**Paneurópska vysoká škola v Bratislave, Fakulta informatiky**

|  |
| --- |
| Bratislava  1. 11. 2011 |

|  |
| --- |
| Adam Suchodolský |
| Prvý semestrálny projekt z predmetu Úvod do informatiky |
| Počítačová kriminalita a informačná bezpečnosť |

Obsah

[Úvod 2](#_Toc307921981)

[Informačná bezpečnosť 3](#_Toc307921982)

[Počítačová kriminalita 6](#_Toc307921989)

[Záver 6](#_Toc307921989)

[Zoznam bibliografických odkazov 6](#_Toc307921989)

# Úvod

V tejto práci sa budeme snažiť rozanalyzovať tému problematiky informačnej bezpečnosti a počítačovej kriminality. Ide o aktuálnu tému vzhľadom na trend nárastu informatizácie spoločnosti, kde čoraz viac informácií sa prenáša prostredníctvom moderných informačných technológií. Prínos týchto technológií je pre spoločnosť jednoznačná, no na druhej strane je tu aj otázka bezpečnosti týchto technológií a možnostiach ich zneužitia. Táto práca sa bude zaoberať práve týmto rizikám využívania IT, pričom sme sa zamerali najmä na aspekt ich využitia vo firmách.

Hlavným cieľom našej práce je poskytnúť čitateľovi bližšie informácie o tejto problematike pričom sa domnievame, že naša práca by mohla pomôcť čitateľovi získať o danej téme viac poznatkov, a takisto by mohla pomôcť čitateľovi k vytvoreniu vlastného postoja k danej téme.

Zdrojom našich informácií boli hlavne názory kompetentných obohatené o všeobecné informácie k tejto problematike, ktoré sme čerpali z odborných zdrojov, pričom väčšina informácií bola čerpaná z www stránok a odborných publikácií.

Túto prácu sme rozdelili na 4 časti. Prvá časť sa bude venovať definovaniu pojmu informačná bezpečnosť, predmetom druhej časti bude počítačová kriminalita, predmetom poslednej časti bude prevencia zabezpečenia informačnej bezpečnosti.

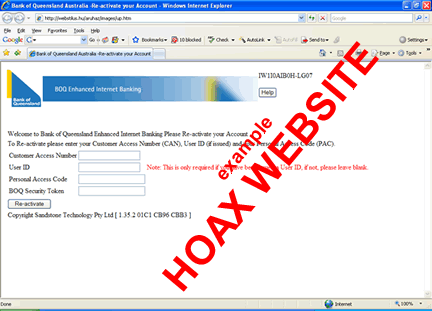
## Informačná bezpečnosť

 Predmetom tejto časti bude definícia pojmu informačná bezpečnosť. „ Informačná bezpečnosť sa v zmysle informatizácie definuje ako schopnosť siete alebo informačného systému ako celku odolať s určitou úrovňou spoľahlivosti náhodným udalostiam, alebo nezákonnému, alebo zákernému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a systémov“( [www.informatizácia.sk](http://www.informatizácia.sk), 2008). Tento pojem má samozrejme viac ako len túto jednu definíciu spoločnosť Disig as. zaoberajúca sa informačnou bezpečnosťou na svojej internetovej stránke definuje pojem informačná spoločnosť takto: „ Informačná bezpečnosť je ochrana informácií pred hrozbami a zraniteľnosťami s cieľom zabezpečiť kontinuálny a úspešný chod činností organizácie, minimalizovať podnikateľské riziko a maximalizovať využitie investícií a obchodných príležitostí“( [www.disig.sk](http://www.disig.sk), dátum neznámy). Tieto dva pohľady na to, čo je to informačná bezpečnosť jednoznačne dokazujú, že ide o závažnú problematiku a v súčasnej dobe by mala každá firma overiť, či je sieť, ktorú používajú bezpečná a či nehrozí problém zneužitia dát a podobne.

Obrázok 1 schéma oblastí do ktorej zasahuje informačná bezpečnosť zdroj: http://www.nextiraone.eu/sk/riesenia/it\_bezpecnostdátum neznámy.

Aj napriek tomu, že „informačná bezpečnosť nie je manažérsky proces ktorý priamo vytvára zisk, ale je v súčasnosti nevyhnutnou podmienkou pre chod procesov, ktoré sa na vytváraní zisku priamo podieľajú. Pritom zisk nemusí byť len materiálny ale aj duchovný. Preto nie je riešenie informačnej bezpečnosti limitované len na privátny sektor, ale  je dôležité aj vo verejnom sektore“( [www.disig.sk](http://www.disig.sk), dátum neznámy).

