ROBOTHADVISELÉS 2009

Az informatikai biztonsági kockázatok elemzése

Muha Lajos PhD, CISM
főiskolai tanár, mb. tanszékvezető
ZMNE BJKMK IHI Informatikai Tanszék

Az informatikai biztonság

Az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a **kockázatokkal arányos**.

A kockázattal arányos védelem

Egy kellően nagy időintervallum-ban a védelem költségei arányo-sak a potenciális kárértékkel, azaz a védelemre akkora összeget és olymódon fordítanak, hogy ezzel a **kockázat** a védő számára még elviselhető, vagy annál kisebb.

Kockázat ?

- ✓ Negatív hatású esemény bekövetkezésének valószínűsége
- ✓ Az esemény által kiváltott kár nagysága

Kockázat

„Általános közgazdaságtani megfogalmazásban a kockázat mérhető valószínűsége az értékvesztésnek, vagy elmaradt haszonnak. Egy másik megfogalmazás szerint veszteség, vagy kár valószínűsége különösképpen pénzeszköz, ill. vagyon vonatkozásában.”

CARISMA

Valószínűségszámítás

„A kockázat (rizikó, riszk – mint reszkíroz) matematikai értelmezése a következő:

$$R = W \times K,$$

ahol

W a bekövetkezés valószínűsége,

K pedig a következmény súlyossága.”

Marx György

MeH ITB 12.

$$r = \sum_{t \in T} \left(p_t \times d_t \right)$$

Ahol

- **r**: a rendszer biztonsági kockázata [pl.: Ft/év],
- **T**: a releváns fenyegetések halmaza,
- $\mathbf{p_t}$: egy adott fenyegetés bekövetkezésének valószínűsége (gyakorisága) [pl.: 1/év],
- $\mathbf{d_t}$: egy adott fenyegetés bekövetkezéséből származó kár [pl.: Ft].

A kockázatelemzés fajtái

Minőségi – csak a kockázat nagyságrendjét mutatja (elviselhető-nem elviselhető, alacsony-közepes-magas, 0..10)

Mennyiségi – konkrét érték

A minőségi KE előnyei

- *Lehetővé teszi a kockázatok prioritás szerinti rendezését;*
- *Egyszerű(bb) és olcsó(bb) kockázatelemzés.*

A minőségi KE hátrányai

- *Hiányzik a következmények számszerű meghatározása;*
- *Az eredmények elnagyoltak.*

A mennyiségi KE előnyei

- *Lehetővé teszi a következmények számszerű meghatározását és ezzel költség-haszonelemzést;*
- *A kockázat pontos értékét adja.*

A mennyiségi KE hátrányai

- *Az eredmények pontatlanok, sőt tévesek is lehetnek;*
- *Drága, nagy tudást, tapasztalatot és eszközöket igényel.*

Minőségi kockázatelemzés

- Preliminary Rik/Hazard Analysis (PRA/PHA): minőségi kockázat/veszély elemzés;
- Hazard and Operability Studies (HAZOP): Brit ipari módszer a lehetséges veszélyek és működési problémák felderítésére.

