

Kandidatuppsats

IT-forensik och informationssäkerhet 180 hp



Sakernas internet - En säkerhetsrisk

En kvantitativ studie om privatpersoners kunskap gällande IoT-enheters säkerhet

Digital forensik 15 hp

Halmstad 2021-06-20

Viktor Andersson och Christer Johansson

Abstract

With the constant growth of units connected to the internet, it's becoming more and more common for private persons to get these units into their homes. With easier accessibility to smart units that can be connected straight to your smart home, and at the same time can make your everyday life easier, may also be the greatest securityrisk of your life.

The focus of this essay is about the internet of things-units (IoT-units) that's considered a large securityrisk. This work is made as a quantitative study about security deficiencies among private persons regarding IoT-units.

The data produced from this work can be used as an answer of what a private person needs to be more vigilant of when it comes to IoT-units, and also what actions the manufacturing industry need to take for the connected community to be secured.

To delve into this, we have chosen to use the methods literature study and a questionnaire study that will be performed to obtain data to answer our questions.

Analysis has been made about what can be seen as an IoT-unit, what security deficiencies there are and then account for how to counteract these risks with help of knowledge.

The result of the answers from the surveys and the picture we have received after a search for a sustainable and a more secure solution is that some knowledge exists, although not to the extent needed.

The conclusion that can be drawn after the analysis of surveys and in the previous research how it should proceed in the current situation is that significantly more resources need to be spent on the right information for the right purpose, when it comes to this important IT-related issue.

Keywords: IoT, Internet of Things, internet-connected devices, smart homes, security risks, security flaws

1. Inledning	4
1.1. Bakgrund - Vad är Internet of Things?	4
1.2. Syfte och mål	5
1.3. Frågeställning	5
1.4. Problematisering av frågeställning	5
1.5. Avgränsningar	5
1.6. Tidigare forskning	6
2. Metod	7
2.1. Metodval	7
2.1.1. Enkätstudie	7
2.1.2. Litteraturstudie	7
2.2. Problematisering av metod	7
3. Teori	9
3.1. Hot mot individens IT-säkerhet	9
3.2. Typer av skadliga IoT hot	9
3.2.1. Malware	9
3.2.2. Phishing	10
3.2.3. Botnet	10
3.2.4. Denial of service attack	10
3.3. Enkätens utformning	11
4. Resultat	12
4.1. Enkät svar	12
4.1.1. Fördelning av respondenter kön och ålder	12
4.1.2. Självskattning av kunskap inom IT	13
4.1.3. Vilka olika IoT-enheter finns i hemmet?	14
4.1.4. Hur många IoT-enheter finns i hemmet?	14
4.1.5. Tidigare kunskap om IoT ?	15
4.1.6. Byte av lösenord på IoT-enheter?	16
4.1.7. Olika lösenord för IoT-enheter?	18
4.1.8. Säkra enheter annat än med lösenord?	19
4.1.9. Om Ja på förra frågan, vad har du gjort för att säkra enheterna?	19
4.1.10. Säkerhet i åtanke vid inköp?	20
4.1.11. Vilka säkerhetsaspekter vid inköp?	21
4.1.12. Fördelning av respondenter jämfört med rikets befolkning	21
4.2. Förstärkning av individens IT-säkerhet	23
4.2.1. Förstärkning av IoT-enheter mot malware attacker	24

4.2.2. Förstärkning mot phishing-attacker	24
4.2.3. Förstärkning av IoT-enheter mot botnet	25
4.2.4. Förstärkning av IoT-enheter mot DDoS attacker	25
4.3. Shodan.io	26
5. Analys	27
5.1. Enkät svar	27
5.2. Internetkällor	28
6. Diskussion	29
7. Slutsats	31
Referenser	I
Bilaga 1 - Enkät	III

1. Inledning

1.1. Bakgrund - Vad är Internet of Things?

Internet of Things, även förkortat IoT, är en kategori hemelektronik som under det senaste decenniet vuxit lavinartat i världen. Den tillväxt av IoT-enheter som pågår spås inte heller avstanna utan fortsätta att öka i antal. Det är svårt att hitta exakta antal av IoT-enheter i världen idag. Olika källor pekar på ett antal mellan 20 och 50 miljarder år 2020[1], så det verkliga antalet kan rimligtvis antas finnas inom det spannet. Antalet IoT-enheter förväntas öka dramatiskt de kommande fem åren vilket innebär att marknaden för IoT-enheter är enorm[2].

Vid sökningar på internet kan konstateras att det inte finns någon direkt standardiserad beskrivning av vad Internet of Things är, förutom att det innefattar uppkopplade saker. Vissa komponenter är vanligt förekommande i saker som definieras som IoT:

- **Sensorer**
Dessa registrerar olika händelser i dess omgivning och samlar in den data den är avsedd för. Det kan vara allt från väder och vind till rörelse.
- **Processor**
För att bearbeta den data som samlats in från sensorerna, så behövs en processor. Denna kan finnas i enheten, i en hub, eller i molnet.
- **Nätverk**
För att enheten skall kunna skicka den insamlade datan till andra enheter eller internet. Nätverk måste inte betyda internetuppkoppling, utan kan vara annan uppkoppling som exempelvis bluetooth.

En IoT-enhet kan även, men måste inte, innehålla ett:

- **Ställdon (aktuator)**
Ställdonets funktion är att fysiskt utföra en åtgärd baserat på bearbetad data, det kan till exempel vara ett brandlarm som ringer för att sensorer i byggnaden registrerat en brand[2].

Genom att beskriva rutinen för ett inbrottslarm som finns i många svenska hem så kan vi visa samspelet mellan ovanstående komponenter. En magnetkontakt (sensorn) sitter på dörrkarmen och känner av att dörren är stängd. Om någon bryter upp eller på annat sätt öppnar dörren bryts kontakten. Sensorn skickar då trådlöst (nätverk) uppgiften om att kontakten brutits till en hub (processor) som sitter i en annan del av huset. Huben är som en spindel i larmnätet och har kontakt med alla sensorer i larmsystemet som magnetkontakter, branddetektorer, kameror etc. Den som öppnat dörren har därefter en viss tid på sig att larma av och därmed avbryta larmrutinen. Om avlarmningen inte sker inom angiven tid så tolkas detta som ett inbrottsförsök och en signal skickas samtidigt från huben till larmcentralen och till en sirén i huset som börjar tjuta (ställdon).

1.2. Syfte och mål

Syftet med den här uppsatsen är att visa hur privatpersoner ser på säkerheten när det gäller Internet of Things. Dessutom undersöker den vilka åtgärder som skulle kunna hjälpa människor att förstå och skydda sig från de risker som är kopplade till IoT-området. Detta arbete skall vara en vägledning för att göra fler personer upplysta om vilka säkerhetsbrister det finns inom IoT samt vad som kan göras för att bekämpa dessa.

1.3. Frågeställning

- Vilken kunskap har privatpersoner kring säkerheten hos IoT-enheter?
- Vilka åtgärder kan vidtas mot bristande säkerhetskunskaper hos privatpersoner angående IoT-enheter?

1.4. Problematisering av frågeställning

Båda våra frågeställningar är öppet ställda för att inte kunna besvaras med ett ja eller nej. Detta innebär att vårt arbete kan få en större bredd när frågeställningarna senare skall besvaras. Frågeställningarna är även ställda på ett sätt som gör det möjligt att få ett resultat från en enkät som skickas ut till privatpersoner. Vi har även begränsat oss till privatpersoner. Utan tydliga avgränsningar kan arbetet växa sig alldeles för stort och bli nästintill ohanterbart vilket kunnat leda till att frågeställningarna blivit svåra att besvara.

1.5. Avgränsningar

I framställningen av detta arbete har vi valt att fokusera på frågan om privatpersoners kunskap inom säkerhet hos IoT-enheter. För att avgränsa detta arbete väljer vi att fokusera på en enkätstudie med specifika frågor riktat mot privatpersoners användning av IoT för att ge en helhetsbild av hur privatpersoner ser på säkerheten inom IoT-enheter. En av frågorna i enkäten är vilken grad av it-kunskap respondenten anser sig ha. Svaren på denna fråga ger en överblick av hur kunniga våra svars personer ser sig själva vara inom i och om högre skattad it-kunskap även visar på ett högre säkerhetstänk.

En annan fråga som hjälper till att avgränsa arbetet är hur många IoT-enheter samt vilka typer av enheter som just nu finns i ett typiskt hem. De frågor vi ställt i enkäten ger arbetet en tydlig avgränsning till att handla om de IoT-enheter som finns i hemmet och hur de som svarar behandlar säkerheten kring sina enheter.

Frågorna som väger tyngst i enkäten handlar om lösenordshantering. Detta är för att få en inblick om privatpersoner har kunskap om att det behöver vara en säkerhetsbarriär mellan IoT-enheter och det uppkopplade hemnätverket.

1.6. Tidigare forskning

En uppsats[3] från Storbritannien behandlar synen på IoT, viktiga begrepp samt fördelar och nackdelar med IoT enheter och dess säkerhet. Storbritannien satsar nationellt på cybersäkerhet genom National Cyber Security Center (NCSC). NCSC är en organisation som stödjer allt från privatpersoner till stora företag, offentlig sektor och cybersäkerhetsexperter i frågor som handlar om cybersäkerhet[4]. De publicerar guider och artiklar för att höja kunskapen inom cybersäkerhet, men ger också råd och vägledning då en incident redan inträffat. Frågor och svar på incidenter inom cybersäkerhet kan hittas på deras hemsida för att öka kunskapen och medvetenheten kring ämnet. NCSC försöker nå ut till så många aktörer som möjligt på detta sätt [4].

I vårt arbete kommer även statistik att analyseras från hemsidor som är relevanta för detta ämne. En studie från Myndigheten för samhällsskydd och beredskap (MSB) med IoT-relaterade risker och strategier[5] har gjorts. Denna studie kommer att vara till stor hjälp för att besvara frågeställningen om vilka åtgärder som kan vidtas gällande bristande säkerhetskunskaper hos privatpersoner och deras IoT-enheter.

Statistik från Shodan[6], som är en databas som aktivt samlar in data från de IoT-enheter som är uppkopplade på internet med bristande säkerhet. Det kan till exempel vara ett fabrikslösenord som inte har blivit ändrat eller att IoT-enheten körs med en gammal uppdatering som innehåller säkerhetshål. En del relevant data för denna studie kommer från Shodan.io. Denna data kommer att presenteras i syfte att sätta de kritiska säkerhetsfrågorna i perspektiv. Hur farligt det egentligen är med osäkra IoT-enheter i hemmet?

2. Metod

De två metoder som kommer att användas i denna uppsats är litteraturstudie samt enkätstudie. I litteraturstudien avser vi använda vetenskaplig litteratur och tidigare utförda studier inom området. Artikelsökningen kommer till stor del att ske via DIVA portal och Google scholar. Enkät kommer att användas där privatpersoner anonymt får besvara frågor gällande IoT-enheter och säkerheten kring dessa.

