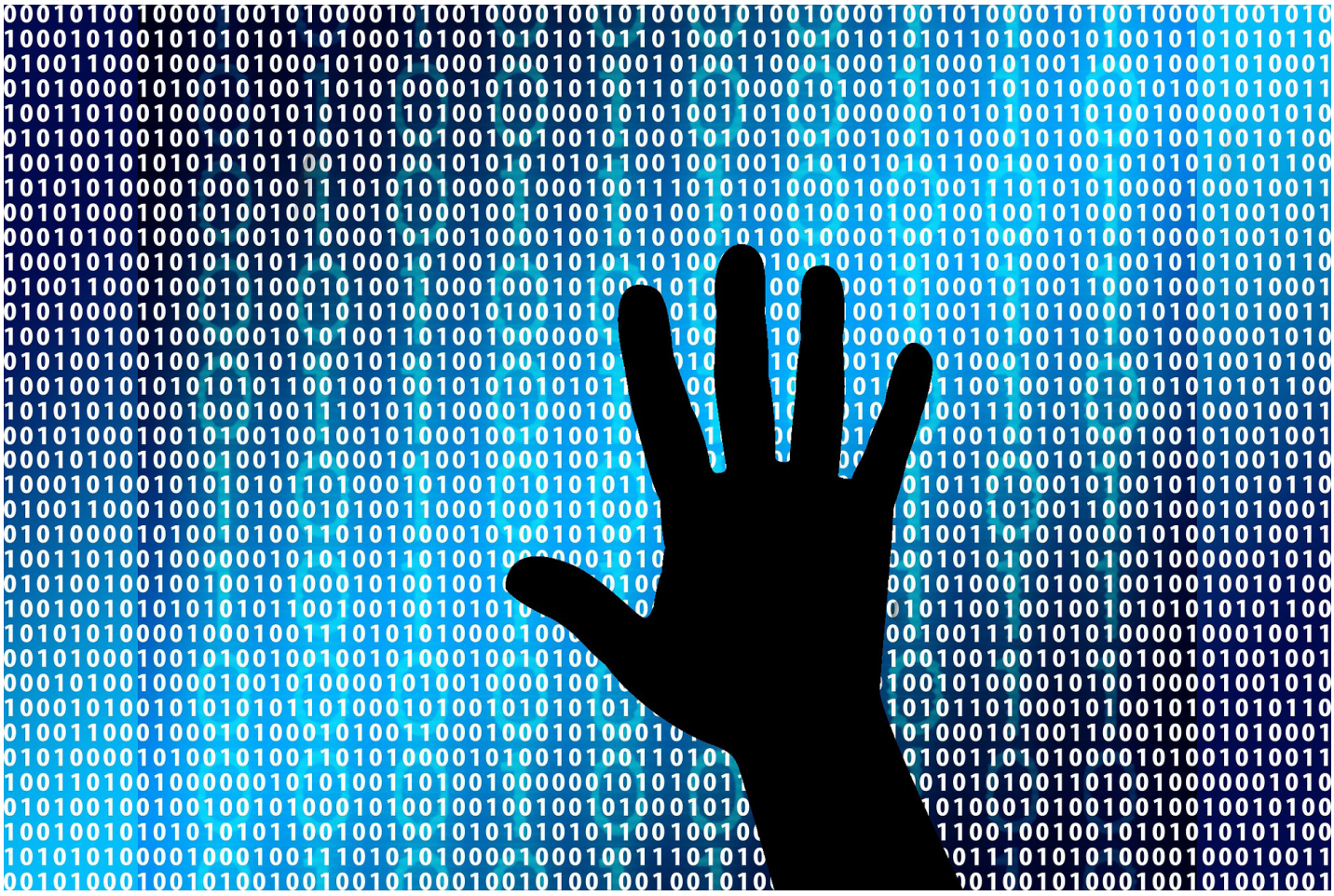
FOI

Litteraturöversikt av samspelet mellan människa, teknik och organisation för IT-säkerhet

PETER SVENMARCK



FOI-R--4425--SE
ISSN 1650-1942 April 2017

Peter Svenmarck

Litteraturöversikt av samspelet mellan människa, teknik och organisation för IT-säkerhet

Titel	Litteraturöversikt av samspelet mellan människa, teknik och organisation för IT-säkerhet
Title	Literature Review of Human Systems Integration for Cyber Security
Rapportnr/Report no	FOI-R--4425--SE
Månad/Month	April/April
Utgivningsår/Year	2017
Antal sidor/Pages	39 p
ISSN	1650-1942
Kund/Customer	FMV
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E32398
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Den ökade användningen av kommunikations- och informationsteknik gör att antagonister försöker få tillgång till och påverka dessa informationsflöden. Vidare är informationssystem särskilt sårbara på grund av snabb hotutveckling, många accesspunkter och stora informationsflöden. Traditionellt har forskning om IT-säkerhet till stor del handlat om tekniska skydd. Successivt ökar insikten om att forskning även behövs om hur IT-säkerhet skapas genom en kombination av organisatoriska processer, tekniska skydd och personal.

Syftet med den här litteraturöversikten av samspelet mellan människa, teknik och organisation för IT-säkerhet är att beskriva frågeställningar som diskuteras och dokumenterade resultat. Urvalet av litteratur begränsades till litteratursökningar på Google Scholar, områdesbevakning på valda konferenser och rekommendationer från andra forskare. Totalt identifierades cirka 500 publikationer varav litteraturöversikten sammanfattar 93.

Litteraturöversikten visar att befintlig litteratur om angripare är begränsad. Några studier beskriver bland annat hur angripare skapar komplexa mentala modeller för att utnyttja sårbarheter som försvararna inte förväntar sig.

Befintlig litteratur om försvarare är mer omfattande. Litteraturen beskriver bland annat komplexiteten i IT-säkerhetsexperters arbete som omfattar analyser, rådgivning och kontroller i interaktion med många intressenter. Litteraturen beskriver hur en viktig del av arbetsuppgifterna är utformning av IT-säkerhetspolicyn. Tyvärr har IT-säkerhetsexperterna sällan tillräckliga kunskaper om verksamheten för att policyn ska blir riktigt användbar. Vidare är intrångsdetektion en viktig funktion för att upptäcka obehöriga personer som försöker ta sig förbi tekniska skydd. Med specifika kunskaper om det aktuella datornätverket kan personalen avgöra vilka larm från tekniska skydd som indikerar faktiska attacker. Befintliga verktyg för intrångsanalyser består ofta av textuella sökfunktioner där operatörer på ett flexibelt sätt successivt kan pröva olika hypoteser.

Slutligen har användare ett ansvar för att inte i onödan skapa sårbarheter. I vilken utsträckning användare respekterar IT-säkerhetspolicyn beror både på individuella och organisatoriska faktorer. Några exempel på individuella faktorer är bland annat attityder, normer, uppfattningen av den egna förmågan att hantera hoten samt förståelsen av IT-säkerhetspolicyn. Några exempel på organisatoriska faktorer är hur ledningens stöd för IT-säkerhet påverkar organisationens IT-säkerhetskultur. Vidare är användare överlag dåliga på att upptäcka så kallat nätverksfiske eftersom det utnyttjar inlärda heuristiker för hur e-post ska hanteras. Snabb hantering av e-post förutsätter ofta heuristiker, men konsekvensen är att mer detaljerade granskning sällan sker av e-post.

Avslutningsvis ges några rekommendationer för fortsatta studier av angripare, försvarare och användare.

Nyckelord: IT-säkerhet, uppgiftsanalys, personalhantering, situationsmedvetenhet, intrångsdetektion, visualisering, användbarhet, spelteori, IT-säkerhetspolicy, IT-säkerhetsmedvetande, IT-säkerhetskultur, autentisering, nätverksfiske, IT-brott

Summary

With the increased use of communication and information technologies, antagonists try access and affect these information flows. Information systems are especially vulnerable for such attacks due to rapid threat development, many access points, and large information flows. Traditionally, cyber security research has mainly focused on technical protection. However, there is a growing amount of research about of how cyber security is created in the integration of organisational processes, technical protection, and personnel.

The report describes a literature review of human systems integration for cyber security. The literature review summarises typical research topics and available results. The literature selection was limited to searches on Google Scholar, recent conferences, and recommendations from other researchers. Of about 500 identified publications, the literature review summarises 93.

The literature review shows that the available literature about attackers is rather limited. Some studies describe how attackers create complex mental models to exploit weaknesses that the defenders do not expect.

The available literature about defenders is more comprehensive. For example, the literature describes the task complexity for cyber security practitioners. Typical cyber security tasks encompass analysis, advice, and audit of cyber security in collaboration with many stakeholders. An important task is development of the cyber security policy. However, cyber security practitioners often do not have sufficient knowledge about the work processes to develop a truly usable policy. Further, intrusion detection is an important function to detect unauthorised access. Here, analysts use their situated knowledge about the network to determine which alerts from intrusion detection systems that indicate actual attacks. Existing tools for analysis of intrusions usually consist of textual search functions where operators can test their hypotheses in a flexible way.

Further, users are responsible for not unnecessarily creating vulnerabilities. Users respect for the cyber security policy depends on both individual and organisational factors. Some individual factors are attitudes, norms, self-efficacy, and understanding of the cyber security policy. Some organisational factors are management support for cyber security, which affects the cyber security culture. Additionally, users are overall poor at detecting phishing since it utilises learned heuristics for managing e-mail, which means that detailed examinations are seldom performed.

Finally, the report provides some recommendations for future studies of attackers, defenders, and users.

Keywords: cyber security, task analysis, personnel management, situation awareness, intrusion detection, visualisation, usability, game theory, policy compliance, security awareness, security culture, authentication, phishing, insider threat

Innehållsförteckning

1 Inledning

Militära organisationer använder kommunikations- och informationsteknik för många funktioner, som till exempel ledning, vapensystem, underrättelseanalys, övervakning och spaning. Informationsteknik ger många fördelar och därför försöker motståndare få tillgång till och påverka dessa informationsflöden. Informationssystem är dessutom särskilt sårbara eftersom hotet utvecklas snabbt, det finns ofta många accesspunkter, påverkan kan ske från en annan plats, stora informationsflöden döljer otillbörligt användning och att påverkan kan ske med minimal infrastruktur. Eftersom IT-säkerhet för informationssystem blir allt viktigare ökar intresset för området i många länder.

Precis som inom många andra riskområden förutsätter IT-säkerhet en avvägning mellan säkerhetsbehov och verksamhetskrav. Det är helt enkelt svårt att göra fullständigt säkra informationssystem eftersom begränsningarna blir så omfattande att det operativa värdet minskar. Vidare skapas IT-säkerhet genom en kombination av organisatoriska processer, tekniska skydd och personal. Organisatoriska processer avgör investeringar i IT-säkerhet, systemadministratörer utför IT-säkerhetspolicyn och både administratörer och användare använder tekniska skydd för att upptäcka och hantera hot. Traditionellt har forskning om IT-säkerhet till stor delen handlat om tekniska skydd. Successivt ökar insikten om att forskning även behövs om hur hela det sociotekniska systemet behöver bli bättre på att hantera IT-hot.

Människans betydelse för IT-säkerhet studeras i Sverige genom till exempel situationsmedvetenhet för IT-säkerhet (Franke & Brynielsson, 2014), intrångsdetektion (Lif, Holm, Sommestad, Granåsen, & Westring, 2016) och säkra IT-system för användare (SECURIT, 2016). För att ta ett helhetsgrepp på det här området finansierar FMV[1] övergripande studier av samspelet mellan människa, teknik och organisation (MTO) för IT-säkerhet. Arbetet omfattar deltagande i forskningsgruppen NATO STO HFM-259 *Human Systems Integration Approach to Cyber Security*, områdesbevakning på konferenser och en litteraturöversikt. Den här rapporten beskriver enbart litteraturöversikten. Övrigt arbete inom HFM-259 beskrivs i Svenmarck (2015) och Svenmarck (2016).

Eftersom människans betydelse för IT-säkerhet är ett brett och till många delar omskrivet område, är det svårt att sammanfatta all litteratur i ett dokument. Syftet med den här litteraturöversikten är enbart att beskriva frågeställningar som diskuteras och dokumenterade resultat utifrån en begränsad litteratursökning. Litteratursökningen begränsades till sökningar på Google Scholar, områdesbevakning på valda konferenser och rekommendationer från andra forskare. Områdesbevakningen gjordes på HCII 2015, HSI 2015 och AHFE 2016. Den begränsade litteratursökningen bedömdes vara representativ för befintlig litteratur, även om den varken var fullständig eller helt stringent. Totalt identifierades cirka 500 publikationer. Litteraturöversikten sammanfattar de publikationer som beskriver vilket problem inom samspelet mellan människor och teknik för IT-säkerhet som studerades, beskriver ett förslag för att hantera problemet samt på något sätt utvärderar förslaget. Totalt uppfyllde 93 publikationer dessa kriterier.

Först sammanfattas litteratur som handlar om angripare. Därefter sammanfattas om försvarare och användare. Skillnaderna i omfattning på tillgänglig litteratur avspeglar i stort vad som görs inom området. Andra relaterade litteraturöversikter är till exempel Boyce m.fl. (2011), Crossler m.fl. (2013), Enrici, Ancilli och Lioy (2010) samt Gutzwiller, Fugate, Sawyer och Hancock (2015). En avslutande diskussion sammanfattar resultatet av litteraturöversikten. Ett antal förslag ges även för fortsatt forskning om humanaspekter för IT-säkerhet.

[1] Inom ramen för projektet C3 Interoperabilitet (C3IOP) och FoT Ledning och MSI, FMV beteckning 389702 - LB892507

2 Litteratur om angripare

En viktig del av IT-säkerhet är att förstå hur angripare tänker och resonerar eftersom det ger försvararna bättre möjligheter att försvåra attacker. Summers (2015) beskriver tre empiriska studier av hur angripares färdigheter och kognitiva egenskaper påverkar hur de lär och projicerar framtida situationer baserat på ständigt förfinade komplexa mentala modeller. Modellerna används för att förutse framtida resultat genom spekulativa prognoser som utgör en grund för förväntade effekter av åtgärder, planering av åtgärder och tolkning av återmatning. Studierna ger förslag på strategier för att förbättra angripares färdigheter. Tyvärr har studien ännu bara presenterades muntligt och avhandlingen som studien bygger på är ännu inte tillgänglig. En av de ingående studierna beskrivs däremot i Summers och Lyytinen (2013). Där beskrivs att attacker handlar om att utnyttja svagheter som försvarare inte förväntar sig och att det därför behövs omfattande tekniska kunskaper om datorsystem och hur de brukar konfigureras. De här kunskaperna bygger på egna erfarenheter och diskurser med andra angripare. Att skaffa dessa erfarenheter förutsätter både nyfikenhet och kreativitet eftersom information om systemens uppbyggnad är väl skyddad. Författarna beskriver processen för att attackera med fem typer av mönster för förklaring, inlärning, förståelse, diskussioner och prediktion.

En annan studie av Stanard m.fl. (2004) beskriver hur angripare använder sina kunskaper om användbara strategier och verktyg för att förstå det sociotekniska system som de ska attackera. Förståelse av organisationen ger en uppfattning om förväntade nätverkstjänster, hur många som sköter nätverket och säkerhetsnivån. Med det underlaget identifieras sårbarheter i nätverk, anslutna datorer och installerade applikationer.

