

# IT-SÄKERHET

– ANVÄNDARBETEENDEN, ORSAKER OCH ÅTGÄRDER

Kandidatuppsats i Informatik

Sanna Andersson  
Ellinor Schiöld

VT 2021KANI31



HÖGSKOLAN  
I BORÅS

**Svensk titel:** IT-säkerhet - Användarbeteenden, orsaker och åtgärder

**Engelsk titel:** IT security - User behavior, causes and actions

**Utgivningsår:** 2021

**Författare:** Sanna Andersson & Ellinor Schiöld

**Handledare:** Stefan Cronholm

## **Abstract**

Organizations today are facing several different threats to their IT security where one of the most common threats is malicious user behaviors that are mainly caused by internal users. It can be difficult for organizations to know what user behaviors can pose a threat and what causes can contribute to these behaviors. In today's society, it is important for organizations to prepare and be aware of the threats a user poses in order to be able to take the right measures if they should arise. The language of this study is written in Swedish and the purpose of this study is to investigate what causes in users' behavior constitute a threat to an organization's IT security and what measures have been taken. A qualitative method in the form of five different interviews has been chosen where an interview guide was the basis for the interview questions. An individual interview was held with a user of the University of Borås and a group interview with the IT department from the University of Borås. The study resulted in 10 user behaviors, 25 causes and 22 measures taken and that there are connections and relationships between them. It can be difficult for organizations to be fully prepared for threats, but according to our study it is possible to identify user behaviors, causes and measures. With education, organizations can make their users more security-conscious and thus reduce the risks of the damage that user behavior can cause.

**Keywords:** IT-security, information security, insider threats, human factors, user behavior, causes, actions

## Sammanfattning

Organisationer står idag inför flera olika hot mot deras IT-säkerhet där ett av de vanligaste hoten är skadliga användarbeteenden som främst orsakas av interna användare. Det kan vara svårt att veta för organisationer vad för användarbeteenden som kan utgöra ett hot samt vilka orsaker som kan bidra till dessa beteenden. Det är i dagens samhälle viktigt för organisationer att förbereda sig samt vara medvetna om de hot en användare utgör för att kunna vidta de rätta åtgärderna om det skulle uppstå. Syftet med denna studie är att undersöka vilka orsaker till användarnas beteenden som utgör ett hot för en organisations IT-säkerhet och vilka åtgärder som har vidtagits. En kvalitativ metod i form av fem olika intervjuer har valts där en intervjuguide låg som grund till intervjufrågorna. En individuell intervju hölls med en användare av Högskolan i Borås samt en gruppintervju med IT-avdelningen från Högskolan i Borås. Studien resulterade i att 10 användarbeteenden, 25 orsaker och 22 vidtagna åtgärder framkom samt att det finns relationer mellan dem. Det kan vara svårt för organisationer att vara helt förberedda på hot men det är enligt vår studie möjligt att identifiera användarbeteenden, orsaker samt åtgärder. Med utbildning kan organisationer göra sina användare mer säkerhetsmedvetna och därmed minska riskerna för de skador användarbeteenden kan utgöra.

**Nyckelord:** IT-säkerhet, informationssäkerhet, insiderhot, mänskliga faktorer, användarbeteende, orsaker, åtgärder

# Innehållsförteckning

<b>1 Inledning</b>	<b>3</b>
1.1 Problemformulering	4
1.2 Syfte och forskningsfråga	4
<b>2 Metod</b>	<b>5</b>
2.1 Forskningsstrategi	5
2.2 Urval	5
2.3 Datainsamling	6
2.4 Dataanalys	6
2.5 Reliabilitet och validitet	7
2.6 Etiska aspekter	8
<b>3 Litteratur</b>	<b>8</b>
3.1 IT-säkerhet	8
3.1.1 CIA-triaden	9
3.1.2 Säkerhetspolicy	11
3.2 Interna användare	12
3.3 Klassificering av säkerhetshot	12
3.4 Varför och när blir insiders farliga	13
3.4.1 Faktorer som leder till attack	14
3.4.2 Tekniska och sociala faktorer som påverkar interna hot	14
3.4.3 Oavsiktligt eller avsiktligt	15
3.4.4 Tillit och lojalitet	16
3.4.5 Utbildning är kritiskt	16
3.4.6 Ökad säkerhetsmedvetenhet	17
3.4.7 Säkerhetskultur	17
3.5 Tidigare forskning	18
<b>4 Resultat och analys</b>	<b>19</b>
4.1 Användarbeteenden	19
4.2 Orsaker	20
4.3 Vidtagna åtgärder	22
4.4 Relationer mellan användarbeteende, orsaker & vidtagna åtgärder	24
4.4.1 Relationer mellan användarbeteenden och orsaker	24
4.4.1.1 Orsaker till användarbeteendet klicka på skadliga länkar	25
4.4.1.2 Orsaker till användarbeteendet laddar ner skadliga filer/bilagor	25
4.4.1.3 Orsaker till användarbeteendet installera okända program	26
4.4.1.4 Orsaker till användarbeteendet dela obehörig information	26
4.4.1.5 Orsaker till användarbeteendet sabotage	27
4.4.1.6 Orsaker till användarbeteendet agera ogynnsamt mot arbetsgivaren	28

4.4.1.7 Orsaker till användarbeteendet nyanställd vågar inte uttala sig gällande eget skadligt beteende	29
4.4.1.8 Orsaker till användarbeteendet missbrukar andras användarkonton	29
4.4.1.9 Orsaker till användarbeteendet avslöja lösenord	30
4.4.1.10 Orsaker till användarbeteendet använda arbetsdator till privat bruk på ett skadligt sätt	30
4.4.2 Vidtagna åtgärder och dess relationer till användarbeteenden och orsaker	31
4.5 Relationer mellan användarbeteenden	33
4.6 Jämförelse mellan litteratur och empiri	34
4.6.1 Klicka på skadliga länkar	35
4.6.2 Ladda ner skadliga filer/bilagor	35
4.6.3 Dela obehörig information	36
4.6.4 Sabotage	37
4.6.5 Avslöja lösenord	38
4.6.6 Installera okända program	39
4.6.7 Agera ogynnsamt mot arbetsgivaren	39
4.6.8 Nyanställd vågar inte uttala sig om ett skadligt beteende	40
4.6.9 Missbrukar andras användarkonto	41
4.6.10 Använda arbetsdator till privat bruk på ett skadligt sätt	41
4.7 Venndiagram utifrån litteratur och empiri	42
4.7.1 Venndiagram Användarbeteende	42
4.7.2 Venndiagram Orsaker	43
4.7.3 Venndiagram Vidtagna åtgärder	43
<b>5 Diskussion</b>	<b>44</b>
5.1 Metodreflektion	44
<b>6 Slutsats</b>	<b>45</b>
<b>7 Framtida forskning</b>	<b>46</b>
<b>8 Källförteckning</b>	<b>47</b>
<b>Bilaga 1: Intervjuguide HB IT</b>	<b>50</b>
<b>Bilaga 2: Intervjuguide HB Användare</b>	<b>53</b>
<b>Bilaga 3: Problemlista</b>	<b>56</b>

# 1 Inledning

Företag upplever idag ett stort värde av information och informationsutbyte vilket gör att informationssystemen inom en organisation har fått en allt större betydelse enligt Leist och Zellner (2006). När organisationer och dess informationssystem växer ökar även sårbarheten och kontrollen minskar menar Mitrović (2004). Enligt Jouini, Rabai & Aissa (2014) är informationssystem ofta utsatta för olika typer av hot som kan leda till skada för organisationen. Skador inom informationssäkerhet kan sträcka sig från mindre förluster till att förstöra hela informationssystem. Effekterna från hoten kan till stor del variera då till exempel några påverkar integriteten eller konfidentialiteten hos datan, medan andra hot påverkar ett systems tillgänglighet. Idag kämpar många organisationer med att försöka förstå vad deras informationstillgångar har för hot samt hur de kan använda de rätta och nödvändiga metoderna för att kunna bekämpa dem, vilket är en konstant utmaning (Jouini, Rabai & Aissa 2014).

Jouini, Rabai & Aissa (2014) menar att hot kan uppstå från olika källor som till exempel anställdas beteenden eller en hackares attacker. Det är därför viktigt för chefer inom organisationer att känna till vilka hot som faktiskt kan påverka tillgångarna men det är också viktigt att identifiera ett hots inverkan så fort som möjligt för att förhindra attacker. Utifrån en studie som gjorts gällande olika typer av hot mot informationssystem visade det sig vara ett anmärkningsvärt stort antal attacker som skedde av mänskliga misstag eller misslyckanden. Whitman (2004) menar då att det är användarnas misstag och missnöje med att följa instruktioner som utgör ett dominerande hot.

Något som kan ses som ett exempel där den mänskliga faktorn utgjorde ett hot eller en risk är den händelse som uppmärksammades av Aftonbladet i mars 2021. Händelsen där den svenska regeringens vaccinsamordnare skickade sekretessbelagd information till sin privata mejladress. Flera IT-säkerhetsexperter påpekade fallet och de ansåg det vara ett sekretessbrott. En IT-säkerhetsexpert samt en professor på Karlstads Universitet och medlem av MSB:s cybersäkerhetsråd reagerade på att vaccinsamordnaren använt sig av Gmail som amerikanska Google är ägare av. De menade på att detta var oroande då det finns lagar som gör att amerikansk säkerhetstjänst enkelt kan få tillgång till informationen. Vaccinsamordnaren utsatte på så sätt både sig själv samt andra för en stor risk. Experterna nämner att de tror att orsaken till vaccinsamordnarens agerande handlar om ren okunskap. En säkerhetschef på internetstiftelsen förtydligar att det faktiskt är väldigt enkelt för information att komma på avvägar och sedan utnyttjas. Det är därför en risk som vaccinsamordnaren bör gjort en bedömning av innan han skickade handlingarna, han skulle ha övervägt nyttan mot den faktiska risken. Säkerhetschefen påpekade även att många organisationer idag har regler mot denna typ av beteende. Aftonbladet var därför även i kontakt med regeringskansliet för att få svar på om det är tillåtet för deras medarbetare att skicka sekretessbelagda handlingar till en privat Gmail. Aftonbladet fick som svar att det kan finnas undantagssituationer där tillgången av tjänstemejl inte finns och då av praktiska skäl behöver en privat e-postadress användas. Vaccinsamordnaren JO-anmälde sedan för sekretess miss och vaccinsamordnaren själv säger att han skickade informationen av praktiska skäl (Aftonbladet 2021).

Med en konstant utveckling av informationsteknik samt ökad tillgänglighet till Internet menar Jouini, Rabai & Aissa (2014) att organisationer idag blir mycket mer utsatta för alla olika typer av hot. En organisations sårbarheter består av svagheter i informationssystemen som utgör en möjlighet för angriparna att utnyttja samt utgöra skada vilket kan leda till en farlig och kostsam påverkan. Enligt Jouini, Rabai & Aissa (2014) beror de större förlusterna på

obehörig åtkomst, virus och stöld av bärbara datorer eller mobila hårdvaror samt att de flesta bedrägerier utförs internt inom en organisation snarare än från externa hot.

## 1.1 Problemformulering

Utifrån inledningskapitlet ovan så formuleras det problem som ska studeras. Information kan ses som en tillgång för en organisation och det behöver i allra högsta grad skyddas från interna hot. Med en god IT-säkerhet och informationssäkerhet kan information och informationssystem skyddas från obehöriga (Jouini, Rabai & Aissa 2014). En användares beteende kan utgöra ett dominerande hot mot organisationer menar Whitman (2004). Det är därför viktigt för organisationer att ta sitt ansvar och vara medvetna om de hot sina användare utgör Jouini, Rabai & Aissa (2014). Men hur ser det ut hos en organisation i verkligheten idag? Hur medvetna är de om sina tillgångar och om de risker interna användare utgör? Utbildas användare för att kunna agera på ett mer säkerhetsmedvetet sätt i sitt arbete och vilka åtgärder vidtar organisationer för att skydda sina tillgångar?

## 1.2 Syfte och forskningsfråga

Uppsatsen har som syfte att undersöka vilka orsaker som kan leda till ett visst användarbeteende som kan utgöra ett hot mot en organisations IT-säkerhet samt vilka åtgärder som vidtas. Perspektivet som kommer att analyseras är utifrån den interna användarens beteenden. Genom frågeställningen nedan kommer uppsatsens syfte besvaras.

*“Vilka orsaker till användarnas beteenden utgör ett hot för en organisations IT-säkerhet och vilka åtgärder har vidtagits?”*

## 2 Metod

Metodavsnittet förklarar det tillvägagångssätt och metod som valts för denna studie. En mer omfattande beskrivning av forskningsstrategi, urval, datainsamling och dataanalys presenteras. I slutet av avsnittet beskrivs reliabilitet och validitet kring studien samt etiska aspekter gällande metodval.

### 2.1 Forskningsstrategi

Jacobsen (2017) nämner att det finns tekniker som kan användas för att ta till sig kunskap om verkligheten. Deduktiv och induktiv är två av de tekniker som nämns. En deduktiv ansats innebär att gå från teori till empiri vilket betyder att sökandet för rapportens empiri ska styras utifrån teoretiska aspekter och antaganden. Då en deduktiv ansats används menar Jacobsen (2017) att det krävs att författarna har en klar och fast teori innan arbetet med datainsamlingen för rapporten påbörjas. Enligt Jacobsen (2017) innebär en induktiv ansats att arbetet sker genom att det går från empiri och verklighet till teori vilket betyder att den teori som finns bör komma samt vara grundad utifrån verkligheten. För att kunna besvara den aktuella frågeställningen har en kvalitativ metod använts med en tillämpning av både induktiv samt deduktiv tillvägagångssätt. Den tidigare insamlade teorin har jämförts med ny empiri via ett deduktivt sätt medans utifrån den kvalitativa metoden utifrån empirin hitta nya teorier via ett induktivt sätt.

En kvalitativ undersökningsmetod valdes i form av intervjuer. Detta eftersom med en kvalitativ metod kan färre enheter undersökas vilket i sin tur gör att närmare kontakt skapas mellan oss som författare och de som skall undersökas. Det ökar även möjligheterna till att få fram en djupare förståelse för situationen och göra processen mer interaktiv enligt Jacobsen (2017).

### 2.2 Urval

Ett urval av informanter från Högskolan i Borås har gjorts utifrån ett urvalskriterium som enligt Jacobsen (2017) benämns som information. En inriktning gjordes på användare som utifrån författarnas egna antaganden besitter större kunskaper kring det område som är intressant för forskningsfrågan. Fem informanter har därför valts med olika roller inom två olika avdelningar men med den gemensamma nämnaren att samtliga är användare av organisationens informationssystem.

Urvalet består av:

- En IT-chef som har kontakt med övriga chefer inom högre utbildning runt om i Sverige. Jobbar även med ett chefsforum vid namn ITCF.
- En informationssäkerhetssamordnare som i en informationssäkerhetsgrupp och IT-säkerhetsgrupp. Arbetar mer med administrativa delar.

- En IT-tekniker som är en systemtekniker som jobbar med IT-säkerhet och identitetshantering.
- En IT-tekniker som jobbar med infrastruktur men även informations och IT-säkerhet.
- En lektor som använder systemet med begränsad behörighet.

Dessa informanter har intervjuats för att belysa olika aspekter av IT-säkerhet.

## 2.3 Datainsamling

En kvalitativ metod för datainsamling har gjorts i form av en individuell intervju samt en gruppintervju. Fem användare från Högskolan i Borås valdes ut för att intervjuas vilket är passande till den kvalitativa metoden som lämpar sig främst när det är ett mindre urval av användare att undersöka. Den öppna individuella intervjun är lämplig då den kan ge tillgång till stora mängder data i form av bandinspelningar eller anteckningar. Metoden är även effektiv för att få fram individens egna tolkning av ett tema menar Jacobsen (2017). En gruppintervju blev aktuell på grund av ett önskemål från organisationens IT-avdelning. Gruppintervju är även mycket tidseffektivt och bidrar med synpunkter från gruppens gemensamma erfarenhet och kompetens kring IT-säkerhet.

Intervjuer kan hållas på flera sätt, ett av de mest traditionella sätten enligt Jacobsen (2017) är fysiska möten ansikte- mot- ansikte. På grund av en rådande pandemi var det inte aktuellt att genomföra ett fysiskt möte, istället genomfördes intervjuerna ansikte- mot- ansikte via den digitala plattformen Zoom.

Den individuella intervjun utfördes med en användare som innehöll både öppna samt slutna frågor, där författarna styrde med förutbestämda frågor men där det även fanns plats för informanten att också styra samtalet med egna åsikter och tankar. Gruppintervjun utfördes med fyra stycken olika informanter från IT-avdelningen, även där med öppna samt slutna frågor. Två olika intervjuguider utformades på grund av intervju deltagarnas olika roller samt uppgifter i systemet. En för-strukturering gjordes först där det bestämdes mer ingående vilka kategorier som skulle belysas i intervjuerna. Detta för att få en struktur i form av användarbeteende, orsak och åtgärd till användarbeteende i intervjuerna. Intervjuguiden hade medelhög struktureringsgrad där antalet underfrågor var begränsade för att informanterna själva skulle ha möjlighet till att styra samt ta upp synpunkter i samtalen. Intervjuerna styrdes utifrån intervjuguiderna för att få en tydlig struktur samt för att ta reda på vilka synpunkter som var mest relevanta (se Bilaga 1).

## 2.4 Dataanalys

För att analysera insamlad data från intervjuer är det bra att reducera komplexiteten, detta för att få en enklare och mer överblickbar struktur enligt Jacobsen (2017). Efter att intervjuerna hade utförts genomfördes först en renskrivning utifrån de anteckningar som togs under tiden. Då intervjuerna fått tillåtelse att bli inspelade gjordes även en transkribering där ljudfilerna skrevs över till en text för att lättare kunna analysera den insamlade informationen.

Synpunkterna från intervjun kategoriserades i tre överordnade kategorier, användarbeteenden, orsaker eller vidtagna åtgärder. För var och en av dessa överordnade kategorier skapades underkategorier. För att analysera intervjuerna markerades användarbeteenden, orsaker samt åtgärder till användarbeteenden i olika färger för att underlätta analysarbetet. Användarbeteenden markerades med färgen blå, orsaker med färgen röd och åtgärder till användarbeteenden med färgen grön. För att underlätta analysarbetet med att identifiera relationer mellan användarbeteenden och dess orsaker genomfördes en problemanalys (Goldkuhl och Röstlinger 2012). Problemanalysen innebar att vi skapade en problemlista (se Bilaga 3) och en problemgraf. Problemlistan utgjordes av alla identifierade användarbeteenden samt orsaker. Syftet med problemgraferna var att visa relationer mellan en orsak som leder till ett användarbeteende (se Figur 2-11). För att visa att användarbeteenden också kan ha relationer till varandra skapades ytterligare en problemgraf (se Figur 12). Detta kallas enligt Jacobsen (2017) axial kodning som är en form av kategorisering då vi identifierat relationer mellan kategorier. En tabell skapades för att tydliggöra och visa förhållanden mellan ett specifikt användarbeteende, specifika orsaker och den specifika åtgärd som vidtagits för att motverka användarbeteendet (se Tabell 4). För att tydliggöra innebörden av vad användarbeteenden, orsakerna samt de vidtagna åtgärderna innebär skapades tre definitionslistor (se Tabell 1-3). För att tydliggöra jämförelsen av empiri och litteratur skapades tre venndiagram (Chen & Boutros 2011). Ett venndiagram för användarbeteende, ett för orsaker samt ett för vidtagna åtgärder (se Figur 14-16).