Den vetenskapliga utgångspunkten för vår uppsats är det tidigare arbetet Internet of Things Securities[3] som tar upp IoT säkerhet. I detta tidigare arbete, som är publicerat i Storbritannien där andra lagar gäller, redogörs för tio utmaningar med IoT säkerheten.

2.1. Metodval

De som valts för detta arbete är både litteraturstudie och enkätstudie. Litteraturstudie där relevant information kring det valda ämnet granskas. Enkätstudie som distribueras digitalt via sociala medier. Varför enkätstudie valdes samt att elektroniska enkäter valdes att skickas ut är för att vi ville samla in information bredare än vad som annars hade kunnat göras med enkäter som delas ut lokalt. Det är en bevisat effektiv metod för att skanna av en större del av en geografisk massa, som sedan kan vara till stor hjälp för att hitta en mer generell syn på problemet (Cohen, Manion & Morrison) [9].

2.1.1. Enkätstudie

Enkäten riktas inte mot någon specifik målgrupp, utan avsikten är att det ska generera ett brett underlag på enkätsvaren för att försöka få en så tydlig bild som möjligt gällande det valda ämnet. Svaren från enkätstudien analyseras. Detta med avsikt att beskriva vilken kunskap respondenterna besitter rent faktamässigt enligt Cohen et al. (2018) [9].

2.1.2. Litteraturstudie

Genom litteraturstudie samlas information från publicerade vetenskapliga artiklar och arbeten. MSB, Statistiska Centralbyrån (SCB) och andra hemsidor som publicerar information och statistik används för att inhämta underlag som ger en bättre överblick av ämnet och möjliggör jämförelser.

2.2. Problematisering av metod

Enkäter är en bra metod för att få en större mängd svar än vid intervjuer. Vi valde att distribuera enkäterna digitalt via sociala medier för att få en stor spridning. Detta kan påverka svaren som kommer in och eventuellt leda till ojämn fördelning av respondenter avseende exempelvis ålder och IT-kunskap. Att en del väljer att inte besvara enkäter och liknande via sociala medier på grund av osäkerhet kring dess ursprung kan innebära att en

del potentiella respondenter missas. Att enkäten försvinner i det stora flödet på sociala medier kan också innebära att många glömmer eller väljer bort att besvara den.

3. Teori

I detta kapitel tar vi upp begrepp som är bra att känna till kring IoT och dess säkerhet genom att beskriva de vanligast förekommande hoten mot IoT-enheter.

3.1. Hot mot individens IT-säkerhet

Definitionen av ett cybersäkerhetshot är en handling vars syfte är att antingen skada, störa, ta över eller stjäla data. Att en IoT-enhet blir attackerad i ett specifikt syfte är för att den dåliga säkerheten bakom dess kod blir ett enkelt byte för hotaktörerna som med en enkel scanning av en aktörs IP-nummer få reda på vilka typer av enheter som möjligen har en osäker port öppen [8].

Att på något sätt ta kontroll över nätverket och dess smarta enheter för någon form av egen vinning är en vanlig typ av attack som görs mot IoT-enheter. I dessa cyberhot finns en mängd listade processer som kan användas för att till exempel ta över ett nätverk med hjälp utav kod som fångslar enheterna till hotaktörens vinning. Att på detta sätt kapa enheter skapar ett botnet. Vad ett botnet är samt vad denna typ av hot kan innebära för en IoT-enhet och dess nätverkssäkerhet förklaras i nästa kapitel. För att lyckas med ett sådant övertagande av ett nätverk kan en phishing-teknik användas för att lura en aktör[8]. Detta kommer också att beskrivas mer ingående i nästa kapitel.

3.2. Typer av skadliga IoT hot

I detta kapitel beskrivs valda hot som kan utgöra en stor risk mot säkerheten inom sakernas internet. Detta är för att klargöra begrepp som används samt att få en djupare förståelse i vad som kan inträffa under en typ av attack eller ett typ av hot mot IoT-enheter.

3.2.1. Malware

Begreppet malware kommer ifrån en kombination av orden malicious och software. Detta är en typ av en skadlig programvara och i gruppen av malware ingår det begrepp som virus, ransomware, internet-maskar och trojaner. Dessa typer av skadlig kod¹ har i syfte att sprida sig, att infektera sina mål samt att på något sätt förstöra, eller eventuellt stjäla, information som kan ses som värdefull [12]. I sin tur kan denna skadliga kod kombineras med att förövarna i frågan tar över enheterna de infekterar så att ett botnät samtidigt bildas.

Denna typ av skadlig malwarekod, som kan hålla företag som gisslan, har enligt Sophos Threat Report 2020 [13] skapat en stor kostnad i form av reparation, underhåll samt utpressningspengar för svenska företag som drabbats av ransomware attacker. Dessa typer av angrepp har kostat de svenska företagen 26 miljoner kronor. Detta är en typ av kod som

¹ Kodning är en färdighet där du tar instruktioner (stegen i en uppgift) och översätter den till ett språk som datorn förstår eftersom datorer inte kommunicerar som människor. De kommunicerar på ett språk som kallas BINÄRT och använder 0 och 1.

krypterar filer och håller dessa som gisslan mot en lösensumma för att låsa upp de infekterade filerna [12]. Utgångspunkten av ett malware förklaras i nästa avsnitt som handlar om hur förövaren lurar sitt mål med att aktivt ladda hem denna skadliga kod.

3.2.2. Phishing

Phishing är en typ av attack som en hotaktör utför mot ett eller flera mål. Vad det innebär att utföra en phishingattack är att en aktör får ett meddelande via exempelvis e-mail med en länk skickad till sig. Hotaktören utger sig för att vara en pålitligt aktör till mottagaren och påstår ofta att den kommer med personlig information som rör mottagaren i fråga. Där uppmanas mottagaren att följa en länk eller ladda ner en fil. När mottagaren trycker på denna typ av länk som erhållits, så innehåller dessa en skadlig programvara. Den skadliga programvaran installeras på enheter och oftast sprids virus via denna bakdörr som hotaktören nu har fått tillgång till. Detta blir nu en ingång för hotaktören att i princip ha full kontroll över ett nätverk om inte säkerhetsåtgärder har vidtagits för att kunna sätta stopp och bekämpa dessa typer av attacker [14].

3.2.3. Botnet

En bot definieras som en typ av programvara och styrs helt automatiskt via kommandon. Därefter arbetar den relativt självständigt utan mänsklig tillsyn. I detta fallet är denna typ av bot i ett botnet ett program som körs i bakgrunden där den inväntar kommandon för agerande [15]. Ett botnet[16] är en typ av nätverk som har blivit kapat och sedan blivit infekterat av skadlig kod. Avsikten med denna typ av attack är att använda enhetens resurser till egen vinning. Denna typ av skadlig kod infekterar enheterna till en grad där förövaren har full kontroll över enheten och dess resurser. En sådan här metod är särskilt användbar när andra typer av resurskrävande attacker ska utföras. Denna process av övertagande bildar ett stort nätverk av övertagna enheter. Dessa bildar ett nät av förslavade enheter, som blir konfigurerade av viruset till att lyssna på kommandon. Dessa kommandon styrs av en enhet som även styr hela havet av bottar.

I en överbelastningsattack är ett botnet en effektiv metod att använda sig av för en belastning från till exempel 30.000 datorer. Dessa når då samtidigt en gemensam slutpunkt exempelvis en webbsida. Denna trafik fyller då nätverket och dess resurser blir överbelastade av alla förfrågningar. Resultatet blir att webbsidan kraschar och eventuellt hålls gisslan av förövaren som på detta sätt kan utöva utpressning. Dessa typer av botnät säljs som stora block och oftast är ett rimligt antal 10.000 slavenheter. Men desto högre antalet är, desto högre är priset för ett nät med bottar [16].

3.2.4. Denial of service attack

En distributed-denial-of-service(DDoS-attack)[17], även kallat överbelastningsattack, är en attack som förklaras i kapitlet ovan om botnet. Attacken utförs genom att rikta resurser för att kapa förbindelsen och överbelasta målets kapacitet för förfrågningar. Denna typ av attack är vanligast när förövaren riktar in sig på att aktivt skada systemet då dessa typer av system oftast inte klarar av en större flod av trafik. Möjligheten finns också att köpa tjänster som

erbjuder denna typ av attack för den som inte har kunskap eller resurser att utföra attacken själv. Det är även svårare att skydda sig mot en DDoS-attack då trafiken som strömmar in från en sådan här attack ses som vanlig datatrafik. I kombination med att trafiken kommer samtidigt och pågår under en längre period får detta oftast förödande konsekvenser [17].

3.3. Enkätens utformning

Enkäten har utformats med både flervalsfrågor och öppna fritextfrågor. I flervalsfrågorna har fasta svarsalternativ getts och i de öppna frågorna har respondenten själv fått formulera sitt svar. Utformningen är tänkt att ge en bred bild av privatpersoners kunskap inom IoT och dess säkerhet.

Arbetets utformning i ålder har gjorts så att personer under 18 år inte får svara eftersom detta är den ålder som anger myndighetsgränsen. Valet är gjort ur ett etiskt förhållningssätt. Vi har delat in åldrarna i fyra olika ålderskategorier. Avsikten är att undersöka om det finns skillnader i kunskap beroende på ålder och då det i utifrån vår andra frågeställning kan finnas olika vägar för att nå ut med åtgärder till olika målgrupper.

Frågorna hur många samt vilka IoT-enheter har du i hemmet formulerades på detta sätt för att respondenten skulle behöva att aktivt reflektera över frågorna. Tanken med dessa frågor är att respondenten skall se sig och sitt hem ur en IoT synvinkel. Detta för att senare kunna svara på frågor om säkerheten kring sina IoT-enheter i hemmet.

Enkätens utformning i sin helhet med kompletta frågeställningar och svarsalternativ kan ses under bilaga 1.

4. Resultat

Här väljer vi att presentera enkäten och de svar vi fått in i text och diagramform samt resultaten av våra litteraturstudier. Analysen av resultaten kommer sedan att presenteras i kapitel 5.

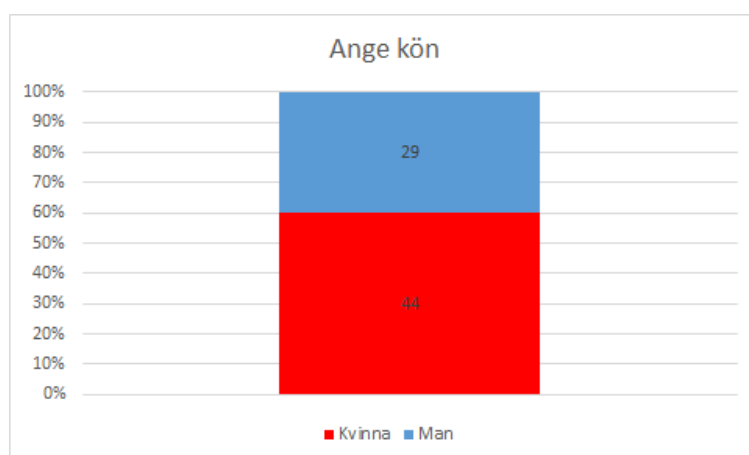
4.1. Enkät svar

Enkäten distribuerades öppet via sociala medier med en önskan att den som svarade på enkäten eller rentav bara såg inlägget skulle dela enkäten vidare. Detta för att enkäten skulle få stor spridning vilket ledde till att vi fick in 73 svar. Vi hade en förhoppning om att kunna få in omkring 80 svar för att få ett bra underlag. Utefter denna förhoppning anser vi 73 svar vara ett bra resultat.

