Högskolan Kristianstad
291 88 Kristianstad
044 250 30 00
www.hkr.se

Examensarbete 15 hp
Kandidatexamen i Informatik
VT 2021

Fakulteten för Ekonomi

Konsekvenser av bristande användbarhet i ett säkerhetsklassat it-system

August Järpemo och Egil Swenning Leyser

Författare

August Järpemo & Egil Swenning Leyser

Titel

Konsekvenser av bristande användbarhet i ett säkerhetsklassat it-system

Handledare

Montathar Faraon

Examinator

Kerstin Ådahl

Sammanfattning

Det finns mycket forskning om designriktlinjer för att öka användbarheten i säkra it-system samt att problem med användbarheten kan ge problem i it-system. Men forskningen om vilka faktiska konsekvenser som kan uppstå av hur användbarhet implementerats i säkra it-system, är begränsad. Syftet med studien är att fylla denna kunskapslucka och genomfördes som en fallstudie som baserar sig på kvalitativa intervjuer med sju deltagare. Deltagarna intervjuades gällande deras användning av it-systemet PRIO, deras svar analyserades sedan för att hitta teman. Dessa teman användes som grund när vi arbetade genom resultatet. Vi hittade att PRIO har bristande användbarhet och hittade konsekvenser på grund av detta: brist på information och brist på enkelhet i it-systemet som leder till handhavandefel, dålig prestanda som leder till långa uppstartstider som i sin tur leder till säkerhetsrisker tack vare den mänskliga faktorn, samt att driftstörningar leder till att it-systemet inte går att använda.

Ämnesord

it-säkerhet, användbarhet, designriktlinjer, konsekvenser

Author

August Järpemo & Egil Swenning Leyser

Title

Consequences of lack of usability in a secure IT system

Supervisor

Montathar Faraon

Examiner

Kerstin Ådahl

Abstract

There is a lot of research on design guidelines to increase the usability of secure IT systems and that problems with usability can cause problems in IT systems. However, research on the actual consequences that can arise from how usability has been implemented in secure IT systems is limited. The purpose of the study is to fill this gap of knowledge and the study was conducted as a case study based on qualitative interviews with seven participants. The participants were interviewed about their use of the IT system PRIO, their responses were then analyzed to find themes. These themes were used as a basis when we worked through the results. We found that PRIO has a lack of usability and found consequences because of this: lack of information and lack of simplicity in the IT system leading to handling errors, poor performance leading to long start-up times which in turn leads to security risks due to the human factor, and that operational disruptions leads to the IT system not being able to be used.

Keywords

it-security, usability, design guidelines, consequences

“PRIO är ett tydligt exempel på när det kan gå fel.
Det är ett typiskt tyskt system — det är superbra om du vet exakt hur det fungerar”
Hultgren (2020)

1 Introduktion 7
1.1 PRIO 9
Figur 1.1 9
1.2 Syfte och frågeställning 10
1.3 Avgränsningar 10
1.4 Begreppsdefinitioner 11
2 Litteraturgenomgång 12
2.1 Informatik 12
2.2 It-säkerhet 12
2.3 Användbarhet 12
2.4 Designriktlinjer för användbarhet 14
2.4.1 Generella designriktlinjer 14
2.4.2 Specifika designriktlinjer för säkra it-system 16
2.4.3 Jämförelse - generella och säkra designriktlinjer 20
2.4.5 Kategorisering av designriktlinjer 21
2.4.5.1 Generella designriktlinjer 21
2.4.5.2 Säkra designriktlinjer 22
3 Metod 24
3.1 Litteratursökning 24
3.2 Urval 24
Tabell 3.1 25
3.3 Intervjuer 25
3.4 Analys 26
3.5 Forskningsetiska principer 26
4 Resultat & Analys 27
4.1 Brist på enkelhet 27

4.1.1 Komplicerat 27
4.1.2 Språk 28
4.2 Effektivitet 29
4.2.1 Specificering 29
4.2.2 Utbildning 29
4.2.3 Trögt system 30
4.3 Brist på information 30
4.4 Motverka fel 31
4.4.1 Byte av koder 31
4.4.2 Mallar 32
4.4.3 Fel i data 32
4.4.4. Avsaknad av felmeddelande 33
4.5 Prestanda 33
4.5.1 Driftstörningar 33
4.5.2 Långsam uppstart 34
5 Diskussion 36
5.1 Resultatdiskussion 36
5.2 Metoddiskussion 40
6 Slutsatser & framtida forskning 42
6.1 Slutsatser 42
6.2 Framtida forskning 43
7 Källor 45
8 Bilaga 1: Tabell 2.1 49
9 Bilaga 2: Tabell 2.2 50
10 Bilaga 3: Frågor 52
11 Bilaga 4: Nya Frågor 53
11 Bilaga 5: Missivbrev 54

1 Introduktion

I och med digitaliseringen har interaktiva enheter och system vuxit fram i större delar av vardagen, inte minst i hemmen och på arbetsplatserna (Janlert & Stolterman, 2017). Detta medför att fler enheter och system blir mottagliga för it-attacker, och att risken för attacker aldrig har varit så hög som nu (Albahar, 2017). It-säkerhet, att skydda data och användare, som område började på 1960-talet när man kopplade upp datorer med varandra (Warner, 2012; Azmi, Tibben & Win, 2018). I Sverige har myndigheter, såsom Försvarsmakten, en skyldighet att skyndsamt rapportera it-incidenter till Myndigheten för samhällsskydd och beredskap, MSB (MSB, 2019; 2020). MSB rapporterar att incidenter gällande handhavandefel har ökat från 14% till 23% mellan 2019 och 2020 (ibid). Det handlar oftast om att uppdateringar inte fungerar som det var tänkt eller incidenter som uppstått till följd av att personal gjort felaktiga inställningar i systemet som därefter leder till att hela eller delar av systemet inte fungerar som de ska. En del av säkra it-system är att upprätthålla användbarheten i systemen.

Användbarhet kan beskrivas till vilken grad ett it-system kan användas av de tänkta användarna enligt Internationella standardiseringsorganisationen, ISO (2018). Användbarhet kan mätas utifrån effektivitet (effectiveness), förmåga (efficiency) och tillfredsställelse (satisfaction) för att uppnå ett mål, både praktiskt och personligt (Arthana, Pradnyana & Dantes, 2019; Bevan, Carter, Earthy, Geis & Harker, 2016). För att upprätthålla användbarheten underlättar designriktlinjer som kan vara till stöd vid design av dessa it-system.

Flera författare har utvecklat olika designriktlinjer för att kunna utvärdera användbarheten av ett system (Nwokedi, Amunga & Rad, 2016; Norman, 2013). För att kunna vidmakthålla säkerheten i it-system och minska handhavandefel skriver Nwokedi, Amunga & Rad (2016) att användbarhet bör ses som ett krav för säkerheten i systemet. Utmaningen är att skapa en balans mellan säkerhet och användbarhet i ett system som ska vara bekvämt att använda och samtidigt säkert (Gordieiev, Kharchenko & Vereshchak, 2017; Mohamed, Chakraborty & Dehlinger, 2017; Allen & Komandur, 2019).

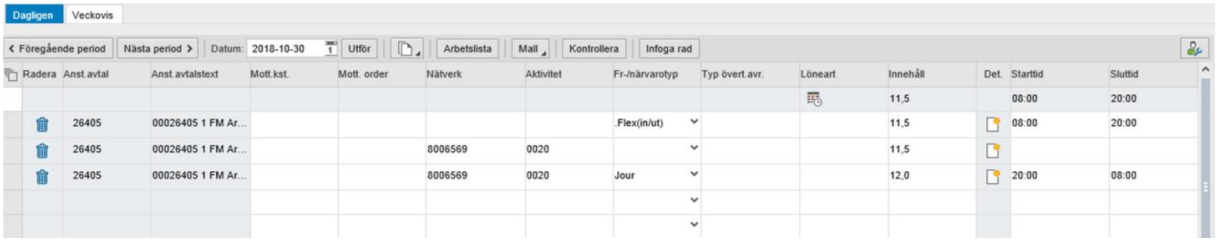
Om användbarhet och säkerhet behandlas i designprocessen kan båda delarna tas hänsyn till för designmålet (Allen & Komandur, 2019). Genom positiva tekniker beskriver Holmes och Ophoff (2019) något som förbättrar produktiviteten och effektiviteten av ett system som nödvändiga och som ger ett direktvärde till användarna, medan säkerhetstekniker är till för att skydda användaren och systemet, men när det implementeras fel kan det uppkomma svårigheter för användaren.

I den allt mer digitaliserade värld som är under ständig utveckling visar tidigare studier att det behövs göras ett fördjupande arbete inom användbarhet och säkra it-system (Nwokedi, Amunga & Rad, 2016; Allen & Komandur, 2019). Baserat på tidigare forskning och statistik finns det en möjlighet att undersöka vidare mer specifikt vilka konsekvenser bristande användbarhet i säkra it-system kan ha.

1.1 PRIO

Försvarsmaktens säkra it-system benämns PRIO och är ett ekonomi- och resursledningssystem. Projektet startade med en analysfas år 2004 och Försvarsmakten började införa programmet år 2009 (Engevall, 2013).

PRIO bygger på affärssystemet SAP S/4HANA som är en oberoende branschlösning och återfinns i våra nordiska grannländer men även hos ett stort antal försvarsmakter världen över. Från förbandsenheters lägsta nivå till den högsta kan PRIO behovsätta och tillgångsredovisa personal, materiel och infrastruktur genom att komplementera SAP med DFPS (Defence Forces and Public Security). Denna undersökning fokuserar på PRIOs tidrapportering, se figur 1.1.



Figur 1.1 *Bild på tidrapportering i PRIO* (Officersförbundet, 2018)

Tidrapporteringen i PRIO låter de anställda inom Försvarsmakten rapportera arbetstid, tillägg och uttag under månaden. Exempel kan vara arbetstimmar, jour, övertid, försvarsmaktsdygn och flextid. Detta görs genom att användaren skriver in koder som är kopplade till olika konton (Nätverk, Figur 1.1), dessa konton belastas när lönerna ska utbetalas. I tidrapporteringen kan anställda skapa en mall utifrån egna preferenser med återkommande konton, typer av tillägg och uttag (från-/närvarotyp, figur 1.1) eller ersättningar. Dessa mallar fungerar som hjälpmedel för att fylla i tidrapporteringen.

1.2 Syfte och frågeställning

Vi har hittat forskning om designriktlinjer för att öka användbarheten i säkra it-system (Yee, 2005; Nwokedi, Amunga & Rad, 2016; Nurse, Creese, Goldsmith & Lamberts, 2011; Still, Cain & Schuster, 2017; Hof, 2015; Hof & Socher, 2016; Sahar, 2013), rapporter om att it-incidenter klassade som handhavandefel har ökat (MSB, 2019; 2020), samt att problem med användbarheten kan få konsekvenser i it-system (Mohammed et al., 2017). Det finns dock ingen forskning om vilka konsekvenserna faktiskt blir av bristande användbarhet i säkra it-system.

För att fylla denna kunskapslucka kommer vi utföra en heuristisk utvärdering i det säkra it-systemet PRIO. Detta för att undersöka användbarheten, genom att se om det följer redan framtagna designriktlinjer, både generella och för säkra it-system, och vilka konsekvenserna är av implementeringen av användbarheten.

Syftet med undersökningen är att undersöka i vilken grad PRIO som ett säkert it-system följer designriktlinjerna i förhållande till implementering av användbarhet och vilka konsekvenser det har med fokus på den del av PRIO där användare registrerar arbetstid (tidsrapportering).

Frågeställningen som vägleder denna undersökning är:

> *Vad är konsekvenserna av hur användbarheten implementerats i det säkra it-systemet PRIO?*

Undersökningen kan potentiellt bidra till ytterligare kunskaper inom området och förhoppningsvis introduceras nytt underlag för vidare forskning. Undersökningen utgår från ett säkert it-system hos en myndighet och skulle kunna bidra till en ökad förståelse för vad konsekvenser gällande användbarhet kan leda till i säkra it-system.

1.3 Avgränsningar

För att göra undersökningen möjlig har vi valt att avgränsa oss till personal inom försvarsmakten inom denna fallstudie.

Undersökningen är också avgränsad till nuvarande anställda soldater inom Försvarsmakten som arbetar på heltid (GSS/K) och använder tidrapporteringen i PRIO. Detta för att de använder PRIO i mer utsträckning och har mer erfarenhet av it-systemet än de som jobbar på deltid (GSS/T).

Denna uppsats är inte en undersökning i hur säkra it-systemen är, utan en undersökning av användbarheten i PRIO och konsekvenserna av den.

1.4 Begreppsdefinitioner

Användbarhet - (**Usability**) I vilken utsträckning en artefakt kan användas för att uppnå sitt mål (Klaassen, van Beijnum och Hermens, 2016).

