2. Managementul riscurilor de securitate

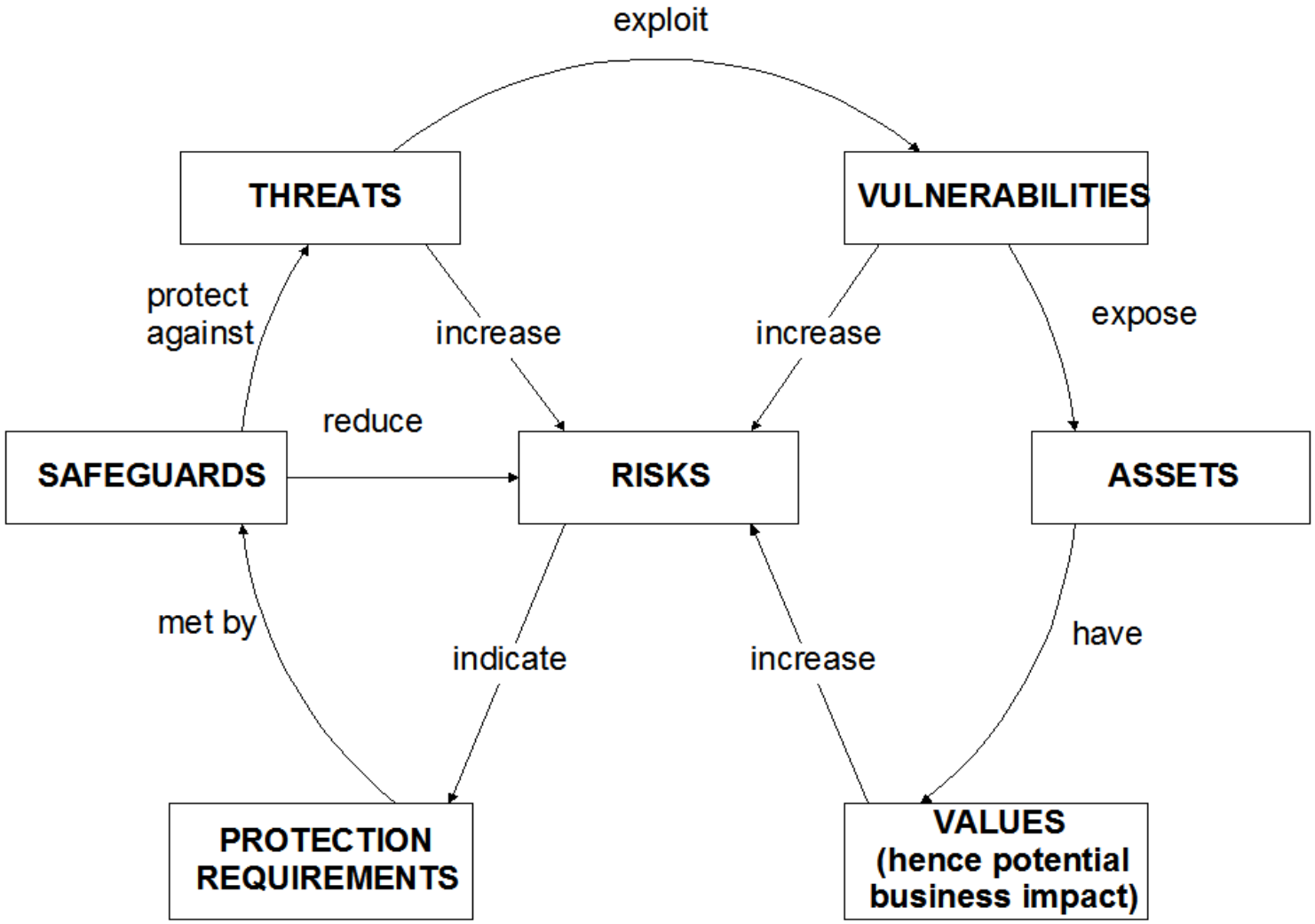
Managementul riscurilor

- “If you know the enemy and know yourself, you need not fear the result of a hundred battles.
- If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
- If you know neither the enemy nor yourself, you will succumb in every battle.” (Sun Tzu – The Art of War)

Definiţii

- Risc - *probabilitatea* ca o un *eveniment* să aibă *consecinţe* negative
  - R = probabilitate x impact
  - (asset, thread, vulnerability)
- Managementul riscurilor - procesul de identificare, evaluare şi reducere al riscurilor
  - Risk Management = Risk Assessment + Risk Treatment
- Riscul nu poate fi niciodată eliminat ci redus la un nivel acceptabil pentru organizaţie

Relaţii şi procese



Evaluarea riscurilor

- **Metode cantitative**
  - cuantificarea exactă a elementelor
- **Metode calitative**
  - folosirea de termeni aproximativi: low, medium, high

- **Etape:**
  - Inventariere bunuri (assets)
  - Identificare ameninţări
  - Identificare vulnerabilităţi
  - Estimare probabilităţi
  - Determinare impact
  - Calcul risc

Inventariere bunuri

- Identificarea bunurilor critice pentru organizaţie şi stabilirea valorii acestora
- Bunuri tangibile sau intangibile

- Primary assets
  - Business processes & activities
  - Information
- Supporting assets
  - Equipment
  - Software
  - Networks
  - Personnel
  - Premises
  - Organisational support