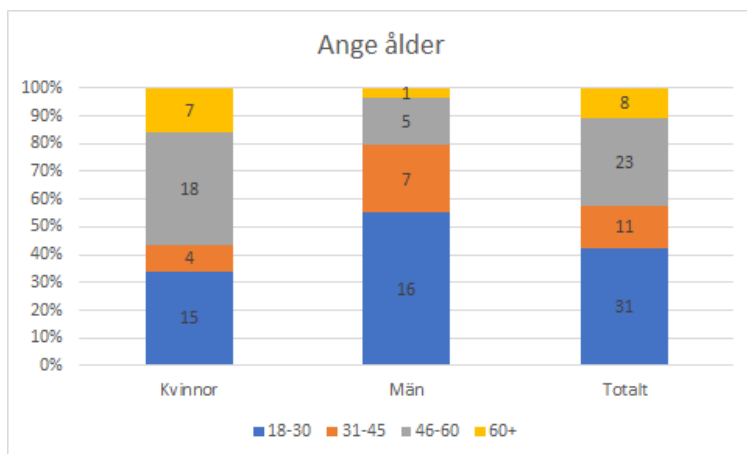
4.1.1. Fördelning av respondenter kön och ålder

Efter att ha sammanställt de 73 inkomna svaren, kan vi se att fördelningen mellan könen är 60% (44st) kvinnor och 40 % (29 st) män (Figur 1). Dessa siffror kan vidare brytas ner för att se hur fördelningen mellan kön och ålderskategorier ser ut (Figur 2).

De svarsalternativ respondenterna fick var följande: 18-30 år, 31-45 år, 46-60 år och 60+ år. 31 st (42%) svarade att de var i spannet 18-30 år och av dessa var 15 st (48%) kvinnor och 16 st (52%) män vilket gör detta till den klart största ålderskategorin av respondenter. Dessutom är detta den kategori med jämnast fördelning av kvinnor och män i enkäten. Inom ålderskategorin 31-45 år var det 11 st (15%) som svarade med fördelningen 4 st (36%) kvinnor och 7 st (64%) män. Gruppen 46-60 år hade 23 st (32%) svarande med en könsfördelning som var 18 st (78%) kvinnor och 5 st (22%) män. Inom kategorin 60+ år är det 8 st (11%) respondenter fördelat på 7 st (88%) kvinnor och 1 st (12%) män vilket gör detta till den minsta kategorin samt den kategori med procentuellt största skillnaden i svaren mellan kvinnor och män.



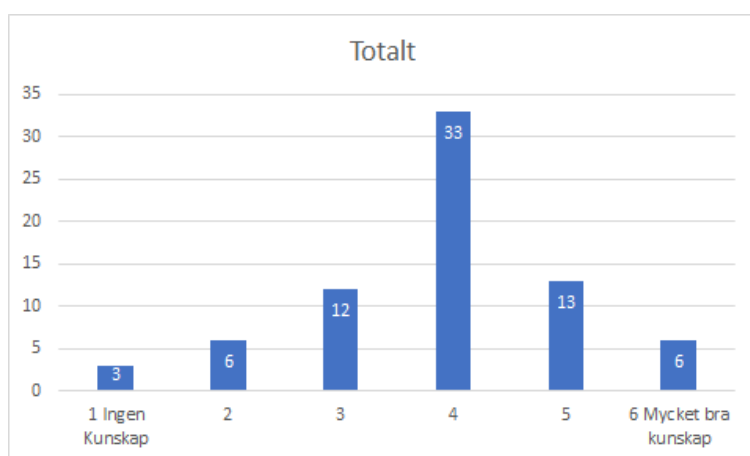
Figur 1 Fördelning av respondenter efter kön i procent med antal i stapeln



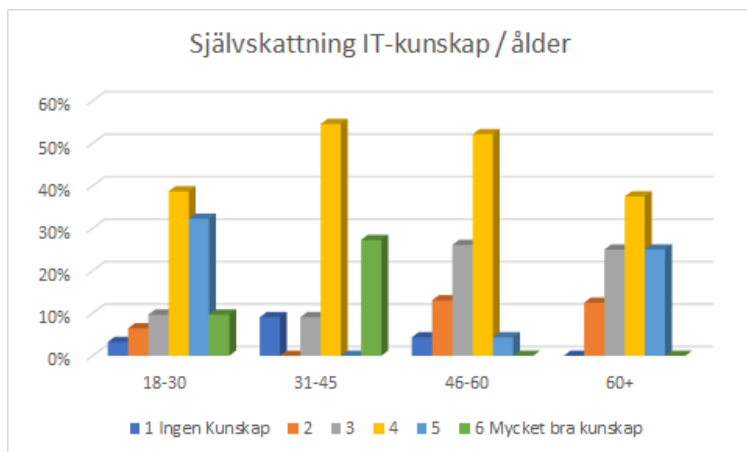
Figur 2 Fördelning av respondenter totalt/ålder samt ålder/kön i procent med antal i tabell

4.1.2. Självskattning av kunskap inom IT

I denna fråga bad vi de svarande att själva skatta sin kunskap inom IT mellan 1-6 där 1 står för ingen kunskap och 6 står för mycket bra kunskap. I Figur 3 kan vi se hur svaren fördelade sig mellan de olika alternativen. I sammanställningen var det alternativ 4 som fick klart flest svar med 45 % (33 st). Mellan alternativ 3 och 5 var fördelningen nära på likvärdig, 17% (12 st) respektive 18% (13 st). Därefter följer alternativ 2 och 6 som fick lika stora andelar av svaren, 8% (6 st). Det alternativ med minst andel svar var alternativ 1 med 4% (3 st).



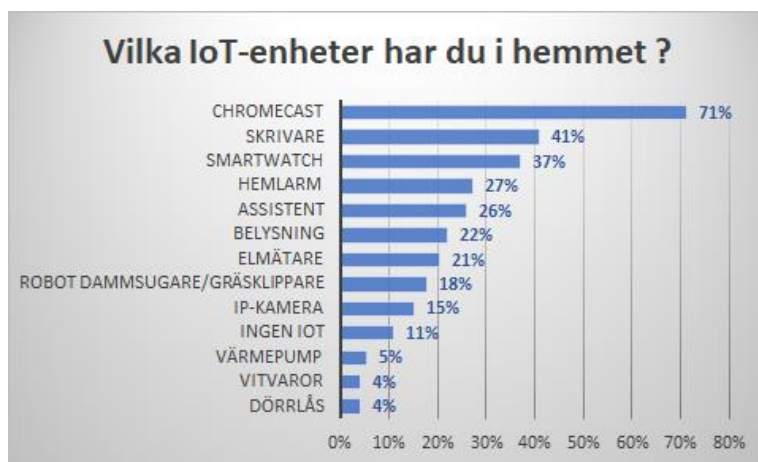
Figur 3 Respondenternas självskattning av IT-kunskap i antal svar per alternativ



Figur 4 Självskattning IT-kunskap / ålder i procent

4.1.3. Vilka olika IoT-enheter finns i hemmet?

Vi ställde frågan "Vilka IoT-enheter finns i hemmet?" och gav ett antal svarsalternativ. Detta för att få en liten överblick över vilka IoT-enheter som är vanligast förekommande i hemmen. Som diagrammet i Figur 5 visar är det chromecast som är överlägset vanligast av de alternativ vi gav. 71% av våra respondenter uppgav att de hade denna enhet i hemmet. Trådlösa skrivare och smartwatches följer därefter och fanns hos 41% respektive 37% av våra svarspersoner. Den kompletta beskrivningen av svarsalternativen till frågan kan ses i enkäten under Bilaga 1.

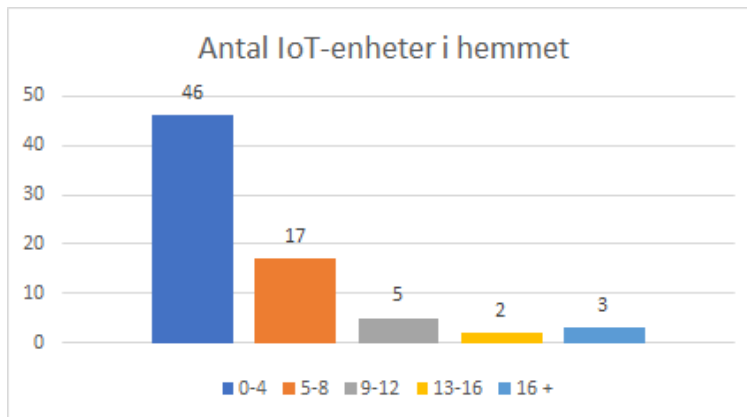


Figur 5 Diagram som visar svaren i procent över vilka IoT-enheter som finns i hemmet, sorterad i fallande ordning

4.1.4. Hur många IoT-enheter finns i hemmet?

När vi frågade hur många IoT-enheter den som svarade på enkäten hade i sitt hem så hamnar mer än hälften av alla svar, se Figur 6, på alternativet 0-4 enheter. 63% (46 st) av alla svarade detta alternativ. 23% (17 st) svarade att de hade 5-8 enheter i hemmet. 7% (5

st) svarade 9-12 enheter, 3% (2 st) svarade 13-16 enheter och slutligen angav 4% (3 st) att de hade fler än 16 IoT-enheter i hemmet.



Figur 6 Visar antalet IoT-enheter i hemmet och antal svar per alternativ

4.1.5. Tidigare kunskap om IoT ?

Här ville vi ta reda på om de som svarade på enkäten sedan tidigare hade någon kunskap om vad IoT var för något. De alternativ som fanns i frågan var följande:

Ja, jag visste vad det var.

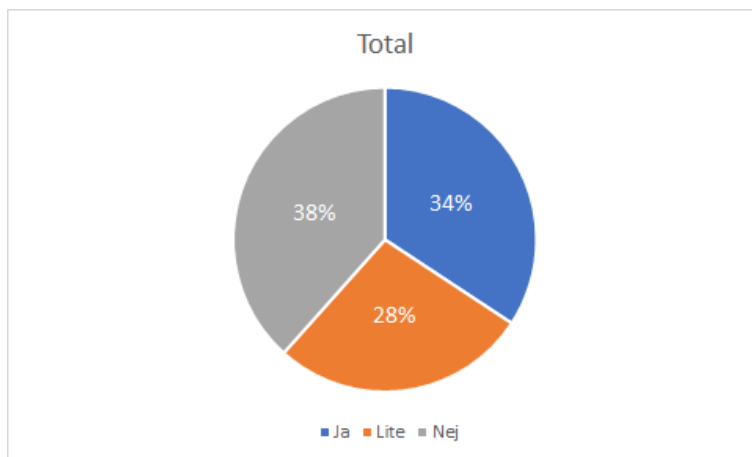
Ja, jag hade hört talas om det, men visste inte riktigt vad det betydde.