Gruppbefäl Soldat Sjöman - Kontinuerligt tjänstgörande (GSS/K) - Anställda soldater som arbetar inom Försvarsmakten på heltid (Försvarsmakten, u.å.).

Säkra it-system - Ett it-system där konfidentialiteten, integriteten och tillgängligheten av information är säkerställd (ISO/IEC, 2018).

2 Litteraturgenomgång

2.1 Informatik

Begreppet informatik myntades inte förrän i mitten på 1900-talet av Steinbuch (1957 i Widrow, Hartenstein & Hecht-Nielsen, 2005). Idag spelar informatik en viktig roll i samhället då digitaliseringen ökar kraftigt. Enligt Goldkuhl (1996) och Goldkuhl och Röstlinger (2019) så innebär informatik att studera människors användning av informationssystem i praktiken.

2.2 It-säkerhet

Forskning om kommunikationssystem är ett gammalt område där en av de första inom det var Auguste Kerckhoffs som skrev om säkra kommunikationssystem (communications security system) och vad som behövdes för att kunna hålla de säkra redan år 1883 (Kerckhoffs 1883 i Gutmann & Grigg, 2005).

Rötterna inom it-säkerhet började dock på 1960-talet när datorer kopplades upp med varandra via nätverk som senare blev grunden till internet (Warner, 2012). En av de tidigare författarna inom området var Peters (1967) som redan då hävdade att en total it-säkerhet är omöjlig att uppnå. Med it-säkerhet menas att säkerställa ett it-system och dess tillgångar, såsom informationstillgångar, användare, programvara, kommunikation, nätverk och enheter (Azmi, Tibben & Win, 2018).

It-säkerhet är idag ett globalt fenomen med komplexa utmaningar för företag och regeringar medan allmänhetens medvetenhet är begränsad. Nyckeln att få ut information till allmänheten är genom att kommunicera it-säkerhet med användarna och skapa policys för it-säkerhet. Genom ökad medvetenhet kan användarna bidra till ett ökat it-säkerhetsklimat och vara bättre förberedda för att undvika missförstånd och osäkerhet (de Bruijn & Janssen, 2017).

2.3 Användbarhet

Internationella standardiseringsorganisationen har kommit ut med standarden ISO 9241-11:2018(E) (2018) som beskriver användbarhet som:

> Extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. … The “specified” users, goals

> and context of use refer to the particular combination of users, goals and context of use for which usability is being considered.
>
> ISO, 2018, s. 2

Enligt ISO baseras användbarheten på hur väl ett system kan användas av de tänkta användarna för att nå specifika mål i användningen. ISO menar att designa för användbarheten inte gör en design direktanpassad till alla användare och uppgifter utan fokuserar på specifik målgrupp och mål. Vidare skriver de att problem vid användning ska hållas så låga som möjligt och låta de problem som uppstår vara minimala. Detta går i linje med det Bevan et. al. (2016) skriver gällande att det är viktigt att ha i åtanke de konsekvenser som kan uppstå vad gäller felaktig användning.

Enligt Hassenzahl och Tractinsky (2006) är huvudmålet med designen att bidra till en förbättrad livskvalitet genom att designa för välbehag istället för frånvaron av obehag. Ett problem med design kan vara att systemutvecklare antar att deras användare kan agera helt rationellt i alla interaktioner med systemet, något som bortser från mänskliga beteenden (Norman, 2013). Handhavandefel på grund av bristande design är något Norman uppmärksammade redan år 1983 (Norman i Cranor & Garfinkel, 2004). Ett dåligt system ökar då riskerna för handhavandefel i och med stress och oförståelse som därmed leder till fel i systemet.

Anledningar till att användare misslyckas att använda säkra system på bästa sätt är att säkerhetssystem fallerar med att implementera användbarhet i deras design (Möller, Ben-Asher, Engelbrecht, Englert & Meyer, 2011). Konsekvenserna, enligt författarna, är att med en högre säkerhet så sänks användbarheten och tvärtom. Nurse, Creese, Goldsmith och Lamberts (2011), som även har utvecklat designriktlinjer för säkra it-system, beskriver användbarhet som en av de viktigaste delarna av it-säkerhet idag där otillräcklig användbarhet ersätts med it-säkerhetsverktyg och funktioner som visar sig begränsa effektiviteten.

Holmes och Ophoff (2019) beskriver två sätt vid förändring av ett system relaterat till användbarhet och säkerhet, positiv design: något som ökar produktiviteten, som ofta uppfattas som nödvändigt och ger ett direktvärde hos användarna. Eller säkerhetsteknologi, som oftast ses som besvärligt hos användarna då implementeringen oftast leder till fler steg för användarna innan de kan använda systemet. Utmaningen enligt Mohammed et al. (2017) är att hitta balansen mellan säkerhetsnivån och förväntningen från användarna. Balansen inom säkra it-system förklaras med att om svårighetsgraden att komma in höjs minskar användbarheten men om man höjer användbarheten riskeras säkerheten, precis som Möller et al. (2011) skriver. Enligt Mohammed et al. (2017) är det upp till utvecklarna att hitta en bra nivå, men också att ett it-system med hög användbarhet leder till färre problem med säkerhet. Allen och Komandur (2019) samt Yee (2005) beskriver användbarhet i säkra

it-system som när användbarhet och säkerhet hjälper varandra. Vad de menar är att säkerhet och användbarhet inte nödvändigtvis behöver vara motpoler, utan att det går att ha båda två samtidigt.

Tidigare studier inom telehälsa i säkra it-system visar att ökad användbarhet i verktygen gör det möjligt att få minskade kostnader och specialiserad vård utan att behöva ta sig till sjukhus (Solana, Cáceres, García-Molina, Opisso, Roig, Tormos & Gómezs, 2014; Klaassen, van Beijnum & Hermens, 2016). Även inom banksektorn har ökad användbarhet lett till minskade kostnader där både användbarhet och säkerhet har implementerats tidigt i utvecklingen av systemen, jämfört med om detta har lagts till i senare stadier (Alarifi, Alsaleh & Alomars, 2017). Detta visar på att det finns fördelar med att ha både användbarheten och säkerheten i åtanke under utvecklingen av ett it-system.

Användbarheten i säkra it-system är som tidigare nämnt en viktig del att ta hänsyn till för att minska handhavandefel och kostnader. Men vilka konsekvenser kan det egentligen leda till om användbarheten brister? Om det är så att användarna inte kan använda sig av systemet (användbarhet) på grund av bristfälliga funktioner och oförståeliga tillvägagångssätt, påverkas säkerheten av det då?

2.4 Designriktlinjer för användbarhet

2.4.1 Generella designriktlinjer

Som del i användbarhet så har flera generella designriktlinjer tagits fram för vägleda utvecklingen av designen av it-system (Norman, 2013; Nielsen, 1994; Nwokedi, Amunga & Rad, 2016). Designriktlinjer handlar om att hjälpa designers skapa artefakter som är enkla att förstå och använda för så många som möjligt. Norman (2013) har sju övergripande designriktlinjer:

1. *Konceptuell modell* (conceptual model) som hänvisar till att designen skapar en god modell av systemet som ska leda till förståelse och kontroll, det förbättrar utvärderingen och upptäckbarhet av resultatet.
2. *Synlighet* (discoverability) som visar möjliga val i ett aktuellt tillstånd i systemet.
3. *Återkoppling* (feedback) där information kontinuerligt visar resultatet av åtgärden i systemet.
4. *Signifant* (signifiers) beskrivs som uppvisandet av de möjliga funktionerna.
5. *Kartläggning* (mapping) är förhållandet mellan kontroller och handlingar som ska följa god logik.

6. *Affordans* (affordances) hur produkten leder till en viss typ av användning.

7. *Begränsningar* (constraints) är tänkt att styra användarens handlingar och underlätta tolkningen av systemet genom bland annat logiska och semantiska begränsningar.

Jakob Nielsen (1994) jämförde och sammanställde en lista på nio designriktlinjer från egna texter och existerande designriktlinjer från olika företag och andra forskare som ska motverka de flesta problem som kan uppstå i en artefakt och leda till ökad användbarhet. Nielsen (ibid.) beskriver processen med att undersöka ett it-system med dessa designriktlinjer som en *heuristisk utvärdering*, som ett sätt att förbättra användbarheten med hjälp av att se var användbarheten sjunker och att komma med förbättringar där det behövs.

1. *Tydlighet i systemstatus* (visibility of system status)

2. *Matcha systemet och den riktiga världen* (match between system and the real world)

3. *Användarkontroll och frihet* (user control and freedom)

4. *Konsekvent och standarder* (consistency and standards)

5. *Förebyggande av fel* (error prevention)

6. *Igenkännande snarare än hågkoms*t (recognition rather than recall)

7. *Flexibilitet och effektiv användning* (flexibility and efficiency of use)

8. *Estetisk och minimalistisk design* (aesthetic and minimalist design)

9. *Hjälp användare känna igen, diagnostisera och återställning av fel* (helping users recognise, diagnose and recover from errors)

Nwokedi, Amunga och Rad (2016) definierar fyra designriktlinjer med målet att minska gapet mellan användbarhet och säkerhet i utvecklingsstadiet.

1. *Bekvämlighet* (convenience) som innebär att förhindra störningar för användaren i systemet som kan uppfattas som besvärliga eller tidskrävande, något som användaren sannolikt kommer stänga av för att minska avbrott.

2. *Förståeligt* (understandable) vilket uppmanar utvecklarna att skapa design som användaren förstår sig på och känner igen snarare än att minnas ett specifikt förfarande.

3. *Inkludernade* (inclusivity) beskriver att anpassa ett säkerhetssystem till alla olika typer av användare, oavsett tidigare färdigheter, intuition eller genom att begränsa friheten. Det ska vara tydligt vad användaren ska göra på alla nivåer.

4. *Krav* (requirement) beräknar egenskaperna som krävs för att nyttja systemet, om systemet har en svårare säkerhetsnivå behöver användarnas tekniska skicklighet och kunskap värderas.

2.4.2 Specifika designriktlinjer för säkra it-system

Utöver de generella designriktlinjerna har flera olika författare presenterat designriktlinjer som är riktade till säkra it-system (Yee, 2005; Nwokedi, Amunga & Rad, 2016; Nurse, Creese, Goldsmith & Lamberts, 2011; Still, Cain & Schuster, 2017; Hof, 2015; Hof & Socher, 2016; Sahar, 2013).

Yee (2005) skriver att en stor del av användbarhet i säkra it-system är att sätta användarnas gränser till så få rättigheter som möjligt samt att det finns tydlighet i vad användaren kan och inte kan göra i systemet, till exempel som att tydligt indikera de konsekvenser som användarens handlingar kommer leda till. Yee (2005) beskriver tio designriktlinjer:

1. *Låt användaren få den enklaste vägen att göra tänkt uppgift med minst antal rättigheter* (Match the most comfortable way to do tasks with the least granting of authority)

2. *Skilj mellan objekt och handlingar med regler som är relevanta för vad användarna vill göra* (Draw distinctions among objects and actions along boundaries relevant to the task)

3. *Låt användarna använda säkerhetspolicys på sätt som passar användarna* (Enable the user to express safe security policies in terms that fit the user's task)

4. *Indikera tydligt konsekvenserna som användarnas handlingar kommer leda till* (Indicate clearly the consequences of decisions that the user is expected to make.)

5. *Auktorisera användare om de visar att de vill det* (Grant authority to others in accordance with user actions indicating consent)

6. *Låt användare ta bort andras auktoritet för att begränsad åtkomst av information* (Offer the user ways to reduce others' authority to access the user's resources)

7. *Håll koll på andras auktoritet i förhållande till användarens val* (Maintain accurate awareness of the user's own authority to access resources)
8. *Håll koll på användarens auktoritet i förhållande till användarens möjlighet att kolla på resurser* (Maintain accurate awareness of others' authority as relevant to user decisions)
9. *Presentera objekt och handlingar med hjälp av särskilda drag* (Present objects and actions using distinguishable, truthful appearances)
10. *Skydda användaren från andra som manipulerar den auktoritet på användarens vägnar* (Protect the user's channels to agents that manipulate authority on the user's behalf)

Vissa av Yees (2005) designriktlinjer fokuserar mer på ren säkerhet och hur den ska implementeras än användbarhet. Undersökningens frågeställning gör det problematiskt att kontrollera ett säkert it-system där sekretess råder, därför valdes dessa bort. Designriktlinjerna från Yee (2005) som valdes bort var: *Håll koll på andras auktoritet i förhållande till användarens val*, *Håll koll på användarens auktoritet i förhållande till användarens möjlighet att kolla på resurser* och *Skydda användaren från andra som manipulerar den auktoritet på användaren vägnar*.