Identificare ameninţări

- De natură umană
  - Acţiuni deliberate
    - acces neautorizat la date şi sisteme
    - denial of service
    - interceptare / modificare trafic
    - mascarada
    - cod maliţios (virus, troian, vierme, spyware)
    - furt sau distrugere de date şi echipamente
    - social engineering
  - Accidente
    - erori de operare
    - omisiuni
- De natură tehnică
  - întrerupere alimentare cu energie
  - defectare echipamente
- De mediu
  - dezastre naturale (cutremure, inundaţii, incendii, furtuni, tsunami)
  - condiţii exterioare (contaminare, interferenţă electromagnetică)

Identificare vulnerabilităţi

- Mecanisme control acces
- Configuraţie echipamente
- Defecte software (bug-uri)
- Tehnologii utilizate
- Mod de organizare
- Încadrare cu personal
- Instruire utilizatori
- Amplasare clădire, camere servere

Estimare probabilităţi

- **Frecvenţa cu care o ameninţare poate exploata o vulnerabilitate**
- **Se estimează pentru fiecare combinaţie (asset, thread, vulnerability)**

Probability	***Definition***	***Scale***
Negligible	*Unlikely to occur*	*0*
Very Low	*2-3 times every 5 years*	*1*
Low	*<= once per year*	*2*
Medium	*<= once every 6 months*	*3*
High	*<= once per month*	*4*
Very High	*=> once per month*	*5*
Extreme	*=> once per day*	*6*

Determinare impact

- **Consecinţa materializării unei ameninţări**
- **Se estimează pentru fiecare combinaţie (asset, thread, vulnerability)**

Harm	*Definition*	*Scale*
Insignificant	No impact	0
Minor	No extra effort required to repair	1
Significant	Tangible harm / extra effort required to repair	2
Damaging	Significant expenditure of resources required Damage to reputation and confidence	3
Serious	Extended outage and / or loss of connectivity Compromise of large amounts of data or service	4
Grave	Permanent shutdown Complete compromise	5

Calcul risc

Risk = Probability x Harm

Scale	*Definition*
0	NIL
1-3	Low
4-7	Medium
8-14	High
15-19	Critical
20-30	Extreme

Calcul risc - Exemplu

Asset	*Threat*	*Vulnerability*	*Prob*	*Harm*	*Risk*
Data Center	Flood	Proximity to river	0	5	NIL
System Administrator	Absence	Lack of cross training	4	2	HIGH
Web Server	Disk crash	Insufficient backup	2	3	MEDIUM
Research work	Theft	Communication channel security	1	4	MEDIUM
Organization Reputation	Server unavailability	External internet interfaces	5	4	EXTREME

Strategii de control al riscurilor

- **Reducerea riscului**
  - eliminare vulnerabilităţi sau reducere impact
  - măsuri tehnice, procedurale sau administrative
- **Transferarea riscului (către o altă organizaţie)**
  - poliţe de asigurare
  - managed security services
- **Acceptarea / asumarea riscului**
  - cost benefit analysis

Metodologii şi unelte pentru managementul riscurilor

- CRAMM
- EBIOS
- ISO/IEC IS 13335-2
- IT-Grundschutz (IT Baseline Protection Manual)
- NIST SP 800-30 - Risk Management for Information Technology Systems
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

- Unelte: Cobra, Proteus, Callio, GStool, RiskWatch, etc.

- ENISA - "*Survey of existing Risk Management and Risk Assessment Methods*"

Metodologii pentru evaluarea / managementul riscurilor

Attributes / Methods	Risk identification	Risk Analysis	Risk Evaluation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only) (Information assessed in June 2006)	Size of organization	Skills needed[8]	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	●●	●	●	●●●	●●●	●●●	●●●	DE	Free	All	**	N	N	Prototype (free of charge)
Cramm	●●●	●●●	●●●					EN, NL, CZ	Not free	Gov, Large	***	N	N	CRAMM expert, CRAMM express
Dutch A&K analysis	●●●	●●●	●●●					NL	Free	All	*	N	N	
Ebios	●●●	●●●	●●●	●●●	●●●	●●●	●●●	EN, FR, DE, ES	Free	All	**	Y	N	EBIOS version 2 (open source)
ISF methods	●●●	●●●	●●●	●●●	●●●	●●●	●●●	EN	For ISF members	All except SME	* to ***	N	N	Various ISF tools (for members)

Metodologii pentru evaluarea / managementul riscurilor (cont.)

Attributes / Methods	Risk identification	Risk Analysis	Risk Evaluation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only) (Information assessed in June 2006)	Size of organization	Skills needed[8]	Licensing	Certification	Dedicated support tools
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	●●	●●	●●	●●	●●●	●●●	●●●	EN	Ca. €100	All	**	N	N	
ISO/IEC IS 17799	●				●			EN	Ca. €130	All	**	N	Y	Many
ISO/IEC IS 27001					●	●		EN, FR	Ca. €80	Gov, Large	**	Y	Y	Many
IT-Grundschutz	●●●	●●●	●●●	●●●	●●●	●●●	●●●	EN, DE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	●●●	●●●	●●●					EN, FR	Not free	Large	*	N	N	
Mehari	●●●	●●●	●●●					EN, FR	€100-500	All	**	N	N	RISICARE
Octave	●●	●●	●●	●●	●●	●●	●●	EN	Free	SME	**	N	N	
SP800-30 (NIST)	●●●	●●●		●●●	●●●	●●●		EN	Free	All	**	N	N