För att identifiera relationerna mellan användarbeteende och orsaker till vidtagna åtgärder (se avsnitt 4.4.2) gjordes en noggrann analys utifrån empirin från intervjuerna. Vid formuleringen av intervjufrågorna delades frågorna upp i våra tre huvudkategorier, användarbeteende, orsaker samt åtgärder för att lättare kunna identifiera relationer utifrån den insamlade empiri vi fick. Med en god analys kunde vi identifiera relationer mellan användarbeteende och orsaker till vidtagna åtgärder.

## 2.5 Reliabilitet och validitet

Under genomförandet av en kvalitativ metod menar Jacobsen (2017) att en kritisk bedömning av studiens reliabilitet och validitet måste göras. Empirin för en undersökning måste uppfylla två krav. Det första kravet är att empirin ska vara giltig och relevant vilket gör den valid. Det andra kravet är att empirin ska vara tillförlitlig och trovärdig vilket gör den reliabel. Giltighet och relevans innebär att den empiri som samlas in under en studie faktiskt besvarar frågeställningen eller frågeställningarna. För att en undersökning ska gå att lita på måste tillförlitlighet och trovärdighet uppfyllas samt att den är trovärdigt genomförd. Enligt Jacobsen (2017) är målet med undersökningen att utföra den på rätt sätt för att få resultat som är korrekta och relevanta samt går att lita på.

För att säkerställa reliabilitet och validitet för vår studie valde vi ut fyra frivilliga informanter som har stora kunskaper inom IT-säkerhet då de arbetar på Högskolan i Borås IT-avdelning där de hanterar IT-säkerheten och systemets användare. Den femte frivilliga informanten valdes på grund av att personen är en förstahandskälla och oberoende av IT-avdelningen som kunde ge upplevelser som användare av Högskolan i Borås system. Då vi genomfört intervjuerna med informanter som har varierande roller fick vi ett resultat som blev mer varierande. Intervjuerna utgick ifrån en intervjuguide med både öppna och slutna frågor som utformats med hjälp av en sakkunnig person vilket var vår handledare. Informanterna kunde själva spontant vid tillfällen styra samtalet vilket enligt Jacobsen (2017) ger empirin större

giltighet och tillförlitlighet, detta då informanterna gav upplysningar utifrån deras egna uppfattningar. Vi genomförde två olika intervjuer, en individuell intervju och en gruppintervju. För att säkerställa att användaren vågade uttrycka sig till fullo utfördes intervjun individuellt. De fyra informanterna från IT-avdelningen intervjuades i form av en gruppintervju vilket var ett önskemål från deras sida, enligt Jacobsen (2017) kan denna situation ge en osann bild då de kan påverka varandra. Däremot uttryckte informanterna att de har en gemensam syn på IT-säkerhet på grund av att de följer rutiner samt riktlinjer för Högskolan i Borås. Informanterna har kritiskt värderats innan de valdes ut då vi ville ha informanter som besitter de kunskaper som behövdes för att öka reliabiliteten samt validiteten för vår undersökning.

## **2.6 Etiska aspekter**

Vid utförandet av en undersökning menar Jacobsen (2017) att det är viktigt att eftersträva tre grundläggande krav inom etiska aspekter av förhållandet mellan forskare och de som ska undersökas.

Informerat samtycke är ett av de krav som Jacobsen (2017) nämner. Informanterna för denna studie har frivilligt deltagit i vår undersökning och uttryckt ett skriftligt samtycke via mejl. En fråga gällande inspelning av intervjuerna ställdes även där samtliga informanter gav samtycke och tillåtelse. Informanterna har också fått tillräckligt med information kring vad studiens syfte innebär så de skulle ha en viss förståelse inför intervjuerna. Ett annat krav som Jacobsen (2017) menar är viktigt är rätten till privatliv, det vill säga att inget gällande identitet eller kön av informanterna framkommer under intervjuerna. I datamaterialet benämns informanterna som antingen HB IT eller HB Användare så varken identitet, kön eller roller avslöjas och informanterna förblir anonyma under hela undersökningens gång. Korrekt presentation av data är ett annat krav som Jacobsen (2017) anser är viktigt för att återge en rättvis presentation av resultatet för undersökningen. Datan utifrån vår undersökning har vi presenterat på ett fullständigt sätt för att skapa förståelse för vårt resultat. Detta då inget tagits ur sitt sammanhang som inte informanterna uppgett.

## 3 Litteratur

Detta avsnitt är ämnat att ge en fördjupad forskning kring IT-säkerhet och orsaker till de hot som interna användare utgör samt vilka åtgärder som finns för att förhindra dessa hot som kan vidtas av organisationer. Avslutningsvis presenteras en sammanställning av de identifierade användarbeteenden, orsaker samt åtgärder som framkommit utifrån den befintliga forskningen.

### 3.1 IT-säkerhet

Informationssäkerhet är en aspekt av IT-säkerhet och kan definieras som något som skyddar information och informationssystem från obehöriga samt skyddar tillgångar menar Andress (2011). Mitrovic' (2004) beskriver att informationssäkerhet omfattar säkerhet vid hantering av information avseende önskad tillgänglighet, sekretess, spårbarhet och kvalitet. Hot mot informationssäkerheten kan bland annat vara virus, attacker mot nätverket och interna användare. Det kan finnas en stor bredd av tillgångar som behöver skyddas och det är olika från organisation till organisation. Det finns både fysiska och icke-fysiska tillgångar som på ett eller annat sätt behöver skyddas. Att skydda mjukvara samt en organisations information är viktigast i dagens miljö som inkluderar användning av datorer i större bredd, men att skydda sin personal är näst viktigast då det inte går att driva en verksamhet utan personal menar Andress (2011).

Informationssäkerhet och IT-säkerhet är två skilda begrepp och kan förtydligas på så sätt att Informationssäkerhet syftar till att skydda information oavsett form. Det kan vara e-post, brev eller hemsidor. Medan IT-säkerhet är ett samlingsnamn på den tekniken som är stödprocess för att etablera och upprätthålla informationssäkerhet på information i ett elektroniskt format. Datasäkerhet är säkerhet med avseende att skydda system och dess data mot obehörig åtkomst och obehörig eller störning vid databehandling. Mitrovic' (2004) förklarar att det är dessa termer som avser IT-säkerhetsskydd för både internt lagrande, bearbetande och överförande i data men även i omgivningen vid inmatning, förvaring, distribution och utskrift. IT-säkerhet riktar in sig mer på att skydda mot hot som är förenade att använda sig av IT. IT-säkerhet handlar om att organisationer skapar sig en förståelse för vad som är viktigt för organisationen och vad vilka tillgångar både internt och externt är viktiga att skydda. Det handlar även om att förstå vilka risker som finns för tillgångarna, det kan vara sabotage, stöld, mänskliga faktorer eller buggar i program. I det stora hela har IT-säkerhet som syfte att skapa en medvetenhet inom organisationen om dess IT-säkerhet. Att arbeta kontinuerligt med IT-säkerhet och säkerhetsstandarder är ett måste samt att föra rapporter vid avvikelser samt arbeta systematiskt för att öka säkerheten och vidta åtgärder där det krävs (SNSC u.å).

Informationssäkerhetssystem är i ett mycket stort behov av en sund hanterings- och säkerhetspolicy i enlighet med en användares natur. Gonzalez & Sawicka (2002) menar att det är ofta en organisation förlitar sig på enbart de tekniska frågorna. Antingen behandlas mänskliga faktorer i olika säkerhetssystem som uppenbara eller så anses faktorerna vara oöverkomliga med ett hopp om att de tekniska lösningar som finns ska göra det möjligt att automatisera säkerheten. Tidigare forskning har visat att detta tillvägagångssätt är meningslöst. När det gäller interaktionen mellan människor och teknik menar Gonzalez & Sawicka (2002) att det är denna interaktion som är den största säkerhetsrisken för alla. För att göra det möjligt att förbättra robustheten i de moderna informationssäkerhetssystemen är det

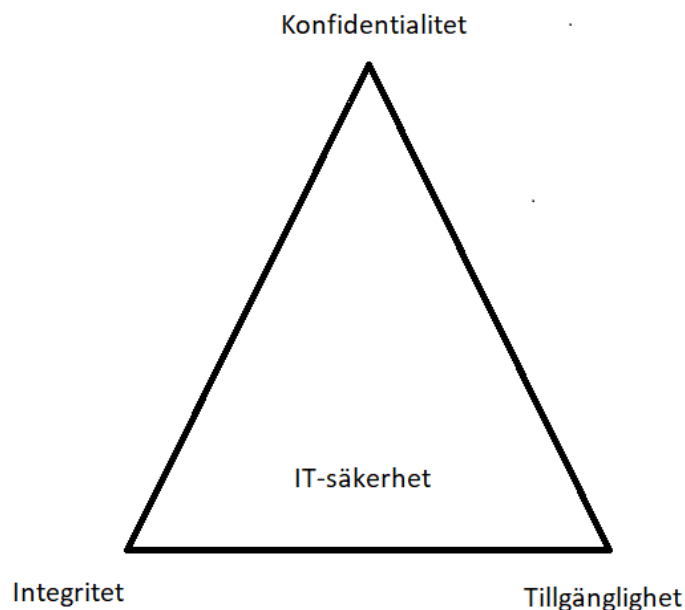
nödvändigt med en mer ökad förståelse för rollen för användare samt mänskliga faktorer, speciellt deras dynamik. Att möjliggöra förståelse för denna dynamik innebär att förstå kausalstrukturen för de uppstående problemen samt att öppna vägar för fler framgångsrika policyer.

### 3.1.1 CIA-triaden

CIA-triaden hänvisar och utgör de grundläggande delarna i informationssystem gällande säkerhetskontroller. Samonas & Coss (2014) menar att det finns tre nyckelterm, konfidentialitet, integritet och tillgänglighet. Dessa har genom tiden format samt informerat en teoretisk förståelse för informationssäkerhet men också den praxis hur säkerhet implementeras och utvecklas i organisationer. Traditionellt sett fokuserade CIA-triaden på tekniska kontroller för att skydda konfidentialitet, integritet samt tillgänglighet av information.

Vid flera tillfällen har CIA-triaden blivit kritiserad på grund av sin tekniska fokus och inriktning. Detta har då lett till en begränsad nytta när större organisatoriska samt sociala aspekter kring säkerhet behöver beaktas. Utöware inom informationssäkerhet ser dock fortfarande ett värde med samt värdesätter CIA-triaden och dess egenskaper som underlättar för dem att förstå samt ta itu med de problem som rör informationssäkerhet. Enligt Samonas och Coss (2014) är det även så att akademisk litteratur inte kasserar CIA-triaden utan försöker snarare förbättra den genom att främst utöka och lägga till nyckelterm, som i huvudsak utvidgar triadens omfattning samt nytta. Detta möjliggör en rikare förståelse för hur organisationer ska hantera säkerhet och förhindra hot..

Konfidentialitet syftar till att ge användare frihet från störningar som kan komma från yttre källor. Farooq, Waseem, Khairi & Mazhar (2015) menar att det är förmågan att ge användaren förtroende för organisationens känsliga information och dess integritet genom att kunna använda sig av olika mekanismer så att information inte avslöjas till obehöriga samt kan endast nås av de användare som är behöriga. Integritet syftar till att skydda användbar information från cyberattacker eller interna störningar, så att information inte kan manipuleras utan att en organisations system fångar upp och förhoppningsvis förhindrar hotet. När kommunikation sker kan data ändras av angripare eller också påverkas av andra faktorer som kan ligga utanför människans kontroll. Enligt Farooq, Waseem, Khairi & Mazhar (2015) syftar tillgänglighet till att garantera en omedelbar tillgång till information för användare som är behöriga, dock inte bara när förhållanden är normala utan också under katastrofala förhållande. På grund av organisationers beroende av tillgänglighet är det väldigt nödvändigt att tillhandahålla brandväggar för att kunna skydda sig och motverka attackerna. Ett exempel på en attack är ”Denial of service” som kan leda till att användare får nekad tillgång. Datatillgänglighet säkerställer också förebyggandet av flaskhalssituationer som syftar till att förhindra informationsflödet.



Figur 1. Figuren är skapad av författarna för att visa hur en CIA-triad kan vara uppbyggd.

### 3.1.2 Säkerhetspolicy

Att ha en IT-säkerhetspolicy är en av de mest viktiga aspekterna i IT-säkerhet. En säkerhetspolicy har som syfte att identifiera regler och rutiner som alla anställda måste följa för att säkerställa konfidentialitet, integritet och tillgänglighet av resurser och data. För att skapa en så god IT-säkerhet som möjligt måste organisationer skapa ett säkerhetsprogram som ger fler lager av skydd och inte bara lägga fokus på ett skydd (Albright 2002).

För att skapa en god IT-säkerhetspolicy är det viktigt att ett samarbete sker mellan de som är säkerhetsansvariga och de som har en god förståelse för organisationens affärsregler menar Albright (2002). En bra policy ska aldrig hindra en organisation från att nå sina uppsatta mål men den kan ge organisationen säkerhet från externa och interna hot.

Enligt Albright (2002) är en god IT-säkerhetspolicy:

- Tydlig, kortfattad och realistisk.
- Identifierar ansvarsområde för användare, administratörer och ledning.
- Ger tillräcklig vägledning för utveckling av specifika processer.
- Identifierar hur incidenter kommer att hanteras.
- Balanserar skydd med produktivitet

Att en policy även ska vara flexibel och anpassningsbar till tekniska förändringar är också väldigt viktig. Den ska alltså ses som ett levande dokument som uppdateras kontinuerligt för att fungera som ett stöd mot organisationens mål. Beroende på storlek, tjänster, teknologi och annat så kan säkerhetspolicy se olika ut för organisationer, men det finns vissa vanligt förekommande aspekter som bör tas med enligt Albright (2002), sex av dessa beskrivs nedan.

Security Definition – En väldefinierad definition av säkerhetsvisionen för organisationen. Den ska vara kort, koncist och tydlig. Det skall även beskrivas varför säkerhetspolicyn är implementerad och vad det innebär, en förklaring hur policyn knyts till organisationens mål och affärsregler.

Enforcement – Ett förtydligande samt identifiering för hur policyn ska tillämpas och hur säkerhetsöverträdelser och uppförande skall hanteras. Det ska även beskrivas om undantag från policyn.

User Access to Computer Resources – Identifiering av roller och ansvar som har tillgång till resurser inom organisationens nätverk.

Password - Lösenord är viktigt och svaga lösenord utgör en risk. Om lösenord hamnar på villovägar kan inkräktare enkelt få tillgång till resurser, vilket leder till tappad konfidentialitet, dataintegritet och tillgänglighet. Det ska tydligt beskrivas vilka krav som ställs på användarna och dess lösenord.

E-mail – En policy måste innehålla ha ett avsnitt som beskriver hanteringen av e-post inom en organisation. Detta då många virus, trojaner och andra hot tar sig in genom att använda e-post.

Awareness Training - Utbildning för att ge organisationens personal en ökad säkerhetsmedvetenhet är ett måste. All personal ska utbildas, detta gäller även säkerhetsansvariga och ledning. Utbildning bör ske vartannat år så personalen hålls uppdaterad.

Höne (2002) poängterar också vikten av att användare inom en organisation ska förstå säkerhetspolicyn och kunna se hur den skall appliceras i deras dagliga uppgifter. Detta är något som Höne (2002) menar allt för ofta blir ett vanligt problem inom organisationer och dess säkerhetspolicys, de är för komplicerade och blir därmed svåra att förstå för en användare. Det är något som i sin tur gör att policyn inte uppnår sitt fulla syfte med att förklara begreppen och behovet av informationssäkerhet till användarna.

### **3.2 Interna användare**

En intern användare även kallad “insider” utgör en anställd hos en organisation som nyttjar informationssystemet. En intern användare har tillgång till stora mängder av information och kunskap om en organisation och det är därför känt att interna användare utgör säkerhetsrisker på grund av denna tillgång. Förtroende, lojalitet och säkerhetsmedvetenhet är viktiga ämnen och de bör göras mer begripliga och urskiljbara för anställda inom en organisation. Det kan göras genom att ett aktivt fokus på beteende finns på arbetsplatsen. Vissa attacker kan endast begås av en insider. Som bland annat att skicka obehörig information eller sabotera en organisations tillgångar. Insiders kan alltså äventyra informationens konfidentialitet, tillgänglighet och integritet. Colwill (2009) påpekar därför att proaktiva åtgärder måste vidtas för att motverka insiderattacker snarare än reaktiva. Att endast tillämpa IT-säkerhet med hjälp av teknik kommer inte ge en godare säkerhet utan det kan leda till katastrofala resultat för att hantera insiderhot. Däremot behöver också den säkerhetsteknik som designas, implementeras och underhålls ha användares beteende i åtanke. Stort fokus på mänskliga faktorer, utbildning och medvetenhet är också extra viktigt (Colwill 2009).

Enligt Woodhouse (2007) rapporterade The Computer Security Institute (CSI) in San Francisco att 60-80% av alla nätverks missbruk som skett i en organisation var utfört av interna användare. Samt 87% av de organisationer som upplevt incidenter kunde identifieras till en intern källa inom organisationen. Enligt Colwill (2009) visar en annan studie att medvetenhet om insiderhot varierar bland företag och sektorer, samt att det hanteras dåligt. Till exempel i Storbritannien gör många organisationer inte tillräckligt för att skydda sina kunder och sig själva. I studien visade det sig att 67% av organisationerna inte gör någonting alls för att förhindra att konfidentiell data hämtas ut via en annan enhet som till exempel ett USB. 57% gör ingen formell säkerhetsriskbedömning och 84% av företagen scannar inte utgående mejl för kontroll av konfidentiella data.

