Examensarbete

VAR KOMMER MYNDIGHETERS LÖSENORDSPOLICYS IFRÅN?

En kvalitativ studie om deras ursprung

WHERE DOES THE AUTHORITIES PASSWORDPOLICYS COME FROM?

A qualtivative study about their origins

Examensarbete inom huvudområdet informationsteknologi

Grundnivå 22,5 högeskolepoäng

Vårtermin 2019

Andreas Naess
a16andna@student.his.se

Handledare: Joakim Kävrestad
Examinator: Marcus Nohlberg

Sammanfattning

Samhället blir mer digitaliserat och fler människor kopplar upp sig mot Internet. Detta innebär att många arbetsuppgifter som hanterar känsliga uppgifter nu utförs på datorer. Det finns även många tjänster som kräver personligauppgifter för att registrera sig och kontouppgifter för att beställa varor eller prenumerera till tjänsten. Denna information är av intresse för brottslingar som kan använda denna för att tjäna pengar. Som en konsekvens av detta har användningen av lösenord ökat och för att försäkra att starka lösenord skapas följs riktlinjer. Dessa lösenordsriktlinjer skapas och sprids ofta utav myndigheter och andra expertorganisationer. Dock saknar de källor för var riktlinjerna kommer ifrån och en förklarning för hur de skapades.

För att belysa detta ämnar studien att eftersöka riktlinjernas ursprung och vad dessa baserades på. Detta är en kvalitativ studie där intervjuer gjorts med informationssäkerhetspecialister från tre myndigheter och en expertorganisation. För att bearbeta data från dessa intervjuer har en tematisk analys utförts för att identifiera de olika källorna som använts vid skapandet av riktlinjerna. Studiens resultat visar att motivationen för riktlinjerna varierar mellan organisationerna. Detta kan observeras genom skillnader i deras målgrupp och fokus. Det har även visat sig att det inte finns några studier att hänvisa till. Dock är ett genomgående mönster att källorna för riktlinjerna ofta verkar vara baserade på de anställdas erfarenheter och expertis. Förutom detta tas inspiration för riktlinjerna från organisationer som NIST.

Nyckelord: *Lösenord, Riktlinjer, Lösenordspolicy, Myndigheter, Expertorganisationer.*

Abstract

Society is getting more digitalized and more people are connecting to the Internet. This means that a lot of work that handles sensitive information is now done using computers. There is also a lot of services that requires personal information for registration and bank account information to order wares or subscribe to the service. This information is of interest to criminal who can use it to make money. Because of this the use of passwords has increased and to make sure that strong passwords are created guidelines are adhered to. The password guidelines are created and spread by authorities and expert organizations. However, there are no sources for where the guidelines came from or an explanation for how they were made.

To shine a light on this, the study aims to explain the guidelines origins and what they were based on. This is a qualitative study where interviews were done with information security specialists from three governmental bodies and one expert organization. After the interviews were completed and data collected, they were analyzed using thematic analysis to identify the sources that were used during the creation of the guidelines. The study's results show that the motivation for the guidelines vary. This can be observed through the differences in target group and focus. It also appears like there are no studies which could be referred to. Although there is a consistent pattern that the sources for the guidelines often seems to be based on the experiences and expertise of their employees. Except for this, inspiration is also drawn from organizations such as NIST

Keywords: *Passwords, Guidelines, Authorities, Password policy, Expert organizations.*

Innehållsförteckning

1 Inledning

Under de senaste tjugo åren har mer och mer av samhället blivit uppkopplat. Denna uppkoppling har gjort det möjligt att enkelt kommunicera runt hela världen. Dock har tillgänglighet av internet har även lett till ett ökat hot från denna källa. Dessa hot kan vara riktade mot samhällskritiks IT-infrastruktur, betalningssystem, företag, organisationer och den vanliga internetanvändaren.

2003 föreslogs en ny strategi för samhällets informationssäkerhet. För att hantera informationssäkerhetshot och säkra informationstillgångar i samhället skapades Samverkansgruppen för informationssäkerhet (SAMFI). SAMFI är ett samarbete mellan olika myndigheter som har ett särskilt ansvar för informationssäkerhetsfrågor. Gruppen arbetar genom att träffas ungefär 6 gånger om året för diskussioner och informationsutbyte. Dock är inte myndigheterna skyldiga att del ta i dessa möten. I denna gruppen ingår just nu 6 myndigheter Myndigheten för samhällsskydd och beredskap (MSB) Post- och telestyrelsen (PTS)Försvarets radioanstalt, (FRA), Säkerhetspolisen (Säpo), Försvarets materielverk (FMV)/Sveriges Certifieringsorgan för IT-säkerhet (CSEC), Försvarsmakten (FM)/Militära underrättelse- och säkerhetstjänsten (MUST) (Myndigheten för samhällsskydd och beredskap, 2014). Utöver detta finns det 14 andra myndigheter som har ansvar för informationssäkerhet (Regeringskansliet, 2015).

Mellan 2006 och 2015 ökade IT relaterade brott med 949 procent de flesta av dessa brott faller under kategorin brott mot person och bedrägeri (Andersson, Hedqvist, Ring & Skarp, 2016). En metod att utföra dessa brott är genom att komma åt eller knäcka lösenord. Då ett lösenords funktion är att skydda ett informationsobjekt och dessa i många fall har ett högt värde blir det viktigt att dessa är svåra att knäcka. Inom SAMFI finns det 4 myndigheter som ger rekommendationer för skapande och hantering utav lösenord. Dessa är MSB, FRA, FM och SÄPO. Förutom dessa myndigheter finns även organisationen Internetstiftelsen (IIS) som också ger rekommendationer. Det finns dock problem med dessa riktlinjer, de saknar källor för vad de har för ursprung och vad de har baserats på. Det gör det problematiskt att bedöma hur bra dessa riktlinjer faktiskt är.

Användare har en tendens att välja svaga och lättgissade lösenord. Därför är det viktigt att lösenordspolicys ger bra rekommendationer då deras funktion är att leda användare till att skapa starka lösenord och hantera dem på ett säkert sätt. Det har till exempel visat sig vara svårare att knäcka lösenord som skapas under en striktare lösenordspolicy. Dock leder för strikta riktlinjer till sämre användbarhet då användare glömmer lösenord eller känner behovet att behöva skriva ner dem (Kelley, Komanduri, Mazurek, Shay, Vidas, Bauer, Christin, Cranor & Lopez, 2012). Därmed är målet med denna studie att undersöka lösenordspolicyer från de olika myndigheterna och organisationerna. Det vill säga de riktlinjer som användare följer för att skapa och hantera sina lösenord. Mer specifikt kommer det att undersökas var rekommendationerna kommer ifrån och vad de grundas på.

2 Bakgrund

Denna del av rapporten kommer att förklara arbetets bakgrund och problematiken vilket ledde till att frågeställningen för arbetet valdes. Avsnittet påbörjas med en förklarning av vad ett lösenord är och hot som existerar mot dem. Sedan förklaras det vad en lösenordspolicy är och dess olika byggstenar. Dessutom kommer NIST:s lösenordsrekommendationer att presenteras. Därefter kommer det information om olika myndigheter som är auktoritära inom informationssäkerhet.

2.1 Lösenord

Lösenord är en simpel autentiseringsmetod förknippat med autentiseringen av användare. Vanligtvis en sträng av tecken tillsammans med ett användarnamn som används för att verifiera att en användare är den de utger sig för att vara. Detta brukar ske genom att det inskrivna lösenordet jämförs med något värde.

Vanligast i moderna system är att lösenordet jämförs med ett *hashvärde*. Detta görs genom att lösenordet körs igenom en *hash*-algoritm för att producera en *hash* vilket är ett värde som är kopplat till lösenordet. Detta jämförs med värdet lagrat i en lösenordsdatabas och om de matchar vet systemet att det är rätt lösenord. Då ett lösenordenords funktion är ett skydda ett informationsobjekt bör detta vara hemligt och endast kännas till av den användare som skapat det, då detta minskar risken att det blir kompromettterat. Lösenord är vanliga då de är lätta att använda och dessutom är ett billigt alternativ för att öka säkerhet (Brose, 2011).

Som en konsekvens av detta krävs det kunskap om vad ett starkt lösenord är då de ofta blir mål för brottslingar. Ett lösenords styrka kan ökas genom längd och komplexitet.

2.1.1 Komplexitet

Ett lösenord kan innehålla bokstäver, siffor och specialtecken. Dessa är vanligtvis begränsade till de tecken som finns tillgängliga via ett tangentbord. Till exempel har ett svenskt tangentbord 26 gemener, 26 versaler, 10 siffor och 33 specialtecken vilket totalt blir 95 olika tecken. Notera att det även finns specialtecken kända som *Unicode* som kan användas genom att utföra kombinationer av tangenttryck på tangentbordet. På ett Windows operativsystem innebär detta tillgång till 65,535 tecken. Användning av en större teckenrymd under skapandet av lösenord kallas lösenordskomplexitet.

En större teckenrymd innebär en ökning av möjliga permutationer. En permutation är en kombination där det finns en strikt ordning på de element som används. Det finns till exempel sex permutationer av a,b och c: abc, acb, bac. bca, cab och cba. Om repetition av tecken tillåts ökar antalet permutationer av a,b och c från 6 till 27, för att räkna ut antalet permutationer med repetitioner kan formeln $P'(n,r) = n^r$ användas där n är teckenrymden och r är antalet tecken (Heckman, 2019). Denna form av permutation är rimlig att använda i lösenordssammanhang då tecken kan förekomma fler gånger i ett lösenord. Om lösenordskomplexitet används på rätt sätt kan en större variation av tecken öka ett lösenords unicitet. Vilket kan leda till starkare lösenord då en ökad variation av tecken minskar risken att lösenordet blir gissat. (Burnett & Kleiman, 2006).