3 Litteratur om försvarare

Några exempel på försvarare är IT-säkerhetsexperter, systemadministratörer, intrångsanalytiker och insatsteam för att hantera intrång (*eng*. Computer Emergency Response Team, CERT). De är alla en del av de personalresurser som arbetar med att konfigurera och hantera tekniska skydd och informationssystem som säkerställer informationens tillgänglighet, integritet och sekretess. Många studier görs om hur dessa försvarare ska rekryteras, utbildas, tränas och organiseras samt vilka stödsystem de behöver för att arbeta effektivt.

Detta kapitel består av åtta avsnitt. De inledande avsnitten sammanfattar litteratur om arbetsuppgifter (avsnitt 3.1), personalförsörjning (avsnitt 3.2) och utbildning inom IT-säkerhet (avsnitt 3.3). Därefter följer fyra avsnitt som sammanfattar litteratur om själva IT-säkerhetsarbetet vad gäller situationsmedvetenhet för IT-säkerhetspersonal (avsnitt 3.4), intrångsdetektion (avsnitt 3.5), visualiseringar för IT-säkerhet (avsnitt 3.6) samt IT-säkerhetsverktygs användbarhet (avsnitt 3.7). Slutligen sammanfattas litteratur om spelteori som studerar interaktionen mellan angripare och försvarare (avsnitt 3.8).

3.1 IT-säkerhetsarbete

Det praktiska arbetet med konfiguration och drift av informationssystem görs av systemadministratörer i samråd med IT-säkerhetsexperter som även ansvarar för hela organisationens IT-säkerhet. Befintlig litteratur beskriver bl.a. typiska arbetsuppgifter, organisation, typiska misstag och hur IT-säkerhetsexperter ser på användares roll för IT-säkerhet.

Werlinger, Hawkey, Botta och Beznosov (2009) beskriver hur IT-säkerhetsexperters interaktion med övriga intressenter omfattar nio aktiviteter: säkerhetsanalyser, utformning av IT-tjänster, användares IT-säkerhetsproblem, IT-säkerhetskontroller, utbildning och träning, sårbarhetshantering, administration av tekniska skydd, incidenthantering och utformning av IT-säkerhetspolicy. Aktiviteterna omfattar både informellt samarbete utan någon tydligt definierad struktur, koordinerat samarbete med formella relationer samt nära samarbete med väldefinierade relationer och ett gemensamt mål. Författarna beskriver att interaktionen kompliceras av organisatoriska faktorer, att många intressenter är involverade och att samtidigt hantera flera relaterade säkerhetsaktiviteter. Organisatoriska faktorer kan vara verksamhetens säkerhetssyn och distributionen av IT-säkerhetsarbete. Intressenter kan även prioritera andra effektivitetsmål och ha bristande IT-säkerhetskultur. Författarna beskriver att komplex IT-säkerhet gör att intressenter inte följer säkerhetsprocedurer, kommunikationen brister och att sårbarheter kan uppstå. Dessutom integrerar befintliga säkerhetsverktyg sällan de kommunikationsmöjligheter som behövs för en bra interaktion.

Vidare kan IT-säkerhetsexperter antingen organiseras som en central stödresurs eller distribuerat för att vara närmare verksamheten. Båda sätten har för- nackdelar. Hawkey, Muldner och Beznosov (2008) beskriver att centralisering av IT-säkerhetsarbetet är gör att det blir effektivare och att en gemensam kontaktpunkt förenklar kommunikationen. Författarna poängterar också att en centraliserad IT-säkerhetsgrupp bara är rådgivande, vilket kan skapa problem om IT-enheterna hantera säkerheten på olika sätt.

Hawkey m.fl. (2008) beskriver vidare att fördelarna med ett distribuerat IT-säkerhetsarbete är att det är mer integrerat med utveckling och drift av IT-system. Efter att ha arbetat centrerat kunde IT-säkerhetsexperterna fortsätta arbeta som en sammanhängande enhet även i den distribuerade organisationen. Trots detta uppstår ändå skillnader i hur IT-säkerheten hanteras, vilket kan skapa problem. I ett distribuerat säkerhetsarbete är det också viktigt att tänka igenom rutiner för kommunikation och samordning. Botta, Muldner, Hawkey och Beznosov (2011) studerade indikatorer för förväntade åtgärder och normer som stöd när det är svårt att veta hur åtgärder påverkar andra personer. Vanliga

indikatorer som inte är explicit riktade till någon explicit mottagare kan vara översiktsbilder och rykten om tillförlitlighet hos tekniska system. Normer kan vara procedurer för informationsspridning och konsistenta IT-system. Författarna beskriver att vanliga problem är att veta vem som har nödvändiga specialistkunskaper och att skapa en ömsesidig förståelse.

Vidare gör systemadministratörer misstag precis som alla människor. Sommestad, Ekstedt, Holm och Afzal (2011) använder ett Bayesianskt nätverk för att beskriva sambandet mellan misstag vid driftsättning av industriella styrsystem och resulterande sårbarheter. Bayesianska nätverk beskriver hur kombinationer av förutsättningar ger sannolikheten för ett utfall. Det resulterande nätverket beskriver hur sex möjliga orsaker (t.ex. systemkomplexitet och bristande krav) ger upphov till fem misstag (t.ex. bristande implementering av systemtillgänglighet och konfiguration av programvara). Nätverket kan användas för att uppskatta sannolikheten för misstag. Den starkaste effekten är hur bristande krav gör att nätverksportar lämnas öppna i onödan.

Slutligen är utformningen av IT-säkerhetspolicy en viktig del av IT-säkerhetsexperters arbete. Problemet är att när IT-säkerhetsexperter utformar policyn saknas ofta tillräckliga kunskaper om verksamheten. Albrechtsen och Hovden (2009) beskriver hur IT-säkerhetsexperter i huvudsak ser användare som en säkerhetsrisk eftersom de varken prioriterar säkerhet eller inser konsekvenser av bristande säkerhet. Även om många IT-säkerhetsexperter pratar om hur viktiga användare är för säkerheten har de bara ytliga kunskaper om hur användare anser att IT-säkerheten påverkar deras prestation. Författarna beskriver vidare att användare istället ser sig som riskmedvetna och en outnyttjad resurs för säkerhetsarbete. Skillnaderna beror delvis på olika tolkningar av risk där användare fokuserar på konsekvenser medan IT-säkerhetsexperter fokuserar på sannolikheter. I kombination med begränsade kommunikation mellan grupperna uppstår en bristande förståelse av varandras synsätt. Konsekvensen av den bristande förståelsen är att IT-säkerhet sällan är anpassad för användares behov.

3.2 Rekrytering, urval och personlig utveckling

Det omfattande behovet av IT-säkerhet skapar ett stor behov av IT-säkerhetspersonal. Befintlig litteratur beskriver bl.a. rekryterings- och urvalsmetoder samt utformning av arbetsuppgifter för att behålla personal.

IT-säkerhetstävlingar är ett vanligt sätt att skapa intresse för IT-säkerhet där team av intresserade personer tävlar mot varandra i att attackera respektive försvara informationssystem. Bashir, Wee, Memon och Guo (2017) beskriver en studie om hur tävlingarna kan bli effektivare rekryteringsverktyg genom att utforma dem för att uppmuntra personlighetsegenskaper som krävs för framtida tjänster. Mätningar gjordes av deltagarnas personlighet, yrkesintressen, kulturellt intresse, beslutsstil och anknytningsstil i tävlingen *Cybersecurity Awareness Week*. Faktorer som har ett positivt samband med intresset av att söka tjänster inom IT-säkerhet var undersökande intressen, rationell beslutsstil och hög tillit till den egna förmågan. Kommande rekryteringstävlingar kan uppmuntra dessa personlighetsegenskaper.

Eftersom antalet personer från ingenjörs- och datorutbildningar inte är tillräckligt för att täcka behovet studeras generella urvalskriterier oavsett bakgrund. Morris och Waage (2015) beskriver några nuvarande ansatser för urval där:

- *Cyber Aptitude and Talent Assessment* (CATA) utgår från att kraven för tjänster inom IT-säkerhet kan beskrivas med två dimensioner. Den ena dimensionen beskriver om uppgifter utförs i realtid eller om de kräver eftertänksamhet och är uttömmande. Den andra dimensionen beskriver om uppgifter kräver reaktiva åtgärder eller om de kräver proaktiva förbyggande åtgärder. Eftertänksamhet förutsätter till exempel kritisk tänkande och att inte förvänta sig omedelbara resultat. För att identifiera specifika färdigheter för IT-säkerhetspersonal beskriver

Saner m.fl. (2016) hur man utarbetat 43 frågor för intervjuer med verksamma operatörer. Frågorna handlar om operatörernas bakgrund, arbetet i sig och specifika uppgifter.

- *Information/Communication Technology Literacy* (ICTL) fokuserar på förmågor som verbala, icke-verbala och matematiska resonemang, problemidentifiering, kreativitet, skriftlig och muntlig förståelse samt perception (Trippe m.fl., 2015).
- *Cyber Talent Targeting Methodology* (CTI) fokuserar på att söka upp och identifiera intressanta personer som sedan deltar i en femdagarskurs. Kursen omfattar psykologiska tester, problemlösning, tävlingar, intervjuer med psykologer och IT-säkerhetsexperter samt en granskningsnämnd som slutligen godkänner lämpliga kandidater (Morris och Waage, 2015).

Morris och Waage (2015) beskriver att enbart ICTL har används i en större omfattning. ICTL är en bra prediktor av godkänt deltagande och slutbetyg för personal i kryptoutbildningar. Författarna bedömer att på längre sikt är CATA det bästa urvalsverktyget. Inga mer fullständiga utvärderingar av urvalsverktyg för IT-säkerhetspersonal identifierades i litteraturöversikten.

Det har konstaterats att repetitiva övervakningsuppgifter där säkerhetsrestriktioner förvårar möjligheten att påverka arbetet gör att många analytiker i IT-säkerhetscenter fort blir utbrända. Risken för utbrändhet kan ge en hög personalomsättning och en vanlig anställningstid för en analytiker är bara 1-3 år. För att identifiera vad som skapar utbrändhet och hög personalomsättning genomförde Sundaramurthy m.fl. (2015) en antropologisk studie av ett IT-säkerhetscenter där en datorstudent utbildades i antropologiska metoder och sedan anställdes som IT-säkerhetsanalytiker vid ett stort företag. Resultaten visar att utbrändheten orsakas av en olycklig interaktion mellan mänskligt kapital, automatisering av uppgifter, operativ effektivitet och ledningens effektivitetsmått. Det mänskliga kapitalet avser de intellektuella tillgångar som personalen utgör i form av kunskaper, färdigheter och erfarenheter. Författarna beskriver att ett ökat mänskligt kapital förutsätter en positiv cykel av färdigheter, rättigheter att utnyttja färdigheterna och utmanande arbetsuppgifter som i sin tur ger lärande och nya färdigheter. I IT-säkerhetscenter störs den här cykeln när oerfarna analytiker anställs för att spara pengar och eftersom de är oerfarna får begränsade rättigheter, vilket förhindrar fortsatt tillväxt. Författarna beskriver vidare att analytiker behöver möjlighet att reflektera över hur uppgifter kan automatiseras. Att bidra till bättre automation är en kreativ process i sig och ger mer tid för mer utmanande arbetsuppgifter. Bättre automation ger i sin tur ökad operativ effektivitet. Slutligen används effektivitetsmått för den interna utvecklingen, löneutvecklingen och i diskussioner med ledningen.

3.3 Utbildning och träning av IT-säkerhetspersonal

IT-säkerhetsarbete förutsätter precis som många tjänster en bra utbildning för att personalen ska prestera bra. Tyvärr saknas systematisk vetenskaplig forskning om hur utbildningen ska bedrivas. Många studier rapporterar enbart hur kurserna är uppbyggda och studenternas reaktioner. Enbart ett fåtal studier rapporterar någon detaljerad empiri av förvärvade kunskaper och hur de motsvarar behoven. Martini och Choo (2014) är ett av de bättre exemplen som beskriver hur kursinnehållet relaterar till brottsförebyggande teorier om avskräckning och färdigheter för IT-säkerhetspersonal. Avskräckning handlar om att öka upplevd ansträngning som krävs för brott, upplevda risker, minska möjliga resultat, minska faktorer som stimulerar brott och öka faktorer som stimulerar korrekt beteende (Cornish & Clarke, 2003). Martini och Choo (2014) beskriver hur 16 av de 31 kompetensområden som utarbetats i USA:s satsning på cyberutbildning relaterar till brottsförebyggande åtgärder (Newhouse, Keith, Scribner, & Witte, 2016).

Ben-Asher och Gonzalez (2015b) beskriver en studie av hur omfattningen på återmatning påverkar intrångsdetektion. Deltagarna fick antingen detaljerad återmatning om exakt

vilka händelser som var otillbörliga så att de kunde se var de valde rätt och fel eller en summarisk återmatning som enbart sammanfattade prestationen. Resultaten visar att med detaljerad återmatning förbättras deltagarnas prestation under hela träningsfasen och de presterar till slut nästan dubbelt så bra som deltagare med summarisk återmatning. Träning med detaljerad återmatning gjorde även att deltagarna presterade bättre på nya scenarier som inte ingick i träningen. Även studier med professionella logganalytiker har gett liknande resultat (Lif m.fl., 2016).

Precis som för rekrytering av IT-säkerhetspersonal är det vanligt att träning för intrångsdetektion görs vid övningar där team försöker attackera respektive försvara något informationssystem. Branlat, Morison och Woods (2011) beskriver en sådan övning och ger en inblick i teamens arbetsprocesser. Författarna beskriver hur en attack handlar om att successivt samla in information och utnyttja sårbarheter för att komma åt datornätverk och system. Attacken genomförs genom att delvis oplanerat pröva olika alternativ utan att egentligen veta vad som är det bästa alternativet. Det är även svårt att balansera strategisk planering och taktiska utmaningar samt att göra avvägningar mellan effektiva åtgärder och risken att avslöjas. När försvararna medvetet eller omedvetet stör attacken försöker angriparna rädda så mycket som möjligt, men sådana reaktiva åtgärder löper större risk att upptäckas av försvararna. Författarna beskriver vidare att för försvararna i sin tur handlar det om att bedöma vilka aktiviteter som är legitima. Det här kan vara svårt att göra på grund av stora datamängder, tvetydigheter om vad som är legitima aktiviteter, ofullständig information om angriparnas åtgärder, många informationskällor och att situationen hela tiden utvecklas. Eventuella åtgärder får inte heller störa det egna nätverket. Eftersom försvararna dessutom aktivt skannar nätverket för att hitta sårbarheter försvåras möjligheten att upptäcka angriparnas avsökningar. Svårigheten är framförallt att förstå angriparnas avsikt.

