Peter Schmidt

BEZPEČNOSŤ A OCHRANA ÚDAJOV Z POHĽADU CLOUD COMPUTINGU

Úvod

Bezpečnosť je pojem o ktorom si každý myslí, že vie čo to je. Ak sa však spýtame hocikoho na definíciu bezpečnosti spravidla odpoveď nie je jednoduchá, prípadne sa dotyčný snaží zovšeobecniť bezpečnostnú definíciu z jeho odbornosti. Táto situácia je zapríčinená hlavne tým, že definícií je pomerne veľa, ale všetky na vysvetlenie samotného pojmu využívajú opozitum bezpečnosti – hrozbu. Nakoľko apercepcia bezpečnosti je prítomná od začiatku histórie ľudstva, ide o pojem, ktorý sa interpretuje vždy „vzhľadom k niečomu“. Je logické, že si každá disciplína vytvorila svoj bezpečnostný pojem ako napr. „štátna bezpečnosť“, „bezpečnosť cestnej premávky“, „počítačová bezpečnosť“, „bezpečnosť a ochrana zdravia“ atď. Každý bezpečnostný pojem má svoju definíciu alebo definícii podobnú charakteristiku, pričom sa často tieto definície ani len nepodobajú. [12].

Ako príklad, na ktorom si môžeme „bezpečnosť“ vysvetliť, si môžeme vybrať bežné pracovisko, ktoré tvorí komplexný systém so svojimi cieľmi. Na splnenie daných cieľov bola vytvorená organizačná štruktúra s príslušným kontrolným aparátom na všetky činnosti vykonávané na pracovisku. Takýto systém je bezpečný len vtedy, ak je schopný cez svoje vstupy a výstupy spolupracovať s okolitým svetom. Vo vnútri tohto systému, funguje podsystém, siahajúci až na najnižšiu úroveň, ktorý pracuje konsolidovane a vyrovnane. V prípade porúch sa aktivujú bezpečnostné protokoly ktoré zabránia vzniku väčších škôd.

Tieto všeobecné zásady by sme mali akceptovať vo všetkých sférach nášho života, či už sme doma, na ulici, alebo práve športujeme v parku. Prevažná väčšina ľudí si vôbec neuvedomuje, že najčastejšie úrazy, ktoré končia zranením sa udejú v domácnostiach alebo pri rôznych aktivitách vo voľnom čase. Je to hlavne preto, že médiá chrlia správy o nehodách a rôznych násilnostiach, čím u ľudí vytvárajú falošný pocit bezpečia v domácom prostredí. Stačí sa len spýtať ľudí, ktorí si dali namontovať bezpečnostné dvere, z akej pohnútky tak urobili. Najčastejší dôvod je samozrejme ten, že boli vykradnutí, prípadne k ich známym sa vlámali.

Kedy si používatelia PC kúpia antivírový program? Až po tom, čo po vážnej infekcii prišli o údaje.

Kedy si používatelia PC začnú archivovať údaje? Až po tom, čo po zlyhaní pevného disku prišli o všetky údaje.

Kedy sa vedenie spoločnosti začne zaujímať o počítačovú bezpečnosť? Až keď im nejaký „hacker“ ukradol citlivé informácie z nezabezpečenej infraštruktúry.

Podobných otázok by sme ešte vedeli napísať veľa, ale na všetky by boli odpovede, ktoré sa vyznačujú tým, že akcia, ktorá sa má vykonať je už vlastne reakcia na nejakú mimoriadnu situáciu. Preto nezaškodí upozorniť na stále hroziace nebezpečenstvo a upriamiť pohľad na už známe, avšak často nepochopené pojmy.

1 OCHRANA ÚDAJOV

Pod ochranou údajov rozumieme zabránenie neoprávnenému prístupu k údajom súkromného, komerčného a nekomerčného charakteru, ako aj k údajom, ktoré podliehajú určitému stupňu utajenia podľa zákona.[1] Tieto údaje však pre oprávnené osoby musia byť, po úspešnej autorizácii a autentifikácii, vždy prístupné.

Na ochranu údajov sa používajú viaceré mechanizmy ako napríklad:

- Systém prístupových oprávnení a správne pridelenie konkrétnych oprávnení jednotlivým osobám.
- Systém kontroly prístupov v reálnom čase.
- Systém evidencie prístupov na základe kontroly prístupov.
- Zabezpečenie spoľahlivej prevádzky systému pri zachovaní integrity a konzistencie údajov.
- Zabezpečenie systematického, pravidelného zálohovania údajov.
- Implementácia kontrolného mechanizmu na včasné odhalenie softvérových a hardvérových porúch a útokov.
- Systém na rýchlu diagnostiku poškodených údajov a ich okamžité obnovenie zo zálohy.

