Network security risk level

Lect.dr. Emil BURTESCU
Universitatea „Constantin Brâncoveanu”

The advantages of the existence of a computers network within any company with pretensions are obvious. But the construction and the existence of a network without meeting some minimum security requirements, although it would be preferable to be optimal, can lead to bad functioning in the performance of the company's business. The vulnerability of a grouping, such as a network, is given by the weakest point in its competence. The establishing of the risk level of each component of the network, and implicitly of the grouping, is highly necessary.

Keywords*: assets, consequence, exposure factor, exposure level, risk analysis, impact rate, impact value, likelihood of occurrence, risk level.*

Asigurarea securităţii reţelelor presupune luarea în considerare a următoarelor elemente definitorii pentru o arhitectură securizată: **identitate**, **integritate**, **confidenţialitate**, **disponibilitate** şi **audit**. Identitatea va cuprinde elementele de autentificare şi autorizare la nivelul reţelei. Integritatea este o componentă a securităţii care cuprinde infrastructura de securitate (accesul fizic şi logic) precum şi securizarea perimetrului. Confidenţialitatea va asigura faptul că transmisiile de date de-a lungul reţelei au caracter privat. Disponibilitatea va asigura faptul că toate resursele reţelei sunt disponibile personalului sau proceselor autorizate. Auditul este necesar pentru monitorizarea şi verificarea securităţii la nivelul firmei.

Analiza de risc presupune un proces de identificare a riscurilor de securitate, determinarea amplitudinii riscurilor, precum şi identificarea zonelor cu risc mare şi care trebuie securizate. Analiza de risc face parte din ansamblul de măsuri care poarta denumirea de **managementul riscului**. Evaluarea riscurilor este un rezultat al unui proces de analiză a riscurilor. **Managementul riscului** va cuprinde totalitatea metodelor de identificare, control, eliminare sau minimizare a evenimentelor care pot afecta resursele sistemului.

În majoritatea cazurilor, ciclul de management al riscului este împărţit în patru etape distincte: (1) analiza riscului şi determinare necesităţi, (2) alegere soluţii, (3) implementare politici şi controale şi (4) monitorizare şi evaluare.

Analiza riscului poate fi făcută folosind una din metodele cele mai des folosite: **analiza calitativă** sau **analiza cantitativă**. Dacă analiza cantitativă lucrează cu date statistice în domeniu şi este foarte laborioasă, analiza calitativă foloseşte estimări şi este mai puţin laborioasă, aceasta pretându-se la firmele medii şi mici. În cele ce urmează se va discuta despre analiza calitativă.

Dacă pentru anliza riscului în general, cel mai important rol îl are proprietarul de resurse, pentru analiza riscului la nivelul reţelei, pe lângă acesta mai sunt şi persoanele din conducerea IT care pot să evalueze la o valoare reală un bun din domeniu. Proprietarul stabileşte ce este important pentru afacerea sa şi defineşte un risc acceptabil pentru afacerile firmei. Grupul de securitate, desemnat de către conducere, va evalua riscurile, va defini cerinţele de securitate impuse de către proprietar, şi va măsura eficacitatea soluţiilor propuse. Grupul IT va fi cel care se va ocupa de proiectarea şi implementarea soluţiilor de securitate, precum şi de exploatare şi suport pentru acestea.

Analiza riscului la nivelul reţelei se face parcurgând următorii paşi:

- Identificarea bunurilor reţelei;
- Determinarea valorii bunurilor;
- Stabilirea nivelului de pierderi şi a nivelului de impact;
- Estimarea probabilităţii de producere;

- Determinarea expunerii;
- Determinarea ratei de impact;
- Identificare controale curente şi determinarea probabilității de impact;
- Determinarea nivelului de risc.

Identificarea bunurilor rețelei va cuprinde un proces amplu de inventariere şi clasificare a tuturor bunurilor care formează şi dau valoare rețelei din firmă. O clasificarea a acestora va putea fi făcută conform tabelului următor (tabelul 1):

Tabelul 1. Clasificarea bunurilor rețelei

Bunul rețelei	**Descriere**
Hardware	Servere, stații de lucru, imprimante, firewall-uri, router-e, switch-uri, modem-uri, conectoare, convertoare, medii de transmisie.
Software	Sisteme de operare (rețea şi locale), programe de aplicații, utilitare, programe de testare şi diagnosticare, programe de comunicare, programe de securizare, surse program, programe obiect.
Date	Baze de date, date stocate online şi date stocate offline, copii de siguranță (backup), date vehiculate în mediu rețelei.
Oameni	Administratorii rețelei, depanatorii şi cei care se ocupa cu întreținerea rețelei, utilizatorii.
Documentații	Proceduri de administrare la nivel de rețea, standarde, îndrumare, evaluări hardware şi software.
Auxiliare	Sisteme auxiliare care mențin în funcțiune elementele hardware ale rețelei.

