

TSIT01 Datasäkerhetsmetoder

Föreläsning 2: Att mäta säkerhet, riskanalys, projekten, exempel på analys

Ingemar Ragnemalm

01001001 01000011 01000111

Förra gången

Prevention - detection - reaction

CIA = Confidentiality, Integrity, Availability

Denna föreläsning

Lite mer om risk och skada: Att mäta säkerhet

Projekten

Exempel på säkerhetsanalys

01001001 01000011 01000111

Föreläsningsfrågor (teasers)

1. Vad är skillnaden på risk och hot?
2. Hur bestämmer vi om en åtgärd är värd att göra?
3. Vad för slags angripare är exemplet Lewis Avery Filer?
4. Hur kan 0.1% sannolikhet för en kärnkraftsolycka vara allvarlig?

01001001 01000011 01000111

Prevention - detection - reaction

Tre olika sätt att bemöta hot

Hur hindrar vi det?

Ser vi att det händer? Kan vi se till att vi ser det?

Vad gör vi när skadan är skedd? Hur reparerar vi?

01001001 01000011 01000111

Confidentiality - Integrity - Availability

Ett sätt att analysera en situation ur flera vinklar. Vilka hot finns?

Vad behöver hållas hemligt?

Är det känsligt att informationen är korrekt?

Vilka behöver komma åt informationen? Vilka kan?

01001001 01000011 01000111

Åtgärder

Baserat på CIA-analysen, vilka åtgärder kan göras?

Följdfråga: Hur bestämmer vi vilka som är lämpliga?

Detta för oss till frågan: Hur mäter vi säkerhet!

01001001 01000011 01000111

Att mäta säkerhet

01001001 01000011 01000111

Att mäta säkerhet

Sätt ett numeriskt värde på säkerheten. Värdet är svårt att mäta!

Hur trolig är skadan?

- Antal öppna portar
- Antal användare (med svaga lösenord)
- Antal uppdaterade program

Hur allvarlig är skadan?

- Förlorade resurser
- Kostnaden är återställning (i pengar eller mantimmar)
- Förlorat rykte

Vad kostar åtgärderna för att hindra skadan?

01001001 01000011 01000111

Riskanalys, grundläggande egenskaper

Tre egenskaper måste finnas för att risk skall finnas:

- Hot - orsaken till den möjliga skadan
- Svagheter - den oönskade systemegenskapen som möjliggör hotet
- Skada - den oönskade händelsens effekt

01001001 01000011 01000111

Exempel, grundläggande egenskaper

Stöld av en ficktjuv är en risk för dig enligt:

- Hot: Ficktjuvar
- Svaghet: Plånboken, dess placering
- Skada: Förlust av plånboken

Hotagent = ficktjuven

Hotobjekt/tillgång = plånboken

01001001 01000011 01000111

När vi snackar ficktjuvar...

"Pickup at South Street"

BILDER BORTTAGNA

01001001 01000011 01000111

Pickup at South Street

Tredubbla hot: Ficktjuv, spion med mikrofilm, poliser på jakt efter... vem?

Multipla *threat agents* (*hotagenter*).

Vilka skall vi bry oss om? Det beror på vem vi gör analysen för.

Vi återkommer till detta fall för analys!

01001001 01000011 01000111

Egenskaper hos hot

Ett hot orsakas av en *hotagent*, en *threat agent*

(Oskarsson kallar threat agents för "hotobjekt". Jag håller inte med.)

Olyckor: agenter utan specifikt mål. Åska mfl katastrofer hot mot *tillgänglighet*

Avsiktliga agenter: individuellt varierade mål

Varje agent har individuella resurser, tid, datorkraft, kunskap...

Agenter har varierande sannolikhet att angripa ditt system.

01001001 01000011 01000111

Nästa exempel: Lewis Avery Filer

BILDER BORTTAGNA

Lewis Avery Filer (Hume Cronyn), Hawaii 5-0

01001001 01000011 01000111

Insiders

En illvillig anställd är ett hot (t.ex. mot finanser) genom angrepp mot dataintegritet mm

Den anställde har intern systemkunskap och kan få tag i mer

BILDER BORTTAGNA

Den f.d. anställde då...?