Dopad informačnej bezpečnosti na spoločnosť je tak nesmierny, pričom pre správne pochopenie tohto pojmu informačná bezpečnosť nezahrnuje len to že aby ste ako užívateľ IT technológií mali antivírus, ktorý je aktuálny, ale ako uviedol portál [www.informatizácia.sk](http://www.informatizácia.sk) „informačná bezpečnosť má veľký záber a pokrýva široké spektrum problematík, pričom s rozvojom IKT sa vynárajú stále ďalšie oblasti, ktoré sem patria a naopak zanikajú niektoré staré, aj keď v porovnateľne menšom meradle. Tieto oblasti vytvárajú "fenomény", ktoré prenikajú aj do bežného života. Z tých najznámejších sú to:

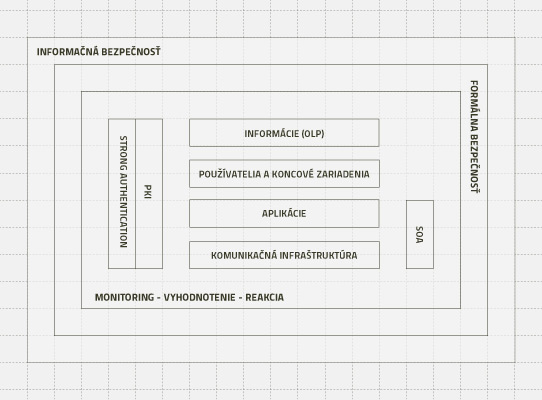
* Hoax

Obrázok 2 príklad na typickú hoax www stránku, zdroj: http://www.boq.com.au/fraud\_warning\_Ts\_Cs.htm, dátum neznámy

* kybernetický terorizmus
* [phishing](http://www.informatizacia.sk/vdok_simple-phishing/2999s3473c)
* [spam](http://www.informatizacia.sk/spam/3000s)
* [spyware](http://www.informatizacia.sk/vdok_simple-spyware/2999s3465c)
* vírusy a červy
* atď“( [www.informatizácia.sk](http://www.informatizácia.sk), 2008).

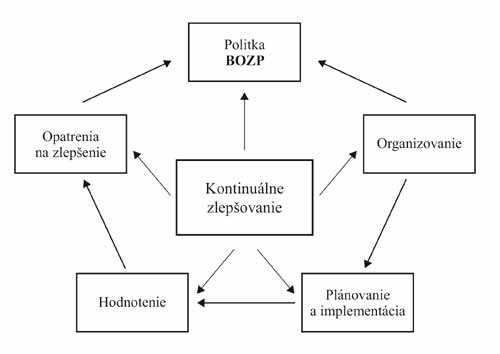
V súvislosti s informačnou bezpečnosťou ďalej portál [www.informatizácia.sk](http://www.informatizácia.sk) uviedol „informačná bezpečnosť je len jedna a je rozhodne odporúčané, aby sa pri jej zavádzaní a dodržiavaní myslelo na všetky jej aspekty, nezávisle od toho, či sa chránia špecifické typy informácií alebo systémov alebo tie úplné všeobecné. Toto odporúčanie je podľa nášho názoru veľmi dôležité a preto by sa s nim mala každá firma stotožniť, pretože len tak budú opatrenia ktoré implementujú do zabezpečenia IT technologií vo firme efektívne.

V nasledújucom obrázku č. 1 je znázornené rozdelenie informačnej spoločnosti podľa firmy Virte, ktorá informačnú bezpečnosť rozdelila do niekoľkých na sebe závislých celkov.



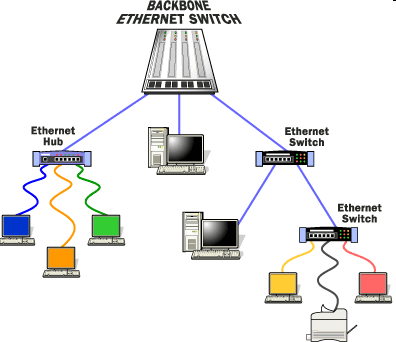
Obrázok 3, zdroj: http://www.virte.sk/produkty-a-sluzby/informacna-bezpecnost/, 2011

Toto rozdelenie výrazne napomáha pochopiť štruktúru informačnej bezpečnosti a firmy. Prostredníctvom neho potom môžu efektívne informačnú bezpečnosť zaviesť do praxe, pričom ku každej samostatnej časti informačnej bezpečnosti podľa ich rozdelenia spoločnosť pridala aj krátky popis.

