ESTIMAREA CANTITATIVĂ ŞI CALITATIVĂ A RISCURILOR INFORMAȚIONALE

Rodica Bulai, drd UTM

This paper briefly describes the quantitative and qualitative risk assessment methods with attention on its advantages and disadvantages when applied in information security.

Estimarea riscurilor informaționale atrage după sine două abordări diametral opuse: cantitativă şi calitativă. Acestea sunt diferite prin natura metricii pe care o utilizează.

Abordarea cantitativă pune în aplicare două elemente fundamentale, şi anume probabilitatea ca un

anumit eveniment să aibă loc şi pierderea estimativă asociată cu acel eveniment.

Se recomandă ca pierderile să fie estimate pentru o perioadă de un an, astfel se poate determina:

- Pierderile Anuale Estimate însumând după categorii de amenințări: (*PAE_ai*),
- Pierderile Anuale Estimate însumând pe categorii de bunuri: (*PAE_bj*), şi
- Totalul Pierderilor Anuale Estimate pentru perechile bun/amenințare: *PAE*.

În ambele cazuri de calculare a pierderilor totale, pe categorii de amenințări sau pe categorii de bunuri, rezultatul trebuie să fie identic. Astfel, se poate genera o matrice amenințări/bunuri şi *PAE*-urile corespunzătoare fiecărui bun, respectiv, fiecărei amenințări şi *PAE-ul global*:

Matricea amenințări / bunuri

	Bunul b1	**Bunul b2**	**…**	**Bunul bn**	**PAE_ai**
Amenințarea a1	V1xE1	V2xE1	…	VnxE1	PAE_a1
Amenințarea a2	V1xE2	V2xE2	…	VnxE2	PAE_a2
…	…	…	…	…	…
Amenințarea am	V1xEm	V2xEm	…	VnxEm	PAE_am
PAE_bj	PAE_b1	PAE_b2	…	PAE_bn	**ΣPAE**

În această matrice, Vj este valoarea bunului bj, iar Ei - frecvența de producere a amenințării ai în decurs de un an.

Se identifică măsurile care pot duce la reducerea vulnerabilității față de amenințarea cea mai costisitoare. Întotdeauna se are în vedere că unele măsuri se pot aplica pentru mai multe categorii de amenințări ori pentru mai multe categorii de bunuri.

Selectarea măsurilor de control trebuie să se țină cont de realizarea următoarelor obiective:

- valoarea Rentabilității Investiției cât mai mare: $RI = r\_cxPAE\_a–C\_c$, unde C_c = Costul anual pentru aplicarea controlului c, r_c = indicele de eficacitate pentru controlul c și PAE_a = Pierderile Anuale Estimate pentru amenințarea a.
- minimizarea *PAE* (Pierderilor Anuale Estimate).

Avantajele abordării cantitative

- Aprecierea şi rezultatele sprijină o analiză statistică semnificativă, deoarece abordarea calitativă se bazează pe metrica şi procesele obiective independente substanțiale.
- Valoarea confidențialității, integrității şi disponibilității informației sunt exprimate în termini monetari cu analiza rațională . Aceasta facilitează înțelegerea pierderilor aşteptate.
- Luarea de decizii legate de bugetul securității informației este sprijinită de o bază credibilă de apreciere a costurilor/ beneficiilor pentru măsurile de atenuare a riscurilor.
- Performanța pentru managementul riscului poate fi urmărită şi evaluată cu uşurință.
- Riscul este mai bine înțeles, iar rezultatele de apreciere a riscului sunt deduse şi exprimate într-o manieră clară. Valoarea monetară, procentajele şi probabilitatea sunt estimate la cota anuală.

Dezavantajele abordării cantitative

- Pentru executarea unei aprecieri cantitative a riscului sunt necesare instrumente automatizate certificate şi o bază de cunoştințe asociată. Sunt de asemenea necesare eforturi manuale.
- Este necesară adunarea unei cantități considerabile de informație despre informația țintă şi mediul tehnologiilor informaționale utilizate.
- Cercetarea pericolului asupra populației şi a frecvenței pericolului trebuie să fie desfăşurate prin eforturile proprii ale utilizatorului, atunci când nu există o bază de cunoştințe relevantă.