(Die Hard 4, Hawaii 5-0)

Vem är Lewis Avery Filer ett hot mot?

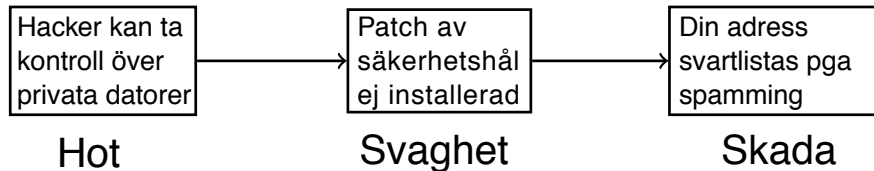
01001001 01000011 01000111

Identifiera svagheter (vulnerabilities)

Svagheter är egenskaper hos ditt system

En svaghet kan existera inuti systemet eller i dess omgivning

Om en svaghet åtgärdas kan det specifika hotet inte längre orsaka skada, eller sannolikheten minskar



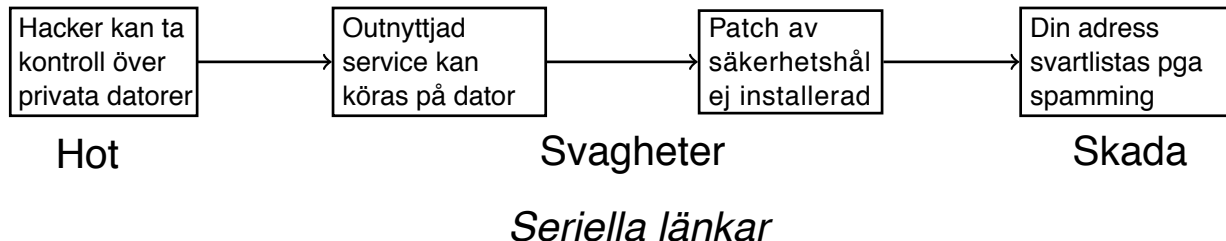
01001001 01000011 01000111

Egenskaper hos svagheter

Svagheter bildar ofta en kedja av steg från hot till skada

Stegen kan vara parallella, vilken som helst av dem kan öppna till skadan, eller seriella, alla behövs

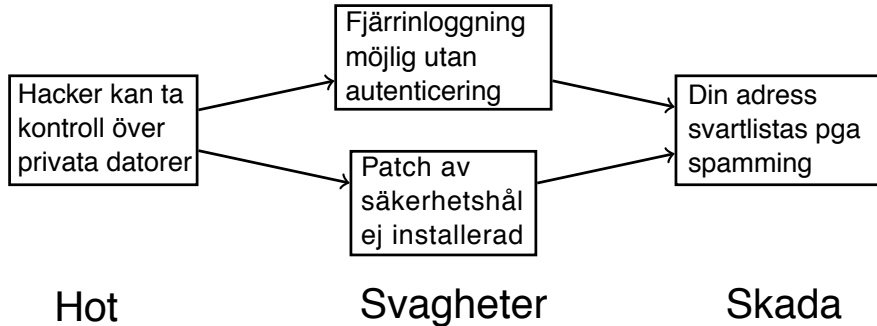
Det räcker att ta bort en seriell länk, men med parallella måste alla åtgärdas



01001001 01000011 01000111

Egenskaper hos svagheter

Med parallella länkar måste *alla* åtgärdas



Parallella länkar

01001001 01000011 01000111

Strikt riskanalys

Uppskatta möjlig skada och magnituden hos hotet. Finn kostnaden, är det motiverat att eliminera svagheten?

Billigare med åtgärder i efterhand (återställning) än att eliminera svagheten?

Lönar sig en åtgärd, ekonomiskt? Minskas skadan mer än kostnaden?

01001001 01000011 01000111

Kvalitativ riskanalys

Uppskatta kvalitativt magnituden av skadan

- Försumbar?
- Hanterbar?
- Allvarlig?
- Katastrofal?