2.1.2 Längd

Att öka ett lösenords längd är ett vanligt, simpelt och ett matematiskt effektivt sätt att öka dess styrka. Dessutom har längre lösenord även fördelen att teckenvariation blir mindre viktigt. Detta då antalet möjliga permutationer av tecken ökar drastiskt då längden av lösenord ökar. Det finns till exempel 294,001,000 fler möjliga permutationer för ett 7 tecken långt lösenord som bara använder gemener än ett 5 tecken långt lösenord som använder sig av hela teckenrymden som ett tangentbord har.

Denna skillnad i permutationer visar hur effektivt det är att öka längden på ett lösenord för att öka dess styrka. Ett alternativ till ett lösenord där längd är nyckeln till dess styrka är en lösenordsfras. Detta är en metod att skapa ett lösenord där lösenordet består av en fras. Ett sätt att skapa en lösenordsfras är att använda slumpade ord för att skapa en mening och sedan lägga till siffor och specialtecken (Burnett & Kleiman, 2006).

2.1.3 Entropi

Skapandet av ett lösenord handlar fundamentalt om att det inte ska gå att kunna gissa vad lösenordet är. En viktig del att göra lösenord svårgissade är slumpmässighet. I ett lösenords fall innebär detta att de skapas med en sekvens av tecken utan något igenkännbart mönster. Det vill säga att det finns entropi, med andra ord en oordning bland tecknen. Slumpmässighet kan delas upp i tre olika egenskaper för att göra det lättare att mäta om ett lösenord faktiskt följer kraven för slumpmässighet. Dessa är normalfördelning, oförutsägbarhet och unicitet (Burnett & Kleiman, 2006).

Normalfördelning innebär att det ska vara lika stor sannolikhet för att alla tecken från den använda teckenrymden ska kunna dyka upp i lösenordet. Det vill säga att om ett lösenord använder sig av gemener som teckenrymd ska sannolikheten för att till exempel a används vara lika stor som att y används. Notera att ett tecken inte måste finnas dock att sannolikheten att det finns är lika stor för alla tecken.

Oförutsägbarhet inom lösenord innebär att det inte ska gå att hitta en relation mellan ett tidigare använt tecken eller en teckensträng. Detta för att denna data inte ska kunna användas för att lista ut resten av lösenordet. Till exempel om frasen *veni vidi vici* skulle användas som lösenord är sannolikheten stor att *veni* skulle kunna användas för att lista ut resten av lösenordet. Då detta är en känd fras som många känner till och ordet *veni* ofta används i denna kontexten.

Unicitet innebär att sekvenser av tecken ej bör dyka upp flera gånger i lösenordet. Då sannolikheten att en likadan sekvens av tecken reproduceras slumpmässigt är liten (Burnett & Kleiman, 2006).

2.2 Hot mot lösenord

Eftersom lösenord är en metod som används för att beskydda ett informationsobjekts sekretess och riktighet finns det naturligtvis hot mot lösenord. En kategori av dessa hot är lösenordsprickning, vanligtvis någon form av *brute force attack*. Det går ut på att en hacker

knäcker ett lösenord på egen hand. Det krävs även att hackern har fått tag på *hash*-algoritmen, användar-id, och lösenords *hashvärde*.

Den simplaste av dessa metoder är att hackern gör lösenordsgissningar. Dessa attacker är möjliga på grund av att personer skapar lättgissade lösenord. Till exempel brukar `123456` och `password` vara vanligt förekommande lösenord. Hackern kan även använda sig av social manipulation för att komma åt personliga uppgifter, vilket också brukar användas i lösenord. Dessa uppgifter kan vara till exempel födelsedagar, husdjursnamn eller favoritband. Dessa uppgifter kan ofta hittas genom olika sociala medier.

En ordboksattack är en annan metod som används för att knäcka lösenord. Denna typ av attack går ut på att förövaren har kompilerat en ordbok som kan användas för att knäcka lösenord. Ordboken består oftast av vanliga lösenord, namn, fiktiva karaktärer, platser och övrigt som kan kopplas till personers liv. Dessa ordboksattacker brukar även innehålla en viss grad av slumpmässighet. Detta innebär att siffor läggs till på slutet av ett ord eller att bokstäver byts ut mot siffror till exempel att skriva Lös3n0rd istället för Lösenord. Bokstäver kan även bytas ut mot specialtecken.

Slutligen finns det en metod som kallas en *ultimate force attack*. Denna metod används för lösenord med en större grad av unicitet. Det vill säga lösenord som inte är vanliga och som inte kan knäckas av en ordboksattack. Den går ut på att testa alla möjliga kombinationer av tecken för att knäcka lösenord. Denna typen av attack kräver en dator som är kapabel till snabbt göra uträkningar av *hash*-algoritmer. Därav krävs en stor mängd datorresurser, i detta fall används flera grafikprocessorer. Detta för att de är lämpade för typen av uträkningar som görs.

Det finns förstås flera hot mot lösenord som till exempel nätfiske och social manipulation. Med dessa metoder spelar det ingen roll hur starkt ett lösenord är eftersom syftet med dem är att användaren ska ge lösenordet till förövaren (Waschke, 2017). Så hur ska en användare veta vad ett bra lösenord är och hur de bör hanterats? Detta brukar göras genom en lösenordpolicy.

2.3 Lösenordspolicys

En lösenordspolicy är en samling av regler som användare ska följa vilket bör leda till säker hantering och skapandet av starka lösenord vilket i sin tur leder till förbättrad säkerhet. En lösenordspolicy består av många olika delar till exempel lösenordskomplexitet, alltså hur ett lösenord måste se ut. Detta inkluderar teckenlängd, användning av gemener och versaler, användning av siffror och specialtecken. Lösenordspolicys kan även innehålla regler för hur länge ett lösenord får användas, Hur gammalt lösenordet måste vara innan det får bytas, om ett lösenord får återanvändas och hur många gånger det får återanvändas, om lösenord får skrivas ned och hur de då ska förvaras (Schaffer, 2013). Dessa lösenordspolicys brukar vara grundade på rekommendationer från myndigheter och expertorganisationer.

2.4 NIST:s Lösenordsrekommendationer

National Institute of Standards and Technology (NIST) är en amerikansk organisation som skapar standarder inom teknologi. Bland annat ger de ut rekommendationer för

lösenordspolicys. Dessa kan hittas i standarden SP 800-63B: *Digital Identity Guidelines: Authentication and Lifecycle Management.* NIST rekommendationer kräver att lösenord ska var minst 8 tecken och som längst 64 tecken långa. De har inga komplexitetskrav dock anses det att alla *ASCII* och *Unicode*-tecken ska kunna användas. Användare ska inte få skapa lösenord som varit med i läckor, använder vanliga ord, har upprepade tecken eller sekvenser av tecken. Det får heller inte använda ord som kan kopplas till kontexten där lösenordet ska användas till exempel namnet på en tjänst. Användaren ska inte behöva byta lösenord efter en viss tid dock måste det alltid bytas om det blivit kompromitterat (Grassi, Fenton, Newton, Perlner, Regenscheid, Burr, Richer, Lefkovitz, Danker, Choong, Greene & Theofanos, 2017).

2.5 Myndigheter och organisationer

I Sverige finns det många myndigheter som anses bära särskilt ansvar när det kommer till informationssäkerhet. Dessa inkluderar samhällsskydd och beredskap (MSB), Datainspektionen, Försvarsmakten (FM), Försvarets materielverk (FMV), Den militära underrättelse- och säkerhetstjänsten (MUST), Försvarets radioanstalt (FRA), Post- och telestyrelsen (PTS), Polismyndigheten, Säkerhetspolisen (SÄPO) och Totalförsvarets forskningsinstitutions (FOI). Eftersom dessa myndigheter är auktoritära inom informationssäkerhet vänder sig organisationer, andra myndigheter och privatpersoner till dem när de behöver rekommendationer inom området (Regeringskansliet, 2015).

En vanlig rekommendation som ges är hur en lösenordspolicy bör se ut. Här uppstår ett problem då de olika myndigheterna ger olika rekommendationer för hur lösenord bör hanteras och se ut. Till exempel rekommenderar FM och MUST att ett lösenord bör vara minst 16 tecken långt (Forsvarsmakten, 2013). MSB föreslår att ett lösenords bör vara minst 12 tecken långt (Frisk, 2018) medan IIS i rapporten rekommenderar lösenord på minst 10 tecken (Eklund Löwinder, 2016.)

2.5.1 Försvarsmakten

Försvarsmakten som myndighet ansvarar för Sveriges militära försvar och sköter även utvecklingen av detta. Som en del av försvaret ingår även cybersäkerhet och informationssäkerhet. Försvarsmakten utvecklar strategier som ska kunna användas som understöd i civilt bruk. Strategierna överses av avdelningen för IT-säkerhetsprodukter och mekanismer för Försvarsmakten (Regeringskansliet, 2015).

2.5.2 Försvarets radioanstalt

FRA har som främst uppgiften att utföra signalspaning. De ska även kunna fungera som stöd vid kriser som har IT-inslag. Därav utför FRA även tjänster som rådgivning och utbildning inom IT-säkerhet. Som del av denna rådgivning ger de rekommendationer för skapning och hantering av lösenord (Regeringskansliet, 2015).

2.5.3 Internetstiftelsen

Internetstiftelsen är en oberoende organisation vars syfte är att garantera en säkrad och starkare infrastruktur för internet. De har också som mål att främja forskning, utbildning och undervisning med internet som inriktning. För att finansiera dessa ändamål har de även

ansvarar för domänen .se och toppdomänen .nu där de även har hand om drift och administration (Internetstiftelsen, u.å.).