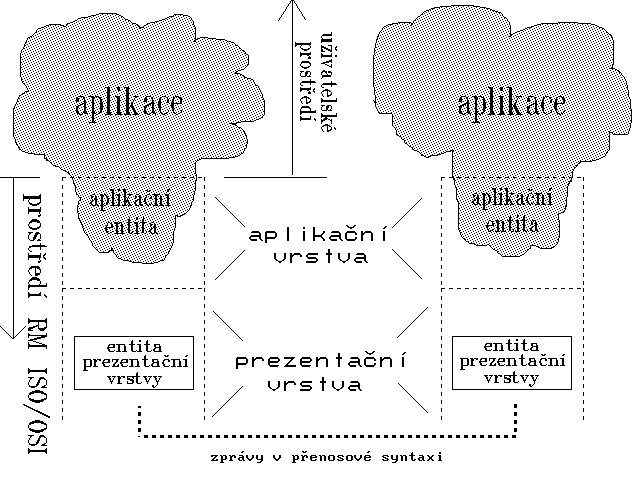


Podľa nášho názoru základným parametrom pre správne fungovanie informačnej bezpečnosti je formálna bezpečnosť. „Formálna bezpečnosť je veľmi dôležitým základom informačnej bezpečnosti, bez definovaných pravidiel bezpečného správania sa v prostredí informačných systémov, fungujú jednotlivé bezpečnostné mechanizmy ako samostatné ostrovy medzi ktorými je možné preplávať. Vďaka formálnej bezpečnosti je možné zabezpečiť aj vymožiteľnosť definovaných pravidiel a minimalizovať výnimky“([www.virte.sk](http://www.virte.sk), 2011).

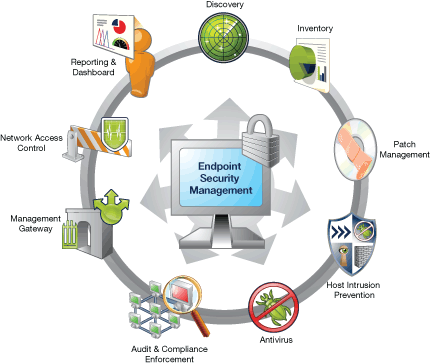
Obrázok 4, znázornenie tvorby formálnej bezpečnosti, zdroj: http://www.poradca.sk/SubPages/OtvorDokument/Clanok.aspx?idclanok=81156, dátum neznámy.

 Na aplikačnú vrstvu potom samozrejme nadväzuje komunikačná vrstva pri ktorej dochádza k výmene informácií „Na úrovni komunikačnej vrstvy je sieťová infraštruktúra. V rámci nej je potrebné vybudovať autonómne celky a chrániť hranice nielen na vstupe ale aj na výstupe“([www.virte.sk](http://www.virte.sk), 2011).

Obrázok 5 Schéma komunikačnej vrstvy, http://213.81.187.151/drupal/?q=node/196, dátum neznámy

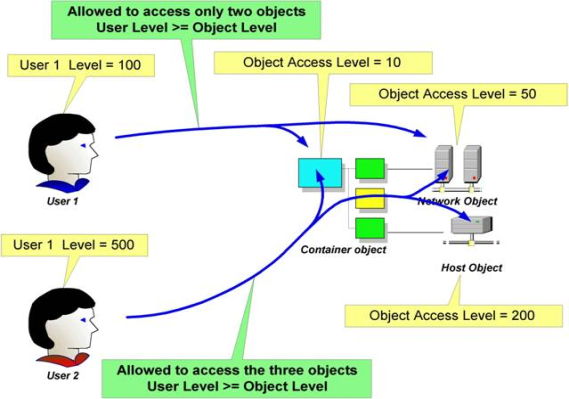
 Pri informačnej bezpečnosti je samozrejme nesmierna aj ochrana aplikácií ktoré používateľ používa . „Ochrana na aplikačnej vrstve je tvorená viacerými systémami. Hlavnou náplňou je ochrana proti malware a spyware. Antivírusové programy sa snažia reagovať a predvídať nové hrozby“([www.virte.sk](http://www.virte.sk), 2011).