### 3.3 Klassificering av säkerhetshot

Det är vanligt att begränsa användningen av klassificeringar av säkerhetshot till en eller två kriterier för att klassificera hot samt andra hot då alla hot inte omfattas av klassificering. Detta kan för mindre organisationer vara tillräckligt för att bibehålla en stabil miljö där säkerhetshot är relativt stabila, dock i miljöer som ständigt har föränderliga miljöer är det ofta organisationer misslyckas med att skydda sig mot insiderhot. Det är viktigt för organisationer att identifiera alla olika hotegenskaper för att mildra deras risker. Klassificering gör det möjligt att känna till hot som påverkar en organisations tillgångar samt de områden som ett hot kan påverka och skada, dock med hjälp av klassificering kan organisationen skydda sig och sina tillgångar i förväg. Ytterligare en fördel med klassificering är att det hjälper chefer att bygga organisationens informationssystem med mycket mindre sårbarheter. En vanlig lösning är att kombinera flera olika klassificeringar och skapa en hybrid. Enligt Jouini, Rabai & Aissa (2014) är då en hybridmodell passande för klassificering av hot för ett informationssystems säkerhet. Jouini, Rabai & Aissa (2014) nämner hybridmodellen som en multi-dimensionell för hotklassificering med syftet att en organisation ska respektera alla principer för klassificering av hot. Huvudidén bakom hybridmodellen är att det ska vara möjligt att kunna kombinera de flesta kriterier som uppstår för klassificering av hot och att kunna visa de potentiella effekter som kan uppstå på grund av dem menar Jouini, Rabai & Aissa (2014).

Kriterier som finns i en klassificeringslista är:

- Säkerhetshotkälla vilket är hotets ursprung, internt eller externt.
- Säkerhetshotsagenter som är de agenter som orsakat hotet, det finns tre identifierade klasser: mänskliga, tekniska samt miljömässiga.
- Motiv för säkerhetshot och utgör det sannolika målet för angriparen som kan vara skadligt eller inte.
- Avsikt om säkerhetshot vilket är avsikten för den människa som utgör hotet, är det avsiktligt eller oavsiktligt.
- Hoteffekter, hot är en säkerhetsöverträdelse och kräver en hotåtgärd där hoteffekter kan identifieras. En hoteffekt kan till exempel vara stöld av information.

Modellen klassificerar säkerhetshot i fem grundläggande kriterier som sedan utgör flera olika hotklasser. Dessa fem kriterier är agent, källa, avsikt, motivation samt effekter och hoten klassificeras i första hand utifrån deras ursprungliga källa. Jouini, Rabai & Aissa (2014) menar att en användares handlingar kännetecknas av vad dennes mål är under användningen, är det skadligt eller icke-skadligt. Detta kan sedan ytterligare undersökas och delas upp i enlighet med angriparens avsikt, är det avsiktligt eller oavsiktligt. Kriteriet ”avsikt om

säkerhetshot” möjliggör rekonstruktion av en användares attackbeteende för att underlätta vikten av att förstå avsikten. Detta är till mycket hjälp för chefer och utsatta organisationer att minska riskerna för en användares hot samt att hjälpa till att ytterligare påskynda det beslutsfattande som ska leda till att hitta den skyldige.

### 3.4 Varför och när blir insiders farliga

Insiderhot kräver prioritering och bedömning. Om det finns misstankar om hot måste det åtgärdas så fort som möjligt för att minska riskerna, om det ignoreras kan det utvecklas och få katastrofala följder. Även om det är känt att insiders är något som existerar finns det organisationer som ignorerar hotet och Colwill (2009) beskriver tre skäl till varför det möjligtvis ignoreras.

- Organisationer är rädda för dålig publicitet
- Organisationer är inte medvetna om att det händer
- Organisationer lever i förnekelse

En annan bakomliggande orsak kan vara att organisationer faktiskt är medvetna om att hotet redan finns inom organisationen men däremot inte vet hur det ska hanteras. Det är inte acceptabelt att förneka att insiderhot existerar menar Colwill (2009). Att identifiera insiderhot kan vara en utmaning och det kan då vara lämpligt att skapa en riskhanteringsstrategi för insiderhot. Det krävs även att en säkerhetsbedömning görs med hänsyn till mänskliga beteenden i samband med förändrade sociala, affärsmässiga och kulturella faktorer.

#### 3.4.1 Faktorer som leder till attack

Insiderhot är ett komplext problem som involverar psykosociala, psykologiska och organisatoriska frågor. Zeadally, Yu, Jeong och Liang (2012) menar att det kan ses som en omöjlig uppgift att helt eliminera insiderhot eftersom det krävs stora resurser och ett helhets engagemang från alla anställda. Det är en stor utmaning att ens identifiera varningssignaler för ett insiderbeteende som kan utgöra skada eller hot (Colwill 2009). Det finns dock flera olika motivationer som kan uppmana en organisations insider att förvandlas till en angripare. Några av dessa motiv inkluderar missnöje, hämnd, manipulation, nyfikenhet och pengar (Zeadally et al. 2012).

I vissa organisationer läggs det ett stort fokus på att försöka identifiera missnöjda anställda som är ansvariga för insiderattacker. Det finns en risk med att detta bara ger en stereotyp samt en förenkling vilket kan leda till att det fokuseras på fel användare som till exempel användare med äkta klagomål. Colwill (2009) menar att det inte finns någon direkt korrelation mellan insiderhot och missnöjda användare men också att den majoritet av användare som är missnöjda aldrig kommer att förråda sin arbetsgivare. En rättvis och sann analys av motivationen till svek kräver en mer psykologisk analys och det kan finnas stora skillnader från individ till individ. Några personliga egenskaper som tros ha konsekvenser för insiderrisk enligt Colwill (2009) är:

- Personliga och sociala frustrationer, ogillande av auktoritet och en benägenhet för hämnd.
- Känsla av brist på bekräftelse eller status som i sin tur leder till hämndlystenhet.

- Etisk flexibilitet, saknad av moralistiska hämningar som vanligtvis förhindrar skadligt beteende.
- Datorberoende, ensamvargar som är dåliga teamspelare. En önskan att utforska nätverk och bryta säkerhetskoder, hacka och utmana säkerhetsproffs.
- Minskad lojalitet mot arbetsgivare
- Brist på empati

### **3.4.2 Tekniska och sociala faktorer som påverkar interna hot**

Säkerhetsbedömningar måste som nämnt ta hänsyn till mänskligt beteende i samband med tekniska, affärsmässiga, förändrade sociala och kulturella faktorer. Teknik kan enligt Colwill (2009) förändra sociala attityder eftersom det ökar tillgängligheten av data och kommunikation. Förmågan att utnyttja nya tekniska möjligheter har också stor påverkan på sociala strukturer och interaktioner, både hemma men även på arbetsplatsen. Detta har medfört att flera organisationer fått anpassa sig efter den tekniska utvecklingen och tillåter sina anställda att nyttja sina privata enheter även på jobbet. Men det kan utgöra ett hot, Colwill (2009) menar att kan det vara svårt för individer att sätta en verklig gräns för arbete och privatliv. Detta är något som även kan härledas till händelsen med den svenska vaccinsamordnaren som tidigare nämnts i uppsatsen. Vaccinsamordnaren skickade enligt Aftonbladet (2021) sekretessbelagda handlingar till sin privata mail och han insåg nog inte själv vart gränsen gick.

### **3.4.3 Oavsiktligt eller avsiktligt**

En intern användare som utgör ett hot kan äventyra organisationens informations integritet, konfidentialitet samt tillgänglighet. Både avsiktliga och oavsiktliga risker måste därför alltid tas i åtanke. Colwill (2009) menar att ibland kan till och med insider aktiviteter som är helt uppenbarlig oskyldig skapa allvarlig skada som till exempel en olämplig internetåtkomst som i sin tur slösar en organisations resurser samt tid men kan även leda till att organisationens nätverk samt system utsätts för olika typer av virusinfektioner och skadliga koder. Det kan även skada organisationens rykte och deras framtida intäkter men det kan också gå så långt som till potentiella rättegångar som till exempel straffrättsliga handlingar som mobbning eller ordskamning.

Enligt Colwill (2009) är illvilliga användare idag för organisationer en stor utmaning att identifiera samt att vidta de rätta och lämpliga åtgärder för att kunna lösa det aktuella problemet. Det kräver stor ansträngning, tid, investeringar men också framförallt organisationens och chefernas engagemang. Ett av de vanligaste resultat som hittas efter att undersökningar gjorts är varningstecken på förändringar i användares beteenden, attityder och även handlingar, det var flera som hade upptäckt och sett det men ingen hade gjort något åt det. Kollegor eller andra användare hade märkt tecken på annorlunda beteenden samt att något inte stod rätt till men misslyckats med att rapportera det vidare på grund av en otillräcklig förståelse om vad dess betydelse var. Det är också vanligt att andra användare känner att det inte är deras jobb att vidta åtgärder som att rapportera men också att de faktiskt inte vet hur de ska göra. Det är viktigt att organisationer tar hand om denna tendens till andra användares passivitet och ser till att det hanteras, varje potentiell egenskap som är misstänksam bör rapporteras för att minska insiderhot.

För att kunna kontrollera personalens avsikt är övervakning något som skulle kunna införas, dock kan detta leda till en kollision mellan mänskliga faktorer samt säkerhetskontroller. Det finns de användare som kommer att vara olyckliga om de tror att de befinner sig under ständig granskning från högre makter medan det finns de som tycker att det är en tröst och utgör en säkerhet. Dessa förväntningar och uppfattningar varierar väldigt mycket från avdelning till avdelning samt också mellan olika organisationer, dock har arbetsgivaren rätt till att övervaka verksamheten och användarnas arbete. Enligt Colwill (2009) finns det inte någon korrekt mall att följa utan enbart att säkerställa en effektiv balans.

Användare kan ha olika behörighet till systemet beroende på vilka uppgifter de ska utföra. Att hitta en balans mellan de behörigheter en användare faktiskt behöver och tillämpning av lämpliga nivåer är optimalt. Colwill (2009) menar att det finns olika former av avsikt där en användare gör försök att manipulera andra användare eller också planera sabotage. Via manipulation kan en användare använda flera påverkande sociala tekniker för att möjliggöra skapandet av situationer där någon villigt ger information eller tillgång till system eller webbplatser till en användare som inte har behörighet. Användare med avsiktliga intentioner kan också använda sig av metoder som att skicka e-post med bilagor som innehåller skadlig kod eller att låtsas ha tappat bort datorlösenord. Motiv för sådana attacker kan till exempel vara hämnd för en upplevelse som uppsägning, dock planeras attacker som dem vanligtvis i god tid och kan därför ge varningstecken. Enligt Colwill (2009) finns det flera metoder som möjliggör för att kunna försvara sig mot användare med avsiktliga avsikter. Exempel på dessa metoder är för organisationer att skaffa specifik utbildning för att upptäcka manipulativa försök, varna personal till att vara uppmärksamma gällande känslig och begränsad information samt säkerhetskopiera information samt förvara en säker kopia någon annanstans.

### **3.4.4 Tillit och lojalitet**

Enligt Colwill (2009) hävdas det ofta att organisationer med en större andel av anställda som arbetat för organisationen en längre tid har mindre risk för insiderhot men inte på grund av säkerhetspolicier utan via en stärkt tillit till organisationen. Sådana situationer stärks och stöds av tydliga och långsiktiga karriärstrukturer samt belöningsystem. Det kan resultera i en organisationskultur som underlättar utvecklingen av personliga relationer mellan anställda och ledningen. Utbildning har visats att hämma utvecklingen av relationer samt band som vanligtvis är en bidragande faktor till att skapa lojalitet mellan användare och organisation. Ett problem som Colwill (2009) menar är att det för organisationer finns olika perspektiv på lojalitet som till exempel lojaliteten mot kunden, lojaliteten mot organisationen, lojaliteten mot land och kultur eller lojaliteten mot yrket för att få betalt. Detta innebär för organisationer att de behöver försöka främja den lojalitet som utgör en positiv påverkan för dem.

### **3.4.5 Utbildning är kritiskt**

Enligt Colwill (2009) krävs det mer än endast tekniska möjligheter för att skapa en bättre IT-säkerhet. Många insiderproblem kan härledas till okunskap snarare än från en motivation att vilja utgöra skada. Utbildning är därför en kritisk och viktig del i IT-säkerhet för att öka säkerhetsmedvetenhet hos användarna. Woodhouse (2005) hävdar att en framgångsrik utbildning inom säkerhetsmedvetenhet kan hjälpa att ändra människors faktiska beteende och tankesätt mot säkerhet. Det har visat sig att när användare har genomfört ett utbildningsprogram där de fått en djupare förståelse för en organisations skyddande åtgärder

och varför de finns, har riskerna för missbruk minskat och säkerhetsmedvetenhet ökat. Woodhouse (2005) poängterar därför att medvetenhet kan ses som en nyckel för att skydda en organisation. Med rätt utbildning kan människor till och med bli det mest effektiva lagret som utgör försvar i en organisation. Men det är viktigt att utbildningen når ut till alla användare. En utbildning ska inte ske för en utvald och isolerad grupp inom organisationerna utan alla nivåer ska inkluderas menar Woodhouse (2005).

Enligt Metalidou et al. (2014) rapporterades en undersökning som bekräftade rollen för användares engagemang inom organisationen kring deras arbetsprestanda samt arbetsmotivation. Då arbetsgivare erbjuder utbildning till användare är detta en faktor som visade sig öka medarbetarnas och användares tillfredsställelse. Dock bör användares utbildning kring säkerhetsrisker samt åtgärder gällande olika typer av attacker organiseras noggrant. Detta på grund av att order och instruktioner bara kommer att påverka en användares beteende så länge de själva medvetet accepterar det, eftersom när en person uppfattar att specifika mål inte är möjliga att uppnå minskar deras engagemang. Det är på grund av detta som organisationer måste säkerställa att målen gällande informationssäkerhet uppfattas som möjliga att nå för att få det engagemang av användare som behövs. Politiken inom en organisation måste vara tillgänglig för användare för att säkerställa att de inte känner sig ignorerade, det måste vara tydligt för dem vad som är deras exakta ansvar samt roll för att uppnå en optimal säkerhet.

### **3.4.6 Ökad säkerhetsmedvetenhet**

Enligt Metalidou et al. (2014) är en ökad säkerhetsmedvetenhet nyckeln för organisationer att kunna minska antalet intrång som är orsakade av insiderhot. Det är viktigt för organisationer att arbeta med olika sätt för att öka medvetenheten på grund av att det resulterar i en bättre kontroll över de organisatoriska svagheter samt insiderhot som riskerar att hota organisationen. Innan en organisation kan förvänta sig att användare och system skyddar information samt infrastruktur är det viktigt att veta vad som finns, vad som är värdefullt och vad som är i fara. Metalidou et al. (2014) menar att användare kan endast hjälpa till att stoppa och förhindra säkerhetsöverträdelser om de faktiskt är medvetna om de faror som finns, samt lära sig att ta hand om och säkra beteenden som en del av sin normala arbetsutbildning. Användares okänslighet är ett vanligt hinder för att organisationer ska kunna skapa en miljö där både ledning och anställda jobbar mot samma informationssäkerhetsmål. Det är viktigt för varje organisation att möjliggöra en kultur där användare delar ansvar för att skydda och försvara verksamheten mot olika typer av attacker. För att säkerställa genomförandet av en säkerhetspolicy behöver policyn vara förståelig. Då användare inte förstår vad som förväntas av dem blir det svårare för dem att följa. Enligt Metalidou et al. (2014) har en politik som inte tar hänsyn till mål och utbildning för organisationen samt som inte reflekterar över det givna affärsuppdraget, risk att förbises varje gång det genererar intäkter samt stör produktiviteten. Det är viktigt för organisationer att också ta hänsyn till att när användare känner sig positiva och engagerade i sitt arbete blir de mer benägna att känna sig nöjda med arbetet och arbetsgivaren vilket leder till att de är motiverade att prestera till sitt allra bästa.

### **3.4.7 Säkerhetskultur**

Säkerhetsmedvetenhet är bara ett steg i riktningen mot aktivt deltagande av anställda i informationssäkerhetsprocessen. Det krävs även en etablerad säkerhetskultur för att

säkerställa aktivt deltagande hos de anställda menar Woodhouse (2005). Informationssäkerhetskulturen är den del av organisationskulturen som definierar hur en anställd uppfattar säkerheten i en organisation. Organisationskulturen kan ses som ett system av lärda beteenden. Dessa lärda beteenden kan i sin tur återspeglas i vilken nivå av medvetenhet en användare har som då även kan ha en effekt på informationssäkerheten. Riskreducering och säkerhet måste därför vara inkluderat i organisationskulturen för att säkerställa att alla är medvetna om säkerhetsfrågor i sin hantering, planering och operativ verksamhet. Enligt Veiga, Astakhova, Botha och Herselman (2020) spelar utbildning av anställda en stor roll i en informationssäkerhetskultur. Att ha skickliga medarbetare med ett fokus på deras kognitiva aspekter är viktigt. En informationssäkerhetskultur vill värdera samt skydda informationstillgångar och anställda för att erhålla sociala och ekonomiska fördelar för organisationen men också samtidigt minimera säkerhetshot.

För att anställda ska kunna agera medvetet och säkert är det en förutsättning att informationssäkerhet är integrerat i företagskulturen. För att skapa en stark informationssäkerhetskultur har Nel och Drevin (2018) identifierat 25 olika element som är en fördel att applicera. Fem av dessa element presenteras nedan.

Strategy – Ledare och ansvariga måste ha en klar strategi gällande genomförandet av medvetenhets- och utbildningsprogram.

Management's perspective – Det är viktigt att ledare inte ser medvetenhets- och utbildningsprogram som något som endast ödslar tid och pengar.

Delegations of responsibility – Specifika uppgifter är tilldelade till de anställda på ett sätt som gör att de är helt säkra på sin roll.

Risk analysis – Alla potentiella risker ska analyseras och hanteras på ett prioriterat sätt baserat på tillgångarnas värde och säkerhetshot.

Fulfilment of personal needs of employees – Genom att lägga vissa resurser på de anställdas personliga behov kan öka en organisations lojalitet och då reducera riskerna för avsiktlig skada från anställda.

Om en organisation ser till att lägga fokus på alla 25 element kan det leda till en mycket stark informationssäkerhetskultur och därmed uppmuntra till ett mer säkert beteende. Organisationer kan med fördel nyttja elementen i sina medvetenhetsutbildningar eftersom den mänskliga dimensionen av informationssäkerhet inte endast kan lösas av tekniska lösningar (Nel och Drevin 2018).

### **3.5 Tidigare forskning**

Enligt tidigare forskning har följande användarbeteenden, orsaker och åtgärder till användarbeteende konstaterats. Enligt Colwill (2009) är användarbeteende de beteenden som en intern användare utför som i sin tur kan utgöra ett hot mot en organisation. Orsaker till användarbeteenden är de skäl eller anledningar som leder till ett eller flera användarbeteenden. Åtgärder till användarbeteenden är de metoder som en organisation vidtar för att förhindra hoten de utgör menar Woodhouse (2005). Nedan presenteras tre listor som en

sammanställning över de användarbeteenden, orsaker och åtgärder till användarbeteenden som framkommit från den tidigare forskning som gjorts.