För bra teamprestation vid intrångsdetektion räcker det inte med enbart tekniska kunskaper utan det är också viktigt att teammedlemmarna arbetar på ett bra sätt tillsammans. Jariwala, Champion, Rajivan och Cooke (2012) beskriver att bra prestation förutsätter bra organisation, kommunikation och ledarskap. Det team som presterade bättre hade tre ledare som delade ledarskapet. Teamet hade även en bra uppfattning av varandras kunskaper och kunde kontinuerligt omfördela uppgifter under övningen. Deras kommunikation var öppen och de hittade sätt att uppdatera varandra om pågående uppgifter samt att fråga efter och ge hjälp när det behövdes. Författarna beskriver att det team som presterade sämre hade samma bakgrund och sammansättning, men bara en teammedlem fungerade som ledare och blev ofta överbelastad. De andra mer erfarna teammedlemmarna var mer intresserade av att arbeta med sina egna uppgifter.

3.4 Situationsmedvetenhet inom IT-säkerhet

Situationsmedvetenhet för IT-säkerhet handlar om att personal och beslutsfattare på alla nivåer både ska ha tillräcklig information och förståelse av situationen för att kunna fatta välavvägda beslut. En vanlig definition av situationsmedvetenhet är att den består av tre nivåer för att uppfatta information om omvärlden, förståelse av vad informationen innebär och att förutse kommande händelser (Endsley, 1995). Bredden på området gör att situationsmedvetenhet för IT-säkerhet bl.a. handlar om identifiering av misstänkta beteenden i nätverkstrafik, informationsfusion som korrelerar flera källor, visualiseringar som förenklar informationsinhämtning, kognitiva processer för att skapa förståelse och policydokument för att öka medvetenheten om IT-säkerhet.

Franke och Brynielsson (2014) beskriver en litteraturöversikt inom situationsmedvetenhet för IT-säkerhet. Författarna sammanfattar 102 artiklar inom situationsmedvetenhet för specifika tillämpningar som industriella reglersystem, krishantering, militära system och nationell säkerhet, verktyg som tekniska system och informationsfusion, visualiseringar, människa-dator interaktion, IT-säkerhetsövningar och informationsutbyte om IT-

säkerhetshot. Författarna beskriver att det finns många förslag på lösningar, men bara ett fåtal har utvärderats systematiskt.

För empiriska utvärderingar av situationsmedvetenhet för IT-säkerhet behövs mer studier av exakt vad personalen behöver vara medveten om för att prestera bra. Ett exempel på en sådan studie är Mahoney m.fl. (2010) som beskriver en kognitiv uppgiftsanalys för att identifiera information som nätverksadministratörer behöver för övervakning av datornätverk. Analysen genomfördes med en nätverksadministratör och använde fem scenarier som handlar om manipulerad information eller överbelastning av systemet. Resultaten visar att nätverksadministratörers situationsmedvetenhet för nätverks-övervakning omfattar systemets övergripande hälsoläge, misstänkta aktiviteter samt beroenden mellan systemkomponenter. Dessutom behöver nätverksadministratörer även situationsmedvetenhet om säkerheten för lagrad information som förändringar, konsistens samt möjliga effekter av obehöriga förändringar av informationen.

3.5 Intrångsdetektion

Intrångsdetektion är en viktig funktion för att upptäcka om obehöriga personer försöker ta sig förbi tekniska skydd. Intrångsdetektion identifierar typiska misstänkta beteenden, men eftersom även behörig nätverkstrafik kan ha samma signatur måste en operatör bedöma vad som är faktiska intrångsförsök. Avsnittet börjar med att sammanfatta litteratur om mänsklig prestation och teamarbete för intrångsdetektion. Därefter beskrivs några experimentmiljöer för att studera intrångsdetektion.

3.5.1 Mänsklig prestation för intrångsdetektion

För att förstå hur experter utför sina uppgifter är det vanligt med studier som jämför experter och oerfarna personer. Ben-Asher och Gonzales (2015a) beskriver en sådan studie som jämför förmågan för IT-säkerhetsexperter och oerfarna personer att detektera intrång med hjälp av ett fiktivt system för intrångsdetektion. Resultaten visar att IT-säkerhetsexperterna var bättra på att identifiera otillbörliga händelser, stöld av konfidentiell information och loggning av lösenord. IT-säkerhetsexperterna var däremot inte bättre på att identifiera kapning av websida och blockering av websida. Överlag var det ingen skillnad mellan IT-säkerhetsexperternas och oerfarna personers förmåga att identifiera om händelsesekvenserna berodde på faktiska attacker. Författarna beskriver vidare att identifikationen av attacker i huvudsak beror på antalet obehöriga händelser som identifieras. IT-säkerhetsexperterna var även mindre benägna att identifiera en attack baserat på ett fåtal obehöriga händelser.

För att identifiera vilka otillbörliga händelser som är faktiska attacker behövs specifika kunskaper om datornätverket samt kunskaper om typiska attackmönster (Goodall, Lutters, & Komlodi, 2009). Den här kunskapen går för närvarande bara delvis att automatisera och därför måste larm från tekniska system för intrångsdetektion granskas av behörig personal. Det räcker inte att enbart använda alarm från system för intrångsdetektion. Sommestad och Hunstad (2013) beskriver att 57 procent av attackerna som systemadministratörer identifierar är korrekta, men bara 11 procent av attackerna som systemet identifierar är korrekta. Systemadministratörer var helt enkelt bra på att känna igen normal nätverkstrafik och typiska attackmönster. De attacker som systemadministratörerna missade berodde till stor del på höga larmfrekvenser eller att de blev missledda av högprioriterade larm.

3.5.2 Teamarbete för intrångsdetektion

Intrångsdetektion genomförs ofta av team där teammedlemmarna till största delen arbetar enskilt tills en incident inträffar. Chen m.fl. (2014) beskriver hur det individuella arbetet för upptäckt av incidenter förutsätter nyfikenhet, undersökande färdigheter samt att kunna skaffa och delge nya kunskaper. Teammedlemmarna behöver även en förmåga att snabbt kunna jämföra olika data, upptäcka mönster och att se när något är fel. Många incidenter

kan hanteras på egen hand, medan andra kräver hela teamets resurser och även samarbete med andra team inom till exempel juridik, interngranskning och rättsväsendet. Författarna beskriver att teammedlemmarna därför behöver kunna växla från individuellt arbete till teamarbete. Ett bra teamarbete förutsätter att teammedlemmarna har färdigheter inom informationsdelning och samarbete samt en vilja att arbeta tillsammans med andra. Dålig kommunikation i teamarbetet kan göra att dubbelarbete sker (Cooke, Champion, Rajivan, & Jariwala, 2014). Dålig kommunikation kan även göra att teammedlemmarna inte informerar varandra om pågående uppgifter utan i första hand fokuserar på den egna prestationen (Champion, Rajivan, Cooke, & Jariwala, 2012).

Cooke m.fl. (2014) beskriver att några orsaker till bristande teamsamarbete är organisatoriska strukturer, säkerhetsregler och otillräckliga system. Det är till exempel vanligt att organisationer har belöningar och karriärvägar som uppmuntrar individuellt arbete snarare än teamsamarbete. Dessutom är varken arbetsmiljö eller tekniska system utformade för teamsamarbete. Många analytiker väljs också för sina tekniska kunskaper snarare än förmågan till teamsamarbete. Rajivan m.fl. (2013) beskriver hur samarbetet kan förbättras genom att uppmuntra teammedlemmarna att arbeta som ett team och att bedöma prestationen på teamnivå. Åtgärderna gjorde att prestationen ökade.

Vidare beskriver Cooke m.fl. (2014) att det heller inte finns någon ensad syn på vilka roller som ska ingå i teamen, varken inom organisationer eller mellan olika organisationer. En orsak till det kan vara att tvärfunktionella team där alla har ett gemensamt ansvar för uppgiften presterar bättre än team med en fix rollfördelning (Mancuso, 2012).

3.5.3 Experimentmiljöer för intrångsdetektion

Eftersom det kan svårt att på ett kontrollerat sätt studera operatörers bedömningar för intrångsdetektion i en operativ miljö utvecklas laboratorieuppgifter med liknande krav. Experimentmiljöerna utvecklas både av forskningsinstitut och på universitet.

Funke m.fl. (2016) beskriver experimentmiljön Air Force Cyber Intruder Alert Testbed (CIAT) som har utvecklats för att studera intrångsdetektion. CIAT simulerar övervakning av ett datornätverk och omfattar system för intrångsdetektion, signaturdatabas, insamling av datapaket och nätverkslista. System för intrångsdetektion genererar ofta många falsklarm, vilket ger en hög arbetsbelastning för att identifiera faktiska intrång. Analysen för att identifiera faktiska intrång görs i tre steg. Den första operatören ska på några minuter avgöra om fortsatta analyser behövs. Den andra operatören ska avgöra om något intrång förmodligen har inträffat genom att kombinera flera informationskällor. Slutligen analyserar den tredje operatören vad som faktiskt hände. Författarna beskriver att många nätverksanalytiker upplever hög stress och arbetsbelastning. En simulering med *Improved Performance Research Integration Tool* (IMPRINT) användes för att hitta lämpliga alarmfrekvenser och andel allvarliga alarm. IMPRINT är ett modelleringsverktyg för att predicera och utvärdera mänsklig prestation och arbetsbelastning i operativa miljöer. Försökspersonernas prestation och mentala arbetsbelastning motsvarade i stort simuleringen. Ökad alarmfrekvens och högre alarmnivåer gör att operatören för eller senare når en gräns och blir överbelastad. När operatören blir överbelastad minskar förmågan att identifiera intrång drastiskt.

Mancuso, Minotra, Giacobe, McNeese och Tyworth (2012) beskriver simulatormiljön idsNETS som har utvecklats för att studera intrångsdetektion. Simulatorn baseras på från data från *Visual Analytics Science and Technology* (VAST) 2011 och använder faktisk nätverkstrafik. Simulatorn består av (1) händelser som kan inträffa, (2) platser där händelser kan inträffa (t.ex. en arbetsstation, server eller brandvägg), (3) information från system för intrångsdetektion och loggar samt (4) resurser för möjliga åtgärder och resurser för kategorisering av händelser. Visualiseringen i användargränssnittet visar platser och relativt antal intrångslarm, detaljinformation om möjliga intrång och ett fönster för att kategorisera och prioritera händelser. Prestationsmåttet kallas *Human-Performance Scoring Model* som beräknas beroende på om rätt åtgärder utförs i rätt tid.

För mer omfattande analyser av eventuella intrång behöver analytiker rådfråga och samarbeta närmare med varandra. Rajivan (2011) beskriver simulatorn CyberCog som utvecklats för att studera situationsmedvetenhet och teamsamarbete för intrångsdetektion. Simuleringen baseras på ett verkligt scenario och använder två bildskärmar som presenterar liknande information som operativa system. Den vänstra bildskärmen presenterar händelser som liknar ett system för intrångsdetektion, nätverksaktiviteter, händelser som operatören har klassificerat samt antingen en nätverkskarta, sårbarhetsanalys eller information om aktuella IT-hot beroende på operatörens roll. Den högra bildskärmen presenterar händelser som delas med andra teammedlemmar för gemensam analys och en åtgärdsplan. Teammedlemmarna får både gemensam och individuell träning inom IT-säkerhet. Genom att teammedlemmarna ansvarar för olika uppgifter måste de dela information, rådfråga varandra samt samarbeta om nya attacker som rapporteras som aktuella hot. Rajivan (2011) beskriver att i en pilotstudie med ett team identifierades 40 % av attackerna och 96 % av falsklarmen korrekt.

3.6 Visualiseringar för IT-säkerhet

Visualiseringar är användbara som komplement till andra verktyg för att ge IT-säkerhetspersonal en överblick av systemets status och för att rikta uppmärksamheten mot avvikande händelser. Några orsaker till att särskilda visualiseringar behövs för IT-säkerhet är bl.a. stora datamängder, tvetydiga tecken på obehörig trafik, avsaknad av konkret fysisk form och stort spann av data från övergripande övervakning till inspektion av enskilda datorpaket. Mycket av forskningen inom visualiseringar för IT-säkerhet tog fart i samband med att den årliga konferensserien *Visualization for Cyber Security* (VizSec) startade 2004.

Det ökande behovet av IT-säkerhet medför att många studier görs inom visualiseringar för IT-säkerhet. Det ökande intresset för visualiseringar inom IT-säkerhet är tydligt i de litteraturöversikter som publicerats. Några exempel på tidigare litteraturöversikter är Tamassia, Palazzi och Papamanthou (2009), Shiravi, Shiravi och Ghorbani (2012) samt Guimaraes, Freitas, Sadre, Tarouco och Granville (2016). Dessa litteraturöversikter klassificerar litteraturen på olika sätt. Tamassia m.fl. (2009) klassificerar litteraturen efter typiska arbetsuppgifter för systemadministratörer som intrångsdetektion, nätverksövervakning, policy för befogenheter och sårbarhetsanalys. Sharivi m.fl. (2012) är istället enbart inriktad på nätverkssäkerhet och klassificerar litteraturen enligt användningsområden som övervakning av servrar, inter och extern kommunikation samt intrångsdetektion. Slutligen kategoriserar Guimarães m.fl. (2016) visualiseringarna enligt *Network and Services Management Taxonomy* som beskriver de flesta arbetsuppgifter inom IT-administration.

IT-säkerhetspersonalens nätverksövervakning handlar framförallt om två uppgifter. Den ena uppgiften att med hjälp av system för intrångsdetektion upptäcka attacker innan de kommer förbi tekniska skydd. Den andra uppgiften är att identifiera obehörig nätverkstrafik som redan är inne i systemet. Tidigare litteraturöversikter beskriver flera visualiseringar för dessa uppgifter. Enbart ett fåtal förslag sammanfattas här som en illustration av typiska visualiseringar. Avsnittet sammanfattar först litteratur om visualiseringar för intrångsdetektion. Därefter sammanfattas litteratur om visualiseringar för övervakning av nätverkstrafik i systemet. Slutligen sammanfattas några erfarenheter för fortsatta studier av visualiseringar för IT-säkerhet.

3.6.1 Visualiseringar för intrångsdetektion

Befintliga verktyg för intrångsanalyser består ofta av textuella sökfunktioner där operatörer på ett flexibelt sätt kan pröva olika hypoteser. Många studier jämför hur textuell information och visualiseringar för intrångsdetektion påverkar analytikers prestation.