Nej, jag hade ingen aning om vad det var.

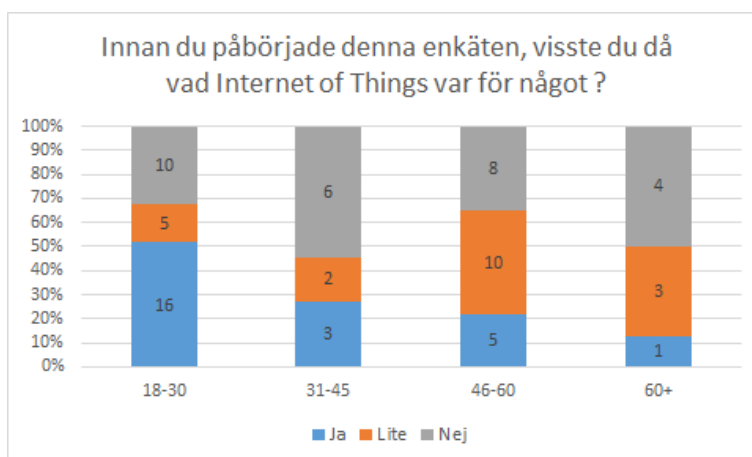
I diagrammet tillhörande Figur 7 har vi förkortat dessa tre alternativ till: ja, lite samt nej.

I Figur 7 ser vi att totalt 62% svarat något av alternativen ja och lite. Detta innebär också andelen hamnar på 38% för svaret att de inte visste innan vad IoT var.

Det vi ser i Figur 7.1 är att den största andelen med svaret ja, 52% (16 st), kom från 18-30 åringarna på denna fråga. De grupper med störst andel som svarade att de inte visste vad det innebar innan var ålderskategorierna 31-45 år och 60+ med 55% (6 st) respektive 50% (3 st) svar på alternativet nej.



Figur 7 Kunskap om IoT före enkät med andel svar per alternativ



Figur 7.1 Kunskap om IoT före enkät med andel svar per ålderskategori

4.1.6. Byte av lösenord på IoT-enheter?

Till frågan om du brukar byta lösenord på dina IoT-enheter fanns fyra svarsalternativ

Ja, byter ofta lösenord (Flera gånger per år),

Ja, byter lösenord ibland (någon gång per år),

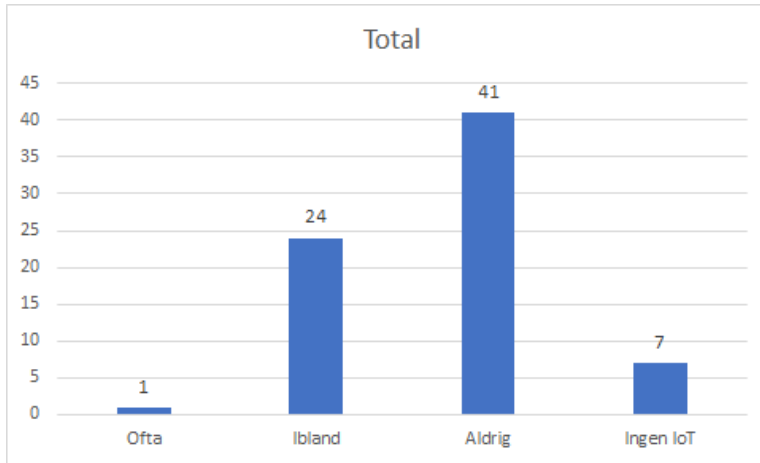
Nej, har aldrig bytt lösenord på mina IoT-enheter,

Jag har ingen IoT-enhet i hemmet.

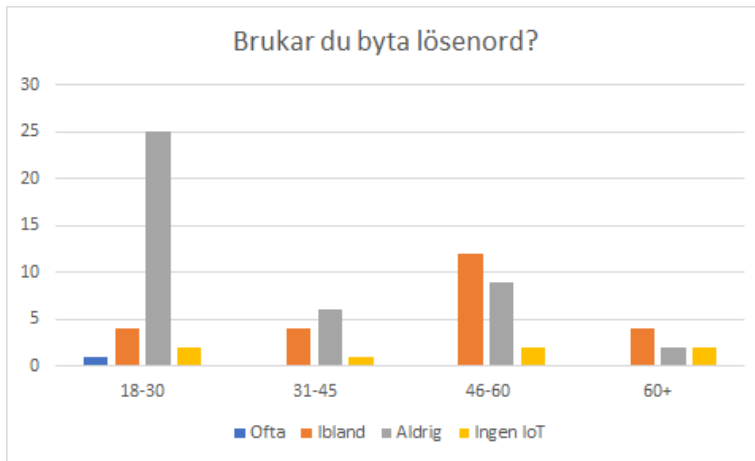
I samma ordning har vi i Figur 8 kallat dessa alternativ för: ja, ibland, nej, ingen IoT.

Det vi ser i figur 8 är att 56% (41 st) har svarat att de aldrig byter lösenord och 33% (24 st) som svarat att de byter lösenord ibland. 10% (7 st) av respondenterna uppger att de inte har någon IoT-enhet i hemmet.

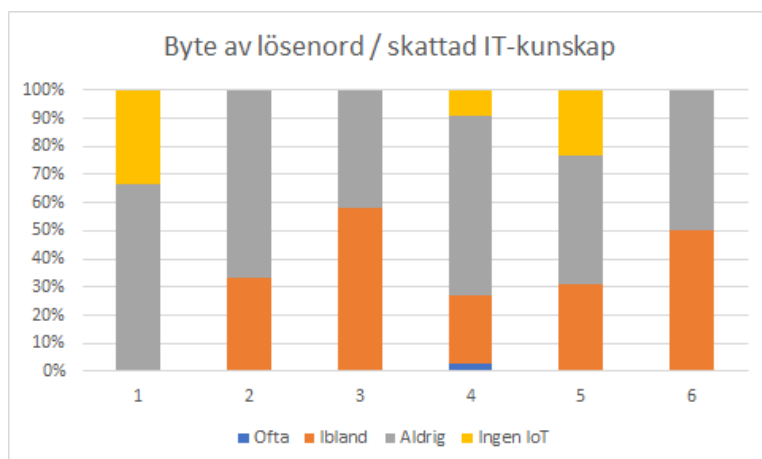
I Figur 9 ser vi på staplarna i diagrammet att respondenterna i åldersgruppen 46-60 är den grupp med högst andel som svarat att de byter lösenord på sina enheter ibland. Dessutom är det väldigt tydligt att åldersgruppen 18-30 år är den grupp med flest antal som svarar att de inte alls byter lösenord på enheterna i hemmet.



Figur 8 Brukar du byta lösenord med antal svar per alternativ



Figur 9 Brukar du byta lösenord på dina enheter med antal svar fördelat per ålder



Figur 10 Visar i procent vilket svarsalternativ som valts baserat på hur respondenten skattat sin egen IT-kunskap

4.1.7. Olika lösenord för IoT-enheter?

Vi bad de som svarat något av ja-alternativen på förra frågan om de brukar byta lösenord att också svara på om de använder olika lösenord på enheterna. Svarsalternativen var:

Ja, olika lösenord på alla enheter,
 Olika till några och samma på resten,
 Nej, Samma lösenord till alla enheter.

Vi har i samma ordning benämnt dessa alternativ med olika, några olika resten samma samt samma i diagrammet Figur 11.

25 personer hade svarat ett jakande alternativ i förra frågan och därmed kvalificerat sig för att även svara på denna fråga. Vi hade dock fått in 43 svar på frågan så efter granskning kunde vi konstatera att 18 personer som svarat "Nej, har aldrig bytt lösenord på mina enheter" ändå svarat på denna fråga. Dessa svar valde vi att ta bort från sammanställningen och bara visa de 25 som svarat jakande på förra frågan.

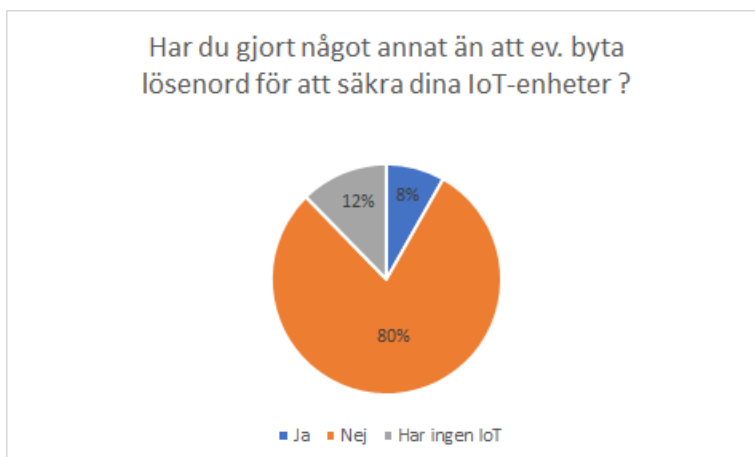
Som kan ses i Figur 11 svarade flest, 52% (13 st), att de har några olika, resten samma när det gäller lösenord på deras IoT-enheter i hemmet. 40% (10 st) svarar att de har olika lösenord på sina enheter och 8% (2 st) uppger att de har samma lösenord på enheterna i hemmet.



Figur 11 Visar andel som har olika eller samma lösenord på sina IoT-enheter med antal svar i stapeln

4.1.8. Säkra enheter annat än med lösenord?

Vi ställde frågan om den svarande har gjort något annat än att eventuellt byta lösenord för att säkra sina IoT-enheter. I figur 12 ses resultatet av hur våra respondenter har svarat. Ja 8% (6 st), Nej 80% (58 st) och 12% (9 st) angav att de ej innehar någon IoT-enhet.



Figur 12 Andel som säkrar IoT-enheter på annat sätt än med lösenord med antal svar i stapeln

4.1.9. Om Ja på förra frågan, vad har du gjort för att säkra enheterna?

Som uppföljning på frågan om enheterna skyddas på något annat sätt än med lösenord ställde vi en öppen fritextfråga där den som svarat ja på föregående fråga kunde ange på vilket sätt den valt att skydda sina IoT-enheter. De svar vi fick in på denna fråga kan ses i punktform nedan. Det vi kan se är att tre av de sex inkomna svaren utgår från att på något sätt separera IoT-enheternas nätverk från nätverket för övriga enheter i hushållet. Två av

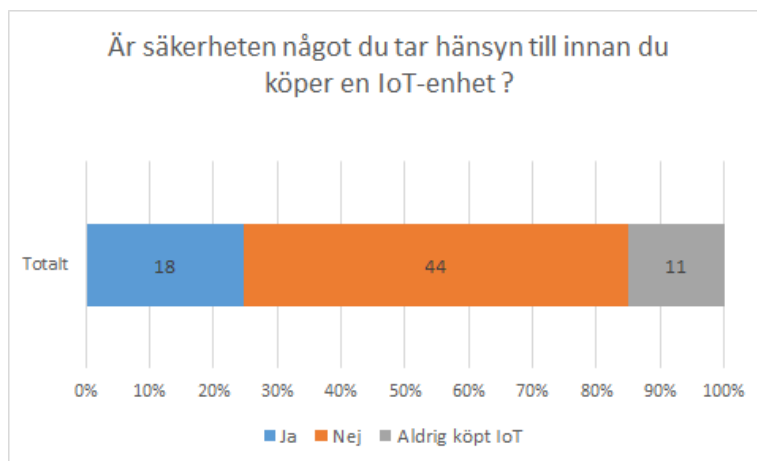
svaren anger att IoT-enheter som inte används kopplas ur eller stängs av för att minska den tid som enheterna är uppkopplade.

