FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

FOI-R--1215--SE
December 2003
ISSN 1650-1942
Metodrapport

Arne Vidström, Lars Westerdahl, Amund Hunstad, Jonas Hallberg

Spårning -

från IT-säkerhetsbrister till bakomliggande orsaker

SÄKRING AV VIKTIG INFRASTRUKTUR

Ledningssystem
581 11 Linköping

TOTALFÖRSVARETS FORSKNINGSINSTITUT
Ledningssystem
581 11 Linköping

FOI-R--1215--SE
December 2003
ISSN 1650-1942
Metodrapport

Arne Vidström, Lars Westerdahl, Amund Hunstad, Jonas Hallberg

Spårning –
från IT-säkerhetsbrister till bakomliggande orsaker

Utgivare Totalförsvarets Forskningsinstitut - FOI Ledningssystem 581 11 Linköping	**Rapportnummer, ISRN** FOI-R--1215--SE	**Klassificering** Metodrapport
	Forskningsområde 1. Analys av säkerhet och sårbarhet	
	Månad, år December 2003	**Projektnummer** E17405
	Verksamhetsgren 3. Forskning, kompetens och resursutveckling	
	Delområde 13. Stöd till säkerhet och beredskap	
Författare/redaktör Arne Vidström Lars Westerdahl Amund Hunstad Jonas Hallberg	**Projektledare** Henrik Christiansson	
	Godkänd av Johan Allgurén	
	Uppdragsgivare/kundbeteckning Krisberedskapsmyndigheten, KBM	
	Tekniskt och/eller vetenskapligt ansvarig Arne Vidström	
Rapportens titel Spårning – från IT-säkerhetsbrister till bakomliggande orsaker		

Sammanfattning (högst 200 ord)

Denna rapport beskriver ett ramverk som är tänkt att vara ett hjälpmedel i arbetet med att kartlägga hur beslut på övergripande organisationsnivåer får konsekvenser i form av IT-säkerhetsbrister. Detta arbete sker genom så kallad *spårning*, vilken går ut på att utreda bakåt från en konstaterad säkerhetsbrist till bakomliggande orsak(er).

Nyckelord Spårning, säkerhetsbrister, bakomliggande orsaker	
Övriga bibliografiska uppgifter	**Språk** Svenska
ISSN 1650-1942	**Antal sidor:** 69 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm	FOI-R--1215--SE	Methodology report
	Programme Areas 1. Security, Safety and Vulnerability Analyses	
	Month year December 2003	**Project no.** E17405
	General Research Areas 3. Research and development of knowledge and resources	
	Subcategories 13. Support to Security, Safety and Preparedness	

Author/s (editor/s)	Project manager
Arne Vidström Lars Westerdahl Amund Hunstad Jonas Hallberg	Henrik Christiansson
	Approved by Johan Allgurén
	Sponsoring agency Swedish Emergency Management Agency, SEMA
	Scientifically and technically responsible Arne Vidström

Report title (In translation)
Tracing - from IT security vulnerabilities to underlying reasons

Abstract (not more than 200 words)

This report describes a framework intended to be an aid when investigating how decisions on a management level in an organization have consequences in the form of IT security vulnerabilities. This work is done by so called *tracing*, which consists of investigating backwards from a discovered vulnerability to its underlying reason(s).

Keywords
Tracing, vulnerabilities, underlying reasons

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 69 p.
	Price acc. to pricelist

Innehåll

Figurer

Förord

Denna rapport är skriven inom ramen för Krisberedskapsmyndighetens ramforskningsprogram *Säkring Av Viktig Infrastruktur* (SAVI). I denna rapport tas ett ramverk fram för att spåra bakomliggande orsaker till att IT-säkerhetsbrister uppstår i organisationer.

Vi vill tacka vår medarbetare Hans Jander från Institutionen för Människa-System-Interaktion som utfört alla intervjuer vid vårt test av ramverket och även bidragit med värdefulla kommentarer till vårt arbete. Vi vill också tacka Henrik Christiansson vid Institutionen för System- och funktionsvärdering för värdefull hjälp samt Banverket som bidragit med underlag rörande verkliga incidenter.

1 Bakgrund

1.1 Syfte

I propositionen *Samhällets säkerhet och sårbarhet* (2001/02:158) påtalas vikten av att upprätthålla en hög informationssäkerhet i hela samhället. För detta har staten inrättat fyra verksamhetsområden i syfte att förbättra informationssäkerheten i samhället. Dessa verksamhetsområden är *omvärldsanalys, IT-incidenthantering, teknikkompetens* (innefattar bland annat aktiv IT-kontroll) samt *evaluering och certifiering*. Ansvar för dessa områden har placerats i ovannämnd ordning hos Krisberedskapsmyndigheten (KBM), Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA) samt Försvarets materielverk (FMV). I propositionen *Fortsatt förnyelse av totalförsvaret* (2001/02:10) beskrivs nyttan med PTS incidenthanteringsfunktion på bland annat följande sätt:

> Denna förädling skapar ett avsevärt mervärde för myndigheterna (de rapporterande, egen kommentar) i deras arbete med att rapportera inträffade incidenter med *påföljande åtgärdsprogram*. Analyserna bör av flera skäl leda till att bättre rekommendationer kan ges beträffande skyddsåtgärder.

Det är oerhört viktigt att dra lärdomar av inträffade incidenter och att dessa leder till relevanta åtgärdsprogram. Dock är det oss veterligen inte formulerat *hur* incidentinformation skall resultera i åtgärdsprogram eller ens vilken typ av data från incidenten som krävs för att detta skall vara möjligt.

I samma proposition finns formuleringar kring syftet med FRA:s verksamhet med aktiv IT-kontroll:

> Ett av de huvudsakliga syftena med genomförandet av en aktiv IT-kontroll är att det kontrollerade informationssystemets systemägare blir *medveten* om säkerhetsbristerna.

Aktiv IT-kontroll kan i någon mening betraktas som kontrollerade incidenter. Dessa bör kanske i ännu högre grad kunna bidra till formulering av åtgärdsprogram med tanke på just möjligheten att samla *alla* relevanta data. Att systemägarna blir medvetna om säkerhetsbristerna är bara det första steget för att avhjälpa dessa. Även här saknas det uppgifter om hur aktiviteten aktiv IT-kontroll skall kunna skapa långsiktigt hållbara åtgärdsprogram.

Syftet med föreliggande studie är därför att från en grundläggande nivå undersöka hur incidenter (inträffade eller inducerade) kan användas för att identifiera bakomliggande orsaker till säkerhetsbrister för att på så sätt kunna konstruera lämpliga åtgärdsprogram. Detta har resulterat i en formulering av ett ramverk för att kunna kartlägga beslut som påverkat eller påverkar IT-säkerhetsfrågor.

1.2 Begrepp

I det här avsnittet används några begrepp som saknar en allmänt vedertagen definition. För att undvika missförstånd följer här ett kort resonemang kring hur begreppen används i rapporten.

Med **IT-säkerhet** avses här de delar av området informationssäkerhet som är av teknisk natur, med en begränsning till sådant som berör datorer och kommunikation mellan datorer.

Med **säkerhetsbrist** avses en teknisk eller administrativ brist, relaterad till området IT-säkerhet, som relativt direkt möjliggör för en angripare att orsaka skada. Med relativt direkt menar vi att bristen är något som en angripare kan upptäcka och utnyttja på en teknisk nivå.

Den **konkreta säkerhetsnivån** avser hur svårt det är för en angripare att i praktiken orsaka skada genom angrepp mot datorer eller kommunikation mellan datorer. Här avses alltså *inte* hur väl en viss säkerhetsstandard är uppfylld eller liknande. Begreppet konkret säkerhetsnivå skall inte tolkas som något man i praktiken kan mäta upp med exakthet, utan som ett abstrakt begrepp som pekar på den egenskap hos ett system som alla säkerhetshöjande åtgärder skall sträva efter att förbättra.

1.3 Problemformulering

Två grundläggande hypoteser utifrån praktisk erfarenhet är följande:

- De som besitter djup teknisk kunskap inom IT-säkerhetsområdet har ofta dålig insikt i övergripande frågor inom en organisation och/eller dåliga möjligheter att påverka dessa.
- De som ägnar sig åt övergripande frågor saknar ofta insikt i vad IT-säkerhet handlar om på djup teknisk nivå.

På en övergripande nivå ägnar man sig, med rätta, inte åt några tekniska detaljer. Däremot har man möjlighet att påverka exempelvis planering av kompetensutveckling, anställning av personal, anlitande av konsulter, arbetsmiljö, organisationskultur, ansvarsfördelning och många andra viktiga

faktorer. Det finns mängder av viktiga faktorer, och mängder av komplexa och svåranalyserbara samband mellan dessa. Varje faktor kan potentiellt, genom orsakskedjor av varierande längd, i slutänden påverka den konkreta säkerhetsnivån i enskilda system. För beslutsfattare på övergripande nivåer skulle det vara användbart att känna till vilka konsekvenser olika beslut får för den konkreta säkerhetsnivån. Man kan inte begära att samma personer ska ha goda kunskaper, erfarenhet, samt möjlighet att påverka, när det gäller både djupa tekniska respektive övergripande frågor. Därför vore det mycket önskvärt att kunna påvisa någon form av relativt lättbegripliga kopplingar mellan nivåerna.

De två ovannämnda hypoteserna gäller i synnerhet inom organisationer med andra kärnområden än inom det informationstekniska. Ett exempel på detta är samhällsviktig infrastruktur där informationsteknik har blivit en kritisk komponent. Ofta har man stora, svåröverskådliga system som dessutom är starkt inhomogena både med avseende på teknik och organisation. Det är inte ovanligt att personer som tidigare arbetat med icke IT-relaterade uppgifter får fler och fler uppgifter inom IT-området trots relativt begränsad vidareutbildning. Dessutom kommer det in rena IT-experter som inte har någon större kompetens inom kärnområdet.

Vårt ramverk är tänkt att vara ett hjälpmedel i arbetet med att kartlägga hur beslut, eller ibland avsaknad av beslut, på övergripande nivåer får konsekvenser i form av konkreta säkerhetsbrister. Kartläggningen sker baklänges genom så kallad spårning (taget från begreppet spårbarhet) från konstaterad säkerhetsbrist till bakomliggande orsak(er).

Det finns exempel på tidigare arbeten med att kartlägga bakomliggande orsaker till IT-säkerhetsbrister men detta har gjorts för specifika tekniska komponenter som operativsystem (Lindskog & Jonsson (2002)). Där var utgångspunkten observationer från icke-specificerade studier.

1.4 Kriterier för vilka säkerhetsbrister som skall studeras

En viktig utgångspunkt vid val av säkerhetsbrister att studera är att alla presenterade slutsatser måste grunda sig på sådant som iakttagits ute i verkligheten för att resultatet inte ska bli rena spekulationer.

Sett från ett nyttoperspektiv är det viktigt att man studerar säkerhetsbrister som verkligen möjliggör för en angripare att orsaka någon form av skada för verksamheten. Det är exempelvis inte relevant att studera vissa avvikelser från en policy som inte skulle kunna få någon skadlig effekt.

Med andra ord kan vi se några viktiga kriterier för vad man baserar sina samband på:

- Man måste studera konkreta säkerhetsbrister
- Säkerhetsbristerna måste finnas i verkliga system, i driftmiljö
- Säkerhetsbristerna måste möjliggöra för en angripare att orsaka skada för verksamheten i fråga

Dessutom tillkommer att man måste ta hänsyn till riskbedömningar och kostnadsberäkningar. Man tvingas alltid acceptera ett mer eller mindre stort antal säkerhetsbrister på grund att det vore för kostsamt, eller praktiskt omöjligt, att åtgärda alla.

Vi kan alltså lägga till ytterligare ett kriterium:

- Säkerhetsbristerna räknas i detta fall inte som brister om det med gott omdöme tagits en kalkylerad risk baserad på en korrekt utförd riskanalys

Det finns flera sätt att hitta säkerhetsbrister på, exempelvis:

- Säkerhetstestning av olika slag
- Inträffade incidenter
- Någon upptäcker en säkerhetsbrist på annat sätt och rapporterar den till lämpliga personer

Dock är det relativt ofta så med rapporter från inträffade incidenter att uppgifterna om vad som har hänt är mycket knapphändiga. Det primära för systemägarna är att städa upp i systemen och få allt att fungera igen.

Det spelar egentligen ingen större roll vid enskilda spårningar hur en brist upptäckts så länge den uppfyller de tidigare beskrivna kriterierna. Om man vill skaffa sig ett stort underlag av brister att arbeta vidare med för att få fram statistik över vilka bakomliggande orsaker som är vanligast, måste man vara noga med att få ett korrekt urval av brister för att uppnå statistisk tillförlitlighet. Sannolikt kommer det vara mycket svårt att lyckas med något sådant. Enligt vår erfarenhet skulle det vara mycket tidskrävande och dessutom skulle det antagligen vara svårt att finna tillräckligt många säkerhetsbrister där det finns tillräcklig indata för en tillförlitlig spårning av bakomliggande orsaker.

2 Vetenskaplig bakgrund till ramverket

Grunden till ramverket ligger i *fallstudier*, *Grounded theory* samt *kognitiv intervjumetodik*. Dessa metoder har flera likheter mellan varandra och stämmer väl med de idéer som ramverket bygger på.

Forskning delas ofta upp i kvalitativa och kvantitativa metoder. Kvantitativa metoder stödjer sig på ett stort urval där syftet är att dra generella slutsatser. Kvalitativa metoder riktar in sig på ett mindre urval med syftet att få en större förståelse. Grovt uttryckt kan man säga att kvantitativa metoder ger svar i siffror medan kvalitativa metoder ger tolkningar utifrån sociala perspektiv vilka inte kan eller bör översättas till siffror (Holme & Solvang (1997), sid.76).

Inledningsvis ges en kort introduktion till kvalitativ forskning i allmänhet för att därefter övergå till en presentation av grundidéerna inom ovan nämnda metoder. Kognitiva intervjuer är ingen forskningsmetod i sig. Dock har intervjumetoden speciella egenskaper och själva intervjumomentet i sig är centralt inom både fallstudier och Grounded theory varvid den förtjänar en egen presentation.

2.1 Kvalitativ forskning

En livlig debatt har förts avseende kvalitativ och kvantitativ forskning. Främst har diskussionen behandlat den kvalitativa forskningens validitet. Ett vanligt förekommande krav på vetenskapliga studier är att forskningsresultat skall vara reproducerbara, det vill säga alla studier och mätningar skall kunna genomföras igen med samma resultat, trots att mätningens ”data” och ”instrument” har ändrats. Med kvantitativ forskning är detta i regel inga problem då de oftast har en bred men distanserad kontakt med forskningsobjektet. Denna markerade distans möjliggör att objektet förblir opåverkat och därmed kan man upprepa metoden. Kvalitativa metoder befinner sig mycket närmare det som studeras, vilket innebär att forskaren har svårt att inte påverka objektet (Chalmers (1999), sid.3). Hur stor påverkan är beror på mål, syfte och metod.

Kvalitativa metoder strävar alltså efter att förstå ett mindre område utifrån dess förutsättningar och begränsningar. Det är inte alls säkert, eller för den delen ens eftersträvansvärt, att resultatet kan generaliseras och på så sätt kunna appliceras i ett större samanhang. Intresset ligger primärt i att beskriva och förstå det unika eller avvikande (Holme & Solvang (1997), sid.78).

Ramverket för att spåra de bakomliggande orsakerna till IT-säkerhetsbrister syftar till förståelse av den miljö där säkerhetsbristen uppstod. Syftet har en klar kvalitativ innebörd då resultatet inte på ett tillfyllestgörande sätt kan beskrivas i siffror utan lämpar sig bättre som ett förklarande resultat.