Utöver Nwokedi, Amunga och Rad (2016) generella designriktlinjer för användbarhet har de även specifika regler utformade för säkra it-system. *Avslöjande* (revelation) syftar till att bevara åtkomstnivåer som är anpassade för användarna och systemet. Ett exempel är genom frekvent popup varning där användaren godkänner cookies som samlar viss information som annars skulle förblivit privat. Nwokedi, Amunga och Rad (2016) har fler designriktlinjer för säkra it-system men på grund av fokus på säkerhet hellre än användbarhet, användarupplevelse eller design valdes dessa att kategoriseras med resterande designriktlinjer. Dessa var *Sekretess*, *Integritet*, *Brytbarhet* och *Överflöd*.

Nurse, Creese, Goldsmith och Lamberts (2011) har tagit fram dessa designriktlinjer för säkra it-system:

1. *Säkerhetsanvändbarhet borde läggas till tidigt* (Cybersecurity usability should be considered early on)
2. *Ackommodera alla typer av användare* (Accommodate all types of users)
3. *Ge relevant feedback* (Give informative feedback)
4. *Erbjud hjälp, tips och dokumentation* (Provide help, advice and documentation)

5. *Motverka fel, handling, återställning/ångra* (Error prevention, handling and recovery/Undo)
6. *Insyn i systemstatus* (Allow for visibility of system state)
7. *Gör säkerhetsfunktionalitet både synlig och lättåtkomlig* (Make security functionality visible and accessible)
8. *Reducera kognitivstress associerad med systemanvändning* (Reduce cognitive load associated with system activities)
9. *Visa vilka uppgifter användarna måste göra och när, ge support vid behov* (Give guidance on what tasks users need to perform and where necessary, provide recommendations support)
10. *Värna en positiv upplevelse och hög nöjdhet hos användarna* (Emphasise a positive system experience and good levels of user satisfaction)
11. *Estetisk och minimalistisk design* (Aesthetic and minimalistic design)
12. *Designa för lättlärdhet* (Design for learnability)
13. *Minimera användningen för tekniska och säkerhetsspecifika termer och uttryck* (Reduce use of technical and security-specific terms and jargon)
14. *Underlätta för skapandet av en tillförlitlig mental modell* (Facilitate the creation of an accurate mental model)
15. *Designa för säkerhet i alla delar av applikationen* (Design security into all application layers)
16. *Designa systemet så att säkerheten inte påverkar prestandan* (Design such that security does not reduce performance)
17. *Verktyg är inte lösningar* (Tools are not solutions)
18. *Dela upp separata koncept* (Separate distinct concepts)
19. *Administrativa verktyg kan behöva ytterligare jobb med användbarheten* (Note that security management interfaces may need additional usability considerations)

Vad gäller Nurse et al. (2011) så väljs designriktlinjerna *Verktyg är inte lösningar* och *Adminverktyg kan behöva ytterligare jobb med användbarheten* bort. Dessa kan tolkas vara mer som specifika synpunkter och observationer än designriktlinjer.

Still, Cain och Schuster (2017) har en lista på sex designriktlinjer som ska leda till enklare användning av säkra it-system, skillnaden beskrivs från förr när pengar togs ut

på banken till nutid där att ladda ner en app är det enda som behövs. Det utgör möjligheten för hackare att få åtkomst till bland annat bankuppgifter från avlägsen plats men med hjälp av människocentrerade tillvägagångssätt av lösenordsverifiering kan användbarhet i systemen förhindra eller åtminstone minska förluster av värdefull information. Still, Cain och Schuster (2017) beskriver designriktlinjerna:

1. *Designa för att vara inkluderande* (Design to be Inclusive)
2. *Undvik att överbelasta användarnas arbetsminne* (Avoid Draining Users' Limited Working Memory Resources)
3. *Informera och undervisa användare om risker* (Inform and Educate Users about Risk)
4. *Undvik fackspråk och underlätta användarens mentala modell* (Eliminate Jargon by Considering Users' Mental Models)
5. *Låt de rätta funktionerna vara lätta att utföra* (Make Appropriate Actions Apparent)
6. *Erbjud snabb åtkomst till möjliga funktioner* (Provide Users Quick Access)

Hof (2015) har forskat fram designriktlinjer utefter egna erfarenheter som it-säkerhetsutbildare under flera år och samtidigt erfaren designer åt produkter som kräver it-säkerhetsmekanismer för användaren. Slutsatsen blev en lista med designriktlinjer som baseras på säkerhetsanvändningsfelen (Hof & Socher, 2016).

Hof (2015) och Hof och Sochers (2016) designriktlinjer beskrivs som:

1. *Låt alla användare förstå systemet* (Understandability for all users)
2. *Bemyndiga användare* (Empowered users)
3. *Effektivisera användarnas uppmärksamhet och memoreringsförmåga* (Efficient use of user attention and memorization capabilities)
4. *Låt användare bara göra informerade beslut* (Only informed decisions)
5. *Undervisa användarna i säkerhet* (Educating reaction on user errors)
6. *Gör användningen så lätt som möjlig* (No jumping through hoops)
7. *Konsekvent* (Consistency)
8. *Säkerhet som standard* (Security as default)
9. *Låt systemet främja säkerhet* (Fearless System)

En viktig fråga i design av moderna datorprogramvara är användbarhet och säkerhet där det fortfarande finns utrymme att förbättra relationen kring lämplig distribution mellan dessa två i funktioner, de fyra designriktlinjer som Sahar (2013) föreslår riktar sig mot utvecklingsprocessen och kan appliceras i säkra it-system:

1. *Tillfredsställdhet och säkerhet* (Satisfaction and Security) syftar till förtroendet för systemet för både användarna och utvecklarna, första prioritet är användarvänlighet och det andra är säkerheten kring informationen, framförallt när det gäller transaktioner och betalningar.

2. *Effektivitet och säkerhet* (Effectiveness and Security) är att prioritera säkerhet från ett tidigt stadie genom att integrera systemet med användbar säkerhetsdesign.

3. *Verkningsgrad och säkerhet* (Efficiency and Security) syftar till att kunna hantera en viss nivå av säkerhetsfunktion i ett specifikt sammanhang med snabbhet och noggrannhet, till exempel vid autentisering och integritet.

4. *Lättlärdhet och säkerhet* (Learnability and Security) överväger processen att lära sig systemet mot säkerheten, med lättlärdhet kan utvecklarna införa korrekt säkerhet kring funktionerna.

2.4.3 Jämförelse - generella och säkra designriktlinjer

De generella designriktlinjerna är utformade till att fokusera på användbarheten i system, artefakter och i digitala fenomen. De generella är användbara mot den stora, ‘generella’, designen, dessa kan appliceras mot de övergripande designpunkterna som en designprocess kan innehålla, men behöver nödvändigtvis inte kunna appliceras mot specifika säkra it-system.

Till skillnad från de generella designriktlinjerna har säkra designriktlinjer utvecklats från erfarenhet, empiri och problematik av redan existerade säkra it-system. Säkra designriktlinjer utformas utifrån empiri, genom förståelse för sämre användbarhet inom säkra it-system finner forskare nya och mer specifika designriktlinjer som tydligt befinner sig där användare har svårigheter att använda sig av säkra it-system. Säkerhet är det tydliga ledordet bland dessa designriktlinjer (se tabell 2.2, bilaga 2), men effektivisering och informering är två vanligt förekommande riktlinjer i olika böjningsformer och definitioner.

Kategorin Effektivisera handlar om att göra uppgifter som användaren vill utföra så enkla som möjligt, framförallt genom att underlätta användarens memoriseringsförmånga. Den andra kategorin är Informera, där systemet bör informera användaren om den information som behövs vid användning.

2.4.5 Kategorisering av designriktlinjer

För att lättare få en helhetsbild över både generella designriktlinjer och riktlinjer för säkra it-system så valde vi att kategorisera dem. Detta ledde till kategoriseringen nedan, se även tabell 2.1 och 2.2 (bilaga 1 respektive 2).

2.4.5.1 Generella designriktlinjer

Utifrån nämnda forskare på generella designriktlinjer listas en sammanställning av fyra kategorier (se tabell 2.1, bilaga 1) och nedan beskrivs varje kategori:

Den första kategorin är *Välbehag* och samlar tre designriktlinjer, dessa är *bekvämlighet* (Nwokedi, Amunga & Rad, 2016), *matcha systemet och den riktiga världen* (Nielsen, 1994), och *konceptuell modell* (Norman, 2013), se tabell 2.1. Dessa designriktlinjer ska ge användaren belåtenhet genom att minska på besvärliga moment, skapa en förståelse kring systemet och uttrycka sig transparent mot det yttre.

Andra kategorin är *Förståelse* som inkluderar *förståeligt* (Nwokedi, Amunga & Rad, 2016)*, tydlighet i systemstatus* (Nielsen, 1994)*, konsekvent och standarder* (ibid.), *synlighet* (Norman, 2013)*, återkoppling, signifanter* och *kartläggning* (ibid.). Utvecklarnas ansvar ligger i att skapa design som fungerar och är lätt att använda, genom synlighet i systemet med tydlig återkoppling, märkbara funktioner och med god designlogik är denna kategori till för att skapa förståelse och harmoni för användarna.

Nästa kategori nummer tre, *Uppmärksamhet*, som innehåller *inkluderande* (Nwokedi, Amunga & Rad, 2016), *användarkontroll och frihet* (Nielsen, 1994), *igenkännande snarare än hågkomst*, *flexibilitet och effektiv användning* (ibid.), *affordanser* (Norman, 2013) och *begränsningar* (ibid.). Designriktlinjerna syftar till vaksamhet och genom att avgränsa användarna från onödiga funktioner och underlätta hanteringen och tolkningen av systemet. Med rätt begränsningar i systemet kan användarna tyda funktionerna bättre och bli mer uppmärksamma på de uppgifter som de har befogenheter att utföra.

Den fjärde och sista kategorin på generella designriktlinjer är *Pretention* och innehåller *krav* (Nwokedi, Amunga & Rad, 2016) och *förebyggande av fel* (Nielsen, 1994). Att ställa behov och förutsättning som utgångspunkt skapar en tydligare designprocess för utvecklarna att från start utforma systemet för de olika användare och användningsområden som systemet kan komma att använda. Med ovan i åtanke förebyggs detta fel längre fram i designprocessen.

2.4.5.2 Säkra designriktlinjer

Utöver generella riktlinjer så har vi även kategoriserat säkra riktlinjer som sammanställt dem i sju kategorier (se tabell 2.2, bilaga 2) och nedan beskrivs varje kategori:

Första kategorin är *Enkelhet* som vill göra det lätt för användaren att förstå systemet, inkludera användaren och skapa tillfredsställdhet. Detta kan göras genom minimalistisk och estetisk design som främjar på lättlärdhet. *Enkelhet* består av designriktlinjerna *Estetisk och minimalistisk design* (Nurse et al., 2011), *Designa för lättlärdhet*, *Ackommodera alla typer av användar*e *(ibid.)*, *Designa för att vara inkluderande* (Still, Cain & Schuster, 2017), *Låt alla användare förstå systemet* (Hof och Socher, 2016), *Bemyndiga användare* (ibid.).

Andra kategorin är *Effektivisering*. Samtliga forskare som nämnts tidigare har minst en designriktlinje i kategorin *Effektivisering*. Många system är främst skapta för en hög säkerhet men glömmer lätt slutanvändaren och säkra it-system generellt kallas oftast för ineffektiva system. Genom att addera säkerhetsanvändbarhet tidigt i designprocessen kan system effektiviseras och underlätta för användaren. Det skapar mindre stress i systemanvändningen och användaren kan enklare lösa tänkt uppgift utan att överbelasta användarens arbetsminne. *Effektivisering* består av designriktlinjerna *Låt användaren få den enklaste vägen att göra tänkt uppgift med minst antal rättighete*r (Yee, 2005), *Skilj mellan objekt och handlingar med regler som är relevanta för vad användarna vill göra* (ibid.), *Avslöjande* (Nwokedi, Amunga & Rad, 2016), *Säkerhetsanvändbarhet borde läggas till tidigt* (Nurse et al., 2011), *Reducera kognitiv stress associerad med systemanvändning*, *Underlätta för skapandet av en tillförlitlig mental modell*, *Dela upp separata koncept*, *Undvik att överbelasta användarnas arbetsminne*, *Ge relevant feedback* (ibid.), *Effektivisera användarnas uppmärksamhet och memoreringsförmåga* (Hof & Socher, 2016) och *Effektivitet och säkerhet* samt *Tillfredsställdhet och säkerhet* (Sahar, 2013).

