ZAVAROVALNICA TRIGLAV, D.D.

Donosnost investicij v informacijsko varnost

Anton Bojanec
Inženir informacijske varnosti

Zavarovalnica Triglav, d.d.

Informacijska varnost

Informacijska varnost mora informacijam zagotoviti:

- **ZAUPNOST,**
- **CELOVITOST,**
- **RAZPOLOŽLJIVOST**
- zanesljivost, nezmožnost zanikanja, …

Ključna vprašanja …

- **Ali investiramo dovolj ?**
- **Ali investiramo preveč ?**
- Kako lahko pomanjkanje varnosti vpliva na produktivnost podjetja oz. na njegovo skupno poslovanje podjetja?
- Kakšen vpliv bodo imeli vpeljani varnostni ukrepi ali rešitve na produktivnost?
- Kakšen vpliv bi na poslovanje podjetja imel katastrofalni varnostni incident?
- Katere so najučinkovitejše (*cost-effective*) rešitve?

=> potrebujemo neko vrsto **VARNOSTNE METRIKE**

Osnovna matematika … - ROI

$$ROI = \frac{\text{pričakovani dobiček – strošek investicije}}{\text{strošek investicije}}$$

Višja matematika … - ROISI

$$ROISI = \frac{\text{(ovrednoteno tveganje x \% odpravljenega tveganja) – strošek investicije}}{\text{strošek investicije}}$$

pričakovani dobiček **(ROI)** = ovrednoteno tveganje x % odpravljenega tveganja **(ROISI)**

Primer … - ROISI

Sistem za zaznavo in odkrivanje škodljive programske opreme

Strošek investicije: **150.000 EUR**
Št. škodljive programske kode: 1.500 / mesec, kar znese **18.000 / leto**
Strošek odpravljanja okužbe: **60 EUR / okužbo**
Odpravljeno tveganje: **95 %**

$$ROISI = \frac{((60\ EUR\ X\ 18.000) \times 0.95) - 150.000\ EUR}{150.000\ EUR}$$

ROISI = 584 %

Vrednost tveganja

ALE =	SLE x ARO

ALE Annual Loss Exposure (Pričakovana letna izguba)
SLE Single Loss Exposure (Pričakovan strošek incidenta)
ARO Annual Rate of Occurance (Pričakovano število incidentov)

- **Ne obstaja standardna metoda za izračun pričakovanega stroška incidenta**
  - Majhni se ne beležijo, z velikimi je preveč drugega dela …
  - Nekje je pomembna tajnost podatkov, drugje produktivnost, časovna komponenta, …dobro ime
  - Ena od možnih rešitev za interno ocenitev vrednosti tveganja: **dobro zasnovan vprašalnik, iz omogoča oz. zahteva kvantitavitne odgovore**

- **Verodostojni podatki so letna poročila**
  - Computer Security Institute (gocsi.com/survey)
  - FBI, Internet Crime Complaint Center (www.ic3.gov/media/annualreports.aspx)

- **Ne obstaja standardna metoda za izračun pričakovanega števila incidentov**

% odpravljenega tveganja

- **Težko ocenljiva (varnost ne prinese dodatne vrednosti, samo prepreči izgubo …)**
- **Sistem za zaznavo vdorov (IDS) je lani zaznal 10 poizkusov vdorov, letos pa le 2 …**
  - Je to posledica naših izboljšav ali pa smo letos pač imeli le 2 poizkusa ?
  - V praksi se kaže dejstvo, da je večina napadov naključnih oz. ne namerno škodljivih
- **V primeru enostavnega vrednotenja % odpravljenega tveganja**
  - V primeru, da varnostna rešitev deluje pravilno bo tveganje odpravila 100 % odpravila (OK, recimo 85 %)
  - % odpravljenega tveganja je torej 95 %
- **Žal ima zgornja trditev določene pomanjkljivosti**
  - Tveganja se ne da izolirati
  - Varnostne rešitve bolje delujejo v koeksistenci
  - Varnostne rešitve so redkokdaj implementirane na najučinkovitejši način
  - Varnostne rešitve sčasoma postajajo manj učinkovite

Najbolj natančno lahko raven odpravljenega tveganja ocenimo z uporabo enega izmed kakovostnih presojevalnih algoritmov
(NIST - csrc.nist.gov, "Performance measurement guide for information security")