2.2 Fallstudier

Inom flertalet forskningsområden görs studier av existerande fall i syfte att exemplifiera de resultat eller samband forskaren vill belysa. En sådan studie kallas allmänt för fallstudie (case study). Utvärderingar är typiska fallstudier där den eller det som utvärderas är ”fallet” (Stake (1995), sid.95).

Fallstudier kan även ses som en forskningsstrategi, vars syfte kan vara att beskriva, testa eller generera nya teorier. Styrkan i fallstudier ligger i att forskaren ges möjlighet att studera en situation på djupet och därmed förstå dynamiken i situationen (Eisenhardt (1989), sid.534-535).

Egentligen finns det ingen begränsning på när fallstudier kan användas. Det är en starkt avgränsad miljö som studeras, där forskaren har liten eller ingen kontroll över händelseförloppet. Dock, till skillnad från ren historie-beskrivning, måste en forskare ha möjlighet att observera händelser samt genomföra intervjuer (Yin (1994), sid.8).

När frågeställningen avseende aktuella händelser innehåller orden ”hur” eller ”varför” är fallstudier ett starkt alternativ som forskningsstrategi (Yin (1994), sid.9).

Vidare är fallstudien en empirisk undersökning, det vill säga man studerar händelser i verklig miljö. I de fall där syftet är att skapa nya teorier är just den empiriska undersökningen en styrka, då kopplingen mellan händelse och sammanhang inte alltid är klar (Yin (1994), sid.13). Eisenhardt (1989) hävdar även att kopplingen mellan empiri och teoribyggnadsprocessen gör att validiteten i teorin ökar (sid.547).

Validitet

Kritiskt inom vetenskap i allmänhet och inom kvalitativ vetenskap i synnerhet är att skapa validitet. Här har kvantitativa metoder ett stort försteg genom ett större urval och möjligheten att utföra deduktion.

Validiteten i en fallstudie byggs in redan i designstadiet. Yin (1994) anger fyra typer av validitetsmått (sid.33):

Skapad validitet: designen måste visa att mätningarna är rätt för det sammanhang man vill belysa. Validiteten skapas genom att

använda olika källor vid faktainsamlingen samt att sortera dessa i en ”kedja av bevis”. Man kan även låta nyckelpersoner ta del av materialet innan det publiceras för att erhålla en mer insatt återkoppling över de förhållanden som rapporten beskriver.

Intern validitet: påvisa möjliga och rimliga händelseförlopp för fallet och på så sätt undvika orimliga slutsatser. Den interna validiteten sätts i analysfasen genom att en väldokumenterad analys genomförs. Intern validitet är endast aktuellt då man utför en förklarande eller relationsbaserad studie.

Extern validitet: specificera det område där resultaten kan generaliseras, något som är väsentligt då man jämför flera fall.

Reliabilitet: beskriver hur mätningar utförts med sådan precision att samma mätningar skulle kunna genomföras igen med resultat som följd. Noggrann dokumentation och hantering av insamlat material stödjer reliabiliteten.

När det gäller att skapa nya teorier är enskilda fall att föredra (Eisenhardt (1991), sid.620). Stake (1995) sammanfattar det hela bra när han säger (sid.8):

The real business of case study is particularization, not generalization.

Nya teorier skapas ur ett avgränsat område för att sedan generaliseras och testas i större miljöer.

Fallstudiedesign

Det första steget i en fallstudie är att sätta upp en plan för hur studien skall se ut. Planen skall omfatta alla steg från problemområdet med inledande frågeställning till hur den slutliga rapportens utformning. Validiteten, och främst reliabiliteten, är synnerligen beroende av planen i kvalitativ forskning. Mycket av den kritik som har riktats mot fallstudier bygger just på bristande riktlinjer för planering av studien. Yin (1994), Stake (1995) och Eisenhardt (1989, 1991) med flera har var och en för sig lagt ner stor möda med att strukturera en design för fallstudier.

Yin (1994, sid.64-65) har gett en överblick över en tänkbar generell design.

Översikt: först görs en grundläggande beskrivning av hela fallet, problemfrågeställningen och begränsningar. Detta är ”kravspecifikationen”, det vill säga det dokument man alltid kan återvända till om man blir osäker på målet eller syftet med undersökningen.

Procedurer: forskaren bör i förhand se till att tillgång ges till personer, platser och dokumentation relevant för studien. Vidare förbereds

eventuell utrustning och dokumentation som forskaren behöver ha med sig under undersökningen.

Frågor: en studie skall svara på flera frågor. Forskaren förbereder specifika frågeställningar vilka genomsyrar hela studien samt väljer ut möjliga källor som kan tänkas ha svar på varje fråga.

Guide för rapport: själva rapporten är resultatet av studien. Det är fördelaktigt att redan i designskedet bestämma hur rapporten skall se ut, främst beroende på att kvalitativa studier har en förmåga att ”växa okontrollerat”.

Designen av studien fungerar som en brygga mellan problemställningen, det man inledningsvis känner till om problemet, vad man behöver ta reda på, guida till slutsatser samt hur man skall presentera resultatet (Tellis (1997), Stake (1995), sid.15).

Datainsamling

Fallstudiens djup relateras till mängden använda informationskällor. Intervjuer är oftast huvudverktyget för datainsamling, även om andra källor finns. Fördelen med att använda flera källor är att triangulering kan genomföras (se Analys). Tellis (1997) har genom Stake (1995) och Yin (1994) identifierat sex informationskällor:

Dokument: aktuell dokumentation med direkt eller indirekt koppling till problemområdet, såsom administrativa dokument, artiklar eller brev vilka är av intresse.

Arkivmaterial: här avses äldre dokument, eller i alla fall dokument vilka inte har en uppenbar koppling till fallet men tjänar som beskrivande eller identifierande för de som ingår i studien.

Intervjuer: som nämndes ovan är intervjuer huvudverktyget i en fallstudie. De ger forskaren en möjlighet att får svar ”mellan raderna”, det vill säga kunna prata med deltagarna om sådant som inte framgår, eller ”syns”, i dokumentation eller genom observation. (För en mer ingående genomgång av intervjuer se Kognitiva intervjumetodik).

Direkt observation: genom att studera miljön ”i arbete” kan forskaren komplettera sina intryck med informationen från intervjuerna. En av huvudorsakerna att genomföra direkt observation är att människor tenderar att skilja på vad man säger att man gör och vad som faktiskt sker. Använder man mer än en observatör ökar reliabiliteten, då observatörens personliga referensram påverkar intrycken från observationen.

Deltagande observation: forskaren kan ingå som en medlem i den grupp som observeras. Man skall vara väl medveten om att i

denna situation kan forskaren påverka gruppen och därmed ge ett missvisande resultat.

Föremål: fysiska föremål som är viktiga för gruppen och resultatet kan vidga förståelsen för forskaren. Det kan röra sig om verktyg, instrument med mera.

Analys

Gränsen mellan insamling och analys är diffust. Exempelvis görs redan under en intervju en preliminär analys i syfte att kunna guida och ställa rätt frågor till den intervjuade. Huvudanalysen görs dock efter varje intervju för att bedöma vad man fått reda på och vad man kan konstatera som preliminär fakta samt hur man går vidare.

Man kan säga att det finns två strategiska inriktningar på analys av fallstudier. Forskaren kan välja att tolka varje enskild instans av ett fall eller samla flera instanser till dess att man kan begränsa en mängd händelser till en klass (Stake (1995), sid.74).

Yin (1994, sid.106-117) anger tre huvudinriktningar på analysmetoder.

Mönsterpassning: en jämförelse görs mellan det empiriska resultatet forskaren erhållit och det i förväg förväntade resultatet. Stake (1995) kallar detta för ”correspondence”. Här är det viktigt att skilja på begreppen ”mönsterpassning” och att ”söka efter mönster”. Mönsterpassning är en utmärkt metod då man vill testa en teori eller tes, medan sökandet efter mönster mer lämpar sig för en explorativ undersökning, då nya teorier eftersträvas eller helt saknas.

Förklaringsmodeller: analysen bygger på att forskaren förklarar en händelse eller ett fenomen. Förklaringen byggs upp genom att finna orsaker till fenomenets uppkomst och dess verkan.

Förklaringsmodeller är av iterativ karaktär. Även om det inte finns mycket skrivet avseende praktiska tillämpningar av iteration så är principen klarlagd. En typisk iterativ ansats inleds med ett antagande om sakers och tings natur och beteende. Detta antagande jämförs sedan med den första instansen av fallstudien, varvid en eventuell revidering av antagandet sker. Processen görs om för varje instans av fallstudien, vilket så småningom resulterar i en slutsats som inte ändras av nya instanser.

Det finns tydliga risker med iterativa modeller, då det kan vara svårt att veta när man skall sluta samt hur man går vidare. En annan risk är att det insamlade materialet blir omöjligt att

överblicka. Problem av denna karaktär minimeras genom en tydlig design av studien samt att forskaren kontinuerligt refererar till denna.

Kronologier: att analysera händelser över tiden ger en möjlighet till mönsterpassning med avseende på kronologi. Precis som med mönsterpassningen ovan handlar det om att jämföra empiriska upptäckter med förutspådda. Kronologier studeras med avseende på:

- *Sekvens*: vissa händelser är beroende av att ske i en viss sekvens för att ett korrekt eller giltigt resultat skall uppstå. Om sekvensen bryts skall önskat resultat vara omöjligt.
- *Kontinuitet*: en del händelser måste efterföljas av andra givna händelser.
- *Luckor*: en del händelser kan inte inträffa förrän en viss tid efter att den inledande händelsen har inträffat.
- *Periodicitet*: händelser som inträffar under en viss tid och som skiljer sig markant från händelser från en annan tid kan sammanföras i en klass.

Ett begrepp som nämndes som hastigast i inledningen av datainsamlingen är triangulering. Inom kvalitativ forskningsmetodik i allmänhet är triangulering en viktig ingrediens för att skapa validitet. Triangulering kan utföras på flera aspekter av fallstudien.

Datatriangulering: transitiviteten i ett fenomen eller fall testas genom att upprepa händelsen med andra förutsättningar.

Observatörstriangulering: en observatör kan inte helt ta avstånd från egna värderingar. Genom att låta en annan observatör studera samma situation kan man jämföra uppfattningen av situationen.

Teoritriangulering: en kompletterande observatör med en annorlunda teorietisk ståndpunkt fungerar som en referens. Ett sätt att uppnå detta är att använda två personer med olika bakgrund vid en intervju eller analys.

Metodisk triangulering: den mest välanvända och erkända metoden för triangulering är att variera med vilken metod data analyseras.

Stake (1995, sid.112-114)

Utopi/Kritik

Vad vi har sett hittills är fallstudier en metod för att beskriva en empirisk situation, en bas för att skapa nya teorier eller förklara fenomen. Oftast används dock fallstudier för att exemplifiera en teori. Vad gör då en fallstudie till en bra fallstudie?

Yin (1994, sid.147-152) menar att en bra fallstudie är en sådan som belyser ett ämne som är av betydelse eller har ett allmänt intresse. Fallstudien måste vara komplett i det avseende att det skall finnas tydliga gränser vilka markerar när ett syfte eller en teori anses bekräftad. Vidare måste studien vara planerad så att den inte avbryts för tidigt på grund av tidsbrist eller brist på data. Forskaren skall i förväg ha bedömt om studien är genomförbar, och därmed värderat förutsättningarna och riskerna. Vidare ökar olika perspektiv validiteten på studien. Avslutningsvis är det läsaren som är i fokus; läsaren har i regel en stor områdeskunskap vilket gör att bevisföringen måste vara tydligt så att läsaren kan dra egna slutsatser och bedöma rapportens slutsatser.

Fallstudier har utsatts för mycket kritik från flera håll. Viss del av kritiken gäller inte enbart fallstudier utan kvalitativa metoder i allmänhet. Ett exempel på sådan kritik är att fallstudier inte kan, eller i alla fall har svårt för att, generaliseras. Detta är till viss del korrekt. Fallstudier är ofta inriktade på att beskriva ett starkt avgränsat område där det unika och speciella inom detta område är det intressanta. Det medför givetvis att resultatet har en begränsad giltighet utanför detta område, men detta gäller när man endast studerat ett fall (Stake (1995), sid.85). I de fall man gör multipla fallstudier och där forskaren kan kontrollera de fasta och rörliga inparametrarna är fallstudier minst lika bra som någon annan kvalitativ metod. Om generalisering är huvudsyftet, och möjligheten finns, bör en kvantitativ metod användas.

Det finns dock kritik direkt riktad mot fallstudier. Eisenhardt (1989, 1991), Stake (1995) och Yin (1993, 1994) med flera har lagt ner stor möda på att besvara kritiken bland annat genom att ge riktlinjer för hur fallstudier bör designas för att resultatet skall ha validitet.

Yin (1994, sid.9-10) menar också att en tänkbar orsak till misstron mot fallstudier beror på en allmän missuppfattning. Han anser det troligt att man blandar ihop fallstudier för undervisning och fallstudier för forskning. I undervisningssituationen är studien tillrättalagt i syfte att demonstrera en specifik poäng i ämnet. Fallstudier för forskningsbruk tillåter inte en förutbestämd miljö där slutsatser och resultat är förutbestämda.

Tidigare nämndes det att fallstudier kan användas för att skapa nya teorier. En forskningsmetod som är besläktad med fallstudier och vars huvudsyfte är att skapa nya teorier är Grounded theory. Nästa kapitel presenterar Grounded theory samt belyser skillnaderna gentemot fallstudier.

2.3 Grounded theory

I de flesta forskningsfall utgår en forskare från en teori vilken skall bevisas eller falsifieras. Således finns det alltid en förutfattad mening om hur eller vad som bör ske i det aktuella fallet. I och med detta blir ofta resultatet teoriberoende. Grounded theory[1] är en empirisk metod vilken endast tar hänsyn till de data varje undersökning genererar. Metoden grundar sig på empiri och induktion till skillnad från deduktion (Glaser (1998), sid.91).

Den grundade teorin skapades av Barney Glaser och Anselm Strauss i slutet av sextiotalet i syfte att underlätta skapandet av nya teorier. Glaser och Strauss ser teoribildning som en process (Glaser & Strauss (1967, sid. 32)), det vill säga en teori är inte komplett bara för att den en gång tryckts på papper. En teori utvecklas hela tiden och ersätts efterhand med en ny teori.

En forskare som utnyttjar Grounded theory startar förutsättningslöst med sin undersökning. Byggstenarna i teoribildningen är den information som finns tillgänglig i det aktuella fallet. Informationen är data såsom fenomen, företeelser och utsagor. Den teorilösa inledningen i Grounded theory är en förutsättning för att forskaren skall kunna ha ett öppet sinne för de intryck som undersökningen ger. Fördelen med uteslutande av förutbestämda teorier och ansatser är att forskaren inte lockas att tvinga fram data för att passa den förutbestämda teorin (Glaser (1992), sid.15). Forskaren inleder istället sin undersökning med en vagt formulerad frågeställning (Plewes (2002)) vilken fungerar mer som en ledstjärna för arbetet än något som skall värderas.