- Brandvägg mellan LAN/WAN.
- Olika vlan med olika behörigheter att kommunicera
- Har separat Wifi för IoT enheter på ett VLAN utanför mina datorer.
- Jag har inte igång de enheter som inte används. Såsom exempelvis skrivare och robotdammsugare, dessa kopplas endast in när de ska användas.
- Koppla ur efter användning
- Väljer ett ologisk lösenord

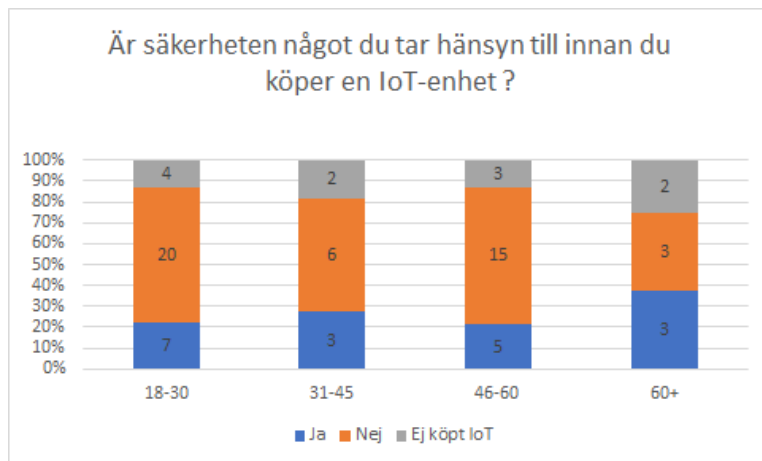
4.1.10. Säkerhet i åtanke vid inköp?

Diagrammet i figur 13 visar att 25% (18 st) svarat att säkerhet är en aspekt i deras inköp av IoT-enheter. Alternativet nej fick 60% (44 st) av de totala svaren och 15% (11 st) uppgav att de aldrig köpt någon IoT-enhet.

I figur 13.1 ser vi att inom åldersgruppen 60+ svarade 38% att de tar hänsyn till säkerheten, vilket innebär att detta är den grupp med högst andel som svarade ja på frågan och när det gäller andelen nej svar är det helt jämnt mellan åldersgrupperna 18-30 och 46-60 där andelen nej svar i båda grupperna är 65%.



Figur 13 Andelen som tar hänsyn till säkerhetsaspekter vid inköp av IoT-enhet, med antal svar i stapeln



Figur 13.1 Andelen som tar hänsyn till säkerhetsaspekter vid inköp av IoT-enhet, fördelat per ålderskategori med antal svar i stapeln

4.1.11. Vilka säkerhetsaspekter vid inköp?

Vi ställde den öppna frågan "Om Ja på förra frågan, vad brukar du tänka på vad gäller enhetens säkerhet? (Valfritt)". Svarefrekvensen var 50%, så av de 18 personer som svarade ja på föregående fråga fick vi följande nio svar:

- Huruvida en enhet behöver vara IoT eller inte.
- Köper inga okända märken, annars ingen speciell tanke om säkerhet vid köp av IoT-produkter.
- Att alltid byta default password och separera dessa från vanliga nätet där jag har mina datorer/mobiler.
- Molnsäkerhet
- Kostnaden
- Brandvägg etc
- Minskad risk för hackning
- Virussydd
- Vill inte att andra ska få åtkomst till det jag gör. Vill heller inte att mina apparater ska kunna hijackas av botnet och användas för exempelvis DDoS-attacker

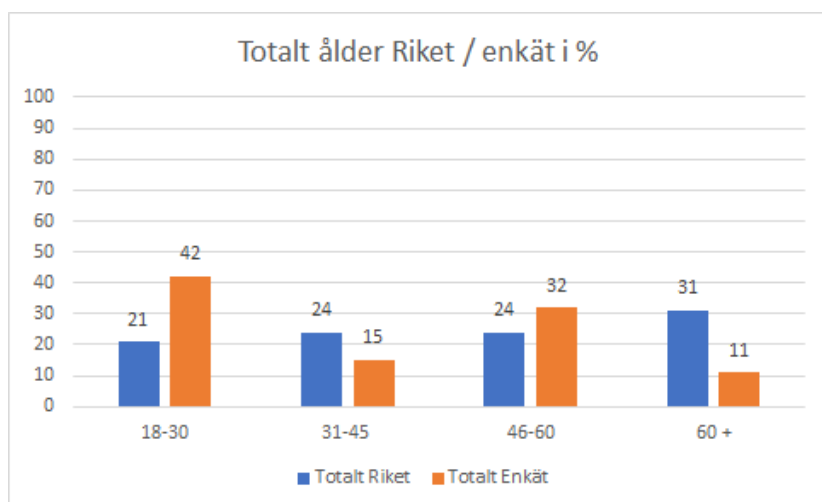
Alla de nio som svarade på denna fråga hade på tidigare frågan om IT-kunskap graderat sig själva mellan betyg 4 och 6. Fyra av dessa hade satt betyg 4, tre stycken betyg 5 och två stycken betyg 6. Tittar vi på åldersfördelningen bland de som svarat här så var det två personer ur vardera ålderskategori 18-30, 31-45, 46-60, och tre personer i åldern 60+.

4.1.12. Fördelning av respondenter jämfört med rikets befolkning

För att se vilken bäring resultatet av vår enkät har gentemot riket så har vi gjort en jämförelse mellan hur fördelningen av våra respondenter ser ut och hur fördelningen ser ut i Sveriges rike. Datan som gäller riket har vi hämtat från statistikdatabasen hos Statistiska centralbyrån [20] och är data som var aktuell per 31 december 2020. 100% i den totala

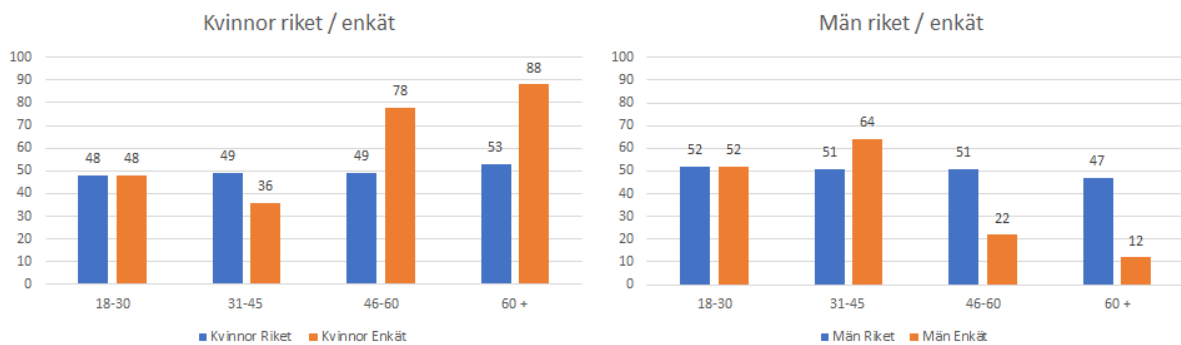
delen avseende riket är alla över 18 år. Detta för att jämförelsen skall bli relevant då alla svar i enkäten kommer från personer över 18 år. Därför har vi exkluderat den del av svenska befolkningen som understiger 18 år.

I Figur 14 kan vi se att när det gäller det totala antalet respondenter oavsett kön, så är det två ålderskategorier där enkät och rike ligger relativt nära varandra. Det är mellankategorierna 31-45 som skiljer 9% samt 46-60 som skiljer 8%. Ytterkategorierna däremot har en betydligt större differens mellan respondenterna och befolkningen. Kategorin 18-30 har en differens på 21% och kategorin 60+ har en differens på 20%. Det vi ser när det gäller den totala jämförelsen är att vi nådde större andel personer i åldrarna 18-30 samt 46-60 i jämförelse med befolkningens andel i motsvarande åldrar. Och omvänt nådde vi mindre andel personer i åldrarna 31-45 och 60+ än rikets motsvarande andel. Möjligtvis hade siffrorna för kategorin 60+ skulle kunna vara mindre om vi begränsat den till exempelvis 60-90 år, eller kanske till och med 60-80 år, eftersom i siffrorna från scb är alla från 60 till 110+ inräknade och vi högst troligt inte hade någon svarande över 80. Detta skulle dock troligtvis endast ändrat siffrorna marginellt och inte påverkat resultatet nämnvärt.



Figur 14 I diagrammet visar orange staplar totala fördelningen av enkätens respondenter, och blå staplar visar hur fördelningen av ålderskategorin ser ut i riket. Källa: Statistikdatabasen SCB [20]

I nästa steg bröt vi ner resultatet av jämförelsen till hur fördelningen ser ut per kön inom ålderskategorierna bland våra respondenter gentemot motsvarande fördelning i riket. Detta visar tydliga resultat att vi både bland kvinnor och män nådde helt eller relativt jämnt med kategorierna 18-30 samt 31-45. I kategorin 18-30 var det helt jämnt med fördelningen gentemot riket, medans 31-45 skiljde 13% med övervikt riket hos kvinnor och övervikt respondenter bland män. De stora differenserna mellan såväl kön som gentemot rikets fördelning ser vi i de två äldsta ålderskategorierna. Här var det kvinnorna som totalt dominerade bland våra svar, något som syns tydligt i diagrammen i figur 15. För dessa kategorier så är differensen 29% mot riket i kategorin 46-60 år och i kategorin 60+ så är motsvarande differens hela 35%.



Figur 15 Diagrammet till vänster avser kvinnor och det högra avser män. Orange staplar visar fördelningen av enkätens respondenter och blå staplar visar rikets fördelning i kön / ålderskategori i procent. Källa: Statistikdatabasen SCB [20]

4.2. Förstärkning av individens IT-säkerhet

I detta kapitel kommer åtgärder redovisas för att beskriva hur säkerheten kan förstärkas för att få en säkrare miljö för IoT-enheter.

Ett lösenord är lättast att komma ihåg om det är samma överallt. Helst kort och enkelt att komma ihåg och gärna också något man kan relatera till som namn på närstående personer eller dylikt. De 200 mest vanliga lösenorden som är presenterade på NordPass, som är en hanteringstjänst för lösenord, visar i sin 2019-2020 rapport[10] de sämsta lösenorden som upptäckts bland läckta lösenord. Detta innebär att de även är de sämsta lösenord att använda i sitt system för att säkra det. Rapporten visar också på att det skulle ta under en sekund för ett program som knäcker lösenord att knäcka de flesta lösenord i denna top 200 lista.

