Roman MORARU,
Departamentul Securitate, BC „Mobiasbanca" SA

INSIDER – AMENINȚAREA DIN INTERIOR

Abstract: *Insider's threats represent a substantial risk for organizations. Yet most organizations and information security researchers currently lack a clear understanding of who are the insiders, how they can affect the organization assets and what is needed to be done to protect from this threats. This document is starting point for understanding and protecting from insiders threats.*

> *„Dacă îți cunoşti duşmanul şi te cunoşti pe tine însuți, nu trebuie să-ți fie teamă de rezultatul bătăliilor. Dacă te cunoşti pe tine însuți, dar nu-ți cunoşti duşmanul, la fiecare victorie câştigată vei suferi şi o pierdere. Dacă nu-ți cunoşti duşmanul şi nu te cunoşti nici pe tine, vei pierde toate bătăliile".*
>
> ***„Arta războiului" de Sun Tzu***

Din punctul de vedere al securității informaționale, toate acțiunile nesancționate reprezintă un risc pentru o organizație, însă problema protejării împotriva acțiunilor insider-ilor în organizații în ultimul timp devine din ce în ce mai acută.

De exemplu, investigarea efectuată de COMPUTER CRIME INSTITUTE a arătat că, începând cu anul 1998, aproximativ 70 la sută din organizațiile ce au fost intervievate au căzut victima atacurilor, dintre care două treimi din atacuri au fost efectuate din interiorul organizațiilor.

Ca demonstrație la cele expuse mai sus, pot fi prezentate informațiile ce apar regulat în serviciile de mass-media, referitoare la „scurgerea" de informație, apariția în vânzare a datelor personale, a tranzacțiilor financiare, a informațiilor despre cartelele de credit. Republica Moldova, ca şi restul statelor, cu părere de rău, nu este o excepție.

Cu atât mai mult, atacurile din interior se petrec tot timpul, însă, ținând cont că majoritatea organizațiilor duc o politică de nedivulgare a informațiilor referitoare la atacurile din interior, acele informații, ajunse să fie expuse public, reprezintă doar vârful vizibil al „hețarului" cu numele de insider.

Totuşi, cine este persoana definită ca „insider". În urma analizei a mai multor definiții, am spune că ***insider*** reprezintă angajatul sau persoana din organizație care deține acces autorizat sau cunoştințe şi are drept scop provocarea daunelor organizației.

Motivul principal al acutizării acestei probleme a devenit în ultimul timp faptul că multe companii sau organizații activează bazându-se pe principiul că este mai bine să lucrezi în pericol şi să nu cunoşti eventualele ameninţări, decât să le analizezi şi să adopți decizii privind minimizarea lor. Cu toate că acest motiv, pare cel mai incredibil, el este întâlnit este cel mai des. Un al doilea motiv ar fi că mulți dintre managerii companiilor sunt convinşi că, angajând o nouă persoană, ea (persoana) face automat parte din grupul angajaților de încredere şi va activa tot timpul în interesul organizației. Dificultatea de a depista, de a se proteja şi a demonstra acțiunile nesancționate ale insider-ului este a treia cauză ce motivează organizațiile de a nu întreprinde măsuri în acest domeniu.

Pentru protejarea împotriva insaider-ilor este necesară întreprinderea unei analize preventive a activelor organizației:

1. În primul rând, determinarea activelor informaționale ce sunt critice pentru continuarea afacerii.
2. Efectuarea analizei eventualelor atacuri şi a punctelor slabe în protecția activelor informaționale.
3. Determinarea nivelului de risc acceptabil de organizație, aşa-zisul risc rezidual. Analiza bazată pe cost-beneficiu este una din metodele utilizate pentru determinarea nivelului de risc acceptabil.

După finalizarea analizei, va fi posibilă alegerea mijloacelor de protecție necesare împotriva atacurilor insider-ilor, cum ar fi:

- *Controlul accesului* – se subînțelege aplicarea principiului minimului de privilegii pentru accesul la activele critice ale organizației. Acest principiu se defineşte ca proces de acordare doar a accesului minim pentru îndeplinirea funcțiilor de serviciu şi excluderea oricăror privilegii suplimentare.
- *Crearea profilurilor statistice* – această metodă se bazează pe date statistice. De exemplu, dacă angajatul accesează în medie 30-40 de cartele pe zi pentru a-şi îndeplini funcțiile de serviciu, respectiv accesarea informației despre 300 de cartele într-o zi sau accesarea întregii baze de date despre cartele ar indica o posibilă scurgere de informație. Însă această metodă are neajunsurile sale, de care trebuie ținut cont, cum ar fi cazul în care angajatul încearcă sa lucreze mai repede şi prelucrează pe zi nu 30-40, ci 50-60 de cartele; în acest caz, un angajat sârguincios va cădea sub suspiciune. Un alt neajuns al acestei metode ar fi că, odată ajunse cunoscute de către angajați, aceste profiluri pot deveni ineficiente, deoarece vor fi uşor evitate.
- *Monitorizarea* – este una din metodele ce permite detectarea acțiunilor neautorizate ale insider-ilor. Însă, înainte de a activa monitorizarea în cadrul organizației, este necesară

înțelegerea consecințelor etice şi legale ale monitorizării acțiunilor angajaților, inclusiv pentru organizațiile multinaționale trebuie să se țină cont de particularitățile legislației din fiecare țară.

- *Divizarea funcțiilor* – reprezintă metoda de distribuire a funcțiilor, în care un angajat nu va îndeplini de sine stătător toate funcțiile din cadrul unui proces.
- *Controlul ulterior* – este actual în special pentru organizația unde nu este posibilă divizarea funcțiilor de serviciu, cum ar fi: administratorii de sistem, administratorii bazelor de date, administratorii de rețea.
- *Acordarea concediului obligatoriu* – există în organizație angajați care nu au plecat în concediu de câțiva ani la rând, poate merită acordarea unui concediu?
- Practica arată că un număr înalt de cazuri de atacuri din interior sunt depistate de colegii de lucru la eliberarea din post a angajatului sau când angajatul se află în concediu. Din aceste considerente, o parte din organizații practică acordarea concediilor anuale obligatorii cu îndeplinirea funcțiilor de către alți angajați ai organizației.
- *Instruirea* – instruirea angajaților este una din metodele eficiente de prevenire şi detectare a atacurilor din interior. Conform datelor statistice, majoritatea atacurilor interne, în special a furturilor, sunt detectate de angajații simpli şi doar o mică parte sunt depistate de către securitate sau securitatea informațională

Bineînțeles că lista de măsuri descrisă nu este deplină şi multe din acestea sunt necesare pentru a fi aplicate numai în baza unei analize profunde, însă de ceea ce trebuie de ținut tot timpul cont este că problema insider-ilor există, este actuală pentru orice organizație, de stat sau comercială, şi necesită a fi inclusă în analiza de risc în domeniul securității informaționale din cadrul organizației.

Bibliografia:

1. Insider Threat, Protecting the Enterprise from Sabotage, Spying, and Theft, Syngress Publishing, Inc., 2005

Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis, 2006 Carnegie Mellon University

2. Do You Really Know What Your Programmers Are Doing? Mintaka Technology Group, 2003
3. Computer crime, information warfare, and economic espionage**,** *Carolina Academic Press*
4. The Insider Threat To Information Systems*,* By Eric D. Shaw, Ph.D., Keven G. Ruby, M.A. and Jerrold M. Post, M.D. Political Psychology Associates, Ltd