Glaser (1992) trycker hårt på att man inte skall ha några förutfattade teorier eller försöka tvinga fram ”passande” teorier;

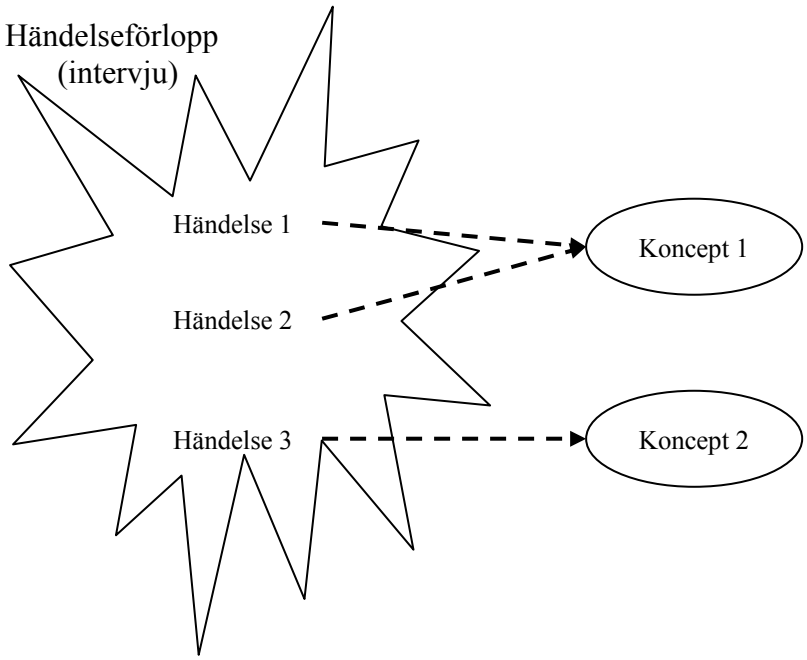
> *...there is no need for force data until it gives up; emergence will happen.*
> Glaser (1992), sid.20

Huvudsyftet med Grounded theory är att skapa nya teorier. Således är Grounded theory inte lämpat för att identifiera och testa teorier och hypoteser (Plewes (2002)). Det är dock viktigt att redan här poängtera att de teorier som skapas med Grounded theory inte handlar om ”specialteorier”, det vill säga en teori som är så detaljerad att den endast passar i en mycket specifik situation. Inte heller är avsikten att Grounded theory skall användas som ”utfyllnad” för att förklara anomalier. En teori skapad med Grounded theory beskriver kärnprocessen i ett problem, det vill säga orsaken till alla händelser (Glaser (2002), sid.8-9).

[1] Grounded theory benämns i viss Svensk litteratur som Grundad teori. Vi har dock valt att använda det engelska uttrycket då detta blir tydligare i sammanhanget.

Koncept

Teorier skapas genom att man ”lyfter” en händelse eller företeelse till en högre abstraktionsnivå. På så sätt beskrivs händelsen ur ett perspektiv vilket inte är beroende av den data abstraktionen utgår ifrån. Abstraktioner av data inom Grounded theory kallas för koncept.
Ett koncept är en abstraktion av ett fenomen, händelse eller utsaga. Det är namnet på ett socialt beteende grundat i tillgänglig data (Glaser (2002), sid.4). Ett beteende är något som en person agerar inom, inte personen i sig själv. Således är ett koncept inte beroende av tid, plats eller människor, vilket gör koncept hållbara, jämfört med beskrivningar vilka snabbt förlorar aktualitet. Likaså kan koncept relateras till varandra likt hypoteser (Glaser (2002), sid.6-10), se figur 3.1.

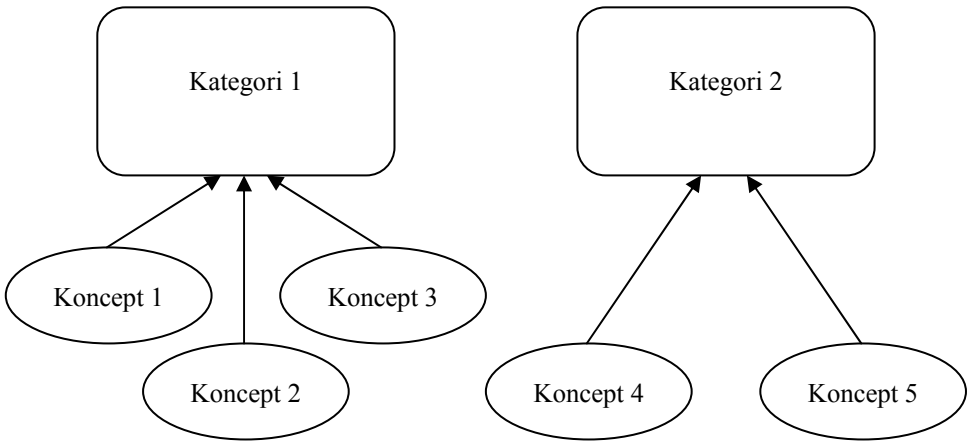


Figur 3.1: Konceptualisering. Händelser är sociala beteenden vilka förklaras i abstrakt form. Den abstrakta formen kalla koncept.

Kategorier

Koncept med gemensamma egenskaper samlas i en kategori. En kategori är en abstrakt namngivning av en samling koncept med liknande egenskaper (Glaser (1992), sid.40). Således är en kategori ett koncept av koncept, det vill säga en högre abstraktionsnivå än koncepten själva. Oftast namnges kategorier med den sociala företeelsen den representerar alternativt med ord

hämtade från den data som ligger till grund för kategorin, det vill säga ett fackord hämtat utifrån den företeelse som studeras (Glaser (1992), sid.45).



Figur 3.2: Kategorier. Koncept med liknande egenskaper samlas i kategorier.

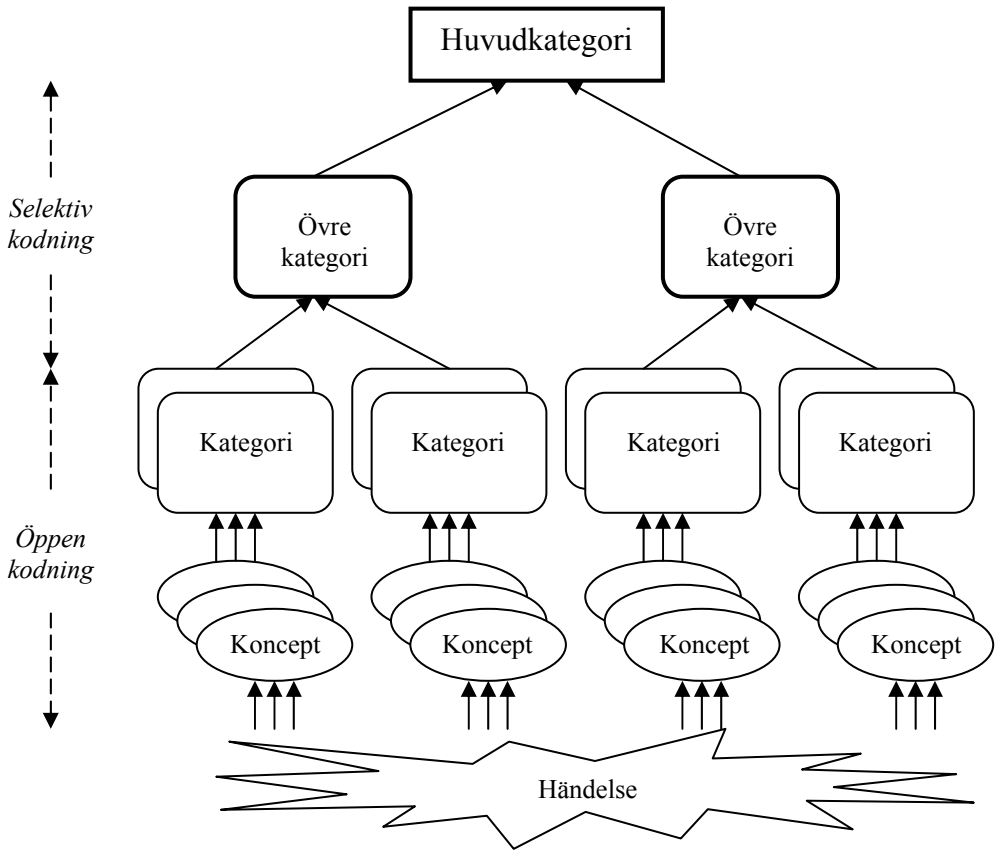
Det är kategorierna som ligger till grund för teoriutvecklingen inom Grounded theory. Inledningsvis skapas flera kategorier för att beskriva koncepten. Dessa kategorier används sedan för att göra högre abstraktioner avseende kategorierna själva, i syfte att till slut nå en huvudkategori. Denna huvudkategori förklarar de underliggande kategorierna och relationerna mellan dessa, det vill säga huvudkategorin är teorin i Grounded theory (Calloway (1996)). Vill man beskriva Grounded theory med kategorier kan man säga att förmågan att göra koncept är huvudkategorin inom Grounded theory (Glaser (2002), sid.2).

Analys

Data är en händelse, det vill säga information vilken endast har betydelse i det sammanhang som den existerar i. Det en människa säger sig ha sagt, tyckt eller gjort är en konkret händelse vilken saknar betydelse i generell form. Det är svårt att jämföra data från ett sammanhang med data från ett annat sammanhang. Grounded theory abstraherar händelser till koncept vilka är beständiga och jämförbara med andra koncept, oberoende av sammanhang. Data är bevis för ett fenomen under den tid som undersökningen sker (Haig (1995)).

Transmissionen från händelse till teori sker i två steg; öppen kodning respektive selektiv kodning[2]. Den inledande öppna kodningen avser övergången från data, via koncept, till kategorier. Här beskrivs även egenskaper för en kategori. Dessa egenskaper är i praktiken koncept av aktuell kategori och således koncept av de koncept en kategori innehåller (Glaser (1992), sid.38).

Den selektiva kodningen innebär att begränsa kodningen till de variabler som refererar till huvudkategorin. Det är huvudkategorin, med sina egenskaper, som förklarar mönster och beteende i de övriga kategorierna (Glaser (1992), sid.75).



Figur 3.3: Grounded theory analys. Analysförloppet från händelse (intervjudata) till huvudkategori.

[2] Strauss och Corbin (1990) vill även införa ett mellansteg med axial kodning där kategorierna relateras till varandra. Just axial kodningen är något som Glaser (1992) emotsätter sig starkt, då han menar att den inte tillför någonting och bryter mot originalidén – Grounded theory är ursprungligen skapad av Glaser och Strauss (1967).

Validitet

Grounded theory är en induktiv metod där teorier bildas utifrån det fenomen som studeras (Pandit (1996)). En induktiv metod är ett starkt val för teoribildning även om den lämnar mycket att önska när det gäller bevisföring. Detta är dock inget problem för Grounded theory då metoden inte är avsedd för att bevisa teorier, utan att skapa dem. Det är även uppenbart att teorin stämmer i minst ett fall, då den grundar sig på de empiriska förhållanden som gäller för fallet. En teori skapad med hjälp av Grounded theory uppfyller fyra krav; passar, fungerar, relevant och modifierbar (Glaser (1992), sid.15).

Passar: En teori som utkristalliseras ur kategorier med tillhörande egenskaper kommer att passa in i den verklighet kategorierna bygger på.

Fungerar: En fungerande teori kan förklara de processer som omger fenomenet man studerar.

Relevant: Om teorin både passar och fungerar uppnås relevans.

Modifierbar: Utfärdaren av teorin skall vara medveten om att ny data kan förändra teorin, det vill säga teorin skall inte vara sådan att den inte går att modifiera.

2.4 Intervjumetodik

I både fallstudier och Grounded theory är intervjun central för datainsamling. Intervjuer kan dock utföras med olika metoder. I det ena änden är det en mycket strukturerad och styrd intervju med i förväg bestämda frågor och svarsalternativ. Resultatet är i de flesta avseenden detsamma som om den intervjuade fick svara på en enkät med fasta svarsalternativ. Den andra änden av spektret är en intervju där varken frågor eller svarsalternativ är bestämda på förhand. Friheten ger en god möjlighet till en djupgående intervju där den intervjuade har stora möjligheter att påverka informationen.

Ser man till grunden på vad en intervju innebär är det ett ensidigt informationsutbyte. Det är den intervjuade som sitter inne med all kunskap. I traditionella intervjuer är det dock intervjuaren som styr intervjun och på så sätt påverkar vilken information som kommer fram men även, i värsta fall, vad den intervjuade skall svara. En metod att undvika styrning och därmed lägga grunden till ett så rikt informationsflöde som möjligt är att använda kognitiva intervjuer.

Kognitiv intervjumetodik

Människans förmåga att minnas saker och händelser är inte lagrade i hjärnan som enskilda poster. Oftast minns vi saker i ett sammanhang eller tillstånd. Detta medför svårigheter att på uppmaning spontant extrahera specifik information. Våra minnesbilder är beroende av den kontext de sparades i. Med detta menas att vi minns händelsen som ett inslag i den miljö och det tillstånd vi befann oss i vid det tillfället.

Traditionell intervjumetodik där intervjuaren ställer frågor och därmed förväntar sig svar har flera begränsningar med avseende på ovanstående stycke. Vid en direkt fråga svarar den tillfrågade ofta ytligt och mycket begränsat. Det innebär inte att den tillfrågade inte vet mer eller, för den delen, undanhåller information. Förmågan att minnas spontant är mycket begränsad. På så sätt blir svaret mer beroende av frågan än av verkligheten.

Om man istället använder öppna frågor och svar i en intervju, det vill säga frågan är mer allmänt hållen och den intervjuade tillåts svara fritt, ökar informationsmängden i svaret. Öppenheten underlättar för den intervjuade i och med att det ges utrymme att tänka och formulera sina svar själv. Vissa problem kvarstår dock i och med att det fortfarande handlar om frågor och svar. Intervjuaren begränsar ofta utrymmet för den intervjuade genom att frågan kan tolkas på flera sätt. Den intervjuade försöker föreställa sig vad intervjuaren vill veta genom att tolka nyanser i röst och ordval. En undersökning som Elander (2001a) hänvisar till beskriver hur intervjuade svarade, beroende på hur frågan ställdes efter att alla har sett samma film. I det aktuella fallet rörde det sig om en sekvens där två bilar kolliderade och de intervjuade fick frågan om hur fort bilarna körde då de kraschade/kolliderade/stötte ihop/träffade/kontaktade varandra. Det visade sig att den uppfattade hastigheten på bilarna stod i relation till hur starkt ord som användes i frågan.

Den kognitiva intervjumetodiken utnyttjar människans behov av att associera ett händelseförlopp med den information man söker. Intervjuaren undviker direkta frågor genom att låta den intervjuade beskriva ett förlopp och på så sätt tillåts återuppleva den totala händelsen. Det har visat sig att kognitiva intervjuer ger fler sanningsenliga svar jämfört med andra metoder (Elander (2001b)). Nu räcker det inte enbart med att återskapa den miljö eller de förutsättningarna som var vid händelsens inträffande. Undermedvetet redigerar människan gärna sina minnesbilder för att framhäva det de uppfattar som intressant. Intervjuaren kan upptäcka detta genom att låta den intervjuade berätta om händelsen i en annan sekvens. Vidare bör man byta perspektiv i syfte att se på händelsen på ett annat sätt (Bennett).

Struktur

En kognitiv intervju genomförs i fem faser: introduktion, fri redogörelse, detaljerad genomgång, återblick samt avslutning (Christianson et al (1998), sid.99).

Introduktion: En stor del av förutsättningarna för hur lyckad intervjun kommer att bli avgörs redan i introduktionen. Det är här intervjuaren sätter stämningen och aviserar relationen mellan intervjuare och intervjuad.

