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

Modul 12: Bezpečnosť pri využívaní IKT

Pojmy z oblasti informačnej bezpečnosti

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

1 Pojmy z oblasti informačnej bezpečnosti

Cieľom informačnej bezpečnosti je identifikovať hrozby a riziká a na základe toho navrhovať a prijímať také opatrenia, ktoré zabezpečia minimalizáciu rizík a dopadov hrozieb pri zachovaní rozumnej miery nákladov v porovnaní s hodnotou chránených informácií a nebudú brániť oprávnenému používaniu informácií. V jednotlivých častiach si vysvetlíme dôležité pojmy používané v tejto oblasti.

1.1 Ohrozenie údajov

V úvode si je potrebné uvedomiť, že údaje sú ohrozené počas prenosu, spracovania aj uchovávania.

Hrozba je existujúca možnosť narušenia bezpečnosti. Medzi objektívne hrozby patria hrozby prírodné a fyzické, ako sú požiar, povodeň, výpadok napájania, havária a pod., spoločne označované ako vyššia moc (vis maior). K subjektívnym hrozbám radíme hrozby od osôb. Medzi neúmyselné patria chyby a omyly používateľov a programátorov, k úmyselným radíme útočníkov (hackeri, crackeri, špióni, teroristi a pod.), prípadne úmyselne zavlečené chyby programátorov - nemusí sa jednať len o osoby zvonku, ale aj zvnútra (nespokojný, pomstychtivý alebo vydieraný zamestnanec).

Riziko je pravdepodobnosť naplnenia hrozby. Riziko nie je konštantné, môže sa meniť. Napríklad riziko požiaru môžeme znížiť používaním nehorľavých materiálov, pravidelnou kontrolou elektrických rozvodov a pod. Zvýšenie hodnoty uložených informácií môže zvýšiť riziko napadnutia informačného systému (ďalej „IS“) útočníkmi.

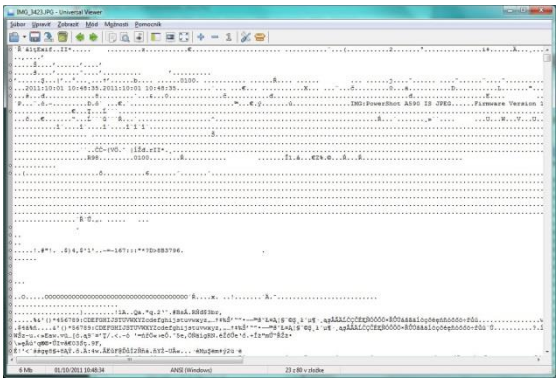
Dopady hrozby sú v podstate následky toho, čo sa stane, ak sa hrozba naplní.

1.1.1 Údaje a informácie

Tieto dva pojmy sa veľmi často zamieňajú. Každá informácia je údaj, no nie každý údaj je informácia. Uvedieme si príklad: 73.

Toto je **údaj**. Sám o sebe nám nič nepovie. Ak tento údaj vidíme na váhe, na ktorú sme sa postavili, máme **informáciu** o našej hmotnosti.

Na pamäťových médiách máme uložené **údaje**. Pri ich správnej interpretácii z nich získame **informácie**. Na ďalších dvoch obrázkoch máme ten istý súbor s **údajmi** (fotka) otvorený v textovom editore a v prehliadači obrázkov.



Obrázok 1: Fotka v textovom editore

Obrázok 2: Fotka v prehliadači obrázkov

Na obrázku (Obrázok 1) si môžeme prečítať **informáciu** kedy a na akom fotoaparáte to bolo odfotené, ale v ďalšej časti nasleduje trochu čudná zmes znakov, tieto **údaje** nám nedávajú žiadnu **informáciu**. Na obrázku (Obrázok 2) máme z rovnakých **údajov** obrazovú **informáciu**, pohľad na pekné skaly v lese.

1.1.2 Čo je to kyberzločin, hacking

Kyberzločin je akýkoľvek zločin, pri ktorom sú využité informačno-komunikačné technológie (ďalej „IKT“) ako prostriedok alebo cieľ. Využitie IKT len ako prostriedku páchania zločinu je napríklad falšovanie dokumentov - úradných listín, dokladov, bankoviek a pod. Typickým príkladom, keď IKT je len cieľom zločinu, je jej fyzické odcudzenie, či už z dôvodu jej predaja, alebo získania informácií, ktoré obsahuje (krádež IKT na predaj však nie je kyberzločinom).

Najčastejšie je IKT využívané aj ako prostriedok aj ako cieľ, napríklad pre prienik do IS sa využívajú počítače a počítačová sieť.

Ďalšími často sa vyskytujúcimi formami alebo druhmi kyberzločinu sú krádež identity a jej následné zneužitie, rozširovanie škodlivého kódu, pomocou ktorého môže útočník spôsobiť priamu škodu (napríklad zničenie údajov), alebo získať informácie pre svoju ďalšiu činnosť.

Hacker, osoba venujúca sa hackingu – počítačový špecialista a programátor s detailnými znalosťami fungovania systému; dokáže s ním výborne pracovať a upraviť ho podľa svojich potrieb. Hacker je aj ten, ktorý obíde obmedzenia operačného systému aby si nainštaloval nejaký softvér (v súčasnosti veľmi často u mobilných zariadení, napr. jailbreak v iOS alebo tzv. rootnutie v Androide). V masmédiách sa ako hackeri nesprávne označujú ľudia, ktorým ide len o zisk resp. napáchanie nejakých škôd.