Uppskatta sannolikheten

- Nästan omöjligt?
- Möjligt?
- Troligt?
- Oundviklig?

01001001 01000011 01000111

Kvalitativ riskanalys

Markera uppskattningen i ett rutnät

Katastrofal				
Allvarlig				
Hanterbar				
Försumbar				
	Nästan omöjligt	Möjlig	Trolig	Oundviklig

01001001 01000011 01000111

Kvalitativ riskanalys

Hantera händelser i prioritetsordning

Katastrofal				
Allvarlig				
Hanterbar				
Försumbar				
	Nästan omöjligt	Möjlig	Trolig	Oundviklig

Men nu måste vi gå vidare med en *kvantitativ* prioritering!
Hur stor är t.ex. sannolikheten?

01001001 01000011 01000111

BILDER BORTTAGNA

så fort det hade hänt rakade ju sannolikheten upp till inte mindre än 100 procent så det var nästan sant att det hade hänt.

men bara nästan sant...

01001001 01000011 01000111

Exemplet Harrisburg...

Säg att risken för en olycka är 0.1% per dag.

Nästan ingenting!

Det betyder 99.9% säkerhet - per dag.

$$0.999^{365} = 0.69...$$

31% risk för olycka på ett år!

01001001 01000011 01000111

Sannolikheter är svåra att bedöma

...men vi måste göra det! Bedöm rimligt redan
innan det smäller!

Sannolikheten, skadan och kostnaden för
åtgärden måste jämföras.

Bedömningen beror på typen av attack.

01001001 01000011 01000111

Uppskatta kostnaden för risken

Attacker som ger skada per gång:

(Uppskattade) medelkostnaden för skadan varje gång hotet orsakar skadan = d

(Uppskattade) sannolikheten per attack = p

(Uppskattade) attacker per år = n

Uppskattade förväntade antalet gånger per år som hotet förväntas orsaka skada $f = n * p$

Riskkostnaden är då $r = f * d$

01001001 01000011 01000111

Uppskatta kostnaden för risken

Attacker som ger sannolikhet per gång men bara skada en gång:

(Uppskattade) kostnaden när attacken lyckas = d

(Uppskattade) sannolikheten per attack = p

Uppskattade förväntade antalet attacker = f

Sannolikheten att ingen attack går igenom = $(1 - p)^f$

Riskkostnaden är då $r = (1 - (1 - p)^f) * d$

01001001 01000011 01000111

Uppskatta kostnaden för risken

Attacker som bara inträffar en gång:

(Uppskattade) kostnaden när attacken lyckas = d

(Uppskattade) sannolikheten att attacken lyckas = p

Riskkostnaden är då $r = p * d$

01001001 01000011 01000111

Uppskatta kostnaden för risken och åtgärden

Slutsats: Beräkningen av riskkostnad beror på situationen.

Riskkostnad utan åtgärd: r

Med åtgärd: Sannolikheten förändras från p till p'

Kostnad för åtgärd: k

Tag fallet där riskkostnaden är $r = p * d$

Efter åtgärd: riskkostnaden blir $r' = p' * d$

Är $r' + k > r$? Då kostar åtgärden mer än skadan!

01001001 01000011 01000111

Projekten

Vad skall ni göra?
Hur skall ni göra det?

01001001 01000011 01000111

Om projekten

Projekt = säkerhetsutvärdering

16 givna fall

Utförs solo eller i par

Analysera och föreslå åtgärder

Använd metoder givna i kursen!

Uppgiftsämnen

- Biljettbeställning över nätet
- Dagligvarubutik
- Distansarbete
- Egen tidigare arbetsplats
- Enmansfirma
- Forskargrupp
- Hasardspel
- Hemstyrssystem
- Kommunal hemtjänst
- Kemiindustri
- Lantbruk
- Morbror August
- Säkerhetsdelen i offert
- Familjen Vringhed
- Vaktbolag
- Veterinärklinik

Innehåll: Analys + åtgärd

CIA-analys

Identifiera brister

Hotanalys

Riskanalys

Åtgärder med prioritering

01001001 01000011 01000111

Storlek och bedömning

Ca 6-8 sidor. Sidanatal är oviktigt, det är innehållet som räknas!

