Rodica GRINIUC, Nicolae PLOTEANU,
Academia „Ştefan cel Mare”, MAI

FORMAREA POLITICII DE SECURITATE A SISTEMELOR INFORMATICE

Abstract: *In this article the authors present modern methods of working out the informational security policy as measures in accordance with the modern process of analyzing and running the informatics systems.*

Actualmente este perceput faptul că asigurarea securității nu reprezintă doar o protecție contra potențialelor pagube materiale, ci şi asigurarea unui atu concurențial, a unei reputații sigure, precum şi câştigarea încrederii partenerilor şi clienților. Pornind de la importanța celor menționate marea majoritate a subiecților care tind la prosperarea şi realizarea unei activități îndelungate şi prospere investesc temeinic în crearea unei politici actuale şi sigure de securitate în propriul sistem informatic.

Sarcina de bază în etapa de exploatare a oricărui sistem informatic este asigurarea unui nivel viabil de securitate. Această cerință este la fel de strictă ca şi cea față de funcționalitatea resurselor şi componentelor sistemului, precum şi a întregii activități a sistemului informatic în general. Exploatarea sistemelor informatice, dotate cu sisteme de securitate contemporane, nu este însă o sarcină uşoară, putem spune că reprezintă o sarcină destul de dificilă şi specifică.

Particularitatea de bază a unui sistem de securitate (spre deosebire de alte componente TI) constă în faptul că sistemul informatic care este protejat astăzi sigur, mâine poate deveni vulnerabil. În acelaşi timp, sistemul de securitate care nu este exploatat în corespundere cu cerințele contemporane sau nu se ia în considerație apariția unor noi pericole, peste câteva luni îşi va pierde actualitatea. În acest sens, producătorii permanent emit noi versiuni ale produselor, care conțin îmbunătățiri, modificări, care introduc noi aspecte funcționale şi corecții de program ce lichidează erorile şi lacunele. Este necesar de a monitoriza aceste modificări şi de a le instalat în propriul sistem. Nu reprezintă un secret faptul că multe vulnerabilități, utilizate pentru desfăşurarea atacurilor asupra sistemelor corporative, la momentul atacului erau deja depistate şi cunoscute producătorilor mijloacelor de protecție sau componentelor TI atacate. Aceste vulnerabilități erau posibil a fi lichidate cu câteva săptămâni până la atac, pur şi simplu instalând patch-ul informațional corespunzător. Pentru a fi la curent cu toate modificările, e necesar de urmărit evoluția lor şi evenimentele legate de ele. Dacă această măsură este ignorată, sistemul de securitate foarte rapid îşi va încetini îndeplinirea sarcinilor sale.

Exploatarea sistemelor informatice protejate reprezintă o particularitate în sine, dat fiind faptul că în structura lor sunt introduse permanent modificări. De regulă, după cum a demonstrat practica, sistemul informatic care asigură activitatea unei organizații mari, practic, nu rămâne static niciodată. Modificările şi completările cu noi componente reprezintă un proces firesc şi continuu, dat fiind faptul că sistemul informatic activează în strânsă concordanță cu procesele de activitate ce se desfăşoară în instituția respectivă: implementarea unor noi segmente de activitate duce la crearea unor noi locuri de muncă şi la apariția de noi servicii informaționale, creşterea volumului de informație implică introducerea noilor tehnologii informaționale, precum şi a necesității de a optimiza sistemul etc., ceea ce duce la micşorarea mecanismelor şi procedurilor de protecție. Deci, apare necesitatea îmbunătățirii nivelului de securitate, coordonând permanent cu structura sistemului informatic ce necesită protejare. De aceea, în sistemele informatice perpetue este importantă nu numai introducerea mecanismelor corespunzătoare de protecție, dar şi asigurarea unui nivel adecvat de securitate în procesul de exploatare. Pentru aceasta este necesară atât asigurarea viabilității mijloacelor de protecție, cât şi efectuarea măsurilor profilactice, materializate prin verificarea nivelului de protecție a resurselor, ceea ce va permite garantarea acestui nivel chiar şi în contextul introducerii modificărilor.