Determinarea valorii bunurilor este o operație destul de subiectivă. Aceasta deoarece, pentru bunurile intangibile, este greu de evaluat valoarea acestora. Din aceste motive, evaluarea unui bun tangibil se face bazându-ne pe **valoarea de înlocuire** a acestuia, iar atunci când bunul este intangibil, se face prin determinarea **valorii impactului** creat prin pierderea bunului respectiv. Impactul generat de pierderea datelor este dat de apartenența acestora la o anumită categorie de date: administrative, financiare, clienți, cercetare, private. Valoarea impactului se va calcula ținând cont de impactul pe fiecare din elementele definitorii în asigurarea securității la nivelul rețelei (identitate, integritate, confidențialitate, disponibilitate şi audit).
Stabilirea nivelului de pierderi şi a nivelului de impact se va face prin gruparea datelor într-un tabel de forma (tabelul 2):

Tabelul 2. Stabilirea valorii clasei de impact

Pierderi (USD)	**Punctaj**	**Clasa de impact**	**Valoarea clasei de impact (VCI)**
<1.000	1	Redus	2
1.001-5.000	2	Redus	
5.001-10.000	3	Redus	
10.001-50.000	4	Mediu	5
50.001-100.000	5	Mediu	
10.001-500.000	6	Mediu	
500.001-1.000.000	7	Înalt	10
1.000.001-5.000.000	8	Înalt	
> 5.000.000	9	Înalt	

Datele din tabel sunt pentru o firmă de nivel mediu. Aceste valori se vor completa stabilind un nivel minim şi un nivel maxim al pierderilor pentru firma respectivă, gruparea acestor valori pe **trei** niveluri şi stabilind în final valoarea clasei de impact.

Estimarea probabilității de producere a unui eveniment se va face ghidându-ne după următorul tabel (tabelul 3).
Determinarea expunerii presupune încadrarea consecințelor unui eveniment într-unul din următoarele (conform tabelului 4).

Tabelul 3. Stabilirea probabilității de producere

Probabilitate de producere	Descriere
Înaltă	**Sigur**. Se produce o dată sau de mai multe ori pe an
Medie	**Probabil**. Eveniment care se poate produce cel putin o dată sau de două sau trei ori pe an
Redusă	**Improbabil**. Eveniment care nu se poate produce în următorii trei ani

Tabelul 4. Determinarea expunerii

Consecințe	Nivel de expunere	Factorul de expunere (FE)	Descriere
Insignifiante	1	100%	Pierderi insignifiante.
Minore	2	80%	Pierderi minore.
Moderate	3	60%	Pierderi moderate. Firma funcționează la capacitate.
Majore	4	40%	Pierderi majore. Firma nu mai funcționează la capacitate.
Catastrofale	5	20%	Pierderi extreme. Firma nu mai funcționează deloc.

Determinarea ratei de impact se va face ținând cont de faptul că:

Rata de impact = Clasa de impact x Factorul de expunere (RI = VCI x FE)

Valorile rezultate ale ratei de impact se pot situa între 0 şi 10.

Rata de impact (RI)	Nivel
7 - 10	Înalt
4 - 6	Mediu
0 - 3	Redus

Identificare controale curente şi determinarea probabilității de impact va presupune o inventariere a controalelor existente în firmă şi care au menirea să asigure securitatea rețelei. Se ştie că între controale şi probabilitatea de impact există o strânsă legătură. Cu cît controalele sunt mai slabe cu atât probabilitatea de producere a unui eveniment este mai mare. Probabilitatea de producere a unui eveniment scade cu aplicarea controalelor.

Determinarea probabilității de impact va presupune stabilirea existenței unei anumite vulnerabilități şi posibilitatea exploatării acesteia, precum şi stabilirea de posibilități ca o anumită vulnerabilitate să fie diminuată prin folosirea controalelor.