Lämnas in på sätt som meddelas senare. Säger jag inget så E-posta. Märk rapporten med LiU-ID i både titel och innehåll!

Plagiera inte! Rapporterna testas i Urkund.

Generativ AI

Viktig aspekt numera: Användning av generativ AI, t.ex. ChatGPT.

Flera varianter:

1) Använd inte ChatGPT alls. Tryggt och säkert.

2) Använd ChatGPT som rådgivare. Dokumentera detta och *kritisera resultatet*. Hitta fel och brister, eller notera anmärkningsvärda positiva saker som inte var väntade.

3) Låt ChatGPT skriva hela rapporten. **INTE TILLÅTET!** Jag ser det och kommer att examinera er hårdare. Det räknas som FUSK och jag måste dessutom rapportera er. Låt bli!

01001001 01000011 01000111

Generativ AI -> muntlig presentation

Ni kommer att presentera era resultat muntligt på seminarier, 3-4 grupper i taget.

Detta är en nödvändig ändring i år på grund av generativ AI. Jag måste kunna kontrollera att ni vet vad ni talar om.

Detta tar plats i december.

01001001 01000011 01000111

Betyg, poängsystem

Poängsystem infördes 2022 för mer rättvis bedömning.
Justeras baserat på de nya redovisningarna. Preliminärt:

Struktur och läsbarhet: 3 poäng

Problemanalys: 5 poäng

CIA eller AAA: 5 poäng

Hotobjekt och hotagenter: 3 poäng

Risikanalys: 5 poäng

Åtgärder med prioritering: 5 poäng

Muntlig presentation: 5 poäng NY!

Max 31 poäng. Preliminära poänggränser: 12 för betyg 3, 17 för betyg 4, 23 för betyg 5.

01001001 01000011 01000111

Viktiga datum

Presentationer i december:

- Era slutsatser muntligt
 - Preliminär rapport.
 - 15 minuter per grupp, 3-4 grupper per pass.
- Anmälningssystem kommer.

Slutversionen lämnas in innan tentaperiodens slut i januari.

Möjlighet till examination senare, med poängavdrag.

01001001 01000011 01000111

Exemplen: Pickup at South Street och Lewis Avery Filer

Låt oss gå igenom två fall för att visa hur analysen går till.

- Problembeskrivning
- CIA
- Risker
- Prevention-detection-reaction
- Åtgärder
- Prioriteringar

01001001 01000011 01000111

Lewis Avery Filer

eller

Over 50? Steal!

01001001 01000011 01000111

Exempel: Lewis Avery Filer

Vem är hotad? Vem är offret? Försäkringsbolaget.

Du skall göra en rapport om detta. Vem är kunden, uppdragsgivaren? Försäkringsbolaget! Du har i uppdrag att analysera säkerheten för försäkringsbolaget!

Vi tar det steg för steg.

BILDER BORTTAGNA

01001001 01000011 01000111

Exempel: Lewis Avery Filer, problemanalys

Problemanalys:

Bolagets kunder har varierande säkerhetsnivå och hanterar stora ekonomiska värden.

Bolagets anställda har stor kunskap om kunderna.

Samgående gav övertalighet, många har avskedats. Många mycket erfarna, 50+, trotjänare. Avskedades enkelt och informellt.

Dessa har kunskap om förväntade tjuvar, beteende och bakgrund samt kundernas säkerhetssystem (kassaskåp mm).

01001001 01000011 01000111

Exempel: Lewis Avery Filer, CIA

Confidentiality: Huvudproblemet! Insiders vet om känslig information.

Integrity: Förfalskade spår som pekar på fel personer. Integrity? Det är ett problem för polisen men inte för vår kund!

Availability: Tillgängligheten för juvelerna helt enkelt.

Vilken sorts angripare: Definitivt blue hat, han är ute efter hämnd. Extern

BILDER BORTTAGNA

01001001 01000011 01000111

Exempel: Lewis Avery Filer, risker

Skicklig tjuv (teknisk kompetent, stor kunskap om målet, använder social engineering), betydande mätbar kostnad = hög risk för nya stölder.

