

Projekten

Repetition och ett fall till

01001001 01000011 01000111

Innehåll: Analys + åtgärd

CIA-analys

Identifiera brister

Hotanalys

Riskanalys

Åtgärder med prioritering

01001001 01000011 01000111

Storlek och bedömning

NYHET: Er rapport = ert presentationsmaterial + kommentarer

Skriv i presentationsprogrammet, lägg till lite kommentarer vid behov, lämna in som PDF.

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

Plagiera inte! Rapporterna testas i Urkund.

Betyg, poängsystem

Poängsystem infördes 2022 för mer rättvis bedömning.
Justeras i år baserat på duggorna. Preliminärt:

Bra presentationsmaterial: 2 poäng
Problemanalys, CIA eller AAA: 4 poäng
Hotobjekt och hotagenter: 3 poäng
Riskanalys: 4 poäng
Åtgärder med prioritering: 5 poäng
Muntlig presentation: 2 poäng

Duggor: 10 poäng

Max 30 poäng. Preliminära poänggränser: 15 för betyg 3, 20 för betyg 4, 25 för betyg 5. Något lägre för soloprojekt.

01001001 01000011 01000111

Viktiga datum

Presentationer i december med era slutsatser muntligt samt visa upp preliminär rapport. 15 minuter per grupp, 3-5 grupper per pass. Anmälningssystem kommer.

Slutversionen lämnas in senast första januari.

Möjlighet till examination senare. Kommer att ge visst poängavdrag.

01001001 01000011 01000111

Exempel #2: Pickup at South Street

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

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

01001001 01000011 01000111

Pickup at South Street

01001001 01000011 01000111

Exempel: "Pickup at South Street"

BILD SKIPPAD

BILD SKIPPAD

BILD SKIPPAD

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! :)

(Inte för att jag gillar kommunistiska spioner utan för att det är deras situation som är intressant.)

I neutralitetens namn så bestämmer jag att 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: Det finns frågor här. Är vi så säkra på att hon verkligen har rätt mikrofilm? Tänk om de snälla syldaverna har bytt ut den och lagt dit en falsk!

Availability: Tillgängligheten för mikrofilmen är kritisk!

Vilken sorts angripare: Beror lite på synvinkel men från din uppdragsgivares synvinkel är syldaverna Black Hat, det är fienden som är ute efter att 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. Kan rentav använda en väska med biometrisk lås så ficktjuven inte ens kan dyrka den.

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 har till uppgift att
 - 1) höja hennes säkerhet, upptäcka hot och åtgärda dem.
 - 2) Ta 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 lite väl 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. Falska 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.

Dock kan mikrofilmen värderas högre, och då blir alla åtgärderna önskvärda. De skall fortfarande ha en prioritetsordning

01001001 01000011 01000111

Kvantifierad lista

- | | |
|--------------------|---------------|
| 1. Bättre väska. | riskkostnad 3 |
| 1. Falsa objekt | riskkostnad 3 |
| 3. Medföljare | riskkostnad 5 |
| 4. Avancerad väska | riskkostnad 6 |

01001001 01000011 01000111

Inte med i exemplen: Parallella och seriella beroenden

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

Seriella åtgärder (på seriella hot) minskar 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! I South Street är det bara en mikrofilm, men finns det flera försök?

01001001 01000011 01000111