Den absolut viktigaste punkten för att skydda sina enheter och sitt nätverk är lösenord. Ett lösenord symboliserar en nyckel för att logga in i system. Nycklar har i huvuduppgift att vara så unika som det bara går för att förhindra inbrottstjuvar och andra med onda avsikter från att kunna ta sig in utan tillgång till rätt nyckel. Lösenord fungerar på exakt samma sätt fast i nätverk och på enheter. Att ha lösenordet till ett specifikt system innebär detsamma som att ha nyckeln till att komma åt information, detta oavsett om det är olagligt eller inte. Det gäller även den unika aspekten av ett lösenord och nycklar[10]. Användning av samma nyckel till ett flertal olika dörrar ökar säkerhetsrisken. Detta gäller också lösenordshantering, att aldrig ha samma lösenord pga att den unika aspekten ska höja säkerheten.

För att skydda sig och förstärka sin lösenordshantering finns några punkter att ta hänsyn till, som att kontrollera om det använda lösenordet kan anses vara ett säkert lösenord. Vad ett säkert lösenord innebär redovisas av Avast[11], i deras rapport om starka lösenord. Där beskrivs att ett starkt lösenord ska innehålla en minst 15 tecken lång kombination med både bokstäver, siffror och specialtecken. I denna rapport nämns även att inga tangentbordskombinationer är bra alternativ. Detta menas med att ta bokstäver som sitter intill varandra som till exempel "qwerty". Något som även tas upp är att inte vara personlig i sitt lösenord som att till exempel ha ett namn på någon eller något som befinner sig i ens

närhet. Ett sätt att skapa enkla men säkra lösenord är genom att sätta samman ord som inte har någon sammankoppling och dessutom innehåller specialtecken till en mening[11].

4.2.1. Förstärkning av IoT-enheter mot malware attacker

Att skydda sig mot malware kan vara en svår uppgift då många olika variabler spelar in. Flera säkerhetsåtgärder måste därför kombineras för att skapa en säker miljö för sina IoT-enheter. Spridningen av malware kan därmed bero på både tekniska och beteendemässiga beslut från användaren [12]. Till stor del är information om malware väldigt viktig när det kommer till att hantera det. Exempel på sådan information är vart malware kan gömma sig, hur skadligt malware kan vara samt vad begreppet virus innefattar. Uppfylls dessa tre punkter så höjs sannolikheten att användaren tar säkerhet på internet på allvar.

För att skydda sig mot malware specifikt kan användaren tänka på vissa punkter som att underhålla alla system man använder i hemmet uppdaterade till den senaste versionen. Detta är just pga att uppdateringar oftast innehåller säkerhetsbrister som har blivit lagade så att man behöver uppdatera sitt system för att få dessa lagade.

Vad som också är bra att införskaffa är antivirusprogram från en pålitlig källa eller återförsäljare. Dessa typer av program kan känna igen mönster av skadlig kod som kallas för signaturer som är rapporterade och lagrade som antivirusprogrammen känner igen som sedan resulterar i att attacker kan stoppas direkt[12]. Dock finns i vissa fall nyare typer av attacker där antivirusprogrammen inte har blivit uppdaterade som i viss mån hade kunnat sprida sig utan att upptäckas av ett virusprogram. Dock så hålls dessa protokoll ständigt uppdaterade för att upptäcka de allra senaste kända varianterna av skadlig kod.

Det är viktigt att vara försiktig och tänka kritiskt kring länkar man får skickade till sig samt program som man laddar ned. Att dessutom endast öppna länkar man vet med all säkerhet kommer från en betrodd källa ger ett starkt skydd mot malwareattacker. Ett sätt att identifiera om meddelandet är från en säker källa eller inte är att granska avsändarens mailadress[12].

Att inte använda sig av ett administratörskonto aktivt när man är inloggad på ett system om det verkligen inte är nödvändigt minskar risken om system blir kapade. Att inte få åtkomst till administratörskontot kan också bidra till att just sådana här attacker upptäcks snabbare [12].

4.2.2. Förstärkning mot phishing-attacker

Att skydda sig från en phishing attack innebär ett liknande förfarande som i kapitlet om att skydda sig mot malware. Det gäller det att försöka vara observant och även här kommer ett antivirusprogram att vara ett bra skydd. Dock så kommer antivirusprogrammet i vissa fall tro att det är användaren som har accepterat programmet som är bifogat i en phishing-attack, när användaren trycker på till exempel en bifogad fil som i själva verket är en skadlig kod [14].

En phishing attack blir svårare att utföra om användaren observant. En typ av attack som riktar sig mot att försöka lura användaren att öppna länkar som hamnar i mejlkorgen brukar

oftast vara felstavat på något sätt. Det ska likna en domän eller ett företag så mycket som möjligt. Ett exempel kan vara att ett mail kommer från en adress som är skriven med dubbla bokstäver som till exempel faktura@blockett.se där det i själva verket ska komma från en domän vars mailadress är faktura@blocket.se. Detta gäller även hyperlänkarna på webbsidor där risken att trycka fel kan få förödande konsekvenser [14]. Att bedöma trovärdigheten i dessa typer av email samt på diverse webbplatser kan vara väldigt svårt men kunskap och att vara uppmärksam bidrar till ökad säkerhet mot phishing-attacker.

4.2.3. Förstärkning av IoT-enheter mot botnet

För att skydda sig mot en etablering av ett botnät kan vara mycket svårt då antivirusprogram i vissa fall tror att programmet som körs är ett program användaren godkänt. Det är också svårt att upptäcka om ens enhet har blivit drabbad av ett övertagande som gör denna till en bot. Det är inte alltid användaren reagerar på att dess enhet kräver mer resurser eller att enheten går långsammare än vanligt. Därför är det viktigt, som i tidigare förklaring om vad ett botnet är, att vara uppmärksam på enhetens resursanvändning [16].

Med anledning av detta är underhåll en väldigt viktig del i att förhindra övertagande samt intrång som kan göra enheten till en del av ett botnät. Att alltid ha den senaste uppdaterade versionen för att förhindra att säkerhetshål utnyttjas för att ta kontroll över enheter. Det är också viktigt att ha uppsikt över enheternas konfiguration samt hur energikrävande de brukar vara[16].

Om enheternas resursanvändning ökar drastiskt, är detta ett utmärkt tillfälle att kontrollera enheterna för skadlig kod. Det bästa i ett sådant fall är att fabriksåterställa enheterna och installera om programvaran vilket oftast leder till att botnätets konfigurationer försvinner. För bästa säkerhet borde en återställning på alla enheter göras rutinmässigt då skadlig kod eventuellt kan finnas på flera enheter i hemmet [16].

4.2.4. Förstärkning av IoT-enheter mot DDoS attacker

Det är svårare att skydda sig mot en överbelastningsattack eller en DDoS-attack som det kallas. Denna typ av attack försöker att överbelasta sitt mål med förfrågningar och data som anses som en vanlig förfrågan. När detta görs med en stor mängd enheter samtidigt överbelastas oftast systemet. Hur ska man då försöka skydda sig mot vanlig trafik? Det är en väldigt komplex fråga men det absolut bästa sättet att skydda sitt nätverk mot förfrågningar, att försöka dela upp det successivt. Detta innebär att nätverket delas upp i olika block vars regler sätts så att inte all trafik får strömma fritt och förfrågningar inte kan nå utifrån det öppna internet. Brandväggar sätts upp för att blockera vissa typer av trafik som då lättare kan regleras. Program som validerar protokoll är ett bra hjälpmedel då spärrar kan sättas för att kontrollera om en viss typ av trafik i viss mängd är validerad mot reglerna som har satts [17].

4.3. Shodan.io

Shodan.io är en databas[6] som aktivt samlar in data på alla internetuppkopplade IoT-enheter som inte har någon direkt säkerhet kopplat till sig. Dessa enheter som kommunicerar med omvärlden över tcp/ip eller udp/ip[18] blir synliga via denna sökmotor. Om det finns kända problem med informationssäkerhet och exponeringar taget ifrån CVE[19] som också är en sökbar motor, bör dessa säkerhetsbrister åtgärdas. På Shodan.io kan man filtrera ut en rad olika parametrar som möjliggör för vem som helst att ta fram till exempel IoT-enheter vars lösenord är "1234" eller ett "default password" som är känt från en tillverkare. Det går även att söka efter webbkameror och andra övervakningsenheter som är sårbara. På det sättet görs dessa tillgängliga och möjliggör för vem som helst att ta sig in i denna typ av enhet[19].

Sökningar gjordes på shodan.io i utbildningssyfte för att ta fram hur det ser ut i Sverige gällande den osäkra IoT enheter. Nedan redovisas svaren från shodan.io data som är taget 06/05/2021[Figur 16].

Sökningen country:SE "default" genererade totalt 46279 resultat. Detta indikerar att dessa enheter fortfarande har någon form av ursprunglig säkerhetsinställning som inte ändrats. Sökningen visar även vilka städer som har flest osäkra enheter. På samma sida som visas i Figur 16 finns det även en högerspalt med IP nummer. Där visas all information om var och en av de 46279 sökbara resultaten från denna sökning. Vi har valt att inte ta med denna typ av data då den kan anses som känslig. Detta då den visar både operatör, ip nummer, klockslag på när information senast är uppdaterad samt i vissa fall vilket företag som enheten ägs av[19].

TOTAL RESULTS

46,279

TOP COUNTRIES



Sweden	46,279
--------	--------

TOP CITIES

Stockholm	28,486
Göteborg	1,976
Malmö	935
Borås	690
Uppsala	524

Figur 16 Sökning på shodan.io under country:SE "default" vilket genererar svenska enheter vars ursprungliga säkerhets-kopplad data inte är ändrat

5. Analys

5.1. Enkät svar

Här analyserar vi och jämför de resultat vi fått i vår enkät som beskrivits i förra kapitlet.

Ett resultat värt att uppmärksamma från vår enkätundersökning är att 40% av våra svars personer inte visste något om vad Internet of things var innan enkäten. Dessutom visar den att 56 % aldrig byter lösenord på sina IoT-enheter. Konsumenterna köper IoT-enheter, det är tydligt med tanke på utvecklingen av IoT-enheter i världen. Men vad många konsumenterna inte riktigt verkar tänka på är att dessa också bör skyddas mot intrång. Om 40 % inte vet vad IoT är, så vet ju dessa personer förmodligen inte heller att dessa bör skyddas och än mindre hur det skall göras. Då ett starkt och unikt lösenord är ett bra sätt för att skydda sig och sin enhet så är det trots allt glädjande att 40 % av de som har bytt lösenord på sina enheter i enkäten uppger att de använder olika lösenord på de olika enheterna. 56 % uppger att de har olika lösenord på några enheter och samma lösenord på resten vilket ändå får ses en aning positivt då det är bättre än att aldrig byta lösenord eller ha samma lösenord på alla enheter.