Astfel, asigurarea securității este posibilă prin exploatarea corectă a sistemului şi prin susținerea politicii de securitate. Aceasta presupune desfăşurarea unui şir de măsuri permanente şi periodice de susținere tehnică a mijloacelor de protecție, monitorizarea şi analiza evenimentelor de securitate ce se derulează în sistem, verificarea periodică a nivelului de protecție a resurselor protejate, aplanarea situațiilor nefaste şi lichidarea consecințelor. De asemenea, administrarea sistemelor de securitate trebuie să fie înzestrată cu un anumit grad de automatizare a funcțiilor de administrare şi a altor funcții de exploatare. Acest punct presupune asigurarea tehnică şi cu programe a administratorilor de securitate şi a şefilor de secții şi servicii (scanere, mijloace de monitorizare şi dirijare cu securitatea), corelarea evenimentelor, analiza gradului de protecție a componentelor TI, mijloace de obținere a statisticii, de generare a concluziilor etc.

Noi mai suntem de părere că asigurarea şi verificarea gradului de protecție a sistemului informatic reprezintă o sarcină comună atât pentru serviciile de securitate, cât şi pentru serviciile TI. În unele cazuri, funcționarii serviciului de securitate trebuie să verifice activitatea serviciului TI; în alte cazuri, există situații zilnice care necesită coordonarea serviciilor. Pentru ca procesul de colaborare între diverse servicii să decurgă eficient şi fluent, e necesar să se respecte câteva condiții: să fie strict delimitate sferele de responsabilitate şi obligațiile tuturor participanților la procesul de asigurare a activității informaționale, periodic să fie anihilate şi preîntâmpinate posibilele conflicte de interese între diferite servicii, verificate prin analiza dărilor de seamă ale

serviciului TI starea de securitate în scopul de a menține la nivel atenția serviciului respectiv față de problema asigurării continue a nivelului competitiv de securitate informațională.

De asemenea, am dori să menționăm că elaborarea unui sistem solid, bine securizat, cu proceduri de acces atât din exterior, cât şi din interior, bine puse la punct, conferă activității sistemului informatic multiple avantaje. Astfel, oricât de mică este instituția, existenta unei politici de securitate este necesară pentru desfăşurarea eficientă a activității propriu-zise. Soluționarea sarcinilor cu privire la elaborarea unei politici eficiente de securitate în etapa actuală, pentru orişicare instituție, organizație, întreprindere, companie, se reflectă în alegerea criteriilor şi indicatorilor de asigurare a protecției, precum şi a gradului de eficiență a sistemului de protecție a informației. Astfel, pe lângă diferite acte normative interne naționale, e necesar de implementat şi recomandările de ordin internațional, în unele cazuri adaptând metodele naționale la standardele internaționale gen: ISO 17799 „Dirijarea cu securitatea informațională", ISO 15408 „Tehnologia informațională – metode de protecție – criteriile de analiză a securității informaționale" etc.

Pentru elaborarea politicii de securitate şi a planurilor de perfecționare a acesteia este necesar:

1. Argumentarea şi realizarea calculului investițiilor financiare în asigurarea securității în baza tehnologiilor de analiză a pericolelor, coraportarea cheltuielilor pentru asigurarea securității cu dauna potențială şi probabilitatea survenirii ei;
2. Descoperirea şi scoaterea la iveală, precum şi blocarea celor mai periculoase lacune până la sesizarea şi atacarea lor de către agresor;
3. Determinarea relațiilor funcționale şi a zonelor de responsabilitate a subdiviziunilor şi persoanelor cu privire la asigurarea securității informaționale a instituției, crearea pachetului necesar de documentație cu privire la organizarea şi dirijarea activității în domeniul respectiv;
4. Elaborarea şi coordonarea cu serviciile şi subdiviziunile instituției, serviciile de supraveghere, proiectul de introducere a complexelor necesare de protecție, care se vor elabora în corespundere cu nivelul modern şi tendințele de dezvoltare a tehnologiilor informaționale;
5. Asigurarea susținerii complexului introdus de securitate în conformitate cu condițiile dinamice de activitate a instituției, perfecționarea dinamică a setului de documentație de organizare şi dirijare cu procesul în cauză, modificarea procesului tehnologic şi a mijloacelor tehnice de asigurare a protecției.

În încheiere, am vrea încă o dată să menționăm că, în prealabil, înainte de a implementa careva soluții de protejare a informației, e necesară elaborarea politicii de securitate

corespunzătoare scopurilor şi sarcinilor unei instituții sau companii moderne. Politica de securitate trebuie să conțină şi să prevadă în special: ordinea de oferire şi folosire a drepturilor de acces de către utilizatori, de asemenea, darea de seamă a utilizatorilor pentru acțiunile întreprinse în problemele ce țin de sfera de securitate. Sistemul de securitate informațională va fi eficient, dacă va corespunde şi va susține sigur regulile de securitate ale politicii de securitate şi viceversa.