Pri tvorbe systému ochrany údajov je vhodné vytvoriť viacúrovňovú štruktúru v závislosti od charakteru údajov. Takto sa dajú vytvoriť kategórie, ktoré budú obsahovať informácie súkromného či finančného charakteru, alebo sa dá zvoliť kritérium podľa NBÚ (Národný bezpečnostný úrad) kde sa údaje rozdeľujú do troch kategórií a to na dôverné, tajné a prísne tajné. Všetky údaje ktoré podliehajú ochrane sa musia riadiť zákonom č. 428/2002 Z. z. o ochrane osobných údajov, ako vyplýva zo zmien a doplnení vykonaných zákonom č. 602/2003 Z. z., zákonom č. 576/2004 Z. z. a zákonom č. 90/2005 Z. z.

Základ ochrany údajov spočíva v jednoznačnom vymedzení a definovaní oprávnení používateľov a ich jednoznačnom identifikovaní v procese pristupovania k údajom.

V podnikových informačných systémoch sú spravidla všetky počítače pripojené do lokálnej siete, kde sú údaje umiestnené na jednom alebo viacerých serveroch, ktoré obhospodarujú prichádzajúce požiadavky, v závislosti od oprávnení používateľa. Preto je dôležité, aby v podnikovom prostredí boli oprávnenia všetkých používateľov jednoznačne stanovené.

[1] Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností

Silným nástupom mobilných zariadení ako sú notebooky, netbooky, tablety či smartphony [4]. sa otvárajú nové možnosti na uchovávanie a prenos údajov, čo zároveň prináša aj ďalšie bezpečnostné riziká. Aj keď ich prínos v oblasti dostupnosti údajov je nesporný, zvýšené riziko najmä v dôsledku straty, alebo odcudzenia je neúmerne veľké. Pri používaní mobilných zariadení má politika správy údajov ešte väčší význam. Na všetky údaje, ktoré sa nachádzajú na pamäťovom médiu prenosného zariadenia sa musíme dívať ako potenciálne ľahko odcudziteľné a preto by sa na prenosných zariadeniach nemali nachádzať údaje, ktoré sú potenciálne zneužiteľné a už vôbec nie také, ktoré by sme podľa zákona kvalifikovali ako tajné či prísne tajné.

2 BEZPEČNOSŤ ÚDAJOV

Bezpečnostné a ochranné aspekty musia tvoriť jednotný usporiadaný celok [2]. Každá organizácia, ktorá chce podstatne zvýšiť svoju informačnú bezpečnosť, si musí utvoriť adekvátny názor na svoje informačné aktíva, zhodnotiť ich význam a zaujať postoj k ich ochrane. Aktíva z bezpečnostného pohľadu sa často delia na hardvérové, softvérové a know-how. Kvalitatívnym ohodnotením aktív sa určuje cena, alebo hodnota konkrétneho aktíva, pričom sa často používa aj hodnotenie vyjadrujúce možný dopad na organizáciu, napr.:

1. Žiadny vplyv na organizáciu.
2. Zanedbateľný vplyv na organizáciu.
3. Problémy či finančné straty.
4. Vážne problémy alebo významná finančná strata.
5. Existenčné problémy organizácie.

V tomto duchu je nutné navrhovať aj riešenie bezpečnosti údajov. Bezpečnosť údajov ovplyvňujú faktory ako je dôsledná identifikácia, autentifikácia a autorizácia používateľov. Rovnako dôležité je zabezpečenie dôveryhodnosti používaných dokumentov, čiže musí byť implementovaný mechanizmus zaisťujúci originalitu dokumentu.

Ďalším kľúčovým bodom pri práci s údajmi, najmä vo forme dokumentov, je ich prenos prostredníctvom komunikačných médií. Bežne vo svete sa používa na zabezpečenie takejto komunikácie asymetrické šifrovanie, ale to zatiaľ nie je na Slovensku veľmi rozšírené. Dokonca aj posielanie zaheslovaných dokumentov je len zriedkavé a to máme na mysli hlavne štátnu správu. Rovnako dôležité je myslieť aj na dokumenty, ktoré sa neposielajú, len sa nachádzajú na samotnom počítači či serveri. Ich bezpečnosť sa najčastejšie rieši firewallmi, čo nemusí byť dostačujúce.

Heslá sú samostatnou bezpečnostnou kategóriou. Spravidla platí, že sa buď neuplatňujú, alebo ak áno, tak nedôsledne. Pri správe hesiel, by sa mali dodržiavať určité pravidlá. Najmä pri prihlasovaní k určitej službe je to veľmi dôležité. Správa hesiel by mala byť jednotná a mala by požadovať splnenie určitých kritérií, ako napr. minimálnu dĺžku hesla, využitie rôznych alfanumerických znakov, dĺžku životnosti hesla či počet pokusov o prístup.

Bezpečnostné riziko predstavuje aj samotná neznalosť základných pojmov, resp. ich obsahovej náplne. Rôzni autori definujú pojmy rôzne a veľmi často sa stretávame s definíciami, ktoré vychádzajú z prvopočiatkov výpočtovej techniky. Uvedieme niekoľko príkladov definícií, ktoré by mali vyhovovať súčasnej dobe.

