Säkerhetsmekanismer och risk

IT i hälso- sjukvården

(28 sidor)

1

Säkerhetsmekanismer

= Skydd

- Avser att öka informationssäkerheten
- Är en typ av informationstillgång

2

Skadlig kod

- Virus (kopierar sig själva inuti andra program)
- Trojaner, makrovirus (koden är inarbetad i ett annat program)
- Spionprogram (spionerar på privat information)
- Logisk bomb (Utför skadlig handling under vissa villkor, Milleniumbomben)
- Maskar (sprider sig via datornätverk)
- Gisslan (ransomware)
- Annonsprogram (omdirigering, sällan skadliga)
- Ondsint annonsering
- https://techworld.idg.se/2.2524/1.718407/nio-typer-av-skadlig-kod---och-hur-du-kanner-igen-dem

3

3

Säkerhetsprodukter, -system och -lösningar

- Brandväggar
  (dator eller program som syftar till avvärja intrång på nätanslutna datorer)
- Antivirusprogram (program som aktivt eller på begäran söker efter, tar bort eller reparerar filer som är infekterade av datorvirus.)

4

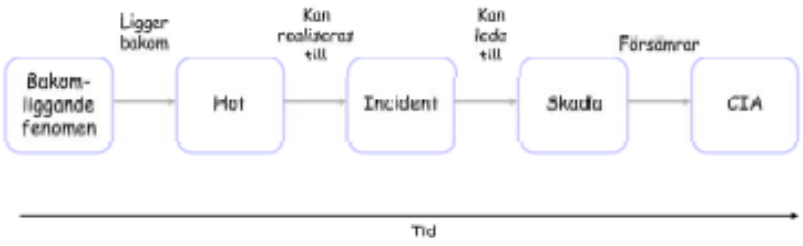
4

Säkerhetsprodukter, -system och -lösningar

- Krypteringssystem (förändrar information till oläslig kod)
- Behörighetskontrollsystem (styr användares åtkomst)
- Säkerhetskopiering
- Lås, dörrar, brandsläckare (gäller fysiska hot)

5

Tidsperspektiv



- Från bakomliggande fenomen till försämring av CIA

6

Tid och säkerhetsmekanism

- Fyra kategorier av säkerhetsmekanismer

Kategorier av säkerhetsmekanismer

- Förebyggande – Utbildning, opinionsbildning
- Avvärjande – Brandväggar, dörrar, lås
- Skadereducerande – Brandsläckare
- Korrigerande – Antivirusprogram som reparerar skadade filer

Sårbarhet

- Avsaknad av säkerhetsmekanismer
- Brister i säkerhetsmekanismer

9

9

Risk

- **Ett mått** på hur allvarligt ett hot är (en tänkbar oönskad händelse)

- Risk =
  Sannolikhet/förväntad frekvens * Potentiell skada

10

10

Risk management

- Handlar om att identifiera och ta fram ett för företaget lämpligt riskhanteringssystem
- Systemet ska bidra till att risker hanteras strukturerat

11

11

Nya risker

- Expertgrupp varnar: Stora risker med känsliga data i molntjänster. Om man använder amerikanska molntjänster för sekretessreglerade data ska de anses röjda.
- https://computersweden.idg.se/2.2683/1.710293/utlandska-moln-data

12

12

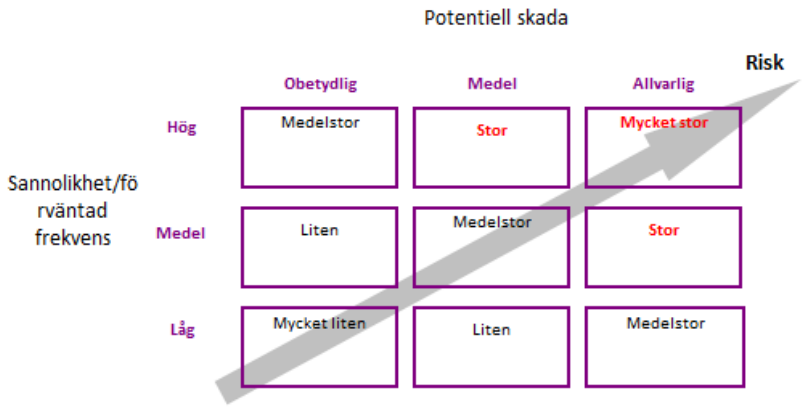
Länkar

- Region Skåne Informationssäkerhet – Riskhantering https://vardgivare.skane.se/uppdrag-avtal/informationssakerhet/