Obrázok 6 Schéma aplikačnéj vrstvy, zdroj: http://www.earchiv.cz/a92/a227c110.php3, 2011



Obrázok 7 Schéma enpoint security, zdroj: http://www.orbital-ltd.co.uk/solutions/security-management/, dátum neznámy

Tieto systémy vedia zabrániť preniknúť do informačného systému firmy z externého prostredia no bohužiaľ neriešia hrozby zvnútra firmy najmä únik citlivých údajov o firme prostredníctvom zamestnancov firmy. „Enpoint security je téma posledných rokov, nakoľko dostupnosť a využívanie prenosných pamäťových zariadení je tak vysoká, že sa stala najväčšou hrozbou úniku informácií a vstupom pre nechcený softvér. Rôzne systémy pre ochranu neoprávneného prístupu k informáciám a na zabezpečenie ich integrity sú iba natoľko účinné, ako je implementované pokrytie všetkých hrozieb“([www.virte.sk](http://www.virte.sk), 2011).

 Tým pádom nastáva problém ako nastaviť ochranu informačného systému tak aby bola naozaj aj účinná . „Posun systému ochrany na samotný dátový objekt nesúci informáciu, minimalizuje počet možných hrozieb, umožňuje ich jednoznačnú identifikáciu a poskytuje mechanizmus na ich elimináciu. Pre tento účel slúži systém Object Level Protection, ktorý je možné integrovať s Right management systémom“([www.virte.sk](http://www.virte.sk), 2011)

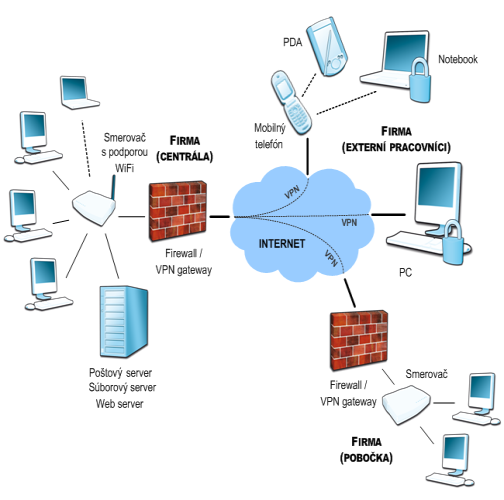
Obrázok 8 Schéma Object level protection systému, zdroj: http://www.loriotpro.com/Products/On-line\_Documentation\_V5/LoriotProDoc\_FR/P16-WEB-Remote\_Access/P16-D4\_User\_Access\_Management\_FR.htm, dátum neznámy.

 Pri rozoberaní tejto témy je nesmierne dôležité venovať sa ešte do hlbšej miery strate informácií v rámci informačnej bezpečnosti firmy. Cena informácie v súčasnosti enormne narastá a v súčasnej dobre sa dokonca stala cenným prostriedkom konkurenčného boja medzi firmami, kde sa firmy snažia získať rôznymi spôsobmi citlivé informácie za účelom dosiahnutia konkurenčnej výhody.

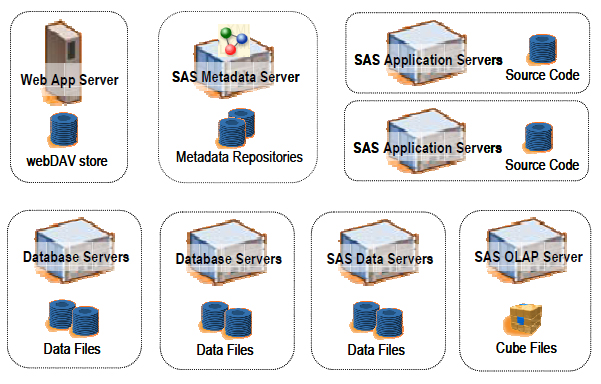
Obrázok 9 zdroj: <http://tomasbily.blog.sme.sk/c/182336/Informacia-znalostpoznanie-mudrost.html>, dátum neznámy

Pre kompletnú ochranu pred únikom citlivých informácií treba ako uviedol Martin Vozár pre časopis Infoware zabezpečiť ich ochranu v týchto sférach:

„ - oc­hra­na in­for­má­cií pri ich po­hy­be v pros­tre­dí,  
- oc­hra­na in­for­má­cií v úlo­žis­kách, kde sú uc­ho­vá­va­né,  
- oc­hra­na in­for­má­cií pri ich spra­co­va­ní na pra­cov­ných sta­ni­ciach ale­bo mo­bil­ných za­ria­de­niach,  
- oc­hra­na in­for­má­cií v ap­li­ká­ciách pri ich uc­ho­vá­va­ní a sprís­tup­ňo­va­ní,  
- opat­re­nia sú­vi­sia­ce s ria­de­ním prís­tu­pu k cit­li­vým in­for­má­ciám,  
- oc­hra­na šif­ro­va­cí­mi me­tó­da­mi, kto­ré riešia bez­peč­ný pre­nos a ulo­že­nie cit­li­vých in­for­má­cií,  
- or­ga­ni­zač­né opat­re­nia, kto­ré sa zväč­ša na­sad­zu­jú tam, kde tec­hnic­ké opat­re­nia zly­há­va­jú ale­bo sú nee­fek­tív­ne z fi­nan­čné­ho po­hľa­du“(M. Vozár, 2011). V nasledujúcom texte si bližšie špecifikujeme jednotlivé súčasti ochrany informácií.

  
 Základom ochrany informácií je ich ochrana pri ich prenose, prostredníctvom tejto ochrany sa zabezpečuje únik informácií z interného prostredia firmy do externého. „Oc­hra­na in­for­má­cií pri ich po­hy­be je po­pu­lár­na me­tó­da, kto­rá umož­ňu­je na zá­kla­de mo­ni­to­ro­va­nia sie­ťo­vej ko­mu­ni­ká­cie de­te­go­vať, za­zna­me­ná­vať, ria­diť a re­por­to­vať tok cit­li­vých in­for­má­cií pri ich po­hy­be. Pred­pok­la­dom na na­sa­de­nie je mož­nosť mo­ni­to­ro­va­nia a ria­de­nia ko­mu­ni­ká­cie, exis­ten­cia pra­vi­diel o po­uží­va­ní a o neop­ráv­ne­nom po­uži­tí in­for­má­cií. Vý­hod­ná je ľah­ká na­sa­di­teľ­nosť, ma­na­žo­va­teľ­nosť, ako aj množ­stvo po­dpo­ro­va­ných ap­li­kač­ných pro­to­ko­lov. Sla­bi­nou je, že ide o tec­hnic­ké rie­še­nie, v rám­ci kto­ré­ho ne­mož­no vždy spo­jiť pria­mo sie­ťo­vú ko­mu­ni­ká­ciu s ob­chod­ný­mi pra­vid­la­mi, čo ve­die k ťaž­kos­tiam pri roz­ho­do­va­ní, či ide o po­ru­še­nie bez­peč­nos­tných pra­vi­diel ale­bo o bež­nú ko­mu­ni­ká­ciu. Prob­lé­my sú­vi­sia aj s po­uží­va­ním šif­ro­va­nia ko­mu­ni­ká­cie. To je však pre niek­to­ré ap­li­kač­né pro­to­ko­ly rie­ši­teľ­né. Ne­vý­hod­né mô­že byť to, že ty­pic­ky tým­to spô­so­bom mož­no de­te­go­vať prib­liž­ne 20 % mož­ných úni­kov, čo ve­die k po­tre­be po­užiť ich v kom­bi­ná­cii s iný­mi me­tó­da­mi. “(M. Vozár, 2011).

Obrázok 10 schéma toku informácií, zdroj: <http://www.mopos.sk/products/com/data/remote/index.html>, dátum neznámy

 S ochranou informácií pri pohybe jednoznačne súvisí aj ochrana priestorov, kde sa informácie ukladajú, čiže úložiskách dát, kde ide o veľmi citlivé miesto v rámci informačnej bezpečnosti firmy nakoľko, v prípade, že sa k nemu dostane neoprávnená osoba môže sa tak dostať k citlivým informáciám a zneužiť ich. „Ty­pic­ky ta­ké­to sys­té­my riešia úlo­hy sú­vi­sia­ce s auto­ma­ti­zo­va­nou iden­ti­fi­ká­ciou a kla­si­fi­ká­ciou cit­li­vých in­for­má­cií v úlo­žis­kách a nás­led­ne ria­dia ich po­uži­tie a mo­ni­to­ru­jú ma­ni­pu­lá­ciu nap­rík­lad so sú­bor­mi na dis­ko­vých sys­té­moch, dá­to­vých zdro­joch a da­ta­bá­zach. Ide o nás­tro­je, kto­ré dopĺňa­jú pred­chád­za­jú­cu sku­pi­nu, pre­to­že mož­no správ­nej­šie po­sú­diť op­ráv­ne­nosť po­uži­tia in­for­má­cií a je či­ta­teľ­nej­šia sú­vis­losť med­zi spra­cú­va­ný­mi in­for­má­cia­mi a de­fi­no­va­ný­mi ak­tí­va­mi“(M. Vozár, 2011).

