EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE
it akadémia

Modul 12: Bezpečnosť pri využívaní IKT

Bezpečná správa údajov

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
www.itakademia.sk
ITMS2014+: 312011F057

7 Bezpečná správa údajov

Pre zabezpečenie dostupnosti informácií len pre oprávnené osoby musíme, okrem zabezpečenia informácií v IS alebo pri ich prenose, urobiť opatrenia, aby:

- sa k pamäťovým médiám nedostali neoprávnené osoby,
- v prípade zlyhania pamäťového média sme údaje nestratili,
- v prípade vyradenia pamäťového média údaje nebolo možné obnoviť.

7.1 Bezpečnosť a zálohovanie

7.1.1 Spôsoby zabezpečenia fyzickej bezpečnosti zariadení obsahujúcich údaje, napríklad ich vhodné umiestnenie, používanie káblových zámkov, kontrola prístupu

Okrem ochrany prístupu k údajom cez počítače a IS je potrebné zabezpečiť aj fyzickú bezpečnosť údajov a zariadení, ktoré tieto údaje obsahujú.

Podobne, ako sú vo firme stanovené pravidlá pre zabezpečenie a prístup k papierovým dokumentom, mali by byť stanovené aj pravidlá pre zabezpečenie a prístup k zariadeniam, ktoré spracúvajú a ukladajú informácie, a k ich pamäťovým médiám.

Servery bývajú väčšinou umiestnené v špeciálnych klimatizovaných miestnostiach chránených bezpečnostným a protipožiarnym systémom („serverovne“). Napájanie zariadení v tejto miestnosti je spravidla chránené záložnými zdrojmi. Servery podľa použitia bývajú umiestnené v špeciálnych stojanoch, ktoré môžu mať vlastný zabezpečovací systém.

Prístup k počítačom bežných používateľov býva zabezpečený ochranou prístupu do miestnosti, kde je počítač umiestnený. V prípade, že sa počítač alebo notebook používajú na mieste s veľkým pohybom cudzích ľudí (verejne dostupné miesta, výstavy, veľtrhy a pod.), sa zvyknú používať mechanické spôsoby ochrany, ako sú káblové zámky a pod.

Ak používateľ má k dispozícii prenosnú techniku, ako je notebook, prenosný disk, tablet, smartfón a pod., mal by ju chrániť pred poškodením (vhodný obal pri preprave, bezpečné miesto na používanie) a pred odcudzením (nenechávať na voľne dostupných miestach bez dozoru, voľne položené na sedadle v zaparkovanom aute).

7.1.2 Prečo je dôležité mať záložné postupy v prípade straty údajov, finančných záznamov, záložiek webových stránok a histórie pohybu po webových stránkach

Pre zabezpečenie dostupnosti údajov aj v prípade zlyhania IS, alebo pamäťového média (porucha, neoprávnený zásah, vyššia moc a pod.) nám pomôže hlavne zálohovanie. V prípade pravidelných záloh s dostatočnou frekvenciou je možné po havárii systému, alebo po strate údajov, obnoviť prevádzku IS v relatívne krátkej dobe. Tým sa môžu minimalizovať straty spôsobené nedostupnosťou, či dokonca stratou údajov, prípadne nedostupnosťou niektorých služieb.

Zálohovať na počítači môžeme rôzne údaje. Samozrejme odporúčame zálohovať údaje, ktoré nie sú bežne dostupné a vytvorili sme ich sami. Dokumenty, záznamy či záložky webových stránok sú príkladmi čo zálohovať. Zálohujeme predovšetkým v čase, kedy na počítači nepracujeme (kedy je záťaž najnižšia). Pravidelným zálohovaním vieme predísť strate dôležitých údajov.

7.1.3 Zásady správneho zálohovania, ako sú pravidelnosť a frekvencia zálohovania, plán zálohovania, umiestnenie dátového úložiska, kompresia dát

Frekvencia zálohovania sa môže líšiť hlavne podľa charakteru spracúvaných údajov. Napríklad bankové IS, ktoré spracúvajú údaje v reálnom čase, potrebujú mať zálohu zo všetkých údajov, ktoré sa do systému dostali. Každý údaj, ktorý sa uloží do bankového IS, sa musí okamžite uložiť aj do zálohy, inak v prípade výpadku primárneho pamäťového média nebude možné obnoviť údaje o všetkých zrealizovaných operáciách, čo by mohlo spôsobiť problémy banke aj jej klientom. Iná situácia je v prípade operačného systému a aplikačného software bankového IS, ktorý sa nemení veľmi často, len pri aktualizáciách. V tomto prípade stačia pravidelné zálohy po úspešnej aktualizácii systému alebo aplikačného software.

Podľa dôležitosti zálohovaných údajov sa mení aj to, kam umiestňujeme zálohy. Bežné zálohy sa robia väčšinou v rámci jednej budovy. Ak chceme mať dostupnú informáciu aj prípade havárie budovy (požiar, bombový útok a pod.), zabezpečíme zálohovanie mimo budovy, napríklad v inej časti mesta. Pre zabezpečenie dostupnosti informácie aj pri problémoch väčšieho rozsahu (silné zemetrasenie, vojnový konflikt a pod.) je vhodné zálohy umiestniť do iného mesta, mimo krajinu, ideálne na iný kontinent.