Integrita

Integrita sa spravidla používa v spojení s informáciami, údajmi či programami na popísanie ich celistvosti a neporušenosti. Pod integritou údajov rozumieme fakt, že sa údaje nemôžu modifikovať bez zásahu oprávnenej osoby, či už osobne, alebo prostredníctvom softvérových nástrojov. V žiadnom prípade nesmie dôjsť k samovoľnej zmene týchto údajov. Toto základné bezpečnostné riziko sa týka aj spracovateľských programov, nakoľko porušenie integrity spracovateľského programu nemusí mať za následok viditeľnú nefunkčnosť, len nekorektne spracované údaje. Takúto nepríjemnú činnosť vykonávajú obvykle vírusy. Korektné údaje sú tie, ktoré majú zachovanú integritu, celistvosť a neporušenosť a správne popisujú skutkový stav.

Vírusy a iný potenciálne nebezpečný kód

Sú také programy či kódy, ktoré boli vyvinuté ilegálne za účelom poškodenia čo najväčšieho množstva používateľov. Dokážu sa šíriť bez vedomia používateľa. Aby sa mohol vírus rozmnožovať, vkladá kópie svojho kódu do iných spustiteľných súborov alebo dokumentov. Nakoľko tieto programy svojím mechanizmom šírenia pripomínajú biologické vírusy, dostali po nich aj pomenovanie. Vírusy sa môžu rozmnožovať v rámci jedného počítača, ale prostredníctvom siete aj medzi viacerými počítačmi. Dávnejšie sa prenášali len pamäťovými médiami disketami, CD, v súčasnosti sa väčšina prenáša internetom a len malé percento USB pamäťovými médiami. Rozlišujeme niekoľko druhov počítačových vírusov: [11]

- vírusy
- červy (internetové, e-mailové)
- trójske kone
- n-árne infiltrácie
- trpaslíci
- škriatkovia
- bomby a míny
- špióni (spyware)
- vydieračské kódy (ransomware)
- kombinácia prostriedkov

Toto vymenovanie samozrejme nie je konečné ani kompletné, lebo sa stále vymýšľajú nové a nové spôsoby napadnutia a šírenia škodlivého kódu. V súčasnosti možno už nie vírusy tvoria najväčší problém, ale iný škodlivý softvér - malvér (ang. malware), pomocou ktorého sa dajú vykonávať na napadnutom počítači rôzne činnosti, od otravných spúšťaní reklám advérom (ang. adware), hijackermi, hoaxmi, až po krádež osobných údajov phishingom, či vybielenie

bankového účtu pharmingom.[2] Aby sa zabránilo a predišlo škodám spôsobeným škodlivým softvérom, je nutné dodržiavať nasledovné postupy:

- nepoužívať cudzie, neznáme pamäťové médiá,
- neotvárať neočakávané a podozrivé e-maily,
- pravidelne zálohovať údaje,
- USB kľúče vždy pred načítaním skontrolovať antivírusom,
- používať rezidentný antivírus,
- používať legálny, originálny software.

Nepodceňovanie vírusovej a malvérovej infiltrácie je asi najmocnejším nástrojom proti tejto bezpečnostnej hrozbe.

Počítačová bezpečnosť je oblasť informatiky, ktorá sa zaoberá odhaľovaním a eliminovaním bezpečnostných rizík spojených s používaním počítača a počítačovej siete. Cieľom počítačovej bezpečnosti je prostredníctvom nastavenia bezpečnostných politík zabezpečiť:

- ochranu pred neoprávneným manipulovaním so zariadeniami počítačového systému,
- ochranu pred neoprávnenou manipuláciou s údajmi,
- ochranu pred nelegálnou tvorbou kópií údajov,
- bezpečnú komunikáciu a prenos údajov,
- bezpečné uloženie údajov,
- integritu, neporušenosť a celistvosť údajov.

Koncepcia počítačovej bezpečnosti spočíva v troch krokoch:

1. **prevencia** - ochrana pred bezpečnostnými hrozbami,
2. **detekcia** - odhalenie neoprávnenej činnosti a slabých miest v systéme,
3. **náprava** - odstránenie slabých miest v systéme.

Vyššie spomenuté bezpečnostné riziká sa týkali viac-menej softvérovej bezpečnosti, aj keď je zrejmé, že softvérová a hardvérová bezpečnosť sa musia vnímať spoločne. Hardvérovú bezpečnosť by sme mohli rozdeliť do dvoch základných skupín a to:

- ochrana údajov pred stratou v dôsledku zlyhania hardvérových prostriedkov,
- ochrana pred odcudzením hardvérových prostriedkov,
- ochrana komunikačných liniek pred poškodením.