Mulți experți susțin că o abordare pur cantitativă nu este practică datorită posibilului impact pe arie extinsă al unui incident şi dificultății de măsurare a unei valori numerice pentru mulți din aceşti factori. Prin urmare, poate fi necesară şi folosirea unei abordări de tip calitativ.

Aprecierea riscului de tip calitativ reprezintă procesul de evaluare a riscului pe baza analizei diferitelor scenarii care explorează impactul potențial şi posibil al diverselor incidente şi amenințări.

Majoritatea metodologiilor de apreciere calitativă a riscului utilizează un număr de elemente interconectate: amenințări, vulnerabilități şi bunuri. Astfel, riscul poate fi determinat prin: *R=Valoarea_bunului+Vulnerabilitate+Amenințare.*

Matricea de evaluare a riscurilor

	Amenințarea	**0**			**1**			**2**		
	Vulnerabilitatea	**0**	**1**	**2**	**0**	**1**	**2**	**0**	**1**	**2**
Valoarea bunurilor	**0**	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

De asemenea, este necesar de a se ține cont de câteva ipoteze foarte importante pentru estimarea calitativă a riscurilor, și anume:

1. Fiecare bun are valoarea sa și fiecare bun este vulnerabil sau nu.
2. În cazul în care un sistem este vulnerabil, există cel puțin o amenințare care poate fi realizată (amenințările și vulnerabilitățile depind unele de altele).
3. O amenințare are o anumită probabilitate de a fi realizată, în dependență de anumite circumstanțe.
4. O amenințare are anumite consecințe care depind de unele circumstanțe.

Bazându-ne pe ipotezele de mai sus, riscul poate fi calculat după următoarea formulă:

*R=Valoarea_bunului*Probabilitatea*Impactul*, unde

Probabilitatea=Vulnerabilitatea+Amenințarea.

Matricea modificată de evaluare a riscurilor

Amenințarea	**Probabilitatea**	**1**			**2**			**3**		
	Impactul (consecința)	**1**	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**
Valoarea bunurilor	**1**	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36
	5	5	10	15	10	20	30	15	30	45

Avantajele abordării calitative

- Calculele sunt simple, de la sine înțelese, nu este necesară determinarea valorii monetare în ceea ce priveşte confidențialitatea, integritatea şi disponibilitatea informației.
- Nu este necesară estimarea costurilor măsurilor de atenuare a riscurilor recomandate sau calcularea costurilor/beneficiilor. Se adresează unei indicații generale a zonelor de risc semnificative.

Dezavantajele abordării calitative

- Aprecierea şi rezultatele riscului sunt în esență subiective atât în ceea ce priveşte procesul, cât şi metrica. Datele metrice independent obiective nu sunt utilizate.
- Percepția asupra valorii bunurilor țintă nu este dezvoltată pe o bază monetară obiectivă, ceea ce ar putea să nu reflecte valoarea efectivă supusă riscului.
- Nu este posibilă urmărirea performanței managementului riscului în mod obiectiv, din moment ce toate măsurile sunt subiective.

Cu toate acestea, nu este posibilă desfăşurarea unei aprecieri pur calitative a riscului. În realitate, cele două abordări au un caracter complementar, şi de aceea sunt recomandate de a fi, întotdeauna, puse în aplicare în combinație.

Bibliografie

1. Hrvoje Segudovic, *Qualitative risk analysis methodcomparison // http://www.infigo.hr/files/INFIGO-MD-2006-06-01-RiskAsses_ENG.pdf*
2. Ion I. Bucur, *Evaluarea și managementul riscurilor de securitate //* http://www.xanderzone.ro/cursurimaster/C-II-4.pdf.
3. Александр Астахов, *Искусство управления информационными рисками*, ДМК Пресс, Москва, 2010.