2.5.4 Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap har som uppgift att hantera frågor som rör skydd mot olyckor, krisberedskap och civilt försvar. Ett av ansvaren de har är att försöka förebygga dessa händelser genom säkerhetsåtgärder. Inom informationssäkerhet innebär detta att MSB ska ge vägledning och råd till kommuner, myndigheter, landsting, företag och organisationer för att förebygga incidenter kopplade till området (Regeringskansliet, 2015).

2.5.5 Säkerhetspolisen

SÄPO som myndighet bedriver underrättelse- och säkerhetsarbete. Ett av områdena som SÄPO har ansvar för är säkerhetsskydd. Detta innebär bland annat att SÄPO genom analyser, registerkontroller, tillsyn och rekommendationer arbetar med att höja säkerhetsnivån i samhället (Regeringskansliet, 2015).

3 Problembeskrivning

Som det noteras i de tidigare kapitlen verkar myndigheter ge olika rekommendationer för vad en bra lösenordspolicy är. Detta kan visserligen bero på att de har olika fokus för sina lösenordsriktlinjer. FRA ett högre fokus på säkerhet än användarvänlighet, detta med tanke på det arbete som de utför är kopplat till nationell säkerhet. IIS fokuserar mer på vanliga användare och därmed ger mer användarvänliga rekommendationer. Som till exempel att lösenord inte periodiskt måste bytas. Dock anges oftast inte några källor för vad deras rekommendationer grundas på eller var de kommer ifrån. Det gör att det blir svårt att faktiskt bedöma hur bra de är. Det går inte att avgöra om de kraven de har på längd och komplexitet för lösenorden leder till bättre säkerhet. Förutom säkerheten finns även möjligheten att rekommendationer inte är användarvänliga. Detta kan till exempel vara att lösenorden blir för komplexa för att kommas ihåg, att de måste bytas för ofta eller en kombination av de båda. Därför kan det vara viktigt att ta reda på var dessa rekommendationer kommer ifrån så det går att verifiera att riktlinjerna faktiskt har deras tänkta effekt.

Det finns dock studier som visar att vissa av myndigheternas riktlinjer kan ha en negativ effekt. Som FM, FRA och MSB rekommendation om att lösenord bör bytas efter en viss tid. Detta anser Chiasson & van Oorschot (2015) har en negativ inverkan på en lösenordspolicys användbarhet och en negligerbar ökning av säkerhet då denna typ av riktlinje endast stoppar attacker där obehöriga har tillgång till konton över en längre tid. Riktlinjen har ingen påverkan på attacker där till exempel *malware* installeras eller filer blir stulna då detta troligtvis kommer att göras så fort de har åtkomst till kontot. Den har dock den negativa påverkan att användare behöver skapa nya lösenord. Detta kan vara ett problem om det finns höga komplexitetskrav då användare har det svårt att skapa nya lösenord under dessa omständigheter. Det har även visat sig att användare har en tendens att skriva ner lösenord i dessa fall då 54 procent av användare gjorde detta om lösenordspolicyn krävde 12 tecken och 3 teckenklasser (Shay, Cranor, Komanduri, Durity, Huh, Mazurek, Segreti, Ur, Bauer & Christin, 2014). Det är värt att notera att dessa krav liknar MSB:s rekommendationer för komplexitet där skillnaden är att MSB:s riktlinjer kräver 4 teckenklasser.

En annan riktlinje som kan ha negativa konsekvenser är FRA:s rekommendation för lösenordsskapande vilket endast är att göra långa lösenord. Enligt Shay, Cranor, Komanduri, Durity, Huh, Mazurek, Segreti, Ur, Bauer & Christin (2016) bör denna typ av lösenordspolicy undvikas. De medger att det är möjligt att skapa starka lösenord genom att endast använda längd. Dock visade det sig att många användare under denna typ av lösenordspolicy skapar svaga och lättgissade lösenord och att det därför bör undvikas. Detta kan observeras då de flesta lösenorden endast innehåller bokstäver, siffror eller en kombination av de båda. Detta kan göra det lättare att skapa en ordbok att använda för att utföra ordboksattacker mot lösenord skapade under denna typ av lösenordspolicy (Kävrestad, Zaxmy & Nohlberg, 2019).

3.1 Frågeställning

Denna studie ämnar besvara frågan: *Vad är källorna för myndigheters och expertorganisationers lösenordsriktlinjer och vad är dessa baserade på?* Det vill säga om rekommendationerna kommer från en annan organisation som är auktoritär inom området.

Om myndigheterna och organisationerna tagit fram rekommendationerna internt, om de grundats på studier eller om det är en blandning av dem båda. Det finns också möjligheten att rekommendationerna grundar sig i erfarenhet inom informationssäkerhetsområdet som de anställda inom organisationen eller myndigheten besitter.

3.2 Avgränsning

Avgränsningen för denna studie är svenska myndigheter och organisationer som har särskilt ansvar för informationssäkerhet eller som är experter inom området. Dessa myndigheter och organisationer måste dessutom ge rekommendationer för lösenord. Anledningen för att endast fokusera på svenska myndigheter är att andra länder kan ha en annan säkerhetskultur. Dessutom kan myndigheter och organisationer i andra länder ha andra lösenordsbehov. Till exempel kan en organisation i USA vara mycket större än i Sverige.

3.3 Förväntat resultat

Vid slutet av denna studie förväntas det att källorna för lösenordsriktlinjerna kommer att vara varierade. Dock att de huvudsakligen är baserade på rekommendationer från organisationer som NIST eller Microsoft. Det förväntas inte att studier kommer vara en stor influens på riktlinjerna. Detta på grund av att få studier har observerats under denna studie som matcher de riktlinjer som hittats. När studien är avklarade förväntas den slutgiltiga produkten att vara en bättre förståelse för hur myndigheter tar fram sina lösenordsriktlinjer och var de kommer ifrån.

4 Metod

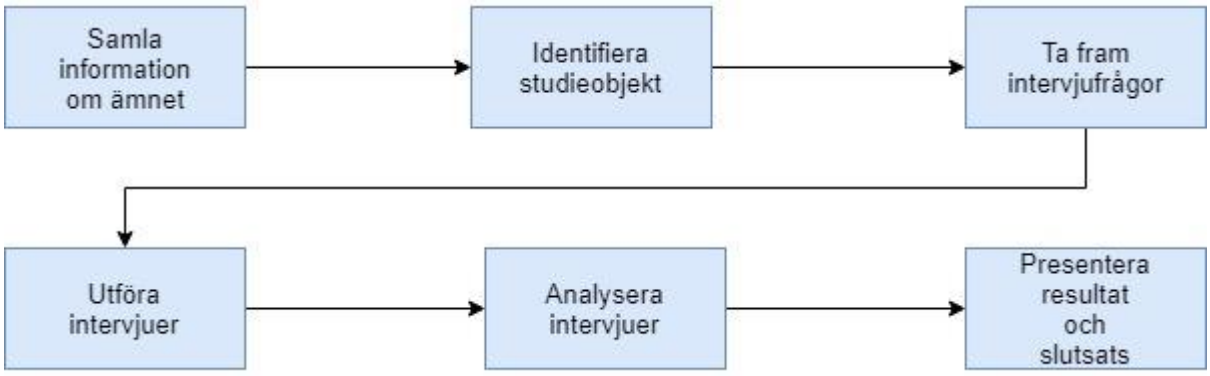
Detta kapitel kommer att förklara metoden som använts för att utföra denna studie. Detta inkluderar intervjumetoden som använts, hur insamlade data analyseras. Det kommer även förklaras hur de myndigheter som ansetts relevanta har identifierats. Slutligen beskrivs de validitetshot som relaterar till denna studie.

4.1 Strategi

För att genomföra denna studie tas en strategi fram i form av mål som ska uppfyllas. Detta kommer göras med olika metoder för att samla in och bearbeta data. Målen kommer att listas här i den ordningen som de kommer att utföras.

- Samla information om ämnet
- Identifiera studieobjekt
- Ta fram intervjufrågor
- Utföra intervjuer
- Analysera intervjuer
- Presentera resultat och slutsats

Efter att dessa mål har uppnåtts anses det att syftet med studien bör ha uppfyllts (Hedin & Martin, 1996). För att uppfylla målen ska en kvalitativ metoden användas. För att utföra intervjuer kommer den semistrukturerade intervjumetoden att användas och för att sedan bearbeta insamlade data kommer tematisk analys att användas. I följande sektioner av kapitlet kommer strategin förklaras i mer detalj.



Figur 4.1.1 processmodell för studiens strategi – (Författarens egen)

4.2 Kvalitativ metod

För denna studie har den kvalitativa metoden valts. Data samlad från denna typ av metod går inte generalisera, dock kan metoden användas explorativt (Hedin & Martin, 1996). Vilket passar denna studie då syftet med studien är att ta reda på något hittills okänt, nämligen vad

för källor myndigheters och organisationers lösenordsriktlinjer har. Den kvalitativa metoden används även för att öka förståelsen inom ett fält men inte att nödvändigtvis ge en förklaring för det (Berndtsson, Hansson, Olsson & Lundell, 2008). Vilket är lämpat för denna studie, då studiens mål är att finna information inom ett fält snarare än att förklara varför det ser ut om det gör i dagsläget.

Då forskaren själv måste samla in data för analys som sedan ska tolkas anses den kvalitativa metoden vara subjektiv (Hedin & Martin, 1996). Metoden hanterar även ofta mänskliga och organisatoriska aspekter när den används inom IT. Eftersom de mänskliga och organisatoriska förhållandena förändras över tid finns möjligheten att resultaten för studien inte går att upprepa (Berndtsson et al., 2008). Vilket stämmer inom IT då det är ett fält där utveckling sker snabbt. I övrigt sker forskningen genom att först undersöka forskningsfrågan för att ta reda på vad som redan är känt. Sedan sker datainsamlings, analys, presentation av resultat och diskussion (Hedin & Martin, 1996).