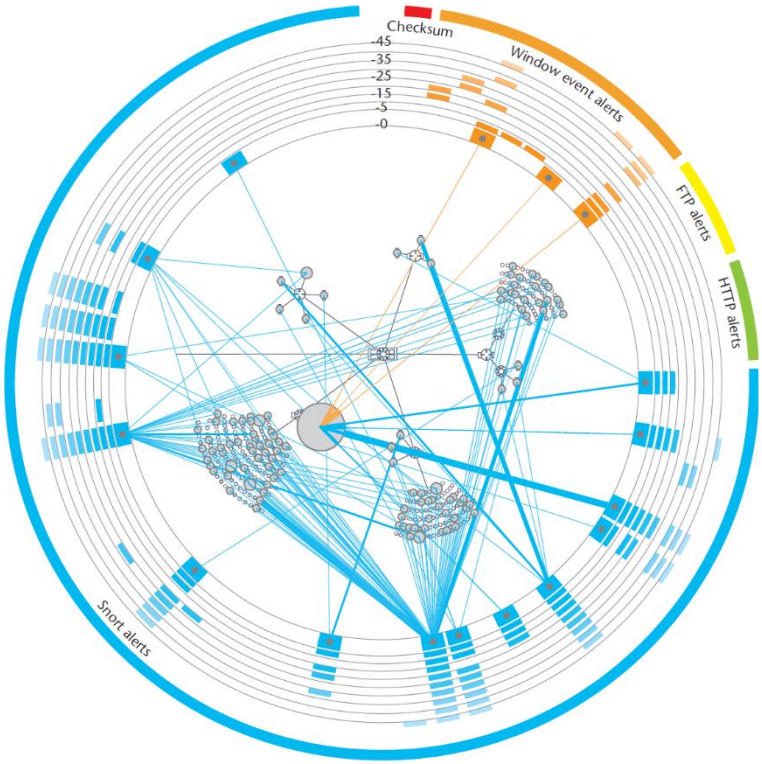
Thompson, Rantanen, Yurcik och Bailey (2007) beskriver en studie som använde visualiseringen VisflowConnect av Yin, Yurcik, Treaster, Li och Lakkaraju (2004). VisflowConnect visar nätverkstrafik för specifika IP-adresser, portar, intern nätverkstrafik samt in- och utgående nätverkstrafik. Resultaten visar att operatörer upptäcker lika många attacker med textuell information som med visualiseringen. Resultaten visar även att textuell information var bättre för att identifiera vilken specifik typ av attack som skedde eftersom kraftfulla sökfunktioner underlättar detaljanalyser. Försökspersonerna hade även högre konfidens för textuell information och föredrog den eftersom det var lättare att göra detaljanalyser. Författarna beskriver att fördelar med visualiseringen var att överblicken underlättar upptäckt av avvikelser från normal nätverkstrafik. Överblicken underlättar upptäckt av andra händelser som kan indikera obehörig aktivitet. Författarna anser att användargränssnitt för intrångsdetektion behöver kombinera båda presentationsformerna.

En liknande studie beskrivs av Giacobe (2013) som använde verktyget GeoViz av Hardisty & Robinson (2011) för att skapa en applikation med flera koordinerade visualiseringar. Informationen i GeoViz omfattar intrångsdetektion, brandväggsloggar och sårbarhetsskanning. Resultaten visar att visualiseringen ökade identifikationen av orsaken till incidenter med ca 28 %. Försökspersonerna upplevde att med visualiseringen behövde de dela uppmärksamheten mer, hantera mer information och var mindre familjära med informationen.

Enkla visualiseringar kan användas för att förenkla tolkning av resultaten från befintliga sökfunktioner. Hao, Healey och Hutchinson (2013) beskriver hur resultaten kan presenteras med cirkeldiagram för proportioner, stapeldiagram för jämförelser, punktdiagram för korrelationer och Gantt-scheman för värdeintervaller (t.ex. när larm inträffar för IP-adresser över tiden). Visualiseringarna väljs automatiskt beroende på vilken information som ska presenteras, men kan ändras av användaren. Genom att välja ut specifika delar för fortsatta analyser går det att genomföra hela analyssekvenser. Den underliggande textuella informationen presenteras enbart när den efterfrågas.

Specialiserade visualiseringar har också utvecklats för intrångsdetektion. Foresti, Agutter, Livnat, Moon och Erbacher (2006) beskriver en visualisering för intrångsdetektion. Figur 1 visar visualiseringen där en nätverksgraf i mitten omges av en cirkel med cirkelsegment som indikerar olika larm från intrångsdetektionssystem. En linje markerar vilka datorer som larmar. Bredden på linjen visar antalet återkommande larm och storleken på datorns cirkel i länkdiagrammet visar antalet typer av larm. Larmen från tidigare tidsperioder visas med ytterligare omgivande cirklar, men utan linjer för vilka datorer som var utsatta. På så sätt går det att se vad som är vilseledning och vilken dator som är det verkliga målet. Många typer av angrepp kan nämligen behövas för att få tillgång till känslig information.

Slutligen är det vanligt att intrångsdetektionssystem genererar många larm även för normal nätverkstrafik. De många larmen förvårar möjligheten att upptäcka faktiska intrång. Bertini, Hertzog och Lalanne (2007) beskriver visualiseringar för att underlätta konfigurering av system för intrångsdetektion. I översiktsbilden representeras tidsperioden som ska visualiseras med en spiral där de tidigaste larmen visas i mitten och de senaste längst ut. Vinkeln anger vilken timme larmen inträffar under dygnet, vilket underlättar identifiering av larm som återkommer samma tid på dygnet. Färgen indikerar typ av larm och storleken allvarlighetsgrad. Histogram visar antalet larm för varje typ av larm, allvarlighetsgrad och användarapplikationer. Alla användare och applikationer visas på varsin rad och linjer mellan raderna indikerar vilka applikationer som används av varje användare. Genom att interaktivt välja ut delar av larmen går det att se vilka situationer som orsakar problem.



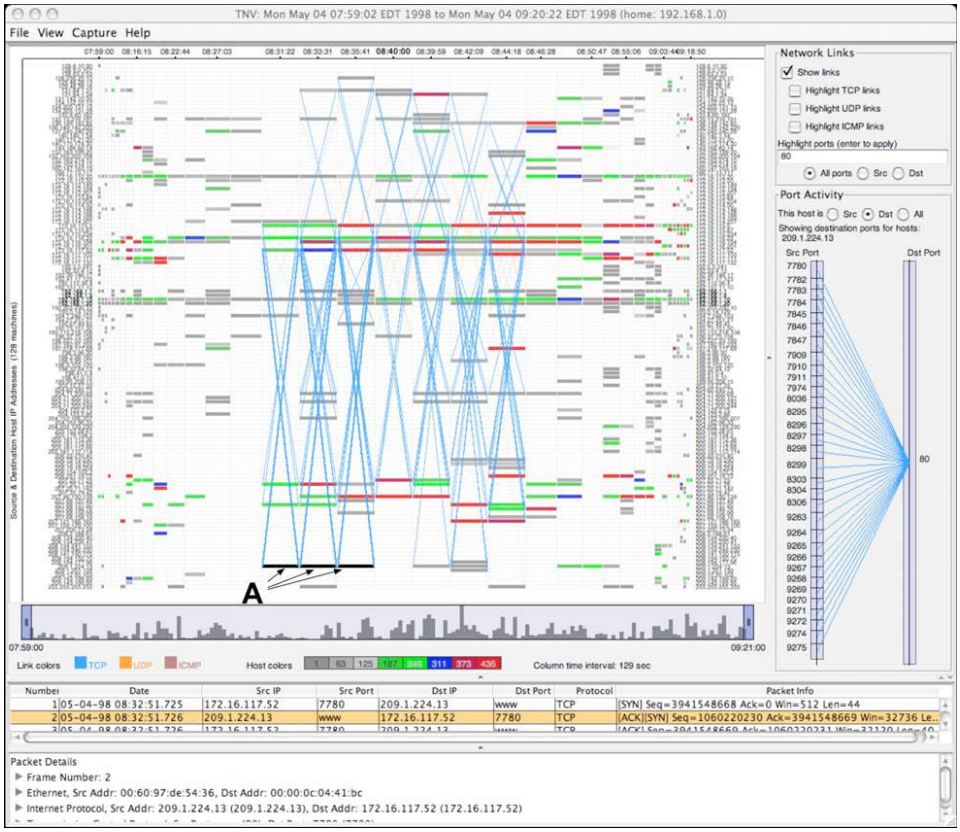
Figur 1. Visualisering för intrångsdetektion (Foresti m.fl., 2006).

3.6.2 Visualiseringar för nätverksövervakning

Nätverksövervakning av obehörig nätverkstrafik omfattar både övervakning av interna datornätverk och övervakning av kommunikation med externa datorer. Olika förutsättningar för intern och extern kommunikation gör att visualiseringar anpassas särskilt för dessa övervakningsuppgifter.

Kintzel, Fuchs och Mansmann (2011) beskriver en visualisering för övervakning av servrar i det interna nätverket. Trafikmängd eller relativa förändring av trafikmängd under det senaste dygnet visas som en cirkel med ett segment för varje timme. Färgen på segmentet indikerar trafikmängd eller förändring. Genom att cirkeln kan göras liten går det att övervaka många servar samtidigt i en matris där undernätverken visas på olika rader. Mer detaljerade visualiseringar visar trafiken för en vald server.

Time-based Network traffic Visualizer (TNV) är ett exempel på visualisering för övervakning av kommunikation mellan interna och externa datorer (Goodall, Lutters, Rheingans, & Komlodi, 2005). Figur 2 visar översiktspresentationen i TNV som består av en matris där raderna representerar IP-adresser och kolumnerna olika tidsintervall. Färgen på rutan indikerar trafikmängd för IP-adressen under tidsperioden. Interna IP-adresser visas med större och kraftigare textstorlek för att förenkla upptäckt av misstänkt extern kommunikation. Diagonala linjer indikerar kommunikation från sändande IP-adress till mottagande IP-adress under tidsperioden. De här linjerna bildar ett kryss när kommunikationen går fram och tillbaka, vilket är vanligast. Om bara en linje visas kan det tyda på avsökning efter aktiva portar. Färgen på linjerna indikerar vilket nätverksprotokoll som används. Tidsintervall i mitten av valt område har större utrymme för att göra det enklare att se detaljer samtidigt som överblicken bevaras.



Figur 2. Översiktspresentationen i *Time-based Network traffic Visualizer* (TNV) (Goodall m.fl., 2005).

Det finns även specialiserade visualiseringar för övervakning av kommunikation mellan interna och externa datorer. Bradshaw m.fl. (2012) beskriver visualiseringen *Flow Capacitor* som består av en virtuell kub. Den övre sidan av kuben representerar sändande IP-adresser och den undre sidan representerar mottagande IP-adresser. Punkter på ovan- och undersidan av kuben indikerar när det finns nätverkstrafik och färgen på punkten kodar både den sändande och den mottagande IP-adressen. Trafik från sändande till mottagande IP-adress visas med många korta linjesegment som rör sig från den övre till den nedre sidan. Segmentens visuella kodning ger ytterligare information om kommunikationen. Ringar mellan den övre och undre sidan används för att samla ihop flöden med liknande attribut som till exempel protokoll och portnummer.

Ett ytterligare exempel på visualisering för övervakning och intern och extern kommunikation är så kallade parallella koordinater. Parallella koordinater representerar dimensionerna som en serie av vertikala streck bredvid varandra och för varje informationspost dras ett streck mellan dimensionerna för att indikera attributvärden. Det här gör det lättare att se informationsposternas fördelning över dimensionerna och hur fördelningen varierar för posterna. Choi, Lee och Kim (2009) beskriver hur parallella koordinater kan användas för att identifiera olika typer av nätverksattacker. Dimensionerna var källadress, destinationsadress och destinationsport. Varje nätverkskommunikation indikeras med ett streck som förbinder dimensionerna. På så sätt går det att identifiera nio typer av attacker som till exempel *Denial of Service*, *Host Scan* och *Port Scan*.

Den finns även flera presentationstekniker för att presentera information på ett mer tillgängligt sätt än vanliga datorskärmar. Förstärkt verklighet (*eng*. Augmented Reality) är en sådan presentationsteknik där särskilda glasögon presenterar information inom synfältet. Användare kan med förstärkt verklighet utföra uppgifter obehindrat och samtidigt få olika typer av stöd. Beitzel m.fl. (2016) beskriver hur förstärkt verklighet kan hjälpa nätverksadministratörer att uppmärksamma när något misstänkt inträffar. Den

förstärkta verkligheten minskade den mentala arbetsbelastningen och förbättrade prestationen.

Slutligen kan så kallade intelligenta användargränssnitt användas för att delvis automatiskt presentera enbart den information som operatören behöver för den aktuella situationen. Intelligenta användargränssnitt använder modeller för att avgöra exakt vilken information som är mest relevant. Senanayake och Denker (2016) beskriver hur de utvecklar en sådan modell för IT-säkerhetspersonals interaktion. En semantisk interaktionsmodell tolkar vad användare gör och en semantisk visualiseringsmodell tolkar vad användare ser. Slutligen presenteras de samlade semantiska modellerna som indikerar hur mycket uppmärksamhet användare ägnar åt varje del. Författarna beskriver att deras fortsatta arbeta kommer använda modellerna för att filtrera relevant information och automatiskt fylla i dialogrutor.

3.6.3 Fortsatta studier av visualiseringar

Tyvärr har det trots omfattande utveckling av visualiseringar för IT-säkerhet visat sig att de i praktiken enbart används i begränsad omfattning. D'Amico, Buchanan, Kirkpatrick och Walczak (2016) beskriver en studie av förutsättningarna för att fortsatt utveckling av visualiseringar verkligen ska motsvara personalens informationsbehov. Studien fokuserade på de två första stegen av incidenthanteringen, övervakning och beslut om fortsatt analys samt preliminär analys och identifikation. Studien genomfördes genom att utvärdera hur 39 påståenden om IT-säkerhetsarbetet från tidigare studier överensstämmer med operatörers nuvarande arbete.

Resultaten från D'Amico m.fl. (2016) visar att påståendena fortfarande är relevanta. Operatörer analyserar stora informationsmängder som ofta är i alfanumeriskt format och försöker att besvara en serie analytiska frågor, vilket är kognitivt ansträngande. Några exempel på analytiska frågor är vad tillförligheten är för angivna IP-adresser, om nätverkstrafiken avviker från det förväntade, om utgående nätverkstrafik orsakas av en angripare, om någon IP-adress växlar mellan att vara klient och server samt vilka samband det finns med övriga händelser (D'Amico, Whitley, Tesone, O'Brien, & Roth, 2005). D'Amico m.fl. (2016) beskriver vidare att en del initiala beslut om fortsatt analys vid övervakning fattas på två minuter eller mindre. Författarna beskriver vidare att visualiseringar behöver kombinera information från flera källor, men information om tekniska och operativa effekter behövs först i senare delar av incidenthanteringen. Visualiseringar som bidrar till att förklara analysen för andra intressenter behövs däremot i alla faser. Författarna anser att befintliga visualiseringar ofta har en bristande integration i analysprocessen.

3.7 IT-säkerhetsverktygs användbarhet

För att IT-säkerhetspersonal ska prestera bra behöver de användbara verktyg, precis som alla andra användare. Tyvärr är det ofta svårt att empiriskt utvärdera verktygens användbarhet genom att studera hur de påverkar personalens prestation. Ett alternativ är istället att användbarhetsexperter utvärderar hur utformningen av verktygen överensstämmer med riktlinjer för användbara IT-system. Riktlinjer kan vara både generella och specifika för en viss tillämpning. Zhou, Blustein och Zincir-Heywood (2004) jämför egenutvecklade riktlinjer för system för intrångsdetektion med Nilsens generella riktlinjer (Nielsen & Molich, 1990). Deras riktlinjer omfattar presentation av systemstatus, konsistens, informationspresentation, navigering, flexibilitet och hjälpinformation. Resultaten visar att med deras specifika riktlinjer hittas fler problem och särskilt allvarliga problem än med Nilsens riktlinjer. Tyvärr beskriver författarna inte riktlinjernas exakta formulering.

