Projekten

Vad skall ni göra?
Hur skall ni göra det?

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**
- **Hemstyrsystem**
- **Kommunal hemtjänst**
- **Kemiindustri**
- **Lantbruk**
- **Morbror August**
- **Säkerhetsdelen i offert**
- **Familjen Vringhed**
- **Vaktbolag**
- **Veterinärklinik**

01000011 01001001 01000001

Kylsystemet - projekt?

Kylar styrs på distans.

Effektivt, man spar pengar på att inte springa runt och justera kylarna en och en.

Mindre risk för handhavandefel.

Attack styrde systemet och ställde det fel.

Kostnader, åtgärder?

OBS: Ta hänsyn till om åtgärden orsakar högre kostnader.

Innehåll: Analys + åtgärd

CIA-analys

Identifiera brister

Hotanalys

Riskanalys

Åtgärder med prioritering

Storlek och bedömning

NYHET FÖRRA ÅRET: 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 (motsv).

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!

01000011 01001001 01000001

Generativ AI -> muntlig presentation

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

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

Detta tar plats i december, innan jul.

Betyg, poängsystem

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

Bra presentationsmaterial: 1 poäng
Problemanalys, CIA eller AAA: 2 poäng
Hotobjekt och hotagenter: 2 poäng
Riskanalys: 4 poäng
Åtgärder med prioritering: 3 poäng
Muntlig presentation: 3 poäng

Duggor: 15 poäng

Max 30 poäng. Preliminära poänggränser: 14 för betyg 3, 19 för betyg 4, 24 för betyg 5.

Viktiga datum

Presentationer i december med era slutsatser muntligt. 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.

Exempel #1: Lewis Avery Filer

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

- Problembeskrivning
- CIA
- Risker
- Prevention-detection-reaction, åtgärder
- Prioriteringar

Lewis Avery Filer

eller

Over 50? Steal!

01000011 01001001 01000001

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.

BILD BORTTAGEN
PGA COPYRIGHT

Exempel: Lewis Avery Filer, problemanalys

Problemanalys:

Bolagets kunder har varierande säkerhetsnivå och hanterar stora ekonomiska värden.

Bolagets anställda har stor kunskap om kunderna.

Bolaget har nyligen gått samman med ett annat och ett betydande antal anställda har avskedats, rationaliserats bort. Många av dessa är mycket erfarna, 50+, har arbetat för företaget i decennier. De avskedades enkelt och informellt.

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

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. Expertnivå.

BILD BORTTAGEN PGA COPYRIGHT

Exempel: Lewis Avery Filer, risker

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

Betydande mätbar kostnad

Kommentar på detta: Underskattning av stöldrisk på grund av god kunskap om andra typer av tjuvar = man trodde att man var säker. Slutsats: Ökad risk är en revision av tidigare uppskattning.

Risk för försämrat rykte om kopplingen till försäkringsbolaget upptäcks.

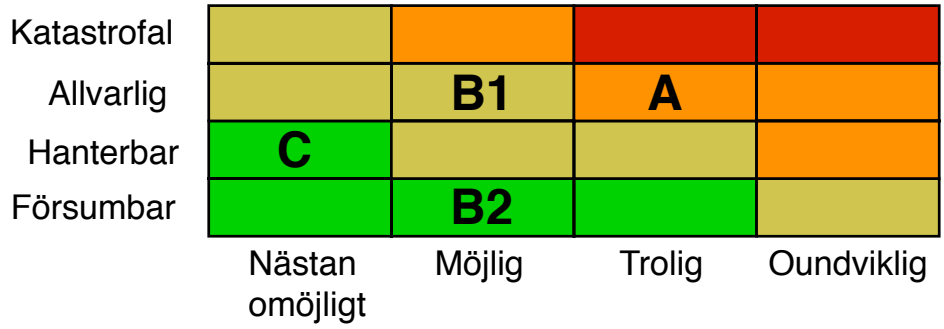
Risk för skador på personal.

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.



01000011 01001001 01000001

Exempel: Lewis Avery Filer, sök åtgärder

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

Prevention: Avskeda folk på ett trevligare sätt. Rejäla avgångsvederlag. Behåll trotjänare med mycket insider-info. 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.

Exempel: Lewis Avery Filer, åtgärder på A0-A1

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

r = p*d = 0.75 * 1 = 0.75

A1. Långsiktig prevention för A: Rejäla avgångsvederlag. Kostnad: Mycket hög. Risk efter åtgärd: försumbar, p' = 0.1. (k ≈ 10M$)

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

Exempel: Lewis Avery Filer, åtgärder på A2-A3

A2. Långsiktig prevention för A: Bra rekommedationsbrev. Kostnad: Mycket låg för brevet, medelhög för framtida konkurrens. Risk efter åtgärd: hanterbar, p' = 0.2. (k ≈ 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 ≈ 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 ≈ 100k$. Risk efter åtgärd: Hanterbar, p' ≈ 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

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*d = 0.4 * 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'*d + k = 0.1 * 0.1 + 0.001 = 0.011

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*d = 0.3 * 0.2 = 0.06

C1. Prevention för C: Hemlighåll kopplingen. Enkelt. Kostnad: Låg (Uppskattas till 0.01M$) Skadan sjunker till 0. Men om det upptäcks! Sannolikhet 0.1, skada 10M$

r'+k = p'*d + k = 0.1 * 10 + 0.01 = 1.01

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.

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 = 1.01

Exempel: Lewis Avery Filer, prioriteringar

A4. Utbilda för att undvika stöld = 0.4 i stället för 0.75
B1: Utbilda personalen, 0.001 i stället för 0.011

Alla andra åtgärder bedöms dyrare än skadan!

Men är mina uppskattning korrekta?

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!

I andra fall kan det finnas flera lönsamma. Vilka är mest lönsamma?

Senare (fö 10):
Pickup at South Street

01000011 01001001 01000001

Inte med i exemplen: 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

Inte heller med i exemplen: 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!

OBS: Åtgärder på Reaction ändrar inte sannolikheten, bara skadan!

Nästa gång:
Websäkerhet, labbarna