4.3 Kvalitativa Intervjuer

Då detta är en kvalitativ studie följer det att en kvalitativ intervju kommer att utföras. Till skillnad från kvantitativa intervjuer där strukturerade verktyg används vilket ger begränsade svar utmärks denna typ av intervju av att öppna frågor ställs vilket leder till att den intervjuade kan svara mer utförligt och flexibelt. Detta är en viktig egenskap då den kvalitativa metoden oftast ämnar besvara komplexa frågor där hittills lite är känt. Vilket därmed kan bidra till att ge en djupare förståelse av problemområdet (Nathan, Newman & Lancaster, 2018)

För denna studie har den semistrukturerade intervjumetoden valts. Denna typ av intervju utförs oftast en person i taget men kan utföras i grupp (Hedin & Martin, 1996). Intervjun brukar påbörjas genom att intervjuaren inleder intervjun med några kommentarer om ämnet. Därefter utförs intervjun och de tänkta frågorna om ämnet tas upp. Slutligen avslutas intervjun och avslutande kommentarer yttras (Robson, 2002). Innan intervjun utförs skapas en intervjuguide med ämnen som ska tas upp under intervjun. Dessa frågor ska vara öppna, då detta ger intervjuaren friheten att ställa följdfrågor till uttalanden som upplevs kunna förbättra förståelsen inom ämnet. Därför ska intervjuguiden inte följas i en strikt ordning då detta skulle besegra syftet med metoden (Nathan, Newman & Lancaster, 2018). Det är också viktigt att samtalet känns naturligt och att den intervjuade självständigt berättar om ämnet utan att intervjuaren måste leda samtalet (Hedin & Martin, 1996). Dock måste intervjuaren ingripa om samtalet strövar för långt från huvudämnet och föra intervjun tillbaka i rätt riktning (Nathan, Newman & Lancaster, 2018).

Denna intervjumetod är lämplig för denna studie då den ämnar besvara en explorativ fråga och då experter inom området kommer intervjuas anses det användbart att kunna ställa följdfrågor. Då dessa kan hjälpa att styrka eller ge ett nytt perspektiv för studien (Nathan, Newman & Lancaster, 2018). När en intervju efterfrågas kommer detta göras genom mejlkorrespondens. Där ska den intervjuade få namn och studieprogram på intervjuaren. Dessutom presenteras studiens inriktning, frågeställning och frågor för att ge den intervjuade bakgrund för studien. Intervjuerna kommer att utföras över telefon eller på plats beroende på

vad som funkar för den intervjuade. Innan intervjun påbörjas kommer den intervjuade frågas om det är acceptabelt att intervjun spelas in och om den intervjuade får användas som referens om detta skulle vara nödvändigt. Möjligheten att rapport och transkribering skickas till den intervjuade kommer även att presenteras. Detta om den intervjuade vill verifiera att det som sagts under intervjun inte har blivit feltolkat.

4.4 Tematisk analys

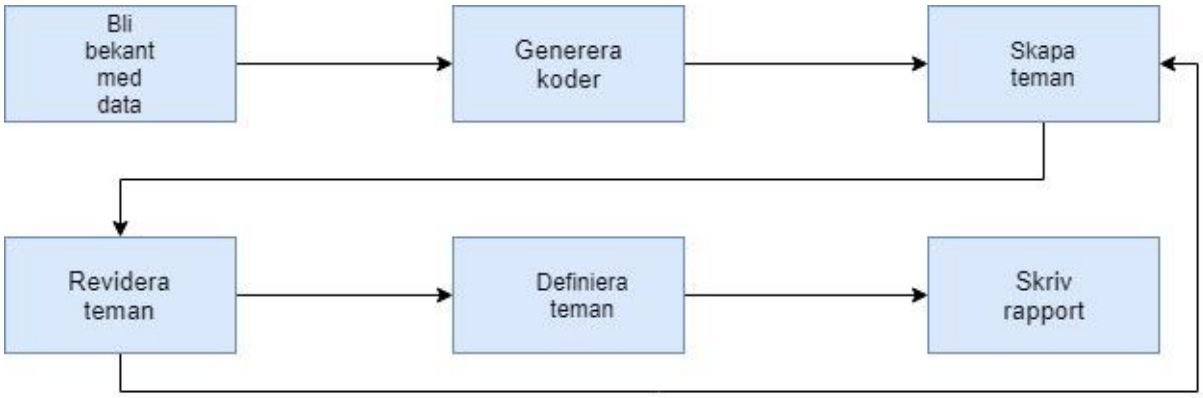
För att bearbeta data som kommer samlas in igenom intervjuer kommer en analys att göras. Detta påbörja genom att först transkribera intervjuerna i sin helhet. Detta innebär bland annat att pauser, felsägningar och skratt inte ska utelämnas (Hedin & Martin, 1996). När detta arbete gjorts kan själva analysen påbörjas. För denna studie ska en tematisk analys användas, tematisk analys är snarare ett samlingsnamn för olika tillvägagångssätt än ett specifikt tillvägagångssätt. För denna studie har det reflexiva tillvägagångssättets valts, den reflexiva analysen är en iterativ process och kodningen av data kan utvecklas under analysen. Till exempel kan nyckelord plockas bort, kombineras med andra eller döpas om. Detta anses vara gynnsamt för studien då det tillåter en viss grad av flexibilitet, på grund av att den tematisk analysen anses vara en analytisk metod snarare än en metodologi. Dessutom förenklas processen att skapa teman, då det från början kan vara svårt att bestämma tema som ett konceptuellt grundat mönster då detta kräver en djup kännedom av data. Reflexiv tematisk analys undviker detta genom att istället skapa en sammanhängande och övertygande tolkning av insamlade data (Braun, Clarke, Hayfield & Terry, 2018).

Analysen påbörjas med att ta fram nyckelord från intervjuerna som kan användas till kodning. Nyckelorden kan sedan användas för att hitta teman genom att hitta kopplingar mellan nyckelorden (Hedin & Martin, 1996). Detta för att kunna ena data som på egen hand inte verkar tillföra förståelse för ämnet som undersöks. Denna data kan tillsammans användas för att förklara meningen bakom ett dataset och därav tillåta forskaren att kunna tolka det (Braun et al., 2018) Då denna studie ämnar ta reda på vilka källor myndigheter och expertorganisationer använder för att ta fram deras lösenordsriktlinjer lämpar sig denna metod. Detta då egenskapen att kunna ta fram teman kan användas för att separera de olika källorna i kategorier vilket bidrar till en klarare översikt av materialet.

För att utföra den reflexiva tematiska analysen ska sex olika faser genomföras:

- Bli bekant med data
- Generera koder
- Skapa teman
- Revidera teman
- Definiera teman
- Skriv rapport

Då denna form av tematisk analys är reflexiv är det inte en strikt ordning som måste följas (Braun et al., 2018). Det anses att följandet av dessa faser bör leda att utkomsten att denna studie blir fullbordad



Figur 4.4.1 processmodell för analys – (Författarens egen)

4.5 Urval

Denna studie är avgränsad till myndigheter som är auktoritära inom informationssäkerhet och expertorganisationer som är baserade i Sverige. Anledningen för detta val är för att det kan finnas kulturella och logistiska skillnader när det kommer till informationssäkerhet och lösenordsriktlinjer i andra länder. Det kunde även bli problematiskt att få kontakt med personer som har insikt i skapandet av lösenordsriktlinjerna om organisationen inte var svensk. För denna studie undersöktes och kontaktades 15 myndigheter, varav fyra levde upp till kraven om att vara auktoritär inom informationssäkerhet och dessutom ge ut lösenordsriktlinjer. En av dessa myndigheter gav inte ut intervjuer och kunde därför inte delta i denna studie. De myndigheter som var kvar och därmed deltog i denna studie är Försvarsmakten, Försvarets radioanstalt och Myndigheten för samhällsskydd och beredskap.

Utöver dessa fyra myndigheter har även Internetstiftelsen deltagit i denna studie. Denna organisation valdes utifrån rekommendationer från båda handledare och myndigheter. Då det är en expertorganisation inom informationssäkerhet som är baserad i Sverige och de ger lösenordsriktlinjer. Dessutom anses Internetstiftelsen vara en trovärdig organisation då de varit involverade i samarbeten med myndigheter när det gäller informationssäkerhetsfrågor. Då det i många fall inte var möjligt att ta reda på vem som hade skapat lösenordsriktlinjerna lämnades valet av intervjuperson till myndighet eller organisation då det ansågs att de har en bättre uppfattning av vilken anställd som kunde svara på studiens frågor. Alla intervjuade är dock anställda som någon form av informationssäkerhetsspeciallist och har stor insyn i lösenordsriktlinjer. För att ge spårbarhet i rapporten har varje organisation blivit tilldelad en kod som kommer att användas under analys och resultat

Intervjuobjekt	Organisation	Kod
1	Försvarsmakten	FM
2	Försvarets radioanstalt	FRA
3	Internetstiftelsen	IIS
4	Myndigheten för samhällsskydd och beredskap	MSB

4.6 Intervjufrågor

Detta är frågorna som kommer ställas under intervjuerna. Förutom dessa är det möjligt att följdfrågor kommer ställas vid behov.

Var kommer rekommendationerna ifrån? Till exempel om de kommer ifrån någon annan organisation, myndighet eller om de själv tagit fram dem.

Vad är rekommendationerna grundade på? Om de vet ifall de är grundade på någon studie eller annan källa.

Är era rekommendationer framtagna för någon specifik målgrupp?