Cracker, osoba venujúca sa crackingu – osoba prenikajúca do cudzích počítačov či databáz (cez sieť) bez toho, aby mala prístupové práva, s cieľom získať z toho prospech resp. urobiť škody. Cracking je aj obídenie ochrany výrobcu a spustenie plateného softvéru bez zaplatenia licenčného poplatku. Cracker môže byť hacker, alebo môže len využívať nástroje vytvorené inými osobami (hackermi) bez znalosti o fungovaní samotného systému.

Etický hacking – snaha odhaliť zraniteľnosť systému s cieľom pomôcť k ich odstráneniu. Robí sa napríklad (ale nielen) na objednávku výrobcu softvéru alebo zákazníka, ktorý si chce softvér otestovať pred jeho zakúpením. Niekedy to môže byť aj aktivita používateľov, ktorí chcú upozorniť na bezpečnostné problémy softvéru.

1.1.3 Ohrozenie údajov zo strany zamestnancov, poskytovateľov služieb ako aj zvonka pôsobiacich jednotlivcov

Okrem vyššej moci údaje ohrozujú útoky, za ktorými sú isté osoby, ktoré môžeme rozdeliť do troch skupín:

- vlastní zamestnanci firmy a klienti firmy,
- zamestnanci u poskytovateľa IKT služieb,
- externé osoby.

V prípade väčšiny úspešných útokov na IS stopy vedú k vlastným zamestnancom a zamestnancom klientov. Tí sa na útokoch podieľali buď vedome, alebo svojou nedbanlivosťou poskytli prístup do informačného systému tretím osobám.

V prípade, že IKT služby zabezpečuje externá firma (outsourcing), môžu byť potenciálnou hrozbou aj oni, keďže majú prístup k systémom zákazníkov.

Podobne aj zamestnanci firiem, ktorí spravujú počítače spoločnosti, môžu získať počas údržby počítačov prístupy k uloženým prihlasovacím údajom, prípadne inštaláciou škodlivého softvéru môžu monitorovať prácu na počítači a tak získať informácie z interných úložísk, prípadne e-mailovej komunikácie. Netreba zabúdať ani na firmy poskytujúce záručné opravy.

Ak majú zamestnanci spoločnosti možnosť pracovať z domu, môžu byť nebezpečným zdrojom informácií aj ich počítače, preto by v takom prípade ich servis mal podliehať rovnakým pravidlám ako počítače spoločnosti.

Ďalšou potenciálnou hrozbou sú poskytovatelia sieťového pripojenia najmä pri práci z domu, prípadne počas služobných ciest, ktorí môžu monitorovaním sieťovej komunikácie získať cenné informácie.

Ochrana informačných systémov spoločnosti voči externým útočníkom býva riešená najdôkladnejšie, preto útoky bez pomoci osôb z vnútra majú najmenší výskyt a vyskytujú sa hlavne tam, kde sú cenné informácie (finančné, politické, priemyselné, vojenské, ...).

1.1.4 Ohrozenie údajov z vyššej moci (vis maior)

Pod pojmom vyššia moc sú zahrnuté udalosti, ktorým nevieme zabrániť. Je to napríklad pôsobenie vody (povodne, prasknuté potrubie a pod.), požiar, zemetrasenie, neplánovaný výpadok dodávky elektrickej energie, úder blesku, porucha, havária, vojna a pod.

Pri plánovaní ochrany údajov musíme s vyššou mocou počítať a urobiť také opatrenia, aby boli prípadné škody minimálne (napr. záloha údajov na rôznych geografických miestach).

1.1.5 Ohrozenie údajov z dôvodu využívania cloud computingu

Cloud computing je na internete založený model používania počítačových technológií.

Možno ho charakterizovať aj ako poskytovanie služieb, programov a úložiska na serveroch na internete s tým, že používatelia k nim môžu pristupovať napríklad pomocou webového prehliadača alebo klienta danej aplikácie a používať prakticky odkiaľkoľvek.

Treba si uvedomiť najmä fakt, že pri používaní cloud computingu, sú dáta klientov uložené a spracovávané na počítačoch tretích strán (poskytovateľov služieb). Tieto dáta a ich bezpečnosť sú teda závislé od týchto poskytovateľov a od ich správania sa k nim. Môže dôjsť napríklad k výpadku poskytovanej služby alebo internetového pripojenia (čím sa naše dáta alebo celkovo služba stanú pre klienta nedostupnými) alebo môže dôjsť k útoku na infraštruktúru poskytovateľa (a teda aj dáta).

K **strate súkromia** pri používaní cloud computingu môže dôjsť najmä dvomi spôsobmi:

- dôjde k útoku na infraštruktúru poskytovateľa služby a k odcudzeniu dát;
- poskytovateľ zámerne hromadí informácie o osobách klientov, prípadne ich predáva ďalším stranám.

1.2 Hodnota informácie

V dnešnom svete majú informácie obrovskú cenu. Prevažná väčšina dôležitých informácií je uložená v elektronickej podobe v rôznych IS (banky, poisťovne, burzy, vládne inštitúcie, firemné IS, ...). Takéto informácie musia byť chránené pred neoprávneným prístupom a manipuláciou, pretože neoprávnená zmena napr. bankových informácií môže spôsobiť stratu alebo neoprávnené obohatenie sa, a firemné informácie v rukách konkurencie môžu viesť k vážnym obchodným stratám.