Nivelul de vulnerabilitate depinde in principal de câteva atribute şi anume: **numărul de atacatori**, **tipul de atac**, **cunoştințele în domeniu** şi **automatizarea procesului**.

Vulnerabilitatea va creşte dacă numărul persoanelor care produc un atac este mare, iar nivelul de pregătire al acestora ridicat, dacă există posibilitatea exploatării de la distanță a anumitor goluri de securitate, documentațiile în domeniul respectiv abundă, şi dacă un tip de atac poate fi automatizat în aşa fel încât să găsească singur şi să exploateze golurile de securitate.

Nivelul de vulnerabilitate este împărțit pe trei mari categorii (tabelul 5):

Tabelul 5. Nivelul de vulnerabilitate

Nivel de vulnerabilitate	Condiții	Punctaj*
Înalt	**1.** Număr mare de atacatori (script-uri); **2.** Atac la distanță; **3.** Privilegii maxime; **4.** Modalități de atac foarte bine cunoscute şi documentate; **5.** Automatizare.	**5**
Mediu	**1.** Număr mediu de atacatori – specialist; **2.** Atac local; **3.** Necesită drepturi de acces; **4.** Metode de atac nedocumentate; **5.** Neautomatizare.	**3**
Redus	**1.** Număr redus de atacatori – cunoştințe arhitectură internă; **2.** Atac local; **3.** Necesită privilegii de Administrator; **4.** Metode de atac nedocumentate; **5.** Neautomatizare.	**1**

* - dacă cel puțin una din condiții este îndeplinită.

Pentru a determina cât de eficiente sunt controalele trebuiesc stabilite o serie de evaluări pe baza unor seturi de întrebări puse. Aceste întrebări pot fi:

1. Responsabilități sunt bine definite şi efectiv aplicate?
2. Sunt atenționările comunicate şi urmărite executările acestora?
3. Procesele şi procedurile sunt bine definite şi învățate?
4. Controalele existente reduc amenințările?
5. Auditarea curentă este suficientă pentru detectare şi control?

Răspunsurile afirmative vor primi nota **0** (zero), în timp ce răspunsurile negative vor primi nota **1** (unu). Deci se poate spune că neaplicarea unui control (nota 1) va face să crească probabilitatea de producere, în timp ce aplicarea controlului (nota 0) va face să scadă probabilitatea de producere. Orice punct acumulat la setul de cinci întrebări va fi un punct în favoarea probabilității de producere.

Însumând punctele de la nivelul de vulnerabilitate cu cele de la eficacitatea controalelor vom obține rata totală de probabilitate. Luând ca exemplu un server şi rețeaua aferentă, se vor obține **5** (cinci) puncte de la nivelul de vulnerabilitate (configurare improprie server) şi încă **3** (trei) puncte de la eficacitate controale.

În final vom avea o rată totală de probabilitate de valoare **8** (**5** de la nivelul de vulnerabilitate şi **3** obținute prin însumarea punctelor de la eficacitate controale).

Determinarea nivelului de risc se va face cu ajutorul formulei:

Nivelul de risc = Rata de impact x Rata de probabilitate (NR = RI x RP)

Rata de impact (RI)			**Rata de probabilitate (RP)**	**Rezultat**	**Nivelul de risc (NR)**
7 - 10	Înaltă	**X**	7 - 10	41 – 100	Înalt
4 - 6	Medie		4 - 6	20 – 40	Mediu
0 - 3	Redusă		0 - 3	0 - 19	Redus

Un nivel de risc înalt este inacceptabil pentru firmă. Chiar şi valorile medii trebuie luate în considerare şi adoptate controale pentru reducerea nivelului de risc. Un nivel minim de securitate este de preferat în locul lipsei acesteia..

Este indicat ca firma să-şi creeze o diagramă anuală de evoluție a riscului, cu detalieri pe zonele unde au fost fluctuații ale nivelului de risc şi, în zonele cu aceste fluctuații, să ia măsurile care se impun..

Bibliografie

- M. Kaeo, *Designing Network Security*, Cisco Press, Indianapolis, Indiana 46290 USA, 1999.
- L. McCarthy, *IT Security: Risking the Corporation*, Prentice Hall PTR, 2003.
- P.E. Proctor, F.C. Byrnes, *The Secured Enterprise*, Prentice Hall PTR, 2002.
- http://www.microsoft.com/technet/security/topics/secrisk/default.mspx