INFORMATION SECURITY AND RISK MANAGEMENT - AN ECONOMIC APPROACH

Lt. col. lect. univ. dr. ing. Cezar VASILESCU
Departamentul Regional de Studii pentru Managementul Resursele de Apărare

Abstract

This paper presents an approach that allows risk management and information security in organizations modeling from an economic point of view. Given that IT&C systems are subject to constant attacks, risk management has become a crucial task to minimize the potential risks that may affect their proper functioning. To prevent organizational difficulties generated by cyber attacks or failure of the information systems there are made continuous investments in various security measures and data protection systems are purchased. Along with the increase of potential risks, the investment of funds in the security and data protection services has become a serious economic problem for many organizations. This paper examines several approaches allow the assessment of the investments from an economic point of view, investments which are necessary for information security goals. This paper introduces methods for identifying assets, threats, vulnerabilities of the IT & C systems and proposes a procedure which allows the optimal investment choice of the necessary security technologies based on the quantification of the values of the protected systems.

1. Introducere

În ultimele decenii, accentuarea schimburilor de informaţii în format electronic, a determinat o dependenţă din ce în ce mai mare a organizaţiilor de sistemele lor informatice şi de furnizorii de Internet. Atacurile potenţiale asupra sistemelor informatice şi eventuala lor defectare pot duce la pierderi de date şi întreruperea activităţii pentru o anumită perioadă de timp. Riscurile de securitate

apar de obicei din cauza defecțiunilor tehnice, vulnerabilităților de sistem, erorilor umane sau datorită unor evenimente externe.

Acesta este cauza pentru care organizațiile investesc fonduri considerabile pentru achiziția de sisteme de securitate informaționale, menite a le proteja confidențialitatea, integritatea şi disponibilitatea de operare. Conştientizarea riscurilor potențiale duce la creşterea investițiilor în acest domeniu. În ciuda acestui fapt incontestabil şi a progreselor înregistrate în ultimii 10 ani, nivelul de securitate al rețelelor de calculatoare nu a fost îmbunătățit considerabil [1]. Acest lucru a dus la necesitatea adoptării unui punct de vedere economic, având în vedere că tehnologia singură nu poate rezolva problema expusă anterior.

Managementul riscurilor de securitate informațională reprezintă un proces care integrează identificarea şi analiza riscurilor la care organizația este expusă, analiza impactului potențial asupra „afacerilor" şi decizia asupra acțiunilor care pot fi întreprinse pentru eliminarea sau reducerea riscului la un nivel acceptabil [2]. Necesită o identificare şi evaluare completă a infrastructurilor informaționale organizaționale, a consecințelor incidentelor de securitate, a probabilității de succes a atacurilor asupra sistemelor IT&C, precum şi a costurilor şi beneficiilor aduse de investițiile în sisteme de securitate informațională.

Managementul riscurilor de securitate informațională constă din:

- identificarea infrastructurilor informaționale organizaționale;
- identificarea amenințărilor şi analiza impactului unui atac informatic încheiat cu succes;
- identificarea vulnerabilităților sistemice pe care respectivul atac le-ar putea exploata;
- analiza riscurilor de securitate;
- măsuri de minimizare a riscului;
- monitorizarea eficienței măsurilor implementate.

Scopul analizei riscurilor de securitate informațională este acela de a identifica şi măsura riscul, pentru a realiza o informare promptă a factorilor de decizie din organizație.

2. Identificarea infrastructurilor informaționale şi a valorii lor pentru organizație

Primul pas al procesului este identificarea infrastructurilor informaționale (în termeni economici numite „active"). Acestea constau din informații şi resurse informaționale care dau valoare organizației. După identificare, activele trebuiesc evaluate. Pentru activele tangibile (infrastructuri fizice - servere, stații de lucru, infrastructură de rețea), acest lucru este uşor, măsura lor fiind banii. Pentru cele intangibile (informații de afaceri, reputația organizației, „cunoaşterea" organizației, proprietatea intelectuală) situația este mai complicată, acestea neputând fi cuantificate direct în unități monetare.

Pentru analiza activelor, acestea sunt de obicei clasificate în clase discrete [3] [4] [5] care facilitează definirea riscurilor globale de securitate şi permit în

primul rând concentrarea asupra activelor critice (date financiare, proprietate intelectuală, etc.). Clasa activelor cu risc moderat cuprinde informațiile interne de afaceri, scheme ale rețelelor informatice, informații asupra site-urilor web, etc. Active cu risc scăzut sunt informațiile asupra paginilor web accesibile public, comunicatele de presă, broşurile privind produsele oferite şi documentația aferentă, etc.