Nemenej hodnotné sú informácie o osobách, tzv. osobné údaje, pomocou ktorých môže útočník uškodiť danej osobe, alebo v pod jej menom spôsobiť škodu niekomu inému.

1.2.1 Základné charakteristiky informačnej bezpečnosti, ako sú dôvernosť, integrita a dostupnosť informácií

Dôvernosť – informácia má byť čitateľná len pre oprávnených používateľov, pre ostatných má zostať utajená.

Integrita – informácia má zostať nezmenená a prípadné zmeny majú byť zaznamenané.

Autentickosť – k informácii vieme priradiť jej autora, pôvodcu.

Dostupnosť – informácia je dostupná pre oprávnených používateľov.

V prípade IS sa dôvernosť dosahuje tým, že pri každej informácii, ktorá je v ňom uložená, je uvedené, kto ju môže meniť, pre koho má byť dostupná len na čítanie a pre ďalších

používateľov má byť nedostupná. Integrita a autentickosť informácie sú zabezpečené zaznamenávaním (logovaním) činnosti používateľov vrátane zmien každej informácie počnúc jej uložením do IS.

Pri prenášaní by informácie mali byť chránené tak, aby sa dostali len k oprávneným používateľom a nie do nepovolaných rúk (dôvernosť), a v prípade, že sa tak stane, neboli pre nich užitočné.

Pri súboroch, ktoré majú byť verejne dostupné (nie dôverné), môžeme integritu a autentickosť zabezpečiť elektronickým podpisom, pri ktorom si môžeme overiť vlastníka podpisu (u vydavateľa certifikátu použitého na podpis) a či bol dokument od podpísania zmenený.

Pre zachovanie dôvernosti môžeme súbory zašifrovať - dostane sa k nim len ten, kto ich vie dešifrovať.

Kombináciou digitálneho podpisu a šifrovania je možné dosiahnuť autentickosť, integritu, dôvernosť aj dostupnosť informácií.

Pri dôležitých informáciách potrebujeme zabezpečiť ich dostupnosť aj v prípade zlyhania pamäťového média (porucha, neoprávnený zásah, vyššia moc a pod.). Na toto je vhodné zálohovanie. Podľa dôležitosti informácií 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 mimo krajinu, ideálne na iný kontinent.

1.2.2 Ochrana osobných údajov, predchádzanie krádeži identity, ochrana pred získaním údajov podvodom

Osobnými údajmi sú údaje, na základe ktorých môžeme určiť fyzickú osobu. Sú to napríklad meno, telefónne číslo, e-mailová adresa, dátum narodenia, adresa, rodné číslo, číslo účtu a akékoľvek iné informácie o vás, ktoré vás identifikujú alebo pomocou ktorých vás možno identifikovať. Pri využívaní elektronických služieb to môžu byť prihlasovacie meno a heslo.

O **krádeži identity** hovoríme vtedy, ak sa niekto vydáva za niekoho iného. Napríklad ak sa niekto dostane k prihlasovacím údajom do vašej elektronickej pošty, môže posielať správy vo vašom mene, alebo z nej získať ďalšie osobné údaje, ako sú registrácia v rôznych IS (banky, e-shopy a pod.) a tieto zneužiť vo svoj prospech. Veľmi častá býva krádež identity na sociálnych sieťach, kde si útočník vytvorí účet inej, väčšinou verejne známej osoby (herec, spevák, politik a pod.), a začne komunikovať a prezentovať v jej mene svoje názory.

Často sa stáva, že obeť poskytne svoje osobné údaje dobrovoľne podvodníkom, ktorí sa vydávajú za dôveryhodné osoby (administrátor IS), ktoré za účelom domnelej pomoci

obeti od nej požadujú jej údaje pre vstup do IS, prípadne za účelom vyplatenia výhry poskytnúť informácie k bankovému účtu.

Základnou prevenciou je nikomu neposkytovať svoje heslá, skutoční administrátori ich nepotrebujú, pretože IS sú takto navrhnuté. Podobne pre prevod peňazí odosielateľ nepotrebuje prístup k účtu príjemcu.

1.2.3 Ochrana obchodne citlivých informácií, predchádzanie krádeži alebo zneužitiu detailov o klientovi, ochrana finančných informácií

Ak sa citlivé informácie firmy (o vývoji, obchodné, finančné, záznamy o klientoch) dostanú do nepovolaných rúk (napríklad ku konkurencii), môže to pre ňu znamenať veľa nepríjemností, napríklad stratu konkurenčnej výhody, dôvery klientov a pod.

Napríklad ak sa pred zverejnením informácie, že firma Klingacik SA so sídlom v Nemecku predala len polovicu objemu výroby v tomto roku a bude nútená prepúšťať zamestnancov, pre burzového makléra v Nemecku to môže byť signál „Pozor, nekupuj akcie tejto firmy, hrozí, že budú klesať.“ alebo „Rýchlo predajme akcie tejto firmy, asi bude klesať ich hodnota a nám hrozí strata.“.

V prípade ak má firma vo svojich informáciách o klientoch uložené aj informácie potrebné pre realizáciu finančných transakcií (napríklad pre pravidelné mesačné platby kreditnou kartou), únik týchto informácií môže priamo poškodiť klientov ak si niekto na ich účet bude nakupovať.

Osobitnou kategóriou sú štátne informácie, najmä tie, ktoré sa týkajú jeho bezpečnosti. Napríklad podrobné plány energetickej sústavy môžu pomôcť naplánovať útok na ňu tak, aby prestala plniť svoju funkciu a tak ohroziť energetickú bezpečnosť krajiny.