13

13

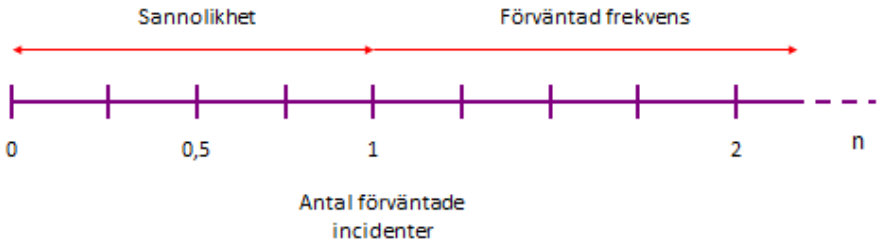
Stora och små risker



14

14

Sannolikhet och förväntad frekvens



- Om färre än en incident = sannolikhet
- Om fler än en incident = Förväntad frekvens

15

Tidsperiod

- Om man ändrar eller delar upp tidsintervallet kan (bör) således växling mellan begreppen ske. Antag t ex att man bedömer att en viss incident kommer att inträffa 3 ggr/år:

  Förväntad frekvens per 5-årsperiod: 15

  Förväntad frekvens per år: 3

  Sannolikhet per kvartal: 75 %

  Sannolikhet per månad: 25 %

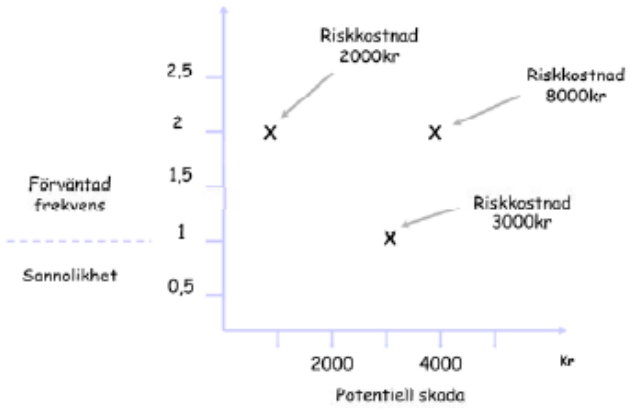
  Sannolikhet per vecka: ca 6 %

16

Potentiell skada

- Möjlig tänkbar skada
- Prognosen behöver inte stämma med utfallet
- Kan värderas på olika sätt (oftast i ekonomiska termer)

Riskkostnad



- Förväntad frekvens/sannolikhet * potentiell skada

Riskuppfattningar

- Är **oftast subjektiva**
- Är oftast **situationsspecifika**
- Kan byggas på olika grunder

19

Fysisk säkerhet

- Mål med fysisk säkerhet SS-ISO/IEC 17799
- Se till att IT-utrustning som används för att behandla personuppgifter har ett gott skydd mot **stöld och händelser som kan förstöra utrustningen**.
- Inför rutiner för hur **portabel IT-utrustning** ska användas och hur utrustningen och personuppgifterna i den ska skyddas. Nivån på skyddet bestäms av hur känsliga uppgifterna är.

20

Skalskydd

- Yttre skydd runt en byggnad, anläggning eller lokal.
- Den tillåtna vägen till en verksamhet bör vara via en reception, informationsdisk eller liknande.
- Detektorer
- Larmanordningar
- Bevakning

21

21

Tillträdeskontroll

- Passerkontroll
- Namnbrickor

22

22

Lokaler

- Allmänna utrymmen
- Externa personer
- Utrymmen med känslig utrustning
  - Vital utrustning
  - Reservutrustning
  - Underhåll av utrustning
  - Avveckling
  - Elförsörjning

23

Personliga arbetsplatser

- Dörrlås
- Fastlåsning av datorer.
- Inlåsning av bärbara datorer
- Dokument mm på skrivbord och i rummet

24

Säkerhetskopiering

- Innebär alltså att man kopierar information och **lagrar denna på ett annat ställe** än originalinformationen.
- SKALL GÖRAS

25

Varför?

- Sekretess, riktighet och tillgänglighet (CIA)
- Skyddar mot många hot

26

Säkerhetskopiering

- Lagringsmedia
  - CD-skivor
  - USB-minnen
  - ZIP-drive
- På nätet (molnet)
- På server

27

27

Rutiner

- Hur ofta?
- Antal kopior – hur många generationer?
- Förvaring – temperatur, vatten, brand etc.
- Märkning – För att snabbt hitta
- Simulering – För att vara beredd

28

28