ANALIZA RISCURILOR LA ADRESA SECURITĂȚII INFORMAȚILOR

Autori: Veronika JINERENCO, Andrei ANGHEL
Cond. şt. Rodica BULAI

Universitatea Tehnică a Moldovei
Email: veronika.jinerenco@gmail.com, andys.zone@yahoo.com, rodica.bulai@ati.utm.md

Abstract: *Creşterea importanței resursei informaționale a condus la escaladarea proporțională a potențialului de amenințare la adresa acesteia, fapt favorizat şi de vulnerabilitățile pe care le prezintă sistemele prin intermediul cărora se gestionează informațiile. Riscul poate fi definit ca o amenințate care poate să exploateze eventualele slăbiciuni ale unui sistem ori a unei întregi organizații. Sunt mai multe modalități de abordare a riscului. Dintre acestea se disting câteva, şi anume: o analiza cantitativă şi o analiza calitativă*

Cuvinte cheie: *risc de securitate, analiza cantitativă, analiza calitativă.*

1. Introducere

Pe fiecare dintre palierele sociale, în fiecare dintre activitățile noastre zilnice operăm cu informații, informații al cărui nivel de sensibilitate variază în funcție de prejudiciul pe care îl poate provoca compromiterea respectivei informații asupra individului sau organizației căreia îi aparține.

În acest sens, nivelul de securitate care trebuie vizat pentru informații trebuie să fie în deplină corespondență cu valoarea informațiilor şi cu prejudiciile pe care le poate genera utilizarea necorespunzătoare a acestora – dezvăluire, degradare sau lipsa disponibilității. Totodată, măsurile de securitate trebuie să țină cont de vulnerabilitățile mediului operațional şi de climatul de amenințare, care justifică aplicarea unui complex de măsuri. În acelaşi timp, costurile aferente asigurării protecției împotriva amenințărilor la adresa informațiilor au crescut, odată cu creşterea amenințărilor şi a vulnerabilităților.

Analiza riscului la adresa securității informaților este un instrument puternic pe care managerii îl au la îndemână în procesul de adoptare a deciziilor cu privire la implementarea unor sisteme eficiente de management al informațiilor şi, în ultimă instanță, în îndeplinirea misiunii organizației. Ca parte a procesului de management al riscului, analiza riscului reprezintă implementarea sistematică a metodelor, tehnicilor şi practicilor de management pentru evaluarea contextului, identificarea, analiza, evaluarea, tratarea, monitorizarea şi comunicarea riscurilor la adresa securității informațiilor şi a sistemelor prin intermediul cărora acestea sunt procesate, stocate sau transmise.

Natura fluidă a mediului tehnologic impune, totodată, necesitatea de a revizui rezultatele analizei riscului la adresa securității informațiilor, prin reluarea periodică a acestui proces. În această direcție, au fost dezvoltate diferite metode calitative şi cantitative de analiză a riscului, al căror scop este acela de a analiza în mod cât mai corect riscurile la care sunt expuse, la un moment dat, informațiile organizației.

2. Metoda cantitativă

În viziunea noastră, algoritmul de evaluare cantitativă a riscurilor informaționale ar consta din următorii paşi:

1. Calculul probabilității de exploatare a amenințărilor pentru a atingerea obiectivului.
2. Calculul probabilității de realizare a amenințărilor prin depăşirea barierelor de protecție.

protecție

3. Identificarea relațiilor cheie: amenințări, resurse protejate, vulnerabilități şi mijloace de protecție
4. Evaluarea riscurilor corespunzător indicatorilor de cost a resurselor, indicatorilor de amenințări şi vulnerabilități prin metoda tabelară (calcularea riscului pentru fiecare resursă protejată şi calcularea riscului total la realizarea fiecărei amenințări)

Din punct de vedere cantitativ, nivelul de risc - este o funcție a probabilității de realizare a unei anumite amenințări şi mărimea posibilelor pierderi.

Riscul, din punct de vedere a unei ameninţări concrete, asociată unei resurse, se poate calcula după formula:

$$R_{mk} = \sum_{l=1}^{d} \sum_{r=1}^{j} C_{mlr} * S_k \,, \qquad (1)$$

unde Cmlr - probabilitatea realizării ameninţării m prin depăşirea barierei de protecţie l, asociată cu vulnerabilitatea r (se ia în considerare că bariera de protecţie poate să lipsească);

Sk – costul resursei protejate;

j – numărul de vulnerabilităţi;

d – numărul de mijloace de protecţie.

