TSIT01 Datasäkerhetsmetoder

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

Ingemar Ragnemalm

01000011 01001001 01000001

Förra gången

CIA = Confidentiality, Integrity, Availability

Prevention - detection - reaction

Denna föreläsning

Lite mer om risk och skada: Att mäta säkerhet

Projekten

Exempel på säkerhetsanalys

Föreläsningsfrågor

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?

5. Vad orsakade problemet med kylarna och frysarna och vad borde man göra åt det?

Senaste nytt:

Butikskylar och frysar hackade – flera butiker drabbade

UPPDATERAD IDAG 18:15 PUBLICERAD IDAG 08:49

Flera Ica-butiker har fått sina frysar och kylar hackade. Även Coop-butiker har drabbats.
– Det är obehagligt, man förstår det inte, säger Hanna Lindén, butikschef på Ica i Hammenhög.

De drabbade butikerna finns i stora delar av landet. Ett flertal ligger i Skåne, men även Öland och Värmland – och flera i Stockholm.

Även sex Coop-butiker i Gävleområdet har drabbats. Axfoods presschef Magnus Törnblom säger att hemleveranser av mat i Göteborg, beställd online från Hemköp eller Willys, påverkas.

01000011 01001001 01000001

Confidentiality - Integrity - Availablility

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?

Prevention - detection - reaction

Tre olika typer av åtgärder, sätt att bemöta hot

Hur hindrar vi det?

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

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

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!

Att mäta säkerhet

01000011 01001001 01000001

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 ouppdaterade program

Hur allvarlig är skadan?
- Förlorade resurser
- Kostnaden är återställning (i pengar eller mantimmar)
- Förlorat rykte

Vad kostar åtgärderna för attt hindra skadan?

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

Exempel, grundläggande egenskaper

Stöld av en ficktjuv är en risk för dig enligt:

• Hot: Det kan finnas ficktjuvar i området

• Svaghet: Du bär plånboken där en skicklig ficktjuv kan komma åt den i en folksamling

• Skada: Förlust av plånboken och dess innehåll

Hotagent = ficktjuven

Hotobjekt/tillgång = plånboken

När vi snackar ficktjuvar...

"Pickup at South Street"

BILD BORTTAGEN
PGA COPYRIGHT

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!

Egenskaper hos hot

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

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

Olyckor som agenter har inget specifikt mål. Åska mfl katastrofer kan vara ett hot mot *tillgänglighet*

Avsiktliga agenter har individuellt varierade mål

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

Agenter har varierande sannolikhet att angripa ditt system.

Nästa exempel: Lewis Avery Filer

BILD BORTTAGEN
PGA COPYRIGHT

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

01000011 01001001 01000001

Insiders

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

Den anställde har intern system-kunskap och kan få tag i mer

Den f.d. anställde då...?

(Die Hard 4, Hawaii 5-0)

BILD BORTTAGEN PGA COPYRIGHT

Vem är Lewis Avery Filer ett hot mot?

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

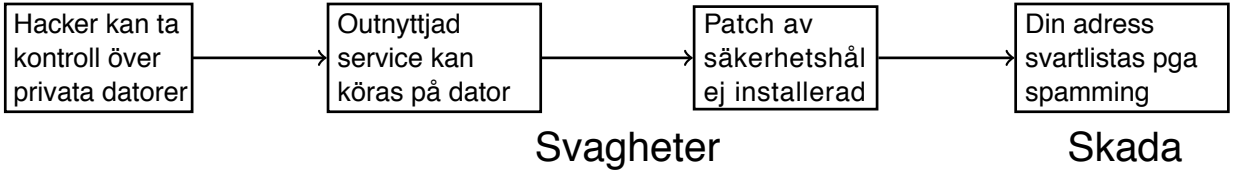


Egenskaper hos svagheter

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

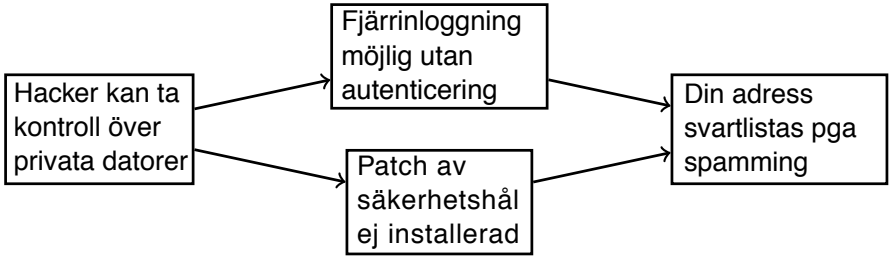
Det räcker att ta bort en seriell länk, men med parallella måste alla åtgärdas



Seriella länkar

Egenskaper hos svagheter

Med parallella länkar måste *alla* åtgärdas



Parallella länkar

Strikt riskanalys

Riskanalys uppskattar möjlig skada och sannolikhet hos hotet för att finna kostnaden för att avgöra om det är motiverat att eliminera svagheten

Om vi vinner mer med åtgärder i efterhand (återställning) än att eliminera svagheten så använder vi motåtgärderna

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

Kvalitativ riskanalys

Uppskatta kvalitativt magnituden av skadan

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

Uppskatta sannolikheten

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

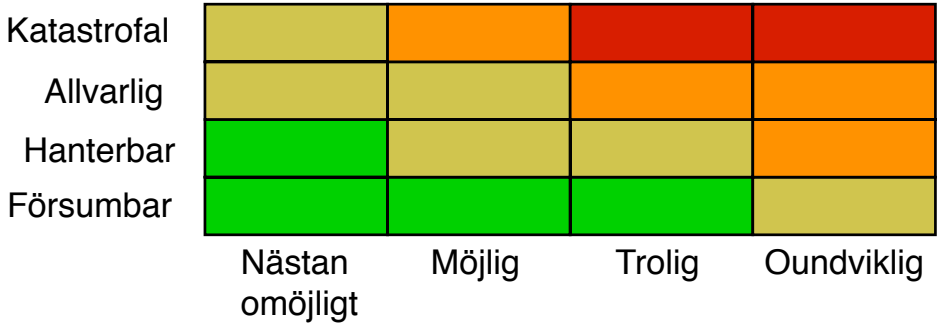
Kvalitativ riskanalys

Markera uppskattningen i ett rutnät

Katastrofal				
Allvarlig				
Hanterbar				
Försumbar				
	Nästan omöjligt	Möjlig	Trolig	Oundviklig

Kvalitativ riskanalys

Hantera händelser i prioritetsordning



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

BILD BORTTAGEN
PGA COPYRIGHT

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...

01000011 01001001 01000001

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!

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.

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 = n * p * d*

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

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*

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!