1.2.4 Bežná ochrana údajov/súkromia a princípy regulácie prístupu k údajom (transparentnosť, legitímne účely, proporcionalita)

Transparentnosť - tento pojem z pohľadu ochrany osobných údajov zahŕňa najmä transparentné pravidlá spracovania voči subjektu spracovania osobných údajov - teda k občanovi, aby mohol robiť kvalifikované rozhodnutia.

Legitímne účely - princíp legitimity účelu zhromažďovaných osobných údajov hovorí hlavne o nutnosti legitímnych a potrebných účelov pre zhromažďovanie osobných údajov.

Proporcionalita - pri spracovaní osobných dát je vyžadované, aby boli spracovaní iba tie dáta, ktoré sú nevyhnutné na spracovanie pre daný účel.

1.2.5 Pojmy dotknutá osoba, prevádzkovateľ/sprostredkovateľ, a princípy ochrany, regulácie prístupu k osobným údajom/súkromiu

Podľa Zákona č. 18/2018 Z. z. o ochrane osobných údajov, ktorý nahradil Zákon č. 122/2013 Z. z.) je dotknutá osoba každá fyzická osoba, ktorej sa osobné údaje týkajú.

Súhlasom dotknutej osoby akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného

potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov.

Prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov.

Prevádzkovateľ je oprávnený na základe písomnej zmluvy poveriť spracúvaním osobných údajov sprostredkovateľa.

Sprostredkovateľom každý, kto spracúva osobné údaje v mene prevádzkovateľa.

Príjemcom je každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov.

Treťou stranou je každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

Zodpovednou osobou osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa tohto zákona.

Pri spracúvaní osobných údajov je potrebné dodržiavať nasledovné zásady.

- Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby - **zásada zákonnosti**.
- Osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv dotknutej osoby - **zásada obmedzenia účelu**.
- Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú - **zásada minimalizácie osobných údajov**.
- Spracúvané osobné údaje musia byť správne a podľa potreby aktualizované; musia sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili - **zásada správnosti**.
- Osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa

osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby - **zásada minimalizácie uchovávania**.

- Osobné údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov - **zásada integrity a dôvernosti**.
- Prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať - **zásada zodpovednosti**.

1.2.6 Význam vytvárania a dodržiavania bezpečnostných zásad a politík, ktoré sa týkajú využívania IKT

Bezpečnosť v organizácii je zvyčajne riadená prostredníctvom vnútorných predpisov, ktoré sú záväzné pre všetkých zamestnancov, prípadne aj pre iné osoby (dodávatelia, zákazníci a pod.).

Základom bezpečnostnej politiky je bezpečnostný projekt a v ňom obsiahnutý bezpečnostný zámer.

Bezpečnostný projekt vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na minimalizovanie hrozieb a rizík pôsobiacich na IS z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti. Vypracúva sa v súlade so základnými pravidlami bezpečnosti IS, vydanými bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná. Obsahuje spravidla:

- Bezpečnostný zámer
- Analýzu bezpečnosti IS
- Bezpečnostné smernice

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu IS pred ohrozením jeho bezpečnosti, a ich formuláciu. Obsahuje minimálne požadované bezpečnostné opatrenia, najmä špecifikáciu technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia, vymedzenie okolia IS a jeho vzťah k možnému narušeniu bezpečnosti a súpis nepokrytých rizík.

Zákon č. 18/2018 Z. z. neukladá, aby prijaté opatrenia boli vyjadrené aj v písomnej forme. Napriek tomu sa odporúča prijať postupy pri riešení bezpečnostných incidentov

v písomnej forme za účelom, aby nimi boli oboznámení všetci zamestnanci. Okrem toho prevádzkovateľ je povinný písomne zdokumentovať každý bezpečnostný incident.

Analýza bezpečnosti IS je podrobný rozbor stavu bezpečnosti IS, ktorá obsahuje kvalitatívnu analýzu rizík, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva IS spôsobilé narušiť jeho bezpečnosť alebo funkčnosť. Výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov, s uvedením rozsahu možného rizika, návrhov opatrení, ktoré odstránia alebo minimalizujú vplyv rizík, súpis nepokrytých rizík, a použitie bezpečnostných štandardov a určenie iných metód a prostriedkov ochrany osobných údajov. Súčasťou analýzy bezpečnosti IS je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardmi, metódami a prostriedkami.

Bezpečnostné smernice upresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovaného IS a obsahujú popis technických, organizačných a personálnych opatrení vymedzených v bezpečnostnom projekte a ich využitie v konkrétnych podmienkach, rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k IS, rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov, spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému, postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou.

Nový Zákon č. 18/2018 Z. z. upúšťa od povinnosti vypracovávania bezpečnostného projektu a bezpečnostných smerníc. Okrem toho nový zákon neukladá povinnosť viesť evidenciu informačného systému a povinnosť oznamovať informačné systémy Úradu na ochranu osobných údajov SR. Namiesto toho sa zavádza **povinnosť viesť záznam o spracovateľských činnostiach**. Záznam sa vedie v listinnej podobe alebo elektronickej podobe a musí obsahovať:

- identifikačné údaje a kontaktné údaje prevádzkovateľa, spoločného prevádzkovateľa, zástupcu prevádzkovateľa, ak bol poverený a zodpovednej osoby,
- účel spracúvania osobných údajov,
- opis kategórií dotknutých osôb a kategórií osobných údajov,
- kategórie príjemcov vrátane príjemcu v tretej krajine alebo medzinárodnej organizácií,
- označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos,

- predpokladané lehoty na vymazanie rôznych kategórií osobných údajov,
- všeobecný opis technických a organizačných bezpečnostných opatrení.