Har era rekommendationer något fokus? Till exempel om de prioriterar säkerhet över användarvänliga aspekter som hur lätt ett lösenord är att komma ihåg.

4.7 Validitetshot

Denna del av rapporten kommer att gå igenom de validitetshot som är relevanta för denna studie. Det vill säga aspekter som har varit i åtanke under utförande av denna studie för att hålla de insamlade resultaten valida och kunna dra tillförlitliga slutsatser. Validitet kan kategoriseras i tre olika kategorier *slutsatsvaliditet, internvaliditet, konstruktionsvaliditet* och *externvaliditet.*

Slutsatsvaliditet rör hot som påverkar förmågan att kunna dra en korrekt slutsats när det kommer till hur behandlingen relaterar till resultatet av studien. Hot mot internvaliditet innebär att det finns okända hot mot kausaliteten av en oberoende variabel. Detta kan komma att påverka slutsatsen om behandlingen och resultatets kausalitetsrelation. Hot mot konstruktionsvaliditet är kopplat till designen av experimentet som kan påverka resultatet. Hot mot externvaliditet är hot som påverka generalisering av resultaten. Dessa brukar påverkas av tre interaktioner med behandlingen personer, plats och tid. De relevanta hoten mot denna studie är interaktion av urval och behandling, otillräcklig preoperativ förklaring av konstruktioner (Wohlin, Runeson, Höst, Ohlsson, Regnell & Wesslén, 2012).

4.7.1 Interaktion av urval och behandling

Interaktion av urval och behandling som ett validitetshot innebär att fel personer har valts att del ta i studien. Vilket skulle innebära att de inte kan representera gruppen som ska del ta i studien (Wohlin et al., 2012). Detta har lösts genom att vara specifik i frågeställningen till de olika myndigheterna för att belysa att denna studie handlar om lösenordshantering och -skapande. Detta för att få kontakt med personer som har expertis inom området.

4.7.2 Otillräcklig preoperativ förklaring av konstruktioner

Otillräcklig preoperativ förklaring av konstruktioner innebär att studiens motivering och frågeställning är dåligt definierad. Detta kan leda till att det som ska undersökas inte är tillräckligt tydligt (Wohlin et al., 2012). Vilket i detta fall skulle kunna leda till att frågorna till intervjuerna fokuserar på fel saker. Detta har lösts genom att ha ett tydligt fokus på vad som skulle besvaras från början.

4.7.3 Fiske efter resultat

Detta innebär att resultat som är önskvärda fiskas efter och oönskade resultat ignoreras. Detta skulle kunna ske genom att ledande frågor ställs för att få specifika resultat. Vilket skulle innebära att intervjuaren påverkar resultaten och att de inte längre är oberoende (Wohlin et al., 2012). För att undvika detta ska öppna frågor ställas för att låta de intervjuade tala fritt om ämnet. Dessutom ska intervjuaren ha ett neutralt tillvägagångssätt för att inte den intervjuades svar ska påverkas.

5 Resultat

Denna del av rapporten kommer att innehålla sammanfattningar av de transkriberade intervjuerna som gjordes med Försvarsmakten, Försvarets radioanstalt, Internetstiftelsen och Myndigheten för samhällsskydd och beredskap. De har blivit tilldelade en kod för spårbarhet och kommer presenteras utifrån teman. Det kommer finnas fyra olika teman.

- **Riktlinjernas ursprung** - Det vill säga varifrån rekommendationerna kommer. Om de kommer från andra organisationer och myndigheter som har expertis inom området, till exempel National Institute of Standards and Technology (NIST) eller om de skapades inom den egna organisationen.

- **Riktlinjernas basis** - Om de är baserade på de anställdas erfarenhet, andra riktlinjer eller studier.

- **Riktlinjernas målgrupp** - Om riktlinjerna skapades med någon specifik målgrupp i åtanke.

- **Riktlinjernas fokus** - Vad myndigheten eller organisationen har prioriterat när rekommendationerna skapades. Om de tänkte mer på säkerhet, användarvänlighet eller om det är en balans mellan de båda.

Myndigheternas lösenordsriktlinjer kommer även att presenteras i detta kapitel för att ge kontext för resultaten. En graf över var de olika myndigheterna får sina riktlinjer ifrån kan ses i slutet av kapitlet (se figur 5.1.1).

5.1 Lösenordspolicys

Här är en samling av de lösenordspolicys som hittats från Försvarsmakten, Försvarets radioanstalt, Internetstiftelsen och Myndigheten för samhällsskydd och beredskap

5.1.1 Försvarsmakten

I dokumentet Handbok Försvarsmaktens säkerhetstjänst, Informationssäkerhet kan försvarsmaktens rekommendationer för en lösenordspolicy hittas. Enligt FM bestäms ett lösenords kvalité efter hur lätt det kan forceras. FM rekommenderar att undvika vanliga ord och fraser då dessa kan vara lätta för en angripare att gissa. De tycker därför att lösenord som innehåller något av detta bör undvikas.

• egennamn (till exempel personer, sällskapsdjur, idrottslag, företag etcetera)

• telefonnummer

• geografiska namn

• organisationsförkortningar

• militära förkortningar

• fordons registreringsnummer

• personnummer

• datum, annat sådant lösenord som kan härledas från användarens personliga förhållanden

• namn eller förkortningar av namn på IT-system eller ord som finns i ordlistor (till exempel ”lösen”, ”hemlig”, ”system”, ”master” eller ”password”).

De påpekar även att dessa vanliga ord och fraser ej bör användas baklänges. FM rekommenderar att ett lösenord bör vara minst 16 tecken långt men påpekar att denna längd kommer att öka då teknologi blir bättre. Helst tycker de att användare ska använda sig av en lösenordsfras, gärna på blandat språk. Dessa ska helst vara fraser som saknar någon slags mening, till exempel ”kokotjo!idetbluelingo nrisetyxskaft”.

FM rekommenderar att ett lösenord endast används för ett IT-system. Då användandet av samma lösenord för flera tjänster eller IT-system betyder att en angripare kan få tillgång till alla dessa. De skriver även att ett lösenord endast får väljas av en person och att om lösenordet ska skrivas ned måste det förvaras med en säkerhetsnivå som motsvarar informationsobjektets värde. Om möjligheten finns rekommenderar de att lösenord genereras slumpmässigt. De påpekar dock att denna funktion måste sortera bort vanliga mönster som ”qwerty”.

FM rekommenderar även att lösenord bör bytas efter en viss tid. Men att denna tid ej bör var för frekvent då användare kommer ha svårt att skapa tillräckligt starka lösenord. Giltighetstider ska även alltid finnas dokumenterat. Lösenord ska alltid bytas om det på något sätt har blivit komprometterat eller om obehöriga inloggningsförsök har noterats. När lösenorden byts bör gamla lösenord aldrig återanvändas (Försvarsmakten, 2013).

5.1.2 Försvarets radioanstalt

FRA ger rekommendationen att lösenord bör vara ungefär 25 till 30 tecken långa och att detta är bättre än korta lösenord med specialtecken. Tanken med detta är att de anser lösenord bör avvecklas för ordinarie användare och ersättas med kort och kod eller annan tvåfaktorsautentisering, dock tror de aldrig att lösenord kommer att försvinna helt. Utan att de som kommer att fortsätta använda sig av lösenord med största sannolikhet kommer att jobba inom IT och säkerhet. Vilket bör innebära att de har kunskapen att skapa starka lösenord eller lösenordsfraser. Dessutom finns också möjligheten att använda lösenordshanterare då de troligen kommer ha mer än ett lösenord.

I dokumentet Åtgärdsförslag Angrepp via tjänsteleverantörer rekommenderas det att på konton med administrativ kontroll bör lösenord bytas och att de bör bytas med jämna mellanrum. Det rekommenderas även att alltid använda tvåfaktorsautentisering vid systemadministration. De menar att detta bör göras för att underrättelsetjänster hackar stora tjänsteleverantörer och att detta är en väg in. Om tjänsteleverantören blir hackad får hackaren tillgång till alla organisationer som hålls i drift av tjänsteleverantören (Försvarets radioanstalt, 2017).

5.1.3 Internetstiftelsen

Som en del IIS forskning inom lösenordsområdet, utfördes en studie våren 2016 vars fokus låg på svenskars lösenordsvanor. I rapporten Lösenord för alla presenteras svenskarnas lösenordsvanor, hur lösenord läcks och vilka konsekvenser detta har. Det ges även förklaring av hur lösenords hackas och rekommendationer och råd för lösenordsskapning och hantering.

IIS rekommenderar att ett lösenord ska vara minst 10 tecken långt, men påpekar att detta inte räcker. Utan säger även att lösenord bör ha hög teckenvariation eller flera ord om det är en lösenordsfras. De rekommenderar även att använda en mening med positiv betydelse för användaren när lösenordet skapas.

De rekommenderar även säkerhetsnivåer för lösenord om användaren har många lösenord att memorera. Vilket innebär att om information som ska beskyddas har ett högt värde bör lösenordet vara starkare. Till exempel lösenord till jobb, e-post och vårdtjänster. Svagare lösenord kan väljas för oviktiga tjänster till exempel e-shoppingsidor eller digitala tidningar. De tycker även att det kan vara acceptabel att inte komma ihåg sitt lösenord utan istället använda glömt lösenord funktionen som finns på de flesta sidorna.