Tredje kategorin är *Informera* och syftar till att erbjuda användaren information och modifikation som passar dess handlingar och skapa medvetenhet. Kategorin innehåller två grupperingar, den första är att informera användaren och ge tips, den andra grupperingen är att undervisa om risker och säkerhet. Användaren ska medvetet ta beslut och när något leder till risker ska användaren förstå vad risken har för konsekvenser. *Informera* innehåller designriktlinjerna *Låt användarna använda säkerhetspolicys på sätt som passar användarna* (Yee, 2005), *Indikera tydligt konsekvenserna som användarens handlingar kommer leda till* (ibid.), *Erbjud hjälp*, *tips och dokumentation* (Nurse et al., 2011), *Informera och undervisa användare om risker* (Still, Cain & Schuster, 2017), *Låt användare bara göra informerade beslut* (Hof & Socher, 2016), *Undervisa användarna i säkerhet* (ibid.).

Fjärde kategorin är *Allmänspråk* och betyder att systemet ska hålla språket på en lämplig kunskapsnivå för användarna, minimera fackspråk och skapa en mental modell för användarna genom att länkar och rubriker är tydliga. Det skapar en förståelse för användarna i systemet *allmänspråk* består av *Minimera användningen för tekniska och säkerhetsspecifika termer och uttryck* (Nurse et al., 2011), *Undvik fackspråk och underlätta användarens mentala modell* (ibid.).

Femte kategorin är *Motverka fel* innehåller flera olika designriktlinjer som tillsammans underlättar användningen av systemen. Lättlärt system, enkelhet i användningen hos de vanliga funktionerna och skapa den design som är konsekvent som bidrar till en naturlig användning av systemen och dess funktioner, vilket bidrar till minskade irritationsmoment. *Motverka fel* innehåller designriktlinjerna *Auktorisera användare om de visar att de vill det* (Yee, 2005), *Låt användare ta bort andras auktoritet för att begränsa åtkomst av information*, *Presentera objekt och handlingar med hjälp av särskilda drag* (ibid.), *Motverka fel*, *handling, återställning/ångra* (Nurse et al., 2011), *Visa vilka uppgifter användarna måste göra och när*, *Ge support vid behov* (ibid.), *Låt de rätta funktionerna vara lätta att utföra* (Still, Cain & Schuster, 2017), E*rbjud snabb åtkomst till möjliga funktioner* (ibid.), *Gör användningen så lätt som möjlig* (Hof & Sochers, 2016), *Konsekvent* (ibid.), *Verkningsgrad och säkerhet* (Sahar, 2013) och *Lättlärdhet och säkerhet* (ibid.).

Sjätte kategorin är *Prestanda* som visar vikten av designriktlinjen *Designa systemet så att säkerheten inte påverkar prestandan* (Nurse et al., 2011). System vars säkerhet ställer till problem i prestandan av systemen skapar irritationsmoment och tid som skulle kunna läggas på arbetsuppgifter än väntetid.

Sjunde kategorin är *Säkerhet* där Yees (2005) designriktlinjer är överrepresenterade främst eftersom auktoritet beskrivs som en tydlig avgränsning för att främja säkerhet. I dessa designriktlinjer sätts användarens auktoritet mot förhållande till valen, förhållande till möjlighet mot resurser och skydda auktoriteten mot andra användare. *Säkerhet* innehåller *Håll koll på andras auktoritet i förhållande till användarens val* (Yee, 2005), *Håll koll på användarens auktoritet i förhållande till användarens möjlighet att kolla på resurser*, *Skydda användaren från andra som manipulera den auktoritet på användaren vägnar*, *Presentera objekt och handlingar med hjälp av särskilda drag* (ibid.), *Säkerhet som standard* (Hof & Socher, 2016) och *Låt systemet främja säkerhet* (ibid.). Samt *Sekretess, Integritet, Brytbarhet och Överflöd (*Nwokedi, Amunga & Rad, 2016)

3 Metod

I detta avsnitt beskrivs hur denna undersökning har gått tillväga och vilka överväganden som gjorts. För att få svar på frågeställningen användes semistrukturerade kvalitativa intervjuer som kan användas vid utforskandet av användarnas upplevelse och perspektiv på systemet (Patel & Davidson, 2011).

Vi utgick från undersökningens frågeställning och genom kvalitativa intervjuer gjordes en användbarhetstestning i form av heuristisk utvärdering (Nielsen, 1994). Heuristisk utvärdering beskrivs som att användare bedömer ett gränssnitt utifrån riktlinjer för att identifiera problem och enklare bedöma gränssnittet (ibid.). Med hjälp av det undersöktes användbarheten i det säkra it-systemet PRIO. Intervjuerna transkriberades efter att de genomförts och bearbetades sedan genom framtagandet av olika teman som relaterade till frågeställningen.

3.1 Litteratursökning

För att samla information från tidigare forskning valde vi att använda oss av HKR Summon och Google Scholar. Vi sökte efter tidigare forskning inom it-säkerhet, användarupplevelse, användbarhet samt designriktlinjer. Sökningen började med resultat som var max 5 år gamla samt vetenskapligt granskade (peer reviewed).

Digitala databaser användes i denna undersökning var: MECS Publisher, Elsevier, Researchgate, Taylor & Francis, ACM, Springer och IEEE Xplore.

Våra sökord som användes i litteratursökningen var: Användarvänlighet, Consequences, Design guidelines interactive, Design guidelines ux, Design principles, Design secure system, Hci usability principle, Informatics, Informatics security design, Information system usability, Information technology, Security, Secure it systems, Security informatics, Security user interface, Security ux, Usability, Usable security, User experience, User friendly, User friendly interface, User friendly ux, Ux design.

3.2 Urval

Urvalskravet var att deltagarna skulle ha aktuell anställning i Försvarsmakten och att de regelbundet använde Försvarsmaktens tidrapporterings-funktion i it-systemet PRIO. Detta för att deltagarna utifrån deras erfarenhet skulle kunna svara på frågor kring deras upplevelse och tillvägagångssätt när de använde it-systemet. Generell datorvana var dock inte ett krav.

Studien bygger på bekvämlighetsurval (Denscombe, 2018) där deltagarna arbetar vid Närskydd på Luftstridsskolan i Uppsala där personal vid start av arbetspasset frågades om de frivilligt ville ställa upp på en intervju angående tidrapporteringen i PRIO.

På arbetsplatsen ställdes en öppen fråga om de närvarande anställda soldaterna var intresserade att delta i studien. Deltagarna blev tillfrågade på samma sätt inför den första studien och den andra studien. De sex första personerna till första studien som uppgav intresse uppfyllde kraven samt de två personerna till den andra studien. Dock var det en av deltagarna från den första studien som missförstod ‘använder PRIO’ till ‘har använt PRIO’, denna person hade använt funktionen för många år sedan och hade inte längre kunskap eller minne om funktionen, vilket ledde till att det blev ett bortfall av en deltagare.

Urvalet bestod av åtta personer, sju män och en kvinna. Första studien bestod av sex personer där frågorna var övergripande och i den andra studien deltog två personer. Åldern på deltagarna var mellan 27 och 34 år, varav sju deltagare var män och en var kvinna.

Tabell 3.1 *Deltagare A1-A6 i första studien, samt B7-B8 i den andra studien.*

Person #	**A1**	**A2**	**A3**	**A4**	**A5**	**A6**	**B7**	**B8**
Kön	M	K	-	M	M	M	M	M
Ålder	27	34	-	33	31	30	33	21
Erfarenhet av PRIO	7 år	5 år	-	7,5 år	9 år	10 år	8 år	2 år

Intervjun skedde dagen efter att frågan om deltagande ställts, för att låta deltagarna få betänketid samt möjlighet till att dra tillbaka sitt godkännande för intervjun.

3.3 Intervjuer

Undersökningen bestod av semistrukturerade kvalitativa intervjuer. Kvalitativa intervjuer inkluderas i en kvalitativ ansats, den insamlade datan fokuserar på mjuka värden, det vill säga immateriella ting, oftast icke mätbara där svaren handlar om användarens upplevelse av systemet vilket kan variera beroende på tidigare erfarenheter, kunnighet och svårighetsgrad (Patel & Davidson, 2011). Målet med intervjuerna var att undersöka deltagarnas upplevelser och uppfattningar av tidrapporteringen i PRIO. De kvalitativa intervjuerna utformades med en låg grad av strukturering.

Intervjuerna genomfördes i ett enskilt rum med en av skribenterna till uppsatsen och en deltagare åt gången. För bättre ljusupptagningsförmåga och ljudkvalitet användes en extern mikrofon till en mobiltelefon och intervjun spelades in genom en inspelningsapp. Samtidigt som intervjun pågick skrevs anteckningar efter hand som deltagaren svarade på frågor eller berättade själv om känslor, situationer och tillvägagångssätt i systemet. Anteckningarna användes för att ställa följdfrågor om intressanta och relevanta svar som deltagaren beskrev.

Studien ändrade frågeställning och syfte under arbetets gång, vilket ledde till att vi genomförde uppföljningsintervjuer med två extra deltagare.

Intervjuerna var mellan 11 till 28 minuter långa.

3.4 Analys

Inspelningarna transkriberades löpande under arbetets gång. Analysen genomfördes allteftersom materialet transkriberades. Det transkriberade materialet lästes igenom flera gånger för att hitta återkommande teman i svaren från deltagarna som var relevanta till frågeställningen. De kategorier som formats utifrån designriktlinjerna ledde tematiseringen för att få en tydligare bild av användbarheten i systemet. Tematiseringen gjordes separat av författarna, sedan jämfördes vad båda kommit fram till och de teman som båda var överens om fastställdes. För varje tema letades det sedan upp överensstämmande svar från deltagarna som sedan sammanställdes i mindre stycken.

3.5 Forskningsetiska principer

I undersökningen har vi tagit hänsyn till de etiska forskningsprinciper som berör deltagarna. Innan intervjuns genomförande läste vi upp missivet (se bilaga 2) där vi informerade deltagarna om syftet med studien och att deltagandet var frivilligt, anonymt, konfidentiellt och att de hade möjlighet att avbryta sitt deltagande innan, under och efter intervjun hade genomförts. Vi har inom ramen för intervjun använt oss av Patel och Davidsons (2011) fyra huvudkrav:

1. *Informationskravet*: informera om forskningens syfte.
2. *Samtyckeskravet*: deltagarna bestämmer själv över sin medverkan
3. *Konfidentialitetskravet*: personuppgifterna förvaras så att obehöriga inte kan identifiera deltagarna
4. *Nyttjandekravet*: uppgifter om deltagarna får endast användas i ändamål för forskningen

4 Resultat & Analys

Detta avsnitt avser att presentera resultatet från de kvalitativa intervjuerna i form av de framtagna temana, och underteman, och tillhörande citat. I resultatavsnittet där dialog genomförts mellan deltagaren och frågeställaren definieras deltagaren utifrån tabell 3.1 och frågeställaren med “F:”.

De teman vi arbetat fram är följande:

- *Brist på enkelhet*
- *Effektivitet*
- *Brist på information*
- *Motverka fel*
- *Prestanda*

4.1 Brist på enkelhet

Studiens första tema, *Brist på enkelhet*, handlar om att deltagarna tyckte PRIO var svårt att förstå, undertemana Komplicerat och Språk beskriver detta närmare.

4.1.1 Komplicerat

Undertemat Komplicerat handlar om hur PRIOs tidrapportering uppfattas som komplicerad och svår att använda. Deltagarna berättar att de har lärt sig systemet på rutin men när de ska göra andra saker så kan det skapa problem för dem.

Både deltagare A1 och B7 berättade om tidrapporteringens flera steg med många val, där B7 lyfte fram hur ett system går att använda fast det inte upplevs som enkelt.

> Det är väl förståeligt i den grad att man har gjort i stort sett samma sak i 8 år, så man har väl lärt sig de delarna. Men för en ny, är det inte speciellt lätt. … Jag gör egentligen samma sak varje vecka, så det har väl blivit lätt med åren. Det är inte så användarvänligt tycker jag.
>
> — B7

Fler håller med, även A4 beskriver det som “så det inte behöver kännas som raketvetenskap för en nyanställd soldat att sätta sig” in i PRIO.

Ett annat problem som B7 tar upp är att han tycker att det är svårt om de behöver göra nya saker.

> Det är väl just det när man ska göra nya saker. Om det blir något utbildning kanske. Eller något extra man ska fylla i. Så blir det andra

> konton, då måste man in och ändra där. Det gör man inte varje vecka, så måste man tänka efter lite. Då är det ett par tre undermenyer man går igenom och ändra lite saker. Just om man ska få ersättning om man bor i anvisat boende till exempel, då är det, det är inte bara att trycka i en ruta så får man det.
> — B7

Jour registrering togs även upp som något komplicerat. Att registrera jour i tidrapporteringen hade A5 och B8 svårigheter med.

> Som jag sa innan, det är komplext. Det följer inte... Det har inte en logisk gång. Tycker inte jag i alla fall. … Sen tycker jag det inte gör det utan det har inte en röd tråd som du kan klicka in för du tror det är dit, för det är förmodligen inte där.
> — B8

> Nja, för mig så är det väl att registrera jour för då blir den lite spegelvänd för tiden som står i PRIO är arbetstid så det blir lite spegelvänt. Så det för mig är lite krångligt.
> — A5

A5 kommenterade även att jouren inte räknades ut automatiskt utan var något han behövde räkna ut själv.