Obrázok 11 Úložiská dát v SAS Bussiness Analytics Framework, zdroj: <http://www.sas.com/offices/europe/slovakia/press/newsletters/feature/tipy_OCT.html>, dátum neznámy

Po tom ako firma zabezpečí ochranu pri pohybe informácií a ich následného ukladania na úložiskách stále nemá boj s IT bezpečnosťou vyhraný. Rovnako dôležité je aj zabezpečenie ochrany informácií pri ich spracovaní. „Rie­še­nia z tej­to sku­pi­ny vy­chád­za­jú z pred­pok­la­du, že väč­ši­nu úni­kov (až 80 %) reali­zu­jú ve­do­me ale­bo ne­ve­do­me sa­mot­ní po­uží­va­te­lia na svo­jich pra­cov­ných sta­ni­ciach. K na­ru­še­niu dô­ver­nos­ti pric­hád­za pri po­uží­va­ní ap­li­ká­cií, lo­kál­nych a sie­ťo­vých dis­kov, pe­ri­fé­rií umož­ňu­jú­cich pre­nos in­for­má­cií z or­ga­ni­zá­cie inak ako pros­tred­níc­tvom sie­te (nap­rík­lad tla­čiar­ne, CD, DVD, kľú­če USB) “(M. Vozár, 2011).

S ochranou informácií pri ich spracovaní úzko súvisí aj ich následné použitie pomocou aplikácií, ktorými firma disponuje. „Ide skôr o oc­hra­nu pred zra­ni­teľ­nos­ťa­mi webo­vých ap­li­ká­cií. Exis­tu­jú pra­vid­lá na návrh a vý­voj bez­peč­ných webo­vých ap­li­ká­cií. Nie­ke­dy sa ne­dodr­žia­va­jú z nez­na­los­ti, ino­ke­dy z dô­vo­du níz­kych roz­poč­tov na vý­voj sys­té­mu. Rie­še­nie na oc­hra­nu webo­vých ap­li­ká­cií sa na­zý­va web ap­pli­ca­tion fi­rewall. Ria­di ko­mu­ni­ká­ciu na zá­kla­de všeo­bec­ných pra­vi­diel a vo väč­ši­ne prí­pa­dov umož­ní od­strá­niť zra­ni­teľ­nos­ti, kto­ré by bo­lo nák­lad­né od­strá­niť prep­rog­ra­mo­va­ním, prí­pad­ne to už ani nie je mož­né, pre­to­že do­dá­va­teľ už neexis­tu­je. Rie­šiť mož­no nie­len ge­ne­ric­ké chy­by, ale aj opat­re­nia, kto­ré chrá­nia špe­ci­fic­ké čas­ti ap­li­ká­cií. Vďa­ka roz­ší­re­nos­ti webo­vých ap­li­ká­cií a po­rtá­lov ob­sa­hu­jú­cich cit­li­vé in­for­má­cie ide o veľ­mi účin­né opat­re­nie. Mno­hým úto­kom z ne­dáv­nej mi­nu­los­ti, kto­ré vied­li po­mo­cou SQL in­jec­tion k úni­ku in­for­má­cií, sa moh­lo za­brá­niť prá­ve ta­ký­mi­to rie­še­nia­mi. Pre rých­ly roz­voj tec­hník útoč­ní­kov a vy­so­ké nák­la­dy na úp­ra­vu webo­vých ap­li­ká­cií je tá­to tec­hni­ka vhod­ná aj pre sys­té­my vy­ví­ja­né v sú­čas­nos­ti“(M. Vozár, 2011).