IIS skriver även i rapporten att regelbundna lösenordsbyten bör undvikas. De menar att detta ej kommer att ha en positiv effekt på säkerheten. Detta för att lösenord som komprometterats kommer att bli använda omgående, vilket betyder att bytet görs i onödan. De påpekar även att det finns en risk att användare kommer att uppfatta lösenord som en mindre känslig säkerhetsåtgärd om det byts ofta. Detta kan då leda till att användare delar med sig av sina lösenord eller att de återanvänds. En annan anledning som anges är att regelbundna byten kan leda till att användare väljer svagare lösenord då det kan var svår att komma på bra lösenord. Detta blir speciellt ett problem om en lösnordspolicy kräver väldigt långa och komplexa lösenord. De påpekar dock att byten av lösenord är acceptabla vid röjning av lösenord eller om lösenordet försvagats genom tekniska innovationer.

IIS rekommenderar även online lösenordsgeneratorer, dock endast för tjänster som inte anses vara viktiga. Detta för att det inte går att veta om dessa är säkra nog då det är svårt att veta om de som går att ha tillit till de som skapat verktyget eller om de har ett högt nog säkerhetstänk. Istället för en online lösenordsgeneratorer rekommenderas lösenordshanterare för känsligare tjänster. Då dessa utför samma uppgift samt hjälper användaren hålla reda på sina lösenord. Dessutom anses det vara lättare att verifiera att utvecklaren går att lita på och dessutom sparas lösenordet lokalt. IIS påpekar att även om det är smidigt att använda funktionen för att spara lösenord i webbläsaren så bör det undvikas då det finns vissa svagheter med det. Till exempel att båda Google Chrome och Mozilla Firefox sparar lösenorden i klartext.

Som en sista rekommendation ges användandet av engångslösenord och tvåfaktorsautentisering. Detta för att det fortfarande finns en risk att en angripare får tag på en användares inloggningsuppgifter. Då kan dessa två funka som en sista barriär för angriparen (Eklund Löwinder, 2016.).

5.1.4 Myndigheten för samhällsskydd och beredskap

På en av MSB:s hemsida www.dinsakerhet.se kan rekommendationer för lösenordspolicys hittas. MSB rekommenderar att lösenord bör vara minst 12 tecken långa. De föreslår även att lösenorden skapas genom att slå ihop tre slumpmässigt valda ord tillsammans med teckenvariation som gemener, versaler, siffor och specialtecken. Alternativ kan en lösenordsfras användas istället då dessa brukar vara starka och lättare att minnas.

När ett lösenord väljs bör det inte kunna kopplas till användaren till exempel bör inte användarens egna namn eller liknande användas. MSB rekommenderar även att vanliga ord eller mönster bör undvikas. Lösenord bör endast användas för en tjänst och bör regelbundet bytas. MSB rekommendera även att tjänster som tvåfaktorsautentisering och lösenordshanterare används. Tvåfaktorsautentisering innebär att en extra säkerhetsmetod används vid inloggning till exempel att en pinkod skickas till användarens mobil för att användas tillsammans med lösenordet. En lösenordshanterare rekommenderas även att användas för att assistera användare med att skapa och lagra komplicerade lösenord (Frisk, 2018).

5.2 Riktlinjers ursprung

FM: Riktlinjerna är i allmänhet skapade inom myndigheten, dock har inspiration hämtats från konferenser med fokus på lösenordsområdet.

FRA: Riktlinjerna skapas helt inom organisationen, utomstående källor används som en referenspunkt för att få insikt i utvecklingen gällande lösenordsriktlinjer.

IIS: Riktlinjerna baseras på expertis från andra organisationer och kommer huvudsakligen utifrån.

MSB: Riktlinjerna kommer främst från andra organisationer.

5.3 Riktlinjers basis

FM: Använde sina anställdas expertis och erfarenheter inom området för att forma sina lösenordsriktlinjer. De har även bevakat konferensen PasswordCon. Dock fanns det inga direkta hänvisningar till källor.

FRA: Påpekas att myndigheten är en expertmyndighet och att ett samarbete av tre olika grupper inom myndigheten tagit fram riktlinjerna. Detta har gjort genom att till exempel forcera lösenord. Då det nämns även att anställda inom dessa grupper besitter kunskap om NIST:s riktlinjer och MSB:s DISA-utbildning.

IIS: Riktlinjerna är baserad på forskning som finns kring lösenord och lösenordshantering. När riktlinjerna skapats har huvudsakligen NIST:s regler använts, men även erfarenhet inom branschen.

MSB: Riktlinjerna är främst baserade på IIS och NIST rekommendationer. De är även baserad på incidentrapporter där de bland annat noterat att lösenord varit väldigt korta.

5.4 Riktlinjers målgrupp

FM: Lösenordsriktlinjerna skapades för medarbetare inom myndigheten, men anses vara generella och lämpliga för allmänheten

FRA: Den primära målgruppen är myndigheter och statligt ägda bolag som anses var särskilt skyddsvärda. Dock påpekas det även att det är bra generella råd. Riktlinjerna var för mycket för en organisation utan en stor hotbild.

IIS: Det påpekas att riktlinjerna skapades för allmänheten.

MSB: Deras målgrupp har varit myndigheter och offentligsektor. Dock har de på senare tid börjat rikta sig mer mot privatpersoner då de har börjat samarbeta mer med andra organisationer.

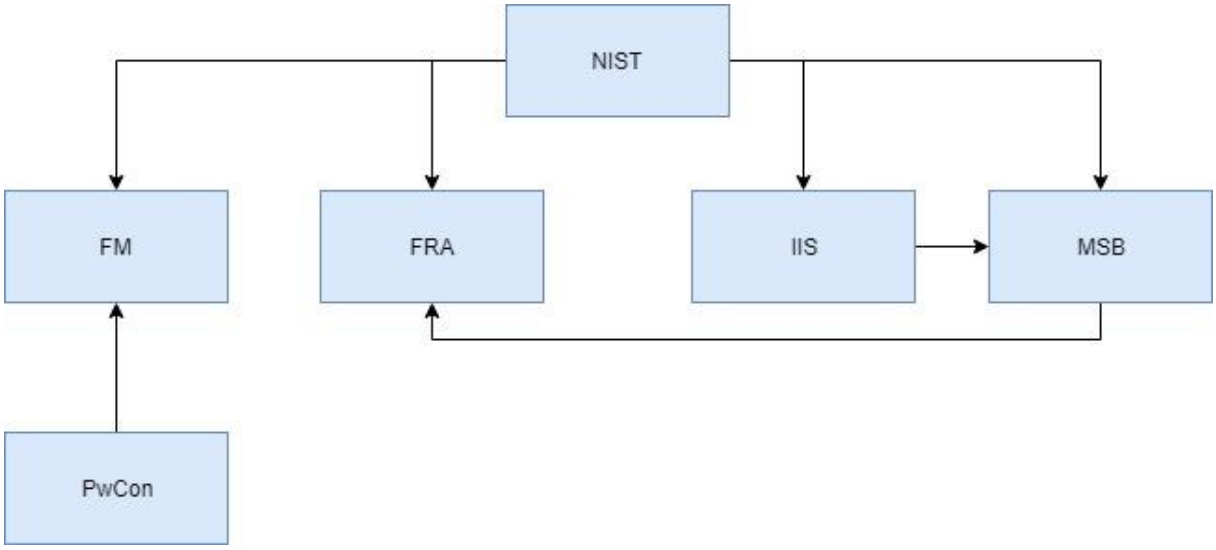
5.5 Riktlinjers fokus

FM: Påpekar att det finns en tydlig korrelation mellan användarvänlighet och säkerhet då de anser att för mycket säkerhet leder till oönskat beteende från användarna. Detta kan vara att användaren väljer lättgissade lösenord som klarar längd och komplexitetskrav till exempel Sommar123!. Den intervjuade förklarar att riktlinjerna baserades på denna insikt.

FRA: Anser att deras fokus ligger på säkerhet över användarvänlighet då deras uppgift rör nationell säkerhet. Men det noteras även att detta alltid är en balansgång som måste göras.

IIS: Det anses att fokus är en balansgång mellan användarvänlighet och säkerhet när rekommendationer tas fram.

MSB: Det påpekas att de främst fokuserar på säkerhet och att som användarvänliga alternativ rekommenderas lösenordsgeneratorer och lösenordshanterare.



(Figur 5.1.1) Graf över riktlinjernas ursprung – (Författarens egen)

6 Analys

Detta kapitel kommer att redovisa analysen som gjort av intervjuerna som utförts under denna studie och kommer ge exempel på hur nyckelord och teman skaptas för den tematiska analysen.

6.1 Kodning och teman

Analysen av intervjuerna påbörjades efter att de hade blivit transkriberade, efter detta följdes de sex faserna som nämndes i kapitel 4.4 tematisk analys. Den först fasen utfördes genom att läsa igenom de transkriberade intervjuerna flertal gånger. Detta för att bli bekant med datan som samlats in och för att få en bättre överblick av intervjuerna. I nästa fas utfördes kodningen av intervjuerna. Detta gjordes för att filtrera materialet och endast behålla de delar som är relevanta för frågeställningen. Utifrån denna kodning kunde sedan teman skapas genom att identifiera relationer mellan nyckelorden som hittats. De nyckelorden som hittats relaterade starkt till frågorna som ställts under intervjuerna och frågorna kunde i stort sätt användas som teman med mindre modifieringar. För att komma fram till de slutgiltiga teman utfördes en iterativ process av revideringar av teman för att testa deras lämplighet mot de funna nyckelorden. De teman som skapades rörde vad för ursprung lösenordsriktlinjerna hade, vilka källor som hade använts vid skapandet av riktlinjerna, vad de hade för målgrupp och fokus.

Intervjuobjekt 2 (FRA)

Fråga: Var kommer rekommendationerna ifrån?