Även om lösenordsbyte är det eventuellt enklaste sättet att skydda sin enhet, så finns det mer att göra för att säkra upp skyddet. Att placera sina IoT-enheter i ett separat nätverk är ett alternativ. Det är också detta alternativ som var det vanligaste bland de som svarade på frågan vad de vidtagit för säkerhetsåtgärder utöver att byta lösenord. Att 80 % av våra svars personer svarade att de inte gjort något annat än att eventuellt byta lösenord är kanske i sig inte så konstigt då dessa övriga åtgärder ofta kräver viss kunskap för att utföra. Detta bekräftas i viss mån när vi tittar närmare på de tre personer som svarat att de separerar IoT-enheter från vanliga hemnätverket. Då visar det sig att alla dessa tre på frågan om hur de skattar sin kunskap inom IT gett sig själva betyget 6 vilket innebär att de anser sig ha mycket stor kunskap. Två av dem är mellan 18-30 år och en är mellan 31-45 år. Dessa uppgifter speglar också svaren på frågan om egenskattad kunskap inom IT, där åldersgruppen 31-45 år var de med störst andel som svarade betyg 6 och åldersgruppen 18-30 år hade störst andel som gav sig själva betyget 5.

Det är också intressant att det på frågan om respondenten brukar byta lösenord på sina enheter var det en överlägsen dominans av personer i åldersgruppen 18-30 år som svarade att de inte brukar byta. Det var även en grupp som stack ut i svaret att de ibland (någon gång per år) byter lösenord och det var respondenterna i ålderskategorin 46-60 år. Endast en person svarade att den byter lösenord ofta (flera gånger per år) på sina enheter. Det var en person i åldern 18-30 år, och denna person hade skattat sin IT-kunskap med betyget 4.

Vad som blir intressant med att jämföra svaren på hur ofta våra svars personer byter lösenord med hur de skattat sin IT-kunskap är att bland de sex personer med högsta självskattade betyget 6 så byter 50% lösenord ibland och 50% byter aldrig. Endast i den grupp som skattat sig med betyg 3 är det fler som svarat att de byter ibland än de som svarat att de aldrig byter lösenord. I betygsgrupperna 1, 2 och 4 är andelen som inte bytt

lösenord omkring 65%. I betygsgrupp 5 är denna andel lägre med 46% som aldrig bytt lösenord och 30% som byter ibland.

5.2. Internetkällor

Som tidigare nämnts i arbetet är lösenord samt dess hantering en viktig del av att hålla en IoT-miljö så säker som möjligt. En jämförelse mellan enkätsvaren i detta arbete samt NordPass rapport om vanligaste lösenord 2020[10] visar med stor sannolikhet att det finns liknelser. Dessutom finns en stor risk att personer inte bryr sig eller har kunskap om hur viktigt det är med lösenordshantering. Detta är en viktig del i säkerheten och kan också vara avgörande till att ett systems säkerhetsnivå höjs avsevärt. Framför allt om det görs med tanke på att de ska klara av kriterierna som Avast[11] beskriver om vad ett starkt lösenord ska innehålla. När Sveriges samhälles IoT-användning höjs avsevärt med hela 90% ifrån föregående år som en undersökning Sentor har gjort,[21] är det viktigt att säkerhetstänk måste fokuseras mer på.

Analysen som gjorts med data hämtad från Shodan visar att 46279 synliga och internetuppkopplade enheter med oförändrade säkerhetsinställningar finns i Sverige i dagsläget. Samtidigt är ett av de vanligaste hoten bland IoT-enheter att det inte finns något ändrat fabrikslösenord på enheten vilket gör dessa till en stor risk. Speciellt privatpersoners tänk på att ändra eller att ha olika lösenord på sina enheter är ett viktigt steg. Resultaten i vår enkät visar att så inte är fallet i ett typiskt svenskt hem idag. Denna säkerhetsinsikt måste normaliseras för att aktivt göra det svårare för förgripare att lyckas med dessa attacker.

6. Diskussion

Enkätundersökningen visar att ett högre säkerhetstänk inom IoT är vanligare hos personer med hög kunskap jämfört personer med lägre kunskap. Detta kan ses som hur en utveckling i hur samhällets säkerhetstänk borde se ut för att nå en säker IoT-miljö. Trots att det procentuellt finns ett högre säkerhetstänk bland personer med hög kunskap i ämnet betyder det inte att de alltid gör rätt. En del av svarspersonerna gör någon form av analys på enheter innan köp, ändrar fabrikslösenord, underhåller enheterna mm. Att tänka utanför säkerhetsboxen är ett sunt tillvägagångssätt. Att alltid vara uppdaterad på de senaste metoderna från IT-säkerhetsbranschens är också ett bra sätt för att få sin IoT-miljö att vara så säker som möjligt.

Enkätundersökningen har varit användbar för att få en inblick i vilka kunskapsbrister det finns hos privatpersoner gällande IoT-enheter samt vilka åtgärder som kan vidtas gällande dessa kunskapsbrister. För att förtydliga svaren på våra frågeställningar anser vi att vår enkätstudie har varit till stor hjälp för att få en bild av kunskapen hos privatpersoner och deras syn på en säker IoT-miljö. Enkäten har även varit till stor hjälp då denna har jämförts med populationsstatistiken som är redovisad från SCB [20].

Vårt mål med enkäten var att nå en bred population med svar från alla våra åldersgrupper, vilket vi i stort anser att vi lyckades med. Även om det vore önskvärt att andelen svarande i de olika åldersgrupperna överensstämde exakt med respektive andel i rikets population. Det kan också vidare diskuteras angående frågor som hade kunnat anses vara bra att ställa som till exempel vart i landet den som svarar befinner sig. Detta för att få en klarare bild av den exakta positionen. För att lyckas med detta så anser vi att vi hade behövt nå ut och täcka ett betydligt större omfång i svar och kanske även mer riktade enkäter. Detta är något som kan tas med och ses som ett förslag till vidare forskning.

Efter analys av resultat som visar bristande säkerhetskunskap bland privatpersoner gällande hantering av sin IoT-miljö gäller det att flera aktörer tar detta på större allvar. Efter detta arbetes datainsamling anser vi även att fler krav gällande säkerheten bakom IoT-enheter borde läggas på tillverkare. Något som skulle leda till att IoT-enheters standardsäkerhet ökar. Detta är en finansiell fråga som gör att många leverantörer av diverse IoT-enheter inte lever upp till den säkerhetsstandarden vi anser att de borde göra. Statistik tagen från Sophos[22], visar på en kostnad på över 12,5 miljoner för att hantera ransomwareangrepp. Denna kostnad hade troligen varit lägre med en högre säkerhetsstandard.

En åtgärd för högre standard kan då vara krav på regelbundna mjukvaru- och/eller säkerhetsuppdateringar från tillverkare för att få tillverka och sälja sin produkt. Detta borde vara en standard av säkerhetsprincip, lika självklart som att det finns krockkuddar i en bil. En annan standard på samtliga IoT-enheter är lösenordsbyte innan första användning. Att privatpersonen måste byta lösenord på enheten vid installation. Detta byte eller generering av lösenord skulle på detta sätt fungera som en "på-knapp" för att enheten skulle fungera. Lika självklart som att ström måste tillföras IoT-enheten för att denna ska fungera. Problemet att tillverkare kapar detta lager för att göra produkten billigare att sälja, visas i Shodans statistik[Figur 16] då det är alldeles för många enheter som är åtkomliga för vem som helst.

Även kommunala och nationella tjänster borde ses som en standard i säkerhet från samhällets sida. Detta för att ha någonstans att vända sig om problem uppstår med teknologi och dess säkerhet. Kontaktmöjligheter finns via många återförsäljare men detta kan ses som en jobb process om något skulle krångla med tekniken.

De kommunala tjänsterna kunde innebära någon form av samarbete med exempelvis hemtjänst för att nå äldre som behöver hjälp men också en kontaktlinje så att andra kan nå den. En kommunal tjänst skulle då kunna arbeta närmare rent fysiskt mot den som behöver hjälpen. Med detta följer dock andra frågor som gäller integritet och övrig säkerhet då någon exempelvis skall hjälpa till med lösenordsbyte. Dessa frågor måste tas i beaktande och lösas med bland annat policys och riktlinjer för personalen. En effekt av detta förslag skulle kunna bli ett högre säkerhetstänk än idag. Utsätts personer regelbundet för problemlösningar så ökar förmodligen också till slut deras säkerhetskunskap. Denna kunskap kan sedan resultera i mindre problem och högre nivå av säkerhetstänk vilket skulle minska riskerna kring IoT.

Vi anser också att någon form av bemannat nationellt IT-center för att tillgodose privatpersoners behov av hjälp med t.ex lösenordsbyte, installation, underhåll mm bör införas. Denna nationella tjänst skulle då kunna vara avsedd för den som kan utföra åtgärden själv på enheten, men som behöver lite guidning i själva förfarandet. Det här är såklart också en kostnadsfråga men tillsammans med högre säkerhetsstandard från tillverkare så skapas möjligheten till en betydligt högre säkerhet.

Dessa kommunala och nationella tjänster borde även aktivt tillhandahålla privatpersoner med diverse broschyrer och reklam samt annonsering för att betona och verkligen påpeka vikten av att t.ex ha säkra lösenord som byts till den standard som ses som mest lämplig. Då elever i skolan ofta får en egen bärbar skoldator redan i första klass och för att resultaten i vår enkät visar att det är personer i åldersgruppen 18-30 som är sämst på att byta lösenord på sina enheter ser vi det som en stor säkerhetsrisk. Vårt förslag på åtgärd kring detta är att utbildning inom IT-säkerhet införs i skolan för att lära elever vikten av säkerhet och hur de skall skydda sig. Med start tidigt i grundskolan för att sedan följa eleverna genom årskurserna upp till skolans slut, som i många fall är studenten. För att skolan sedan aktivt skall kunna jobba med detta måste det också skrivas in i läro- och kursplaner för att få ett ämne motsvarande, eller kanske inom hem och konsumentkunskap och med lärare som kan och förstår ämnet .

7. Slutsats

En slutsats som kan dras efter en analys av privatpersoners kunskap gällande säkerheten hos IoT-enheter är att åtgärder måste vidtas. Speciellt information gällande hur man ska gå tillväga för att säkra sin IoT-miljö samt hur man skall gå tillväga ifall något inträffar.

I ett typiskt svenskt hem är det vanligt att förekommande med ett flertal IoT-enheter. Samtidigt visar vår enkät att 40 % av de som svarade inte visste vad IoT var för något. Att inte veta vad IoT är innebär att dessa enheter oftast inte heller aktivt skyddas. Detta bekräftas via svaren på frågorna som handlar om lösenord och övrig säkerhet. I vårt arbete har vi tagit fasta på att den absolut viktigaste punkten för att skydda sina enheter och sitt nätverk är lösenord[10]. Kopplat till detta visar enkätsvaren att 56 % av respondenterna aldrig bytt lösenord på sina IoT-enheter. Lösenordet kan ses som nyckeln till ytterdörren i ditt IT-hem. Därför är det av största vikt att använda unika lösenord för att skydda sina enheter och sitt nätverk[10]. 80 % av våra svarspersoner har inte gjort något annat än att eventuellt byta lösenord. Den vanligaste åtgärden bland de som gjort något annat är att placera IoT-enheterna i ett separat nätverk.