3. Identificarea amenințărilor

Activele informaționale ale organizațiilor sunt implicit expuse amenințărilor, care pot fi definite ca "orice eveniment potențial cu impact nedorit". Organizațiile trebuie să identifice cu claritate potențialele amenințări, pentru a-şi îmbunătăți gradul de protecție şi stabilirea unor strategii viabile de securitate.

Cele mai uzuale amenințări se exercită asupra unor ținte cum ar fi rețelele de calculatoare, software-ul instalat, datele vehiculate precum şi componentele fizice ale acestora.

Amenințările pot fi clasificate în dezastre naturale şi acțiuni umane (intenționate sau neintenționate). Pot fi amintite aici câteva acțiuni umane intenționate / amenințări: furtul, pierderea sau distrugerea unui activ informațional, frauda, accesul neautorizat la serviciile de rețea, furtul de identitate în rețea, etc.

Consecințele economice ale breşelor de securitate pot fi considerabile. Conform [6], majoritatea pierderilor financiare sunt cauzate prin fraudă, de către viruşi, viermi şi/sau spyware, precum şi prin accesul neautorizat de la distanță.

Impactul asupra organizației poate fi imediat, tradus prin pierderi imediate sau sau ulterior, materializat prin pierderi indirecte. Din multitudinea pierderilor imediate se pot aminti diminuarea veniturilor, scăderea productivității muncii şi creşterea costurilor, care în multe situații pot fi doar o mică parte din totalul pierderilor generate de incidentele de securitate.

De obicei, pierderile indirecte au un impact negativ de lungă durată asupra activității organizației, privind mulțimea potențialilor clienți, a partenerilor de afaceri, furnizorilor, pieței financiare [7]. Acestea influențează şi reputația organizației, aducând atingere încrederii clienților în serviciile oferite.

Conform [8], pierderile datorate unor breşe de securitate sunt de obicei asociate cu integritatea şi confidențialitatea datelor, precum şi cu disponibilitatea activelor informaționale.

Cu toate acestea, din perspectivă economică, date credibile privind costurile reale produse în urma incidentelor de securitate sunt foarte dificil de obținut. Unul dintre motive este acela că majoritatea organizațiilor nu țin o evidență sistematică şi nu documentează adecvat aceste incidente. De asemenea, organizațiile tratează aceste probleme ca pe evenimente interne, pentru a evita publicitatea negativă. Cele mai relevante date provin din rapoartele anuale ale organizațiilor specializate în securitate informațională (CERT, CSI, DTI).

4. Identificarea vulnerabilităţilor

Vulnerabilitatea reprezintă o slăbiciune a procedurilor de securitate, a metodelor de control tehnice, fizic sau de altă natură ale infrastructurii informaţionale pe care o ameninţare poate exploata. Cele mai multe incidente de securitate sunt cauzate de vulnerabilităţile generate datorită defectelor software-ul.

Vulnerabilităţile sunt de obicei cunoscute ca fiind o problemă tehnică. Cu toate acestea, există vulnerabilităţi provocate de factorul uman. Acest tip de vulnerabilitate sunt cauzate de utilizatori care îşi dezvăluie parolele lor sau folosesc parole "slabe", de neînţelegerea sau ignorarea politicilor de securitate, de deschiderea email-urilor provenite de la persoane necunoscute, de vizitarea site-urilor web nesigure, etc.

Un bun mecanism de asigurare a securităţii este acela de a considera vulnerabilităţile o "marfă de schimb". Acest lucru înseamnă că un dezvoltator software oferă o recompensă pentru prima persoana care detectează o vulnerabilitate în codul sursă, recompensa putând creşte odată cu trecerea timpului.

În contrast, The Computer Emergency Response Team (CERT) acţionează ca un intermediar între persoane care raportează în mod voluntar vulnerabilităţi informatice. Pentru a se asigura că astfel de notificări publice nu sunt exploatate de atacatori, CERT contactează dezvoltatorul software în scopul creării de patch-uri corespunzătoare şi aşteaptă un moment convenabil pentru a face publică vulnerabilitatea.

Se pune întrebarea - de ce furnizorii de software nu fac produsele lor mai sigure din primul moment. Răspunsul este determinat de aspectele economice. Securitatea produselor software este dificil de măsurat, iar utilizatorii fac cu greu distincţia între cele mai sigure şi cele mai puţin sigure. De asemenea, costurile de scriere, testare şi implementare a unor protocoale sigure de securitate sunt mari, iar utilizatorii nu sunt dispuşi să plătească suplimentar pentru aceasta.