7.1.4 Zálohovanie údajov

Zálohovanie je vytváranie kópie potrebných údajov na iné médiá klasickým kopírovaním, alebo pomocou špecializovaného softvéru.

V prípade IS spoločnosti riešia zálohovanie väčšinou na viacerých úrovniach.

Prvou býva samotné primárne pamäťové médium, ktoré nie je jednoduchý pevný disk, ale pole diskov, kde sa každý údaj zapisuje na minimálne dva disky súčasne, čím sa eliminuje problém pri zlyhaní jedného disku. Pri takejto poruche stačí vymeniť chybný disk a software diskového poľa sa postará o obnovenie údajov na novom disku. V takomto prípade dostupnosť údajov nie je vôbec narušená.

Pri IS, pri ktorých je potrebná vysoká dostupnosť (banky, telekomunikácie, armáda a pod.), býva ďalšou úrovňou zálohy on-line kópia údajov po sieti na iné pamäťové médium, prípadne úplná záložná kópia celého IS (možno aj v inej budove). V prípade výpadku primárneho pamäťového média, či dokonca celého primárneho IS, preberie celú záťaž záložná kópia IS. Čo sa týka dostupnosti údajov, jej výpadok býva na úrovni jednotiek až desiatok sekúnd, pričom rozhodujúca je konfigurácia kontrolných algoritmov, ktoré rozhodujú o automatickom prepnutí na záložný systém.

Ďalšou úrovňou zálohovania je kópia údajov spravidla s frekvenciou raz za 24 hodín na pamäťové médium umiestnené v inej budove. Týmto sa zabezpečí dostupnosť údajov aj v prípade požiaru alebo havárie budovy, v ktorej je umiestnené primárne pamäťové médium. Obnova údajov z takejto zálohy býva náročnejšia, výpadok dostupnosti býva na úrovni až desiatok hodín.

V závislosti od hodnoty informácií sa môžu vytvárať ďalšie úrovne záloh geograficky dostatočne vzdialené, aby v prípade prírodnej katastrofy sa údaje nestratili.

V domácich podmienkach sa zvyknú robiť jednoduché kópie súborov, najmä fotografií a videí, kopírovaním do iného priečinka alebo na externé pamäťové médium, napr. USB kľúč, alebo napaľovaním na CD-R alebo DVD-R médiá. V spoločnostiach sa takéto zálohy robia už zriedka (napr. napaľovaním na optické médium pre archívne účely pri ukončení projektu).

Veľmi často sa podceňuje zálohovanie prenosných zariadení, hlavne mobilných telefónov. Zálohy týchto zariadení nemusíme robiť denne, ale s intenzitou ich používania by mala rásť frekvencia ich zálohovania. Používateľa to väčšinou obťažuje, ale veľmi to ocení v prípade straty alebo vážneho poškodenia telefónu.

7.1.5 Obnovenie údajov zo zálohy a ich overenie

V prípade potvrdenej poruchy primárneho úložiska údajov, prípadne celého IS, je potrebné obnoviť dostupnosť údajov, resp. sprevádzkovať IS, v čo najkratšom čase. Obnova údajov môže byť automatická (po výmene chybného disku v diskovom poli údaje na nový disk automaticky obnoví softvér diskového poľa), alebo ručná (po zlyhaní servera sa na nový server obnoví zo zálohy operačný systém a aplikačný softvér a následne sa obnovia údaje z poslednej zálohy).

Pri zálohách, vytvorených ako jednoduché kópie, obnova je v podstate skopírovanie súborov zo záložného priečinka alebo pamäťového média na pôvodné miesto. Pred kopírovaním by sme si mali overiť, či sú záložné súbory v poriadku.

Najmä v prípade externých záloh je potrebné overiť autenticitu a integritu zálohovaných údajov. Obnovením nesprávnych údajov môžeme napáchať viac škody než úžitku.

7.2 Bezpečné vymazanie a likvidácia

7.2.1 Rozdiel medzi vymazaním údajov a ich trvalým odstránením

V operačných systémoch pre bežných používateľov, ako sú napr. MS Windows 7/10, MAC OS X, Ubuntu, pri vymazaní alebo odstránení súboru alebo priečinka z lokálneho pamäťového média, sa tieto presunú do špeciálneho priečinka, ktorý sa v MS Windows označuje „Kôš“. Z Koša je možné súbory alebo priečinky jednoducho obnoviť na pôvodné miesto.

Ak chceme, aby súbory alebo priečinky neboli štandardne dostupné z operačného systému, môžeme ich z Koša trvalo odstrániť. Trvalé odstránenie z lokálneho pamäťového média neznamená fyzickú likvidáciu uložených údajov, ale len sprístupnenie oblastí, na ktorých boli uložené údaje odstránených súborov, pre ďalšie použitie. Týmto sa stanú súbory a priečinky nedostupné pre bežného používateľa. Pokiaľ sa tieto oblasti nepoužijú pre uloženie údajov iných súborov, ostávajú v nich uložené pôvodné údaje, a pomocou špeciálnych programov ich môžeme prečítať, prípadne aj obnoviť pôvodné súbory.