Strata údajov v dôsledku zlyhania hardvérových prostriedkov už v súčasnosti nepatrí medzi najvážnejšie riziká. Pozitívny vývoj situácie v tejto oblasti majú na svedomí ľahko dostupné vysokokapacitné pamäťové médiá, ktorých integrácia do počítačového systému nepredstavuje veľkú finančnú záťaž. Máme na mysli

[2] Phishingom sa rozumie podvodné vylákanie citlivých informácií od používateľa, podstrčením falošnej webstránky. Ak sa použije pri internetbankingu tak hovoríme o pharmingu.

riešenia, ako je zrkadlenie diskov, zdvojenie diskov či tvorba RAID[3] polí. Samozrejme aj v tejto oblasti existujú nákladné riešenia ako je klastering[4], či realizácia distribuovaného systému. Druhá cesta je využitie stále viac rozšírených cloudových riešení.

3 CLOUD COMPUTING A BEZPEČNOSŤ

Cloud computing (CC) patrí medzi technológie, ktoré sa už pravidelne využívajú. Nakoľko podstata cloudu spočíva v distribúcii zdrojov a dát, pričom ich konkrétne umiestnenie je pred používateľom skryté, veľa používateľov má obavy práve z pohľadu bezpečnosti. Používatelia, ktorí chcú mať plnú kontrolu nad svojimi dátami sa pre cloud rozhodujú ťažšie, práve preto, že nevedia, kde konkrétne sú ich dáta v rámci cloudu uložené a či sú patrične zabezpečené [13]. V niektorých oblastiach je však bezpečnosť údajov lepšie zabezpečená, ako v prípade tradičného spôsobu. [1]. Pre hackera je jednoduchšie dostať sa na lokálny počítač, ako na server veľkej spoločnosti (Amazon, Google, ...), ale aj v cloude existujú vážne bezpečnostné riziká spojené s nedodržiavaním zákonov, dostupnosťou či integritou dát. Je naozaj potrebné zvyšovať odolnosť proti zlyhaniu. Jedným z problémov býva, že zákazník nemá tušenie ani skoro žiadnu kontrolu nad tým, kde sa jeho údaje nachádzajú (v akej krajine, v ktorom dátovom centre, ...). V prípade citlivých informácií je dôležité, aby neboli premiešané s ostatnými, cudzími údajmi, ako je to na zdieľaných serveroch. Veľmi vážnym problémom, ktorý môže nastať, je ak sa na jednom fyzickom serveri okrem našich údajov (a stoviek ďalších) nachádzajú aj údaje súvisiacou s trestnou činnosťou, v dôsledku čoho môže dôjsť k zadržaniu servera orgánmi činnými v trestnom konaní. K takýmto prípadom dochádza pomerne často pri serveroch umiestnených na území USA. Takáto situácia môže nastať v prípade porušenia zákonov, podozrenia z porušovania autorských práv, prípadne podozrenia zo šírenia nelegálneho obsahu. Fungovanie cloudu vďaka distribúcii údajov nebýva ovplyvnené, avšak údaje sa dostanú k analytikom a ďalej sa spracovávajú, a citlivé informácie sa môžu objaviť vo vyšetrovacích spisoch, alebo sa môžu dostať aj do nepovolaných rúk. Zákon totiž nemôže chrániť údaje na cloude umiestnené na inom kontinente tak, ako v prípade cloudu umiestneného na Slovensku. Pravdou však ostáva, že ak sa vzdajú spoločnosti určitej kontroly nad svojimi údajmi, môžu výmenou za to získať omnoho hospodárnejšie náklady a tým sa stanú konkurencieschopnejší [9].

Aj keď je na pohľad tradičný spôsob bezpečnejší, nie je tomu vždy tak. Hlavným zdrojom úniku informácií, či porušenia bezpečnosti bývajú práve zamestnanci a používatelia počítačov. Toto ohrozuje hlavne tradičný spôsob

[3] RAID je skratka pre označenie redundantného ukladania údajov na viac nezávislých diskov

[4] Klaster (ang. Cluster) je skupina voľne viazaných a navzájom spolupracujúcich rovnakých počítačov.