Kommentar på detta: Underskattning av stöldrisk, antar andra typer av tjuvar = outsiders. Slutsats: Ovanstående ökad risk är en revision av tidigare uppskattning.

Risk för försämrat rykte om kopplingen till försäkringsbolaget upptäcks.

Risk för skador på personal.

01001001 01000011 01000111

Exempel: Lewis Avery Filer, riskanalys

A: Risk för ekonomisk förlust: Hög sannolikhet (0.75), rätt hög skada.

B: Risk för skador på personal: Liten (0.4). Hög skada enbart om de är försäkrade hos företaget.

C: Risk för försämrat rykte. Mycket liten risk. (0.1) Måttlig skada.

Katastrofal				
Allvarlig		B1	A	
Hanterbar	C			
Försumbar		B2		
	Nästan omöjligt	Möjlig	Trolig	Oundviklig

01001001 01000011 01000111

Exempel: Lewis Avery Filer, sök åtgärder

Hitta åtgärder genom att dela upp dem i prevention-detection-reaction.

Prevention: Avskeda på trevligare sätt. Rejäl avgångsvederlag. Var medveten om att dessa har insider-info! Värdera företagets trotjänare högre. Ändra informationen.

Detection: Trivialt. Han ser till att angreppet syns, tydligt! Men att upptäcka det i förväg är svårare.

Reaction: Förutse troliga nästa mål, förbättra säkerheten, ändra rutinerna. Hjälp polisen gripa tjuven.

01001001 01000011 01000111

Exempel: Lewis Avery Filer, åtgärder på A0-A1

A0. Reaction på A: Ingen åtgärd. Betydande summor måste betalas ut. Kostnad: Hög ($d \approx 1\text{M\$}$) Risk efter åtgärd: Samma.

$$r = p * d = 0.75 * 1 = 0.75$$

A1. Långsiktig prevention för A: Regjäla avgångsvederlag. Kostnad: Mycket hög. Risk efter åtgärd: försumbar, $p' = 0.1$. ($k \approx 10\text{M\$}$)

$$r' + k = p' * d + k = 0.1 * 1 + 10 = 10.1$$

01001001 01000011 01000111

Exempel: Lewis Avery Filer, åtgärder på A2-A3

A2. Långsiktig prevention för A: Bra rekommendationsbrev.

Kostnad: Mycket låg för brevet, medelhög för framtida konkurrens.

Risk efter åtgärd: hanterbar, $p' = 0.2$. ($k \approx 2M\$$)

$$r'+k = p'*d + k = 0.2 * 1 + 2 = 2.2$$

A3: Långsiktig prevention på A: Sparka INTE 50+are! Kostnad:

Ganska låg: lön mot fortsatta insatser. Viss kostnad pga övertalighet, kan ge vinst men kan kosta upp till $k \approx 5M\$$. Låt oss säga 2.5. $p' = 0$.

$$r'+k = p'*d + k = 0 * 1 + 2.5 = 2.5$$

Exempel: Lewis Avery Filer, åtgärder på A4-A5

A4. Prevention för A: Utbilda personalen om riskerna, speciellt social engineering. Kostnad: Medel, $k \approx 100\text{k\$}$. Risk efter åtgärd: Hanterbar, $p' \approx 0.3$

$$r'+k = p'*d + k = 0.3 * 1 + 0.1 = 0.4$$

A5. Prevention för A: Förändra hos kunderna för att göra insidesinformationen meningslös. Kräver sponsring av kunderna! Risk efter åtgärd: Hanterbar, 0.3. Kostnad: Hög (Uppskattas till 5M\$)

$$A5. r'+k = p'*d + k = 0.3 * 1 + 5 = 5.3$$

01001001 01000011 01000111

Exempel: Lewis Avery Filer, åtgärder på B

B0. Reaction på B: Ingen åtgärd, betala sjukhusräkningarna.