Svar: Vi är expertmyndighet vi har.. det finns massvis med smarta människor här. Sen är vi ju inte bortkopplade från resten av världen Min grupp arbetar ju med IT-säkerhet typ 100 procent av tiden så och vi har några andra människor som bland annat lägger väldigt mycket krut på att just forcera lösenord. Som är väldigt väldigt duktiga på det. Av våra erfarenheter på hur… hur ser det ut med lösenorden särskilt inom statlig förvaltning. I större organisationer generellt och vad behöver man göra för att skydda sig. Så det är väl.. rekommendationerna är väl påhittade, dom satt vi och skrev ihop.

Exempel på kodning som gjorts under analysen

Nyckelord: *Smarta människor*

Inte bortkopplade från resten av världen

Forcera lösenord

Våra erfarenheter

Påhittade

Tabell över teman som använts under analysen.

Tema: Riktlinjers ursprung	Tema: Riktlinjers basis	Tema: Riktlinjers målgrupp	Tema: Riktlinjers fokus
Den intervjuade påpekar att rekommendationerna skapats internt av FRA. Men att de håller koll på vad andra experter inom området kommit ut med. Om FRA till exempel noterar att deras rekommendationer skiljer sig från andras, så undersöker dem vad det beror på. Den intervjuade påpekar att NIST är en organisation som de kollar på då de anses var moder-skeppet för rekommendationer och standardisering.	Den intervjuade påpekar att FRA är en expertmyndighet när det kommer till informationssäkerhet och att den intervjuades grupp jobbar exklusivt med IT-säkerhet. Denna grupp jobbar mycket med att forcera lösenord. Detta tillsammans med deras erfarenheter av hur det ser ut med lösenord i statlig förvaltning och större organisationer har lett till att de skapat dessa lösnordsrekommendationer. Den intervjuade påpekar att rekommendationerna togs fram i ett samarbete av tre olika grupper på FRA. Där det ingår den nätverkssäkerhetsenhet som jobbar med tekniskdetektering, varningssystem och som kollar på kvalificerade IT-hot mot Sverige. Vilket innebär att denna enhet består av en stor grupp IT-säkerhetsexperter. Denna expertis gör det möjligt att formulera rekommendationerna FRA går ut med.	Den intervjuade påpekar att deras primära målgrupp är myndigheter och statligt ägda bolag som anses var särskilt skyddsvärda och att det främst är dem de vill nå. Påpekar även att det är bra generella råd. Dock är det kanske för mycket för en organisation utan en stor hotbild.	Den intervjuade påpekar att deras fokus ligger på säkerhet över användarvänlighet. Då deras uppgift rör nationalsäkerhet. Det noteras även att det alltid är en balansgång som måste göras. Dessutom att det finns en skillnad på vad som är rimligt för deras målgrupp. Till exempel att militärer förmodligen kan följa en strikt lösenordspolicy bättre än anställda på någon annan myndighet.

6.2 Analys av intervjuer

Analysen visar att det varierar i de olika organisationerna, dock är ett genomgående mönster att NIST används som en referenspunkt och även bas för riktlinjer. Den visar även att anställdas expertis och erfarenhet inom området brukar användas.

6.2.1 FM

Försvarsmakten har en lösenordspolicys där målgruppen är medarbetare inom myndigheten. Dock är lösenordsrekommendationerna väldigt generella och kan användas i vilket IT-system som helst. Då de tyckts ha hittat en korrelation mellan säkerhet och användarvänlighet har fokuset skiftat mot det.

Rekommendationerna i handboken är till den största del baserade på erfarenheter som författarna hade inom området och insikten att användarvänlighet och säkerhet är starkt korrelerade. De ska dessutom ha bevakat presentationer på *passwordcon*. Vilket är en mässa som fokuserar på säkerheten kring lösenord och autentiseringsmetoder Till mässan kommer säkerhetsforskare, Lösenordscrackers och lösenordsexperter för att göra presentationer kring de olika aspekterna av lösenord (Passwordscon.org, u.å.).

6.2.2 FRA

Försvarets radioanstalts lösenordsrekommendationer har den primära målgruppen myndigheter och statligt ägda bolag. Även i detta fall anses rekommendationerna vara bra generella råd. Även om de möjligtvis skulle vara lite överflödigt för mindre organisationer. FRA:s rekommendationer har ett starkt fokus på säkerhet då de jobbar med nationell säkerhet.

FRA:s rekommendationer skapas internt inom myndigheten. De har tillgång till många säkerhetsexperter som bara jobbar med informationssäkerhet. De har till exempel en grupp som lägger väldigt mycket tid på att forcera lösenord.

De har även koll på vad andra organisationer som anses vara experter inom området och vad de har för rekommendationer. Till exempel den amerikanska organisationen NIST.

6.2.3 IIS

Internetstiftelsens rekommendationer riktar sig till allmänheten som målgrupp. De har inget direkt fokus utan gör en balansgång mellan säkerhet och användarvänlighet då de säger att det finns en stark koppling mellan de båda.

IIS rekommendationer baseras mycket på NIST:s regler till exempel att lösenord inte bör bytas regelbundet. Något som tas upp i artikeln *Time to rethink mandatory password changes* (Cranor, 2016). Även på IIS används de anställdas expertis och erfarenhet för att skapa rekommendationer.

6.2.4 MSB

MSB har haft myndigheter och offentlig sektor som målgrupp. Dock allt eftersom de börjat samarbeta med andra organisationer har de även börjat rikta sig mot allmänheten. Deras fokus för rekommendationer ligger på säkerhet.

När de tagit fram sina egna rekommendationer har de kollat på andra organisationer bland annat IIS. Men de även kollat på NIST rekommendationer och tar upp rekommendationen om att inte byta lösenord regelbundet. De har även kollat på incidentrapporter där det visat sig att lösenord varit för korta.

7 Diskussion

Denna del av rapporten innehåller diskussion om etiska aspekter, samhälleliga aspekter, vetenskapliga aspekter, en slutsats och en diskussion om framtida arbeten.

7.1 Etiska aspekter

De etiska överväganden som gjort för denna studie relaterar till hur intervjuerna har gjorts. När kontakt har tagits med myndigheterna eller organisationen som ska intervjuas har personen som ska utföra studien introducerats med namn, var och vad denna studerar. Dessutom har studiens område alltid presenterats. När intervjuer har utförts har den intervjuade blivit frågad om det är okej att intervjun blir inspelad och om den intervjuade kan användas som referens i rapporten om detta skulle krävas. Det är även en etisk fråga om myndigheterna bör vara mer transparanta om var deras riktlinjer faktiskt kommer ifrån och presentera detta. Då de har auktoritet inom området lyssnar privatpersoner, myndigheter och andra organisationer på vad de har att säga om området. Om dessa inte vet var riktlinjerna kommer ifrån och inte vet om det är bra riktlinjer är det endast deras förtroende för myndigheten eller organisationen som får dem att följa riktlinjerna. En möjlig etisk konsekvens av denna studie är att personer skulle kunna bli missnöjda med de källorna som använts för riktlinjerna då de inte är tillräckligt konkreta. Personer med illvilliga avsikter skulle även kunna använda studien för att försöka underminera myndigheterna. Vilket skulle kunna leda till ett minskat förtroende för dem.

7.2 Samhälleliga aspekter

Att känna till var lösenordsriktlinjer kommer ifrån och vad de baseras på kan hjälpa företag att välja vad som ska implementeras i deras egen organisation då detta kan ge dem möjligheten att gå tillbaka till källan för riktlinjerna i de fallen de blivit baserade på till exempel NIST:s rekommendationer. Studien kan också leda till att fler personer undersöker varför rekommendationer ser ut som de gör idag vilket möjligtvis skulle kunna leda till en bättre förståelse av lösenordsriktlinjer.

7.3 Vetenskapliga aspekter

Vetenskapligt kan denna studie användas som en startpunkt för att påbörja andra studier. Då denna studie har undersökt ett område där inte mycket var känt och ger en inblick i hur lösenordsriktlinjer skapas på myndigheter och expertorganisationer. Detta skapar en möjlighet att kunna undersöka området djupare. Det kan göras genom att fokusera mer på en av aspekterna av riktlinjeskapandet. Till exempel att undersöka var ifrån informationssäkerhetsspecialisterna som framställer dessa riktlinjer fått sin information.

8 Slutsats

Inom lösenordsområdet finns det mycket olika tankar kring hur en lösenordspolicy ska se ut. Detta kan bero på att de olika myndigheterna har olika målgrupper till exempel att FRA:s målgrupp är myndigheter och statligt ägda bolag som anses var särskilt skyddsvärda vilket innebär att de fokuserar på det viktigaste och det mest samhällskritiska. Det leder till att de kommer att fokusera väldigt mycket på säkerhetsaspekten av lösenordspolicys. Detta kan sättas i kontrast till IIS som inriktar sig mer på att ge råd och rekommendationer till allmänheten där inte lika starka lösenord krävs. Dessa skillnader i målgrupper och i fokus kan vara en godtycklig anledning till att lösenordsrekommendationer och råd skiljer sig så mycket.

Något som noterats under denna studie är att det inte verkar finnas några direkta hänvisningar till studier vilka skulle använts för att skapa lösenordsrekommendationer utan det verkar som rekommendationerna ifrån dem som deltagit i denna studie för det mesta verkar baseras på en kombination av de anställdas erfarenhet och expertis från andra organisationer. Till exempel har NIST nämnts som en organisation som alla verkar ha använt som grund för många av deras rekommendationer eller för att ha koll på vad som händer inom området.

Det har även nämnts i intervjuerna att det är vanligt att personer som jobbar inom området träffas på till exempel mässor. Det skulle kunna var möjligt att rekommendationer och tankar kring lösenord och autentisering sprids genom sådan möten. Till exempel verkar det som att alla som har deltagit på intervjuer har åsikten att användare bör röra sig bort från lösenord och istället använda tvåfaktorsautentisering. Detta får det att verka som att det definitivt finns rekommendationer som anses vara självklarheter. Trots att det inte finns några studier att hänvisa till. Slutligen som svar på studiens frågeställning:

Vad är källorna för myndigheters och expertorganisationers lösenordsriktlinjer och vad är dessa baserade på?

