Information Security Management

Magdaléna Cárachová
Ekonomická univerzita, Fakulta hospodárskej informatiky, KAI
Dolnozemská 1, 852 35 Bratislava
e-mail:carach@euba.sk

Abstrakt:

Údaje, softvérové vybavenie, technologická a technická infraštruktúra, realizované procesy, pracovníci - to všetko predstavuje hodnotu informačného aktíva, ktorú si firma intenzívne uvedomí v prípade narušenia niektorého z bezpečnostných aspektov. Škála následkov zlyhania informačnej bezpečnosti je široká - od malých incidentov až po krízové stavy, ktoré zásadne ohrozujú schopnosť podniku plniť záväzky voči klientom, infiltrácia systémov, strata, alebo poškodenie firemných údajov, únik informácií o zákazníkoch, vyzradenie obchodného tajomstva. Všetky tieto skutočnosti majú nepríjemné následky, predovšetkým poškodenie reputácie a finančné dopady v rôznej výške. Riadenie podnikových rizík je proces, do ktorého by sa malo zapojiť nielen vedenie firmy, ale všetci zamestnanci a ktorého cieľom je identifikovať potenciálne udalosti, ktoré by mohli ovplyvniť jej fungovanie, a riadiť riziká v súlade s prijatou stratégiou tak, aby firma mohla napĺňať ciele, ktoré si stanovila.

Kľúčové slová:

Riadenie informačnej bezpečnosti, krízové udalosti, analýza rizík

Abstract:

There are data, software and hardware infrastructure, implemented and operated processes together with adequate workers or employees and play a role of great importance, when considering an information capital or a set of information resources. This aspect is considered to be important in the firm or company, especially in the case of information security problems or failures. However, there is a large scale of results of consequences when an information security problem or failure is observed. At the beginning some small incidents may be observed. However, there may be observed a large scale critical or fatal situations as well which represent a menace for the firm or company who is closely related to its capability in fulfillment of duties for clients, system infiltration, lost or damage of the company's data, information escape concerned to the firm or company clients or a trade secret revelation. All of the above-mentioned aspects create a lot of unfavorable results or consequences, while a reputation violation and a set of different financial negative impacts may be postulated first of all. The risk management problems are not only a matter of the company top management, however all employees should be involved in this process as well. The risk management aim is to provide an adequate control and regulation of management processes, incl. potential risks and threats with respect to an appropriate business strategy and pre-determined goals within firm or company.

Keywords:

Software and hardware infrastructure , Information Security Management, the risk management

Úvod

Bezpečnosť vo všeobecnom slova zmysle označuje odolnosť vecí proti negatívnym dôsledkom ich používania. V 21. storočí žijeme v informačnej spoločnosti, v ktorej s rastom závislosti na informačných systémoch a nimi poskytovaných službách je zaistenie bezpečnosti informácií jednou zo základných požiadaviek. Informačné a komunikačné technológie vstupujú do nášho každodenného života. V informačných systémoch sa spracovávajú rôzne údaje, ktorých účel je tiež rôzny – od zdroja zábavy až po riadenie podnikových procesov. Najmä v podnikateľskom svete účel spracúvaných dát zvyšuje ich hodnotu a citlivosť na bezpečnostné aspekty – dôvernosť, integritu a dostupnosť. Bezpečnosť IT prostredia je problematika, ktorá siaha od fyzickej bezpečnosti konkrétnych zariadení až po zabezpečenie údajov. Na jednej strane je hrozba straty týchto údajov z dôvodu fyzického zlyhania dátového nosiča, alebo napadnutia vírusom, na druhej strane je riziko získania dát treťou stranou. Ďalší možný zdroj ohrozenia je znefunkčnenie podnikového prostredia napadnutím mailového servra, alebo zahltením sieťovej infraštruktúry, čo spôsobí na určitý čas prerušenie elektronickej komunikácie, čím okamžite vznikajú finančné straty. Informačná bezpečnosť sa ako každá oblasť ľudského života dynamicky vyvíja. Nové typy útokov, dodatočné legislatívne požiadavky, meniace sa prostredie – to všetko vplýva na potreby v oblasti informačnej bezpečnosti. Bezpečnostná úroveň, ktorá sa minulých rokoch považovala za dostatočnú, dnes uspokojí už len málokoho. Vzhľadom na to sa v súčasnosti prejavujú nové trendy nielen v samotných bezpečnostných mechanizmoch, ale aj v celkovom systéme riadenia informačnej bezpečnosti.