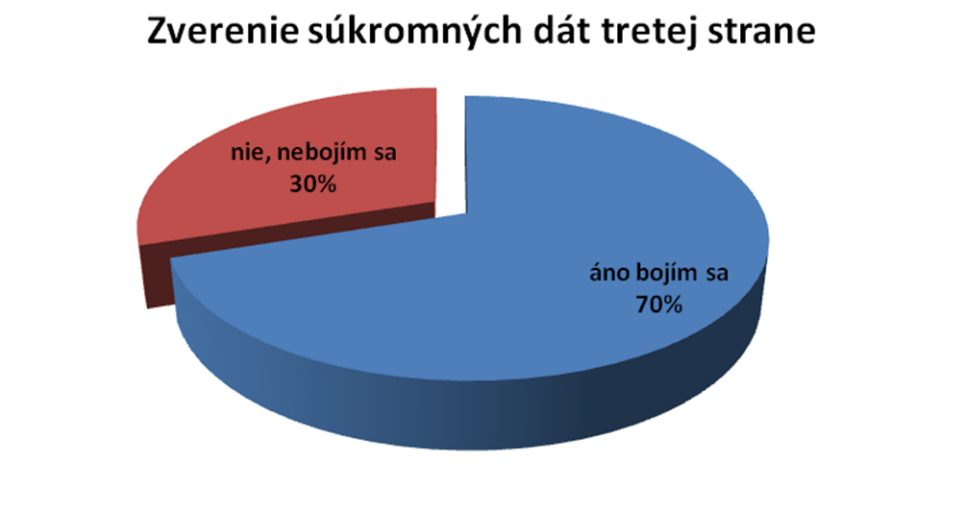
poskytovania služieb. „Hoci veľké podniky sa zatiaľ nemôžu spoliehať na zabezpečenie implementované priamo v cloud computingu, malé spoločnosti môžu vďaka CC získať lepšiu ochranu." [5]. V prípade, že je kritická chyba v systéme (aplikácii), je jednoduchšie a rýchlejšie jej odstránenie v cloudovom riešení, ako v tradičnom. Technik aktualizáciou opraví chybu u všetkých zákazníkov naraz a v krátkom čase, kým pri tradičnom spôsobe musí technik aktualizovať aplikáciu na každom počítači.

3.1 Mikroanketa

Cloud computing patrí medzi tie technológie, ktorých masívny rozmach sa očakáva v najbližších rokoch. Preto sme boli zvedaví na akceptáciu CC u mladých informatikov v zrkadle bezpečnostných rizík s ním spojených. Opýtali sme sa 100 študentov informatiky na druhom stupni VŠ štúdia na ich postoje ohľadne bezpečnosti na cloude.

Táto mikroanketa nemala za cieľ monitorovať názory mladej generácie na CC, ale poukázať na názory takých mladých ľudí, ktorých informatické znalosti sú hlbšie než je priemer. Ich postoje sú vyjadrené v nasledujúcich grafoch.

V prvej otázke sme boli zvedaví, ako respondenti pristupujú k poskytovaniu súkromných dát tretím stranám. Z obr. 1 je evidentné, že pri poskytovaní súkromných dát majú obavy, z čoho by sme mohli predpokladať, že budú aj opatrnejší a zvážia bezpečnostné riziká.



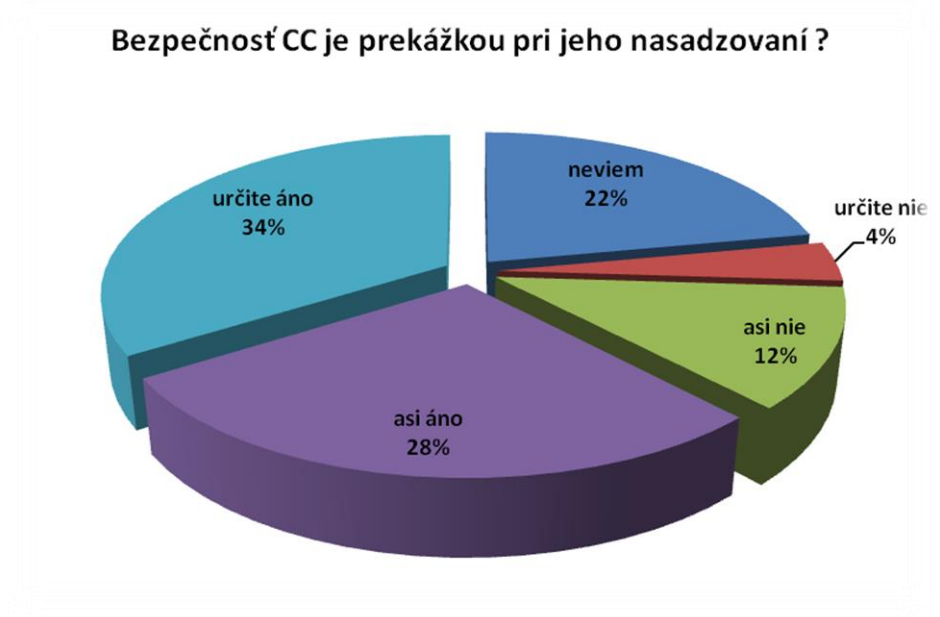
Obr. 1: Zverenie súkromných údajov tretej strane

V druhej otázke nás zaujímali názory respondentov na bezpečnosť úložiska. Výsledok bol prekvapujúci a svedčil o nedôvere ku cloudovým riešeniam. Len 11% respondentov si myslí, že úložisko dátového centra je

bezpečnejšie než vlastné pamäťové médium. Pri tejto otázke by možno bolo zaujímavé zisťovať, koľko respondentov už stratilo svoj USB kľúč.

Obr. 2: Názory na bezpečnosť interného a externého úložiska

Pri tretej otázke už bol rozptyl názorov väčší, čo vidno aj z posledného grafu. Viac ako polovica opýtaných (62%) si myslí, že problémy s bezpečnosťou cloudových riešení je prekážkou pri nasadzovaní CC do praxe.