Vzor záznamu o spracovateľských činnostiach je zverejnený na webovom sídle Úradu na ochranu osobných údajov SR.

1.3 Osobná bezpečnosť

Osobná bezpečnosť v elektronickom svete zahŕňa podobné pravidlá ako v reálnom svete. Chránime si informácie o svojej osobe a poskytujeme ich len dôveryhodným osobám resp. inštitúciám. A tak, ako v hoteli správcovi budovy nedávame svoje kľúče od izby, pretože má vlastné resp. univerzálny, tak ani administrátorovi IS, kde máme svoj účet (e-mail, banka a pod.), nepotrebujeme dať svoje prihlasovacie údaje. V tejto časti si popíšeme aké hrozby číhajú na našu (nielen) elektronickú identitu.

1.3.1 Sociálne inžinierstvo a jeho následky, ako sú zhromažďovanie informácií, podvodné konanie, neoprávnený prístup k počítačovým systémom

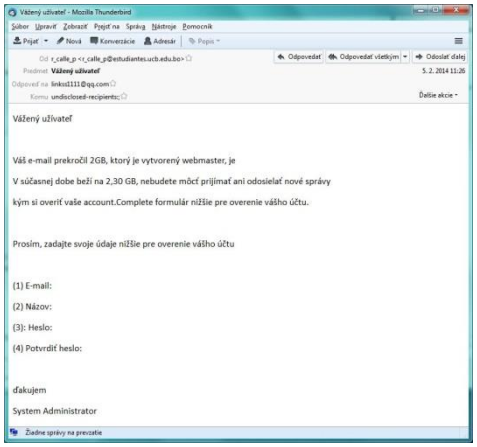
Sociálne inžinierstvo je spôsob získavania dôverných informácií využívajúci manipuláciu osôb za účelom vykonania určitej akcie (napríklad spustenia nejakého súboru) alebo získania určitých informácií. Môže prebiehať osobne, prostredníctvom komunikačného prostriedku (telefón, e-mail, ...) alebo prostredníctvom úpravy prostredia (napríklad zanechanie média na dostupnom mieste). Obrana voči všetkým formám sociálneho inžinierstva je takmer nemožná.

So sociálnym inžinierstvom sa v našich životoch stretávame dennodenne, či už je to v mestskej hromadnej doprave, v práci alebo pri surfovaní na webe. Sociálni inžinieri útočia na naše najcitlivejšie miesta a snažia sa získať si našu dôveru alebo súcit. Určite ste už niekoľko krát videli ľudí bez nôh ako žobrú o pár centov na jedlo (často krát sa však stáva, že majú len nohy zložené pod sebou, aby ich nebolo vidno) a vy ste im tých pár centov dali, pretože vám ich bolo ľúto. Súcit a ľútosť patria medzi vlastnosti ľudí, ktoré dokážu sociálni inžinieri zneužiť a dostať sa tak k hmotným (napr. spomínané centy) ale i nehmotným veciam (prístupové kódy, citlivé osobné údaje atď.).

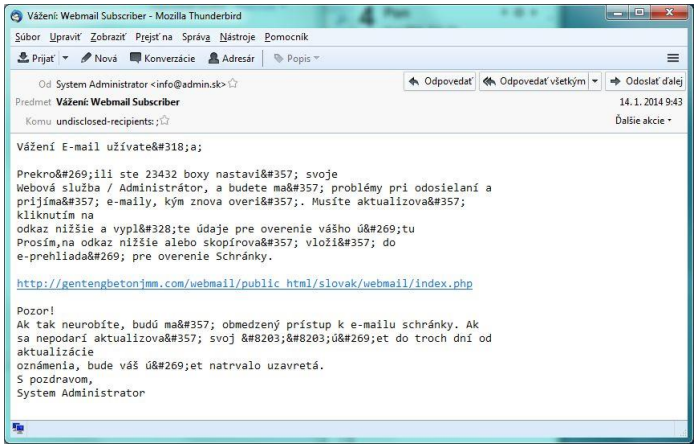
Sociálneho inžiniera môžeme definovať ako človeka, ktorý využíva rôzne manipulačné techniky voči ľudom a snaží sa tak získať prístup k IS, citlivým údajom a pod. V dobe, kedy je Internet každodennou súčasťou života, ľudia sami uľahčujú prácu sociálnych inžinierov. Internet poskytuje ľudom falošný pocit anonymity, nevystopovateľnosti. Strácame úctu k súkromiu iných a zabúdame chrániť svoje vlastné. Dobrovoľne zverejňujeme osobné (často intímne) informácie na rôznych sociálnych sieťach bez toho, aby sme sa zamysleli, čo nám toto počínanie môže priniesť v budúcnosti. To čo dnes uverejníte na sociálnej sieti môže ktokoľvek nájsť a zneužiť aj o 10 rokov (napríklad „neslušné“ fotky z mladosti na vydieranie v zrelom veku).