Fri redogörelse: Tyngdpunkten i den kognitiva intervjun ligger i den intervjuades fria redogörelse. Här får den intervjuade återskapa situationen där händelsen inträffade och fritt berätta sin version av händelsen. Det är viktigt att intervjuaren gör så få avbrott som möjligt utan att för den delen verka frånvarande. Intervjuaren kan efterhand ändra minnesperspektiv och minnesordning i syfte att få den intervjuade att minnas mer.

Detaljerad genomgång: Efterhand som förmågan att minnas mer från den intervjuade avtar övergår intervjun till en detaljerad genomgång. Här ställer intervjuaren öppna frågor för att reda ut oklarheter eller inkonsistens i den tidigare berättelsen. Varje fråga skall vara ställd så att den intervjuade kan återuppta sin fria redogörelse.

Återblick: Intervjuaren summerar det som behandlats under intervjun genom att berätta hur han/hon har förstått informationen. Syftet är att intervjuaren och den intervjuade skall ha samma bild av händelsen och att den intervjuade åter ges en möjlighet att komplettera och om möjligt utveckla en starta en ny redogörelse.

Avslutning: Intervjun avslutas med att intervjuaren avrundar det hela och tackar samt informerar den intervjuade om värdet av intervjun och den intervjuades delaktighet. Att avsluta på ett positivt sätt möjliggör framtida kontakter om så skulle behövas. Det är mycket viktigt att den intervjuade lämnar intervjun med en positiv inställning och känner att hans/hennes deltagande har varit betydelsefullt.

Övergången mellan faserna är glidande då skarpa avgränsningar kan verka hämmande på den som intervjuas. En kognitiv intervjumetodik ställer höga krav på intervjuaren. Även om intervjuaren skall undvika att avbryta med frågor gäller det att ge ett intresserat och alert intryck. Ett positivt uppträdande påverkar även den intervjuade positivt och därmed ökar viljan att delge den kunskap den intervjuade besitter.

3 Praktisk beskrivning av ramverket

I detta kapitel beskrivs det tidigare metodavsnittet i dess praktiska tillämpning. Ramverket används från det att en sårbarhet uppdagats till dess att en lösning finns i en rapport.

Arbetet löper över flera steg med syfte att förstå problemet och dess ursprung. Först måste utredaren förstå miljön där sårbarheten upptäcktes samt dess verkan, för att sedan kunna spåra den eller de bakomliggande orsakerna.

Följande delkapitel preciserar de steg ramverket passerar från initiering till resultat.

3.1 Initiering

Det här ramverket kommer först till användning då en säkerhetsbrist har uppdagats. Vare sig det är en verklig incident eller resultatet av en säkerhetsundersökning, är det ändå ett ramverk som är avsett att användas i efterhand.

När beslut tas att utnyttja ramverket bör man utse en kontaktperson vid den studerade organisationen. Denna kontaktperson är den initierande punkten i organisationen. Av denna anledning är det nödvändigt att kontaktpersonen har en god kännedom om företaget och beslutsgångarna. Om kontaktpersonen själv inte är inblandad, det vill säga ingen information tyder på detta, i incidentförloppet eller beslutet att initiera ramverket bör kontaktpersonen minst känna till vilka de inblandade aktörerna är.

Tänkbara kontaktpersoner kan vara; IT-chef, IT-säkerhetschef, Systemansvarig eller Avdelningschef.

3.2 Bakgrund

Innan några intervjuer och analyser med lämpliga personer kan påbörjas måste ramverkets arbetsgrupp skapa sig en god förståelse av det aktuella systemet samt företagets organisation. Mycket av den bakgrundsinformation som är nödvändig bör komma från kontaktpersonen såväl skriftligt som muntligt.

Ett rikt bakgrundsmaterial spar tid vid intervjuerna. Det möjliggör för dem som utnyttjar ramverket att förstå vilka personer och roller som agerar inom ramen för det som har hänt. Likaså minskar det risken för missförstånd

avseende struktur och ansvarsförhållanden inom organisationen samt det system som studeras.

Systemförståelse

Även om det tidigare har antytts att det främst inte är de tekniska orsakerna som ramverket är ute efter att finna, ligger dessa till grund för verksamheten. De som använder ramverket måste förstå den tekniska miljön där bristen har upptäckts samt vara så insatt i de tekniska förutsättningarna att intervjuerna och analysen blir meningsfull.

För att kunna gå vidare från en incident är det dock nödvändigt att ha full förståelse för var incidenten uppkom och hur den påverkade systemet. Uppkomsten är avgörande för hur ramverket skall implementeras och påverkan är ett kriterium för värdering av de beslut som tagits under systemets utveckling, driftställande eller drift.

En komplett beskrivning av systemets syfte, kopplingar till andra system och rättmätiga användare bör komplettera incidentbeskrivningen, tillsammans med en beskrivning av konsekvensen av incidenten.

Organisation

En viktig komponent i ramverket är förståelsen för organisationen där ramverket tillämpas. Det är inom organisationen beslut tas och implementeras, vilket påverkar funktionaliteten och kvalitén hos ett system. Oavsett om systemet är helt eller delvis egenutvecklat, eller inköpt av tredje part, har ett antal bedömningar och beslut tagits innan dess att bristen har haft möjlighet att uppstå.

För att kunna analysera de bakomliggande orsakerna till att en brist har uppstått är det nödvändigt att känna till beslutsgångarna inom organisationen, samt vilka ansvarsområden som är satta. De som bär det yttersta ansvaret för systemet och därmed rätten att påverka systemets utformning, de om ansvarar för systemets drift samt användarna, är primära val till vilka som kommer att intervjuas.

Dokumentation

Genom att begära dokumentation får man en uppfattning om hur väldokumenterat ett system och en organisation är, men även ett underlag för intervjuer och analyser. Exempel på lämplig dokumentation kan vara:

System	Organisation
• Viktiga funktioner som IT-systemet tillhandarhåller • Hård- och mjukvara • Upphandlingsdokument • Nätverksarkitektur • Konsultverksamhet	• Organisationsskisser • Roller • Policys • Konsultverksamhet

3.3 Intervjuer

Den första intervjun startar så fort arbetsgruppen för ramverket har fått en förfrågan om att genomföra en spårning av den bakomliggande orsaken till att en säkerhetsbrist har uppstått. Alla personer gruppen talar med är pusselbitar i spårningen. Ett rimligt antagande är att den första personen gruppen talar med är en chef eller ansvarig för det aktuella systemet. Det första mötet syftar till att skapa en förståelse för systemet och den organisation systemet finns inom.

Med den information som tillhandahålls vid första mötet görs en lista över primära intervjukandidater. Dessa kandidater informeras sedan om att de är inbjudna till en intervju och varför.

Introduktion

Platsen för intervjun är viktig med avseende på att den intervjuade skall ges ett neutralt intryck. Den intervjuades eget arbetsutrymme är inte att föredra då det kan finnas flera störande element, så som ringande telefoner och kollegor som kommer förbi. En speciell lokal markerar avskildhet samt motverkar vardagliga störmoment.

Intervjuaren bör placera sig så att inga ”maktbarriärer” uppstår. Att sitta på var sin sida om ett bord markerar avstånd och formalitet. Om man inte kan undvika bord kan båda sitta på samma sida eller vid ett hörn för att på så sätt få ett så kort avstånd från varandra som möjligt. Märk väl att ett neutralt avstånd är att föredra, det vill säga inte så nära att integriteten kränks men inte längre ifrån än att det informella intrycket består.

Redan då den intervjuade kommer till lokalen bör en positiv och avslappnad stämning finnas i lokalen. Detta kan framhävas genom att intervjuaren inte är upptagen med något annat och kan möta den intervjuade i dörren med sedvanliga hälsningsfraser.

Genom att förmedla ett artigt och positivt intryck från start har intervjuaren redan kommit en bra bit in i introduktionen, det vill säga det första steget i den kognitiva intervjumetodiken. I detta läge presenteras syftet med intervjun och vad intervjuaren hoppas åstadkomma genom intervjun.

Fri redogörelse

Introduktionen övergår till den fria redogörelsen när kontexten är lagd, det vill säga när det står klart för den intervjuade vilken situation som skall behandlas. I detta läge kan det vara en fördel att inleda intervjun som ett samtal avseende miljö och rutiner runt omkring det system där säkerhetsbristen har uppstått. På så sätt skapas en gemensam syn på vad man talar om och det ger den intervjuade något konkret att börja med. Intervjuaren bör dock vara försiktig så att inte den intervjuade upplever en allt för snäv gränssättning av området.

Under redogörelsen är det lämpligt att intervjuaren inte avbryter eller lägger sig i mer än absolut nödvändigt. Luckor i berättelsen eller inkonsekventa skeenden behandlas senare. Det viktiga för situationen är att låta den intervjuade ge sin bild av situationen och på så sätt skapa en så bra helhetsbild som möjligt.

Detaljerad genomgång

Efterhand som den intervjuade inte känner att han/hon har något mer att återge och intervjuaren inte kan vinkla berättelsen mer övergår man till att detaljgranska vad som berättats. Redogörelsen kan ha innehållit luckor eller inkonsekventa detaljer vilka nu skall redas ut. Intervjuaren inleder diskussionen med öppna frågor vilka skall uppmuntra den intervjuade till att återuppta sin redogörelse med den information som framkommer vid frågorna.

Steget mellan fri redogörelse och detaljerad genomgång är vagt och situationen hoppar naturligt mellan dessa. Syftet med en detaljerad genomgång är att få den intervjuade att återuppta sin redogörelse och därmed motverka att intervjuaren leder den intervjuade med sina frågor. Dock kan intervjuaren, med fördel, påtvinga den intervjuade att byta perspektiv på sin berättelse. Ett perspektivbyte, det vill säga att vinkla berättelsen från en annan synvinkel, är ett sätt att frambringa eftertanke hos den intervjuade och därmed tvinga denne att tänka efter eller ta ställning till händelseförloppet från någon annans perspektiv.

Återblick

Till slut kommer man inte längre, varken med redogörelse eller med genomgång. Intervjuaren sammanfattar nu vad som har sagt och ger sin bild av

situationen. Det är viktigt att intervjuaren berättar vad och hur han eller hon har uppfattat saker och ting, då det ger den intervjuade en möjlighet att korrigera missuppfattningar och felaktigheter. Här är även en sista chans att på nytt påbörja en redogörelse av en specifik situation.

Avslutning

En positiv avslutning av intervjun är viktig för framtida kontakter – både med den intervjuade men även med dennes kollegor. Även om en exakt återgivelse av vad som har berörts kanske inte sprids, så är det möjligt – för att inte säga troligt – att känslan av intervjun sprids vidare, det vill säga hur den intervjuade uppfattade situationen.

Intervjuaren bör tacka artigt för den tid som intervjun har tagit för den intervjuade samt informera om värdet intervjun har haft för hela undersökningen. Genom att lämna en positiv känsla, något som man bör eftersträva under hela intervjupasset, möjliggör man för vidare kontakter om så skulle behövas.

En intervju utförs med fördel av en person. Syftet med en intervjuare är att undvika en obalans i maktförhållandet mellan intervjuare och intervjuad. Om man väljer att använda två personer i en intervjugrupp bör den ena av dem leda själva intervjun, medan den andra intervjuaren lyssnar och kompletterar med frågor när första intervjuaren ber om detta. Ett samtidigt agerande från de båda intervjuarna kan hämma den fria redogörelsen från intervjupersonen.

3.4 Analys

Efter varje intervju görs en analys av intervjumaterialet. Syftet med analysen är att extrahera ny information om incidenten i form av att konceptualisera händelser samt att avgöra om en ny person (roll) bör intervjuas.

Själva analysen görs med fördel på en utskrift av intervjun. Det är möjligt att genomföra den med bandupptagning av intervjun men det underlättar för analysgruppen om intervjun finns nedskriven. I de fall då intervjuerna har genomförts med samma grupp som genomför analysen behöver man inte lägga tid på att sätta sig in i intervjumaterialet innan analysen.

Inledningsvis konceptualiserar man intervjun, det vill säga höjer händelser en abstraktionsnivå till koncept. Praktiskt innebär det att man söker händelser i intervjun, det vill säga sådant som sagts och kan strykas under i intervjuutskriften. Dessa händelser konceptualiseras genom att man beskriver dem i mer generella ordalag och därmed utelämnar information bunden till den specifika intervjun. På så sätt får man en beskrivning vilken är obero-

ende av tid, plats och rum. Värt att notera avseende koncept är att hjärnan ofta utför detta moment utan att vi medvetet tänker på det. I det här sammanhanget blir det viktigt att man stannar upp och tänker efter på vad som är en händelse, det vill säga vad som är bundet till en fysisk person och dennes agerande, och vad man redan har generaliserat till ett koncept, det vill säga formulerat om till ett socialt beteende. En intervju bör ge ett flertal koncept vilka grupperas i kategorier.

För att uppnå ett lyckat resultat med spårningen är det nödvändigt att man genomför en analys efter varje intervju. Det är svårt att ”se” händelser i efterhand. Oftast tänker man i ”konceptform” vilket gör att en händelse lätt ersätts med ett koncept, vilket i förlängningen gör det svårt att kategorisera koncept på ett korrekt sätt.

Varje kategori beskrivs sedan i form av koncept, vilket innebär att man gör koncept av koncept. På detta sätt beskriver man egenskaper av händelser med gemensamma egenskaper.

Efter ett antal repetitioner – i det här fallet intervjuer – kommer kategoribeskrivningarna leda fram till en huvudkategori, det vill säga den kategori som beskriver alla andra kategorier. Huvudkategorin är tillika även teorin och därmed den bakomliggande orsaken till att säkerhetsbristen uppstod. Den passar även in med de tidigare beskrivna reglerna för hur en Grounded theory valideras, det vill säga den passar, fungerar, är relevant och modifierbar (Glaser (1992), sid.15).

Det kan hända att huvudkategorin befinner sig på en sådan abstraktionsnivå att den inte är lämplig att förklara säkerhetsbristen med. I ett sådant fall kan det vara lämpligt att gå tillbaka ett steg i processen och acceptera en tidigare nivå med fler kategorier. Således kan man erhålla flera (om än inte många) "huvudkategorier" vilka beskriver problemet tydligare än en övergripande kategori.

3.5 Rapport

Arbetet med intervjuer och granskning av tillhandahållna dokument presenteras i en rapport. Själva rapportskrivandet pågår kontinuerligt under hela arbetet, allteftersom de olika stegen passeras.

Rapporten bör beskriva den kunskap arbetsgruppen erhållit i varje del av arbetet samt vilka orsaker som låg bakom varje beslut om hur man gick vidare. Integritet och etik är prioriterat när rapporten skrivs. Syftet med rapporten, och hela undersökningen, är att finna de orsaker som låg bakom säkerhetsbristen, inte att peka ut enskilda medarbetare.

4 Test av ramverket

Vid konstruktionen av ramverket var det viktigt att iterera mellan någon form av inträffad incident och metodframtagningen. I detta syfte samlades ett antal beskrivningar av incidenter som inträffat under ett antal månaders tid hos en stor myndighet med ansvar inom samhällsviktig infrastruktur[3]. Alltför många försvårande omständigheter identifierades vid analysen av dessa händelser för att de skulle kunna användas vid framtagandet av ramverket. Dels uppfyllde de allra flesta händelserna inte kriterierna som beskrivits (det vill säga var inte tillräckligt allvarliga eller rörde inte alls säkerhetsbrister enligt vår definition), dels var det mycket få som var tillräckligt väl dokumenterade för att just kunna användas vid testning av ramverket. Detta är i sig inte så underligt eftersom incidentrapporteringen inte är tänkt att tjäna som underlag för den typ av studier som beskrivs i denna rapport. Underlaget var dock viktigt i bemärkelsen att det skapade en förståelse för vilka typer av incidenter som upptäcks och hanteras i skarpa miljöer.