Obr. 3: Bezpečnosť ako bariéra pri nasadzovaní CC

Z uvedených grafov je evidentné, že mladí ľudia so znalosťami v oblasti informatiky, nepodceňujú možné bezpečnostné riziká pri využívaní cloudu, ak sú si vedomí, že cloud využívajú. Ich obavy z hľadiska technického zabezpečenia asi nie sú oprávnené, avšak z hľadiska možnosti úniku informácií sú pochopiteľné. Preto sa väčšina používateľov snaží uchovávať svoje údaje na lokálnych pamäťových médiách, čo pri nemalom počte stratených USB kľúčov asi nebude najlepšie riešenie. V prípade informácií zdieľaných na sociálnych sieťach by sme pravdepodobne dostali iné výsledky, nakoľko si používatelia vôbec neuvedomujú, že používajú cloudové riešenia.

4 ÚNIK INFORMÁCIÍ

Za posledné roky nastal pozitívny posun aj vo fyzickom zabezpečení serverových prostriedkov. Organizácie vynakladajú značné prostriedky na zabezpečenie vlastnej hardvérovej infraštruktúry. Ide hlavne o fyzickú bezpečnosť serverov organizácie, jednoznačným vyšpecifikovaním prístupových oprávnení k fyzickým prostriedkom a nepodceňovanie bezpečnostných rizík. Na druhej strane, už spomínaným mohutným nástupom mobilných zariadení, ktoré sú schopné uchovávať veľké množstvá údajov, fyzické odcudzenie servera už zďaleka nie je tak lákavé, ako odcudzenie samotných údajov na mobilnom zariadení. Máme na mysli údaje, ktoré sú dostupné aj zamestnancom na nižšom stupni hierarchického rebríčka organizácie, pritom pre organizáciu môžu mať strategický význam. Aj na Slovensku rezonovali aféry týkajúce sa úniku a

zverejnenia určitých informácií, ktoré sa týkali utajovaných skutočností, napr. z prostredia vojenského spravodajstva.

V oblasti priemyselnej výroby najmä v čase krízy rastie snaha o získanie určitých výhod aj nekalým spôsobom a rastie tak počet pokusov o odcudzenie informácií od konkurenčných spoločností. Tu si však treba uvedomiť jeden závažný fakt a to je ľudský faktor. Takmer všetky úniky informácií, ktoré sa vykonali fyzickým prenosom informácií na mobilné pamäťové médium, majú na svedomí vlastní zamestnanci organizácie. Na toto bezpečnostné riziko sa organizácia zameria až po prvom úniku informácií, pričom vzniknuté škody sú neporovnateľne vyššie ako náklady, ktoré by zabezpečili spokojnosť a lojalitu zamestnanca. Táto hrozba patrí medzi najväčšie, nakoľko k úniku informácií môže dôjsť aj keď sa využíva špičkový, dobre navrhnutý a zrealizovaný bezpečnostný systém. Nezanedbateľným bezpečnostným rizikom je zdieľanie fyzických úložísk viacerými subjektmi, pričom niektoré subjekty využívajú tieto systémy na nezákonnú činnosť. Odhalením tejto činnosti a následným konaním príslušných orgánov sa môžu stať naše údaje nechránené vo fyzickom aj právnom zmysle slova.

Záver

Otázka informačnej bezpečnosti vyžaduje systémový prístup a nie „látanie bezpečnostných dier“ po incidente. Budovanie a certifikovanie systémov riadenia informačnej bezpečnosti v posledných rokoch dosiahol medzinárodné rozmery. Dôkazom je skutočnosť, že britský štandard BS 7799 [7] (uvedený ešte v roku 1995) bol s malými úpravami prevzatý do sústavy štandardov ISO/IEC. Systém manažmentu informačnej bezpečnosti, známy ako SMIB, je podľa BS 7799 časť celkového systému riadenia, založená na prístupe k rizikám organizácie, ktorej úlohou je implementovať, prevádzkovať, monitorovať, revidovať, udržiavať a zlepšovať informačnú bezpečnosť. Vo svetovom meradle je budovanie a certifikácia SMIB podľa ISO/IEC 17799 [8] bežnou vecou, avšak na Slovensku sa aj po rokoch stále len rozbieha. Celosvetovo uznávaných štandardov určených na budovanie systému riadenia bezpečnosti nie je veľa. Medzi najrozšírenejšie patrí ISO / IEC 27001 - Information Security Management Systems známy ako ISMS. Účelom tejto medzinárodnej normy je poskytovanie podpory pre vytvorenie, implementáciu, prevádzkovanie, monitorovanie, udržiavanie a zlepšovanie systému riadenia informačnej bezpečnosti, podobne ako pri SMIB. Odborníci na bezpečnosť už dlho vedia, že nestačí systém len zaviesť, ale sa oň treba neustále starať, rozvíjať a aktualizovať, aby bol pripravený na stále narastajúci počet bezpečnostných incidentov. V roku 2005 bol uvedený do platnosti štandard, zahŕňajúci tie najaktuálnejšie poznatky z oblasti komplexnej informačnej bezpečnosti - ISO 27001, ktorý je postavený na základoch BS 7799/ISO 17799. Jedným z najčastejšie používaným modelom v rámci ISMS je model PDCA. Je to skratka vytvorená zo začiatočných písmen slov Plann, Do, Check a Act, čiže plánuj, urob, kontroluj a konaj. Keďže ide o kontinuálny systém