1.3.2 Metódy sociálneho inžinierstva, ako sú telefonáty vrátane napodobenín automatických telefonických hlások, podvodné získavanie prístupových údajov (phishing), odpozorovanie displeja (shoulder surfing)

Phishing (z anglického password fishing – doslova rybolov hesiel) je činnosť, pri ktorej sa útočník snaží podvodným spôsobom vylákať od používateľov prístupové údaje (napr. prihlasovacie mená a heslá k e-mailovému účtu). Často phishing prebieha tak, že sa rozposielajú e-maily, ktorými „administrátor“ oznamuje používateľom problémy s účtom alebo potrebu jeho overenie a tak láka heslá priamo (Obrázok 3), alebo ponúkne odkaz na falošnú stránku (Obrázok 4).

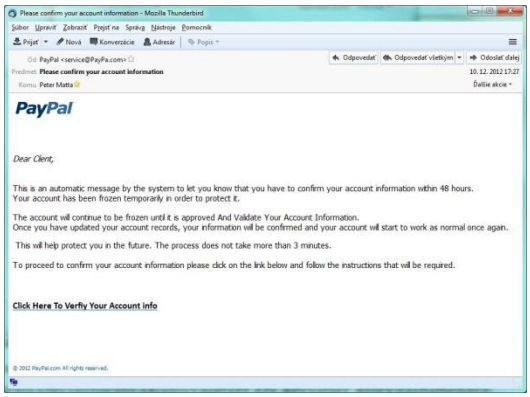


Obrázok 3: Vyžiadanie mena a hesla

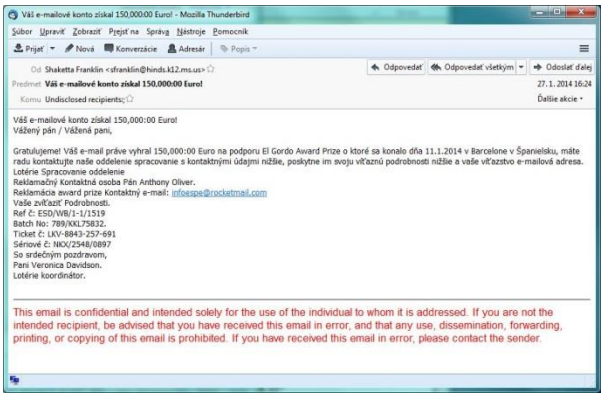


Obrázok 4: Odkaz na falošnú stránku

Ďalšími typmi podvodných e-mailov (vyzerajúce ako by boli odoslané z oficiálnej adresy napr. PayPa.com namiesto paypal.com) sú tie, ktoré požadujú od Vás prihlásenie do Vášho účtu na portáli finančných služieb (v tomto prípade PayPa.com (Obrázok 5) s reálnymi prihlasovacími údajmi, alebo Vám oznamujú výhru (Obrázok 6) a na jej prevzatie máte poskytnúť svoje údaje alebo najprv skontaktovať kanceláriu lotérie, ktorá v ďalšej komunikácii bude od Vás požadovať citlivé osobné a bankové údaje, prípadne vopred zaplatiť daň z výhry.



Obrázok 5: Správa od služby PayPa



Obrázok 6: Správa oznamujúca výhru

Najlepšia ochrana proti phishingu je nedôverovať e-mailom, ktoré chcú vylákať citlivé údaje, hlavne heslá. Skutočný administrátor nepotrebuje vedieť Vaše heslo aby vedel

pracovať s Vašim kontom. Ďalším stupňom ochrany je používanie rôznych prihlasovacích údajov pre rôzne účely.

Vishing (= voice phishing) je podobne ako phishing podvodné získavanie prihlasovacích údajov, ale v tomto prípade pomocou falošnej hlasovej služby, napríklad bankovej.

Shoulder surfing (= pozeranie ponad plece) je metóda odpozerania prihlasovacích údajov. Pôvodne útočník pri tom stál za používateľom a sledoval prihlasovacie údaje ponad plece napadnutej osoby. V súčasnosti sa využívajú rafinovanejšie metódy. Útočník navodí situáciu, kedy obeť použije svoje prihlasovacie údaje (prihlásenie do sociálnej siete, e-mailového účtu, internetbankingu a pod.), a tie „odsleduje“ buď klasicky pozeraním ponad plece, alebo pomocou elektronických prostriedkov ako sú webovej kamery, miniatúrne kamery a pod.

1.3.3 Krádež identity a jej osobné, finančné, obchodné a právne dôsledky

S krádežou identity sa stretávame od nepamäti, v súčasnosti sa zmenila len jej podoba. Niekedy sa identita osoby potvrdzovala zovňajškom (najmä odev, šperky, účes a pod.) alebo listinami (potvrdenie o pôvode, rodný list, neskôr preukazy), v dnešnej dobe by takým potvrdením identity mohlo byť použitie uniformy, prípadne služobných odznakov, rôznych preukazov a pod. Na to, aby sa niekto vydával za inú osobu stačí dôkladne napodobniť jej zovňajšok (napr. použiť uniformu), použiť jej listiny (napr. pas, občiansky preukaz, splnomocnenie), a tak v jej mene vykonať aj právne úkony a tým získať pre seba nejaký prospech, poškodiť dobré meno dotknutej osoby, alebo len utajiť svoju identitu.

Okrem fyzickej, osobnej identity máme v súčasnosti aj svoju elektronickú identitu v počítačovom svete, napr. účet na sociálnej sieti, e-mailové konto, kontá v rôznych IS. Krádež identity sa môže udiať dvoma spôsobmi:

1. pri registrácii, napr. na sociálnej sieti, zadaním falošných údajov,
2. po zaregistrovaní neoprávneným získaním prihlasovacích údajov.