Även Jaferian, Hawkey, Sotirakopoulos, Velez-Rojas och Beznosov (2014) jämför egenutvecklade riktlinjer som är särskilt anpassade för IT-säkerhetsarbete med Nilsens generella riktlinjer. De egenutvecklade riktlinjerna baserades på 164 riktlinjer från

befintlig litteratur om användbarhet för säkerhetsverktyg. Riktlinjerna sammanfattades med sju riktlinjer utifrån aktivitetsteori som är en övergripande teoribildning för hur aktörer använder objekt för att uppnå ett syfte. Riktlinjerna omfattar visualisering av status för aktiviteter, historik för åtgärder, flexibla informationspresentationer, presentation av regler och begränsningar, planering av arbetsfördelning, informationsdelning och verifiering av åtgärder. Även i den här studien visar resultaten att med de egenutvecklade riktlinjerna hittas fler allvarliga problem än med Nilsens heuristiker.

3.8 Spelet mellan angripare och försvarare

På en övergripande nivå kan interaktion mellan angripare och försvarare ses som ett så kallat icke-kooperativt spel. I det här spelet gör både angripare och försvarare ett antal val för att maximera sin vinst och samtidigt minimera kostnader. Många egenskaper hos angripare och försvarare abstraheras bort i den här typen av studier. Några av dessa studier av icke-kooperativa spel sammanfattas här gemensamt även om de kan användas för att studera många delar i incidenthanteringen.

Maqbool, Pammi och Dutt (2016) beskriver ett icke-kooperativt spel som studerade hur relationer mellan angripare och försvarares vinst påverkar deras beteende. Vinsten var antingen lika för angriparen och försvararen, mer vinst till angriparen eller mer vinst till försvararen. Angriparen kunde välja mellan att attackera och inte attackera och analytikern kunde välja mellan att försvara och inte försvara. Resultaten visar att proportionen attacker och försvar ökade när angriparen fick högre vinst. Eftersom det ökade försvaret inte är spelteoretiskt optimalt är förvararna överambitiösa när angriparen får en hög vinst vid en lyckad attack. Försvararnas överambition kan ge högre kostnader för försvar. Författarna beskriver att för att få rätt nivå av försvar är det viktigt att belöna bra prestation för upptäckt.

Dutt, Moisan och Gonzalez (2016) använde ett icke-kooperativt spel för att studera effekten av ett system för intrångsdetektion som inte var helt tillförlitligt. Möjliga åtgärder var att attackera eller inte attackera och att försvara eller inte försvara med lämpliga vinster och kostnader för varje kombination. Resultaten visar att försökspersonerna presterar spelteoretiskt optimalt utan systemet, men enbart försvararna ignorerade systemet när det hade 50 % tillförlitlighet. När systemet hade 10 % eller 90 % tillförlitlighet minskade antalet försvar, men inte tillräckligt enligt den spelteoretiska analysen. Från ett spelteoretiskt perspektiv är det troligt att försvararna i den här studien har för hög tillit till systemet för intrångsdetektion. Dessutom gjorde angriparna genomgående fler attacker än vad som var spelteoretiskt optimalt. Författarna beskriver att det precis om i den här studien kan vara bra att informera angripare om systemets prestation för att få mer information om deras beteende.

Det icke-kooperativa spelet mellan angripare och försvarare kan även kompletteras med mer detaljerade simuleringar av tekniska system. Canzani och Pickl (2016) beskriver en IT-säkerhetspolicy kan optimeras genom att använda ett simulerat strategiskt spel mellan angripare och försvarare för kritisk infrastruktur. En systemdynamisk modell av infrastruktur användes för att studera när man ska agera. Studien jämförde även effekten av proaktivt och reaktivt försvar. Resultaten visar att för det proaktiva försvaret är det mer effektivt att uppdatera systemet oftare än att investera i senaste tekniken för IT-säkerhet. För det reaktiva försvaret är det däremot bättre att ha så bra teknik som möjligt.

4 Litteratur om användare

Tekniska skydd är viktiga för att upptäcka och förhindra många typer av intrång. Tekniska skydd blir dessutom allt bättre, vilket får angripare att i ökande utsträckning fokusera på sårbarheter i användares tillgång till IT-system. Även användare har därför ett ansvar för att inte i onödan skapa sårbarheter i IT-säkerhet.

Användares tillgänglighet till IT-system regleras ofta med en IT-säkerhetspolicy som anger vad användare får och inte får göra. Ett problem är att det kan uppstå konflikter mellan verksamhetskrav och IT-säkerhetspolicyn som kan vara svåra att hantera för användare. Derbentseva, Fraser, Gibbon och Hawton (2015) beskriver hur sårbarheter kan uppstå vid användningen av lösenord, e-post, användarkonton, flyttbara lagringsmedia, privata enheter, sociala media, systemunderhåll, beteenden på Internet och sammanblandning av arbete och privatliv. Sårbarheter kan uppstå genom misstag, lurendrejeri, bristande förståelse av IT-säkerhetspolicyn eller medvetna brott mot policyn. Motiven för att bryta mot IT-säkerhetspolicyn kan vara produktivitetskrav, bristande motivation eller att risken inte upplevs så stor.

Detta kapitel består av sex avsnitt. De inledande avsnitten sammanfattar litteratur om faktorer som påverkar hur användare hanterar konflikter mellan säkerhetskrav och verksamhetskrav. Först sammanfattas litteratur om hur teoretiska modeller för mänskligt beteende förklarar användares respekt för IT-säkerhetspolicy (avsnitt 4.1). Därefter sammanfattas litteratur om träningsstrategier för att öka användares medvetenhet om IT-säkerhet och ge dem en bättre förståelse av IT-säkerhetspolicyn (avsnitt 4.2). Avsnittet därefter sammanfattar litteratur om hur den gemensamma synen på IT-säkerhet i form av IT-säkerhetskultur påverkar respekten för IT-säkerhetspolicyn (avsnitt 4.3). Därefter följer ett avsnitt som sammanfattar litteratur om för- och nackdelar med olika autentiseringstekniker (avsnitt 4.4).

De avslutande avsnitten sammanfattar litteratur om användares förmåga att upptäcka nätverksfiske (avsnitt 4.5) och interna IT-brott (avsnitt 4.6). Nätverksfiske är när e-post används för att lura användare att skapa sårbarheter eller uppge konfidentiell information. Vid interna IT-brott gör anställda medvetet intrång som skadar organisationen.

4.1 Respekt för IT-säkerhetspolicy

Användarnas respekt för IT-säkerhetspolicyn är delvis en avvägning mellan IT-säkerhetskrav och verksamhetskrav. Flera försök har gjorts att med sanktioner öka användarnas personliga kostnader för att bryta mot policyn. Enligt *General Deterrence Theory* (GDT) gör användare ett medvetet val om de ska bryta mot policyn eller inte. Om kostnaden för att bryta mot policyn upplevs tillräckligt hög är det mer rationellt att följa den (D'Arcy & Herath, 2011). Men formella sanktioner är bara en del av alla faktorer som påverkar beslutsfattande och effekten av sanktioner är väldigt varierande beroende på omständigheterna. D'Arcy och Devaraj (2012) beskriver till exempel hur policybeslut också påverkas av informella sanktioner som social acceptans och personlig moral. Personlig moral hade störst effekt på intentionerna att följa policyn. Totalt förklarar deras modell 47 % av variansen av intentionen att följa policyn. I en annan studie beskriver Hu, Xu, Dinev och Ling (2011) hur policybesluten påverkas mest av upplevda fördelar. Andra faktorer kan till exempel vara självkontroll och uppfattningen av den egna förmågan att kunna hantera IT-system (D'Arcy & Herath, 2011).

Sommestad, Hallberg, Lundholm och Bengtsson (2014) beskriver en meta-studie av totalt 61 faktorer som har studerats i litteraturen om vad som påverkar policybeslut. Faktorerna omfattar bl.a. personlighet, normer, riskuppfattning, säkerhetsmedvetenhet, organisatoriska faktorer och legitimitet. Faktorerna påverkar attityd, intention och beslut både vad gäller att respektera policyn och att missbruka IT-system. Författarna beskriver att överlag är personliga övertygelser och värden bättre prediktorer än objektiva faktorer

som belöning och formella risker. Teorimodeller med en överlag bättre prediktionsförmåga för policybeslut är *Theory of Planned Behavior*, *Protection Motivation Theory* och *Neutralization Theory*. Resten av avsnittet sammanfattar litteratur om hur dessa teorier förklarar användares respekt för IT-säkerhetspolicyn.

Theory of Planned Behavior (TBP) beskriver hur beteenden föregås av intentioner som i sin tur påverkas av attityder, subjektiva normer och upplevd kontroll av beteendet (Ajzen, 1991). Vidare påverkas beteenden även av den faktiska kontrollen av beteenden. Sommestad och Hallberg (2013) analyserade flera studier av hur TBP beskriver respekten för IT-säkerhetspolicyn. Resultaten visar att TBP förklarar i genomsnitt 47 % av variansen av intentionen att respektera IT-säkerhetspolicyn. Resultatet är likvärdigt för hur TBP generellt sett förklarar variansen av intentioner.

Vidare använder många studier ofta bara delar av TBP och kombinerar den med andra faktorer som kan påverka policybeslut. Cox (2012) beskriver en av få studier som enbart omfattar TBP. Resultaten visar att TBP förklarar 71 % av variansen av intentionen och 25 % av variansen av beteenden att respektera policyn. Resultaten visar att subjektiva normer påverkar intentionen mest. Överlag har däremot attityder, subjektiva normer och upplevd kontroll av beteende ungefär samma betydelse för intentionen att respektera policyn (D'Arcy & Herath, 2011).

Protection Motivation Theory (PMT) beskriver hur användares motivation att skydda sig mot hot påverkas både av hur hotfullt de upplevs och möjligheten att hantera dem (Maddux & Rogers, 1983). Högre hotvärdering och bättre möjlighet att hantera hot ger ökad motivation att faktiskt skydda sig. Värderingen av hot påverkas av hur allvarligt det är, sårbarhet mot hotet om ingenting görs och belöning för att inte hantera hotet. Värderingen av möjligheten att hantera hotet påverkas av hur effektiva möjliga åtgärder är samt egen förmåga och kostnad för att utföra åtgärder. Sommestad, Hallberg, Lundholm och Bengtsson (2014) analyserade flera studier av hur PMT beskriver respekten för IT-säkerhetspolicyn. Resultaten visar PMT förklarar i genomsnitt 42 % av variansen i motivationen att respektera IT-säkerhetspolicyn. PMT förklarar också mer av variansen för frivilliga än obligatoriska säkerhetsbeteenden samt om hoten är personliga och möjligheten att hantera hoten är konkreta och specifika. Överlag påverkas motivationen mer av möjligheten att hantera hoten än av hotvärderingen. Även Bauer och Bernroider (2016) beskriver en studie av hur PMT förklarar intentionen att respektera IT-säkerhetspolicyn. Resultaten visar att PMT förklarar 45 % av variansen i beteenden om respekt för IT-säkerhetspolicyn. Även i deras studie påverkas intentionen mest av den upplevda effekten och den egna förmågan att respektera policyn.

Eftersom både TBP och PMT överlag är bra på att förklara variansen i säkerhetsbeteende görs även studier som kombinerar modellerna. Till exempel beskriver Ifinedo (2012) hur modellerna tillsammans förklarar 70 % av variansen av intentionen av respektera IT-säkerhetspolicyn. Attityden var den enskilt viktigaste faktorn för intentionen, men de flesta faktorerna visade sig vara betydelsefulla förutom kostnaden för att utföra åtgärder. Ett ytterligare exempel är Yoon och Kim (2013) som beskriver hur modellerna tillsammans förklarar 61 % av variansen av intentionen av respektera IT-säkerhetspolicyn. Intentionen påverkas framförallt av attityden som beror på förmågan att hantera hotet och upplevd moralisk skyldighet som beror på subjektiva och organisatoriska normer.

Slutligen beskriver *Neutralization Theory* hur beteenden som inte respekterar regler och normer beror på att deras betydelse neutraliseras. Neutraliseringen görs genom olika tekniker som gör att reglerna inte längre upplevs relevanta för den enskilde personen. Vanliga tekniker är att förneka ansvar, förneka att beteenden får några negativa konsekvenser, skylla på att normerna är orättfärdiga, att hänvisa till övergripande lojalitetskrav samt att eventuella avsteg inte har någon betydelse i förhållande till alla tillfällen när normerna har respekterats. Siponen och Vance (2010) beskriver hur dessa tekniker i kombination med GDT förklarar 47 % av variansen av intentionen att respektera IT-säkerhetspolicyn. Neutraliseringsteknikerna hade störst betydelse för intentionen att respektera IT-säkerhetspolicyn.

4.2 Träning för IT-säkerhetsmedvetande

För att öka användares respekt för IT-säkerhetspolicyn genomför många organisationer särskilda utbildnings- och träningsprogram. Träningsprogrammen följer ofta modellen för övrig internkommunikation där en expert på uppdrag av högre ledning sprider information genom presentationer, e-post och intranätssidor. Många träningsprogram fokuserar också på möjliga sanktioner mot användare som inte respekterar IT-säkerhetspolicyn för att minimera oönskade beteenden. Tyvärr har den här typen av träningsprogram enbart begränsad effekt på användares respekt för IT-säkerhetspolicyn. Flera studier beskriver alternativa typer träningsstrategier som har bättre effekt.

Parsons, McCormac, Butavicius, Pattinson och Jerram (2014) beskriver en studie för hur kunskaper om och attityden till IT-säkerhetspolicyn påverkar respekten för policyn. Kunskaper, attityd och beteenden för policybeslut mättes för sju fokusområden. De sju fokusområdena var användning av Internet, email, sociala medier, lösenord, handburna enheter, incidentrapportering och informationshantering. Resultaten visar att kunskaper om IT-säkerhetspolicyn förklarar 66 % av variansen i attityder till policyn. Tillsammans förklarar kunskaper och attityder 78 % av variansen i beteenden. Träning för IT-säkerhetsmedvetande ska därför inte bara förmedla kunskaper om förväntade beteenden enligt IT-säkerhetspolicyn. Genom att förklara varför policyn är viktigt kan träningen förbättra attityden till policyn.

Vidare beskriver Puhakainen och Siponen (2010) en studie av träning för IT-säkerhetsmedvetande baserad på *Universal Constructive Instructional Theory* (UCIT) och *Elaboration Likelihood Model* (ELM). UCIT beskriver hur träningen utformas baserat på en tydlig formulering av uppgiften och användarnas kunskapsnivå. Träningen utformas utifrån hur kunskaper förvärvas, memoreras och används. ELM innebär att den personliga relevansen betonas eftersom det ökar motivationen att kognitivt reflektera över situationen. Den kognitiva reflektionen är viktig eftersom den har mer långtgående effekter än att enbart träna igenkänning och åtgärder för perceptuella indikatorer. Författarna beskriver hur träningen genomfördes med en instruktörsledd diskussion om användning av e-post, analys av e-post som deltagarna skickat och diskussion om möjliga konsekvenser av att konfidentiell information sprids. Resultaten visar att diskussionerna ledde till en mer användbar policy för e-post, mer e-post krypterades och en ökad medvetenhet om konsekvenser av att sprida konfidentiell information.