riadenia informačnej bezpečnosti v organizácii, jednotlivé kroky zaručujú, že zavedenie systému nebude len jednorazovou činnosťou, ale súvislým kolobehom. Norma jasne popisuje, postup pri zavádzaní ISMS a taxatívne nariaďuje, ktoré ciele a bezpečnostné opatrenia musia byť dosiahnuté.

Niektoré organizácie majú dobre zvládnutú infraštruktúru informačnej bezpečnosti, avšak založenú zväčša na subjektivite prístupov, úloh a zodpovedností. Organizáciám na Slovensku taktiež často chýba dostatočná motivácia, ktorá by posunula realizáciu informačnej bezpečnosti o krok vpred smerom k hierarchickému manažérskemu prístupu, čoho dôsledkom je „oneskorenie“ o 4 až 6 rokov oproti krajinám EÚ.

Organizácií, ktoré sa venujú ochrane a bezpečnosti informácií je veľa a priestor malý, preto spomenieme len jednu. Spoločnosť HP je jedným z lídrov v tomto segmente, o čom svedčí aj to, že rozšírila svoje portfólio bezpečnostných riešení, ktoré organizáciám umožňuje spravovať, transformovať a optimalizovať svoje bezpečnostné procesy a využívať ich proaktívnu ochranu [10]. Iniciatívy v oblasti cloudu, mobilných technológií a spravovania objemných dát pomáhajú organizáciám s riešením stále väčších technologických problémov. Súčasne pritom urýchľujú „adaptáciu“ týchto noviniek v ich IT prostrediach. Ponúkajú väčší priestor pre inovácie, rozšírené možnosti správy IT infraštruktúry a optimalizujú náklady.

Žiaľ, môžu vznikať aj bezpečnostné komplikácie týkajúce sa nesprávneho pochopenia bezpečnosti cloudových služieb a ťažkosti so správou objemných dát. Bežné reaktívne možnosti ochrany dát však v súčasnosti už zďaleka nestačia. Organizácie potrebujú inteligentné proaktívne technológie, ktoré spoja tradičné i hybridné modely poskytovania služieb a zároveň vyriešia nové problémy v IT sfére. Organizácie, ktoré pôsobia vo verejnom sektore, musia neustále „bojovať“ s rastúcim množstvom bezpečnostných hrozieb, stále zložitejšími nariadeniami a znižujúcimi sa rozpočtami. Vďaka riešeniu HP Security for Public Sector, ktoré združuje všetky dôležité bezpečnostné služby HP, môžu tieto organizácie dosiahnuť splnenie všetkých svojich náročných štandardov oveľa ľahšie.

Nakoľko je oblasť bezpečnosti a ochrany veľmi široká, nie je možné sa venovať na takomto malom priestore všetkým bezpečnostným rizikám. Snažili sme sa skôr poukázať na fakt, že inštalácia antivírusu a firewallu, z hľadiska bezpečnosti nie je zďaleka dostačujúce riešenie, ak nechceme prísť o svoje údaje. Uvedomenie si podstaty základných pojmov môže značne pomôcť v pochopení podstaty pojmov bezpečnosť a ochrana dát.

Kľúčové slová

bezpečnosť, ochrana, Cloud computing, ISMS, SMIB

Klasifikácia JEL

K22

LITERATÚRA

[1] SCHMIDT, P; KULTAN, J. 2012. Cloud computing v miestnej samospráve, In Ekonomické aspekty v územnej samospráve II [elektronický zdroj] : recenzovaný zborník príspevkov z vedeckej korešpondenčnej konferencie : Košice 2012, ISBN 978-80-7097-932-7. - S. 159-167.

[2] KALUŽA F.: Manažérsky prístup v riešení informačnej bezpečnosti firmy. Security Revue - ISSN 1336-9717, [online]. [cit. 2012-25-09] http://www.securityrevue.com/article/2006/06/manazersky-pristup-v-rieseni-informacnej-bezpecnosti-firmy/

[3] KRISTOVÁ, G., LÉVARDY, F. 1998. Bezpečnosť v elektronickom obchode. In Transformácia ekonomiky skúsenosti Slovenska a ďalších krajín Strednej Európy : medzinárodná vedecká konferncia, Bratislava 14.-16. 5. 1998. - Bratislava : Ekonóm, 1998. - ISBN 80-225-0991-4. - S. 186-189

[4] KRAUSPE, K., PITTNER, J., .SCHMIDT, P.. Apple data security and data theft, In Trends and Innovation in E-business, Education and Security = Zborníkov z konferencie, dňa 19.11.2014 : Proceedings, dňa 19.11.2014 / recenzenti: Miroslav Hudec, Jaroslav Kultán. - Bratislava : Ekonomická univerzita v Bratislave, 2014. - ISBN 978-80-225-3987-6. - pp. 60-67 CD-ROM.