Kostnad: Rätt hög (för det är Hawaii = USA) Uppskattas till 100k\$

Risk efter åtgärd: Oförändrad

$$B0. r = p \cdot d = 0.4 \cdot 0.1 = 0.04$$

B1. Prevention för B: Utbilda personalen att inte provocera tjuven till våld. Kostnad: Låg (Uppskattas till 1k\$) Risk efter åtgärd: Försumbar (0.1).

$$B1. r' + k = p' \cdot d + k = 0.1 \cdot 0.1 + 0.001 = 0.011$$

01001001 01000011 01000111

Exempel: Lewis Avery Filer, åtgärder på C

C0. Reaction på C: Ingen åtgärd. Kopplingen är offentlig. Risk 0.3, måttligt troligt att kunderna reagerar. Skadan är måttlig, lite förlorade intäkter. (Uppskattas till 0.2M\$)

$$r = p \cdot d = 0.3 \cdot 0.2 = 0.06$$

C1. Prevention för C: Hemlighåll kopplingen. Enkelt. Kostnad: Låg (Uppskattas till 0.01M\$) Skadan sjunker till 0.

$$r' + k = p' \cdot d + k = 0.01 = 0.01$$

01001001 01000011 01000111

Exempel: Lewis Avery Filer, skada och kostnad

p = sannolikhet (probability), antar linjär skada/kostnad

p' = sannolikhet efter åtgärd

k = kostnad för åtgärd

d = skadan, kostnad om attacken lyckas

$$A0. r = p * d = 0.75 * 1 = 0.75$$

$$A1. r' + k = p' * d + k = 0.1 * 1 + 10 = 10.1$$

$$A2. r' + k = p' * d + k = 0.2 * 1 + 2 = 2.2$$

$$A3. r' + k = p' * d + k = 0 * 1 + 2.5 = 2.5$$

$$A4. r' + k = p' * d + k = 0.3 * 1 + 0.1 = 0.4$$

$$A5. r' + k = p' * d + k = 0.3 * 1 + 5 = 5.3.$$

01001001 01000011 01000111

Exempel: Lewis Avery Filer, skada och kostnad

p = sannolikhet (probability), antar linjär skada/kostnad

p' = sannolikhet efter åtgärd

k = kostnad för åtgärd

d = skadan, kostnad om attacken lyckas

$$B0. r = p * d = 0.4 * 0.1 = 0.04$$

$$B1. r' + k = p' * d + k = 0.1 * 0.1 + 0.001 = 0.011$$

$$C0. r = p * d = 0.3 * 0.2 = 0.06$$

$$C1. r' + k = p' * d + k = 0.01 = 0.01$$

01001001 01000011 01000111

Exempel: Lewis Avery Filer, prioriteringar

A4. Utbilda för att undvika stöld = 0.4 i stället för 0.75

C1: Hemlighåll, 0.01 i stället för 0.06

B1: Utbilda personalen, 0.001 i stället för 0.011

Alla andra åtgärder bedöms dyrare än skadan!

Men är mina uppskattning korrekta?

01001001 01000011 01000111

Exempel: Lewis Avery Filer, slutsats

Många åtgärder är alldeles för dyra.

Enbart utbildning av personalen bedöms som rimligt för att undvika stöld.

Det är också lönsamt att undvika personskador!

01001001 01000011 01000111

Pickup at South Street

01001001 01000011 01000111

**Exempel: "Pickup at South
Street"**

BILDER BORTTAGNA

Lite mer komplext fall!

Eller är det det?

01001001 01000011 01000111

Exempel: Pickup at South Street

Vem är hotad? Alla! Vem är vår kund?

Spionorganisationen! :)

Kommunisterna är bordurier och de bestulna är syldaver.

Du skall göra en rapport om detta.

01001001 01000011 01000111

Exempel: Pickup at South Street

Problemanalys:

Spionerna stjälar en hemlig mikrofilm och skall frakta den ur landet till det onda kommunistlandet Bordurien.

De väljer att låta detta göras av en söt och till synes oskyldig flicka som lägger den i handväskan och åker tunnelbanan som vanligt.