En ytterligare träningsstrategi är att genom gruppdiskussioner aktivt diskutera personliga erfarenheter och reflektera över IT-säkerhetsexperters kunskaper för att skapa gemensamma insikter om hur IT-säkerhet ska hanteras i verksamheten. Albrechtsen och Hovden (2010) beskriver en studie av gruppdiskussioner som stimulerar det kollektiva tänkandet och förmedlingen av kunskaper mellan användare och IT-säkerhetsexperter. Gruppdiskussionerna genomförs i en workshop med ett begränsat antal användare. Vid diskussionerna användes sju scenarier för hur användarna såg på hantering av ID-kort, låsning av datorer när de inte används, delning av lösenord, spridning av personlig information, användning av privat e-post och åtgärder vid nödsituationer. Resultaten visar att träningen förbättrar säkerhetsmedvetandet i form av eget ansvar, motivation, avvägningen mellan IT-säkerhet och funktionalitet samt betydelsen av IT-säkerhetspolicyn. Träningen ökar även IT-säkerhetsbeteenden som att låsa datorer, hanteringen av ID-kort och manuella viruskontroller.

Slutligen kan träning av IT-säkerhetsmedvetande genomföras genom att till viss del efterlikna arbetsmiljön där bedömningar av IT-säkerhet görs för att få en bättre förståelse av hur man ska agera. Molchanova och Borilin (2016) beskriver träningsmiljön *Kaspersky Interactive Protection Simulation* (KIPS). KIPS förbättrar kommunikation mellan användare och IT-säkerhetsexperter om avvägningen mellan risk och verksamhetskrav. Målet med träningen är att skapa positiva förebilder för hur man ska agera istället för att ge negativ bestraffning. Författarna beskriver att träningen överlag ger en bättre förståelse av sårbarheter och reder ut vanliga missförstånd som att enskilda angripare försöker

komma åt informationen. Flest angrepp görs vanligtvis av organiserad brottslighet. Enligt författarna dubblerar träningen användningen av IT-säkerhetskunskaper i det dagliga arbetet.

4.3 Effekter av IT-säkerhetskultur

Användares respekt för IT-säkerhetspolicyn påverkas även av det organisatoriska sammanhanget för hur chefer och medarbetare ser på IT-säkerhetens betydelse för verksamheten. Organisationens syn på IT-säkerheten kan beskrivas med organisationens IT-säkerhetskultur för de gemensamma attityder, mentala modeller och aktiviteter som formas över tiden (Karlsson, Åström, & Karlsson, 2015). Eftersom IT-säkerhetspolicyn aldrig kan beskriva exakt vad som ska göras i alla upptänkliga situationer är IT-säkerhetskultur särskilt viktigt för riskbedömningar som inte tydligt regleras av IT-säkerhetspolicyn.

Parsons m.fl. (2015) beskriver en studie av sambandet mellan IT-säkerhetskultur och användares respekt för IT-säkerhetspolicyn. IT-säkerhetskultur omfattar bl.a. prioritering av deadlines och upplevelse av medarbetares beteende. Policybeslut beskrivs med modellen *Knowledge, Attitude, Behavior* (KAB). KAB beskriver hur ökade kunskaper förbättrar attityden som i sin tur i kombination med ökade kunskaper ger färre riskfyllda beteenden (Kruger & Kearney, 2006). Resultaten visar ett starkt samband mellan IT-säkerhetskultur och kunskaper, attityder och beteende som respekterar IT-säkerhetspolicyn. Vidare jämfördes betydelsen av sanktioner mot att inte respektera och belöningar för att respektera IT-säkerhetspolicyn. Resultaten visar att mer sanktioner ger ökade kunskaper om IT-säkerhetspolicyn, men inte nödvändigtvis mindre riskfyllt beteende.

Vidare beskriver Alnatheer, Chan och Nelson (2012) en studie av hur IT-säkerhetskultur påverkar användares IT-säkerhetsmedvetande och det egna IT-säkerhetsansvaret. IT-säkerhetskultur påverkas i sin tur av hur ledningen prioriterar och är involverade i säkerhetsarbetet, användningen av sanktioner mot att inte respektera policyn samt hur användare utbildas och tränas i IT-säkerhet. Resultaten visar att ökad ledning, sanktioner och utbildning förbättrar IT-säkerhetskulturen som i sin tur ökar de anställdas IT-säkerhetsmedvetande och eget ansvar. Totalt förklarar modellen 43 % av variansen i IT-säkerhetskultur.

Slutligen beskriver Hu, Dinev, Hart och Cook (2012) en av få studier som knyter ihop hela kedjan från ledningens stöd för IT-säkerhet, effekter på IT-säkerhetskultur och hur de tillsammans påverkar attityder och normer för intentionen att respektera policyn. Ledningens stöd för IT-säkerhet gör att den får högre legitimitet samt ökar personalens engagemang och möjligheter att påverka dess utformning. IT-säkerhetskultur beskriver i sin tur individens ansvar för IT-säkerhet och betoningen av att respektera befintliga regler och procedurer. Resultaten visar att ledningens stöd för IT-säkerhet har en markant effekt på både individens ansvar och respekten för regler. En förbättrad IT-säkerhetskultur förbättrar därefter attityder, normer och upplevd kontroll av beteendet enligt TBP, vilket ökar intentionen att respektera IT-säkerhetspolicyn. Totalt förklarar modellen 55 % av variansen av intentionen att respektera IT-säkerhetspolicyn.

4.4 Autentiseringsteknikers användbarhet

Ett exempel på studier av konflikten mellan IT-säkerhetskrav och verksamhetskrav är typiska krav i IT-säkerhetspolicyn på användares lösenord. Sasse, Brostoff och Weirich (2001) beskriver hur policyn för lösenord kan kräva att användare har starka lösenord, olika lösenord för varje system som används och att lösenorden byts ofta. De flesta människor har svårt att leva upp till de kraven eftersom kryptiska lösenord visserligen är starka, men samtidigt svåra att komma ihåg. Det är även lätt att blanda ihop lösenord, särskilt när de byts ofta. Författarna beskriver hur många användare hanterar den här typen

av krav genom att skriva upp lösenord, återanvända lösenord eller använda lösenord som är lätta att komma ihåg, men samtidigt mindre säkra. Den här typen av beteenden ökar sårbarheten i autentisering med lösenord.

Hur stora problemen är för användare beror delvis på deras attityd. Choong och Theofanos (2015) beskriver hur användare med en positiv attityd till policykraven upplever mindre svårigheter med långa och komplexa lösenord, mindre svårigheter med att skapa och minnas lösenord samt inser betydelsen av ett bra skydd. Till exempel anser 53 % av deltagarna som tycker att lösenorden är för långa och komplexa att ett intrång inte får några konsekvenser. Däremot anser enbart 32 % av deltagarna som tycker att lösenordslängden och komplexiteten är ungefär rätt att ett intrång inte får några konsekvenser.

Tyvärr finns det ännu inget sätt att helt undvika användbarhetsbrister med alfanumeriska lösenord, men flera tekniker kan minska problemen. Ett sätt är så kallade mnemoniska lösenord där användaren utgår från en fras som användaren minns väl. Frasen kodas sedan till ett lösenord genom att den första bokstaven i orden kombineras med siffror och symboler. Tyvärr har många användare problem även med mnemoniska lösenord. McEvoy och Still (2016) beskriver en studie där lösenorden innehöll kontextuella ledtrådar. Deltagarna valde själva den kontextuella ledtråden som kunde läggas in var som helst i lösenordet. Resultaten visar att den kontextuella ledtråden ökade förmågan att komma ihåg lösenorden från 20 % till 65 %.

Ett ytterligare sätt att förenkla alfanumeriska lösenord för användaren är att gruppera liknande tecken tillsammans. Greene (2015) beskriver en studie av så kallade permuterade lösenord där stora bokstäver kommer först följt av små bokstäver, siffror och symboler. Permutationen minskar säkerheten, men om lösenorden samtidigt ökar andra beteenden som förbättrar säkerheten kan säkerheten i sin helhet förbättras. Resultaten visar att deltagarna upplever att permuterade lösenord med 14 tecken är enklare att använda än vanliga komplexa lösenord med 10 tecken. De permuterade lösenorden upplevdes enklare på både persondatorer och mobila enheter. Resultaten är framförallt intressanta för systemgenererade lösenord eftersom många användare redan grupperar liknande tecken för att komma ihåg lösenord bättre.

Slutligen ökar användningen av mobila enheter, vilket gör att autentisering på den här typen av enheter blir allt viktigare. Eftersom det är svårare att skriva in alfanumeriska lösenord på mobila enheter studeras andra typer av autentisering. Ett alternativ är grafiska lösenord där användaren sveper fingret över ett valt mönster. Cain, Chiu, Santiago och Still (2016) beskriver en studie av hur sårbara grafiska lösenorden är för en angripare som tittar över axeln på användar. Mobila enheter används ofta i publika miljöer, vilket gör dem extra sårbara för den här typen av attacker. Resultaten visar att grafiska lösenord blir mer såbara om svepen görs horisontellt och vertikalt samt om visuell återmatning används för att indikera när positioner registreras. Symmetriska lösenord där till exempel vänster och höger sida av svepen formar spegelbilder av varandra var däremot mindre sårbara eftersom svepen sker snabbare. Författarnas rekommendation är att stänga av visuell återmatning för grafiska lösenord och använda lösenord som består av diagonala svep.

4.5 Upptäckt av nätverksfiske

Ett vanligt IT-hot som involverar användare är så kallat nätverksfiske. Nätverksfiske innebär att försåtlig e-post lurar användare att klicka på länkar och bilagor som gör att skadlig programvara installeras eller att konfidentiell information sprids. Ferreira, Coventry och Lenzini (2015) beskriver hur nätverksfiske kan ses som en form av bedrägeri genom övertalning. Deras modell integrerar tre taxonomier för övertalning i form av principer för påverkan, psykologiska triggers och bedrägeri. Taxonomierna omfattar fem principer för auktoritet, övertalning, igenkänning, åtaganden och distraktion. Resultaten visar att den vanligaste principen för nätverksfiske var att försöka skapa igenkänning hos användare. Författarna beskriver också att vissa principer kombineras

beroende på bedragarens avsikter. För till exempel stöld av konfidentiell information är det vanligt att igenkänning kombineras med distraktion och referens till en auktoritet.

Canfield, Fischhoff och Davis (2016) beskriver en studie av hur användares upptäckt och hantering av nätverksfiske kan analyseras med signaldetektionsteori (SDT). SDT används ofta för att beskriva förmågan att detektera när en signal uppkommer i en normal bakgrund av aktivitet. Svårigheten att korrekt detektera signaler gör att de ibland missas och ibland att normal aktivitet identifieras som en signal. SDT tar även hänsyn till den upplevda kostnaden för dessa misstag och hur det påverkar identifieringen av signaler. Resultaten visar att även när deltagarna informerades om nätverksfiske och var vaksamma hade de enbart begränsad förmåga att upptäcka nätverksfiske. I kombination med deltagarnas tendens att inte klicka på länkar gav det 61 % falsklarm och 28 % missade upptäckter av nätverksfisken. Resultaten visar även att det fanns ett positivt samband mellan deltagarnas förmåga att upptäcka nätverksfiske och deras konfidens. Däremot fanns det inget samband mellan deltagarnas förmåga att upptäcka nätverksfiske och hur allvarligt de uppfattade konsekvenserna av nätverksfiske. Författarna beskriver även att det är stora individuella variationer i förmågan att upptäcka nätverksfiske. Det är därför viktigt att veta om sårbarheten påverkas mest av den sämsta, bästa eller genomsnittet av användare.

Genom att utforma försåtlig e-post som liknar vanligt e-post uppmuntrar nätverksfiske till att använda inlärda heuristiker för hur e-posten ska hanteras. Det gör att användare inte upptäcker nätverksfiske lika bra som när de använder en mer utförlig och medveten granskning. Vishwanath, Herath, Chen, Wang och Rao (2011) beskriver till exempel hur hanteringen av e-post beror på hur indikatorer uppmärksammas och granskas i förhållande till befintliga kunskaper. Resultaten visar att uppmärksammande av e-postens källa och grammatik ökar detektionen av nätverksfisket, medan uppmärksammande av e-postens angelägenhet och ämne minskar detektionen av nätverksfisket. Vidare ökar användarens engagemang detektionen av nätverksfisk. Användare som får mycket e-post har helt enkelt svårt att hantera den, vilket även minskar effekten av nätverksfiske. Författarna beskriver vidare att den medvetna granskningen av indikatorer enbart hade en mindre effekt på detektionen av nätverksfiske. Hanteringen av e-post bedöms nästan enbart på ytliga indikatorer och kunskaper som kan nyansera bedömningen används inte.

Flera studier görs även av hur personliga erfarenheter och egenskaper påverkar risken att bli offer för nätverksfiske. Ett exempel är Wright och Marett (2010) som beskriver hur datorvana, tidigare användning av Internet och kunskaper om IT-säkerhet minskar risken att bli offer för nätverksfiske. Tyvärr förklarar dessa faktorer enbart 36 % av variansen för vilka som blir offer. Flera andra faktorer påverkar därför beslutet att lita på försåtlig e-post.

4.6 Interna IT-brott

Bedrägerier mot den egna organisationen förekommer i många former. Interna IT-brott innebär att anställda och underleverantörer utnyttjar sina befogenheter och kunskaper om organisationen för att få tillgång till IT-system och orsaka skada utan att väcka misstankar. Nurse m.fl. (2014) beskriver en modell för interna IT-brott baserat på en analys av 179 rapporterade fall. Modellen omfattar personlighetsegenskaper, psykologiskt tillstånd, attityd till arbetet, motiv, färdigheter, beteenden och tillfällen att begå brott. En kombination av faktorer orsakar ofta någon form av stress redan innan attacken. En utlösande orsak som till exempel uppsägning, arbetskonflikter eller personliga problem gör sedan att organisationen attackeras. Författarna beskriver vidare att själva attacken genomförs i ett syfte. Attacken består av spaning, rekrytering av medbrottslingar, tillgång till och extraktion av data samt att dölja spåren.

Den här bilden av interna IT-brott bekräftas av Hugl (2015) som beskriver en litteraturöversikt där många attacker görs av tidigare anställda som har jobbat lång tid i organisationen. Även negativa värderingar och brist på sociala relationer påverkar risken att begå brott. Själva bedrägeriet är en kombination av rationalitet, tillfälle och någon

händelse som skapar ett tryck på personen. Författarna anser att bättre organisationskultur, ledarskap, kontrollstrukturer och analys av riskfaktorer kan minska antalet bedrägerier.

5 Diskussion

Litteraturöversikten beskriver hur attacker föregås av omfattande planering där angriparna använder sina tekniska kunskaper för att försöka utnyttja sårbarheter som försvararna inte förväntar sig (avsnitt 2). Angriparnas kunskaper bygger på både egna erfarenheter och diskurser med andra angripare. Planeringen görs i flera steg från sårbarheter på organisatorisk nivå till sårbarheter i nätverk, anslutna datorer och applikationer. Med mentala modeller försöker angriparna förutse möjliga effekter av åtgärder under attacken, hur de ska tolka resultaten av åtgärder och samt lämpliga efterföljande åtgärder. Eftersom angriparnas kunskap om informationssystemen trots planeringen är ofullständig och osäker prövar de ett antal alternativ för att få mer information om informationssystemen (avsnitt 3.3). Vad som är lämpliga åtgärder är en avvägning mellan risken att avslöjas och effektivitet för att få så mycket information som möjligt.