Användarbeteende:

- Klicka på skadliga länkar (Colwill 2009)
- Ladda ner skadliga filer (Colwill 2009)
- Dela obehörig information (Colwill 2009)
- Avslöja lösenord (Colwill 2009)
- Sabotage (Colwill 2009)

Orsaker till användarbeteende:

- Brist på kunskap (Colwill 2009)
- Brist på tillit (Colwill 2009)
- Brist på lojalitet (Colwill 2009)
- Missnöje (Zeadally et al. 2012)
- Manipulation (Zeadally et al. 2012)
- Behörighet (Zeadally et al. 2012)
- Brist på bekräftelse Colwill (2009)
- Hämnd och svek (Zeadally et al. 2012)
- Datorberoende och ensamvarg (Colwill 2009)
- Nyfikenhet (Zeadally et al. 2012)
- Brist på empati (Colwill 2009)
- Rekrytering av fientliga externa enheter eller grupper (Colwill 2009)
- Förändrad attityd (Colwill 2009)
- Syn på auktoritet (Colwill 2009)
- Pengar (Zeadally et al. 2012)

Vidtagna åtgärder för att motverka användarbeteende:

- Utbildning (Woodhouse 2005)
- Ökad säkerhetsmedvetenhet (Woodhouse 2005)
- IT-säkerhetspolicy (Albright 2002)
- CIA-triaden (Samonas & Coss 2014)
- Säkerhetsstandarder (SNSC u.å)
- Säkerhetskultur (Woodhouse 2005)
- Kontinuerligt arbete med IT-säkerhet (SNSC u.å)
- Säkerhetsklassificering (Jouini, Rabai & Aissa 2014)
- Begränsad behörighet (Colwill 2009)

## 4 Resultat och analys

I detta avsnitt presenteras resultat och analys av intervjuerna från Högskolan I Borås IT-avdelning (HB IT) samt Högskolan i Borås användare av systemet (HB Användare). HB Användare kommer även benämnas som användaren vid vissa tillfällen för att undvika upprepning. De resultat som framkom från intervjuerna med HB IT och HB Användare presenteras tillsammans som ett gemensamt resultat, dock är vidtagna åtgärder av uppenbara skäl endast identifierade utifrån HB IT:s intervjusvar.

De användarbeteenden, orsaker samt vidtagna åtgärder som identifierats från intervjuerna kommer redovisas med hjälp av tabeller (se Tabell 1-4), problemgrafer (se Figur 2-12), venndiagram (se Figur 14-16) i detta avsnitt. Avsnittet innehåller tabeller (se Tabell 1-3) men en tillhörande definition samt visar relationer mellan användarbeteende och orsaker i problemgrafer (se Figur 2-11) där det finns en graf för varje användarbeteende samt dess relation mot de identifierade orsakerna. Därefter kommer en tabell (se Tabell 4) som presenterar relationer mellan samtliga identifierade användarbeteenden, orsaker samt vidtagna åtgärder. Som en ytterligare aspekt i vår analys har en problemgraf (se Figur 12) över relationer mellan användarbeteenden skapats för att visa att det även finns relationer mellan olika användarbeteenden. Avslutningsvis görs en jämförelse mellan empiri och litteratur med hjälp av venndiagram (se Figur 14-16) samt en utvecklad text där en mer ingående jämförelse görs.

### 4.1 Användarbeteenden

Under intervjuerna kunde flera användarbeteenden identifieras. Det var totalt 10 användarbeteenden som identifierades, de presenteras med en tillhörande definition i tabellen nedan.

Tabell 1.

Användarbeteende:	Definition:
Klicka på skadliga länkar	Användarbeteendet innebär att en användare klickar på en länk som utgör skada
Ladda ner skadliga filer/bilagor	Användarbeteendet innebär att en användare laddar ner filer eller bilagor som utgör skada
Dela obehörig information	Användarbeteendet innebär att en användare tilldelar en annan person obehörig information
Avslöja lösenord	Användarbeteendet innebär att en användare avslöjar sitt lösenord så en annan person får tillgång till det
Sabotage	Användarbeteendet innebär att en användare med syfte och avsikt förstör för en annan användare eller för organisationen

Installera okända program	Användarbeteendet innebär att en användare installerar okända program som utgör skada
Agera ogynnsamt mot arbetsgivaren	Användarbeteendet innebär att en användare på olika sätt agerar negativt mot arbetsgivaren
Nyanställd vågar inte uttala sig gällande eget skadligt beteende	Användarbeteendet innebär att en nyanställd användare inte vågar uttala sig vid misstag som sedan utgör ett skadligt beteende
Missbrukar andras användarkonto	Användarbeteendet innebär att en användare utan tillåtelse och på ett skadligt sätt använder en annan användares konto
Använda arbetsdator till privat bruk på ett skadligt sätt	Användarbeteendet innebär att en användare nyttjar sin arbetsdator privat som leder till skada

## 4.2 Orsaker

Intervjuerna resulterade i att 25 stycken orsaker kunde identifieras, se dem med tillhörande definition i tabellen nedan.

Tabell 2.

<b>Orsaker:</b>	<b>Definition:</b>
Brist på kunskap	En användare besitter inte tillräckliga kunskaper inom IT-säkerhet och vet därför inte vad som utgör skada.
Brist på engagemang	En användare saknar förmågan av att bry sig gällande IT-säkerhet och skadligt användarbeteende.
Stress	En användares sinnessillvaro agerar för snabbt.
Nyfikenhet	En användare som är styrs av förmågan att vilja veta.
Ignorans	En användare som ignorerar konsekvenser.
Arrogans	En användare som agerar nonchalant utan att bry sig om konsekvenser.
Missnöje	En användare som inte känner sig belåten med hur tillvaron är.

Slarv	En användare som saknar känsla av agera på ett försiktigt och säkert sätt.
Längd på anställning	Hur länge en användare varit anställd hos arbetsgivaren.
Manipulation	En användares avsiktliga handlingar för att förstöra för organisationen och dess IT-säkerhet.
Brist på tillit	En användares avsaknad av förtroende gentemot sin arbetsgivare eller kollegor.
Brist på säkerhetsmedvetenhet	En användare som inte besitter tillräckligt med förståelse för att kunna agera mot en god IT-säkerhet.
Bekvämlighet	En användares förmåga att agera på rutin.
Obetänksamhet	En användare som agerar oförståndigt.
Hjälpsamhet	En användares vilja att inte vara en bromskloss för andra kollegor.
Social engineering	En användare som blir manipulerad eller lurad till att utföra oavsiktliga handlingar.
Högre behörighet	En användares tilldelade tillgänglighet inom systemen och på arbetet.
Uppsägning	En användare som blivit antingen tvingad eller själv avsluta sin anställning.
Brist på lojalitet	En användare som inte agerar till fördel för arbetsgivaren.
Brist på bekräftelse	En användare som inte tilldelas positiv feedback för ett bra arbete eller känner sig tillräcklig inom sin arbetsuppgift.
Brist på professionell hjälp	En användare som upplever att ingen ordentlig hjälp kan fås från arbetsgivare eller andra ansvariga för ett ärende.
Tystnadskultur	En användare som upplever ett grupp beteende som resulterar i rädslan av att uttala sig.
Avstängd för skadligt beteende	En användare som betett sig hotfullt mot IT-säkerheten och där arbetsgivaren vidtagit disciplinära åtgärder.

Dåliga ideer	En användare som tror sig utföra smarta handlingar som resulterar i skada mot IT-säkerheten.
--------------	--

### 4.3 Vidtagna åtgärder

Intervjun med HB IT gav svar på vilka åtgärder som de vidtar för att motverka de identifierade användarbeteendena. Det resulterade i 22 stycken åtgärder, se dem med en definition i tabellen nedan.

Tabell 3.

Vidtagna åtgärder:	Definition:
Utbildning	Åtgärd som innebär att HB IT utbildar sina användare till att bli mer säkerhetsmedvetna och få mer kunskap för IT-säkerhet.
Informerar via utskick	Åtgärd som innebär att HB IT informerar sina användare om till exempel IT-säkerhet, hot samt tips via mejlutskick.
Analyserar och klassificerar	Åtgärd som innebär att HB IT alltid gör en analys av de skadliga ärenden som kommer in och gör en prioritering/klassificering av hotbilden.
Säkerställer hur skadlig länken är i skyddad miljö	Åtgärd som innebär att HB IT medvetet klickar på skadliga länkar i en kontrollerad miljö för att se hur länken fungerar och agerar så de kan motverka hotet.
Laddar ner skadliga filer i kontrollerad miljö	Åtgärd som innebär att HB IT medvetet laddar ner skadliga filer i en kontrollerad miljö för att se hur filen fungerar och agerar så de kan motverka hotet.
Blockerar och spärrar länk	Åtgärd som innebär att HB IT blockerar och spärrar de länkar som konstaterats utgöra skada för användarna och systemet.
Återkoppla till avsändare och fråga om trovärdighet	Åtgärd som innebär att HB IT försöker kontakta den avsändare som skickat eller delat med sig av till exempel skadliga länkar eller filer. HB IT rekommenderar även sina användare att alltid återkoppla till avsändare vid minsta misstanke om hot.

Skickar ut varningar	Åtgärd som innebär att HB IT skickar ut varningar till användare när de får information om att det kan finnas hot som cirkulerar.
Blockering och spärrar filer	Åtgärd som innebär att HB IT blockerar och spärrar en skadliga filer som utgör ett hot.
Antivirusprogram	Åtgärd som innebär att HB IT har ett antivirusprogram som skyddar systemet.
Informera om informationsklassning och skyddsvärde	Åtgärd som innebär att HB IT anser att det är bra att informera användarna att förstå värdet av information och vad som behöver skyddas samt varför.
Begränsad behörighet	Åtgärd som innebär att HB IT tilldelar sina användare begränsad behörighet vilket gör att användarna endast ta del av begränsad mängd information och funktioner.
Tvåfaktorsautentisering	Åtgärd som innebär att HB IT använder sig av vad de kallar för Tvåfaktorsautentisering. Det är ett sätt för HB IT att stärka säkerheten genom att användarna använder till exempel en app för extra autentisering utöver användarens lösenord.
Ökad säkerhetsmedvetenhet	Åtgärd som innebär att HB IT försöker göra användarna mer medvetna om IT-säkerhet för att kunna minska risken för skadliga användarbeteenden.
Spärra alla ställen där användaren har behörig	Åtgärd som innebär att HB IT spärrar alla ställen som en användare har tillgång till.
Ha samma inloggning till många system	Åtgärd som innebär att HB IT yrkar på att en användare ska ha samma inloggningsuppgifter till alla ställen för att det ska vara lättare för dem att spärra en användare om det behövs.
Utredning samt spårning	Åtgärd som innebär att HB IT gör en utredning samt spårning när ett skadligt ärende kommer in. För att ta reda på vad som skett.
Kontakta berörd person	Åtgärd som innebär att HB IT kontaktar en användare om det finns misstankar om skadligt beteende

Informerar om risker	Åtgärd som innebär att HB IT på olika sätt informerar användarna om de risker som finns.
Anmälan för olaga dataintrång	Åtgärd som innebär att HB IT kan anmäla en användare som gjort sig skyldig till dataintrång.
Informerar gällande riktlinjer	Åtgärd som innebär att HB IT informerar användare kring de riktlinjer som finns gällande IT-säkerhet.

## 4.4 Relationer mellan användarbeteende, orsaker & vidtagna åtgärder

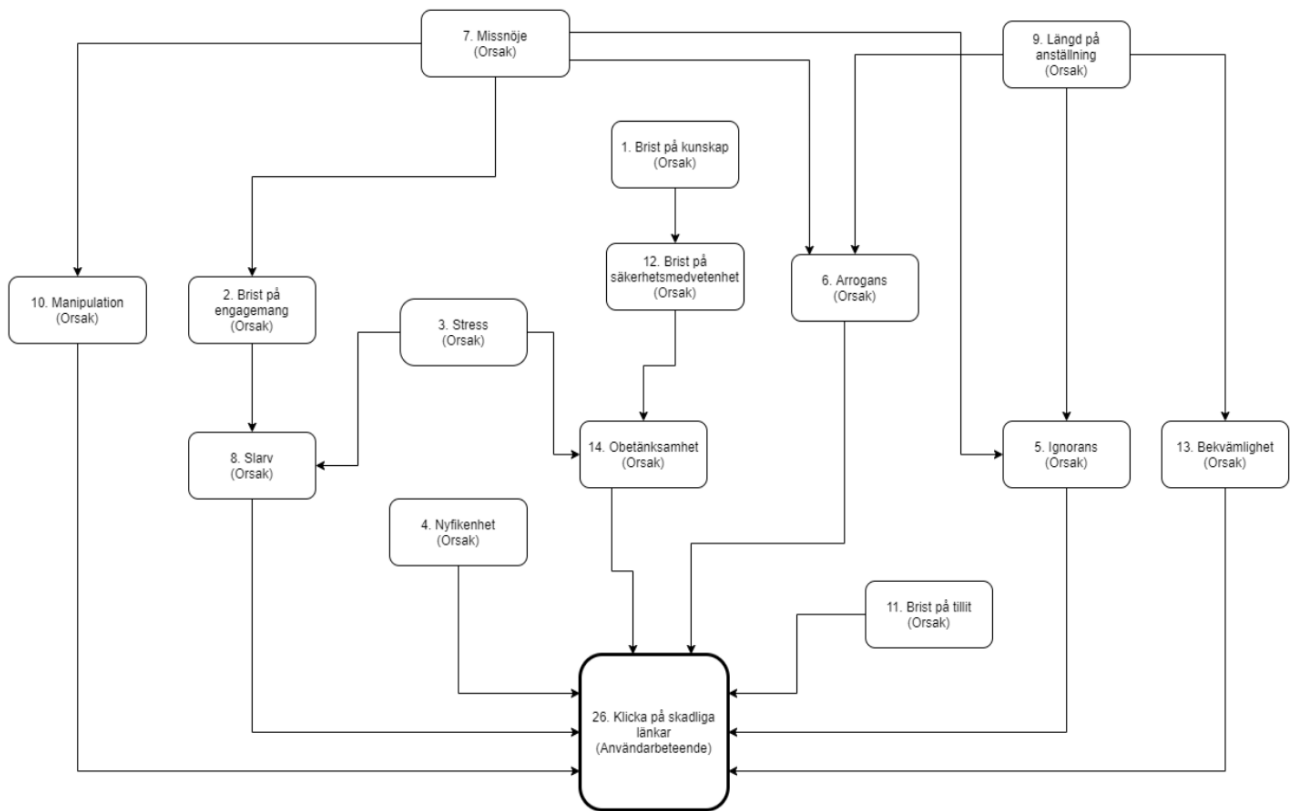
Syftet med detta avsnitt är att visa de relationer mellan användarbeteenden, orsaker samt vidtagna åtgärder som identifierats utifrån de genomförda intervjuerna. Avsnittet presenterar relationer mellan användarbeteenden och orsaker i flera problemgrafer (se Figur 2-11). Relationer mellan användarbeteende, orsaker samt vidtagna åtgärder visas i form av en tabell (se Tabell 4).

### 4.4.1 Relationer mellan användarbeteenden och orsaker

Problemgraferna (se Figur 2-11) är baserade på den empiri som samlats in under de genomförda intervjuerna och visar sambanden mellan användarbeteende och dess orsak. Varje problemgraf utgår från ett specifikt användarbeteende samt de relaterade orsakerna. För att skilja på orsaker och användarbeteenden har vi skrivit i parentes i symbol legenden vad det är för typ, samt för att förtydliga extra mycket har vi gjort en symbol legend för användarbeteende med tjockare linjer. För att se en komplett problemlista (se Bilaga 3). Vi har även identifierat att en och samma orsak kan ligga bakom flera användarbeteenden och att ett användarbeteende kan ha flera orsaker. Vi har även konstaterat att orsaker kan leda till andra orsaker som sedan leder till ett användarbeteende.

#### 4.4.1.1 Orsaker till användarbeteendet klicka på skadliga länkar

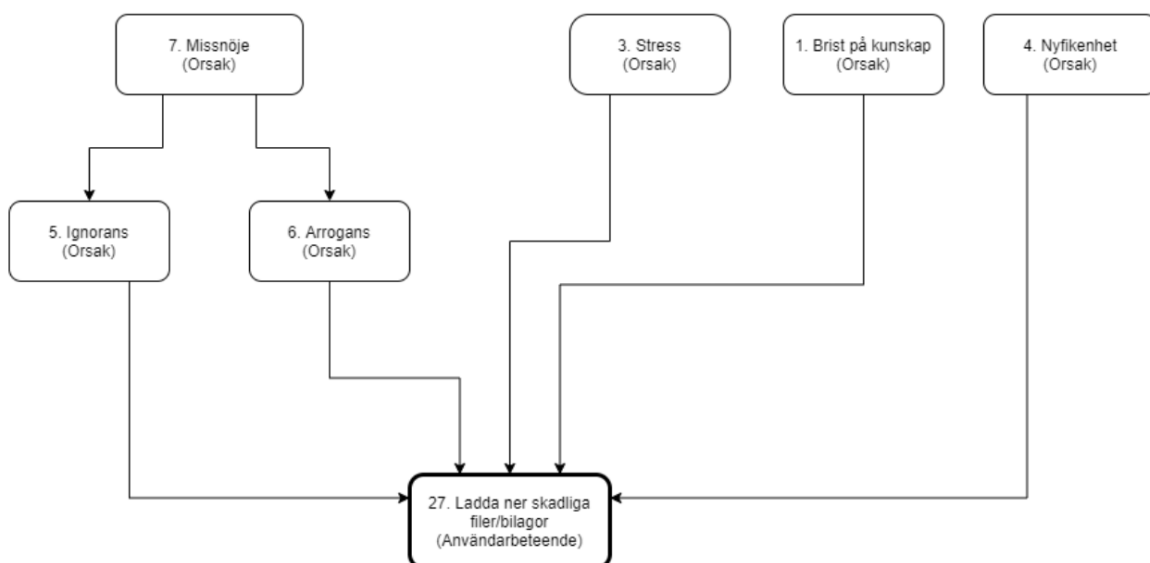
För användarbeteendet klicka på skadliga länkar har vi identifierat ett stort antal orsaker vilket visar på att detta är ett av de främst komplexa användarbeteenden (se Figur 2). Vi kan konstatera att orsaker i många fall kan påverka varandra för att sedan leda till användarbeteendet.



Figur 2.

#### 4.4.1.2 Orsaker till användarbeteendet laddar ner skadliga filer/bilagor

För användarbeteendet laddar ner skadliga filer/bilagor har vi identifierat ett flertal orsaker (se Figur 3). Vi kan även här konstatera att detta användarbeteende är relativt komplext.



Figur 3.