Det finns en viss risk att hon är bevakad av polisen, men hon är omgiven av en massa vanligt folk så man räknar med att hon försvinner i mängden.

01001001 01000011 01000111

Exempel: Pickup at South Street

Confidentiality: Håll stölden och transporten hemlig.

Integrity: Har hon verkligen rätt mikrofilm? Tänk om de snälla syldaverna har lagt dit en falsk!

Availability: Tillgängligheten för mikrofilmen är kritisk!

Vilken sorts angripare: För din uppdragsgivare är syldaverna Black Hat, det är fienden som vill förstöra dina planer.

01001001 01000011 01000111

Exempel: Pickup at South Street

Risker:

- Hon blir tagen av polisen
- Ficktjuvar
- Väskryckare
- Hon tappar bort väskan av misstag
- Hon har fått fel mikrofilm
- Personskada på grund av strid med polis eller tjuv
- Personskada på grund av bestraffning

01001001 01000011 01000111

Exempel: Pickup at South Street, prevention

Prevention:

Blir tagen av polisen:

- Utbildning. Få henne att upptäcka om hon är skuggad och lär henne hur man smiter undan.
- Lär henne hur man snyggast gör sig osynlig i folkmassor.
- När det inte kan undvikas, göm undan mikrofilmen så en kollega kan få tag i den senare.
- Spring av bara katten.

01001001 01000011 01000111

Exempel: Pickup at South Street, prevention

Ficktjuvar:

- Bättre väska. Lås på väskan. Väska med biometrisk lås?
- Väskryckningssäker.
- Vilseled angriparen: Ha falska saker lättstulna, värdefullt dolt.

Tappa bort väskan av misstag: Se nedan, medföljare.

Både polis och ficktjuvar:

- Ha en medföljare som
 - 1) höjer hennes säkerhet, upptäcker hot och åtgärdar dem.
 - 2) Tar tillbaka mikrofilmen om den stjäls.

01001001 01000011 01000111

Exempel: Pickup at South Street, prevention

Prevention:

Fel mikrofilm:

- Utför kontroller tidigast möjligt.
- Analysera situationen. Var mikrofilmen tydligt falsk? Var det en "honungsfälla" för att sätta dit spionerna?

01001001 01000011 01000111

Exempel: Pickup at South Street, detection

Ganska enkelt i detta fall.

- Upptäck ficktjuvar och poliser innan de hinner göra skada
- Upptäck om mikrofilmen är falsk

01001001 01000011 01000111

Exempel: Pickup at South Street, reaction

Reaction:

Tjuv & polis: Försök ta tillbaka mikrofilmen från polisen eller tjuven. Förfölj dem tills det är möjligt.

Falsk mikrofilm:

Avbryt och gör ny plan.

01001001 01000011 01000111

Exempel: Pickup at South Street, riskanalys

A: Ficktjuv/väskryckare: Stor risk på tunnelbanan. 0.5

B: Polis: Ganska stor risk. 0.3

C: Slarv: Låg risk. Hon vet att hon bär något värdefullt. 0.1

Samtliga fall ovan ger stor skada.

D: Personskada på grund av konflikt (0.2)

E: Personskada på grund av bestraffning (0.4)

Dessa fall ger låg skada. Spionerna bryr sig inte om sin personal men i fallet D kan det vara personal med visst värde.

01001001 01000011 01000111

Exempel: Pickup at South Street, risker

Hot om personskada varierar lite med olika hot. Låg skada för bestraffning, högre när det är strid mot tjuv eller polis.

Vi sammanfattar alla hot mot mikrofilmen som ett, "förlust av mikrofilmen" med total sannolikhet 0.7.

1. Strid med ficktjuv (i sig 0.5). Låg sannolikhet för personskada. 0.1
Skada 3.
2. Strid med polisen (0.3). Medelhög sannolikhet för personskada. 0.5
Skada 3.
3. Bestraffning (0.7). Hög sannolikhet efter förlust av mikrofilm (0.8)
Skada 1.