Försvar mot angripares attacker hanteras av flera specialister som till exempel IT-säkerhetsexperter, systemadministratörer, intrångsanalytiker och insatsteam (CERT) för att hantera intrång (avsnitt 3). Försvararnas uppgifter kan ha vitt skilda karaktärer från att utföra åtgärder i realtid till uppgifter som kräver reflektion och eftertanke. Uppgifterna kan även vara reaktiva eller proaktiva (avsnitt 3.2).

Litteraturöversikten beskriver hur IT-säkerhetsexperter ansvarar för hela organisationens IT-säkerhet (avsnitt 3.1). Tillsammans med andra intressenter gör IT-säkerhetsexperterna analyser och kontroller samt hanterar problem, sårbarheter och incidenter. Arbetet kompliceras av många intressenter med olika säkerhetssyn och många relationer mellan säkerhetsaktiviteter. IT-säkerhetsexperternas verktyg har sällan de kommunikationsmöjligheter som behövs för en bra interaktion. Användbara verktyg för IT-säkerhet bör omfatta visualisering av status för aktiviteter, historik för åtgärder, flexibla informationspresentationer, presentation av regler och begränsningar, planering av arbetsfördelning, informationsdelning och verifiering av åtgärder (avsnitt 3.7).

För att förhindra intrång används tekniska skydd som övervakas av försvarare (avsnitt 3.5). Analysen av möjliga intrång görs i tre steg (avsnitt 3.5.3). I det första steget beslutas om fortsatta analyser behövs. I det andra steget avgörs om något intrång förmodligen har inträffat genom att kombinera flera informationskällor. Slutligen i det tredje steget analyseras vad som faktiskt har inträffat. Det första stegen i intrångsanalysen kan ge hög stress och arbetsbelastning om tekniska skydd genererar många falsklarm. Det första stegen är även repetitiva och ger sällan analytikerna möjlighet att i någon större utsträckning använda sina kunskaper och färdigheter (avsnitt 3.2). Analytiker som enbart arbetar med dessa uppgifter riskerar att bli utbrända. Ett sätt att förbättra arbetsmiljön är att ge analytikerna mer tid att reflektera över vilka uppgifter som kan automatiseras. Det här är en kreativ process som ger mer tid för utmanande arbetsuppgifter. Bättre automation ökar även den operativa effektiviteten.

Nätverksanalytiker har omfattande tekniska kunskaper och premieras ofta för sin förmåga att upptäcka intrång. För många incidenter är det tillräckligt med en enskild analytikers förmåga, medan andra incidenter kräver att analytikerna arbetar tillsammans som ett team (avsnitt 3.3, 3.5.2 och 3.5.3). För omfattande incidenter behöver analytikerna kunna växla från individuellt arbete till teamarbete. Ett bra teamarbete förutsätter att teammedlemmarna har färdigheter inom informationsdelning och samarbete samt en vilja att arbeta tillsammans med andra. Bristande teamarbete kan göra att dubbelarbete sker och att den gemensamma prestationen försämras. Mer omfattande incidenter kan även försvåra teamkoordinationen. För mer omfattande incidenter kan ledarskapet behöva delas mellan flera teammedlemmar.

Nätverksanalys handlar till stor del om att bedöma vilka aktiviteter som är legitima (avsnitt 3.3). Den här bedömningen kan vara svår att göra på grund av stora datamängder, tvetydigheter om vad som är legitima aktiviteter, ofullständig information om angriparnas åtgärder, många informationskällor och att situationen hela tiden utvecklas. Åtgärder får

inte heller störa nätverket eller försvåra möjligheten att upptäcka angriparnas åtgärder. Det är framförallt svårt att förstå angriparnas avsikter. Analysen kräver både kunskaper om vad som är normal nätverkstrafik för det aktuella nätverket och kunskaper om typiska attackmönster (avsnitt 3.5.1). Det kan ta tid att bygga upp den här expertisen. Precis som inom många andra områden förbättras inlärningen med tydlig återmatning om attacker (avsnitt 3.3 och avsnitt 3.8). För att upptäcka intrång är det bland annat intressant att veta vilka datorer som larmar, hur många larm och larmtyper som tekniska skydd larmar för, förändringar över tiden och regelbundet återkommande larm (avsnitt 3.6.1). Attacker kan kombinera många typer av angrepp med vilseledning.

Nätverksanalysen görs ofta med hjälp av textuella sökverktyg där analytikerna på ett flexibelt sätt kan pröva olika hypoteser för att besvara en serie analytiska frågor (avsnitt 3.6.1 och avsnitt 3.6.3). Några exempel på analytiska frågor är vad tillförligheten är för angivna IP-adresser, om nätverkstrafiken avviker från det förväntade, om utgående nätverkstrafik orsakas av en angripare, om någon IP-adress växlar mellan att vara klient och server samt vilka samband det finns med övriga händelser. Enkla visualiseringar kan förenkla tolkningen av den alfanumeriska informationen (avsnitt 3.6.1). Visualiseringar kan även ge en överblick som gör det lättare att upptäcka oväntade avvikelser.

Den händer även att angripare tar sig in system utan att upptäckas. Nätverksadministratörer övervakar därför både interna datornätverk och kommunikationen mellan interna och externa datorer för att upptäcka obehörig nätverkstrafik (avsnitt 3.6.2). För övervakningen behöver nätverksadministratörer information om hur trafikmängden förändras, misstänkta aktiviteter baserat på till exempel kommunikationsmönster eller förändringar av information, systemets övergripande hälsoläge samt beroenden mellan systemkomponenter.

När tekniska skydd blir allt bättre fokuserar angripare i ökad utsträckning på sårbarheter i användares tillgång till IT-system (avsnitt 4). Sårbarheter kan uppstå vid användningen av lösenord, e-post, användarkonton, flyttbara lagringsmedia, privata enheter, sociala media, systemunderhåll, beteenden på Internet och sammanblandning av arbete och privatliv. Hur sårbarheterna ska minimeras beskrivs ofta i en IT-säkerhetspolicy som anger vad användare får och inte får göra. Om användare bryter mot policyn skapas ytterligare sårbarheter som angriparna kan utnyttja. Vanliga motiv för att bryta mot policyn kan vara produktivitetskrav, bristande motivation eller att risken inte upplevs så stor. Användare kan även uppleva att det är befogat att bryta mot IT-säkerhetspolicy när den inte är tillräckligt anpassad för verksamheten. Bristande anpassning av policyn beror delvis på att IT-säkerhetsexperter som utformar policyn ibland har enbart ytliga kunskaper om verksamheten (avsnitt 3.1).

Ledningens stöd för IT-säkerhet påverkar markant hur användarna ser på sitt eget ansvar för IT-säkerhet och respekten för regler och procedurer (avsnitt 4.3). Om ledningen prioriterar och är involverade i IT-säkerheten får den högre legitimitet, vilket ökar användarnas engagemang. Ledningen kan även stödja IT-säkerhet genom att ge användare möjlighet att påverka utformningen, ge användare utbildning och träning i IT-säkerhet samt införa sanktioner mot att inte respektera IT-säkerhetspolicyn. Om ledningen stödjer IT-säkerhet får organisationen en bättre IT-säkerhetskultur. IT-säkerhetskulturen påverkar i sin tur användares IT-säkerhetsmedvetande, kunskaper, attityder och beteende för hur IT-säkerhetspolicyn respekteras.

Många organisationer genomför särskilda utbildnings- och träningsprogram för att öka användares respekt för IT-säkerhetspolicyn (avsnitt 4.2). Förutom kunskaper behöver träningsprogrammen även ge användarna en bättre attityd till policyn genom att förklara varför den är viktig. Träningsprogrammen kan också genomföras som gruppdiskussionerna. Gruppdiskussioner ger gemensamma insikter om hur IT-säkerhet ska hanteras i verksamheten och större möjlighet att reflektera över IT-säkerhetsexperternas kunskaper. Träningsprogrammen och IT-säkerhetskulturen kan tillsammans påverka många faktorer som påverkar användarnas respekt för IT-säkerhetspolicyn. Några faktorer som kan påverkas är till exempel social acceptans och upplevda fördelar av att bryta mot

policyn, normer, attityder, värdering av hot och den egna förmågan att hantera hot (avsnitt 4.1). Andra faktorer som kan vara svårare att påverka men också har en effekt på respekten för IT-säkerhetspolicyn är personlig moral samt personliga värden och övertygelser. Att enbart öka sanktioner är sällan tillräckligt för att öka respekten för IT-säkerhetspolicyn.

Slutligen utsätts många användare för så kallat nätverksfiske (avsnitt 4.5). Nätverksfiske innebär att försåtlig e-post lurar användare att klicka på länkar eller bilagor som kan vara skadliga eller skapa sårbarheter. Nätverksfiske utnyttjar att användare hanterar e-post med inlärda heuristiker och sällan gör en medveten granskning av all information i e-post. Typiska principer för nätverksfiske är att hänvisa till någon auktoritet, övertala, skapa igenkänning, ge förväntade åtaganden samt distrahera användare. Att skapa igenkänning är den vanligaste principen. Genom att utnyttja användares heuristiker för att hantera e-post är det svårt även för tränade och uppmärksamma användare att upptäcka nätverksfiske. Några sätt att öka upptäckten av nätverksfiske är att uppmärksammande e-postens källa och grammatik samt öka användares engagemang. Det är även stora individuella variationer i användares förmåga att upptäcka nätverksfiske.

6 Slutsatser

Litteraturöversikten bekräftar uppfattningen att bara ett fåtal studier har presenteras inom IT-säkerhet i tidskrifter och på konferenser som är inriktade på *human factors*. Men att påstå att det finns väldigt lite forskning inom området är däremot missvisande. Många *human factors* studier inom IT-säkerhet har nämligen gjorts inom människa-dator interaktion. Men även om mycket är gjort finns det fortfarande stora forskningsbehov inom humanaspekter för IT-säkerhet.

Ett förslag på fortsatt forskning om angripare utifrån litteraturöversikten är:

- Angripare vill av många skäl vara dolda och anonyma, vilket försvårar studier av hur de tänker och resonerar. Fortsatt forskning av angripares kognitiva processer är väsentlig för att få en bättre förståelse av hur attacker kan försvåras.

Sju förslag på fortsatt forskning om försvarare utifrån litteraturöversikten är:

- Det behövs mer forskning om träning. Det finns många beskrivningar av IT-säkerhetsutbildningar för personal och träning i samband med IT-säkerhetstävlingar. Många deltagare är nöjda, men det behövs tydligare mått på kunskaper och prestationsförmåga precis som inom andra kompetensområden.
- Många försök har gjorts för att identifiera vad som kännetecknar situationsmedvetenhet för IT-säkerhet genom intervjuer och observationer av operativ personal. Hittills är resultaten begränsade, vilket delvis beror på områdets snabba utveckling och skiftande karaktär. Det är hela tiden är en utmaning att identifiera otillbörlig trafik i stora legitima informationsmängder. Det kan därför finnas anledning att även pröva andra angreppssätt som till exempel att studera själva processen för att skapa situationsmedvetenhet (*eng*. situation assessment). Svårighet är att validera vad som är bra process. Förmodligen finns det även en del att hämta från de senaste årens forskning om situationsförståelse (*eng*. sensemaking).
- Eftersom många IT-säkerhetstävlingar redan använder så kallade röda team som angripare är steget inte långt till att genomföra offensiva cyberoperationer. Flera forskare har börjat studera området, men mer forskning behövs om kunskapskrav, operativa metoder, etiska problem och integration med den militära ledningsprocessen.
- Under flera år har omfattande studier gjorts av visualiseringar för IT-säkerhet. Tyvärr användas endast få av dess visualiseringar i praktiken. En anledning till att så få visualiseringar används är bristande analyser av analytikernas informationsbehov. Många förslag har antingen utvecklats av personer som inte är så insatta i IT-säkerhet eller av systemadministratörer som inte är så insatta i visualiseringstekniker. För att komma vidare behövs förmodligen bättre analyser av vilka typer av frågor som analytiker försöker besvara. Den faktiska informationen som används för analyserna varierar däremot från fall till fall.
- Det finns många verktyg för att identifiera tekniska sårbarheter, men hur sårbarheter uppstår som en kombination av människa, teknik och organisation är däremot mindre utforskat. Bättre verktyg för sårbarhetsanalyser förbättrar systemadministratörers möjligheter att balansera alla faktorer som påverkar IT-säkerheten.
- I många studier har ledningen för organisationen en undanskymd roll som enbart ansvarar för tilldelning av resurser och i övrigt har svårt att förstå IT-säkerhetsfrågor. Mer forskning behövs om ledning och aktiv styrning av IT-säkerhet.

- IT-säkerhet består överlag av många processer som till exempel kognitiva processer, teamprocesser, organisatoriska processer och sociala processer. För närvarande finns enbart ett antal fragmenterade studier inom modellering och simulering av dessa processer och framförallt är modellerna sällan integrerade. Mer forskning om modellering och simulering för IT-säkerhet behövs för att förstå de olinjära processerna.

Sju förslag på fortsatt forskning om användare utifrån litteraturöversikten är:

- Många studier visar att IT-säkerhetspolicyn utformas utan tillräcklig hänsyn till användares förutsättningar och arbetssituation. Det här beror ofta på en bristande kommunikation mellan användare och IT-säkerhetsexperter. Mer forskning behövs om konkreta metoder för att förbättra kommunikationen och skapa användbar IT-säkerhet.
- Vilka faktorer som påverkar användares respekt för IT-säkerhetspolicyn har studerats i förhållandevis många studier. Men även om modellerna successivt blir allt bättre på att förklara intentionen att respektera policyn finns det ännu ingen ensad syn på vilken modell som är bäst. Mer forskning behövs för att utveckla mogna modeller som integrerar relevanta faktorer.
- Studier av IT-säkerhetskultur blir allt vanligare, men det är fortfarande ett omoget forskningsområde. Befintliga studier är ofta på en konceptuell nivå. Fler studier behövs av användbara metoder för att förbättra IT-säkerhetskulturen.
- IT-säkerhetsmedvetande är viktigt för att användare på ett flexibelt sätt ska kunna göra avvägningar mellan säkerhetskrav och verksamhetskrav i situationer som inte beskrivs i IT-säkerhetspolicyn. Flera förslag finns för hur säkerhetsmedvetandet kan förbättras, men bristen på enhetliga mätmetoder hämmar utvecklingen och gör det svårt att jämföra möjliga träningsstrategier. Mer forskning behövs om hur IT-säkerhetsmedvetande ska mätas.
- Även informerade och vaksamma användare har svårt att upptäcka nätverksfiske. Förutom mer utbildning kan även tekniska stödsystem hjälpa användare att uppmärksamma kritiska detaljer. Ett sätt att identifiera lovande tekniker kan vara att utveckla kognitiva modeller för användares beslutssituation. Med sådana modeller går det att utvärdera vilken typ av information som är mest effektiv för att påverka besluten.
- Ny autentiseringstekniker utvecklas kontinuerligt för nya typer av klienter, användningsmiljöer och hot. Men inga tekniker ser ännu ut att kunna ersätta lösenord för autentisering i många tillämpningar trots alla problem de innebär för användare. Vanliga problem är till exempel att vid upprepade tillfällen behöva skapa och minnas lösenord som samtidigt är svåra för en angripare att forcera. Mer forskning behövs om riktlinjer för både användbara och säkra lösenord.
- Interna IT-brott där personal eller tidigare anställd personal utnyttjar sina kunskaper för att komma åt känslig information är en allt större risk för många organisationer. Många studier har gjorts för att identifiera riskfaktorer, men det finns ännu ingen ensad syn på vilka faktorer som är viktigast. Mer forskning behövs för att identifiera de faktorerna och för att utveckla validerade mätinstrument som indikerar risk för interna IT-brott.