Av ovan nämnda anledning ansågs det nödvändigt att ”konstruera” en incident som kunde tjäna som underlag vid test av ramverket.

4.1 Konstruktion av ett scenario för test av ramverket

För att kunna göra ett första test av ramverket konstruerade vi ett scenario kring en incident hos organisationen XYZ. I scenariot hade XYZ råkat ut för ett omfattande intrång och vi skapade rollbeskrivningar åt fem personer som spelade anställda vilka på något sätt varit inblandade i incidenten. Scenariot har ingen som helst verklighetsbakgrund förutom att det är konstruerat med verkliga generella förhållanden i åtanke.

Inom det konstruerade scenariot så har inte XYZ kunnat bedöma de fulla konsekvenserna av intrånget, men inget har hindrat angriparen från att stjäla all tänkbar information i organisationens filservrar. Detta gör att den inträffade incidenten är mycket allvarlig för organisationen.

Den tänkta situationen när spårningsarbetet inleds är att intervjuare och analytiker har fått möjlighet att komma till XYZ för att testa sitt ramverk i praktiken för första gången.

[3] Banverket ansvarar bland annat för drift och underhåll av järnvägstrafiken i Sverige.

Det material som användes, i form av rollbeskrivningar och en mycket kortfattad rapport från en utredning av incidenten, finns att läsa i sin helhet i appendix A.

4.2 En kort beskrivning av scenariot

Organisationen XYZ har ungefär 100 anställda. Huvuddelen av dessa har kontorsdatorer med Windows som operativsystem och alla ingår i samma domän. För några månader sedan skedde ett intrång i ett stort antal av XYZs datorer. Ett externt konsultföretag, SäkertOchBra AB, anlitades för att reda ut vad som hänt och efter några veckor överlämnade man en mycket kort rapport över resultatet. Informationen i SäkertOchBra AB:s rapport och i rollbeskrivningarna är inte komplett eftersom ingen person i scenariot har den kompletta bilden. Detta var ett medvetet val eftersom det är ett realistiskt läge efter en incident.

Det inträffat vid incidenten var att en av de anställda, Anders (systemadministratör), hade hackat sig in i en gammal oanvänd domänfristående webbserver via ett känt säkerhetshål. Därefter körde han ett lösenordsknäckningsprogram på kontodatabasen och fick ut lösenordet till bland annat kontot ”terf72”. Detta konto tillhörde Bo (systemadministratör), som använde samma kontonamn och samma lösenord till sitt domänadministratörskonto. Nu kunde Anders logga in som Bo i alla datorer i domänen. Anders motiv var bland annat att han ville påvisa den dåliga säkerheten hos XYZ och själv få ta över efter Walter (IT-ansvarig), som snart skulle sluta för att istället börja arbeta på ett konsultföretag. Anders ville också misskreditera Bo och Peter (ansvarig för brandvägg och antivirusprogram) som var hans främsta konkurrenter när det gällde positionen som IT-ansvarig.

4.3 Bakgrund till scenariovalet

En aspekt vid valet av scenario var vilken teknisk nivå det skulle ligga på. Ett alternativ var att konstruera ett mer eller mindre teknikoberoende scenario genom att på något sätt utelämna specifika tekniska detaljer. Ett annat alternativ var att konstruera ett scenario kring ett tekniskt sett mycket sofistikerat intrång. Det slutgiltiga valet föll på ett scenario någonstans däremellan. Den främsta anledningen till detta är att majoriteten av de incidenter som uppkommer i praktiken inte alltid har en komplicerad teknisk orsak. Tekniken finns närvarande men behöver inte vara dominant. Nivån i scenariot svarar enligt vår erfarenhet relativt väl mot den genomsnittliga verkliga IT-säkerhetsincidenten.

Valet att låta en av de anställda vara den som utförde intrånget baserades framför allt på två önskemål från forskargruppen. Dels att skapa problem

vid spårningsarbetet i form av införande av falsk information. Dels också för att betona att angripare långt ifrån alltid kommer utifrån. Exakt hur stor andel av alla angrepp som har sitt ursprung utifrån respektive inifrån är en omtvistad fråga (Shaw et al (1998)). Vad som däremot är ganska klart är att de potentiella skadorna genomsnittligt är mycket större vid ett angrepp utfört av en insider, eller en angripare utifrån som samarbetar med en insider, än vid angrepp där ingen insiderhjälp finns att tillgå så länge övriga förutsättningar är lika [CERT].[4]

4.4 Brister i scenariokonstruktionen

När scenariot konstruerades var utgångspunkten den bakgrund som beskrivits i förra stycket. Därefter lades fokusen på den tänkta händelsekedjan och utifrån denna skrevs rollbeskrivningar et cetera. Förhållandevis lite fokus lades på att försöka förutsäga eventuella frågor i intervjuerna och inkludera lämplig information i rollbeskrivningarna från det perspektivet. På grund av detta dök det flera gånger under intervjuerna upp frågor vars svar borde ha ingått i rollbeskrivningarna, till exempel vem som är den intervjuades närmaste chef. I praktiken löste sig detta för det mesta genom improvisation från de intervjuade personernas sida. Detta underlättades sannolikt genom att de personer som spelade rollerna hade valts för att passa respektive roll. Flera hade tidigare erfarenhet av liknande, om än inte exakt samma, arbetsuppgifter som sin rollkaraktär. Dessutom togs hänsyn till att varje deltagares personlighet i någon mån skulle kunna passa för att spela respektive roll.

4.5 Övrigt om upplägget av scenariospelet

Inför scenariospelet gjordes valet att införa fyra typer av uppgifter hos deltagarna:

- Rollinnehavare (5 personer)
- Intervjuare (1 person)
- Analytiker (1 person)
- Observatörer (3 personer)

Som intervjuare valdes en medarbetare från FOI:s institution för Människa-system-interaktion med erfarenhet av kognitiva intervjuer. Övriga deltagare kom från FOI:s institution för Systemanalys och IT-säkerhet.

[4] Den amerikanska säkerhetstjänsten och CERT® CC genomför under åren 2002-2004 en analys av vilka konsekvenser som kan uppstå om en illvillig insider angriper IT-system i den kritiska infrastrukturen. I detta arbete ingår en anonym enkät riktad mot organisationer inom den kritiska infrastrukturen. (https://www.survey.cert.org/InsiderThreat/)

Vid varje intervju deltog, förutom intervjuaren och en rollinnehavare, dessutom de tre observatörerna varav två hade tagit del av det kompletta materialet kring scenariot. Observatörerna deltog också vid det efterföljande analysarbetet. Deras roll var att i tysthet iaktta händelseförloppet och föra anteckningar kring detta för att utvärdera resultatet av spårningen. Dessutom bandades alla intervjuer och skrevs sedan ut i efterhand.

Analysarbetet utfördes av intervjuaren och analytikern tillsammans. I detta arbete skulle analytikern också kunna bidra med extra teknisk kompetens. Före varje analysomgång lyssnade analytikern igenom bandinspelningarna av den föregående intervjun.

I ett verkligt fall är det fortfarande önskvärt att bara använda en intervjuare. Däremot kan det behövas flera analytiker med olika kompetens, exempelvis inom specifika teknikområden, organisationsteori, beteendevetenskap et cetera.

5 Erfarenheter från intervjuerna

Ett exempel på en intervju finns utskriven i appendix B.

I den följande texten används citat från bandutskrifterna för att belysa olika erfarenheter vi fått från intervjuerna. Talat språk är sällan uppbyggt av kompletta och grammatiskt korrekta meningar vilket gör att det kan se konstigt ut när det överförs ordagrant till skriven form. Vi har ändå valt att inte ”snygga till” citaten av den anledningen att detta skulle medföra att citaten i så fall blir en kombination av vad som verkligen sagts och vår tolkning av vad som sagts. Att läsaren får anstränga sig för att tolka det som sagts kan också ha ett egenvärde i form av att det då blir ännu mer uppenbart hur stor mängd egen tolkning som krävs för att man ska få upplevelsen av en helhet hos den förmedlade informationen. Denna insikt kan lätt falla bort när processen normalt sker automatiskt och undermedvetet.

5.1 Allmänt

I intervjuerna med Walter, Tommy och Anders kommer det kognitiva intervjukonceptet verkligen till sin rätt. De intervjuade personerna pratar fritt och det framkommer mycket information som intervjuaren inte behöver fråga efter överhuvudtaget.

Ibland kan det vara svårare att få en person att berätta saker utan att själv behöva ställa så många frågor. Till exempel så ingick det i rollbeskrivningen för Bo att han inte ville säga så mycket för att han trodde att Walter var ute efter att peka ut honom som en ännu större syndabock. Det finns många tänkbara anledningar till varför någon inte kan eller vill prata helt obehindrat under en intervju, och när detta inträffar bör man inte låsa sig helt vid det kognitiva konceptet utan exempelvis öka mängden frågor eller detaljnivån i frågorna för att få svar på det man undrar över.

5.2 Dokumentation

Vid jämförelse mellan anteckningarna från intervjuerna och utskrifterna från bandinspelningarna framgick att fel lätt smyger sig in bland anteckningarna.

Här följer ett utdrag från intervjuutskrifterna:

> *Intervjuaren – Mm. Vilka personer skulle kunna tjäna på något sådant här?*

Walter – Kan vara någon som har fått … slutat, någon anställd, som fortfarande är anställd som är missnöjd med någonting, eller som vill diskreditera någon annan på …, för att själv få en bättre ställning i organisationen. Det är ju känt nu att jag kommer att sluta här inom …, om ett halvår ungefär. Och det är flera stycken som naturligtvis är intresserade av att bli IT-ansvarig.

Det som uppfattades av en av observatörerna från detta svar var ”*Jag vill inte misskreditera någon…*” och det som antecknades var därför att Walter inte ville nämna några namn för att inte misskreditera någon. Ett sådant fel skulle exempelvis ha kunnat leda till att man i onödan avstått från att försöka få fram konkreta namn från Walter om ytterligare intervjuer gjorts.

Det finns flera tänkbara orsaker till att man får felaktiga anteckningar, exempelvis:

- Rena hörfel
- Förväntningar på vad som ska sägas förvränger uppfattningen av vad man hör
- Bristande koncentration
- För kortfattade anteckningar för att de ska kunna tolkas otvetydigt i efterhand

Det bör också nämnas att i det här försöket var det enbart observatörerna som antecknade, och dessa deltog inte aktivt i intervjun. I ett verkligt fall skulle det bli ännu värre eftersom intervjuaren då är ensam och måste koncentrera sig både på intervjun i sig men också på att anteckna. Slutsatsen av detta är att det är önskvärt att man bandar intervjuerna för att öka tillförlitligheten. Ett alternativ är att låta varje intervjuad person läsa igenom och godkänna anteckningarna från sin egen intervju.

5.3 Felaktiga uppgifter

Det är viktigt att tänka på att de personer som intervjuas kan komma att lämna felaktiga uppgifter både medvetet och omedvetet. I det här fallet vet man som yttre betraktare att Anders medvetet lämnar felaktiga uppgifter för att öka sina chanser att få ta över Walters arbetsuppgifter. Det står i Walters rollbeskrivning att han anser att Anders står först på tur att ta över som IT-ansvarig och att Peter kommer på andra plats. Vetskapen om att det kan finnas konkurrens mellan Anders och Peter skulle till viss del förändra trovärdigheten i uppgifterna de bägge lämnar, men detta framkommer aldrig för intervjuarna. Under intervjun med Walter kommer en fråga om vilka som kan tjäna på intrånget, men inga namn nämns.

Intervjuaren – Mm. Vilka personer skulle kunna tjäna på något sådant här?

Walter – Kan vara någon som har fått … slutat, någon anställd, som fortfarande är anställd som är missnöjd med någonting, eller som vill diskreditera någon annan på …, för att själv få en bättre ställning i organisationen. Det är ju känt nu att jag kommer att sluta här inom …, om ett halvår ungefär. Och det är flera stycken som naturligtvis är intresserade av att bli IT-ansvarig.

Intervjuaren – Mm.

Walter – Det kan ju finnas en viss konkurrens mellan några stycken personer här.

Intervjuaren – Och anledningen till att Du slutar, har det något med den här incidenten att göra?

Därefter fortsätter intervjun bort från frågan om vilka som kan tjäna på det inträffade. Hade intervjuaren dröjt sig kvar en aning kring vilka personerna är så kanske Walter hade lämnat namn på dessa. Mot slutet av intervjun kommer ämnet upp som kortast i ett svar på en annan fråga, men Walter fortsätter genast att prata om andra saker och därefter byts ämnet igen.

Intervjuaren – Ja, och det är ingenting annat som, du har ingen …, någon maggropskänsla själv på vad som du anser skulle kunna va … kunna leda in utredningen in i rätt riktning, för om du skulle ha suttit i den som ska genomföra analysens kläder. Vart skulle du ha riktat din uppmärksamhet någonstans?

Walter – Jag skulle tittat, som du gör här, övergripande först, jag tycker att det är helt fel att bestämma sig för att det kan var, att det är troligen det här och sedan då kommer man sannolikt fel. Det är inte någon sådan här uppenbar…, uppenbart att det måste så att säga vara någon speciell person och så vidare.

Det är viktigt att man, så långt möjligt, försöker bilda sig en uppfattning om vilka motiv de intervjuade personerna kan tänkas ha till att leda spårningen i en viss riktning. Dessa motiv behöver inte ha att göra med direkt skuld till en inträffad incident, utan kan exempelvis ha att göra med att någon är negativt inställd till förändringar och tror att en lyckad spårning kommer leda till förändringar i verksamheten.

5.4 Förvirring kring vad man pratar om

Under intervjun med Peter blev det tydligt hur viktigt det är att försäkra sig om att man pratar om samma saker; i det här fallet samma datorer, samma loggar och så vidare.

> *Intervjuaren – Har du kollat de loggarna och sett om det kommit in någonting ..., som man sett*
>
> *Peter – Eh, var någonstans, tänkte du?*
>
> *Intervjuaren – Jag tänkte om det här angreppet var som ..., ja enligt den här utredningen du hade läst, så insinuerar de att den här loggen skulle ha, ... eller att angreppet skulle ha kommit utifrån.*
>
> *Peter – Ja just det. Precis. Mm… Jo det har det väl troligen gjort mh... . Tänkte Du på loggarna i brandväggen eller?*
>
> *Intervjuaren – Ja.*
>
> *Peter – Den här burken eller.*
>
> *Intervjuaren – Ja det, det…, ja jag tänkte egentligen på båda delarna både brandväggen och eller både loggarna i brandväggarna och i burken.*
> *…*
> *Peter – Ja brandväggen sparar vi ju då. Så det skulle man kunna titta på. Men det är ju en hel del trafik. Det vet jag inte riktigt hur, om det kan synas där. Om de är tillräckliga då brandväggarna eh det får vi ta och undersöka. Men den andra maskinen är tyvärr raderad då och ominstallerad då.*

Peter syftar på arbetsstationen som den fristående servern hackats från när han pratar om ”den andra maskinen” som är ominstallerad men det klargörs aldrig. Vid den efterföljande analysen tolkas uttalandet istället som att den fristående servern ominstallerats.

Följaktligen är det mycket viktigt att alltid försäkra sig om att intervjuaren och den intervjuade personen avser samma saker. Ett sätt att klarlägga vad som är vad kan vara att till exempel rita upp en skiss över hur nätverket är uppbyggt och rita in de olika datorerna.

En faktor som ökar risken för sammanblandning är om analysgruppen inte besitter tillräckligt detaljerad teknisk kompetens inom det berörda området.