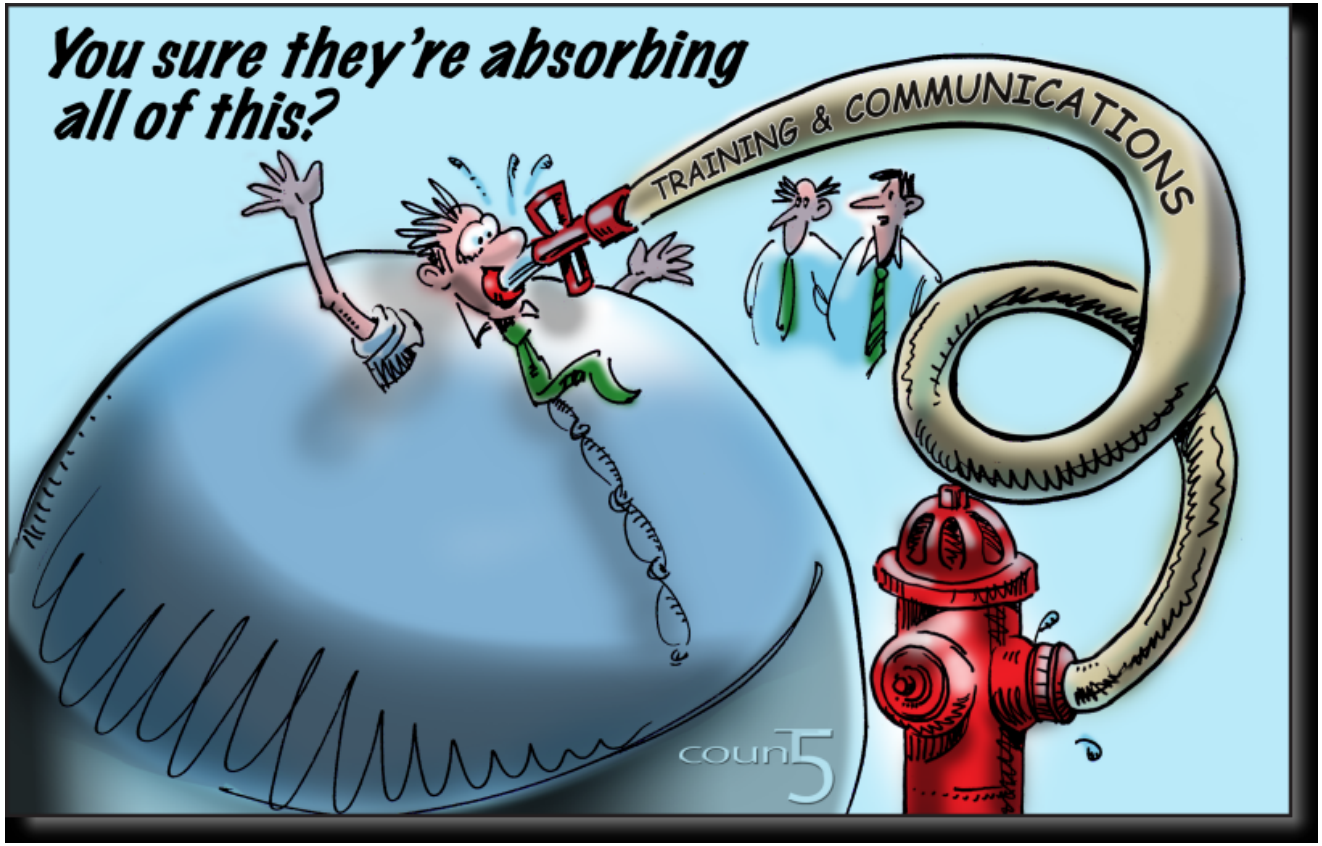
Strošek investicije

- **Ne obstaja standardna metoda za izračun stroška investicije**
  - Sam strošek investicije je običajno samo najbolj vidni del stroška
- **Stranski učinek zvišanja varnosti je ponavadi vpliv na produktivnost**
  - običajno negativno, včasih pa tudi pozitivno …
- **Tudi tega lahko izmerimo z dobro zasnovanim vprašalnikom**

Zaključek

- **Tudi informacijska varnost mora upoštevati "donosnost" …**
  - Obstajajo izjeme ….
- **Za izračun ROISI niti ni važno, da operiramo s točnimi podatki …**
  Pomembno je, da za njegov izračun uporabljamo konsistentno metodologijo !!
- **Varnostne rešitve, ki stane več, kot je ocenjeni strošek varnostnega incidenta, ki naj bi ga ta rešitev preprečila, ni smiselno vpeljati.**

ROISI v praksi …



ZAVAROVALNICA TRIGLAV, D.D.

Donosnost investicij v informacijsko varnost

Anton Bojanec
Inženir informacijske varnosti

Zavarovalnica Triglav, d.d.