Prvý spôsob krádeže identity sa týka väčšinou známych osobností, ako sú speváci, herci či politici. Útočník si zaregistruje zatiaľ nepoužité konto na meno známej osoby (najčastejšie na sociálnej sieti), pridá si do svojho profilu niekoľko informácií, ktoré nájde na internete, a začne komunikovať v jej mene. Cieľom môže byť „užiť si slávu“, zdiskreditovať dotknutú osobu publikovaním nevhodných informácií v jej mene, prípadne obohatiť sa na jej účet (falošná charitatívna zbierka, ktorú zorganizuje známa osoba, ale peniaze idú na účet útočníka).

Druhý spôsob je väčšinou náročnejší, ale tak sa môže útočník dostať aj napr. k existujúcemu bankovému účtu alebo do IS firmy alebo organizácie a tým spôsobiť rozsiahle škody.

Dôsledky krádeže identity môžu byť rôzne.

Osobné – útočník môže zdiskreditovať dotknutú osobu (napr. publikovaním nevhodných informácií) v jej okolí (rodina, pracovný kolektív) či v širokej verejnosti.

Finančné – v prípade získania prístupu do bankového účtu sú možné dôsledky zjavné, ale nemalé problémy môže spôsobiť úverová zmluva uzavretá v mene dotknutej osoby, ktorá môže okrem priamej finančnej ujmy zdiskreditovať túto osobu a sťažiť jej získanie úveru v budúcnosti.

Obchodné – získaním prístupu do IS dodávateľa môže útočník urobiť objednávky v mene dotknutej osoby a tým poškodiť jej meno voči obchodným partnerom, alebo pri oslovovaní klientov zdiskreditovať dotknutú osobu, prípadne jej firmu, v očiach zákazníkov a tým spôsobiť ich odliv ku konkurencii.

Právne – sa môžu pridružiť ku všetkým predchádzajúcim dôsledkom (osobné, finančné i obchodné), napr. ak sú porušené zmluvné záväzky, prípadne poškodená iná osoba alebo spoločnosť zverejnením nepravdivých informácií.

Osobitnou kapitolou je ak sa ukradnutá identita použije na spáchanie trestného činu. Dotknutá osoba musí dokázať, že tento čin nespáchala, keďže boli použité jej prihlasovacie údaje.

1.3.4 Metódy krádeže identity, ako sú information diving, skimming, pretexting

Information diving (vyhrabávanie informácií) je v podstate vyhľadávanie informácií v odpade, resp. v odpadkoch. Klasicky sa vyhľadávajú vyhodené dokumenty s citlivými informáciami, napr. výpisy z banky, bločky, faktúry, listy, zdravotné záznamy a pod. V súčasnosti je veľký záujem o vyhodené pamäťové médiá, ktoré málokedy sú dostatočne dobre vymazané alebo inak poškodené, a trochu skúsenejší útočník môže obnoviť údaje na nich uložené a tým prípadne získať citlivé informácie, ako sú prihlasovacie údaje a pod.

Skimming je neoprávnené kopírovanie údajov, typicky z platobných kariet. Väčšinou sa to deje pri bankomatoch, kedy pridaná nenápadná čítacia hlava prečíta informácie z magnetického prúžku karty a uloží ich do pripojenej pamäte, prípadne ich odošle do riadiaceho zariadenia. Zároveň malá kamera sníma klávesnicu bankomatu a tak útočník získa aj PIN.

V súčasnosti sa rozširuje používanie bezkontaktných platobných kariet. Ich slabinou je možnosť bezkontaktne prečítať údaje z nich.

Pretexting je vmanipulovanie dotknutej osoby do pripraveného scenára za účelom získania citlivých údajov. Útočník sa zväčša vydáva za nejakú autoritu (pracovník banky, správca e-mailového servera), ktorý volá (alebo posiela e-mail) v urgentnej záležitosti (zablokovanie konta a pod.) a pre odstránenie problému potrebuje prihlasovacie údaje.