B8, B7 och A6 beskriver att inloggningskortet behövs för att kunna använda PRIO.

> Om man då inte har det där kortet med sig en vecka så ska man försöka leta rätt på alla de här grejerna i efterhand och aaa...det blir struligt om man inte reggar, eller har kortet på sig hela tiden och kan regga veckovis om man säger så.
> — A6

4.1.2 Språk

Vad gäller undertemat Språk tyckte A4 att språket inte var optimerat för de som använder tidrapporteringen, det vill säga soldaterna.

> Det är gjort på ett väldigt, väldigt, korrekt och militäriska, och det är inte... Hade man suttit och googlat synonymer så hade man fått upp det ord man söker. Eh, men det är också stylat det, vad det känns som i alla fall, efter någon som sitter på ett kontor och arbetar och som vet exakt var de olika placeringarna ligger i systemet.
> — A4

4.2 Effektivitet

Andra temat vi kom fram till var *Effektivitet*, detta handlar om att PRIO upplevs som oeffektivt av deltagarna. Undertemana Specificering, Utbildning samt Trögt system förklarar detta närmare.

4.2.1 Specificering

A1 berättar om att användaren måste specificera mycket själv under användningen.

> Det jag anser är krångligt är att det går liksom inte att bara knappa in "att göra det avdraget" utan då måste jag ha, jag måste visa att ska dra det från ett speciellt konto vilket oftast är svårt att veta på förhand och det är rätt svårt att hitta i menyerna vart, vilket avdrag man ska göra. Man måste hitta en speciell spes som man ska använda då.
> — A1

A4 beskriver också att det är mycket att specificera när man ska skriva in vad man gjort i PRIO.

> Ja det gör jag efter varje pass egentligen … Registrera exakt hur man har jobbat. Vanlig arbetstid. Som har varit planerad. Jouren, om man har ätit mat på jobbet, eller tagit med själv. Knappar in det också. Om man blivit väckt på natten, kanske fått övertid någon timme, ska man fylla i det också.
> — A4

4.2.2 Utbildning

A4, A5 och B8 har fått utbildning, det A4 kallar för brukarutbildning och A5 kallar för grundutbildning. Medan A6, A2 och B7 inte har fått någon utbildning i PRIO.

> Vi har ju fått lite brukarutbildning allt eftersom, säkert att någon har varit officiell. Men ingen i närtid vad jag minns.
> — A4

> Nej som sagt, idag klarar jag mig med det jag har lärt mig med tiden men hade jag lärt mig det från början då hade det nog gått mycket enklare. Då hade jag nog sparat många felskrivningar och eventuellt sparat mig ekonomiskt en del pengar som jag har gått miste om genom åren på grund av det här.
> — A6

Från vad deltagarna har berättat är det olika om de har fått utbildning i PRIO, där vilka som har fått den och inte är blandat. Dock verkar det från intervjuerna inte leda till en effektivare användning av PRIO, detta strider mot det Still, Cain & Schuster (2017), Hof (2015), Hof & Socher (2016) visar som menar att utbildning ska hjälpa användningen.

4.2.3 Trögt system

Ett annat problem deltagarna tog upp var att systemet låser sig. En försvårad situation kan skapa irritation och A1 beskriver hur det är när det inte är enkelt.

> Ja, det är väl allmän frustration … För hela systemet låser sig om man gör någonting fel när man försöker spara. … Ja, då måste man veta vad man gjorde fel och hur man ska kunna... vad man ska byta till för att det ska bli rätt liksom.
> — A1

Hastigheten i PRIO var något som togs upp av flera deltagare.

> Systemet är ju inte så snabbt heller alla gånger så ibland när man vet precis vad man ska fylla i, då vill man hoppa mellan olika fälten ganska snabbt. …Det känns ibland som att när systemet jobbar så kanske det är på tre-fyra FPS så grejerna laggar fram lite.
> — A4

FPS betyder Frames Per Second, bilder per sekund, dessa var dock inte de faktiska bilderna per sekund, utan A4:s upplevelse av hastigheten i PRIO. A5, A6 och B8 beskrev även att hastigheten i PRIO är långsam.

4.3 Brist på information

Tredje temat var *Brist på information*, det handlar om hur deltagarna uppfattar hur it-systemet berättar om de möjliga handlingarna som går att genomföra vid specifika tillfällen under användningen. A5 tyckte att PRIO var svårförståeligt och att det inte gav tillräckligt med hjälp om hur användaren skulle genomföra de olika momenten.

> Jag tycker det svårt och inte särskilt användarvänligt. … Det finns inte så mycket information om hur man gör saker, ingen hjälptext till exempel, bara allmänt komplicerat.
> — A5

Även A1 hade problem med användningen och det är något som även B8 nämner: “Jag har ju ingen aning om hur jag arbetar mig runt i systemet för att åtgärda det här felet. Jag skulle ju inte kunna lösa det själv.” Det beskriver B7 också.

> Det är mycket, knappt cheferna vet vad som är fel egentligen när det blir fel. Så man får ju ringa helpdesk, blir det väl, HR. … Som har öppet kanske två timmar per dag. Inte super hjälpsamt.
> — B7

B7 berättar också att han inte vet vad som ska göras om han får ett felmeddelande och ingen hjälpfunktion finns tillgänglig. Även B8 håller med om att användarna inte vet vad som behöver göras vid ett felmeddelande.

Med vad deltagarna beskriver tyder resultatet på att det är svårt att åtgärda problem som uppstår, men också veta vad som behöver göras vid olika tillfällen under användningen. Detta tyder på att it-systemet strider mot det Hof (2015), Hof & Socher (2016), Nurse et al. (2011), Still, Cain & Schuster (2017), Yee (2005) skriver om att indikera tydligt vilka konsekvenser användarens handlingar kommer leda till samt att hjälpa användarna i systemet, att låta användare bara göra informerade beslut och att informera om risker.

4.4 Motverka fel

Fjärde temat var *Motverka fel*, i detta så har vi även grupperat 4 underteman (Byte av koder, Mallar, Fel i data samt Avsaknad av felmeddelande) som visar på olika problem.

4.4.1 Byte av koder

A1 kommenterar att upplägget i PRIO inte är logiskt, något som A4 håller med om.

> Ett rörigt, krångligt program. Det är inte, vad säger man, logiskt uppbyggt. Jag hade väldigt svårt att sätta mig in i det. Det blir ju inte bättre att det byts konton och koder. Det finns väldigt mycket att välja på men som känns helt orelevant och onödigt, som skulle kunna rensas bort. … Jag tycker när man går in i olika rullmenyer så ligger det väldigt mycket olika saker att välja på. Och jag har till och med svårt att se när ska det här användas?
> — A1

A4 och A6 nämnde också att det var många koder att hålla reda på som komplicerade användningen:

> Det var ju inget enkelt sätt man gjorde det på utan man var tvungen att hitta rätt koder, lägga in dem på rätt ställen, sen så bläddra i antingen i en förutbestämd katalog eller typ i friskrift länka till sidor och såna saker.
> — A6

Detta var något som även A2 höll med om: “Det blir ju inte bättre att det byts konton och koder. Det finns väldigt mycket att välja på men som känns helt orelevant och onödigt”. A1 och A4 tycke att för mycket hängde på användaren fyller i rätt koder för var pengarna ska dras ifrån.

4.4.2 Mallar

Mallarna var något som uppskattades i tidsplaneringen, men funktionen upplevs inte vara fulländad. Flera av deltagarna nämner hur en förbättrad funktion skulle kunna underlätta användningen mer i PRIO.

A1 och A6 berättar om användandet av mallar.

> Och om jag inte har det redan, man kan göra mallar, så det ser ut likadant hela tiden, och jag inte har gjort en mall så kommer jag behöva knappa in att jag vill belasta det här kontot.
> — A1

> Det beror ju på, de byter ju varje år. Så oftast får man den i början av året så gäller det ju för en själv och spara det, annars står det på olika stället där jag arbetar, just våran nakt då. Men sen sparar man ju det i en mall så man slipper ha den i huvudet.
> — A6

Utöver det så har skulle A1 även vilja kunna döpa mallarna för underlätta användningen av dem.

> Jag önskar att jag kunde döpa mallarna, och det har jag inte hittat att man kan göra, så man enklare när man sitter har fusk-tavlan framför sig att man vet vilket konto som är vilket. För sitter man helt plötsligt vid en annan dator och då är det inte lika självklart när jag tittar där: vilket var mitt hundkonto och vilket kontot för det här. Så bara kunna döpa dem skulle underlätta massor.
> — A1

4.4.3 Fel i data

A5 tyckte att det var jobbigt när inlagda tider i tidsregistreringen inte stämde vilket ledde till att chefer behöver redigera i efterhand och det kunde vara

tidskrävande.

> Ibland kan det stå fel arbetstid. Då får vi säga det till chefen så får de korrigera. Det kan ta ett tag ibland. … Han kan ju lösa det dagen efter. Han kanske har mycket och göra, då kanske det tar en eller två dagar. Men jag som pendlar från och till jobbet från en annan ort, längre bort från min arbetsplats, så kan du istället för mig betyda att jag får göra det om en eller två veckor.
> — A5

4.4.4. Avsaknad av felmeddelande

Deltagarna berättade även att det går att göra fel i PRIO, utan att det visar det. Den enda tillsägelse som användaren har fått är utanför PRIO.

> Det har hänt flera gånger att jag har fått fel lönekonto. Och då har man fått tillsägelse att "du ska inte belasta det här kontot. Nu har du tagit, ja, medel för någon annan som inte kan använda det."
> — A1

4.5 Prestanda

Femte temat, *Prestanda*, handlar om prestandan i PRIO. Prestandan är hur bra it-systemet fungerar i den vanliga användningen. Det är något som visade sig i PRIOs laddtider, det låg nere, var långsamt, det kraschade, samt dess uppdateringar, de underteman som tar upp dessa problem är Driftstörningar och Långsamt.

4.5.1 Driftstörningar

Både A1 och A5 tar upp att PRIO ofta kraschar.

> PRIO har också en tendens att krascha och ligga nere flera gånger. … Då måste jag vänta någon vecka tills jag är tillbaka och hoppas på att det funkar igen och det är inte alltid det gör. … Det är inte säkert att det är löst det det har hänt flera gånger att man kommer tillbaka och det fortfarande ligger nere. Eller de har fixats och så det ligger nere av ett annat problem …. Det står att man bara inte kan logga in eller så säger cheferna att PRIO ligger nere igen, Och så får man rycka på axlarna och se arg ut.
> — A5

A1 beskriver problem som kan uppstå då användaren försöker starta upp PRIO.

> Då måste jag först logga in. Och det gör jag med att vi har ett sånt där inloggningskort. Och då behöver man oftast vänta i fem minuter för att datorn ska starta. Därefter behöver jag vänta i nästan fem minuter till för att systemet PRIO ska gå igång. Och ibland gör det inte det och behöver starta om det flera gånger och startar man om det för många gånger så tycker datorn att "nu gör du något konstigt", så då vill den inte starta programmet alls.
> — A1

Det förekommer även driftstörningar på grund av uppdateringar i systemet.

> Ja, först loggar jag in med mitt kort och min kod. Sen öppnar jag PRIO om det inte ligger nere som det kan göra lite då och då. … Ja, det är att de i tid och otid har de ju, att de har olika körningar där de uppdaterar sina system. … Betyder att systemet kan ligga nere. Allt från några timmar till en hel helg, en hel vecka. Det är ju svårt att planera inför, för det kan dyka upp ett meddelande när startar upp PRIO. … Jag får då hoppas att om jag kanske ska åka hem på måndagen, att de har startat upp det igen. Annars får jag vänta tills nästa pass.
> — A4

Detta är något som kan göra så att de anställdas lön blir försenad till nästa månad.

> I värsta fall kan det gå över det datumet där lönen måste godkännas för att hamna på nästa lön. Så i värsta fall kan jag ju bli av med ett, kanske flera pass, det kan ju betyda ganska mycket pengar.
> — A4

4.5.2 Långsam uppstart

Kortet som A1 nämner är inloggningskontot som används för att logga in i PRIO. A2 berättade om hur lång tid inloggningen kan ta.

> Ja, jag använder mig av ett elektroniskt id-kort, som man startar datorn med. Där har man ju sin personliga kod och sen brukar det vara ganska lång väntetid. Det är gamla datorer. Så du kan gå och ta en kaffekopp under tiden och vänta tills den har startat upp.
> — A2

Utöver att inloggningen tar tid så kan ibland PRIO tycka att man behöver logga in igen.