#### 4.4.1.3 Orsaker till användarbeteendet installera okända program

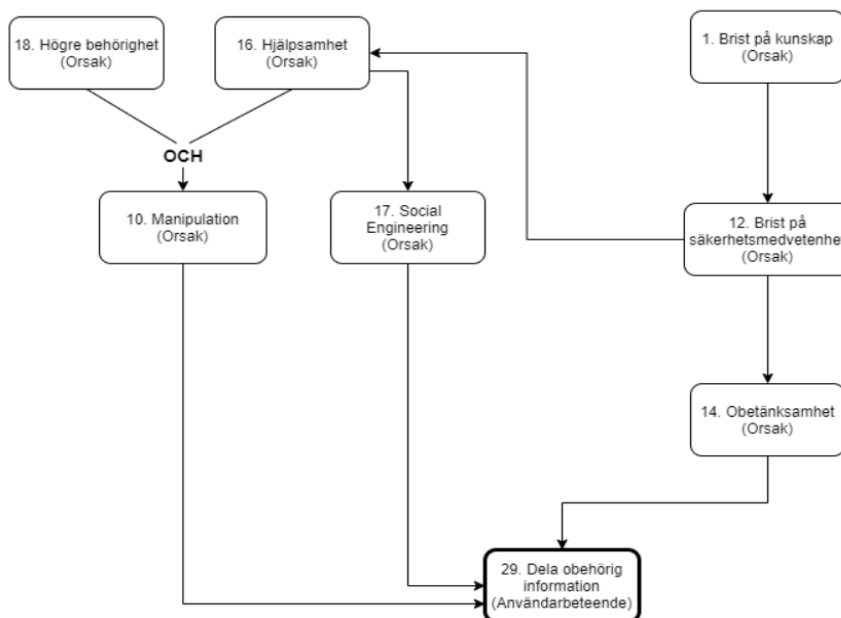
För användarbeteendet installera okända program har vi identifierat få orsaker (se Figur 4). Det kan därför se som ett mindre komplext användarbeteende.



Figur 4.

#### 4.4.1.4 Orsaker till användarbeteendet dela obehörig information

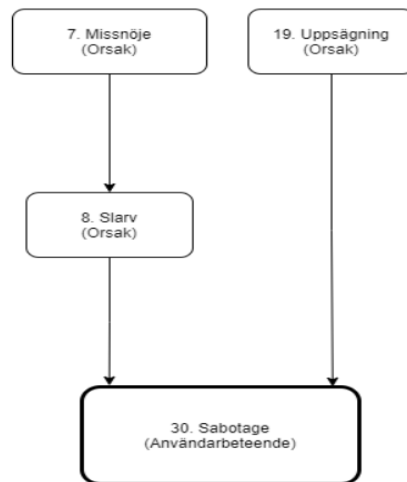
För användarbeteendet dela obehörig information har vi identifierat flera orsaker (se Figur 5). Vi har även konstaterat att två orsaker tillsammans bidrar till en annan orsak som sedan leder till användarbeteendet. Detta användarbeteende kan uppfattas som delvis komplext på grund av mängden orsaker.



Figur 5.

#### 4.4.1.5 Orsaker till användarbeteendet sabotage

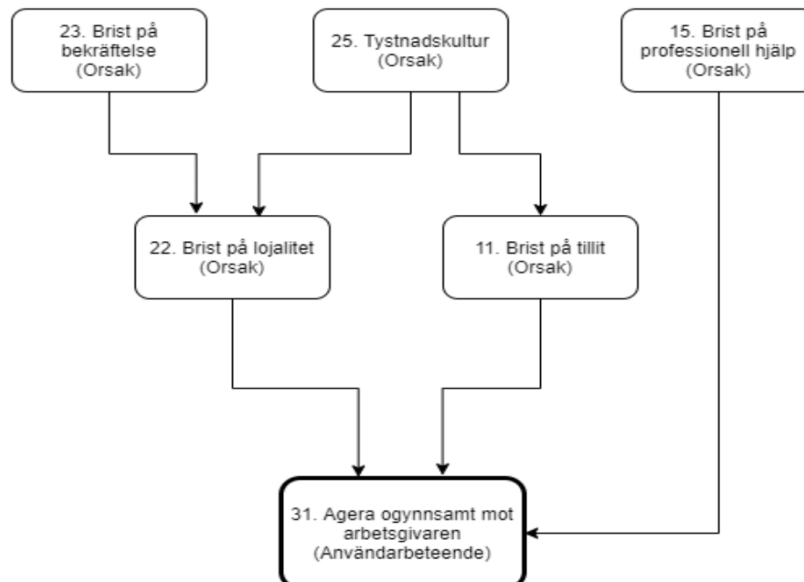
Vi har identifierat tre orsaker till användarbeteendet sabotage (se Figur 6) och är ett mindre komplext beteende. Vi kan konstatera att orsakerna kan påverkas av varandra men kan även leda direkt till det skadliga användarbeteendet.



Figur 6.

#### 4.4.1.6 Orsaker till användarbeteendet agera ogynnsamt mot arbetsgivaren

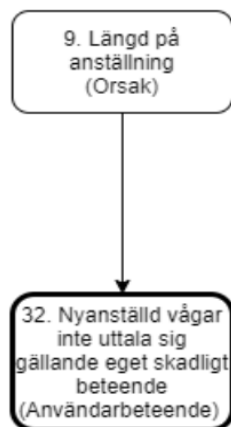
Användarbeteendet agera ogynnsamt mot arbetsgivaren är på gränsen till att bli ett mer komplext beteende då det finns ett flertal olika orsaker identifierade (se Figur 7).



Figur 7.

#### 4.4.1.7 Orsaker till användarbeteendet nyanställd vågar inte uttala sig gällande eget skadligt beteende

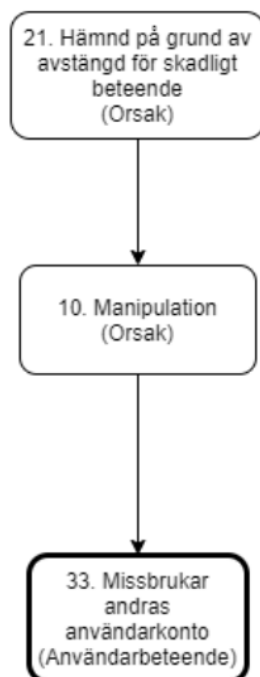
Användarbeteendet nyanställd vågar inte uttala sig gällande eget skadligt beteende har endast en identifierad orsak och är det minst komplexa användarbeteende som identifierats (se Figur 8).



Figur 8.

#### 4.4.1.8 Orsaker till användarbeteendet missbrukar andras användarkonton

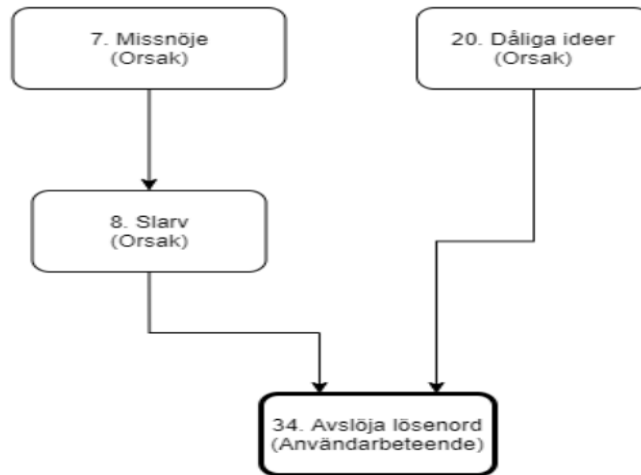
Missbrukar andras användarkonton är även detta ett av de mindre komplexa användarbeteenden som identifierats (se Figur 9). Här leder den ena orsaken till den andra orsaken som bidrar till användarbeteendet.



Figur 9.

#### 4.4.1.9 Orsaker till användarbeteendet avslöja lösenord

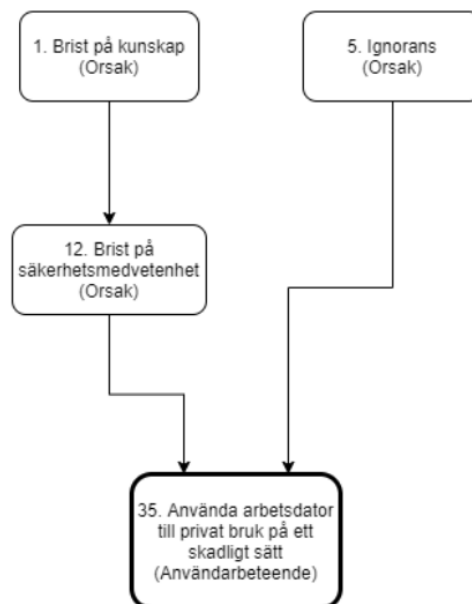
Användarbeteendet avslöja lösenord har färre orsaker identifierade och är inte heller något komplext problem (se Figur 10).



Figur 10.

#### 4.4.1.10 Orsaker till användarbeteendet använda arbetsdator till privat bruk på ett skadligt sätt

Använda arbetsdator till privat bruk på ett skadligt sätt har också få orsaker identifierade (se Figur 11). Det är inte något komplext problem på grund av de få orsaker som leder till användarbeteendet.



Figur 11.

#### 4.4.2 Vidtagna åtgärder och dess relationer till användarbeteenden och orsaker

Syftet med tabellen är att visa identifierade relationer mellan användarbeteenden, orsaker samt vidtagna åtgärder. De presenteras i tre olika kolumner som en sammanställning utifrån intervjuerna med HB IT samt HB Användare. Ett användarbeteende kan bero på en eller flera orsaker och kan ha en eller flera vidtagna åtgärder. En och samma åtgärd kan också ha vidtagits för flera olika användarbeteenden.

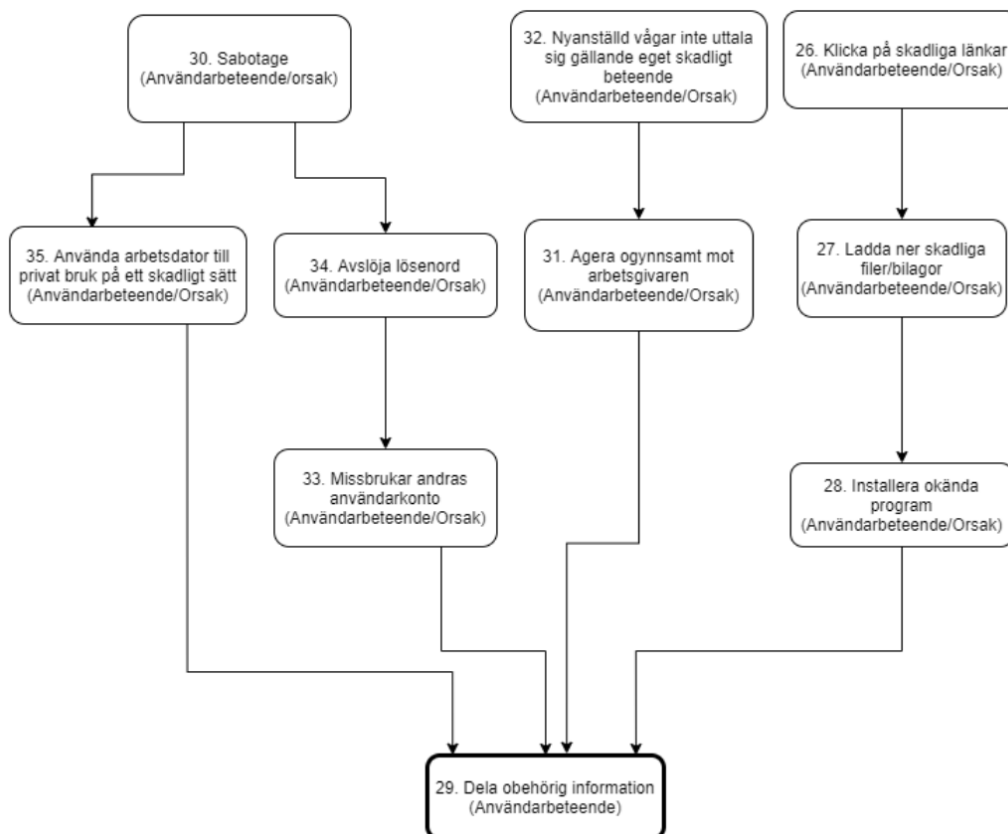
Tabell 4.

Användarbeteende	Orsak till användarbeteende	Vidtagen åtgärd
Klicka på skadliga länkar	<ul style="list-style-type: none"> <li>- Brist på kunskap</li> <li>- Brist på engagemang</li> <li>- Stress</li> <li>- Nyfikenhet</li> <li>- Ignorans</li> <li>- Arrogans</li> <li>- Missnöje</li> <li>- Slarv</li> <li>- Längd på anställning</li> <li>- Manipulation</li> <li>- Brist på tillit</li> <li>- Brist på säkerhetsmedvetenhet</li> <li>- Bekvämlighet</li> <li>- Obetänksamhet</li> </ul>	<ul style="list-style-type: none"> <li>- Utbildning</li> <li>- Informerar via utskick</li> <li>- Analyserar och klassificerar</li> <li>- Säkerställer hur skadlig länken är i skyddad miljö</li> <li>- Blockerar och spärrar länk</li> <li>- Återkoppla till avsändare och fråga om trovärdighet</li> <li>- Skickar ut varningar</li> </ul>
Ladda ner skadliga filer/bilagor	<ul style="list-style-type: none"> <li>- Brist på kunskap</li> <li>- Stress</li> <li>- Nyfikenhet</li> <li>- Ignorans</li> <li>- Arrogans</li> <li>- Missnöje</li> </ul>	<ul style="list-style-type: none"> <li>- Utbildning</li> <li>- Informerar via utskick</li> <li>- Analyserar och klassificerar</li> <li>- Laddar ner skadliga filer i kontrollerad miljö</li> <li>- Säkerställer hur skadlig filen är i skyddad miljö</li> <li>- Återkoppla till avsändare och fråga om trovärdighet</li> <li>- Skickar ut varningar</li> <li>- Blockering och spärr</li> </ul>
Installera okända program	<ul style="list-style-type: none"> <li>- Brist på kunskap</li> <li>- Nyfikenhet</li> </ul>	<ul style="list-style-type: none"> <li>- Informerat via utskick</li> <li>- Antivirusprogram</li> <li>- Begränsad behörighet</li> </ul>
Dela obehörig information	<ul style="list-style-type: none"> <li>- Brist på kunskap</li> <li>- Obetänksamhet</li> </ul>	<ul style="list-style-type: none"> <li>- Informera om informationsklassning</li> </ul>

	<ul style="list-style-type: none"> <li>- Hjälpsamhet</li> <li>- Social engineering</li> <li>- Högre behörighet</li> <li>- Manipulation</li> <li>- Brist på säkerhetsmedvetenhet</li> </ul>	<ul style="list-style-type: none"> <li>och skyddsvärde</li> <li>- Begränsad behörighet</li> <li>- Tvåfaktorsautentisering</li> <li>- Ökad säkerhetsmedvetenhet</li> </ul>
Sabotage	<ul style="list-style-type: none"> <li>- Missnöje</li> <li>- Slarv</li> <li>- Uppsägning</li> </ul>	<ul style="list-style-type: none"> <li>- Spärra alla ställen där användaren har behörig</li> <li>- Ha samma inloggning till många system</li> <li>- Tvåfaktorsautentisering</li> </ul>
Agera ogynnsamt mot arbetsgivaren	<ul style="list-style-type: none"> <li>- Brist på lojalitet</li> <li>- Brist på tillit</li> <li>- Brist på bekräftelse</li> <li>- Brist på professionell hjälp</li> <li>- Tystnadskultur</li> </ul>	<ul style="list-style-type: none"> <li>- Utbildning</li> </ul>
Nyanställd vågar inte uttala sig gällande eget skadligt beteende	<ul style="list-style-type: none"> <li>- Längd på anställning</li> </ul>	<ul style="list-style-type: none"> <li>- Skickar ut information</li> <li>- Utbildning</li> </ul>
Missbrukar andras användarkonto	<ul style="list-style-type: none"> <li>- Hämnd på grund av avstängd för skadligt beteende</li> <li>- Manipulation</li> </ul>	<ul style="list-style-type: none"> <li>- Utredning samt spårning</li> <li>- Kontakta berörd person</li> </ul>
Avslöja lösenord	<ul style="list-style-type: none"> <li>- Dåliga ideer</li> <li>- Slarv</li> <li>- Missnöje</li> </ul>	<ul style="list-style-type: none"> <li>- Anmälan för olaga dataintrång</li> <li>- Informerar om risker</li> <li>- Spärra alla ställen där användaren har behörig</li> <li>- Ha samma inloggning till många system</li> <li>- Tvåfaktorsautentisering</li> </ul>
Använda arbetsdator till privat bruk på ett skadligt sätt	<ul style="list-style-type: none"> <li>- Brist på kunskap</li> <li>- Ignorans</li> <li>- Brist på Säkerhetsmedvetenhet</li> </ul>	<ul style="list-style-type: none"> <li>- Informerar gällande riktlinjer</li> </ul>

## 4.5 Relationer mellan användarbeteenden

Vi som författare upptäckte att det kan finnas relationer mellan användarbeteenden, vilket innebär att ett användarbeteende kan leda till ett annat användarbeteende. För att visa dessa relationer skapade vi en problemgraf (se Figur 12). I problemgrafen finns enligt vår tolkning ett huvudproblem vilket är dela obehörig information som kan orsakas av flera andra användarbeteenden. De övriga användarbeteendena kan ses som en orsak, det vill säga att de kan både vara ett användarbeteende och en orsak.



Figur 12.

## 4.6 Jämförelse mellan litteratur och empiri

Syftet med detta avsnitt är att jämföra litteratur med empiri. Först kommer ett kapitel där vi har valt att dela upp användarbeteendena i rubriker, där vi under varje rubrik skriver om en jämförelse av användarbeteenden och dess relationer till orsaker samt vidtagna åtgärder (se Tabell 4) som byggs på från tidigare litteratur samt intervjuresultat. Rubrikerna delades in utefter användarbeteendena på grund av att vi som författare anser att det är själva användarbeteendet som utgör den faktiska handlingen som resulterar i ett hot och skada.

Intervjusvaren är indelade i två delar där en del representerar HB IT (se Bilaga 1) och den andra HB Användare (se Bilaga 2). Då intervjun med HB IT skedde i form av en gruppintervju kommer svaren presenteras som ett svar från gruppen. Det var en av intervjudeltagarna från HB IT som valde att föra talan för gruppen medans de andra

bekräftade och fyllde i. Detta med samtycke av samtliga deltagare i gruppen då de ansåg sig vara väldigt eniga i sina svar eftersom de arbetar som ett team dagligen och utgår från samma riktlinjer gällande Högskolan i Borås IT-säkerhet.