Riscul total de realizare a unei ameninţări concrete, se poate calcula după formula:

$$R_m = \sum_{k=1}^{n} R_{mk} \,, \qquad (2)$$

unde n – numărul de resurse protejat.

Estimarea Rentabilităţii Investiţiei (RI) va fi obţinută pentru fiecare măsură de control prin formula:

$$RI = r_l * R_m - C_l, \qquad (3)$$

unde C_l = costul anual pentru aplicarea barierei de protecţie l,

r_l = indicele de eficacitate pentru bariera l,

Metoda cantitativă expusă are însă anumite neajunsuri, printre acestea se pot enumera:

- Dificultatea de a găsi un număr care să cuantifice cât mai exact frecvenţa de producere a unui eveniment.
- Dificultatea de a cuantifica anumite valori. De exemplu, sunt foarte greu de definit disponibilitatea unei informaţii şi calculul pierderilor când această caracteristică lipseşte.
- Metoda nu face distincţie între ameninţările rare, dar care produc dezastre mari ca valoare (incendiu, cutremure, tornade etc.), şi ameninţările dese care produc dezastre mici ca valoare (erori de operare), în ambele cazuri efectele financiare fiind asemănătoare.
- Alegerea numerelor folosite poate fi considerată subiectivă, muncă laborioasă care necesită timp şi consum de resurse.

2. Metoda calitativă

Metoda nu foloseşte date statistice. În schimb, se foloseşte ca dată de intrare potenţialul de pierdere. Metoda operează cu termeni ca:

• des/înalt, mediu, rar/redus – referitor la probabilitatea de apariţie a riscurilor şi impactul acestora.

• vital, critic, important, general şi informaţional – referitor la tipul şi clasificarea informaţiilor.

• numere, 1, 2, 3.

În viziunea noastră, algoritmul de evaluare calitativă a riscurilor informaţionale ar consta din următorii paşi:

1. Identificarea ameninţărilor la adresa sistemului informaţional cu estimarea calitativă a probabilităţii de producere a lor într-un interval de timp, bine precizat.
2. Identificarea vulnerabilităţilor considerate în sistemul informaţional cu evaluarea calitativă a posibilităţilor de folosire a lor de către instruşi.

3. Identificarea resurselor care urmează să fie protejate, urmată de o evaluare calitativă a costului fiecărei resurse pentru organizație (în acest caz, resursa nu reprezintă doar componentele sistemului informațional, dar şi personalul ce asigura funcționarea infrastructurii, precum şi valorile nemateriale cum ar fi reputația organizației).
4. Descrierea mijloacelor de protecție în limitele sistemului informațional.
5. Identificarea modalităților de atingere a obiectivului - impactul asupra resurselor.
6. Analiza posibilității de a depăşi mijloacele de protecție asociate fiecărei vulnerabilități.
7. Descrierea sistemului de securitate prin relații de identificare: resursele protejate şi amenințări, vulnerabilități şi resurse protejate, resurse protejate şi mijloace de protecție.

Metoda are şi dezavantaje:

- Greu de cuantificat (ca şi la metoda anterioară) anumiți termeni (de ex. *important* – este un termen greu de definit în management).
- Numerele sunt de această dată şi mai subiective. Dacă la metoda anterioară acestea erau date statistice, acum sunt alese subiectiv.

3. Concluzii

Aceste analize de risc se fac cu precădere în cadrul organizațiilor mari şi eventual în cadrul celor medii. Organizațiile mici nu au nici personal specializat şi nici bani pentru a plătii o astfel de evaluare. Cu toate acestea, un minimum de preocupări privind securitatea trebuie considerate.

Noi ne punem ca scop dezvoltarea unei aplicații software, asociată instrumentului teoretic de analiză a riscului, în vederea facilitării desfăşurării acestui proces şi accesibilă tuturor tipuri de organizații.

Bibliografie

1. Табаков Rot Artur, *IT Risk Assessment: Quantitative and Qualitative Approach*, Proceedings of the World Congress on Engineering and Computer Science, WCECS 2008, October 23-24, San Francisco, USA.
2. Măzăreanu P. Valentin, *Risk management and analysis: risk assessment (qualitative and quantitative)*, Analele ştiințifice ale Universității „Alexandru Ioan Cuza”, Iaşi, 2007.
3. Ion I. Bucur, *Evaluarea şi managementul riscurilor de securitate* // http://www.xanderzone.ro/cursurimaster/C-II-4.pdf.
4. Полянский Д.А., Файман О.И., Методика аудита информационной безопасности объекта информатизации //