K dosiahnutiu efektívnej IT bezpečnosti vo firme je potrebné aj určenie riadenia prístupu, teda jednoducho povedané určenie ktorí pracovník bude mať prístup k citlivým informáciám a ktorí nie. Firma tak predíde prípadným problémom, v prípade že sa informácia dostane k nesprávnej osobe. „Me­tó­dy na ria­de­nie prís­tu­pu sa vy­my­ka­jú spo­med­zi os­tat­ných uve­de­ných. Ne­riešia to­tiž únik in­for­má­cií, ale neop­ráv­ne­ný prís­tup k in­for­má­ciám. Ria­de­nie prís­tu­pu sa vo všeo­bec­nos­ti vní­ma ako ne­vyh­nut­ná po­dmien­ka na rie­še­nie oc­hra­ny in­for­má­cií a je za­bez­pe­čo­va­né sa­mot­ný­mi ap­li­ká­cia­mi. V prí­pa­de, že ap­li­ká­cie ta­ké­to pr­vky ne­ma­jú, mož­no rie­šiť tú­to prob­le­ma­ti­ku bez­peč­nos­tnou nad­stav­bou pred­ra­de­nou pred webo­vý­mi ap­li­ká­cia­mi, kto­rá vy­ko­ná auten­ti­zá­ciu, auto­ri­zá­ciu a nás­led­né ria­de­nie prís­tu­pu“(M. Vozár, 2011).

Problém však môže nastať v prípade, že firma potrebuje odoslať informácie do externého prostredia nad ktorým firma nemá kontrolu. Firma na takéto účely využíva ochranu šifrovaním. „ Jej for­my sú ur­če­né na oc­hra­nu in­for­má­cií v ne­dô­ve­ry­hod­nom pros­tre­dí. Po­uží­va­jú sa pri pre­no­se cit­li­vých in­for­má­cií cez inter­net, nap­rík­lad mai­lom, pri vzdia­le­nom pri­po­je­ní do inter­nej sie­te a pri pri­po­je­ní na webo­vú ap­li­ká­ciu. V prí­pa­de neop­ráv­ne­né­ho prís­tu­pu k no­si­čom in­for­má­cií ale­bo pros­tried­kom IT úni­ku dát za­brá­nia me­tó­dy, ako je šif­ro­va­nie sú­bo­rov, ce­lých no­si­čov dát a úda­jov v da­ta­bá­zach“(M. Vozár, 2011).

Tento problém má však dve úrovne jednou je zabezpečenie ochrany IT prostredia firmy, tá je však často nesmierne nákladná a musí sa neustále vyvíjať vzhľadom na neustály nárast nových a nových ohrození týchto systémov. Druhou úrovňou je prevencia, ktorá je menej nákladná a podľa nášho názoru ju reprezentujú najmä organizačné opatrenia medzi ktoré patria napríklad postihy za neoprávnenú manipuláciu s informáciami prípadne ich zneužitie. „Or­ga­ni­zač­né opat­re­nia sú neod­de­li­teľ­nou sú­čas­ťou kaž­dé­ho rie­še­nia. Umož­ňu­jú zní­žiť ri­zi­ká sú­vi­sia­ce s ne­ve­do­mý­mi únik­mi in­for­má­cií. Zvy­šu­jú in­for­mo­va­nosť po­uží­va­te­ľov, prí­pad­ne de­fi­no­va­ním zod­po­ved­nos­tí a san­kcií ich uve­do­me­losť“(M. Vozár, 2011).

### Počítačová kriminalita

Predmetom druhej časti bude počítačová kriminalita, pričom vzhľadom na to, že sme sa zamerali na pohľad na tému tejto práce z podnikateľského hľadiska v tejto časti nadviažeme na predošlú časť a budeme sa v nej venovať aby sme sa neopakovali už len definícií pojmu počítačová kriminalita a dohovoru EÚ o počítačovej kriminalite z roku 2011, ktorí SR ratifikovala a prispôsobilo právo oblasti IT kriminality na SR podľa neho . „Pod pojmom počítačová kriminalita alebo High-Tech Crime sa skrýva využívanie informačných technológií, najmä počítačov na páchanie trestnej činnosti. Jej rozmach je priamoúmerný postupujúcej informatizácii spoločnosti. Európske krajiny považujú túto formu trestnej činnosti za jednu z globálnych hrozieb a jedným z nástrojov na jej potieranie je Dohovor o počítačovej kriminalite z 23. novembra 2001. Slovenská republika tento dohovor ratifikovala v roku 2007“( <http://www.minv.sk>, dátum neznámy).