#### **4.6.1 Klicka på skadliga länkar**

Både Colwill (2009) samt HB IT menar att en användares förmåga att klicka på skadliga länkar utgör ett stort hot mot IT-säkerheten. Utifrån intervjun med HB IT (se Bilaga 1) menar de att det finns flera olika orsaker samt åtgärder till detta användarbeteende (se Tabell 4). Brist på kunskap samt brist på säkerhetsmedvetenhet är två av orsakerna till detta användarbeteende och HB IT nämnde att de är vanliga orsaker som återfinns i flera olika användarbeteende. För att förhindra detta användarbeteende framkom det att en viktig åtgärd är utbildning av användare. Tillsammans med utbildning menar HB IT att det också är viktigt att informera användare via utskick samt skicka ut varningar när det förekommer hotfulla attacker som till exempel nätfiske. Även Woodhouse (2005) menar att utbildning är en viktig del i att motverka hot samt skapa en god IT-säkerhet. Utbildning är en viktig del men det är den metod som är minst populär på grund av att det är svårt att motivera användarna att genomföra utbildning. Under intervjun med HB IT framkom det även orsaker som nyfikenhet, ignorans och arrogans. De berättade att de upplevt situationer där användare medvetet klickat på länkar som de vet kan utgöra en skada. Detta av ren nyfikenhet, arrogans och att användare helt ignorerar konsekvenserna. Enligt Zeadally et al. (2012) är missnöje en orsak som kan leda till denna typ av användarbeteende, att klicka på skadliga länkar vilket också HB IT bekräftar, de nämner att om en användare är missnöjd ökar benägenheten till att klicka på en skadlig länk.

Under intervjun med HB Användare (se Bilaga 2) berättades det om en incident där användaren själv på grund av stress och slarv råkade ut för en skadlig länk. Användaren fick ett mail från en student med en länk och klickade obetänksamt, men var dock snabb med att kontakta IT-avdelningen som åtgärdade incidenten genom att först säkerställa hur skadlig länken var i en skyddad miljö samt sedan blockera och spärra den. Utifrån incidenten framkom det att numera vidtar användaren själv åtgärder gällande liknande situationer, vilket antingen kan vara att ta bort mejl som känns osäkra eller istället återkoppla till avsändaren och fråga om trovärdigheten. Utefter den forskning som gjorts har vi fått en uppfattning om att denna situationen även kan bero på längden av en användarens anställning. HB Användare har arbetat inom Högskolan i Borås under en längre tid vilket har lett till att användaren blivit mer bekväm och rent rutinmässigt klickade på länken. Under intervjun ställdes det en fråga till HB Användare kring definitionen av vad trojanvirus samt nätfiske är. Svaret blev att användaren inte visste vad nätfiske var men att trojanvirus var mer bekant. I vår mening kan detta bero på okunskap vilket kan leda till onödiga incidenter. Under intervjun med HB Användare framkom det även att användaren inte genomgått den utbildning som IT-avdelningen nyligen skickat ut. Vi tror även att detta kan vara en orsak till användarens agerande då även om användaren själv menar att det finns en säkerhetsmedvetenhet där, är det alltid bra med att kontinuerligt utföra säkerhetsutbildningar. Detta stärks även av Albright (2002) som också menar att ett kontinuerligt arbete med utbildning bör ske vartannat år för att hålla användare uppdaterade vilket minskar risken för att en användares beteende utgör ett hot.

#### 4.6.2 Ladda ner skadliga filer/bilagor

Gällande användarbeteendet ladda ner skadliga filer är orsakerna liknande (se Tabell 4) de som vi tagit upp hittills gentemot användarbeteendet klicka på skadliga länkar. HB IT nämner under intervjun (se Bilaga 1) att det finns ett helt spektrum av orsaker till användarbeteendet som till exempel brist på kunskap samt stress, arrogans och ignorans. De har även vid ett tillfälle skickat ut ett aprilskämt till sina användare för att indirekt utföra ett litet test för att se hur användarna agerar. Resultatet av detta aprilskämt visade att användarna till stor del klickar på det mesta då flera användare gick på skämtet. HB IT vidtar samma åtgärder för detta användarbeteende som när en användare klickar på skadliga länkar. Vid misstanke om nedladdad skadlig fil analyserar och klassificerar de hotet. HB IT laddar ner den skadliga filen i en kontrollerad miljö för att sedan säkerställa hur skadlig den är. De försöker utbilda sina användare och informerar via utskick för att minska riskerna för detta användarbeteende. Som vi nämnt är utbildning av användare viktigt och även Woodhouse (2005) menar att det definitivt är den åtgärd som organisationer bör vidta för att minimera denna typ av användarbeteende.

#### 4.6.3 Dela obehörig information

Att dela obehörig information är ett användarbeteende som enligt Colwill (2009) är en vanlig attack som kan utföras av en intern användare. I tabellen (se Tabell 4) finns det flera olika orsaker till detta användarbeteende. HB IT nämner under intervjun (se Bilaga 1) att det kan beror på obetänksamhet, hjälpsamhet, brist på säkerhetsmedvetenhet samt en form av manipulation vid namn social engineering. HB IT uttrycker sig:

*“Användaren förstår kanske inte värdet av informationen, vi brukar prata en del om informationsklassning och att användarna behöver också förstå skyddsvärdet av informationen de hanterar.”*

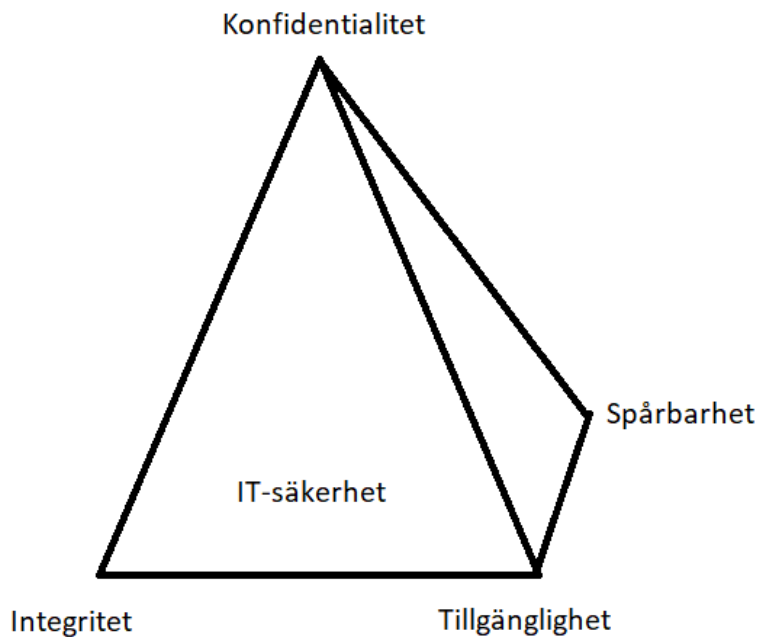
Gällande hjälpsamhet förklarar HB IT att människor gärna vill hjälpa andra, som exemplifieras nedan:

*“Folk vill hjälpa till man vill inte vara den som sätter käppar i hjulen, man vill vara hjälpsam”*

För att eliminera det hot detta användarbeteende utgör har HB IT applicerat åtgärder som att tilldela begränsad behörighet till användare. Colwill (2009) menar att det är viktigt med en balans gällande en användares behörighet baserat på vilka uppgifter de faktiskt utför. Under intervjun med HB Användare (se Bilaga 2) framkom det att användaren upplever sig ha för hög behörighet och kan till och med tänka sig att ha lägre. Detta då HB användare inte nyttjar all behörighet som användaren blivit tilldelad. Tvåfaktorsautentisering är även detta en åtgärd som HB IT vidtar mot att dela obehörig information för att minska risken att någon kan ta sig in i systemen.

Enligt Colwill (2009) kan användarbeteendet dela obehörig information göra att en organisations konfidentialitet, tillgänglighet och integritet utsätts för risk. Samonas och Coss (2014) menar att den så kallade CIA-triaden är uppbyggd på tre nyckeltermerna, konfidentialitet, integritet och tillgänglighet. CIA-triaden är en grundläggande del i arbetet mot en ökad

IT-säkerhet. Under intervjun ställdes frågan till HB IT (se Bilaga 1) om de applicerar CIA-triaden, svaret var ja då de menar att hela informationssäkerhetsområdet bygger på den. HB IT har däremot lagt till en egen fjärde parameter som de kallar spårbarhet. Nedan presenteras vår tolkning av HB IT:s CIA-triad där den fjärde parametern spårbarhet är tillagd.



Figur 13. En figur som visar författarnas egna tolkning av HB IT:s tillämpning av CIA-triaden.

#### 4.6.4 Sabotage

Enligt Colwill (2009) kan användare med avsikt planera sabotage till syfte att i vissa fall förstöra hela informationssystem. Intervjun med HB IT (se Bilaga 1) resulterade i att orsaker som missnöje och uppsägning framkom (se Tabell 4). De menar att ett missnöje hos användare kan leda till slarv vilket i sin tur kan bidra till avsiktligt sabotage. Ett annat avsiktligt sabotage kan uppstå grund av en uppsägning med kort varsel eller om en anställd tvingas bort från sin tjänst. De åtgärder som HB IT vidtar vid sådana situationer är att användarna redan till en början har samma inloggningsuppgifter i samtliga system. Detta tillvägagångssätt gör det lättare för HB IT att omedelbart spärra alla system som en användare har behörighet till. Enligt Colwill (2009) kan sabotage även bero på en orsak som hämnd som framkommit på grund av en uppsägning. Sådana attacker planeras vanligtvis i god tid och kan utgå varningstecken vilket gör det enklare att kunna försvara sig mot användare med avsiktliga användarbeteenden som sabotage. Utifrån undersökningar som gjorts kan varningstecken vara förändringar i attityd och handlingar hos användare. För att upptäcka varningstecken i tid krävs det att alla användare är uppmärksamma på annorlunda beteenden samt rapporterar misstankar till sin chef vilket då också kräver deras engagemang. Utifrån intervjun med HB Användare (se Bilaga 2) framfördes det av användaren att det som rapporteras inte alltid tas till vara på av ledningen. Detta är något både vi och HB Användare menar kan öka riskerna till att en användare avstår från att rapportera in. Som förslag på åtgärd menar HB Användare att någon form av feedback hade varit uppskattat när en rapportering skett. Två åtgärder för sabotage som Colwill (2009) nämner kan vara att

uppmärksamma personal gällande skyddsvärdet i begränsad och känslig information samt ha rutin för säkerhetskopiering av information. Ytterligare en åtgärd för att förhindra användarbeteendet sabotage är att införa övervakning samt säkerhetskontroller mot användare, detta för att möjliggöra kontroll av avvikande och avsiktliga beteenden. Under intervjun med HB IT (se Bilaga 1) framkom det att de inte genomför någon typ av kontroll eller övervakning alls. De menar att Högskolan i Borås inte är en skyddad arbetsplats jämfört med till exempel polisutbildningen där utdrag från register görs på alla användare. Dock berättade de att det är något de önskar var tillgängligt för alla nyanställda användare för att kunna göra det lättare att förutse avsiktliga användarbeteenden.

#### 4.6.5 Avslöja lösenord

För användarbeteendet avslöja lösenord finns det flera orsaker (se Tabell 4) som kan leda till att en användare avslöjar sitt lösenord. HB IT menar att användarbeteendet kan orsakas av slarv, dåliga ideer, manipulation samt missnöje. Metalidou et al. (2014) menar för att minska risken av intrång som både är avsiktliga eller oavsiktliga är en ökad säkerhetsmedvetenhet nyckeln för att organisationer ska kunna reducera dessa hot. Både HB IT och Colwill (2009) menar att detta användarbeteende även kan bero på ett missnöje hos användare. Colwill fortsätter att poängtera att en användares avsiktliga handling att avslöja lösenord kan orsakas av manipulation. Baserat på tidigare forskning anser vi att lathet också kan vara en orsak i att detta användarbeteende inträffar. Genom att inte bry sig tillräckligt samt att en användare inte förstår skyddsvärdet av vad ett lösenord innebär blir det ett riskfyllt användarbeteendet. HB IT berättade i intervjun (se Bilaga 1) om en incident gällande just avslöja lösenord där en student med en dålig idé försökte stjäla en lärares lösenord. Incidenten anmäldes och slutade med villkorlig dom för studenten som sedan dömdes för olaga dataintrång mot Högskolan i Borås. De nämner dock att sådana fall är betydligt mindre förekommande än att en användare klickar på en skadlig länk. Albright (2002) nämner även vikten av hur stora konsekvenser det kan bli om lösenord hamnar på villovägar. Han menar att det kan leda till förlorad tillgänglighet, konfidentialitet samt dataintegritet och yrkar på vikten av att användare har starka lösenord. Detta är något HB IT vidtar som åtgärd då de berättade under intervjun (se Bilaga 1) att de informerar sina användare kring risker gällande lösenord. De uppmanar även sina användare till att ha samma inloggningsuppgifter för att HB IT enklare ska kunna spärra alla ställen där den involverade användarens lösenord har behörighet.

Under intervjun med HB Användare (se Bilaga 2) ställdes en fråga om användaren känner att sitt användarbeteende någon gång utgjort en risk. HB Användare svarade:

*“Nej det känner jag inte. Jag är försiktig men jag är också misstänksam eftersom att jag vet att det kan hända saker. Jag sätter till exempel inte upp post-it lappar med lösenord men jag borde byta lösenord oftare. Det finns ett slags ramverk som informerar att jag ska byta lösenord.”*

Utifrån detta svar anser vi att användaren är medveten om sitt användarbeteende gällande risken med lösenord. Det nämns även att lösenordsbyte dock behövs göras oftare vilket är något som HB IT uppmanar sina användare att göra via utskick angående IT-säkerhet.

Lösenord är även en viktig aspekt i en säkerhetspolicy och ökar möjligheterna för att en organisation ska kunna upprätthålla en god IT-säkerhet enligt Albright (2002). Vid frågan om

HB IT har en säkerhetspolicy samt om den är välkänd för deras användare blev svaret ja. De har en säkerhetspolicy publicerad på Högskolan i Borås webbsida för alla användare att ta del av. De var dock tveksamma till om alla användare aktivt tar del av policyn då HB IT nämnde att deras säkerhetspolicy ligger på en väldigt hög nivå. Enligt deras mening ska den ses mer som en riktning till vad användarna vill åstadkomma med sitt arbete och som sedan ska återspeglas i rutiner och riktlinjer på en lägre nivå. HB IT förtydligar att de menar att varje användare inte behöver förstå deras säkerhetspolicy utan att det räcker med att användarna känner till de regler och riktlinjer som huvudsakligen ger tillräckligt med stöd. Enligt vår tolkning av det som HB IT nämner gällande att varje användare inte behöver förstå säkerhetspolicyn i sin helhet håller vi inte med. Vi menar däremot att detta kan bli en bidragande orsak till att användarna blir mindre säkerhetsmedvetna vilket kan leda till att olika användarbeteenden kan utgöra hot. Detta bekräftas även enligt Höne (2002) som poängterar raka motsatsen mot HB IT:s mening. Höne (2002) menar att det faktiskt är viktigt att användarna i en organisation ska förstå alla delar av en säkerhetspolicy. En säkerhetspolicy ska inte heller vara för komplicerad för användarna att förstå, då mister säkerhetspolicyn sitt fulla syfte. Vi anser att en svårsläst säkerhetspolicy gör att användarna istället avstår från att läsa policyn och därför tror vi att en mindre komplicerad och enklare säkerhetspolicy kan leda till att fler användare tar sig tid till att läsa samt förstå vilket kan göra användarna mer säkerhetsmedvetna.

#### **4.6.6 Installera okända program**

HB IT nämnde under intervjun (se Bilaga 1) installera okända program som ett användarbeteende som kan utgöra hot. De tror att orsakerna till detta användarbeteendet beror på nyfikenhet samt okunskap (se Tabell 4). Användare kan vara nyfikna på att installera okända program för att se vad som händer och har därmed inte tillräckligt med kunskap för att förstå konsekvenserna av detta användarbeteende. Enligt HB IT kan brist på kunskap i detta fall leda till att en användare faller offer för ett så kallat trojan virus. HB IT framförde även att de har som åtgärd för detta användarbeteende att informera sina användare via utskick samt ett antivirusprogram som kan lösas ut i ett sista skede för att skydda systemet mot hot. Colwill (2009) menar även att utbildning är en viktig åtgärd för att minska risken för att användare installerar okända skadliga program. Han menar att det är viktigt att en användare tänker igenom varje steg de tar innan en handling utförs.

#### **4.6.7 Agera ogynnsamt mot arbetsgivaren**

Agera ogynnsamt mot arbetsgivaren kunde utifrån intervjun med HB Användare (se Bilaga 2) identifieras som ett användarbeteende (se Tabell 4). Användaren tror själv att orsaker som brist på tillit och bekräftelse samt lojalitet kan vara bidragande orsaker som kan utlösa ett sådant användarbeteende. Enligt HB Användare kan väldigt låg tillit till arbetsgivaren göra att rapportering av ärenden inte sker i samma utsträckning som det borde. Användaren har upplevt situationer där ingen bekräftelse eller korrekt hjälp vidtogs vilket skapade en frustration hos användaren. HB Användare uttrycker att:

*“Om ett sådant beteende sätter sig kan det bli att man ignorerar arbetsgivaren totalt, eller inte ignorerar utan att man får så lite tillit att man känner att varför berätta om det här, det landar ändå ingenstans hos någon som verkligen förstår det”*

Vid en annan fråga gällande om HB Användare känner bekräftelse och uppskattning av sina chefer var svaret:

*“Absolut inte! Aldrig! Nej ingenting! Det kvittar hur bra kursutvärdering jag har eller hur mycket jag sliter för mina kurser.”*

HB Användare fick även en följdfråga om detta skulle kunna göra så att användaren agerar mindre åt arbetsgivarens bästa intresse och svaret blev nej. Användaren beskriver att glädjen i att utföra sitt jobb väger över och eliminerar riskerna till att agera på ett ogynnsamt sätt mot arbetsgivaren. Detta är något som även Colwill (2009) nämner, han menar att det inte verkar finns någon koppling till att en användares missnöje kan leda till ett ogynnsamt agerande mot en arbetsgivare. HB Användare nämner däremot att en form av tystnadskultur existerar som kan bidra till att folk inte vågar uttrycka sig mot chefer och ledning. Arbetsmiljöfrågor är enligt HB Användare mycket viktigt och användaren tror på en kultur där allt från studenter, forskning, system och rättvisa ses som lika viktiga. Men när kulturen inte är på det viset så kan däremot säkerhetsfrågorna rasa ner och försämrats upplever HB Användare. Gällande organisationskultur och IT-säkerhet menar även Nel och Drevin (2018) att för att anställda ska kunna agera säkerhetsmedvetet är det en förutsättning att informationssäkerhet är integrerat i hela organisationskulturen och att det är viktigt att det tas på allvar.