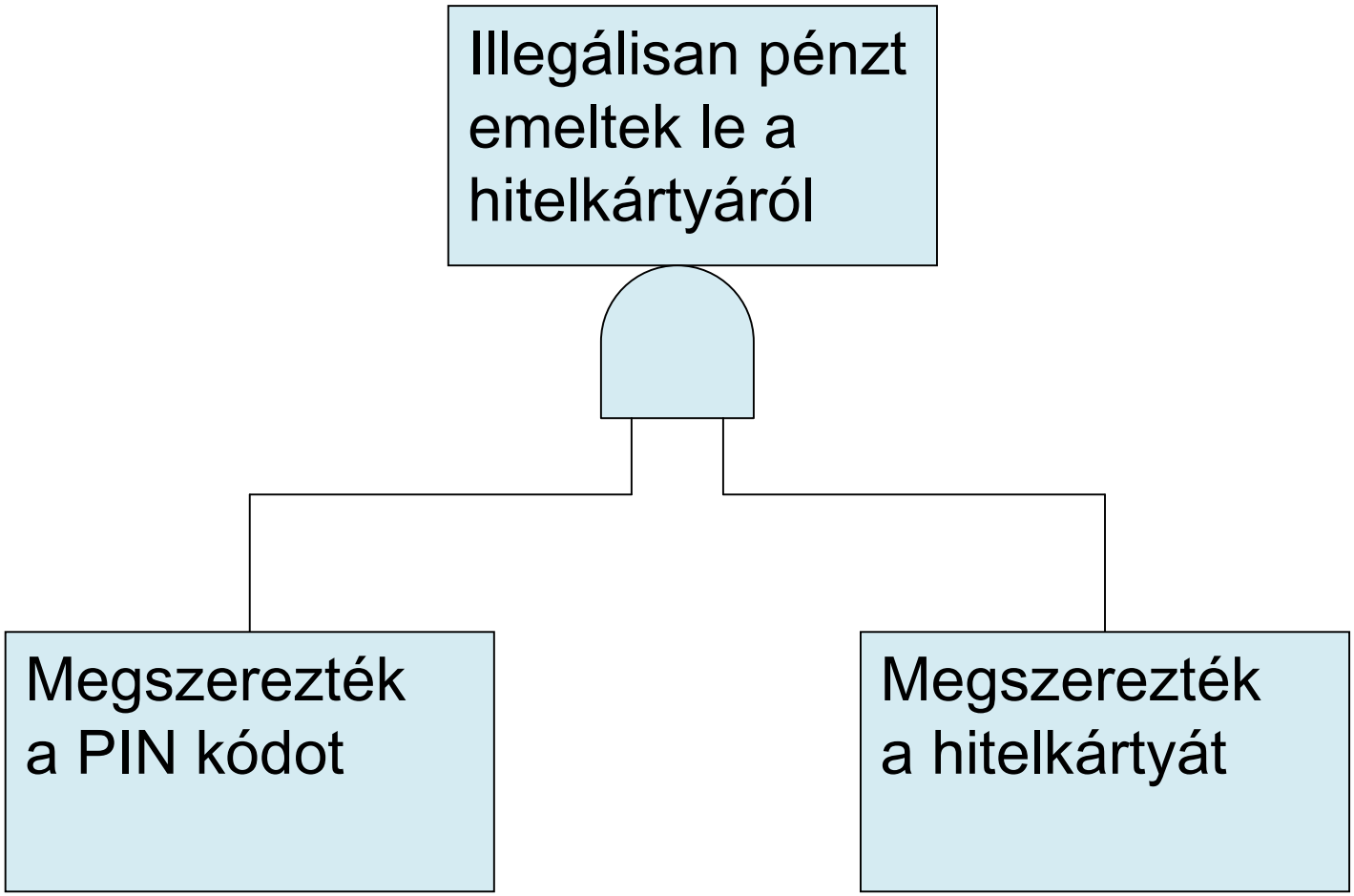
Minőségi kockázatelemzés

Failure Mode and Effects Analysis (FMEA), Failure Mode and Effects Criticality Analysis (FMECA): USA katonai módszer egy rendszer fő hibaforrásainak azonosítására, így a fegyverzet megbízhatóságának meghatározására. Ma is használatos pl. az űrkutatásban és az autógyártásban. E használható.

Fastruktúra

Fault Tree Analysis (FTA): Bináris logikán alapuló deduktívmódszer. A hibás állapothoz vezető hibakomponensek logikai összefüggései.

FTA


Illegálisan pénzt emeltek le a hitelkártyáról
Megszerezték a PIN kódot
Megszerezték a hitelkártyát

Fastruktúra

- Event-tree Analysis (ETA): Bináris logikán alapuló induktív módszer, melyben egy esemény vagy megtörténik, vagy nem. Egy nem kívánt esemény következményeinek felmérésnél használható.

A bekövetkezés gyakorisága

„Egy egyszeri véletlen eseménnyel kapcsolatban a tudomány nem tehet többet, mint hogy megállapítja annak véletlen jellegét.”