1. Analýza rizík

Analýza rizík je neodmysliteľnou súčasťou systému riadenia informačnej bezpečnosti. V podstate sa jedná o systém zavádzania informačnej bezpečnosti do praxe, ktorý sa realizuje podľa rôznych postupov, prípadne štandardov. Informačná bezpečnosť sa nemôže obmedziť len na implementáciu firewallov a antivírusových programov. Je to predovšetkým úspešné riadenie všetkých, ktorí majú prístup k podnikovým informáciám. V rámci zavádzania a riadenia systému manažérstva informačnej bezpečnosti by si mala firma vydefinovať systematický prístup na preskúmavanie rizík, identifikovať ich, analyzovať ich, ohodnotiť riziká a ohodnotiť možnosti ich ošetrenia. Analýza rizík v IS je základom pre vytvorenie účinného systému ochrany informačných technológií. Analýza rizík zahŕňa analýzu aktív, analýzu hrozieb a analýzu zraniteľnosti. Analýzu rizík môže zrealizovať podnik v princípe tromi spôsobmi. Môže si zaobstarať softvérovú vybavenie, prostredníctvom ktorého zrealizuje analýzu rizík vo firme. V druhom prípade sa môže poverený pracovník oboznámiť s príslušnými právnymi predpismi a technickými normami a podľa nich postupovať. V treťom prípade je možné ponechať celý proces analýzy rizík na tretiu osobu.

Výsledkom analýzy rizík je odhad hodnoty rizika, ktoré vyjadruje stupeň hrozby pre dané aktívum. Táto hodnota je priamoúmerná veľkosti zraniteľnosti, veľkosti hrozby a hodnote aktíva.

1.1 Identifikácia modulov aktív

Informačné systémy sa skladajú z prvkov informačných, personálnych, hardvérových a softvérových aktív. Nemali by sa ohodnocovať samostatne, ale v rámci modulov aktív – procesy, informácie, údaje, softvér, hardvér, ľudské zdroje. Z pohľadu informačnej bezpečnosti má napr. pri zachovaní rovnakej hardvérovej a softvérovej konfigurácie pracovná stanica so súkromnými dokumentmi zamestnanca inú hodnotu pre firmu, ako pracovná stanica na ktorej sú osobné údaje pracovníkov firmy. Pri identifikovaní jednotlivých modulov aktív by sa mali ohodnotiť podľa významnosti pre danú firmu. Najdôležitejšie kritériá ohodnotenia jednotlivých aktív sú porušenie právnych predpisov, strata dobrého mena, vyzradenie obchodného tajomstva, ohrozenie osobnej bezpečnosti, prerušenie obchodnej činnosti, užitočnosť, nahraditeľnosť, význam pre konkurenciu a náklady na obnovu.

1.2 Identifikácia hrozieb

Hrozbou sa rozumie označenie konkrétne fyzicky existujúceho subjektu, resp. javu schopného spôsobiť stratu integrity, dostupnosti, či dôvernosti aktív IS. Je potrebné uvedomiť si, že zoznam hrozieb sa dynamicky vyvíja. K identifikácii hrozieb je možné pristupovať v podstate tromi spôsobmi.

Intuitívne vyhľadávanie rizík - pri tomto spôsobe je základom dôkladná úvaha nad všetkými situáciami, ktoré môžu v informačnom systéme nastať.

Inšpirácia inými zoznamami hrozieb je druhý spôsob, pri ktorom sa zvolí zoznam, ktorý bol vytvorený pre podobné prostredie. Zoznam je potrebné individualizovať podľa vlastného systému.

Využitie podrobných dotazníkov je tretí spôsob identifikácie hrozieb. Pre rôzne časti prostredia sú vytvorené komplexné dotazníky. Pri identifikácii rizík potom bezpečnostný expert prechádza otázku za otázkou a zisťuje, ako je na tom daný systém v danom prostredí. Výhodou tohto spôsobu je pomerne vysoká kvalita, nevýhodou je časová náročnosť.

1.3 Vlastná analýza rizík

Úlohou vlastnej analýzy rizík je zistiť, aké nebezpečenstvá konkrétnym aktívam hrozia a vytvorenie zoznamu aktív, ktorým sú priradené jednotlivé hrozby. Každej dvojici aktívum - hrozba je možné priradiť pravdepodobnosť výskytu danej hrozby. Je možné teda kvalifikovane rozhodnúť, proti akej pravdepodobnosti hrozieb je potrebné informačný systém chrániť. Prostredie, v ktorom sa informačný systém nachádza sa priebežne mení. Menia sa aktíva, menia sa hrozby, mení sa pravdepodobnosť ich výskytu a je teda vhodné analýzu realizovať opakovane po určitom čase.