Under intervjun med HB IT framkom det att de tror att tillit, lojalitet samt kunskap hos användarna minskar riskerna för att en användare ska agera ogynnsamt mot sin arbetsgivare. De menar att tillit och lojalitet tillsammans med att också utbilda användarna till att förstå riskerna kan vara en bra kombination. En starkare tillit och lojalitet till organisationen är något som även Colwill (2009) menar kan minimera riskerna för hotfulla användarbeteenden.

#### **4.6.8 Nyanställd vågar inte uttala sig om ett skadligt beteende**

Under intervjun med HB IT (se Bilaga 1) kunde användarbeteendet nyanställd vågar inte uttala sig om ett skadligt beteende identifieras (se Tabell 4). Det framkom att HB IT tror att användare som har varit anställda en kortare tid inte vågar uttala sig eller rapportera in när misstag och fel har skett. Medan en användare som har varit anställd en längre period har en större förståelse för värdet av Högskolan i Borås information och har bättre kunskap av systemen samt vet vem de kan prata med. Detta stärker även Colwill (2009) som menar att organisationer som har en större andel av användare som har varit anställda en längre tid utgör mindre risk för insiderhot.

Utifrån intervjun med HB Användare (se Bilaga 2) skiljer sig svaret då användaren istället tror att nyanställda utgör en mindre risk rent allmänt då de är mer uppmärksamma och måste enligt HB Användare tippa på tå. HB Användare tror inte att det är bra att arbeta på en och samma arbetsplats för länge och uttrycker sig:

*“Nej, jag tror man blir så här hemmavan och får hybris. Jag tror inte man ska vara för länge på en arbetsplats. Det finns risk att man tror och vet att man kan allt. Sen tror jag att det är bättre med nyanställda som är uppmärksamma på att det här gäller.”*

HB IT upplever dock att det är lättare för dem att upprätthålla en god IT-säkerhet med användare som varit anställda en längre period än med nyanställda. Samt att de till alla

nyanställda skickar kontinuerligt ut säkerhetsinformation samt erbjuder utbildning som en åtgärd för att minska risken för detta typ av användarbeteende. Colwill (2009) menar att detta också kan ha att göra med lojalitet mellan en användare och organisation. Att organisationer behöver försöka främja en lojalitet som utgör en positiv påverkan för dem för att få användare att våga uttrycka sig.

#### 4.6.9 Missbrukar andras användarkonto

Under intervjun som genomfördes med HB IT (se Bilaga 1) framkom användarbeteendet missbrukar andras användarkonto. Detta då HB IT berättade om en incident där en student hade missbrukat en annans students konto. Studenten var sedan tidigare avstängd på grund av olagliga aktiviteter men hade ändå kommit till Högstskolan och bett en annan student om att få låna dennes användarkonto. Då studenten som lånade ut sitt konto var tvungen att gå satt den avstängda studenten kvar och började missbruka kontot genom att göra olika typer av olagliga aktiviteter. HB IT fick vidta åtgärder där de först utförde en utredning samt spårning på de olagliga handlingarna, sedan fick de även kontakta den student som lånat ut sitt användarkonto för att förhöra och undersöka vems handlingar det egentligen var. När HB IT intervjuades fick de frågan om vilka orsaker de tror kan leda till detta skadliga användarbeteende (se Tabell 4). De svarade då att manipulation kan vara en orsak men även hämnd på grund av om en användare har blivit avstängd sedan tidigare. Enligt Colwill (2009) kan en användare använda sig av flera olika tekniker av manipulation för att skapa en situation för att få tillgång till något användaren inte har behörighet till. Precis som HB IT menar Colwill (2009) att en orsak till detta användarbeteende kan vara hämnd på grund av uppsägning eller avstängning. För att förhindra hotet detta användarbeteende utgör finns det även enligt Colwill (2009) åtgärder som behövs vidtas. Vilket då bland annat kan vara att utforma en specifik utbildning för användare som fokuserar på att upptäcka manipulativa försök samt också att varna användare till att vara extra uppmärksamma när de hanterar känslig information.

#### 4.6.10 Använda arbetsdator till privat bruk på ett skadligt sätt

Att använda sin arbetsdator till privat bruk på ett skadligt sätt är ett användarbeteende som utifrån intervjun (se Bilaga 1) med HB IT kunde identifierats. De menar att det kan bero på brist på kunskap, ignorans eller brist på säkerhetsmedvetenhet (se Tabell 4). Under intervjun med HB Användare (se Bilaga 2) ställdes en fråga om det är svårt att veta vart gränsen går gällande vad som är tillåtet att göra när den bärbara arbetsdatorn nyttjas. Användaren svarade:

*“Nej det är inte svårt, jag har mappar där jag lägger privata grejer. Jag tror att man inte får göra så men gör det ändå. Jag tror inte man får använda sin jobbmail till annat än jobbrelaterat men det kan slinka in något annat. Det kan vara familjen som skickar något roligt, då lägger jag det i en privat mapp och det tror jag inte det är riktigt okej men jag gör det ändå.”*

HB Användare är medveten om att det medför risker att nyttja sin arbetsdator till privat bruk men gör det delvis ändå. Detta är något vi tolkar som att användaren är ignorant och inte bidrar fullt ut för att minska hotfulla aktiviteter. Vi anser också att användarens säkerhetsmedvetenhet inte är tillräcklig då användaren inte helt förstår vilka risker det kan medföra. HB IT berättade under intervjun (se Bilaga 1) att de informerar sina användare

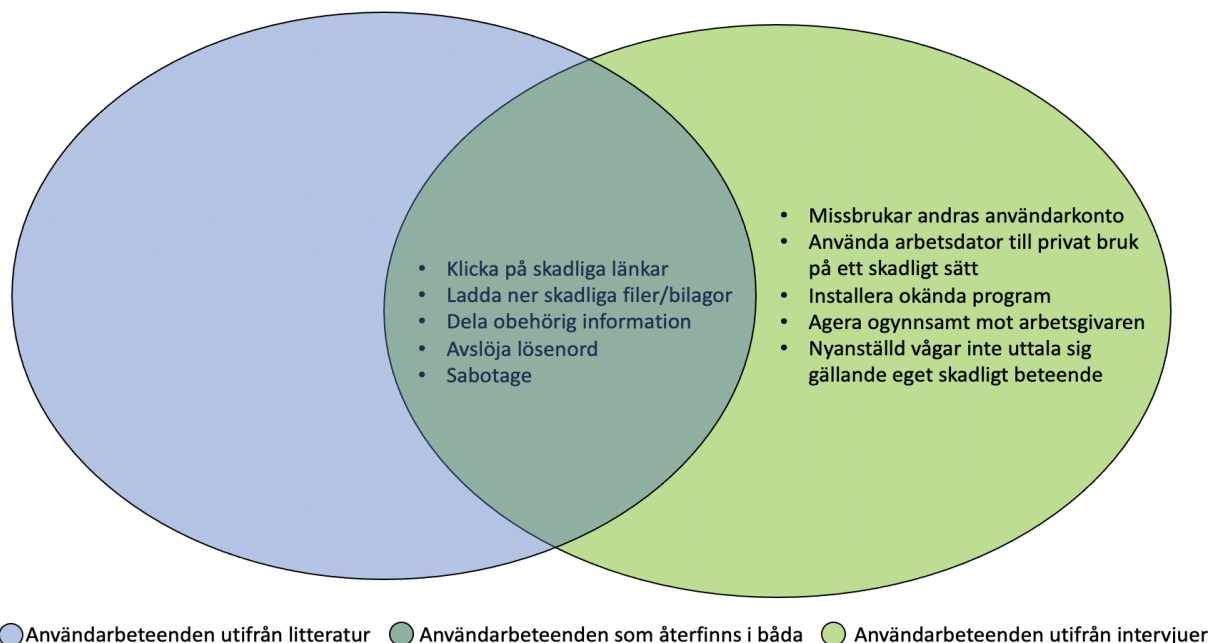
gällande de riktlinjer som finns kring användning av arbetsdator till privat bruk, vilket är en åtgärd de vidtar för att försöka motverka att skadliga handlingar av denna typ uppstår. Vi menar även att det kan vara bra att utbilda användarna kring detta beteende då enligt Metalidou et al. (2014) är utbildning bra för en användares engagemang kring deras arbetsprestanda samt arbetsmotivation. När en arbetsgivare erbjuder utbildning har det visat sig öka användarnas tillfredsställelse vilket i HB IT:s fall kan leda till att användarna känner sig mer engagerade och faktiskt följer de riktlinjer de informeras om och att de blir mer säkerhetsmedvetna.

## 4.7 Venndiagram utifrån litteratur och empiri

Avsnittet presenterar tre venndiagram (se Figur 14-16) där varje diagram visar en jämförelse av användarbeteenden, orsaker och vidtagna åtgärder mellan litteratur och empiri. Till vänster av varje diagram visas det som identifierats utifrån litteratur, till höger visas det som identifierats utifrån intervjuer och i mitten av diagrammet visas det som återfinns i båda.

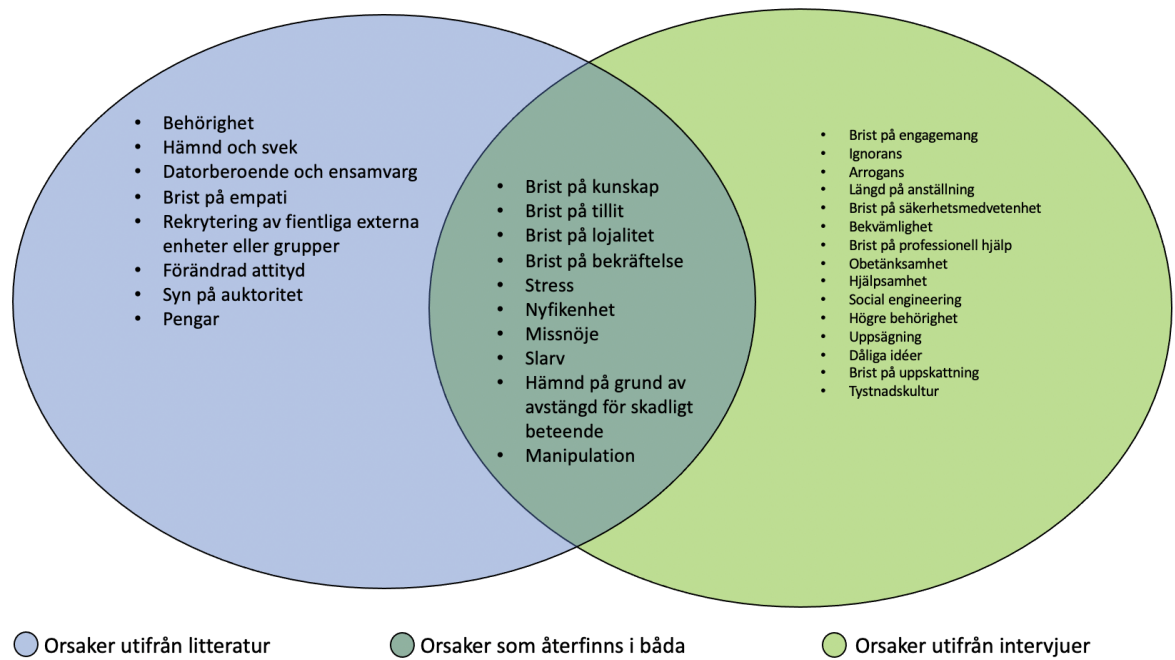
Vi har utifrån våra resultat och analyser kunnat relatera orsaker som leder till ett specifikt användarbeteende samt vidtagna åtgärder till varandra vilket inte gjorts i litteraturen. I litteraturen kunde inga direkta samband finnas med ett specifikt användarbeteende men intervjuerna har resulterat i att vi har kunnat identifiera samband mellan ett visst användarbeteende och dess orsaker samt vidtagna åtgärder. Vi anser att det är en styrka för oss att vi har lyckats identifiera relationer mellan orsaker, användarbeteenden och åtgärder.

### 4.7.1 Venndiagram Användarbeteende



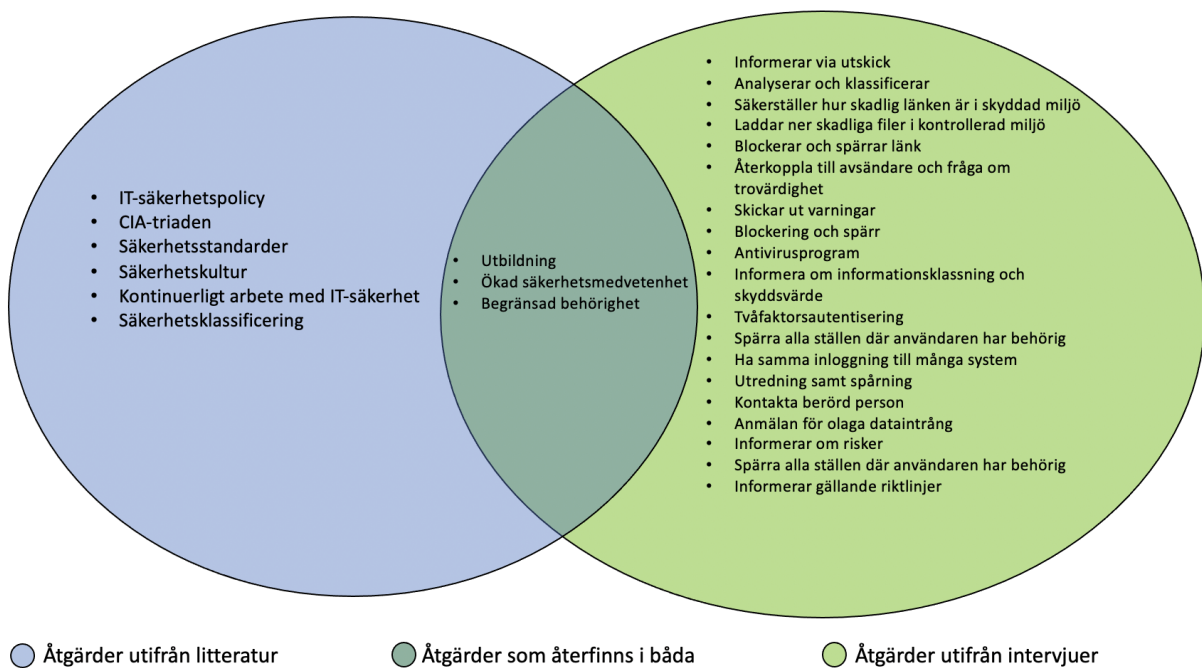
Figur 14.

#### 4.7.2 Venndiagram Orsaker



Figur 15.

#### 4.7.3 Venndiagram Vidtagna åtgärder



Figur 16.

## 5 Diskussion

Enligt det resultat som framkommit utifrån studien finns det flera olika orsaker som kan leda till ett eller flera användarbeteenden. Det har även konstaterats att de vidtagna åtgärderna kan tillämpas på en eller flera användarbeteenden. Från litteraturen identifierade vi 5 användarbeteenden, 15 orsaker och 9 åtgärder medan utifrån intervjuerna framkom 10 användarbeteenden, 25 orsaker och 22 vidtagna åtgärder. Resultatet blev bättre än väntat då det framkom fler användarbeteenden än vad vi till en början trodde var möjligt. Detta då vi uppfattar användarens beteende som ett komplext område som kan bero på mängder av orsaker eftersom alla användare är olika och agerar olika. Denna komplexitet skapade en känsla av osäkerhet hos oss som författare för att inte tillräckligt med användarbeteenden skulle kunna identifieras.

Utöver fynden av användarbeteenden, orsaker och vidtagna åtgärder har studien även resulterat i funna relationer mellan dem. I tidigare litteratur finns ingen direkt relation mellan ett specifikt användarbeteende, orsak samt vidtagen åtgärd. Colwill (2009) har endast lyckats framföra personliga egenskaper vilket är det samma som orsaker som han vidare skriver tros ha konsekvenser för ett användarbeteende. För att vidare styrka detta nämner Colwill (2009) ett exempel gällande orsaken missnöje hos användare. Han menar att det inte finns någon direkt koppling mellan ett insiderhot och missnöjda användare. Colwill (2009) påpekar dock det vi också har upptäckt under studiens gång att för att göra en mer rättvis analys av orsak till ett användarbeteende är det till fördel att vidta en mer psykologisk analys. Det vi anser ofta förekommer i litteraturen är uppräddade orsaker som saknar relation gentemot användarbeteenden. Zeadally et al. (2012) styrker även detta genom att också endast rada upp flera orsaker som saknar en vidare relation till användarbeteenden. Zeadally et al. (2012) nämner att det är en stor utmaning att identifiera användarbeteende som kan utgöra hot mot en organisation. Detta var även en utmaning för oss men under studiens gång lyckades vi hitta relationer med hjälp utav välformulerade intervjufrågor som specifikt utgick ifrån att försöka få fram relationer mellan användarbeteende, orsaker och vidtagna åtgärder.

En annan intressant upptäckt framkom även under studiens gång gällande användarbeteendens relation till varandra. Detta framkom vid en mer ingående analys kring vad som orsakar användarbeteendena, vi upptäckte att det kan vara så att ett användarbeteende kan leda till andra användarbeteenden. Även detta är något som vi inte anser förekommer i tidigare litteratur men som vi menar är en värdig poäng att ta med i vår studie. Detta kan även vara en intressant teori att undersöka djupare i framtida forskning.

### 5.1 Metodreflektion

Den metod som använts för att utföra denna studie är en kvalitativ metod i form av intervjuer. Tillvägagångssättet har varit optimalt för vår studie och har bidragit till att vi har fått den empiri som behövs för att kunna utföra vår studie. Vi tycker att det har varit en passande metod att använda till vår studie för att kunna svara på vår frågeställning.

Vi anser att en styrka med vår metod är att valet av intervjudeltagare visade sig vara lyckat. Detta då de kunde bidra med sina expertkunskaper vilket resulterade att vi utifrån intervjuerna fick tillgång till behövt material för att genomföra studien. Med intervjudeltagarna kunde vi få ut två olika perspektiv, ett utifrån en användares samt ett utifrån en IT-avdelning som gav

oss en bredare förståelse för användarbeteenden, orsaker samt vidtagna åtgärder.

Eftersom vi ville få ut så mycket information som möjligt utifrån intervjuerna upplevde vi att det var en utmaning för oss att formulera intervjufrågorna. Området är enligt vår uppfattning ett komplext område vilket bidrog till utmaningen med att skriva intervjufrågorna då vi inte visste hur vi skulle formulera frågorna för att få ut användarbeteenden, orsaker och vidtagna åtgärder. Trots denna utmaning lyckades vi formulera intervjufrågor som var till fördel för vår studie.

## 6 Slutsats

Vi kan med denna studie konstatera att det finns flera olika orsaker som kan vara orsaken till ett eller flera användarbeteenden som utgör ett hot samt att det finns åtgärder som en organisation kan vidta mot dessa användarbeteenden.