7 Referenser

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179–211.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476–490.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection: An intervention study. *Computers & Security*, *29*(4), 432–445.

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. In *PACIS 2012 Proceedings*, Paper 144, http://aisel.aisnet.org/pacis2012/144.

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, *65*, 153–165.

Bauer, S., & Bernroider, E. W. (2015). The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring. In T., Tryfonas, & I. Askoxylakis (Eds.), *Third International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS 2015)* (pp. 154-164). LNCS 9190, Springer International Publishing.

Beitzel, S., Dykstra, J., Huver, S., Kaplan, M., Loushine, M., & Youzwak, J. (2016). Cognitive performance impact of augmented reality for network operations tasks. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 139–151). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

Ben-Asher, N., & Gonzalez, C. (2015a). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61.

Ben-Asher, N., & Gonzalez, C. (2015b). Training for the unknown: the role of feedback and similarity in detecting zero-day attacks. *Procedia Manufacturing*, *3*, 1088–1095.

Bertini, E., Hertzog, P., & Lalanne, D. (2007). SpiralView: Towards security policies assessment through visual correlation of network resources with evolution of alarms. In D. Ebert, & T. Ertl (Eds.), *2007 IEEE Symposium on Visual Analytics Science and Technology (VAST 2007)* (pp. 139–146). IEEE.

Botta, D., Muldner, K., Hawkey, K., & Beznosov, K. (2011). Toward understanding distributed cognition in IT security management: the role of cues and norms. *Cognition, Technology, & Work, 13*, 121–134.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human performance in cybersecurity: A research agenda. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 55, No. 1, pp. 1115–1119). SAGE Publications.

Bradshaw, J. M., Carvalho, M., Bunch, L., Eskridge, T., Feltovich, P. J., Johnson, M., & Kidwell, D. (2012). Sol: an agent-based framework for cyber situation awareness. *KI-Künstliche Intelligenz*, *26*(2), 127–140.

Branlat, M., Morison, A., & Woods, D. D. (2011). Challenges in managing uncertainty during cyber events: Lessons from the staged-world study of a large-scale adversarial cyber security exercise. In *Human Systems Integration Symposium 2011* (pp. 10–25).

Cain, A. A., Chiu, L., Santiago, F., & Still, J. D. (2016). Swipe authentication: Exploring over-the-shoulder attack performance. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 327–336). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors*, *58*(8), 1158–1172.

Canzani, E., & Pickl, S. (2016). Cyber epidemics: Modeling attacker-defender dynamics in critical infrastructure systems. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 377–389). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

Champion, M. A., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). Team-based cyber defense analysis. In *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support* (pp. 218–221). IEEE.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy*, *5*(12), 61–67.

Choi, H., Lee, H., & Kim, H. (2009). Fast detection and visualization of network attacks on parallel coordinates. *Computers & Security*, *28*(5), 276–288.

Choong, Y. Y., & Theofanos, M. (2015). What 4,500+ people can tell you–employees' attitudes toward organizational password policy do matter. In T., Tryfonas, & I. Askoxylakis (Eds.), *Third International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS 2015)* (pp. 299–310). LNCS 9190, Springer International Publishing.

Cooke, N., Champion, M., Rajivan, P., & Jariwala, S. (2014). Cyber situation awareness and teamwork. *Transactions of Security and Safety, Special Section on: The Cognitive Science of Cyber Defense*. Institute for Computer Science, Social Informatics, and Telecommunications Engineering (ICST).

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies*, *16*, 41–96.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*, 1849–1858.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101.

D'Amico, A., Buchanan, L., Kirkpatrick, D., & Walczak, P. (2016). Cyber Operator Perspectives on Security Visualization. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 69–81). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 49, No. 3, pp. 229–233). SAGE Publications.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: testing a contemporary deterrence model. *Decision Sciences*, *43*(6), 1091–1124.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658.

Derbentseva, N., Fraser, B., Gibbon, S., & Hawton, A. (2015). What do we know about threats from well-intentioned users. In Y. Yanakiev (Ed.), *Proceedings of International Conference on Human Systems Integration Approach to Cyber Security* (pp. 63–78), 28-29 September, 2015, Rakovski National Defence College, Bulgaria.

Dutt, V., Moisan, F., & Gonzalez, C. (2016). Role of Intrusion-Detection Systems in Cyber-Attack Detection. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 97–109). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(1), 32–64.

Enrici, I., Ancilli, M., & Lioy, A. (2010, May). A psychological approach to information technology security. In T. Pardela, & B. Wilamowski (Eds.), *3rd International Conference on Human System Interaction*. May 13-15, 2010, Rzeszów, Poland. IEEE.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In T., Tryfonas, & I. Askoxylakis (Eds.), *Third International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS 2015)* (pp. 36–47). LNCS 9190, Springer International Publishing.

Foresti, S., Agutter, J., Livnat, Y., Moon, S., & Erbacher, R. (2006). Visual correlation of network alerts. *IEEE Computer Graphics and Applications*, *26*(2), 48–59.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & Security*, *46*, 18–31.

Funke, G., Dye, G., Borghetti, B., Mancuso, V., Greenlee, E., Miller, B., & Vieane, A. (2016). Development and validation of the air force cyber intruder alert testbed (CIAT). In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 363–376). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

Giacobe, N. A. (2013). A picture is worth a thousand alerts. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 57, No. 1, pp. 172–176). SAGE Publications.

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People*, *22*(2), 92–108.

Goodall, J. R., Lutters, W. G., Rheingans, P., & Komlodi, A. (2005). Preserving the big picture: Visual network traffic analysis with TNV. In *IEEE Workshop on Visualization for Computer Security 2005 (VizSEC 05)* (pp. 47–54). IEEE.

Greene, K. K. (2015). Effects of Password Permutation on Subjective Usability Across Platforms. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 59–70). Springer International Publishing.

Guimaraes, V. T., Freitas, C. M. D. S., Sadre, R., Tarouco, L. M. R., & Granville, L. Z. (2016). A survey on information visualization for network and service management. *IEEE Communications Surveys & Tutorials*, *18*(1), 285–323.

Gutzwiller, R. S., Fugate, S., Sawyer, B. D., & Hancock, P. A. (2015). The human factors of cyber network defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 59, No. 1, pp. 322-326). SAGE Publications.

Hao, L., Healey, C. G., & Hutchinson, S. E. (2013). Flexible web visualization for alert-based network security analytics. In *Proceedings of the Tenth Workshop on Visualization for Cyber Security* (pp. 33-40). ACM.

Hardisty, F., & Robinson, A. C. (2011). The geoviz toolkit: Using component-oriented coordination methods for geographic visualization and analysis. *International Journal of Geographical Information Science*, *25*(2), 191–210.

Hawkey, K., Muldner, K., & Beznosov, K. (2008). Searching for the right fit: Balancing IT security management model trade-offs. *IEEE Internet Computing*, *12*(3), 22–30.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54-60.

Hugl, U. (2015). Putting a hat on a hen? Learnings for malicious insider threat prevention from the background of German white-collar crime research. In T., Tryfonas, & I. Askoxylakis (Eds.), *Third International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS 2015)* (pp. 631–641). LNCS 9190, Springer International Publishing.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95.

Jaferian, P., Hawkey, K., Sotirakopoulos, A., Velez-Rojas, M., & Beznosov, K. (2014). Heuristics for evaluating IT security management tools. *Human–Computer Interaction*, *29*(4), 311–350.

Jariwala, S., Champion, M., Rajivan, P., & Cooke, N. J. (2012). Influence of team communication and coordination on the performance of teams at the iCTF competition. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 56, No. 1, pp. 458–462). SAGE Publications.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246–285.

Kintzel, C., Fuchs, J., & Mansmann, F. (2011). Monitoring large IP spaces with clockview. In *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, Article No. 2. ACM.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289-296.

Lif, P., Holm, H., Sommestad, T., Granåsen, M., & Westring, E. (2016). *Försöksverksamhet inom logganalys för cybersäkerhe*t. FOI-R--4328--SE. Stockholm: Totalförsvarets forskningsinstitut.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479.

Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010). A cognitive task analysis for cyber situational awareness. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 54, No. 4, pp. 279–283). SAGE Publications.

Mancuso, V. (2012). *An Interdisciplinary Evaluation of Transactive Memory in Distributed Cyber Teams*. Unpublished doctoral dissertation, College of Information Sciences and Technology, The Pennsylvania State University, State College, PA.

Mancuso, V. F., Minotra, D., Giacobe, N., McNeese, M., & Tyworth, M. (2012). idsNETS: An experimental platform to study situation awareness for intrusion detection analysts. In *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support* (pp. 73–79). IEEE.

Maqbool, Z., Pammi, V. C., & Dutt, V. (2016). Influence of motivational factors on hackers' and analysts' decisions in dynamic security games. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 239–251). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

Martini, B., & Choo, K. K. R. (2014). Building the next generation of cyber security professionals. In *Proceedings of European Conference on Information Systems (ECIS) 2014*, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0.

McEvoy, P., & Still, J. D. (2016). Contextualizing mnemonic phrase passwords. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 295–304). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

Molchanova, E. & Borilin, V. (2016). Cyber security, or cyber safety culture? Converting the weakest link into a force. Presented at *The 2nd International Conference on Human Factors in Cybersecurity*, July 27–31, 2016, Walt Disney World, FL.

Morris, J. D., & Waage, E. (2015). Cyber aptitude assessment: Finding the next generation of enlisted cyber soldiers. *The Cyber Defense Review*, Nov 2015.

Newhouse, B., Keith, S., Scribner, B., & Witte, G. (2016). *NICE Cybersecurity Workforce 2 Framework (NCWF)*. NIST Special Publication 800-181, National Institute of Standards and Technology.

Nielsen, J., & Molich, R. (1990). Heuristic evaluation of user interfaces. *Proceedings of the CHI 1990 Conference on Human Factors in Computer Systems*. New York: ACM.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. In *2014 IEEE Security and Privacy Workshops (SPW)* (pp. 214–228). IEEE.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778.

Rajivan, P. (2011). CyberCog. A Synthetic Task Environment for Measuring Cyber Situation Awareness. Master Thesis, Arizona State University, AZ.

Rajivan, P., Champion, M., Cooke, N. J., Jariwala, S., Dube, G., & Buchanan, V. (2013). Effects of teamwork versus group work on signal detection in cyber defense teams. In *International Conference on Augmented Cognition* (pp. 172–180). Springer Berlin Heidelberg.

Saner, L. D., Campbell, S., Bradley, P., Michael, E., Pandza, N., & Bunting, M. (2016). Assessing aptitude and talent for cyber operations. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 431–437). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131.

SECURIT (2016). https://www.foi.se/securit

Senanayake, R., & Denker, G. (2016). Towards more effective cyber operator interfaces through semantic modeling of user context. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 19–31). Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing.

Shiravi, H., Shiravi, A., & Ghorbani, A. A. (2012). A survey of visualization systems for network security. *IEEE Transactions on visualization and computer graphics*, 18(8), 1313–1329.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

Sommestad, T., Ekstedt, M., Holm, H., & Afzal, M. (2011). Security mistakes in information system deployment projects. *Information Management & Computer Security*, *19*(2), 80–94.

Sommestad, T., & Hallberg, J. (2013). A review of the theory of planned behaviour in the context of information security policy compliance. In *IFIP International Information Security Conference* (pp. 257–271). Springer Berlin Heidelberg.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: a systematic review of quantitative studies. *Information Management & Computer Security*, *22*(1), 42–75.

Sommestad, T., & Hunstad, A. (2013). Intrusion detection and the role of the system administrator. *Information Management & Computer Security*, *21*(1), 30–40.

Stanard, T., Lewis, W. R., Cox, D. A., Malek, D. A., Klein, J., & Matz, R. (2004). An exploratory qualitative study of computer network attacker cognition. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 48, No. 3, pp. 401–405). SAGE Publications.

Summers, T. (2015). *How hackers think: A discussion on the mental models and cognitive patterns of high-tech wizards*. Doctoral Dissertation. Weatherhead School of Management, Case Western Reserve University, OH.

Summers, T., & Lyytinen, K. (2013). How hackers think: A study of cybersecurity experts and their mental models. In *Third Annual International Conference on Engaged Management Scholarship* (pp. 1–25), Atlanta, Georgia, 2013.

Sundaramurthy, S. C., Bardas, A. G., Case, J., Ou, X., Wesch, M., McHugh, J., & Rajagopalan, S. R. (2015). A human capital model for mitigating security analyst burnout. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)* (pp. 347–359).

Svenmarck, P. (2015). *Kvartalsrapport 1 HSI Cyber Security*. FOI MEMO 5460. Stockholm: Totalförsvarets forskningsinstitut.

Svenmarck, P. (2016). *Delrapport 2 HSI Cyber Security*. FOI MEMO 5820. Stockholm: Totalförsvarets forskningsinstitut.

Tamassia, R., Palazzi, B., & Papamanthou, C. (2009). Graph drawing for security visualization. In I. G. Tollis & M. Patrignani (Eds.), *Graph Drawing* (pp. 2–13). LNCS, Vol. 5417. Springer.

Thompson, R. S., Rantanen, E. M., Yurcik, W., & Bailey, B. P. (2007). Command line or pretty lines? Comparing textual and visual interfaces for intrusion detection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1205–1215). ACM.

Trippe, D. M. Reeder, M. C., Brown, D. Jose, I. J., Heffner, T. S., Wind, A. P., Canali, K. G., & Thomas, K. I. (2015). *Validation of the information/communications technology literacy (ICTL) test*. Washington, DC: US Army Research Institute.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586.

Werlinger, R., Hawkey, K., Botta, D., & Beznosov, K. (2009). Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies*, *67*, 584–606.

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems, *27*(1), 273–303.

Yin, X., Yurcik, W., Treaster, M., Li, Y., & Lakkaraju, K. (2004). VisFlowConnect: netflow visualizations of link relationships for security situational awareness. In *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security* (pp. 26–34). ACM.

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People*, *26*(4), 401–419.

Zhou, A. T., Blustein, J., & Zincir-Heywood, N. (2004). Improving intrusion detection systems through heuristic evaluation. In *Canadian Conference on Electrical and Computer Engineering 2004*. (Vol. 3, pp. 1641–1644). IEEE.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se