SECURITATEA OPERAȚIUNILOR ÎN PROTECȚIA INFORMAȚIILOR DIN CADRUL UNEI ÎNTREPRINDERI

Aureliu ZGUREANU
Academia de Studii Economice a Moldovai, Republica Moldova, Chişinău, str. Mitropolit Gavriil Banulescu-Bodoni 61, ase.md, +373 22 402 872, zgureanu.aureliu@ase.md
Corresponding author: zgureanu.aureliu@ase.md

Abstract. *Computerization in the modern society not only offers benefits - it is accompanied by multiple risks and vulnerabilities. Ensuring a sufficient level of information protection within an enterprise should be a major concern, imposing the responsibility of using not only traditional techniques, but also some others, which have been proven effective in other areas.*

The purpose of the research is to find new directions for applying the operations security in the process of ensuring information protection within an enterprise.

The research methods used were analysis, generalization and modeling. Using them there were synthesized the content of operations security as an important element of the entire information protection process within an enterprise or organization. There are described steps, presented some of the best practices and proposed some examples of using of the operations security.

Key words**:** *securitatea informaţiei, securitatea operaţiunilor, securitatea operaţională, analiza riscurilor.*

Jel Clasification: **D89, G18, L88**

INTRODUCERE

Securitatea operaţiunilor (*OPSEC* - *Operations security*), cunoscută şi sub denumirea de securitate procedurală, este un proces de gestionare a riscurilor care încurajează managerii să examineze operaţiunile din perspectiva unui potenţial adversar în scopul de a proteja informaţia sensibilă de nimerirea ei la persoane sau procese inacceptabile.

Securitatea operaţiunilor este adesea confundată cu securitatea operaţională (Operational security), iar aceşti doi termeni sunt adesea folosiţi interschimbabil, ceea ce poate duce la o mare confuzie şi la o informare necorespunzătoare. În realitate, deşi ambii termeni sunt deseori abreviaţi drept „OPSEC", fiecare se referă la tipuri distincte de securitate.

OPSEC (în sensul de Securitate a Operaţiunilor) este procesul prin care privim la operaţiunile noastre din punctul de vedere al adversarului. În rezultat sunt stabilite contramăsurile corespunzătoare pentru a diminua indicatorii potenţiali, ce ar putea ajuta adversarul să determine cu ce ne ocupăm la un moment oarecare. În comparaţie cu aceasta, Securitatea Operaţională este cel mai bine descrisă ca fiind securitatea care o aplicăm pentru a proteja o anumită operaţiune. În termeni mai simpli, Securitatea Operaţiunilor se referă la program, proceduri, mentalitate etc., în timp ce Securitatea Operaţională se referă la o anumită operaţiune şi este aplicată în mod particular de la caz la caz [3].

Deşi iniţial folosită de armată [1], OPSEC devine tot mai populară şi în sectorul privat. Sub incidenţa securităţii operaţiunilor cade, de exemplu, monitorizarea comportamentelor şi obiceiurilor de pe site-urile de social media, precum şi descurajarea angajaţilor de a partaja acreditările de autentificare prin e-mail sau prin mesaje text.

OPSEC mai poate fi privită ca practica protejării informaţiilor în contextul activităţilor de zi cu zi şi poate include diverse instrumente şi reglementări pentru protejarea datelor. Securitatea operaţiunilor se concentrează şi pe conştientizarea modului în care dezvăluirile de informaţii aparent inofensive pot fi folosite de către atacatori.

ETAPELE ŞI CELE MAI BUNE PRACTICI ALE SECURITĂŢII OPERAŢIUNILOR

Procesele implicate în securitatea operaţiunilor pot fi clasificate în cinci etape [1, 2] (figura 1):

1. *Identificarea datelor sensibile*, inclusiv cercetările referitoare la produsele dezvoltate, proprietatea intelectuală, situaţiile financiare, informaţiile despre clienţi şi informaţiile despre angajaţi. Acestea vor fi datele de care avem nevoie să le cunoaştem şi pentru care ne vom concentra resursele destinate protecţiei informaţiei.

2. *Identificarea posibilelor ameninţări*. Pentru fiecare categorie de informaţii pe care managerii le consideră sensibile, ar trebui să fie identificate toate tipurile existente de ameninţări. Însă, concomitent cu atenţia acordată terţelor părţi care ar putea încerca să fure sau să altereze informaţiile sensibile, ar trebui de avut grijă şi de ameninţările interne, cum ar fi de exemplu angajaţii neglijenţi sau muncitorii nemulţumiţi.