Prijatie tohto dohovoru predstavuje obrat v oblasti boja počítačovej kriminality vzhľadom na to, že podľa nášho názoru je dôležitá súdržnosť medzi krajinami a vzájomná spolupráca v boji s týmto fenoménom súčasnej doby. „Dôležitosť tohto dohovoru potvrdzuje aj fakt, že Rapídny nástup informačných technológií priniesol nárast určitých špecifických foriem páchania trestnej činnosti a to najmä z dôvodu rýchlosti, ktorou je možné vďaka výkonu jednotlivé úkony vykonať. Prečo práve internet priniesol rapídny nárast podobných aktivít. Dôvodov je viacero, pokúsme sa pomenovať aspoň niektoré z nich“ (J. Oster, dátum neznámy).

Tabuľka 1 Dôvody nárastu IT kriminality, informácie čerpané z: http://zodpovedne.sk/kapitola4.php?cl=kriminalita\_it, dátum neznámy

|  |
| --- |
| * cenová dostupnosť technológií |
| * pocit anonymity |
| * technologická nenáročnosť |
| * rýchlosť vykonania operácie |

Páchatelia IT kriminality majú tým pádom v dnešnej dobe vytvorené veľmi dobré podmienky na páchanie svojej trestnej činnosti, vzhľadom na náročnosť vyšetrovania takéhoto trestného činu. Jaroslav Oster uviedol „ práve vyššie uvedený Dohovor o počítačovej kriminalite zaviedol zaujímavú kategorizáciu činov namierených proti dôvernosti, dostupnosti a integrite počítačových systémov, sietí a počítačových údajov“(J. Oster, dátum neznámy).Túto kategorizáciu sme spracovali do tabuľky č. 2.

Tabuľka 2 Kategorizácia činov namierených proti dôvernosti, dostupnosti a integrite počítačových systémov, sietí a počítačových údajov informácie čerpané z: http://zodpovedne.sk/kapitola4.php?cl=kriminalita\_it, dátum neznámy

|  |  |
| --- | --- |
| 1. Trestné činy proti dôvernosti, hodnovernosti a dostupnosti počítačových údajov a systémov: | * nezákonný prístup do počítačového systému * nezákonné zachytávanie údajov * zasahovanie do údajov – poškodenie, vymazanie, zhoršenie kvality, pozmenenie údajov alebo zamedzenie prístupu k údajom * zasahovanie do systému – marenie funkčnosti počítačového systému * zneužívanie zariadení |
| 1. Počítačové trestné činy: | * falšovanie počítačových údajov * počítačové podvody |
| 1. Trestné činy týkajúce sa obsahu: | * trestné činy týkajúce sa detskej pornografie |
| 1. Trestné činy týkajúce sa porušenia autorských a príbuzných práv |  |

Toto rozdelenie je však pomerne dosť rozsiahle, preto považujeme za potrebné uverejniť aj jednoduchšie rozdelenie. Ako Jaroslav Oster ďalej uviedol „ z pragmatického hľadiska je možné dnes rozdeliť IT kriminalitu na dve základné oblasti, pričom toto rozdelenie sme spracovali do tabuľky č. 3 .

Tabuľka 3 Zjednodušené rozdelenie IT kriminality na dve skupiny, informácie čerpané z: http://zodpovedne.sk/kapitola4.php?cl=kriminalita\_it, dátum neznámy

|  |  |  |
| --- | --- | --- |
| 1. IT kriminalita kde IT (počítače, softvérové vybavenie, hardvérové vybavenie) sú prostriedkom | | * pozmeňovanie a falšovanie peňazí a cenín * ohováranie, zastrašovanie, vydieranie * úverové podvody – fiktívne doklady * prechovávanie a šírenie dát v rozpore so zákonom (napr.pornografia) |
| 1. IT kriminalita kde IT aktíva sú cieľom aktivít považovaných za trestnú činnosť: | * porušovanie autorského práva | * využívanie SW bez/v rozpore s platnou licenciou * nelegálne šírenie SW a audiovizuálnych diel * hard disk loading * nelegálne šírenie televízneho signálu pomocou IT |
| * cielené útoky zamerané voči dôvernosti, dostupnosti, integrite informačných systémov a dát, ktoré sú v nich spracované | * zneužívanie a poškodzovanie dát na nosiči informácií * neoprávnené nakladanie s údajmi dôverného charakteru (napr.osobné údaje). |

#### Záver

##### **Zoznam bibliografických odkazov**

1.

2.

3.

4.

5.

6.

7.