> Det kan hinna komma upp diverse fönster som vill att jag loggar in igen fast man ska inte rör det fönstret utan den inloggningen ska ju följa med

> från att jag redan har satt i mitt elektroniska id-kort, så nej det, onödigt att det kommer upp där.
> — A2

Även B7 och B8 berättade om att inloggningen kunde ta tid.

A5 berättar att PRIO inte alltid reagerar vid uppstart: “Ja ibland får man klicka flera gånger på den där ikonen för att den faktiskt ska logga in.” B7 tycker att PRIO har blivit bättre, men att det ibland fortfarande kan vara långsamt.

Tekniska problem eller underhållsarbete kan bli ett irritationsmoment och deltagarna kan inte alltid få ut rätt lön vid utbetalning. Detta tyder att det Nurse, Creese, Goldsmith & Lamberts (2011) skriver om att säkerheten i it-system inte ska påverka prestandan av dem.

5 Diskussion

Syftet med denna undersökningen att undersöka vad konsekvenserna av hur användbarheten implementerats i det säkra it-systemet PRIO är.

5.1 Resultatdiskussion

I temat *Brist på enkelhet* beskriver deltagarna under undertemat Komplicerat att de har svårt att förstå systemets tillvägagångssätt och det tyder på att systemet inte har kunnat implementera dessa mål med att så många som möjligt ska kunna använda systemet (Nielsen, 1994; Nwokedi, Amunga & Rads, 2016). Kategorin av designriktlinjer som vi kallar Enkelhet yrkar för en design som är lättlärd och inkluderande. Att designa enkla och lättförståeliga scenarion till användare skapar en bättre förutsättning att kunna utföra handlingar och uppnå tänkt slutmål med användningen av it-systemet (ibid.). PRIO upplevs som komplext, krångligt och det medför ett par falluckor när användaren genomför diverse steg i sin process. Med förankring i resultatet genom de intervjuer som gjordes kan vi påvisa att PRIO inte följer de riktlinjer för Enkelhet vad gäller designriktlinjer i användningen och har missat att skapa en förståelig grund för användarna genom vad som vanligtvis ska vara lättlärt och inkluderande. Konsekvensen av detta blir då att deltagarna fastnar och inte vet vad de ska göra, vilket leder till att de inte kan använda sig av systemet. Vad gäller undertemat språk så var det bara en deltagare som kommenterade på att språket kunde försvåra. Detta är i linje med kategorin Allmänspråk vad gäller designriktlinjer, där ett mer lättförståeligt språk underlättar användbarheten (Nurse et al., 2011; Still, Cain & Schuster, 2017). Konsekvenser av ett komplicerat språk skulle kunna vara att information feltolkas vilket kan leda till handhavandefel. Att tidrapportera som ny användare skulle inte vara en lätt uppgift beskriver deltagarna, flera av de vi intervjuade hade använt systemet under flera års tid men tycker systemet skulle behöva vara mer förståeligt. Konsekvensen av detta är att tidsrapportera som nyanställd kräver tid och mycket arbete. Detta kan då innebära att tid tas från andra arbetsuppgifter istället.

I temat *Effektivitet* tas specificering upp som ett undertema, det vill säga att deltagarna behöver att specificera mycket information vid varje registrering. Detta strider mot vad flera författare har skrivit med att effektivisera användarnas memoriseringsförmåga (Still, Cain & Schuster, 2017; Hof, 2015; Hof & Socher, 2016).

Även utbildning tas upp som ett undertema. Vi ser att deltagarna har bristfällig utbildning inom PRIO, deltagarna upplever systemet som komplext utan en logisk gång. Konsekvensen av detta är att vissa av deltagarna inte kan vara säkra på hur de faktiskt ska använda sig av PRIO. En annan konsekvens är av bristande utbildning i PRIO är att det hade kunnat sparat deltagarna felskrivningar och andra problem. Flera

av designriktlinjerna pekar på att undervisa användarna om både risker och säkerhet inom systemet för att öka användbarheten och med det minska riskerna för handhavandefel (Still, Cain & Schuster, 2017; Hof, 2015; Hof & Socher, 2016).

Utöver det så är det ofta att it-systemet är långsamt under användning vilket skapar irritation. Detta är något som strider mot designriktlinjen flexibilitet och effektiv användning (Nielsen, 1994).

Temat *Brist på information* visar på att PRIO är svårförståeligt och att det inte gav tillräckligt med hjälp om hur användaren skulle genomföra olika moment. Vi noterar att användarna kan fastna vid ett fel och de vet inte hur ska göra för att åtgärda felet i systemet. Anledningen till att handhavandefel inträffar inom säkra it-system kan bero på att användbarheten inte är anpassad efter användarna. I kategorin Informera vad gäller designriktlinjerna så tas vikten av information i ett system upp för bra användbarhet (Hof, 2015; Hof & Socher, 2016; Nurse et al., 2011; Still, Cain & Schuster, 2017; Yee, 2005). Det handlar om att indikera tydligt kring konsekvenser vad användarens handlingar kommer leda till, att hjälpa användarna i systemet, att låta användare bara göra informerade beslut och att informera om risker (ibid.). Detta pekar på att information kan vara användbart för att minska handhavande fel och missbedömningar av handlingar, precis som Norman i Cranor och Garfinkel (2004) skriver. De skriver också att handhavandefel kan ske på grund av bristande design. PRIO har, i denna aspekt, låg användbarhet då det inte verkar hjälpa användarna med detta. Bättre information i PRIO skulle kunna öka medvetenheten och förståelsen av systemet, och samtidigt undervisa kring specifika delar.

Temat *Motverka fel* tog upp undertemat Byte av koder. Systemet är uppbyggt på så sätt att användarna själva skriver in vilka konton som ska belastas och var kostnaderna ska dras ifrån med hjälp av koder. Dessa koder får användarna utanför systemet och vi ser en risk för fel när användarna inte har korrekt informationen som de lägger in i systemet. När det är många koder att hålla reda på, och de dessutom byts ut regelbundet kan det tyckas vara extra viktigt med tydligheten kring detta. Detta går hand i hand med problematiken kring temat *Brist på enkelhet* samt temat *Brist på information*. Otydlighet i systemet gör att användarna inte förstår när det kan bli fel, genom synlighet dessa fel kan användarna själva motverka sina egna fel. Detta visar på låg användbarhet då Nielsens (1994) designriktlinje Förebyggande av fel samt Nurse et al:s (2011) designriktlinje Motverka fel förespråkar motsatsen för bra användbarhet. Konsekvenser för detta är att användarna kan skriva in fel koder när de har bytts vilket leder till att det skapar förvirring och svårigheter vilket kan leda till merarbete för användarna. Att koderna byts ut skulle kunna vara något som tillämpats för att höja säkerheten, men det verkar som att svårigheten detta skapar för användarna

Vad gäller undertemat Mallar så gavs det verktyg som underlättar tidrapportering vad gäller konton, koder och nätverk. Dessa mallar är dock begränsade på så sätt att det inte går att spara någon beskrivning på olika konton, egna noteringar, döpa om mallen

eller skapa flera mallar. Deltagarna visserligen fått hjälp till viss del, men inte fullt ut eftersom det endast är en rudimentär hjälp i form av mallen och den går inte att specificera för enstaka användare. Konsekvensen blir då att det fortfarande finns en förvirring över vad som ska göras i systemet. Detta kan kopplas till designriktlinjen Låt alla användare förstå systemet (Hof, 2015; Hof & Sochers, 2016), vi ser här att mallarna förenklar för användarna, men att det inte gör det fullt ut eftersom de inte går att anpassa. Detta kan också kopplas till kategorin Information med designriktlinjer för att inte tvinga användarna till att komma ihåg mer än nödvändigt (Nurse et al., 2011; Still, Cain & Schuster, 2017; Hof, 2015; Hof & Socher, 2016). Mallarna hjälper även med detta, men som tidigare nämnt är de begränsade. Här är en del i PRIO där användbarheten är något bättre, vilket minskar konsekvenserna.

Vad gäller undertemat Fel i data så stämde ibland inte datan som PRIO automatiskt fyller i med de tider som deltagaren faktiskt har jobbat. Detta är inget som användarna kunde ändra på själva och behöver kontakta sin chef för att kunna rätta till det. Designriktlinjen Låt de rätta funktionerna vara lätta att utföra (Still, Cain & Schuster, 2017) handlar om att rätt sak inte ska vara svår att göra. I detta fall så försenas och försvåras det hela eftersom användaren inte kan göra något själv för att åtgärda felet. Konsekvensen med detta är att saker skjuts upp blir försenade och att merarbete skapas, vilket i sin tur kan leda till försenad lön. Förvisso så skulle det kunna vara en säkerhetsfunktion att endast en person med behörigheter kan ändra datan i systemet, men eftersom datan ändå inte alltid stämmer så blir det fel. Det hade eventuellt kunnat spara tid och merarbete om deltagarna kunde ändra koderna själva och cheferna (som har behörigheten) bara kunde godkänna det.

En deltagare berättade att han vi ett tillfälle hade fått fel koder som han sedan har använt i tidrapporten och sedan skickat in utan att PRIO meddelat att det är fel koder som används. Detta går hand i hand med de problem som deltagarna tar upp i undertemat Byte av koder, att koderna kan vara förvirrande.

Att inget felmeddelande skickas ut strider mot designriktlinjen Motverka fel, handling, återställning/ångra (Nurse et al., 2011) i att it-systemet borde låta användare ångra sig och gå tillbaka till ett tidigare steg. Konsekvensen av detta blir att om användarna inte vet att de använder sig utav fel kod och det inte kommer upp något felmeddelande innan de skickar in tidrapporten så kan det leda till att de ändringar som behöver göras blir sena vilket i sin tur kan problem med utbetalning av lönen. Problematiken som tas upp här dyker även upp i temat *Brist på information*. Att inte få felmeddelanden, så att man kan motverka felen kan också ses som brist på information.

I temat *Prestanda* togs undertemat Driftstörningar upp. Deltagare berättade att PRIO har en tendens att krascha och ligga nere vilket leder till att systemet inte gick att använda när det var tänkt. Detta kan kopplas till Nurse et al:s (2011) designriktlinje Designa systemet så att säkerheten inte påverkar prestandan. Vad gäller det andra

undertemat Långsam uppstart så berörs även detta av Nurse et al:s (2011) designriktlinje. Detta är även något som strider mot den generella designriktlinjen Krav som handlar om att sätta minimumkrav på hårdvaran så att den faktiskt klarar av att köra it-systemet (Nwokedi, Amunga & Rad, 2016).

Försvarsmakten bibehåller hög säkerhet (Sahars, 2013) genom att deltagarna använder sig av inloggningskort och personlig kod för att kunna använda sig av PRIO på Försvarsmaktens intranät. Det vi ser är att denna inloggningsprocess tar lång tid för användarna, dock kan vi inte exakt säkerställa orsaken då vi själva inte hade tillgång till PRIO. Om detta är på grund av att säkerhetens laddtid att logga in användaren eller om datorerna inte är tillräckligt kraftfulla för att kunna köra programmet fick vi inte svar på. Oavsett om detta är ett problem med prestandan eller med säkerheten så kan vi konstatera är att användarna i vissa fall lämnar datorn för att göra andra saker, till exempel hämta kaffe. Konsekvensen av detta är att det leder till en stor säkerhetsrisk när datorn och de personliga inloggningskorten lämnas utan uppsikt när deltagarna inte är vid datorn. Att använda sig av inloggningskort är något som gör systemet säkrare, men om laddtiderna gör att användaren lämnar både dator och inloggningskort utan uppsikt leder det till säkerhetsrisker. Det här är ett bra exempel på vad som kan hända när säkerheten har legat i fokus för framtagandet av systemet och inte användbarheten. Vad gäller säkerheten så finns det alltså incidenter, utöver systemdesign, som påvisar människans irrationella beteenden vid interaktioner med systemet. Det vi ser här är faktumet att systemets inverkan på användaren medför säkerhetsrisker som ett utfall av systemets funktionalitet. PRIO, ur denna aspekt, upplevs inte implementera rätt nivå av användbarhet i it-systemet (Möller et al., 2011). Säkerhet och användbarhet behöver inte begränsa varandra utan kan arbeta mot samma mål, med en förhöjd användbarhet av system kan många problem undvikas genom att skapa bättre säkerhet i systemet (Allen & Komandur, 2019).

Vad gäller Hof (2015) och Hof & Sochers (2016) designriktlinjer om Säkerhet som standard samt Låt systemet främja säkerhet så handlar de om synlig och lättåtkomlig säkerhetsfunktionalitet. De handlar även om att designa för säkerhet i alla delar av applikationen, och detta kan appliceras på att PRIO kräver inloggningskort för användning, och utan kortet låses systemet. Det gör det enkelt att använda sig av denna säkerhetsfunktion. Holmes och Ophoff (2019) skriver om säkerhetsteknologi som vi också kopplar till den problematik användarna har kring långa inloggningstider vid uppstart, vilket leder till att användare lämnar datorn utan uppsikt. Ändå upplevs deltagarna vara medvetna om varför de behöver använda inloggningskortet till systemet, detta bidrar till ett ökat it-säkerhetsklimat i och runt datorerna och systemet PRIO (de Bruijn & Janssen, 2017). Här ser vi dock ett medvetet förbiseende från denna säkerhetsdetalj på användarsidan, vilket då gör att it-säkerhetsklimatet minskar. Att tro att användarna alltid kommer att göra rätt bortser från mänskliga beteenden (Norman, 2013).