Som tidigare nämnts är lösenordet en mycket viktig del i säkerheten kring IoT-enheter. Som vår enkät visar, så finns det brister i lösenordshanteringen hos ett flertal av våra respondenter. Anledningar till detta kan antas vara okunskap, bekvämlighet och brist på information. Detta är anledningar som hackare och andra med onda avsikter utnyttjar för att komma åt enheter och annan information som finns i nätverket. Uppgifter om enheter med svag eller obefintlig säkerhet kan hittas i öppna databaser som till exempel Shodan. Detta faktum gör det tydligt att var och en måste skydda sina enheter. För att förstärka säkerheten behöver åtgärder vidtas från flera olika aktörer på marknaden och i samhället, men även hos individen själv.

Tillverkare måste ta sitt ansvar för att deras produkter håller en hög standardsäkerhet redan från början. Att enhetens lösenord måste bytas vid installation för att kunna användas är en relativt enkel åtgärd för att höja enhetens säkerhet. Ett annat sätt för att höja säkerheten är genom regelbundna mjukvaruuppdateringar.

Samhällets ansvar bör ligga i att stödja och informera privatpersoner gällande säkerhet och risker på både lokal och nationell nivå genom exempelvis bemannade IT-center. Detta för att hjälpa invånarna med de mest grundläggande säkerhetsfrågor där deras egna kunskaper brister. Även genom skolan bör samhället se till att unga skall få med sig denna kunskap om säkerhet redan från tidig ålder och sedan genom hela skoltiden. Att ha med det här i läro- och kursplaner är en förutsättning för att skolan skall ha möjlighet att lära ut detta ämnet.

Det åligger även individen att ta ansvar för att hålla sina enheter, nätverk och personlig information skyddad. Att tillägna sig den kunskap som behövs kan göras genom att lägga tid på att läsa på om de olika eventuella risker och problem som kan drabba ens IoT-enheter. Genom att göra detta så finns kunskapen om hur du skall gå tillväga, veta vart du skall vända dig när något inträffar eller om du märker att något inte är som det brukar vara. Att aldrig vara nog nyfiken eller vaksam på de enheter du kopplar upp mot internet bör ses som

ett krav, en ny norm. Något vi alla måste hjälpas åt att driva framåt med anledning av den ständigt växande marknaden och uppkopplingen på internet. För i slutändan så är sakernas internet, en säkerhetsrisk.

Referenser

- [1] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., Zanella A. (2019). IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. Hämtad 2021-02-24 från:
https://polese.io/assets/pdf/2019_menegheelo_iot.pdf
- [2] Sundström, T. (2016). Internet of Things -En guide till sakernas internet. IIS Internetguide #43. Internetstiftelsen. Hämtad 2021-02-25 från:
<https://internetstiftelsen.se/app/uploads/2021/01/internet-of-things.pdf>
- [3] UKEssays. (November 2018). Internet of Things Securities. Hämtad 2021-02-25 från:
<https://bit.ly/3a4pLt8>
- [4] The National Cyber Security Centre - What we do. Hämtad 2021-04-07 från:
<https://www.ncsc.gov.uk/section/about-ncsc/what-we-do>
- [5] Hedtjärn Swaling, V., Johansson, J. (April 2018). NCS3 Studie IoT-relaterade risker och strategier. Myndigheten för samhällsskydd och beredskap. Hämtad 2021-02-24 från:
<https://www.msb.se/RibData/Filer/pdf/28550.pdf>
- [6] Shodan - The search engine for Internet-connected devices. Hämtad 2021-04-15 från:
<https://www.shodan.io/>
- [7] Folkhälsomyndigheten. (16 januari 2020). Nytt coronavirus upptäckt i Kina. Hämtad 2021-03-02 från:
<https://www.folkhalsomyndigheten.se/nyheter-och-press/nyhetsarkiv/2020/januari/nytt-coronavirus-upptackt-i-kina/>
- [8] Tyas Tunggal, A. What is a Cyber Threat? UpGuard. Hämtad 2021-03-15 från:
<https://www.upguard.com/blog/cyber-threat>
- [9] Cohen, L., Manion, L., Morrison, K. (2018). Research Methods in Education. Storbritannien: LCSH: Education–Research–Great Britain. [S.335] doi:
<https://doi.org/10.4324/9781315456539>
- [10] Nordpass. (2021). Top 200 most common passwords of the year 2020. Hämtad 2021-04-16 från:
<https://nordpass.com/most-common-passwords-list/>
- [11] Empey, C. (15 augusti 2018) How to create a strong password. Avast. Hämtad 2021-04-16 från:
<https://blog.avast.com/strong-password-ideas>

- [12] Sentor. Vad är malware? Hämtad 2021-04-05 från:
<https://www.sentor.se/kunskapsbank-it-sakerhet/malware/>
- [13] Levy, J. (2019) Sophos 2020 Threat Report. Sophos. Hämtad 2021-04-12 från:
<https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf>
- [14] Sentor. Vad är phishing/nätfiske? Hämtad 2021-03-18 från:
<https://www.sentor.se/kunskapsbank-it-sakerhet/natfiske-phishing/>
- [15] IDG (2018). Bot. I IT-ord. Hämtad 2021-04-12 från:
<https://it-ord.idg.se/ord/bot/>
- [16] IT-Säkerhet. Vad är en botnet? IT-säkerhet.com. Hämtad 2021-04-05 från:
<https://www.xn--itskerhet-x2a.com/botnet/>
- [17] Sentor. Vad är en DDoS-attack/överbelastningsattack? Hämtad 2021-04-05 från:
<https://www.sentor.se/kunskapsbank-it-sakerhet/ddos-attack/>
- [18] Dobos, L. (2019). Hitta dina sårbara enheter med Shodan – annars gör hackarna det åt dig. Techworld. Hämtad 2021-05-06 från:
<https://techworld.idg.se/2.2524/1.714085/sa-anvander-du-shodan-sarbar-enhet>
- [19] CVE - Common Vulnerabilities and Exposures. Hämtad 2021-05-06 från:
<https://cve.mitre.org/>
- [20] Folkmängden efter ålder och kön . År 1860 - 2020. Hämtad 2021-04-16 från:
https://www.statistikdatabasen.scb.se/pxweb/sv/ssd/START__BE__BE0101__BE0101A/BefolkningR1860N/
- [21] Sentor. (2020). Svenskarnas syn på IT-säkerhet 2020. Hämtad 2021-05-06 från:
[https://content.sentor.se/hubfs/Rapporter%20\(PDF\)/svenskarnas-syn-pa-it-sakerhet-2020.pdf?hsLang=sv-se](https://content.sentor.se/hubfs/Rapporter%20(PDF)/svenskarnas-syn-pa-it-sakerhet-2020.pdf?hsLang=sv-se)
- [22] Sophos. (2021). The State of Ransomware 2021. Hämtad 2021-05-16 från:
<https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf>

Bilaga 1 - Enkät

IoT enhetens säkerhet hos privatpersoner

En enkät som handlar om privatpersoners Internet of Things (IoT)-enheter och dess säkerhet.

Svaren kommer att vara anonyma och sedan bearbetas för att användas som del av underlag till vår kandidatuppsats på 15 HP inom programmet IT-Forensik och Informationssäkerhet vid Högskolan Halmstad.

Vi är oerhört tacksamma över att du vill ta dig tid att svara på denna enkät.

Tack !

Christer Johansson och Viktor Andersson

Våra hem blir mer och mer uppkopplade med så kallade smarta enheter. Ibland för nytta, ibland för nöje och ibland en kombination av de båda. Vår uppsats kommer att bygga på hur privatpersoner ser på säkerheten gällande deras Internet of Things (IoT)-enheter i hemmet. IoT är enheter som t.ex din Google home-högtalare, din smartwatch på armen, glödlamporna som du styr via mobilen, ditt hemlarm eller det digitala låset på ytterdörren.

Inledande frågor

Ange kön

Man

Kvinna

Ange ålder

18-30

31-45

46-60

60+

På en skala 1 -6, hur skulle du skatta din samlade kunskap inom IT ?

1 ▽ till 6 ▽

1 Mycket dålig

6 Mycket bra

IoT-enheter

Vilka IoT-enheter har du i hemmet ? Om du kommer på att du har enheter som inte finns med i listan, vänligen lägg till dessa under annat.

- Assistent (Google home, Amazon Alexa eller motsvarande)
- Chromecasts eller motsvarande
- Glödlampor/belysning som styrs via app eller assistent
- Hemlarm som är uppkopplat
- Ytterdörrlås som är uppkopplat
- Värmepump/element som kan styras från distans
- Vitvaror som är uppkopplade (T.ex kyl/frys med skärm, kaffebruggare eller tvättmaskin m.m som kan styras via app)
- Robotdammsugare och/eller Robotgräsklippare som kan styras och övervakas via app
- Smartwatch
- IP-kamera för övervakning inomhus eller utomhus
- Trådlös skrivare som är uppkopplad via WiFi
- Elmätare som skickar information om elförbrukning direkt till elbolaget
- Jag har ingen IoT-enhet i hemmet
- Annat...

Om du tittar runt eller tänker efter, hur många IoT-enheter har du i hemmet ?

- 0-4
- 5-8
- 9-12
- 13-16
- Fler än 16

Innan du påbörjade denna enkäten, visste du då vad Internet of Things var för något ?

- Ja, jag visste vad det var.
- Ja, jag hade hört talas om det, men visste inte riktigt vad det betydde.
- Nej, jag hade ingen aning om vad det var.

IoT-enheternas säkerhet

Brukar du byta lösenord på dina IoT-enheter ?

- Ja, byter ofta lösenord (Flera gånger per år)
- Ja, byter lösenord ibland (någon gång per år)
- Nej, har aldrig bytt lösenord på mina IoT-enheter
- Jag har ingen IoT-enhet i hemmet

Om du svarat ja på förra frågan, använder du då olika lösenord på dina enheter?

- Ja, olika lösenord på alla enheter.
- Olika till några och samma på resten.
- Nej, samma lösenord till alla enheter.

Har du gjort något annat än att ev. byta lösenord för att säkra dina IoT-enheter ?

- Ja
- Nej
- Jag har ingen IoT-enhet i hemmet

Om Ja på förra frågan, vad har du gjort för att säkra enheterna ? (Valfritt)

...Svarstext....

Är säkerheten något du tar hänsyn till innan du köper en IoT-enhet ?

- Ja
- Nej
- Jag har aldrig köpt någon IoT-enhet

Om Ja på förra frågan, vad har du gjort för att säkra enheterna ? (Valfritt)

...Svarstext....

Christer Johansson

Viktor Andersson



Besöksadress: Kristian IV:s väg 3
Postadress: Box 823, 301 18 Halmstad
Telefon: 035-16 71 00
E-mail: registrator@hh.se
www.hh.se