2. Oblasti bezpečnosti

Pracovníci, ktorí sa starajú o bezpečnosť IT by sa mali orientovať na 5 základných oblastí.

Program bezpečnosti

Efektívne programy riadenia rizík v oblasti bezpečnosti IT musia detekovať bezpečnostné hrozby a s nimi súvisiace náklady na zabezpečenie proti nim. Mal by byť vytvorený program bezpečnosti, ktorý tieto hrozby minimalizuje, mala by byť určená činnosť firmy v zmysle bezpečnostných aspektov vyplývajúcich z príslušných ustanovení. Celková architektúra bezpečnosti sa musí realizovať tak, aby obsahovala program bezpečnosti firmy. Firmy musia stanoviť, ktoré procesy a aspekty riadenia bezpečnosti musia byť centralizované a ktoré môžu presunúť na jednotlivé útvary. Rozsah plánovacej činnosti a rozvoj v tejto oblasti obsahuje riadenie rizík,

administratívne záležitosti, dôverný charakter a ochranu duševného vlastníctva, bezpečnosť obchodných aplikácií a bezpečnostné služby a financovanie.

Bezpečnosť infraštruktúry

Bezpečnosť infraštruktúry firmy sa skladá z nástrojov a technológií, ktoré sa poskytujú s cieľom ochrániť sieť a vnútorné zdroje. Najdôležitejšie je zabezpečenie neohrozenosti funkcie technológií, teda dostupnosť údajov a aplikácií. Ich chod môže byť principiálne ohrozený v troch základných oblastiach. Prvou je dátová a softvérová doména ako najčastejší zdroj hrozieb – počítačové vírusy, softvérové kolízie, vonkajší nepovolený prístup, atď. Do fyzickej bezpečnosti hardvérových prostriedkov patria poruchy hardvéru, chyby obsluhy, odcudzenie, alebo zneužitie zariadení, pôsobenie prírodných živlov, teda narušenie hardvéru v mieste inštalácie. Treťou oblasťou sú technológie, ktoré tvoria základné podmienky pre chod výkonnej časti IT súhrnne označované ako NCPI (Network Critical Physical Infrastructure).Táto činnosť je sťažená zavedením nových zariadení, aplikačných metód a spôsobov pripojenia do siete. Tradičná infraštruktúra bezpečnosti sa zamerala na ochranu sieťového systému, ale s nárastom využívania mobilných zariadení a sprístupnením interných zdrojov na internete zákazníci a dodávatelia vyžadujú vyššiu úroveň ochrany firemných vnútorných zdrojov. Do účinnej infraštruktúry bezpečnosti patria systémy ochrany prístupu, ochrana a prevencia proti vniknutiu do systému, ochrana proti vírusom a filtrovanie obsahu údajov, bezpečnosť mobilných a bezdrôtových systémov, kódovanie a riadenie bezpečnosti IT.

Riadenie bezpečnosti IT

Kvalitné riadenie bezpečnosti sa sústreďuje na prevádzkové technológie a optimálne koncepcie, ktoré zabezpečujú bezpečný prístup k aplikáciám a zdrojom a poskytuje jednotnosť systémových princípov a konfigurácií. Do riadenia bezpečnosti patria webové služby a infraštruktúra pre verejný prístup, riadenie stupňa bezpečnosti systému, konfigurácia bezpečnostného systému a riadenie opravných procesov a riadenie procesov overovania totožnosti a udeľovania prístupu. Firmy nedosiahnu uspokojujúcu návratnosť svojich investícií v oblasti plánovania bezpečnosti a stimulov rozvoja bez efektívneho riadenia a realizácie.

Riadenie kontinuity

Riadenie kontinuity obchodnej činnosti prekročilo svoj tradičný rámec obnovy systému po havarijných udalostiach smerom k zahrnutiu plánovacej činnosti a návrhu systémov IT a obchodných procesov, ktoré budú odolné voči výpadkom v činnosti. Tento vývoj čiastočne podporuje rastúce prepojenie IT a obchodných procesov, pretože firmy poskytujú čoraz viac aplikácií v reálnom čase, ktoré sa orientujú smerom k zákazníkom a súčasne podporujú základné obchodné činnosti. Organizácie musia realizovať komplexné programy kontinuity obchodnej činnosti, ktoré sa orientujú na obnovu obchodnej činnosti, na plánovanie tejto obnovy a na alternatívne plánovanie a riadenie krízových stavov. Plánovanie kontinuity obchodnej činnosti, ktoré musí byť súčasťou procesov obchodnej činnosti a pracovných cyklov IT, by malo byť zamerané na stratégiu a optimálne koncepcie, technológiu, nástroje a služby.