En annan problematik vad gäller långsam uppstart är att ibland så visas inloggningsfönstret fast användaren redan har auktoriserat sig och ibland reagerar inte it-systemet när användarna försöker starta det. Det leder till fler försök att öppna inloggningsfönstret till PRIO som till slut låser sig som säkerhetsåtgärd. Att användaren gör ett nytt försök om inget svar ges vid första försöket känns förståeligt och konsekvensen blir att användaren blir straffad för att hen tror sig göra rätt. Här handlar det också om att systemet inte ger tillräckligt tydlig information, precis som i temat *Brist på information*.

Designen av tidrapporteringen i PRIO bidrar till en oförståelse av systemet och i slutändan kan felen i stor utsträckning bero på systemets design. Därför lyfter vi att it-systemet inte tycks ha implementerat någon tydlig del av användbarhet eller välbehag inom dess ramar för systemet (Möller et al., 2011; Norman i Cranor & Garfinkel, 2004; Hassenzahl & Tractinsky, 2006). Det vi ser är att systemet är ett strukturerat program men med alldeles för många möjliga valmöjligheter för användarna, utan tillräcklig information, och en implementering av användbarhet har endast visats genom undertemat Mallarna. Detta visar även på att PRIO inte följer ISO:s (2018) definition med hur väl användarna kan använda system i deras tänkta användning av it-systemet.

5.2 Metoddiskussion

För att besvara frågeställningen om huruvida designriktlinjer kan användas för att bedöma användbarheten av säkra it-system valde vi att använda oss av metoden kvalitativa intervjuer (Patel & Davidson, 2011). Metoden för urvalet blev bekvämlighetsurval för att hitta deltagare till intervjuerna. En av uppsatsens författare genomförde samtliga intervjuer på dennes kollegor inom samma arbetsplats, vilket kan leda till att svaren har blivit färgade av detta. Konsekvensen blir att deltagarna kan känna sig medvetet eller omedvetet påverkade av relationen till den som intervjuar. I denna undersökning hade den studenten som inte hade anknytning till deltagarna eller PRIO kunnat genomföra intervjuerna. Detta för att minska färgning under intervjun. Intervjuerna genomfördes på arbetsplatsen och inte en neutral plats, vilket även det kan ha färgat svaren från de intervjuade. Detta hade vi kunnat motverka om vi hade intervjuat deltagarna någon annanstans än på jobbet. Anledningen till att vi valde att intervjua på arbetsplatsen var för att det var den mest tillgängliga platsen och det var lättare att hitta deltagare som ville medverka om de inte behövde ta sig någon annanstans. Detta är också anledningen till att endast en av författarna intervjuade då arbetsplatsen är ett säkerhetsklassat område som kräver behörighet för tillträde.

Något vi försökte eftersträvade men inte blev lyckades med var att sprida ut vilka som deltog i intervjun gällande variation av ålder (27-34) och kön (7 män, 1 kvinna). Detta

skulle ha kunnat motverkas om vi hade haft fler deltagare vilket skulle kunna leda till en större spridning.

Hade vi inte haft ett bekvämlighetsurval hade vi kunnat få ett mer blandat urval av deltagare vad gäller kön och ålder. Men på grund av frågeställningen och vilket it-system vi valde att undersöka, så blev det svårt att få till detta.

Utifrån vår fallstudie har vi i undersökningen valt att slumpmässigt göra urvalet av de soldater som befann sig på arbetsplatsen vid intervjutillfället och som frivilligt ville medverka.

Vi använde oss av det Nielsen (1994) kallar för heuristisk utvärdering och för att undersöka detta så använde vi oss av intervjuer. I och med det baserade vi intervjufrågorna på detta. Andra sätt att mäta användbarheten hade kanske kunnat ge andra svar, men många av dem kräver tillgång till it-systemen, vilket gjorde att vi valde att använda oss av en heuristisk utvärdering. Brister i den utvärdering är att den endast är så bra som du ställer frågorna till deltagarna.

Vi upplever att intervjuer var den mest lämpade metoden för denna frågeställning, det baserar vi på tidigare studier som säger att en fördjupning är önskvärd och borde ses över som till exempel (Nwokedi, Amunga & Rad, 2016). Det var därför vi valde kvalitativa intervjuer med öppna frågor för att deltagarna själva skulle få förklara och berätta utifrån egna tankar och vad de tycker om systemet.

I intervjuerna pratade inte alla deltagare om alla problem, något som skulle kunna vara för att de inte tänkte på det eller att de inte ser det som ett problem. Hade vi varit uppmärksamma på detta i intervjuerna så kanske vi hade fått data om alla de saker som designriktlinjerna tog upp från alla deltagare.

6 Slutsatser & framtida forskning

6.1 Slutsatser

> *Vad är konsekvenserna av hur användbarheten implementerats i det säkra it-systemet PRIO?*

Resultatet kring användbarhet vi har visat upp bekräftar svårigheter mellan it-systemet PRIO och dess användare. I detta arbete har vi inte kunnat utvärdera säkerheten men mycket tyder på att PRIO skulle behöva hitta en balans mellan användbarhet och säkerhet. Det vi har fått fram genom intervjuer visar på att PRIO inte följer varken generella designriktlinjer eller designriktlinjer för säkra it-system, vilka är framtagna för att ge bra användbarhet. Detta leder till ett it-system med hög säkerhet och bristande användbarhet. Den bristande användbarheten i PRIO har lett till dessa konsekvenser:

1. *Brist på information* och *Brist på enkelhet* var de teman som genomsyrar stora delar av intervjuerna, det återfanns många av de andra temana. PRIO leder inte användarna genom användningen vilket gör att användarna fattar felaktiga beslut vilket leder till att de fastnar i de moment de utför och kan då inte komma vidare i användningen. Detta verkar ske på grund av att användarna tycker att PRIO är komplext och krångligt. Dyker det upp fel så vet inte användarna hur dessa ska åtgärdas vilket leder till handhavandefel. Den hjälp som finns är en rudimentär hjälp då det inte går att specificera för de enstaka användarna. Utöver det så meddelar inte PRIO när deltagarna skickar in felaktiga tidrapporter leder detta till att deras löner kan komma ut senare än tänkt eller vara felaktiga. I denna grupp hör även *Motverka fel* in i då hjälpmedlen för att motverka fel är inte tillräckliga för användarna, och kan då skapa handhavandefel. Eftersom PRIO ibland inte loggar in användarna när de försöker göra det så låser sig systemet om användarna försöker för ofta utan att visa felmeddelanden. Konsekvensen av detta är att användarna inte kommer in i PRIO när de behöver använda sig av det, vilket gör systemet otillgängligt och oanvändbart.
2. *Prestandan* och den långsamma uppstarten av PRIO gjorde att användarna lämnade datorn och inloggningskortet för att hämta kaffe under väntetiden. Detta gjordes trots att deltagarna förstår varför de behöver använda sig utav inloggningskorten, en säkerhetsåtgärd, men konsekvensen är då att det blir en säkerhetsrisk. Här är det den mänskliga faktorn som gör att detta sker, och som

inte tagits i beaktande. En annan problematik kring prestandan var driftstörningar som kunde leda till att användarna inte kan använda sig av systemet när de behöver.

3. Temat *Effektivitet* visades i att användarna inte alltid har fått utbildning i PRIO så är de inte säkra på hur de ska använda sig av it-systemet. Det gjorde att temat Brist på information speglades även i detta tema. I och med att ge utbildning i PRIO har ett försök gjorts av att underlätta användningen, men utbildningen ger inte alla de kunskaper som behövs för användandet av PRIO.

6.2 Framtida forskning

I examensarbetet undersöktes det säkra it-systemet PRIO, vi kan inte dra några slutsatser hur resultatet vi har kommit fram till kan appliceras i andra säkra it-system. Resultatet pekar på att problem även skulle kunna finnas i andra säkra it-system, något som skulle kunna undersökas. Vi undersökte dessutom bara tidrapportering inom PRIO och kan inte dra några slutsatser i hur de andra delarna av PRIO eller PRIO som helhet är. Kan en designändring av stora säkerhetsklassade it-system vara ett omfattande arbete och inte vara lönt? Webbaserade system upplevs sträva efter användbarhet för användarna där till exempel hemsidor idag har flera dynamiska och kraftfulla verktyg som gör det enklare att förändra design, kan det vara svårare att ändra designen till förmån för användbarheten i säkerhetsklassade it-system?

Vi använde oss av en liten grupp deltagare vilket gör att resultatet inte går att generalisera, därför föreslås ett större urval av deltagare för att vidare kunna generalisera resultatet, men trots det kunde vi ändå se vissa tendenser. I diskussionen tar vi upp vilken betydelse den mänskliga faktorn har för säkerheten i ett it-system som skulle kunna fördjupas. En konceptdriven designforskning kan vara en möjlig vidareforskning på ämnet. Vi föreslår även mer forskning inom området av användbarhet inom säkra it-system. I framtida forskning skulle man kunna genomföra formulär för kunna nå ett större antal GSS/K soldater, för att få ett större underlag och med det se om konsekvenserna är de samma även i större grupper. Vi kommer även fram till att det skulle behövas mer forskningen gällande konsekvenser kring användbarhet i säkra it-system. I den här undersökningen reflekterar vi över åldern på systemet och varför det byggdes med ett sådant stort fokus på it-säkerhet utan att applicera användbarhet, utan att tänka på vad konsekvenserna av detta skulle leda till. Framtida forskning baserar vi på resultat, lärdomar och egna tankar kring denna undersökning.

Balansen av säkerhet och användbarhet behöver adresseras och noggrannare undersökas i it-system så som PRIO för att minimera negativa konsekvenser. En allt vanligare trend är att företag arbetar agilt inom it-utveckling och vi tror att om Försvarsmakten har möjlighet till en dedikerad it-avdelning som arbetar med

utvecklandet av PRIO skulle de kunna projektera en framtida lösning och vilka åtgärder som är nödvändiga för att förbättra systemet, däribland användbarhet.

7 Källor

Alarifi, A., Alsaleh, M. & Alomar, N. (2017). A model for evaluating the security and usability of e-banking platforms. *Computing*, 99(5), ss.519-535. DOI: 10.1007/s00607-017-0546-9.

Albahar, M. (2017). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, 25(4), ss.993-1006. DOI: 10.1007/s11948-016-9864-0.

Allen, C.G. & Komandur, S. (2019). The Relationship Between Usability and Biometric Authentication in Mobile Phones. *International Conference on Human-Computer Interaction*. Orlando, Florida, USA 26-31 Juli, ss. 183-189. Springer, Cham. DOI: 10.1007/978-3-030-23522-2_23

Arthana, I.K.R., Pradnyana, I.M.A. and Dantes, G.R. (2019). Usability testing on website wadaya based on ISO 9241-11. *Journal of Physics: Conference Series* (Vol. 1165(1), ss.1-8. DOI: 10.1088/1742-6596/1165/1/012012

Azmi, R., Tibben, W. & Win, K.T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, 3(2), ss.258-283. DOI: 10.1080/23738871.2018.1520271

Bevan, N., Carter, J., Earthy, J., Geis, T. and Harker, S. (2016). New ISO standards for usability, usability reports and usability measures. I *International conference on human-computer interaction.* Toronto, Canada 17-22 July, ss.268-278. Springer, Cham. DOI: 10.1007/978-3-319-39510-4_25

Cranor, L. & Garfinkel, S. (2004). Guest editors' introduction: Secure or usable?. *IEEE Security & Privacy*. 2(5), ss.16-18 . DOI: 10.1109/MSP.2004.69

de Bruijn, H. & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), ss.1-7. DOI: 10.1016/j.giq.2017.02.007

Denscombe, M. (2018). *Forskningshandboken: För Småskaliga Forskningsprojekt Inom Samhällsvetenskaperna*. Lund: Studentlitteratur AB. ISBN: 978-91-4412-288-5

Engevall, T. (2013). *PRIO-information februari 2013*. https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/prio-info-pm-4-130219.pdf.

Försvarsmakten. (U.å). *Soldater, sjömän och gruppbefäl*. https://jobb.forsvarsmakten.se/sv/jobba-i-forsvarsmakten/tre-inriktningar/soldat-sjoman/ [2020-10-07]

Goldkuhl, G. & Röstlinger, A. (2019). *Digitala resurser i verksamheter*. VITS, http://www.vits.org/publikationer/dokument/803.pdf.