Andra organisationer inom området, arbete som utförts av myndigheten eller organisationen, konferenser och de anställda är de källor som har identifierats för riktlinjerna. Riktlinjerna verkar huvudsakligen vara baserade på en kombination av expertis och rekommendationer som skaptas av NIST. Dock har de också baserats på lärdomar från undersökningar av incidentrapporter, forceringen av lösenord och olika lösenordskonferenser. Dessa riktlinjer har dessutom påverkats av vilket fokus och vilken målgrupp som myndigheten eller organisationen har.

8.1 Framtida arbete

Då det inte fanns några direkta studier med resultat för att ge en förklarning till varför just dessa rekommendationer används. Skulle ett framtida arbeta vara att testa dessa rekommendationer till exempel att forcera lösenord baserade på rekommendationerna. Undersöka användarvänligheten av rekommendationerna och hur användbara de är. En undersökning av var NIST får sina rekommendationer ifrån skulle också kunna vara tänkbar. Att undersöka hur kunskap om lösenord och dess rekommendationer vanligen sprids till dem

som arbetar inom området då många av lösenordspolicyerna verkar vara baserade på de anställdas erfarenheter och expertis inom området.

Referenser

Andersson, F., Hedqvist, K., Ring, J. & Skarp, A. (2016). *IT-inslag i brottsligheten och rättsväsendets förmåga att hantera dem*. © Brottsförebyggande rådet 2016. Tillgänglig på Internet: https://www.bra.se/download/18.3c6dfe1e15691e1603ec36fc/1475217105668/2016_17_Itinslag_i_brottsligheten.pdf
[Hämtad: 2017-03-04]

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B. (2008). *Thesis Projects: A Guide for Students in Computer Science and Information Systems.* (2:a uppl). London: Springer, ss.13-14. Tillgänglig via: https://link.springer.com/book/10.1007/978-1-84800-009-4
[Hämtad: 2019-08-02].

Burnett, M. & Kleiman, D. (2006). *Perfect Password: Selection, Protection, Authentication*. Rockland: Syngress, ss.23-67. Tillgänglig på internet: https://books.google.se/books?hl=sv&lr=&id=18PMr6ra0UQC&oi=fnd&pg=PR1&dq=Perfect+passwords+:+selection,+protection,+authentication&ots=hSaUZJFKnm&sig=aJi5ck939NxC0Sn6T4NAaXLv2EM&redir_esc=y#v=onepage&q=Perfect%20passwords%20%3A%20selection%2C%20protection%2C%20authentication&f=false
[Hämtad: 2019-07-20].

Braun, V., Clarke, V., Hayfield, N. & Terry, G. (2018). *Thematic Analysis. Handbook of Research Methods in Health Social Sciences*, ss.1-18. Tillgänglig på internet: https://link.springer.com/content/pdf/10.1007%2F978-981-10-2779-6_103-1.pdf
[Hämtad: 2019-08-06].

Brose, G. (2011). *Password*. I: *Encyclopedia of Cryptography and Security*. Boston: Springer, ss.916-918. Tillgänglig på internet: https://link.springer.com/referenceworkentry/10.1007/0-387-23483-7_294
[Hämtad: 2019-08-02].

Chiasson, S. & van Oorschot, P. (2015). *Quantifying the security advantage of password expiration policies.* Designs, Codes and Cryptography, 77(2-3), ss.401-408. Tillgänglig på internet: https://link.springer.com/article/10.1007/s10623-015-0071-9
[Hämtad: 2019-08-14].

Cranor, L. (2016). *Time to rethink mandatory password changes*. Federal Trade Commission. Hämtad från internet: https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes
[Hämtad: 2019-04-15].

Davidsson, P. & Findahl, O. (2015). *Svenskarna och internet: 2015 års undersökning av svenska folkets internetvanor.* internetstiftelsen. Tillgänglig på internet: https://internetstiftelsen.se/docs/Svenskarna_och_internet_2015.pdf
[Hämtad: 2019-05-09].

Eklund Löwinder, A. (2016). *Lösenord för alla Statistik, råd och rekommendationer för bättre säkerhet*. Internetstiftelsen.se. Tillgänglig på internet: https://internetstiftelsen.se/docs/Rapport_Losenord_for_alla.pdf
[Hämtad: 2019-03-16].

Frisk, J. (2018). *Säkra dina lösenord*. Dinsakerhet.se. Hämtad från internet: https://www.dinsakerhet.se/sakrare-hemma/skydda-din-information/losenord/
[Hämtad: 2019-03-05].

Försvarets radioanstalt. (2017). *Åtgärdsförslag Angrepp via tjänsteleverantörer*. (1:a uppl). FRA, s.5. Tillgänglig på internet: https://www.fra.se/download/18.60b3f8fa16488d849a5106/1531472534288/Atgardsforslag-Angrepp-mot-tjansteleverantorer.pdf
[Hämtad: 2019-03-06].

Försvarsmakten. (2013). *Handbok Säkerhetstjänst Informationssäkerhet*. Tillgänglig på internet: https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/handbocker/handbok-sak-infosak-andring-2.pdf
[Hämtad: 2019-03-08].

Grassi, P., Fenton, J., Newton, E., Perlner, R., Regenscheid, A., Burr, W., Richer, J., Lefkovitz, N., Danker, J., Choong, Y., Greene, K. and Theofanos, M. (2017). *Digital identity guidelines: authentication and lifecycle management*. Tillgänglig på internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
[Hämtad: 2019-08-28].

Heckman, K. (2019). *Permutations with repetition*.Vcalc.com. Hämtad från internet: https://www.vcalc.com/wiki/vCalc/Permutations+with+repetition
[Hämtad: 2019-07-20].

Hedin, A. & Martin, C. (1996) *En liten lathund om kvalitativ metod med tonvikt på intervju*. Tillgänglig på Internet: https://goo.gl/Pbrf4O
[Hämtad: 2019-08-02]

Internetstiftelsen. (u.å.). *Om oss - Internetstiftelsen*. Hämtad från internet: https://internetstiftelsen.se/om-oss/
[Hämtad: 2019-03-17].

Kelley, P., Komanduri, S., Mazurek, M., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. & Lopez, J. (2012). *Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms*. 2012 IEEE Symposium on Security and Privacy, ss.523-537. Tillgänglig på internet: https://ieeexplore-ieee-org./document/6234434
[Hämtad: 2019-08-14].

Kävrestad, J., Zaxmy, J. & Nohlberg, M. (2019). *Analysing the Usage of Character Groups and Keyboard Patterns in Password*. In: Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019). University of Plymouth Press, ss.155-165. Tillgänglig på internet: https://www.cscan.org/?page=openaccess&eid=21&id=410
[Hämtad: 2019-08-30].

Myndigheten för samhällsskydd och beredskap (2014). *Samverkansgruppen för informationssäkerhet, SAMFI.* Tillgänglig på internet: https://rib.msb.se/filer/pdf/25966.pdf
[Hämtad: 2019-08-27].

Nathan, S., Newman, C. & Lancaster, K. (2018). *Qualitative Interviewing. Handbook of Research Methods in Health Social Sciences*, ss.1-20. Tillgänglig på internet: https://link.springer.com/content/pdf/10.1007%2F978-981-10-2779-6_77-1.pdf [Hämtad: 2019-08-02].

Passwordscon (u.å.). *About – PasswordsCon*. Hämtad från internet: https://passwordscon.org/about/
[Hämtad: 2019-05-06].

Regeringskansliet (2015). *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten*. (1:a uppl). Stockholm: Elanders Sverige AB, ss.93-123. Tillgänglig på internet: https://www.regeringen.se/49bb84/contentassets/8ae8ef6d5d3f45058c981cbab4e297de/informations--och-cybersakerhet-i-sverige.-strategi-och-atgarder-for-saker-information-i-staten-sou-201523
[Hämtad: 2019-03-02].

Robson, C. (2002). *Real world research*. (2:a uppl.). Oxford, UK: Blackwell Publishers, s.278.

Schaffer, K. (2013). *Passwords, Privacy, and Policies: Can They Do Business Together?* Computer, 46(12), ss.76-79. Tillgänglig på internet: https://ieeexplore.ieee.org/document/6689283 [Hämtad: 2019-08-14].

Shay, R., Cranor, L., Komanduri, S., Durity, A., Huh, P., Mazurek, M., Segreti, S., Ur, B., Bauer, L. & Christin, N. (2014). *Can long passwords be secure and usable?*. Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14. Tillgänglig på internet: https://dl-acm-org.libraryproxy.his.se/citation.cfm?id=2557377 [Hämtad: 2019-08-27].

Shay, R., Cranor, L., Komanduri, S., Durity, A., Huh, P., Mazurek, M., Segreti, S., Ur, B., Bauer, L. & Christin, N. (2016). *Designing Password Policies for Strength and Usability*. ACM Transactions on Information and System Security, 18(4), ss.1-34. Tillgänglig på internet at: https://dl.acm.org/citation.cfm?doid=2928292.2891411 [Hämtad: 2019-08-27].

Waschke, M. (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime*. Berkeley: Apress, ss.12, 65-67. Tillgänglig på internet: https://link.springer.com/book/10.1007/978-1-4842-2430-4 [Hämtad: 2019-08-01].

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M., Regnell, B. & Wesslén, A. (2012). *Experimentation in Software Engineering*. Berlin, Heidelberg: Springer, ss.68-69, 102-110. Tillgänglig på internet: https://link.springer.com/book/10.1007/978-3-642-29044-2 [Hämtad: 2019-05-09].