Ochrana základnej infraštruktúry

Ochrana globálnej základnej infraštruktúry je najdôležitejšou oblasťou. Väčší dôraz na technológiu, obmedzené finančné zdroje a nárast celkovej neistoty v oblasti bezpečnosti nútia firmy, aby chránili svoje základné infraštruktúry pred ohrozeniami v oblasti IT. Bezpečnostné systémy IT v oblasti energetiky, dopravy, finančných služieb a vo vládnom sektore sa stávajú samozrejmosťou. Medzi technologické a obchodné ciele patria pochopenie priemyselne orientovaných optimálnych koncepcií smerujúcich k ochrane základnej infraštruktúry, ďalej ochrana firmy s obmedzenými finančnými zdrojmi a odozva na globálne smernice v oblasti priemyslu.

3. Identity Management

Súčasné využívanie IT v organizáciách prináša problematiku prístupu oprávnených osôb k zdrojom organizácie. Túto problematiku pomáha riešiť Identiry Management tak po technickej ako aj procesnej stránke. Riadenie prístupu k aktívam organizácie je jednou zo základných úloh bezpečnosti a ochrany aktív. Identity management je definovaný ako množina procesov, nástrojov z zmlúv na vytváranie, udržovanie, využívanie a odstraňovanie digitálnych identít pre ľudí, systémy a služby s cieľom umožniť bezpečný prístup k podnikovým zdrojom. Má silné prepojenie so správou bezpečnosti, dôvery a súkromia. V súčasnosti je mažment identít najčastejšie spájaný ako nástroj na riadenie prístupu do IS. V praxi nie je manažment identít súčasťou len virtuálneho priestoru, ale samozrejme aj fyzického priestoru. Z toho vyplýva, že manažment identít sa využíva v prostredí a priestore kde je to potrebné pre zabezpečenie ochrany aktív a teda oblasť pôsobnosti rozdeľujeme na virtuálny a fyzický priestor. Virtuálny priestor je interaktívne prostredie informačných zdrojov, ktoré je vytvorené kooperáciou programových prostriedkov a samotnými počítačmi. Vo virtuálnom priestore je digitálna identita chápaná ako individuálny prejav fyzického jedinca – zamestnanca organizácie. Manažment identít vo virtuálnom priestore je potom nástroj na riadenie používateľských účtov

a oprávnení na prístup do koncových IS. IS môžu vo virtuálnom priestore vystupovať ako jeden virtuálny celok. Manažment identít je v podnikovom prostredí jedným z kritických procesov a to v závislosti od počtu IS, ktoré obsluhuje. S vyšším počtom IS rastie aj miera jeho kritickosti. Implementácia a spravovanie vhodných nástrojov na manažment identít je úlohou informačnej bezpečnosti v organizácii.

Riadením prístupu vo fyzickom priestore je chápané ako umožnenie, tak odmietnutie vstupu fyzického jedinca do určitých fyzických priestorov vo vlastníctve, nájme alebo správe organizácie, v ktorých sú umiestnené aktíva organizácie.

Záver

Informatizácia procesov v spoločnostiach a nástup riešení realizujúcich tiež prenos a uchovávanie informácií prináša ako daň pokroku zvýšené riziko ich úniku. Migrácia zamestnancov medzi konkurenčnými spoločnosťami tiež predstavuje vysoké riziko straty dôležitých poznatkov pri odchode týchto zamestnancov z organizácie. Systematický prístup k informačnej bezpečnosti prispeje k efektívnemu riadeniu všetkých procesov a informačných tokov. K bezpečnosti informácií je potrebné pristupovať komplexne a využívať v súčasnosti i u nás normované medzinárodne uznávané postupy a efektívne riadiť, merať a zlepšovať bezpečnosť informácií.

Literatura

[1] Doseděl, T.: Počítačová bezpečnost a ochrana datComputer Press 2004 ISBN 80-251-0106-1

[2] Mlýnek, J.: Zabezpečení obchodních informací, Computer Press, a. s. Brno, 2007 ISBN 978-80-251-1511-4

[3] Kučera, R.: HP OpenView Identity Management. eFocus, 4/2005