Goldkuhl, G. (1996). Informatik-Ett ämne i, om och för förändring. Föreläsning vid professorsinstallation 12 oktober 1996. Linköping.

Gordieiev, O., Kharchenko, V.S. & Vereshchak, K. (2017). Usable Security Versus Secure Usability: an Assessment of Attributes Interaction. *ICTERI*, ss.727-740.

Gutmann, P. & Grigg, I. (2005). Security usability. *IEEE security & privacy*. 3(4), ss.56-58. DOI: 10.1109/MSP.2005.104

Hassenzahl, M. & Tractinsky, N. (2006). User experience - a research agenda. *Behaviour & Information Technology*, 25(2), ss.91-97. DOI: 10.1080/01449290500330331

Hof, H.J. & Socher, G. (2016). POSTER: Security Design Patterns With Good Usability. I *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks.* Darmstadt, Germany 18-22 juli 2016, ss. 227-228. DOI: 10.1145/2939918.2942423

Hof, H.J. (2015). User-centric IT security-how to design usable security mechanisms. arXiv: 1506.07167v1

Holmes, M. & Ophoff, J., (2019). Online Security Behaviour: Factors Influencing Intention to Adopt Two-Factor Authentication. I *14th International Conference on Cyber Warfare and Security: ICCWS 2019.* Stellenbosch, South Africa 28 februari-1 mars, s. 123. Academic Conferences and publishing limited.

Hultgren, F. (2020). Ingen ska ha magont på jobbet. *Officerstidningen*. (2), s. 53. https://www.officersforbundet.se/globalassets/pdfer/officerstidningen/2019-2020/officerstidningen-2_2020.pdf

Internationella standardiseringsorganisationen. (2018). *ISO 9241-11:2018 (E) Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts*. Geneva: ISO.

Internationella standardiseringsorganisationen/International Electrotechnical Commission. (2018). *ISO/IEC 27000 (en) Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Geneva: ISO/IEC.

Janlert, L.E. & Stolterman, E. (2017). The meaning of interactivity—some proposals for definitions and measures. *Human–Computer Interaction*, 32(3), ss.103-138. DOI: 10.1080/07370024.2016.1226139

Klaassen, B., van Beijnum, B. & Hermens, H. (2016). Usability in telemedicine systems—A literature survey. *International Journal of Medical Informatics,* 93, ss.57-69. DOI: 10.1016/j.ijmedinf.2016.06.004

Mohamed, M., Chakraborty, J. & Dehlinger, J. (2016). Trading off usability and security in user interface design through mental models. *Behaviour & Information Technology*, 36(5), ss.493–516. DOI: 10.1080/0144929X.2016.1262897

Möller, S., Ben-Asher, N., Engelbrecht, K.-P., Englert, R. & Meyer, J. (2011). Modeling the behavior of users who are confronted with security mechanisms. *Computers & Security*, 30(4), ss.242-256. DOI: 10.1016/j.cose.2011.01.001

Myndigheten för samhällsskydd och beredskap (MSB). (2020). *Årsrapport It-incidentrapportering 2019: Vad har hänt, varför har det hänt, och vad ska göras för att undvika att det händer igen?*. Karlstad: MSB. ISBN: 978-91-7927-027-8

Myndigheten för samhällsskydd och beredskap (MSB). (2019). *Årsrapport It-incidentrapportering 2018: En sammanställning och analys av de statliga myndigheternas it-incidentrapportering*. Karlstad: MSB. ISBN: 978-91-7383-907-5.

Nielsen, J. (1994). Enhancing the explanatory power of usability heuristics. I *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*. Boston, MA, USA 24-28 april, ss.152-158. DOI: 10.1145/191666.191729

Norman, D. (2013). *The Design Of Everyday Things*. New York, New York, United States: Basic Books. Epub-bok. ISBN: 978-0-465-07299-6

Nurse, J.R., Creese, S., Goldsmith, M. & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. I *2011 third international workshop on cyberspace safety and security (CSS)*. Milan, Italien 8 september, ss. 21-26. IEEE. DOI: 10.1109/CSS.2011.6058566

Nwokedi, U., Onyimbo, B. & Rad, B. (2016). Usability and Security in User Interface Design: A Systematic Literature Review. *International Journal of Information Technology and Computer Science*, 8(5), ss.72-80. DOI: 10.5815/ijitcs.2016.05.08

Officersförbundet. (2018). Se över din jourregistrering. [online]. https://www.officersforbundet.se/nyheter/2018/se-over-din-jourregistrering [16 April 2020].

Patel, R. & Davidson, B. (2011). *Forskningsmetodikens Grunder*. Lund: Studentlitteratur. ISBN: 978-9-144-06868-8

Peters, B. (1967). Security considerations in a multi-programmed computer system. I *Proceedings of the April 18-20, 1967, spring joint computer conference*. Atlantic City, NJ, USA 18-20 April, ss. 283-286. DOI: 10.1145/1465482.1465524

Sahar, F. (2013). Tradeoffs between usability and security. *IACSIT International Journal of Engineering and Technology*, 5(4), ss.536-540. DOI: 10.7763/ijet.2014.v5.591

Solana, J., Cáceres, C., García-Molina, A., Opisso, E., Roig, T., Tormos, J.M. & Gómez, E.J. (2014). Improving brain injury cognitive rehabilitation by personalized telerehabilitation services: Guttmann neuropersonal trainer. *IEEE journal of biomedical and health informatics*, 19(1), ss.124-131. DOI: 10.1109/JBHI.2014.2354537

Still, J.D., Cain, A. & Schuster, D. (2017). Human-centered authentication guidelines. *Information & Computer Security*. ss.2-12. DOI: 10.1108/ICS-04-2016-0034

Warner, M. (2012) Cybersecurity: A Pre-history. *Intelligence and National Security*, 27(5), ss.781-799, DOI: 10.1080/02684527.2012.708530

Widrow, B., Hartenstein, R. & Hecht-Nielsen, R. (2005). *Eulogy: 1917 Karl Steinbuch 2005*. IEEE Computational Intelligence Society. http://helios.informatik.uni-kl.de/euology.pdf

Yee, K.P. (2005). Guidelines and strategies for secure interaction design. I Cranor, L.F. and Garfinkel, S. (red.) *Security and usability: designing secure systems that people can use*. Sebastopol, CA: O'Reilly Media, Inc. ss.256-264. ISBN: 978-0596008277

8 Bilaga 1: Tabell 2.1

Jämförelse mellan författarnas olika generella designriktlinjer. (Nwokedi, Amunga & Rad, 2016; Nielsen, 1994; Norman, 2013)

	Nwokedi, Amunga & Rad (2016)		Nielsen (1994)		Norman (2013)
1	bekvämlighet	→	matcha systemet och den riktiga världen	→	Konceptuell model
2	förståeligt	→	tydlighet i systemstatus, konsekvent och standarder, estetisk och minimalistisk design	→	Synlighet, feedback, signifanter, kartläggning
3	inkluderande	→	användarkontroll och frihet, igenkännande snarare än hågkomst, flexibilitet och effektiv användning, hjälp använde känna igen, diagnostisera och återställning av fel	→	Affordanser, begränsningar
4	krav	→	förebyggande av fel	→	x

9 Bilaga 2: Tabell 2.2

Jämförelse mellan författarnas olika designriktlinjer för säkra it-system. (Yee, 2005; Nwokedi, Amunga & Rad, 2016; Nurse, Creese, Goldsmith & Lamberts, 2011; Still, Cain & Schuster, 2017; Hof, 2015; Hof & Socher, 2016; Sahar, 2013)

	Yee (2005)	Nwokedi, Amunga & Rad (2016)	Nurse, Creese, Goldsmith & Lamberts (2011)	Still, Cain & Schuster (2017)	Hof (2015), Hof & Socher (2016)	Sahar (2013)
1	×	×	Estetisk och minimalistisk design, Designa för lättlärdhet, Ackommodera alla typer av användare	Designa för att vara inkluderande,	Låt alla användare förstå systemet, Bemyndiga användare	×
2	Låt användaren få den enklaste vägen att göra tänkt uppgift med minst antal rättigheter, Skilj mellan objekt och handlingar med regler som är relevanta för vad användarna vill göra.	Avslöjande	Säkerhetsanvändbarhet borde läggas till tidigt, Reducera kognitivstress associerad med systemanvändning, Reducera kognitivstress associerad med systemanvändning, Underlätta för skapandet av en tillförlitlig mental modell, Dela upp separata koncept, Ge relevant feedback	Undvik att överbelasta användarnas arbetsminne	Effektivisera användarnas uppmärksamhet och memorisirings förmåga	Effektivitet och säkerhet, Tillfredsställdhet och säkerhet
3	Låt användarna använda säkerhetspolicys på sätt som passar användarna, Indikera tydligt konsekvenserna som användarens handlingar kommer leda till.	×	Erbjud hjälp, tips och dokumentation,	Informera och undervisa användare om risker	Låt användare bara göra informerade beslut, Undervisa användarna i Säkerhet	×
4	×	×	Minimera användningen för tekniska och säkerhetsspecifika termer och uttryck	Undvik fackspråk och underlätta användarnas mental modell	×	×

5	Auktorisera användare om de visar att de vill det, Låt användare ta bort andras auktoritet för att begränsad åtkomst av information	×	Motverka fel, handling, återställning/ångra, Visa vilka uppgifter användarna måste göra och när, ge support vid behov	Låt de rätta funktionerna vara lätta att utföra, Erbjud snabb åtkomst till möjliga funktioner	Gör användningen så lätt som möjligt, Konsekvent	Verkningsgrad och säkerhet, Lättlärdhet och säkerhet
6	×	×	Designa systemet så att säkerheten inte påverkar prestandan	×	×	×
7	Håll koll på andras auktoritet i förhållande till användarens val, Håll koll på användarens auktoritet i förhållande till användarens möjlighet att kolla på resurser, Skydda användaren från andra som manipulera den auktoritet på användaren vägnar, Presentera objekt och handlingar med hjälp av särskilda drag.	Sekretess, Integritet, Brytbarhet, Överflöd	×	×	Säkerhet som standard, Låt systemet främja säkerhet	×

Riktlinjer som inte passar in i tabellen ovan:

Verktyg är inte lösningar

Adminverktyg kan behöva ytterligare jobb med användbarheten

10 Bilaga 3: Frågor

- Berätta vad tycker du om PRIO i allmänhet?
    - Varför tycker du det?
    - Vad är det som gör det
- Berätta precis hur det går till från när du sätter dig vid datorn tills att du kan börja använda dig av PRIO…
- Beskriv några exempel du använder PRIO till?
- Hur gör du när du använder du dig av X?
        - Hur går du tillväga?
        - Ser du några svårigheter?
- Hur skulle det kunna förbättras?
- Berätta om något som PRIO inte riktigt lyckas med..
- Vilket råd skulle du ge till de som ska ta fram “nästa PRIO”?
- Hur skulle du sammanfatta PRIO i ett nötskal?

11 Bilaga 4: Nya Frågor

- Hur är det att använda PRIO, med tanke på din vanliga användning?
- Ge ett exempel på hur du använder PRIO
- Vad i den vanliga användningen är lätt/inte lätt?
- Upplevs PRIO som förståeligt?
- Vet du vad som gör vad av de olika funktionerna?
- Kommer du ihåg hur du ska göra X utan hjälpmedel etc.
- Är PRIO konsekvent i auktorisering/användning
- Har du fått utbildning i varför du behöver göra på ett specifikt sätt vid, till exempel inloggning, tidrapportering?
- Vet du vad du ska göra/inte göra vid X?
- Hur är laddtiderna? / Behöver du vänta vid auktorisering, till exempel inloggning
- Hur är språket i PRIO? Är det lättförståeligt/komplicerat? Beskrivs de olika delarna på ett bra sätt

11 Bilaga 5: Missivbrev

Till deltagande i studien om PRIO

Vi som gör den här uppsatsen heter Egil Swenning och August Järpemo, vi går kandidatprogrammet Digital Design från Högskolan i Kristianstad. Denna uppsats är avslutningen av våran kandidatutbildning och en del av uppsatsen innefattar intervjun.

I och med digitaliseringen har interaktiva enheter och system vuxit fram i större delar av vardagen, det medför att fler enheter och system blir mottagliga för it-attacker.

Syftet med studien är att förbättra utvecklandet av säkra it-system, som PRIO, och förbättra användningen av dem. Med intervjun hoppas vi att kunna samla in material för att förbättra användningen av säkra it-system.

Deltagandet i intervjun är frivilligt och kommer vara helt anonymt. Materialet kommer att behandlas konfidentiellt och vi kommer vara de enda som hantera det insamlade materialet. Väljer du att att avbryta deltagandet kommer inget av materialet att användas.
Intervjun kommer att ta ungefär 20 minuter.

Uppsala 2020-04-18