3. *Analiza breşelor de securitate şi a altor vulnerabilităţi*. Este necesar de a evalua măsurile de protecţie actuale şi de a determina care lacune sau deficienţe, dacă acestea există, pot fi exploatate de către răuvoitori pentru a avea acces la datele sensibile.

4. *Evaluarea nivelului de risc asociat cu fiecare vulnerabilitate*. Este necesară evaluarea şi clasificarea vulnerabilităţilor utilizând factori cum ar fi: probabilitatea producerii unui atac, amploarea eventualelor pagube, cantitatea de muncă sau timpul necesar pentru recuperare. Cu cât este mai probabil şi mai dăunător un atac, cu atât mai mult ar trebui să i se acorde prioritate atenuării riscului asociat.

Luarea de contramăsuri relevante. Ultima etapă a securităţii operaţiunilor este crearea şi implementarea unui plan de eliminare a ameninţărilor şi de atenuare a riscurilor. Aceasta ar putea include actualizarea hardware-ului, crearea de politici noi privind datele sensibile sau instruirea angajaţilor cu privire la politicile companiei şi la cele mai bune practici de securitate. Contramăsurile ar trebui să fie directe şi simple, iar angajaţii ar trebui să poată implementa măsurile necesare din partea lor, cu sau fără formare suplimentară.

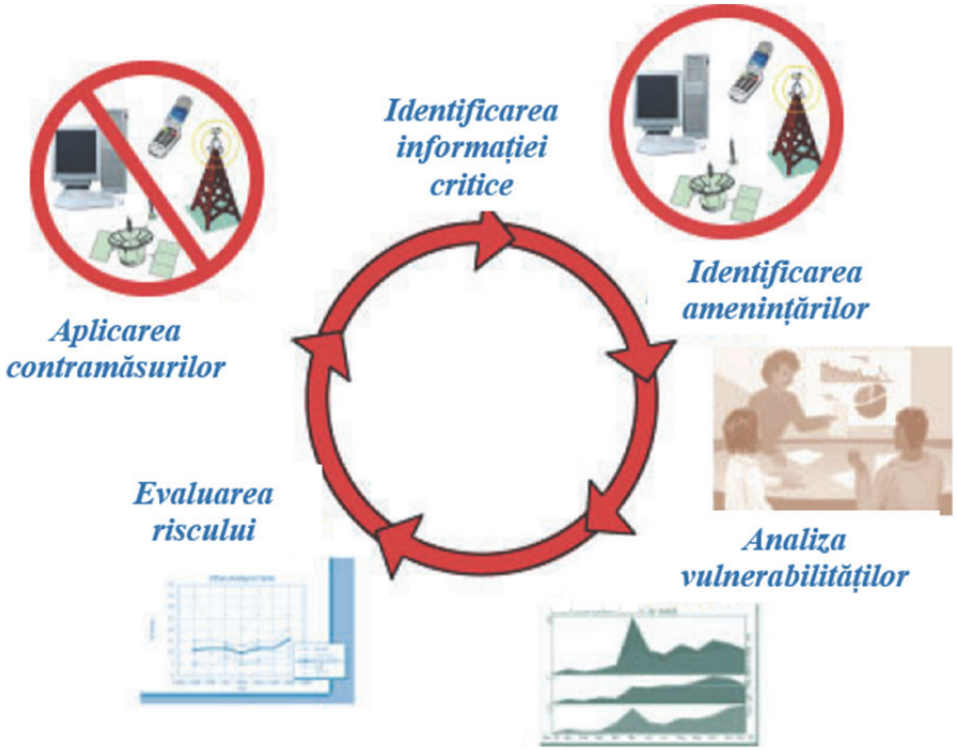

Fig. 1. Procesul securităţii operaţiunilor [2]

Pentru a implementa un program robust şi cuprinzător de securitate a operaţiunilor este necesar de urmat *cele mai bune practici de securitate*, cu ar fi de exemplu:

- *Implementarea proceselor precise de gestionare a modificărilor* pe care angajaţii companiei ar trebui să le respecte atunci când se efectuează, de exemplu, modificări ale reţelei. Toate modificările trebuie înregistrate şi controlate astfel încât să poată fi monitorizate şi supuse auditului.
- *Restricţionarea accesului la dispozitivele de reţea* utilizând autentificarea AAA *Authentication, Authorization, Accounting*). De exemplu în entităţile militare şi alte entităţi guvernamentale, este adesea utilizată o bază "need to know" ca regulă generală în ceea ce priveşte accesul şi schimbul de informaţii.
- *Acordarea accesului minim necesar angajaţilor* pentru îndeplinirea sarcinilor de lucru şi practicarea principiului celor mai mici privilegii.
- *Implementarea controlului dual*. Este necesar de asigurat că cei care lucrează în reţeaua corporativă nu sunt aceiaşi oameni care se ocupă de securitate.
- *Automatizarea sarcinilor pentru a reduce nevoia de o intervenţie umană*. Oamenii sunt cea mai slabă legătură în iniţiativele de securitate a operaţiunilor ale oricărei organizaţii, deoarece fac greşeli, uită detaliile, uită lucrurile şi procesele de bypass.
- *Răspunsul la incidente şi planificarea recuperării în caz de dezastru* sunt întotdeauna componente esenţiale ale unei poziţii de securitate temeinică. Chiar dacă măsurile de securitate a operaţiunilor sunt robuste, trebuie de avut un plan de identificare a riscurilor, de răspuns la acestea şi de atenuare a eventualelor daune.

Aici mai trebuie de menţionat că odată ce au fost stabilite măsurile concrete de securitate a operaţiunilor – ele sunt obligatorii pentru realizare (de altfel ca şi oricare dintre celelalte măsuri de securitate).

În continuare sunt prezentate unele exemple de OPSEC care, utilizate în parte sau împreună cu altele, vor îmbunătăţi în ansamblu nivelul de securitate a informaţiilor în cadrul unei organizaţii sau întreprinderi.

Exemplul 1. *Instruirea pentru conştientizarea necesităţii securizării informaţiilor*. Într-o organizaţie au se petrec cursuri de instruire în domeniul securităţii informaţiilor, unde sunt prezentate inclusiv cazuri memorabile prin care procesele sociale au permis divulgarea informaţiilor care, la rândul lor, au permis realizarea atacurilor de securitate.

Exemplul 2. *Criptarea*. Criptarea tuturor datelor din spaţiul de stocare şi de tranzit pe toate dispozitivele organizaţiei.

Exemplul 3. *Politicile pentru discuţii*. Dezvoltarea şi implementarea de Politici care au drept scop împiedicarea angajaţilor de a discuta afaceri confidenţiale în afara locaţiilor securizate.

Exemplul 4. *Locaţiile securizate*. Negocierile referitoare la fuziuni sau achiziţii se desfăşoară într-o locaţie privată asigurată, de exemplu, de băncile consiliere. Discuţiile pot fi limitate la o singură încăpere (locaţie), punând accentul pe folosirea documentelor pe suport de hârtie care nu pot fi îndepărtate din încăperea dată.

Exemplul 5. *Curăţarea biroului*. O organizaţie cere angajaţilor să păstreze birourile libere de hârtie şi să îşi blocheze dispozitivele atunci când nu sunt prezente.

Exemplul 6. *Utilizarea de unelte software*. O afacere mică rulează unele programe şi/sau browserele web într-un instrument de tip sandbox, care limitează atacurile informatice într-un mediu virtual.

CONCLUZII

1. Gestionarea riscurilor implică identificarea ameninţărilor şi a vulnerabilităţilor înainte ca acestea să devină probleme.
2. Securitatea operaţiunilor îi forţează pe managerii de securitate se pătrundă profund în operaţiunile lor ca să îşi dea seama unde ar putea fi penetrate cu uşurinţă informaţiile lor sensibile.
3. Privind operaţiunile din perspectiva unei persoane terţe rău intenţionate managerii pot detecta vulnerabilităţile pe care altfel le-ar fi ratat şi, în acest fel, vor putea implementa contramăsurile adecvate pentru a proteja datele sale sensibile.
4. Securitatea operaţiunilor ne permite să cunoaştem ameninţările, să cunoaştem ce să protejăm şi, în final să realizăm protecţia.

BIBLIOGRAFIE

[1]. JOINT CHIEFS OF STAFF WASHINGTON DC, *Operations Security*. *Joint Publication* 3-13.3. 04 January 2012.
[2]. U.S. NAVY NTTP 3-13.3M. *Operations security* (*OPSEC*). Edition september 2017.
[3]. RĂDUCAN, Octavian. *Securitatea operaţiunilor.* Revista Intelligence, http://intelligence.sri.ro/securitatea-operatiunilor /.
[4]. https://www.opsecprofessionals.org/, The Operations Security Professional's Association official website.