7.2.2 Prečo je potrebné trvalé odstránenie údajov z pamäťových médií a zariadení

Veľmi často dochádza k úniku informácií neopatrným zaobchádzaním s nepotrebnými pamäťovými médiami. Ak z nejakého dôvodu potrebujeme vyradiť pamäťové médium (napr. pri výmene pamäťového média za väčšie, pokazené alebo poškodené médium a pod.), mali by sme zabezpečiť, aby sa z nich nedali údaje prečítať, ani obnoviť. Veľmi často sa zabúda na vyradené zariadenia s pamäťovými médiami, ako sú počítače, notebooky, mobilné telefóny, tablety a pod. Pri neodbornej likvidácii uložených údajov ich môže skúsený špecialista pomerne jednoducho obnoviť, a tak získať aj citlivé údaje, ktoré boli predtým na nich uložené.

7.2.3 Trvalosť vymazania obsahu pri službách ako sociálne siete, blog, internetové fórum a cloud služby

Pri používaní rôznych služieb ako sociálne siete, blogy, internetové fóra a iné cloud služby si musíme uvedomiť fakt, že všetky informácie, ktoré na týchto službách zadáme už nikdy nebude možné trvale zmazať. Aj v prípade, že nahrané dáta neskôr zmažeme totiž nemôžeme mať istotu, že si ich medzitým nikto neskopíroval. Tiež je známym faktom, že niektoré sociálne siete obsah nemažú, zostáva uložený aj naďalej. Informácie o používateľoch sú takto zhromažďované a strojovo spracované pre ďalšie použitie v budúcnosti.

7.2.4 Metódy na trvalú likvidáciu údajov, napríklad: skartácia, fyzická likvidácia zariadení a médií, demagnetizácia (degaussing), používanie softvérových prostriedkov na likvidáciu údajov

Na trvalú likvidáciu údajov sa používajú rôzne postupy, ktoré sa líšia podľa typu pamäťového média, požadovaného stupňa utajenia, prípadne či sa pamäťové médium má ešte dať použiť.

Asi najznámejšia forma fyzickej likvidácie pamäťových médií je **skartácia**, kedy je médium rozdelené na množstvo malých častí. V domácich alebo kancelárskych podmienkach je použiteľná na pamäťové média ako papier, platobné karty, CD, DVD a Blu-ray médiá, diskety. Na skartáciu pevnejších médií, ako sú USB kľúče, pevné disky, mobilné telefóny, tablety a pod., sú potrebné priemyslové skartovačky, ktorými disponujú firmy špecializujúce sa na likvidáciu pamäťových médií. Tieto fyzicky zlikvidujú aj pevnejšie materiály, aké sú v rámoch mobilov, tabletov a pevných diskov, či v obaloch niektorých USB kľúčov. Čím je požadovaný vyšší stupeň utajenia (menšia pravdepodobnosť obnovenia údajov), tým menšie kúsky majú vzniknúť po skartácii. Dobré skartovačky rozdelia vložené predmety na časti do veľkosti cca 5 mm.

Demagnetizácia (degaussing) je metóda, ktorá je použiteľná na odstránenie údajov na všetkých pamäťových médiách, ktoré využívajú magnetický záznam. Údaje sú ukladané ako riadené striedanie oblastí s rôznou magnetizáciou. Úlohou demagnetizácie je nastaviť vo všetkých oblastiach buď nulovú alebo rovnakú magnetizáciu na celom záznamovom médiu (disku, páske a pod.). Poznáme dva typy demagnetizačných zariadení. Striedavé demagnetizátory vytvoria najprv silné striedavé magnetické pole, ktoré postupne slabne až na nulu, čím rozkmitajú magnetizáciu záznamového média a postupne ju znížia v celom objeme až k nule. Jednosmerné demagnetizátory vytvárajú vysoké jednosmerné magnetické pole, ktoré nastavia rovnakú magnetizáciu v celom objeme záznamového média. Po demagnetizácii sú pamäťové médiá v princípe použiteľné, ale najmä u nových pevných diskov, ktoré si ukladajú niektoré systémové informácie priamo na magnetické platne (riadiace stopy, firmware a pod.), môže byť na ich opätovné uvedenie do prevádzky potrebné použiť špeciálny softvér, prípadne aj hardvér.

Softvérové prostriedky na likvidáciu údajov využívajú mnohonásobný prepis jednotlivých oblastí na záznamovom médiu a tým úplne zlikvidujú pôvodne uložené údaje. Problémom môžu byť pamäťové médiá, u ktorých nemáme priamy prístup do jednotlivých oblastí, resp. pamäťových buniek (mobilné zariadenia ako telefóny a tablety, niektoré novšie SSD disky a pod.), u nich zostáva jedine možnosť fyzickej likvidácie zariadenia.