Tekniken utvecklas hela tiden och det gör även det som kan utgöra ett hot mot organisationer. Enligt vår uppfattning spelar det ingen roll hur stort skydd en organisation vidtar då det alltid finns möjligheter för hot att ta sig in. En användare är enligt vår mening många gånger oförutsägbar och trots utbildning eller ökad säkerhetsmedvetenhet kan vad som helst hända. Utifrån vår studie har vi sett vad missnöje hos användare kan leda till för konsekvenser. Detta kan både leda till att en användare inte vill ta del av säkerhetsutbildning och utgör en större risk för att utföra skadliga användarbeteenden. Vi anser därför att det är varje organisations ansvar att vara medveten om vad som behöver skyddas, hur systemen ska skyddas och inkludera sina användare att försöka få mer kunskap kring vilka hot som finns samt vilka hot en användare faktiskt kan utgöra. Det är svårt att veta när ett hot ska ske eller när ett användarbeteendet kommer orsaka en skada. Vi anser därför att utbildning är den främsta åtgärd för organisationer att vidta för att kunna minska riskerna för skadliga användarbeteenden. Alla användare bör dock ta ett eget individuellt ansvar men det är organisationers främsta ansvar att se till att deras användare får rätt förutsättningar för att kunna agera på ett säkert sätt. Något som kan vara svårt för användare är att veta var gränsen går för vad som är okej och inte. Att då som arbetsgivare i den största möjliga mån det går förtydliga detta för sina användare kan göra en skillnad och möjligtvis förhindra förvirring, misstag och risker.

Studiens syfte har varit att besvara frågeställning som lyder: *“Vilka orsaker till användarnas beteenden utgör ett hot för en organisations IT-säkerhet och vilka åtgärder har vidtagits?”*. Frågeställningen har besvarats då 10 användarbeteenden, 25 orsaker och 22 vidtagna åtgärder har identifierats. Dessa samt deras relationer redogörs tydligt i en resultattabell (se Tabell 4).

En styrka med studien är att vi har lyckats hitta relationer mellan de användarbeteenden, orsaker samt vidtagna åtgärder som identifierats under de genomförda intervjuerna, vilket vi anser inte har framkommit i litteraturen. Vi anser även att den upptäckt vi gjort av användarbeteenden och dess koppling till andra användarbeteenden är en styrka då den öppnar upp för nya möjligheter till framtida forskning. Att studien resulterat i så många användarbeteenden, orsaker samt vidtagna åtgärder ser vi också som en styrka då vi kunnat identifierat dessa.

En svaghet med studien anser vi är att användarbeteenden kan påverkas av flera aspekter som till exempel psykologi. Vi tror därför att för att kunna göra en rättvis analys av en användares beteende krävs det erfarenhet från flera parter som besitter relevant kunskap inom flera områden. En annan svaghet var att HB IT inte kunde ge oss en direkt koppling gällande alla användarbeteenden och dess vidtagna åtgärder, detta på grund av att det är svårt att i förebyggande syfte veta vilken åtgärd som kan vidtas vid ett specifikt användarbeteende. Åtgärderna är till för att förhindra flera olika hot och hotfulla användarbeteenden.

Avslutningsvis anser vi att det är möjligt att identifiera användarbeteenden, orsaker samt vidtagna åtgärder för en organisation men också även att det finns och går att hitta relationer mellan dem. Vi upplever att den största utmaning gällande IT-säkerhet för organisationer är att, med hjälp av utbildning försöka få sina användare att uppnå en högre nivå av

säkerhetsmedvetenhet. Vi tycker även att alla användare inom en organisation ska inkluderas och ta del av säkerhetsutbildning för att uppnå en god IT-säkerhet.

## 7 Framtida forskning

Vi anser att vår studie har fått ett lyckat resultat och uppnått sitt syfte. Men vi ser även att det finns stora möjligheter för framtida forskning kring området.

För att utöka forskningen inom området i framtiden tror vi att det krävs att fler parter är involverade. Med andra parter syftar vi till bland annat psykologer, beteendevetare och IT-säkerhetsexperter, detta då vi anser att människan och dess beteenden är komplexa. Att fler parter med expertkunskaper involveras kan enligt vår mening leda till att ytterligare användarbeteenden, orsaker och vidtagna åtgärder identifieras, samt ger en mer rättvis och tydligare relation. En rekommendation från oss som författare till framtida forskning är att involvera fler intervjudeltagare för att få en bredare uppfattning kring hur en användare kan bete sig.

Ytterligare två aspekter att forska vidare på är användarbeteenden och åtgärder. Som vi tidigare nämnt anser vi att det inte finns någon tidigare forskning kring användarbeteendernas relation till varandra och det tycker vi är en intressant faktor att undersöka vidare. Gällande de åtgärder som framkommit via vår studie har vi inte utvärderat om de har varit lyckade eller inte, därför rekommenderar vi även en fortsatt forskning där åtgärderna faktiskt utvärderas djupare. Detta för att ta reda på om åtgärderna blev lyckade och om de resulterade i att oönskade användarbeteenden minskade eller upphörde.

Vi anser att mer forskning behövs kring ämnet eftersom det är högst relevant och viktigt för organisationer att skydda sina tillgångar. Inget får tas för givet och IT-säkerhet är ett område som bör arbetas med kontinuerligt.

## 8 Källförteckning

Aftonbladet (2021). *Regeringens vaccinsamordnare skickade hemlig info till privat mejl*.  
<https://www.aftonbladet.se/nyheter/a/OQWv6A/anvander-privat-mejl-for-hemliga-vaccin-uppgifter/salesposter?useFlexbox=true&shared=false&reason=denied> [2021-04-10]

Albright, J.G. (2002). The Basics of an IT Security Policy. *GSEC Practical Requirement V. 1.3 SANS Institute of Technology, 1*

Andress, J. (2011). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Nederländerna: Elsevier.

Chen, H., & Boutros, P. C. (2011). VennDiagram: a package for the generation of highly-customizable Venn and Euler diagrams in R. *BMC bioinformatics*, 12(1), 1-7.

Colwill, C. (2009). Human factors in information security: The insider threat—Who can you trust these days?. *Information security technical report*, 14(4), ss.186-196.

Da Veiga, A., Astakhova, L.V., Botha, A. & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, 92, s.101713.

Farooq, M.U., Waseem, M., Khairi, A. & Mazhar, S., 2015. A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, 111(7).

Goldkuhl, G. & Röstlinger, A., 2012. Förändringsarbete och förändringsanalys enligt SIMMetoden. *VITS/IEI, Linköpings universitet*.

Gonzalez, J.J. & Sawicka, A. (2002). A framework for human factors in information security. *In Wseas international conference on information security, Rio de Janeiro* ss. 448-187.

Höne, K. & Eloff, J.H.P., 2002. What makes an effective information security policy?. *Network security*, 2002(6), ss.14-16.

Jacobsen, D, I. (2017). Hur genomför man undersökningar? *Introduktion till samhällsvetenskapliga metoder*. Lund: Studentlitteratur AB.

Jouini, M., Rabai, L.B.A. & Aissa, A.B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, ss. 489-496.  
<https://www.sciencedirect.com/science/article/pii/S1877050914006528>

Leist, S. & Zellner, G. (2006). *Evaluation of Current Architecture Frameworks*. Diss. Germany: University of Regensburg.  
<https://dl-acm-org.lib.costello.pub.hb.se/doi/pdf/10.1145/1141277.1141635>

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, 147, ss.424-428.

Mitrovic', P. (2003). *Handbok i IT-säkerhet, 3 upplagan*. Sundbyberg:Pagina Förlag AB.

Nel, F. & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*.

Samonas, S. & Coss, D. (2014). THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. *Journal of Information System Security*, ss. 21-45. <http://www.proso.com/dl/Samonas.pdf>

Snsc(u.å). *It-säkerheten*. [snsc.se/it-sakerhet.html](http://snsc.se/it-sakerhet.html) [2021-02-22]

Whitman, M.E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 24(1), ss.43-57.

Woodhouse, S. (2007). Information security: End user behavior and corporate culture. In *7th IEEE International Conference on Computer and Information Technology (CIT 2007)* ss. 767-774. IEEE.

Zeadally, S., Yu, B., Jeong, D.H. & Liang, L. (2012). Detecting insider threats: Solutions and trends. *Information security journal: A global perspective*, 21(4), ss.183-192.

# **Bilaga 1: Intervjuguide HB IT**

**Kan ni beskriva vad ni arbetar med på Högskolan i Borås?**

**Vad innebär IT-säkerhet för er?**

**I vår teori anses användarbeteende vara ett av de största hoten mot IT-säkerhet, hur ställer ni er kring det, håller ni med eller inte?**

**Vilka av Högskolans system skulle ni säga är mest utsatta för hot på grund av olämpliga användarbeteenden?**

**Vilka användarbeteenden har ni identifierat som utgör ett hot mot Högskolans IT-säkerhet?**

- till exempel ladda ner filer, klicka på länkar eller berätta obehörig information.

**Laddar ni ner filer till er arbetsdator?**

- Om ja, har du koll på vad som kan vara en farlig fil? - Om ja, hur ser ni det och vet det?  
Om nej, vad är anledningen till att du inte kan se skillnad på en farlig fil och en ofarlig?

**Om ni mottar ett mejl från en okänd källa kan ni beskriva hur ni agerar?**

**Om ni mottar ett mejl från en kollega där det finns en länk bifogad i mailen, hur agerar ni då?**

- Klickar du på länken?
- Skickar du ett mail tillbaka och frågar vad det är för länk?
- Beskriv situationen.
- Varför gör du så?

**Vad tror ni orsaken kan vara att en användare laddar ner filer som kan utgöra skada?**

**Vad tror ni orsaken kan vara att en användare klickar på länkar som kan utgöra skada?**

**Vad tror ni orsaken kan vara att en användare berättar om obehörig information till någon som inte har rätten till den informationen?**

**Vad tror ni okunskap kan leda till för användarbeteende?**

**Vad tror ni missnöje kan leda till för användarbeteende? Med missnöje menar vi missnöje generellt med arbetsplatsen/arbetsgivaren.**

**Vad tror ni lojalitet kan leda till för användarbeteende? Med lojalitet menar vi att man alltid agerar till fördel mot arbetsgivaren.**

**Vad tror ni tillit kan leda till för användarbeteende? Med tillit menar vi att det finns ett förtroende till arbetsgivare.**

**Vad tror ni gällande längden på hur länge en användare arbetat på arbetsplatsen kan leda till för användarbeteende? Alltså om en anställd har arbetat på arbetsplatsen under en längre tid.**

**Vad tror ni brist på empati kan leda till för användarbeteende?**

**Vad tror ni manipulation kan leda till för användarbeteende? Med manipulation menar vi till exempel manipulera kollegor till att berätta obehörig information.**

**Anser ni att en anställd med högre behörighet kan utgöra en större risk än någon med begränsad behörighet?**

**Vet ni vilka av Högskolans användare som utgör det största hotet mot Högskolans IT-säkerhet? t.ex studenterna, lärare**

**Vilken åtgärd har ni vidtagit för att eliminera skadlig nedladdning av filer?**

- var dessa åtgärder tillräckliga?
- om nej, hur är ni beredda att agera om det skulle hända?

**Vilken åtgärd har ni vidtagit för att eliminera att en användare klickat på skadliga länkar?**

- var dessa åtgärder tillräckliga?
- om nej, hur är ni beredda att agera om det skulle hända?

**Vilken åtgärd har ni vidtagit för att eliminera att obehörig information har kommit ut till fel användare?**

- var dessa åtgärder tillräckliga?
- om nej, hur är ni beredda att agera om det skulle hända?

**Har ni en säkerhetspolicy, hur ser den ut och hur arbetar ni med den?**

**Om ni har en säkerhetspolicy, känner anställda till denna?**

- Om ja, hur gör ni för att göra anställda medvetna?
- Om nej, varför?

**Följer ni någon säkerhetsstandard? (ISO 27001)**

**Genomför ni utbildningar/kurser i IT-säkerhet för Högskolans användare?**

- Utbildning där ni informerar användarna hur de ska agera vid olika situationer, t.ex om de mottar ett mail från en okänd källa?

**Hur ofta genomför ni säkerhetsutbildningar/kurser?**

- Enligt en källa bör en utbildning/uppdatering ske mot alla användare vartannat år.

**Är det obligatoriskt för användarna att genomföra de säkerhetsutbildningar ni erbjuder?**

- Om ja, varför anser ni att det ska vara obligatoriskt?
- Om nej, varför är det ej obligatoriskt? - Tror ni inte att det kan utgöra en risk?

**Har ni någon gång kunnat förutse hot mot Högskolans IT-säkerhet med hjälp av kontroller och granskning av anställda?**

- Om ja, beskriv situationen, från upptäckt till åtgärd.
- Om nej, tror ni att det är möjligt att förutse hot?

**Gör ni någon säkerhetsklassificering av era hot? (Bedömning, Prioritering)**

**Applicerar ni CIA-triaden i Högskolans IT-säkerhet ?**

- Om ja, beskriv hur.
- Om nej, varför?

**Vad skulle ni säga är Högskolan styrkor och svagheter gällande IT-säkerhet?**

**Tycker ni att era åtgärder för att uppnå en god IT-säkerhet är tillräckliga?**

**Upplever ni att era användare är säkerhetsmedvetna**

**Har ni något tips till oss som ni tycker att vi ska ta upp i våran kandidatuppsats gällande IT-säkerhet rent generellt som är viktigt?**

**Avslutningsvis, vill ni tillägga något eller är det något ni känner vi har glömt att ta upp?**

## **Bilaga 2: Intervjuguide HB Användare**

**Vad arbetar du som på Högskolan i Borås, beskriv din roll?**

**Kan du förklara vad du gör i systemet, de funktioner du använder?**

**Vad är din ställning till IT-säkerhet?**

**Följer du rutiner och säkerhetspolicys som används för att skydda Högskolan mot säkerhetshot?**

- Om ja, hur ofta läser du den för att hålla dig uppdaterad? Tar du eget ansvar eller blir du påmind av någon ansvarig att hålla dig uppdaterad.
- Om nej, kan du beskriva varför du inte följer dom?

**Tycker du att du har blivit tilldelad rätt behörighet?**

- Saknar du något?
- Tror du att du med din behörighet utgör ett större hot än någon med lägre behörighet? Till exempel en student.
- Har du blivit informerad om varför du har en viss typ av behörighet?

**Känner du att ditt användarbetende någon gång utgjort en risk?**

- Om ja, beskriv situationen.
- Om nej, varför?
- Om "jag vet inte", varför känner du dig osäker att svara varken ja eller nej - kan det bero på till exempel omedvetenhet eller okunskap?

**Om du mottar ett mejl från en okänd källa kan du beskriva hur du agerar?**

- Beskriv situationen.
- Varför gör du så?

**Har du någon gång eller vet du någon som blivit utsatt för manipulation av en kollega? Till exempel att berätta om obehörig information?**

**Om du mottar ett mail från en kollega där det finns en länk bifogad i mailen, hur agerar du då?**

- Klickar du på länken?
- Skickar du ett mail tillbaka och frågar vad det är för länk?

**Anser du att det är svårt att veta vart gränsen vad du får göra när det gäller jobb och privatliv när du nyttjar din bärbara arbetsdator?**

**Laddar du ner filer till din arbetsdator?**

- Om ja, har du koll på vad som kan vara en farlig fil? - Om nej, vad är anledningen till att du inte kan se skillnad på en farlig fil och en ofarlig?

**Vilka beteenden tror du att du själv har som kan utgöra ett hot mot Högskolans IT-säkerhet?**

- Som till exempel ladda ner en okänd fil.

**Känner du dig osäker på vad du får lov att göra i systemet?**

**Är du medveten om vad Phishing/Nätfiske är?**

- Om ja, är du medveten om vilka risker det utgör?
- Om nej, vad är anledningen till att du inte känner till det?

**Är du medveten om vad ett Trojan virus är?**

- Om ja, är du medveten om vilka risker det utgör?
- Om nej, vad är anledningen till att du inte känner till det?

**Tror du att en användare/anställd som arbetat länge på Högskolan i Borås kan utgöra ett mindre hot jämfört mot en som arbetat en kortare tid?**

- Om ja, kan du förklara varför du tror det och vad kan det bero på?
- Om nej, kan du förklara varför du tror det och vad kan det bero på?

**Känner du att det finns tillit mellan dig och arbetsgivaren?**

- Om ja, känner du en lojalitet till att utföra ett bra arbete på grund av det?
- Om nej, tror du att brist på tillit kan utgöra en risk mot Högskolans IT-säkerhet?

**Känner du att du får bekräftelse och uppskattning av dina chefer?**

- Om ja, känner du att det kan göra så att du agerar mer åt Högskolans bättre intresse?
- Om nej, känner du att det kan göra så att du agerar mindre åt Högskolans intresse som i sin tur kan bli ett hot mot Högskolans IT-säkerhet?

**Vilka orsaker tror du kan utgöra ett hot för Högskolans IT-säkerhet? Som till exempel missnöje och slarv.**

**Ser du positivt eller negativt kring Högskolans maktpositioner/chefer?**

**Upplever du att Högskolan i Borås arbetar aktivt med IT-säkerhet?**

**Vad tycker du att Högskolan i Borås kan vidta för åtgärder för att öka IT-säkerheten?**

**Har du genomgått någon utbildning intern inom Högskolan i Borås gällande IT-säkerhet eller någon form av genomgång där du som användare blivit informerad hur du ska agera ur ett IT-säkerhetsperspektiv?**

**Anser du att Högskolan tar sitt ansvar att göra dig som användare mer säkerhetsmedveten?**

- Om nej, vad önskar du att de kunde göra mer för dig?

**Avslutningsvis, vill du tillägga något eller är det något du känner vi har glömt att ta upp?**

## Bilaga 3: Problemlista

1. Brist på kunskap
2. Brist på engagemang
3. Stress
4. Nyfikenhet
5. Ignorans
6. Arrogans
7. Missnöje
8. Slarv
9. Längd på anställning
10. Manipulation
11. Brist på tillit
12. Brist på säkerhetsmedvetenhet
13. Bekvämlighet
15. Brist på professionell hjälp
14. Obetänksamhet
16. Hjälpsamhet
17. Social engineering
18. Högre behörighet
19. Uppsägning
20. Dåliga ideer
21. Hämnd på grund av avstängd för skadligt beteende
22. Brist på lojalitet
23. Brist på bekräftelse
24. Brist på uppskattning
25. Tystnadskultur
26. Klicka på skadliga länkar
27. Ladda ner skadliga filer/bilagor
28. Installera okända program
29. Dela obehörig information
30. Sabotage
31. Agera ogynnsamt mot arbetsgivaren
32. Nyanställd vågar inte uttala sig gällande eget skadligt beteende
33. Missbrukar andras användarkonto
34. Avslöja lösenord
35. Använda arbetsdator till privat bruk på ett skadligt sätt



# HÖGSKOLAN I BORÅS