Man skulle i och för sig kunna tänka sig att använda sig av en teknisk expert som intervjuare men det har minst två stora nackdelar. För det första finns en betydande risk att en teknisk expert med hjälp av sin befintliga kunskap ”fyller i luckor” i den intervjuade personens beskrivning av hur saker och ting förhåller sig. Detta kan medföra att experten inte leder in intervjun på områden som skulle ha varit mycket viktiga för att få en korrekt bild av vad som faktiskt skett. För det andra kommer vetskapen om att intervjuaren är en teknisk expert sannolikt göra att den intervjuade personen avstår från att berätta vissa saker på grund av tveksamhet om sin egen kunskap och risken att visa sig tekniskt mindre kunnig än intervjuaren.

5.5 Missförstånd kan upptäckas vid sammanfattningen

Mot slutet av intervjun görs en sammanfattning där intervjuaren förklarar hur han uppfattat det som framkommit under intervjun. Vid sammanfattningen under intervjun med Peter upptäcktes ett missförstånd om hur lösenordshanteringen gått till. Intervjuaren hade trott att administratörerna delar användarnamn och lösenord med varandra men Peter har menat att varje administratör har använt sitt lösenord på flera servrar.

> *Intervjuaren – Om jag förstår det rätt då, så att när man då får reda på sina kollegors användarnamn och lösenord …*
> *…*
> *Peter – Du menar om jag skulle känna till hans ….,*
>
> *Interjuaren – Ja.*
>
> *Peter – Vi jobbar ju inte så då utan …. Eh Han har ju tagit hand om vissa burkar och jag om andra då …, vi har liksom inte delat med oss … lösenordet till varandra, direkt.*

Nyttan med en sammanfattning är alltså inte enbart att man kan få fram ny information utan att man dessutom kan upptäcka felaktigheter i det man tror sig ha hört och förstått. Det sistnämnda kan i och för sig också uppnås genom att man låter den intervjuade godkänna materialet från intervjun efteråt.

5.6 Att fråga vad den intervjuade personen anser är problemet

Genom att fråga vad den intervjuade personen anser är problemet kan man ha tur att få ett svar som är ganska rakt på sak och just det man är ute efter.

Även om det är viss improvisation i svaret nedan jämfört med rollbeskrivningen så kommer här ett exempel:

> *Intervjuaren – Nej. Tänkte om du skulle …, vad tycker du är .., vad anser du är problemet i det här, … det här angreppet då… vad skulle gjorts bättre från början? Bara …*
>
> *Bo – Jaa, det att man inte hinner … man hinner .. man kan inte vara på två ställen samtidigt. Man får prioritera saker och ting och då … de här säkerhetsgrejerna de kommer .., det är ju ingen som .. de ligger ju bara i vägen egentligen. Och de är det ingen som bryr sig om förrän det är någonting som har hänt. Och då får man inte tid till de sakerna.*

5.7 Information som inte framkommer

Eftersom det finns ett facit när man intervjuar inom ett konstgjort scenario så är det möjligt att jämföra hur mycket information som varje intervjuobjekt kände till med hur mycket information som framkom under respektive intervju. Vi tar intervjun med Walter som exempel, där dessa saker inte framkom:

- Det finns ingen speciellt utsedd IT-säkerhetsansvarig så därför har Walter den rollen indirekt i egenskap av IT-ansvarig. Hans uppfattning är dock att rollen ska vara fördelad mellan alla anställda eftersom var och en måste tänka på säkerheten inom sitt område.
- Walter har uppfattningen att det skulle ta för lång tid att göra en skriftlig IT-säkerhetspolicy och att den ändå inte skulle bli komplett nog eftersom det finns så många saker att tänka på.
- Anders står först i tur att få ta över som IT-ansvarig eftersom han visat sig väldigt ansvarsfull och noggrann. Därefter står Peter på tur.
- Domänadministratörskontot som angriparen kom över lösenordet till tillhör Bo.

De bägge första punkterna har relevans för vilka slutsatser som kan dras om bakomliggande orsaker till de uppkomna säkerhetsbristerna. Det faller sig ganska naturligt att detta inte framkommer i en första intervju med Walter eftersom de ligger på en nivå relativt långt ifrån de faktiska säkerhetsbristerna. I och med att det bara gjordes en intervju med varje person så uppkom aldrig fler naturliga möjligheter att få fram informationen i fråga. I ett verkligt fall är det mycket viktigt att man utför fler intervjuer med samma person(er) om man tror att det finns lösa trådar kvar som är värda att följa upp. Även om man fått fram en synbar förklaring till varför en viss säkerhetsbrist uppkommit är det viktigt att fråga sig om detta verkligen är en

grundorsak eller om förklaringen i sig i själva verket är en konsekvens av något annat. Självklart måste man nöja sig vid någon punkt utan att gå vidare bakåt i kedjan, men det är lämpligt att intervjua relevanta personer rörande de bakomliggande orsaker man tror sig hittat eftersom detta kan ge ytterligare uppslag. Enligt Grounded theory fortsätter man med intervjuer till dess de inte tillför något nytt utan bara bekräftar det man redan kommit fram till.

Den tredje punkten har redan behandlats (se 5.3). Den fjärde punkten visar sig inte spela någon roll eftersom samma uppgift framkommer i en senare intervju, och det är aldrig någon risk att man ska missa den eftersom den ligger längs en uppenbart ”röd tråd” i scenariot.

6 Erfarenheter från analyserna

Grounded theory kan inledningsvis upplevas som svår att använda för analys av intervjumaterial. Mycket av problematiken som uppstod under analysen grundade sig i frågeställningar avseende vad som är en händelse, koncept och kategori.

Analysen utfördes i samarbetsform mellan intervjuaren och en medanalytiker. Medanalytikern tillförde en djupare IT-kunskap vilket var syftet med att ha en medanalytiker. Intervjumaterialet fanns dokumenterat i ljudform vilket medanalytikern hade lyssnat igenom innan analysen påbörjades.

Det faktum att intervjumaterialet endast fanns i ljudform underlättade inte analysen. När händelser skall utkristalliseras är det en fördel om man har tillgång till ett skriftligt intervjumaterial. På så sätt kan man påvisa en händelse genom att stryka under de ord i intervjumaterialet som motsvarar den händelse man vill analysera.

Resultatet av att enbart ha tillgång till en ljudupptagning blev att både intervjuaren och medanalytikern gjorde koncept av händelserna innan de började diskutera dem. Detta medförde vissa kommunikationsproblem då försök gjordes att ”gå tillbaka” och finna händelser efter det att koncept, och i vissa fall även kategorier, hade specificerats.

Genom att utgå från ett skriftligt material, och därmed fysiskt kunna peka på en händelse, underlättas förloppet med att finna en händelse och konceptualisera denna.

Ett annat problem med analyserna var att de var relativt korta. De första analyserna inriktades mer på att definiera vad man vet om incidenten och vem som kan tänkas komplettera bilden av denna. Som en konsekvens av detta gjordes inte någon strikt analys enligt Grounded theory förrän efter ett antal intervjuer. Tyvärr är ett rikligare intervjumaterial från flera intervjuer inledningsvis inte till hjälp vid analys när man använder Grounded theory. Händelser, koncept och i viss mån kategorier bör specificeras efter varje intervju. Görs detta kan man diskutera koncept när man jämför intervjuer och placerar dessa koncept i kategorier. Händelserna i sig är oftast inte lämpade för en direkt jämförelse.

En kommentar från analysgruppen i övningsscenariot var att Grounded theory i och för sig var svårhanterligt men att det gav struktur åt analysen.

6.1 Slutsatser från analysen

En tydlig slutsats från analysen var att både intervjuaren och medanalytikern bör vara mer insatt i teorin bakom Grounded theory. Även om de inte inledningsvis har någon praktisk erfarenhet från att konceptualisera händelser, bör de vara väl bekanta med grunderna avseende händelse och koncept.

Som en konsekvens av svårigheterna med just Grounded theory utfördes, i alla fall inledningsvis, en mer traditionell analys enligt principen ”orsak och verkan”.

Under scenariot valde vi att ha en intervjuare med specialkunskaper inom intervjutekniker och en medanalytiker med djupare kunskap inom datalogi. Det finns inget som tyder på att detta är den mest lämpliga lösningen för ett tillförlitligt resultat. Om övningen skulle göras om vid ett annat tillfälle vore det lämpligt att prova en annan kombination, till exempel med en intervjuare med djupare kunskap inom datalogi. Syftet med en djupare kunskap redan på intervjustadiet är att undvika missförstånd som vid ett senare tillfälle uppdagas men är svårare på ett smidigt sätt korrigera. Ett annat alternativ är att använda båda personerna under intervjun, dock med ”den mer insatte” som passiv part i en understödjande roll.

7 Slutsatser samt fortsatt arbete

Så här långt har vi bland annat arbetat med idén bakom spårning och funderat över olika tillämpningar. Vi har förändrat vår uppfattning om tillämpningarna allt eftersom vi blivit medvetna om diverse begränsningar i form av brist på underlag kring verkliga incidenter, stor tidsåtgång för att utföra tillförlitlig spårning av många incidenter et cetera. Vi har också tagit fram ett ramverk som vi förfinat i flera steg, och utfört en spårning av bakomliggande orsaker inom ett konstruerat scenario för att testa vårt ramverk och våra idéer.

Vi har bland annat kommit fram till följande:

- För att kunna utföra spårning krävs tillräckligt underlag kring exempelvis inträffade incidenter i form av dokumentation, insatta personer att intervjua och så vidare. Det är ingen självklarhet att allt detta finns tillgängligt på en myndighet eller ett företag. En viktig framtida uppgift är att ta fram riktlinjer för vad som behöver dokumenteras inom en organisation för att man ska kunna utföra en spårning vid inträffade incidenter eller utifrån på annat sätt konstaterade säkerhetsbrister. Det mesta tyder på att det underlag som behövs inte överensstämmer med det som vanligtvis sparas. Även om man sparar material för att senare kunna polisanmäla en inträffad incident så betyder inte det att man har ett tillräckligt underlag för att utföra en spårning. Det material som är viktigt för en spårning av denna karaktär handlar framför allt om vad som inträffar fram till att en viss säkerhetsbrist uppdagas, medan det material som är viktigt vid en polisanmälan till största delen handlar om vad som inträffar först när en angripare utnyttjar denna säkerhetsbrist.
- Det går åt en hel del tid för att utföra spårning. Spårningen utifrån vårt konstruerade scenario tog ungefär en vecka för bara en enda incident. Vi hade ganska lätt att avtala intervjutider med de personer som spelade respektive roll. I praktiken skulle det antagligen dyka upp många hinder i form av personer som inte är tillgängliga när man behöver intervjua dem (man vet ju inte vilka som behöver intervjuas i god tid före i ett verkligt fall), som är upptagna med annat och är stressade och ovilliga att lägga tid på intervjuer, befinner sig på olika platser i landet och så vidare.
- Det finns många tänkbara anledningar till varför någon inte kan eller vill prata helt obehindrat under en intervju, och när detta inträffar bör man inte låsa sig helt vid det kognitiva konceptet utan exempelvis öka mängden frågor eller detaljnivån i frågorna för att få svar på det man undrar över.

- Det är viktigt att man, så långt möjligt, försöker bilda sig en uppfattning om vilka motiv de intervjuade personerna kan tänkas ha till att leda spårningen i en viss riktning. Dessa motiv behöver inte ha att göra med direkt skuld till en inträffad incident, utan kan exempelvis ha att göra med att någon är negativt inställd till förändringar och tror att en lyckad spårning kommer leda till förändringar i verksamheten.
- Även om man fått fram en synbar förklaring till varför en viss säkerhetsbrist uppkommit är det viktigt att fråga sig om detta verkligen är en grundorsak eller om förklaringen i sig i själva verket är en konsekvens av något annat. Självklart måste man nöja sig vid någon punkt utan att gå vidare bakåt i kedjan, men det är lämpligt att intervjua relevanta personer rörande de bakomliggande orsaker man tror sig hittat eftersom detta kan ge ytterligare uppslag. Enligt Grounded theory fortsätter man med intervjuer till dess de inte tillför något nytt utan bara bekräftar det man redan kommit fram till.
- Det är mycket viktigt att alltid försäkra sig om att intervjuaren och den intervjuade personen avser samma saker. Ett sätt att klarlägga vad som är vad kan vara att till exempel rita upp en skiss över hur nätverket är uppbyggt och rita in de olika datorerna. På samma sätt kan man göra med avseende på organisation och andra relevanta egenskaper hos det studerade objektet.
- En faktor som ökar risken för sammanblandning är om analysgruppen inte besitter tillräckligt detaljerad teknisk kompetens inom det berörda området. Man skulle i och för sig kunna tänka sig att använda sig av en teknisk expert som intervjuare men det kan ha minst två stora nackdelar. För det första har en teknisk expert normalt sett en mer eller mindre färdig bild av hur saker fungerar, eller i alla fall borde fungera. Det gör att det med största sannolikhet blir svårt att förhålla sig tillräckligt objektiv för att få fram vad den intervjuade personen anser har inträffat och vad det beror på. För det andra kommer vetskapen om att intervjuaren är en teknisk expert sannolikt göra att den intervjuade personen avstår från att berätta vissa saker på grund av tveksamhet om sin egen kunskap och risken att visa sig tekniskt mindre kunnig än intervjuaren.