01001001 01000011 01000111

Exempel: Pickup at South Street, riskanalys

Katastrofal	C	B	A	
Allvarlig				
Hanterbar		D		
Försumbar			E	
	Nästan omöjligt	Möjlig	Trolig	Oundviklig

01001001 01000011 01000111

Exempel: Pickup at South Street, åtgärder mot stöld

Vi sammanfattar alla hot mot mikrofilmen som ett, "förlust av mikrofilmen" med total sannolikhet $p = 0.7$ och maximal kostnad på 10. (Jag väljer här tiogradig skala på skada och kostnad.)

1. Bättre väska. Kostnad: Låg ($k = 1$). $p' \approx 0.2$
2. Avancerad väska. Kostnad: Hög ($k = 5$). $p' \approx 0.1$
3. Falsa objekt. Kostnad: Låg ($k = 2$). $p' \approx 0.1$
4. Medföljare. Kostnad: Medel ($k = 2$). $p' \approx 0.3$
5. Utbildning. Kostnad: Medel ($k = 3$). $p' \approx 0.4$

01001001 01000011 01000111

Kostnaden för risken och åtgärden

p = sannolikhet (probability), antar linjär skada/kostnad

p' = sannolikhet efter åtgärd

k = kostnad för åtgärd

d = skadan, kostnad om attacken lyckas

- | | |
|--------------------|--------------------------------------|
| 0. Ingen åtgärd | $r = p*d = 0.7*10 = 7$ |
| 1. Bättre väska. | $r'+k = p'*d + k = 0.2 * 10 + 1 = 3$ |
| 2. Avancerad väska | $r'+k = p'*d + k = 0.1 * 10 + 5 = 6$ |
| 3. Falsa objekt | $r'+k = p'*d + k = 0.1 * 10 + 2 = 3$ |
| 4. Medföljare | $r'+k = p'*d + k = 0.3 * 10 + 2 = 5$ |
| 5. Utbildning | $r'+k = p'*d + k = 0.4 * 10 + 3 = 7$ |

Exempel: Pickup at South Street, åtgärder, personskador

Utbildning och medföljare är de effektiva åtgärderna. Riskerna sammanfattas till $1 - (1-0.5)*(1-0.3)*(1-0.1) = 0.7$

Förväntad skada är maximala $d = 0.7*3 = 2.1$

1. Ingen åtgärd. $r = p*d = 0.7 * 2.1 = 1.5$
2. Medföljare. $p' \approx 0.3$. $r'+k = p'*d + k = 0.3*2.1 + 2 = 2.6$
3. Utbildning. $p' \approx 0.4$. $r'+k = p'*d + k = 0.4*2.1 + 3 = 3.8$

Slutsats: Låg kostnad utan åtgärd. Svag påverkan på prioriteringen.

Vi kan gå längre genom att koppla åtgärderna till att de påverkar flera risker och därmed gör dubbel effekt.

01001001 01000011 01000111

Exempel: Pickup at South Street, slutsats

Högsta prioritet är väskan samt falska objekt. Båda har stor effekt för låg kostnad.

Efter denna kommer medföljaren.

Avancerad väska är dyrt.

Utbildning har lägst prioritet, hög kostnad och låg effekt

Hela listan av motivation, risker, åtgärder och prioriteringar levereras till uppdragsgivaren.

Värdera mikrofilmen högre? Då blir alla åtgärderna önskvärda. De skall fortfarande ha en prioritetsordning

01001001 01000011 01000111

Inte med i exempen: Parallella och seriella beroenden

Både hot och åtgärder kan ha beroenden, som gör dem parallella eller seriella.

Seriella åtgärder (på seriella hot) minskar den totala risken för hela kedjan

Parallella åtgärder (på parallela hot) minskar risken på en gren men gör inget åt den andra, så effekten blir mindre

01001001 01000011 01000111

Inte heller med i exempen: Ett eller flera tillfällen

Kan vi ha flera attacker som lyckas, och vi tar skadan och fortsätter, eller är allt kört efter en attack?

Ovan klumpar jag ihop det. Filer kan göra flera stölder, och vi samlar total skada för alla, medan Harrisburg behöver bara haverera en gång för att vara en katastrof!

01001001 01000011 01000111