Rényi Alfréd: Valószínűségszámítás

Módszerek

COBRA = Consultative, Objective & Bifunctional Risk Analysis

CORA = Cost-of-Risk Analysis

RiskPAC

ASSSET = Automated Security Self-Evaluation Tool

Módszerek

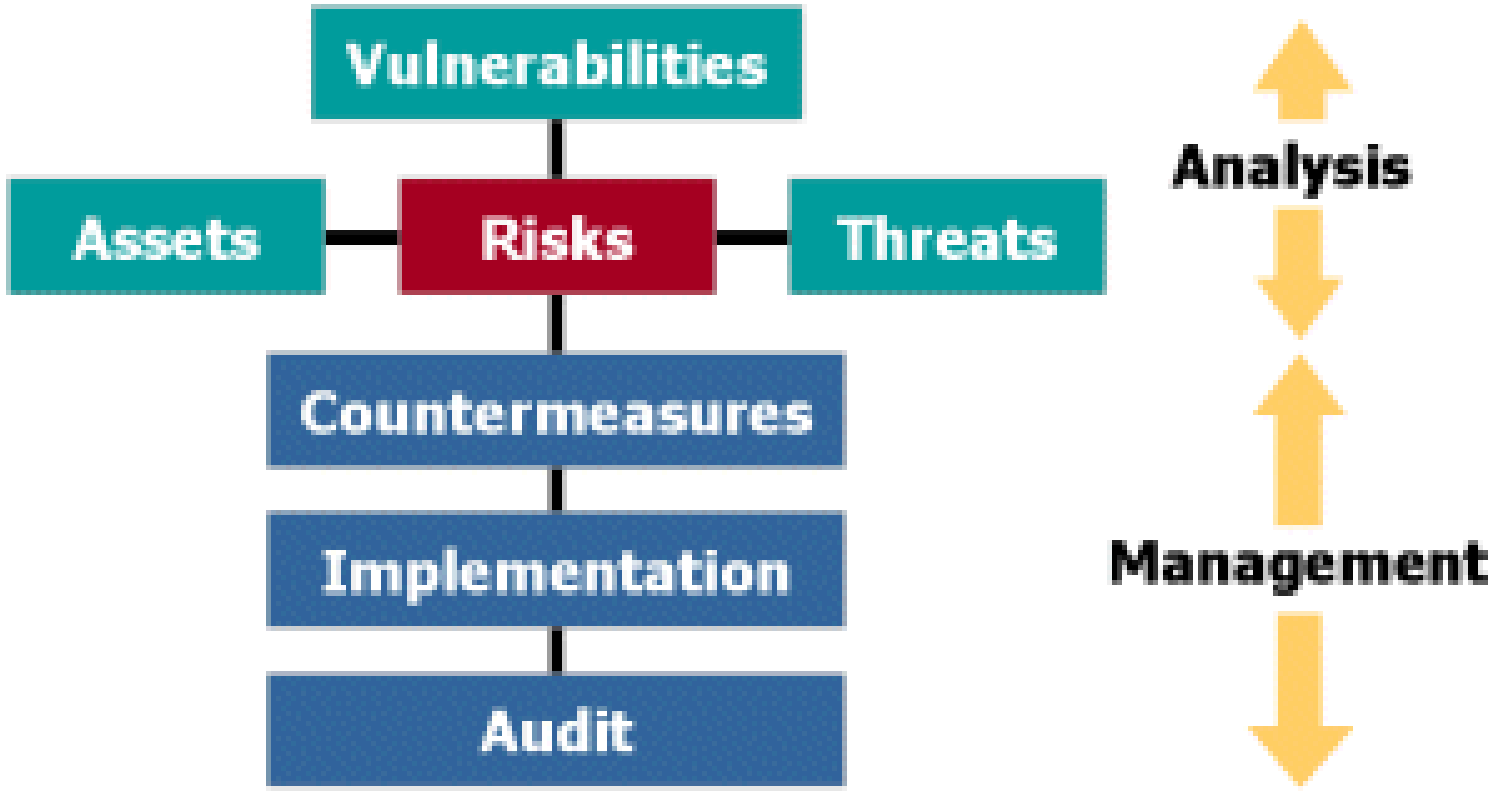
CRAMM = CCTA Risk Analysis and Management Methodology

(CCTA = Central Computer and Telecommunications Agency, ma OGC Office of Government Commerce)

Minőségi kockázatelemzési módszertan

(MeH ITB 8. => KIB 25. 1-3. IBIV)

CRAMM


Vulnerabilities
Assets
Risks
Threats
Countermeasures
Implementation
Audit
Analysis
Management

CRAMM

Express

Expert

NATO (The NATO version of CRAMM is only available by special arrangement with the NATO Office of Security!)

Siemens

(http://www.cramm.com/)

Módszerek

NIST = National Institute of Standards and Technology)

NIST Special Publication 800-30, Risk Management Guide. 2001

Minőségi kockázatbecslési módszertan

(KIB 25. 1-3. IBIV)

Köszönöm a figyelmet!

Muha Lajos PhD, CISM
főiskolai tanár, mb. tanszékvezető
ZMNE BJKMK IHI Informatikai Tanszék

muha.lajos@zmne.hu