De aceea, pentru a repara vulnerabilităţile, dezvoltatorii de produse software recurg la aşa-numitele "patch-uri". Conform CERT, 95% din incidentele de securitate pot fi prevenite menţinând sistemele informatice cu patch-urile la zi. În ultimul timp, intervalul de timp între identificarea vulnerabiltăţilor şi crearea unor instrumente de exploatare a acestora (exploit-uri) s-a diminuat simţitor. Cu toate acestea, multe sisteme sunt lăsate neactualizate pentru lungi intervale de timp, ceea ce poate conduce la consecinţe economice dramatice.

5. Abordări de evaluare a riscurilor de securitate informaţională

Odată ce riscurile de securitate au fost identificate, acestea trebuie să fie evaluate în funcţie de pierderile potenţiale pe care le pot produce şi probabilitatea lor de apariţie. Evaluarea riscurilor reprezintă determinarea impactului potenţial al unui riscului individual, prin evaluarea probabilităţii ca acesta să aibă loc, precum şi impactul ce care l-ar avea în cazul în care apare. Evaluarea ajută organizaţiile să ia o decizie în ceea ce priveşte investiţiile în sisteme de securitate pentru maximizarea beneficiului afacerilor.

Există mai multe metodologii pentru evaluarea riscurilor. Analize cantitativă a riscului încearcă să atribuie valori numerice probabilității de apariție, impactului riscurilor, precum şi costurilor şi beneficiilor legate de introducerea unor măsuri şi sisteme de securitate.

Scopul măsurilor de securitate este acela de a diminua riscul până la un punct în care costul marginal de punere în aplicare a măsurii este egal cu valoarea totală a incidentelor de securitate.

În contrast cu abordarea cantitativă, analiza calitativă a riscului operează cu valori relative şi nu atribuie valori exacte activelelor financiare, pierderilor aşteptate, şi costului controalelor şi a sistemelor. Analiza calitativă a riscurilor este de obicei efectuată printr-o combinație de chestionare şi grupuri de discuții colaborative.

Ambele abordări (calitativă şi cantitativă) au avantaje şi dezavantaje. Problema analizei cantitative de risc constă în inexistența unei metode standard de calcul a valorilor activelor şi a costului măsurilor şi sistemelor de securitate necesare. Avantajul unei abordări calitative este acela că procesul în sine necesită personal mai puțin şi nu este necesară calcularea exactă a valorii activelor şi a costului implementării măsurilor de securitate. Dezavantajul este că rezultatele sunt de obicei vagi, deoarece au fost obținute pe baza unor valori relative ale activelor.

De obicei organizațiile de dimensiuni mici, cu resurse de obicei limitate, vor găsi abordarea calitativă mai convenabilă.

6. Concluzii

Managementul riscurilor de securitate informațională reprezintă o preocupare fundamentală a tuturor organizațiilor. Aceasta lucrare prezinta o analiză a problemei asociată cu determinarea necesarului economic de investiții în securitatea informațiilor. Rezultatul analizei reprezintă o recomandare care ar putea fi transformată într-o abordare standardizată.

Abordarea conține o enumerare a etapelor procesului de gestionare a riscurilor, care permite identificarea activelor. Acest lucru oferă bună înțelegere asupra a ce anume ar trebui să fie protejat în special în organizație şi motivația asociată.

Analiza amenințărilor oferă informații despre amenințări şi despre mediul de securitate în care "evoluează" o organizație pe parcursul desfăşurării proceselor de afaceri. Fiecare etapă a procesului este analizată din punct de vedere al securității informaționale şi a aspectelor economico-financiare pe care le implică.

Până în prezent, un există un model standardizat de determinare a riscului financiar asociat cu incidentele de securitate, de aceea recomandarea este de a le utiliza combinat pe cele parțiale existente, adaptate la circumstanțele specifice existente.

Bibliografie

1. Whitman, M. E. (2003). *Enemy at the gate: Threats to information security*. Communications of the ACM, 46(8), 91–95.
2. Anderson, R., Schneier, B. (2005). *Economics of information security*. IEEE Security and Privacy, 12–13.
3. FIPS (2004). *Federal Information Processing Standards (FIPS) publication*. Security Categorization of Federal Information and Information Systems.
4. Microsoft (2004). *Microsoft security Risk Management Guide*. http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspxS.
5. NIST (2004). *Mapping types of information and information systems to security categories.* National Institute of Standards and Technology (NIST) Special Publication.
6. CSI (2007). *CSI Survey 2007*. The twelfth annual computer crime and security survey, http://www.gocsi.com/forms/csi_survey.jhtml.
7. Rowe, B. R., Gallaher, M. P. (2006). *Private sector cyber security investment strategies: An empirical analysis*. The fifth workshop on the economics of information security (WEIS06).
8. Bohme, R., Kataria, G. (2006). *Models and measures for correlation in cyber-insurance*. The fifth workshop on the economics of information security.