[5] SCHWARTZ, EPHRAIM: Cloud computing skrýva rad nebezpečenstiev. [online]. [cit. 2012-28-09] http://www.itnews.sk/spravy/bezpecnost/2009-07-29/c123308-cloud-computing-skryva-rad-nebezpecenstiev

[6] Zákon o ochrane osobných údajov č. 428/2002 Z. z.

[7] BS 7799:2002: Britský štandard: Systémy riadenia informačnej bezpečnosti – Špecifikácia s radami na použitie

[8] BS ISO/IEC 17799: 2000: Britský štandard: Informačné technológie – Kódex praxe riadenia informačnej bezpečnosti

[9] EURACTIV : Cloud computing: Právny hlavolam pre EÚ (aktualizácia: 12.04.2011).[online]. [cit. 2012-18-09] http://www.euractiv.sk/rozsirovanie/zoznam_liniek/cloud-computing-pravny-hlavolam-pre-eu-000279

[10] Web stránka spoločnosti HP http://www8.hp.com/us/en/hp-news/press-kit.htm

[11] Web stránka spoločnosti Kaspersky http://usa.kaspersky.com/internet-security- center/ threats/

[12] SZABO, L. 2012. WHAT IS THE SAFETY?, In Trendy a inovácie v internetovej podpore podnikania a vzdelávania. Medzinárodná vedecká internetová videokonferencia vedeckých pracovníkov a doktorandov. *Trendy a inovácie v internetovej podpore podnikania a vzdelávania : recenzovaný zborník [príspevkov] : II. medzinárodná vedecká internetová videokonferencia vedeckých pracovníkov a doktorandov : 7. november 2012, [virtuálne EU Bratislava]* [elektronický zdroj]. Zostavili Gabriela

Kristová, Peter Schmidt, Janette Brixová, Ján Pittner. [Bratislava : Vydavateľstvo EKONÓM, 2012]. CD-ROM [80 s.]. ISBN 978-80-225-3553-3.

[13] SCHMIDT, P., RUBÓCZKI, E. 2016. Implementácia cloudových služieb v podnikovom prostredí z hľadiska bezpečnosti. In International scientific days 2016. The agri-food value chain: challenges for natural resources management and society : conference proceeding of reviewed articles : May 19-20, 2016 Nitra, Slovak Republic / Reviewers: Izabela Adamičková, Natália Turčeková. - Nitra : Slovak university of agriculture, 2016. - ISBN 978-80-552-1505-1. - S. 216-222.

RESUMÉ

Cieľom tohto príspevku je poukázať na problematiku bezpečnosti a ochrany dát nielen z hľadiska informatickej vedy. Zaoberáme sa so súvislosťami s medzinárodnými normami a štandardmi. Ďalej špecifikujeme niektoré kľúčové definície, ako sú bezpečnosť dát, hardvérová a softvérová bezpečnosť, atď.. Na základe prieskumu uskutočneného v univerzitnom prostredí medzi študentami informatiky, sa snažíme poukázať na niektoré bezpečnostné riziká ako problém v prijatí cloudových technológií. Úspech novej technológie je v nemalej miere závislý od jej akceptácie budúcimi používateľmi. Preto je dôležité akceptovať názory budúcich používateľov v otázke bezpečnosti cloudových riešení. Tento článok sa zaoberá potenciálnymi hrozbami pre bezpečnosť a aktuálnymi variantmi bezpečnostných rizík. Príspevok nemá ambície pôsobiť ako istý návod, ale skôr chce poukázať na reálne ohrozenie.

SUMMARY

The aim of this paper is to highlight the issue of safety and security not only in terms of computer science. We deal with the context of the international norms and standards. Further specifies some key definitions such as data security, hardware and software security, etc. Based on the survey conducted in the university among science students, we try to highlight some security risks as a problem in the adoption of cloud technologies. The success of the new technology is largely dependent on its acceptance of future users. Therefore, it is important to accept the views of future users to the security of cloud solutions. This article discusses potential threats to safety and security risks. Paper hasn't ambition to act as a sure guide, but rather seeks to demonstrate a real threat.

Kontakt

Ing. Mgr. Peter Schmidt, PhD., Katedra aplikovanej informatiky, Fakulta hospodárskej informatiky, Ekonomická univerzita v Bratislave, Dolnozemská cesta 1, 852 35 Bratislava, e-mail: peter.schmidt@euba.sk