Fortsatt arbete bör innefatta framför allt följande punkter:

- Ta fram riktlinjer för vad som behöver dokumenteras för att man ska kunna utföra spårning (se ovan)
- Göra försök med spårning på verkliga incidenter och resultat från intrångstester

Referenser

Bennet, Margo & Hess, John E.: “Cognitive Interviewing”, tillgänglig via http://www.totse.com/en/law/justice_for_all/coginte.html, besökt 21 februari 2003

Chalmers, Alan F.: *What is this thing called Science* (3rd edition), Hackett Publishing Company, Inc., 1999

Christianson, S-Å., Engelberg, E., Holmberg, U.: *Avancerad förhörs- och intervjumetodik*, Natur och kultur. Bokförlaget. (1998)

Eisenhardt, Kathleen M.: ”Better stories and better constructs: The case for rigor and comparative logic”, Academy of Management Review, vol. 16, no. 3, 1991, sid. 620-627

Eisenhardt, Kathleen M.: ”Building Theories from Case Study Research”, Academy of Management Review, vol. 14, no. 4, 1989, sid. 532-550

Elander (a), James: “Effects of misleading information and leading questioning”, 2001, tillgänglig via http://www.lgu.ac.uk/psychology/staff/elander/Effects.html, besökt 24 februari 2003

Elander (b), James: The Cognitive Interview, 2001, tillgänglig via http://www.lgu.ac.uk/psychology/staff/elander/Cognitive.html, besökt 24 februari 2003

Glaser, Barney G.: ”Conceptualization: On theory and theorizing using grounded theory”. International Journal of Qualitative Methods, 1 (2). Article 3. 2002, tillgänglig via http://www.ualberta.ca/~iiqm/backissues/1_2Final/html/glaser.html, besökt 7 februari 2003

Glaser, Barney G.: *Doing Grounded Theory: Issues and Discussions*, Sociology Press, 1998

Glaser, Barney G.: *Basics of Grounded Theory Analysis, Sociology Press*, 1992

Glaser, Barney G. & Strauss, Anselm L.: *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Aldine Publishing Company, 1967

Haig, Brian D: “Grounded Theory as Scientific Method”, 1995, tillgänglig via http://www.ed.uiuc.edu/EPS/PES-Yearbook/95_docs/haig.html, besökt 6 februari 2003

Holme, Idar H. & Solvang, Bernt K.: *Forskningsmetodik* (2:a utgåvan), Studentlitteratur, 1997

Lindskog, Stefan & Jonsson, Erland, *Different Aspects of Security Problems in Network Operating Systems.Proceedings of the Third Annual International Systems Security Engineering Association Conference* (2002 ISSEA Conference), Orlando, Florida, USA, Mars 13-15, 2002, tillgänglig via http://www.ce.chalmers.se/research/Security/Publications/pubs/lindskog_session5A.pdf, besökt 5 december 2003

Pandit, Naresh R: “The Creation of Theory: A Resent Application of the Grounded Theory Method”, The Qualitative Report, vol. 2, no. 4, 1996, tillgänglig via http://www.nova.edu/ssss/QR/QR2-4/pandit.html, besökt 6 februari 2003

Plewes, Louise: “A Grounded Thory Approach to Analysis of Interview Data from UCL’s TQEF ‘Learning Resources’ Project”, 2002, MS Power Point presentation, tillgänglig via http://www.ucl.ac.uk/epd/tqef/resources/cheri.ppt, besökt 5 februari 2003

Shaw, Eric D., Ruby, Keven G. & Post, Jerrold M.: *The Insider Threat to Information Systems: The Psychology of the Dangerous Insider*, Security Awareness Bulletin No. 2-98, september 1998

Stake, Robert E.: *The Art of Case Study Research*, Sage Publications, 1995

Strauss, A. & Corbin, J.: *Basics of qualitative research: Grounded theory procedures and techniques*, Sage Publications, 1990

Tellis, Winston: “Introduction to Case Study”, The Qualitative Report, volume 3, number 2, July, 1997, tillgänglig via http://www.nova.edu/ssss/QR/QR3-2/tellis1.html, besökt 24 januari 2003

Yin, Robert E.: *Case Study Research: Design and Methods* (2nd edition), Sage Publications, 1994

Yin, Robert E.: *Applications of Case Study Research*, Sage Publications, 1993

Appendix A – Scenariounderlag

A.1 SäkertOchBra AB:s rapport ”Utredning av intrång i arbetsstationer och servrar”

Angriparen hade raderat säkerhetsloggarna i alla arbetsstationer utom en. Efter genomgång av loggen kunde det konstateras att intrånget skett med hjälp av domänadministratörskontot ”terf72”. I och med att angriparen har haft tillgång till ett domänadministratörskonto har han eller hon kunnat komma åt alla filer även i domänens servrar. Säkerhetsloggarna i servrarna visar att angriparen varit inloggad i dessa över nätverket vid flera tillfällen, men eftersom ingen loggning av filåtkomst varit aktiverad så har vi inte lyckats avgöra exakt vilken skada som skett.

Vidare kunde vi konstatera att lösenordet på kontot ”terf72” var så pass starkt (”jms97zJN”) att i kombination med den aktuella konfigurationen av utelåsning av konton tycks det mycket osannolikt att angriparen lyckats komma över lösenordet direkt. Vi fick också reda på att ett par domänadministratörer kräver att få lokala administratörskonton på alla fristående servrar. Vid en kontroll upptäckte vi att administratören med konto ”terf72” alltid har använt samma användarnamn och lösenord som han haft till sitt domänadministratörskonto. Efter analys av dessa servrar kunde vi konstatera att det inledande intrånget skett i en gammal oanvänd fristående server via webbserverprogramvaran IIS4. Denna hade inga uppdateringar utförda och angriparen hade tagit sig in via ett känt hål i RDS. Därefter har angriparen sannolikt utfört lösenordsknäckning på SAM-databasen för att få fram lösenordet till kontot ”terf72”.

A.2 Rollbeskrivningar

Anders (Domänadministratör)

Det var du som utförde intrånget i fråga. Du visste att Walter skulle sluta och ville försäkra dig om att ledningen skulle se dig som mer lämplig som efterträdare än Bo och Peter. Bo är redan ute ur spelet men Peter kan fortfarande vara aktuell så därför vill du misskreditera honom under intervjun om det går. Du vet att utredningen av intrånget är avslutad och att den här intervjun ingår i någon form av forskningsprojekt. Därför är det inte så sannolikt att intervjuaren kommer avslöja att det var du som utförde intrånget, men det är säkrast att du är försiktig med vad du säger i alla fall. Om du lyckas få

intervjuaren att tro på negativa saker du säger om Peter kanske det når ledningen och det vore bra för dig.

Din inställning ska vara att intrånget var väldigt onödigt. Du har länge försökt rycka upp säkerheten men det är inte så lätt att få gehör alla gånger. Det är ingen hemlighet att du antagligen kommer bli ny IT-ansvarig när Walter slutar. I så fall kommer du definitivt ta itu med ett och annat, till exempel skriva en ordentlig IT-säkerhetspolicy.

Du förväntar dig att intervjuaren inte talar om att det här kommer från dig, men du ”vet” att Peter krånglade till det med den automatiska uppdateringen av antivirusprogrammen. Han konfigurerade om brandväggen så att uppdateringen slutade fungera i några veckor innan han upptäckte att något var fel. Det är inget han kommer erkänna för han vill ju inte få skulden för det som hände, men du ”är övertygad” om att det var då den där hackern lyckades ta sig in i en av arbetsstationerna genom att skicka in en trojan i ett e-mail. Det är viktigt att intervjuaren tror att Peter slarvar med allt möjligt mest hela tiden men alltid hinner dölja det som går galet innan någon annan upptäcker det.

Du ska inte verka ha något emot att bli intervjuad men var försiktig med vad du säger och säg så lite som möjligt. Det viktigaste är att misskreditera Peter på ett diskret sätt och dessutom får dig själv att verka pålitlig. Om du får frågor om annat än vad som berörs här så svara att du inte vet eller inte tänkt på det, förutom om frågorna har uppenbara svar.

Övriga personer som du känner till och kan hänvisa till:

- Peter (Ansvarig för bland annat brandvägg och antivirusprogram)
- Bo (Administratören med kontot terf72)
- Anders (Domänadministratör)
- Walter (IT-ansvarig)

Bo (Administratören med kontot terf72)

Det är ju inte så lätt att komma ihåg en massa olika lösenord. Därför brukade ni använda samma lösenord så mycket som möjligt. Såklart valde ni bra lösenord och det gör dem ju ännu svårare att komma ihåg. Du kommer inte ens ihåg när du installerade den fristående servern men du gjorde likadant på den som ni alltid gjorde förut. Alla utom Anders förstås. Han var tydligen den ende som alltid valde olika lösenord på varje dator han installerade. Det har blivit krångligare nu när ni har olika lösenord överallt, men inte så farligt som du hade trott att det skulle bli.

Egentligen finns det väl inte så mycket mer att säga om det som hände. Du är inte så pigg på att prata om det för du fick en rejäl utskällning av Walter efteråt och han verkar fortfarande vara arg på dig. Han klagar på dig för att ni inte loggade vilka filer som användes av olika användare på servrarna. Nu gör ni det men loggarna roterar så snabbt, eftersom det genereras så fruktansvärt mycket information, att det blir meningslöst med loggningen. Men Walter är ju i alla fall nöjd.

Du är inte speciellt pigg på att samarbeta längre för du tror att Walter är ute efter att peka ut dig som en ännu större syndabock. Om du får frågor om annat än vad som berörs här så svara att du inte vet eller inte tänkt på det, förutom om frågorna har uppenbara svar.

Om du får frågor om central loggning så säg bara att du tycker att det är Walters uppgift att ta itu med det. Säg inget om det om du inte blir tillfrågad.

Övriga personer som du känner till och kan hänvisa till:

- Peter (Ansvarig för bland annat brandvägg och antivirusprogram)
- Bo (Administratören med kontot terf72)
- Anders (Domänadministratör)
- Walter (IT-ansvarig)

Peter (Ansvarig för bland annat brandvägg och antivirusprogram)

Du jobbar egentligen mest som vanlig administratör. Antivirusprogrammen uppdaterar sig automatiskt över Internet med jämna mellanrum (tillräckligt ofta) och brandväggen behöver inte konfigureras om mer än några få gånger per år. Bägge delarna har fungerar perfekt hela tiden du jobbat här.

Du tycker att intrånget i fråga var väldigt konstigt. Konsulten från SäkertOchBra AB som utredde det kom fram till att någon hackat sig in i en fristående server och knäckt Bos konto där. Ni hade aldrig tänkt att någon skulle kunna ta sig in på ert interna nät i och med att ni har både brandvägg och antivirusprogram överallt. Du brukade själv lägga in ett konto med samma lösen som till ditt domänadministratörskonto varje gång du installerade fristående servrar förut. Det var inget du ens reflekterat över egentligen. Domänadministratörslösenordet går ju ändå att använda i hela domänen så det föll sig naturligt att det skulle gå att använda i de fristående servrarna också. Numera använder du olika lösenord överallt och skriver upp dem på en lista som du förvarar inlåst i ett skåp. Walter sa åt er på skarpen att absolut inte använda samma lösen på flera ställen efter att intrånget uppdagats.

Det du tycker är riktigt konstigt är hur hackern kunde ta sig in på ert interna nät. Konsulten hade ingen ordentlig förklaring på det men menade att det antagligen varit genom någon specialskriven trojan som inte antivirus-programmet upptäckt. Konsulten lyckades få fram vilken dator som använts för att hacka den fristående servern, men tyvärr gick det inte att få fram något ur den eftersom den hade blivit ominstallerad precis innan utredningen inleddes.

Du är allmänt öppen och berättar gärna om det du vet. Om du får frågor om annat än vad som berörs här så svara att du inte vet eller inte tänkt på det förutom om frågorna har uppenbara svar.

Om intervjuaren uttryckligen frågar varför ni inte till exempel skickar alla loggar till en central loggserver så ska du svara att du tänkt på det flera gånger men att du inte tror den funktionen finns i Windows. Däremot ska du inte säga något om det om du inte blir tillfrågad.

Övriga personer som du känner till och kan hänvisa till:

- Bo (Administratören med kontot terf72)
- Anders (Domänadministratör)
- Walter (IT-ansvarig)

Tommy (Ansvarar för den fristående servern)

När intrånget skedde använde ni inte ens den fristående servern längre. Den installerades för länge sedan. Ni använde den senast i ett projekt som tog slut ett par månader före intrånget och efter det lät ni den stå kvar ifall ni skulle ha nytta av den senare. Att installera uppdateringar var det ingen som tänkte på och SAG (SystemAdministratörsGruppen) hjälper ju bara till med det om man uttryckligen ber dem. Du hade aldrig en tanke på att servern skulle behöva uppdateras. Du vet ju att det finns hackers men du trodde att de alltid gissar lösenord för att ta sig in i datorer. Det är det enda sättet att ta sig in i en dator som du sett - att man anger ett lösenord.
Du vet faktiskt inte så mycket om vad som hände. Alla i din grupp är webb-designers och kan inget om säkerhet. Tydligen hade hackern tagit sig in i något som hette RGS eller RGF eller något i den stilen. Du har ingen aning om vad det är.

Du har inget emot att berätta om allt du vet men du vet tyvärr inte så mycket. Om du får frågor om annat än vad som berörs här så svara att du inte vet eller inte tänkt på det förutom om frågorna har uppenbara svar.

Övriga personer som du känner till och kan hänvisa till:

- Walter (IT-ansvarig)

Walter (IT-ansvarig)

Du är IT-ansvarig inom organisationen. Någon speciellt utsedd IT-säkerhetsansvarig finns inte så du har den rollen också, men tycker att den ska vara fördelad mellan alla anställda. Var och en måste ju tänka på säkerheten inom sitt område.

Ni har 75 arbetsstationer och 8 servrar i en Windowsdomän. Dessutom finns det ett antal fristående servrar som används inom enskilda projekt. Man kan få hjälp av någon i SAG (SystemAdministratörsGruppen) med installation och drift av en fristående server eller så kan man sköta det själva inom projektet. I SAG jobbar bland andra Bo, Anders och Peter.

Om ett halvår kommer du sluta på ditt nuvarande arbete och börja på DataKonsultFöretaget AB istället. Just nu lutar det åt att Anders kommer ta över efter dig. Han har visat sig väldigt ansvarsfull och noggrann. Om inte det blir han så blir det antagligen Peter.

I det aktuella fallet hade någon tagit sig in i en fristående server, som används i ett projekt som Tommy ansvarar för, och fått fram lösenord ur kontodatabasen. Ett av kontona var ”terf72” och det tillhör Bo. Han hade hjälpt till med installationen och då hade han lagt till ett lokalt administratörskonto åt sig själv med samma lösenord som han använde till sitt domänadministratörskonto. Du vet inte exakt hur hackern tagit sig innanför brandväggen men det borde Peter kunna svara på.

Ni har ingen nedskriven IT-säkerhetspolicy. Däremot finns en person som sköter brandväggen och antivirusprogrammen, nämligen Peter. I Windowsdomänen har ni ett rullande schema där varje administratör ansvarar för installation av säkerhetsuppdateringar en vecka i taget. Dessutom har ni ett filter som gör att man inte kan välja allt för dåliga lösenord i Windowsdomänen. Det har alltid räckt förut - ni har inte haft några intrång förutom i en extern webbserver ett par gånger. Att göra en ordentlig nedskriven IT-säkerhetspolicy skulle ta mycket mer tid än du tycker dig ha till ditt förfogande, och dessutom anser du att den ändå inte skulle bli komplett nog. Det verkar ju finnas tusentals saker att tänka på.

Konsulten på SäkertOchBra AB som utredde intrånget har flyttat utomlands och går inte längre att få kontakt med för att få reda på mer information.

Du är allmänt öppen och berättar gärna om det du vet. Om du får frågor om annat än vad som berörs här så svara att du inte vet eller inte tänkt på det, förutom om frågorna har uppenbara svar.

Övriga personer som du känner till och kan hänvisa till:

- Peter (Ansvarig för bland annat brandvägg och antivirusprogram)
- Tommy (Ansvarar för den fristående servern)
- Bo (Administratören med kontot terf72)
- Anders (Domänadministratör)

Appendix B – Intervjuutskrift

B.1 Intervju 1 - Utredaren (U) och Walter (W)

U	OK. Då får jag. Vad … öh .. Vad heter Du?
W	Ja, jag heter Walter.
U	Och vad har Du för befattning på det här företaget, Säkert och Bra.
W	Jag ska, jag är IT-ansvarig inom organisationen.
U	Ja, öh och ja, det här intrånget som har uppkommit, vad…, vad vet du om vad som har hänt.
W	Ja, vi satte ju till en utredning som skulle göras av en extern konsult för att vara säker på att inte någon, att det ska bli en helt opartisk utredning. Och det var en firma som heter Säkert och Bra, som du kanske hört talas om, som skulle göra det här och de kom med en mycket kort rapport om vad som hade hänt.
U	Ja, öh …
W	Däremot sa de egentligen inte särskilt mycket om varför eller hur det hade gått till.
U	Nej, nej, precis. De konstaterade bara vad exakt som hade hänt.
W	Ja det är ju intressant i och för sig men ….
U	Ja.
W	Men vi är inte särskilt hjälpsamt när man ska försöka säkra upp systemet.
U	Nej. Men kan Du berätta lite om det här företaget som Du är IT- ansvarig på.
W	Ja. Det är ju ett medelstort företag och vi har 75 arbetsstationer och 8 servrar uppkopplade i en Windows-domän. Och utöver de här 8 servrarna finns det ett antal fristående servrar också som används för enstaka, speciella projekt och sådant.
U	Ja ... De här 75 arbetsstationerna. Är det 75 anställda på företaget också totalt?
W	Ja ungefär så. En del har tillgång till upp till .. flera arbetsstationer, men

	ungefär så.
U	De här fristående servrarna och de fristående arbetsstationerna är det …. p.g.a. säkerhetsaspekter som man har frikopplat dem från …
W	Ja, man kan göra prov och försök och andra sådana saker, som man inte vill ska vara, vara åtkomliga från alla håll. Utan, därför att de andra servrarna är ju tillgängliga på nätet.
U	Mm.. Vad jobbar företaget med? Vad sysslar ni med för någonting?
W	(Jag kan ju inte gärna svara, att det vet jag inte.) Men …, vi är ett allmänt service och handelsföretag.
U	Ja. Och, om man då utgår från den här incidenten då som har hänt. Vad .., om Du skulle berätta lite om vad du anser, problem… eller vilka personer har varit inblandade, vi kan börja med det.
W	Ja, de personer som sysslar med IT-frågor menar du?
U	Mm …
W	Ja. Jag har då ett antal medarbetare här Peter som då sysslar med brandväggen och antivirusprogram och skyddsfunktioner för vårt nätverk. Den server som så att säga är skulden till det här, den sköts av kille som heter Tommy och sedan så har vi då ett par administratörer Anders och Bo som är administratörer för…, för nätverket.
U	Det är alltså 4 personer som är inblandade att arbeta med …
W	Ja, som var och en antagligen vet mer än vad jag gör så att säga, som är experter på …, inom respektive område.
U	Ja. Kan det finnas någon annan som skulle kunna ha, inneha information om vad som har hänt?
W	Det vet vi inte i dagens läge…. Det är väl lite din uppgift att försöka räkna ut det. Men för ögonblicket, nej.
U	Tänkte det här…, den angripen som då varit inne och raderat de här säkerhetsloggarna. Vad…, när upptäckte man, vad som hade hänt och när?
W	Det var ungefärligen fyra veckor sedan.
U	Och hur tidigt blev den här konsulten från Säkerhet och Bra AB klar med sin utredning?
W	Ungefär en två veckor, höll de på med det.

U	Ja. Och det är alltså ungefär fyra veckor från och med nu som det här intrånget uppdagades och sen så, och två veckor efter det så, så blev det …. Det har alltså gått två veckor sedan den här Säkert och Bra AB blev klar med sin utredning.
W	Ja. Man kan säga att det dröjde väl några dagar naturligtvis innan vi kom underfund med att vi behövde engagera en utomstående konsult, så att det var väl drygt en vecka sedan som vi fick Säkert och Bra:s utredning och därefter så konstaterade vi att du behövde komma in i sammanhanget för att hjälpa oss vidare.
U	Ja. Tänkte å företagets vägnar hur allvarlig är den här incidenten, hur kan det påverka er verksamhet och ….
W	Ja det är det som vi egentligen inte vet. Vi vet ju inte vad den här inkräktare har gjort på de olika servrarna. Och han har raderat säkerhetsloggarna. Så vi vet ju inte med säkerhet. Men för ögonblicket så rullar systemet och går. Men vi kan ju inte så att säga riktigt lita på databaser och annat sådant.
U	Nej.
W	Vi jobbar, men vet inte hur tjock isen är som vi går på.
U	Nej och ni vet inte om det rör sig om…, alltså om det är någon som har gjort det bara för att det är roligt att tränga sig in i systemet eller om det kan vara någon, om det kan röra sig om något företagsspioneri eller motsvarande?
W	Om den här personen kommer… ja. Det kan vara det. Det kan vara det. Det kan också naturligtvis vara ett sabotage och i så … någon som utifrån eller inifrån som vill skada företaget. Bara liksom att orsaka en sänkning av systemet eller bristande tilltro till systemet kanske snarare.
U	Mm. Vilka personer skulle kunna tjäna på något sådant här?
W	Kan var någon som har fått … slutat, någon anställd, som fortfarande är anställd som är missnöjd med någonting, eller som vill diskreditera någon annan på …, för att själv få en bättre ställning i organisationen. Det är ju känt nu att jag kommer att sluta här inom …, om ett halvår ungefär. Och det är flera stycken som naturligtvis är intresserade av att bli IT-ansvarig.
U	Mm.
W	Det kan ju finnas en viss konkurrens mellan några stycken personer här.
U	Och anledningen till att Du slutar, har det något med den här incidenten att göra?

W	Nej, nej. Det har varit bestämt sedan ganska länge tillbaka. Jag ska börja på ett datakonsultföretag. Eller ett annat sådant rättare sagt. Men det är helt klart mellan mig och företaget ingen konflikt om den saken.
U	Nej. Tänkte, de här personerna Peter, Tommy och Anders och Bo.
W	Mm.
U	Har vi tillgång till att rycka dem från sina tjänster för att genomföra liknande intervjuer med dem, när vi anser att vi behöver det?
W	Ja det är självklart, det måste du kunna göra.
U	Ja. Det är jättebra. Eh …
W	De vet att Du ska komma och titta på det här, så de är nog… de är beredda på att du kommer.
U	Ja, och det är ingenting annat som, du har ingen …, någon maggropskänsla själv på vad som du anser skulle kunna va … kunna leda in utredningen in i rätt riktning, för om du skulle ha suttit i den som ska genomföra analysens kläder. Vart skulle du ha riktat din uppmärksamhet någonstans?
W	Jag skulle tittat, som du gör här, övergripande först, jag tycker att det är helt fel att bestämma sig för att det kan var, att det är troligen det här och sedan då kommer man sannolikt fel. Det är inte någon sådan här uppenbar…, uppenbart att det måste så att säga vara någon speciell person och så vidare. Anledningen till att det här har hänt är ju i ..., att den här servern, den fristående servern som han angrep, inte var uppdaterad den hade stått oanvänd under ganska länge och …, av antagligen slentrian så hade man inte patchat upp den så den var säker ordentligt. Vi får ju in sådana rapporter om säkerhetshål och annat och det ankommer naturligtvis på administratörerna att lägga in de säkerhetspatchar och annat så att …, men det hade man alltså missat på den här maskinen, eftersom den inte var aktiv under ett slag. Sen när den sattes igång så, så var det väl ingen som tänkte på det, som det ibland brukar bli .. hända.
U	Mm.
W	Och då var den inte särskilt svår att komma åt.
U	Nej.
W	Däremot, den kan alltså varit åtkommen utifrån. Den kan naturligtvis ha accessats för det här ändamålet inifrån nätet också.
U	Den har stått ingång och gått hela tiden då så att….

W	När vi upptäckte felet på den så har den stängts av.
U	Ja. Jag tänkte på …, ska se …
W	Vad jag skulle göra. Om man nu ska så att säga ska ge dig några råd. Så är det naturligtvis intressant att titta på brandväggen och loggarna där. De finns såvitt vad jag förstår kvar. Så att man kan, om möjligt, spåra var …, om intrånget har gått via brandväggen. Kan man hitta någonting i de loggarna så kan det vara en god hjälp. Och den som du ska prata med i det sammanhanget det är Peter då som kan brandväggskonfigurationen bäst av alla.
U	Ja.
W	Om det visar sig att det inte kommit den vägen, så är det väl tänkbart att det kommit inifrån.
U	Mm…. Ja, men, det är bra. Då kan jag bara kort sammanfatta det du har sagt nu så jag har förstått allting rätt och …. Företaget då som ni har anlitat heter Säkerhet och Bra AB och de har…, hur länge jobbade de som konsulter på det här uppdraget för att spåra eller göra de spårningar som man kunde göra?
W	De jobbade ungefär i två veckor och de kunde ju då tala om vad som hade hänt, och hur det hade gått till. En väldigt kort …, kort rapport och … jag tycker också att du naturligtvis ska prata med Tommy, som då är den som är ansvarig för den här angripna servern och se om man där kan … få fram någon, några loggar ur den. Vad jag har förstått så, loggarna på de enskilda maskinerna, arbetsstationerna alltså, de har raderats i alla fall utom ett. Men servrarna har man inte gjort det på, vad jag har förstått.
U	Nej.
W	Så att där … Och de loggarna från servern vad man kan få fram där, körda mot loggarna på brandväggen kan möjligtvis ge en indikation på varifrån angreppet har kommit. Däremot kan det vara en insider som har kommit…, gått utifrån, så det kan …, men det kan bli en god hjälp i alla fall.
U	Ja. Och den här utredningen … förlåt
W	Ja, ja samtidigt … så bör du naturligtvis också prata med den administratör som hade det här kontot som …, han hade samma lösenord och samma konto på den här servern som han har på själva winsystemet, och … vilket naturligtvis inte är så där jättebra. Men, så du bör när du pratar med både Bo och Anders också och jämföra deras beskrivningar av hur det hela sammanlagda systemet fungerar. De ser det ur lite grann …, lite grann olika synpunkter.
U	Mm

W	Intressant är ju också att veta vilka som …, om de kan varandras lösenord exempelvis, vilket de inte borde behöva kunna. Men det ingår naturligtvis självklart i den utredning som du gör.
U	Precis.
W	Det brukar vara en sådan där standardfråga.
U	Det är ingenting i den här utredningen som Säkerhet och Bra AB har…, som de har gjort som verkar ologisk eller på något sätt …
W	Det var ett slag sedan …, jag ska just titta på det, vi ska titta på det här så får vi se om det …. (paus) En sak som du kanske skulle också diskutera med de här administratörerna är att Säkert och Bra påstår att olika domänadministratörer har bett att få konton på alla servrar, även om de, så att säga inte har …, även de servrar som de inte själva är ansvariga för i första hand. Och det kan vara intressant att veta varför, om det finns något vettigt skäl till detta va. I övrigt så, sakförhållandena som de redovisar förefaller ju att vara rimliga**.**
U	Mm.
W	Om än inte bra, så vet man så här brukar det många gånger gå till i praktiken.
U	Ja. Mm. Nej. Då tror jag faktiskt att jag har fått den informationen nu som jag behöver tills vidare och om det nu skulle vara att …
W	Kan vi säga att om du på servarna finner att det inte finns några, några …, att loggarna inte visar egentligen några intrång, vilket är ganska tänkbart, så .... Men det förutsätter att du kollar om det finns några bakdörrar om man lagt in några trojaner eller någonting sådant. Det är inte alls omöjligt att man har tagit sig in via det här kontot ter 72 och sedan lagt in en bakdörr och sedan ser man inte vilka ytterligare accesser man har gjort i maskinen. Det förutsätter jag att du kollar.
U	Mm. Under den här utredningens gång nu, så kommer jag ju att ta kontakt med de här, ja först då de här fyra personerna som du har nämnt …
W	Mm.
U	… och sen om det skulle framkomma någon ytterligare information som gör att jag behöver kontakta dig igen, så ..., har jag möjlighet att göra det då?
W	Så är du hjärtans välkommen.
U	Tackar.

W	Det här måste vi ju reda ut, och så att vi kan lita på systemet i fortsättningen och framförallt hitta vad, vad var det som gick fel, egentligen.
U	Precis. Ja då får jag tacka så mycket för nu.
W	Du är välkommen tillbaka.
U	Ja, tack.
W	Tack ska du ha.

Appendix C – Planeringsmall

Denna planeringsmall kan användas som stöd när ramverket skall utnyttjas för spårning av bakomliggande orsaker till att en säkerhetsbrist har uppkommit.

C.1 Initiering och bakgrund

Under initieringen ligger fokus på att definiera säkerhetsbristen och dess konsekvenser. Här sker även den första kontakten med den organisation som har säkerhetsbristen.

Den person som är utsedd till kontaktperson för organisationen är den första intervjupersonen. Kontaktpersonen fungerar även som en guide i organisationen.

Frågor som kontaktpersonen kan svara på, eller tala om var man kan få svar, är till exempel:

- Säkerhetsbristen
  - Beskrivning av säkerhetsbristen
  - Säkerhetsbristens konsekvenser
- Organisationen
  - Organisationsstruktur
  - Roller
  - Formell ansvarsfördelning
- Dokumentation
  - Organisation
  - Infrastruktur

Spårningsgruppen bör efter instudering och en första intervju med kontaktpersonen ha en övergripande förståelse för hur organisationen, vilka roller som finns, samt om säkerhetsbristen och dess konsekvenser.

Gruppen skall även här besluta vem som skall intervjuas först.

C.2 Intervjuer

För att en intervju skall bli innehållsrik och uppriktig är behovet av en avslappnad miljö viktigt. Val av lokal och tidsuttag påverkar intervjuresultatet. Likaså spelar intervjuaren en nyckelroll för resultatet.

Under de första faserna av den kognitiva intervjun lägger intervjuaren ramen för intervjun. Intervjuaren anger vad som är fokus för intervjun och kontrollerar med den intervjuade att han/hon har samma uppfattning.

Huvudsyftet med en kognitiv intervju är att den intervjuade själv skall berätta så mycket som möjligt och att intervjuaren endast skall fungera som stöd. Några få, öppna och endast grovt riktade frågor lämnar mycket utrymme för den intervjuade att svara efter egen förmåga.

Intervjuaren bör i det längsta undvika direkta frågor. Att be den intervjuade svara på samma typ av fråga en gång till, fast i ett annat perspektiv, ger ofta ett mer innehållsrikt svar än en riktad fråga.

Summeringen är intervjuarens kontrollskott. Här kontrollerar intervjuaren att han/hon har förstått vad den intervjuade har berättat, samt ger den intervjuade möjlighet att komplettera med förtydliganden eller ny information.

C.3 Analys

Analysen underlättas i storgrad av ett utskrivet intervjumaterial. En utskrift medför att man exempelvis kan markera händelser med en överstrykningspenna. En händelse är något konkret vilket kan markeras.

Utifrån de understrykningar man har gjort i en utskrift skapas koncept av varje händelse. Ett koncept beskriver en händelse, vilket i praktiken innebär att man med ett fåtal ord skriver ner vad man uppfattade som en händelse.

Ett exempel på en händelse (hämtat ur övningsscenariot) är: *...rutiner det alltså, det är ytterligare en sådan sak som man vet att man måste göra och försöker att få tid till, men det blir kanske lite ad-hoc mässigt* (från intervju med Bo). Ur denna händelsen kan man göra flera koncept, såsom *dåligt med tid att utföra sina uppgifter* och *ad hoc-mässiga rutiner*. Vid en annan intervju framkom händelsen *Vi har ingen egentlig IT-säkerhetspolicy* (Anders) vilken konceptmässigt kan beskrivas som både *saknar IT-säkerhetspolicy*, men även *bristande rutiner*. Sammanfogar man koncepten *ad hoc-mässiga rutiner* och *saknar IT-säkerhetspolicy* får man en kategori som man kan kalla för *Bristande rutiner*. Det finns fler händelser/koncept i dessa intervjuer, men även i andra, som kommer att hamna i denna kategori.

När analysgruppen har specificerat händelser och koncept samt eventuella kategorier avgör man vem som skall intervjuas härnäst.

C.4 Rapport

Efterhand som man utfört de intervjuer man anser nödvändiga samt analyserat dessa, var för sig och tillsammans, bör analysgruppen funnit den bakomliggande orsaken till att bristen uppstått. Hur resultatet rapporteras beror givetvis på hur uppdragsgivaren vill ha det.

Som några generella regler för rapportering kan sägas att rapporten, det vill säga de som författat den, ansvarar för att ingen information i rapporten är kränkande för de inblandade. Direkt användning av namn på personer är olämpligt, även om en läsare i praktiken kan räkna ut vem som avses genom att ha kunskap om organisationen. Det bör dock påpekas att syftet med en spårning är att finna den bakomliggande orsaken till att en brist har uppstått så att man kan åtgärda den och därmed undvika att en liknande brist uppkommer igen.