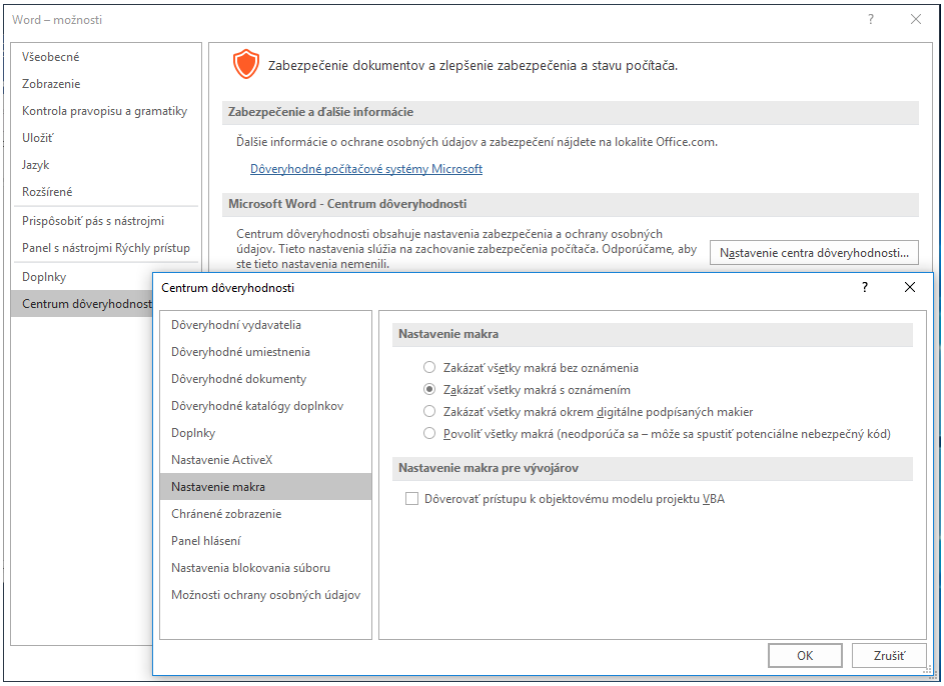
1.4 Bezpečnosť súborov

Bezpečnosť súborov v tejto kapitole bude rozobratá z dvoch uhlov. Prvý je spojený s potenciálnym nebezpečenstvom, ktoré môže ukrývať dokument kancelárskeho balíka (ktorý na prvý pohľad nie je programom). Sú to tzv. makrá, ktoré sa hojne využívajú v dokumentoch kancelárskeho balíka MS Office. Druhý je spojený s bezpečnosťou uloženia informácií v súbore.

1.4.1 Bezpečnostné dôsledky spojené s povolením / zakázaním makier.

Makrá automatizujú často používané úlohy a šetria čas strávený nad klávesnicou a myšou. Spájame ich hlavne s používaním aplikácií kancelárskeho balíka. Tie jednoduchšie sú v podstate záznamom toho, kam a ako kliknúť myškou, prípadne čo stlačiť na klávesnici aby sme vykonali napr. nejaké zložitejšie nastavenie. Niektoré makrá však predstavujú potenciálne riziko zabezpečenia - používatelia so zákernými úmyslami môžu do dokumentu zahrnúť deštruktívne makro, ktoré môže vo vašom počítači spustiť neželanú akciu.

Keďže sa po otvorení súboru v MS Office môžu makrá spustiť automaticky, máme možnosť nastaviť toto správanie. V programe (v našom prípade je to napr. MS Word) prejdeme na záložku "Súbor", vyberieme vľavo položku "Možnosti". V okne "Možnosti" vyberieme vľavo "Centrum dôveryhodnosti" a klikneme na tlačidlo "Nastavenie centra dôveryhodnosti".



Obrázok 7: Centrum dôveryhodnosti – nastavenie makra

Tu je možné nastaviť jednu zo 4 možností (Obrázok 7):

1. Zakázať všetky makrá bez oznámenia - všetky makrá a upozornenia zabezpečenia týkajúce sa makier sú zakázané.

2. Zakázať všetky makrá s oznámením - makrá sú zakázané, ale v prípade prítomnosti makra sa zobrazí upozornenie. Makrá potom môžete povoliť v závislosti od konkrétnej situácie.
3. Zakázať všetky makrá okrem digitálne podpísaných makier - makrá sú zakázané, ak je však makro digitálne podpísané, môže sa spustiť, ak je vydavateľ zaradený medzi dôveryhodných vydavateľov. Ak tam nie je zaradený, zobrazí sa upozornenie a vy môžete povoliť podpísané makro a zaradiť vydavateľa medzi dôveryhodných vydavateľov.
4. Povoliť všetky makrá (neodporúča sa, môže sa spustiť potenciálne nebezpečný kód) - povolí sa spustenie všetkých makier.

Ak nechceme vôbec spúšťať makrá, vyberieme prvú možnosť. Vtedy nemusia byť dostupné niektoré funkcionality. Ak je možné, že niekedy budeme potrebovať spustiť makro, vyberieme si druhú, prípadne tretiu možnosť. Zostáva na našom uvážení ktoré makro spustíme, prípadne či vydavateľa pridáme do zoznamu dôveryhodných vydavateľov. Poslednú možnosť vyberáme len v prípade, že pracujeme výhradne s vlastnými dokumentmi obsahujúcimi makrá.

1.4.2 Výhody a obmedzenia pri šifrovaní súborov

Základnou výhodou šifrovania súborov je dôvernosť uložených informácií. Bez znalosti dešifrovacieho kľúča (hesla) sú informácie v zašifrovanom súbore nedostupné.

Z toho plynie niekoľko nevýhod. V prípade zabudnutia dešifrovacieho kľúča stratíme všetky informácie. Zašifrované dáta nie je možné kontrolovať antivírusovým programom, preto ak je táto kontrola povinná pre prílohy e-mailu, nemusí sa nám podariť úspešne odoslať správu so zašifrovanou prílohou.

1.4.3 Šifrovanie

Údaje môžu byť zabezpečené šifrovaním. Zašifrované môžu byť jednotlivé súbory alebo aj celé pamäťové médiá. Poznáme šifrovanie dvojakého typu - symetrické a asymetrické. Nižšie si rozpíšeme základné princípy týchto typov šifrovania, ktoré sú nevyhnutné na pochopenie a správne používanie šifrovania.

Symetrické šifrovanie je typ šifrovania, pri ktorom sa používa rovnaký kľúč (heslo) na šifrovanie aj dešifrovanie, teda utajenie kľúča je pri tomto type šifrovania zásadné. Problémom tohto šifrovania pri výmene dát je to, že je nutné aby daný kľúč poznali obe strany, čo je v praxi často ťažko dosiahnuteľné bez rizika vyzradenia kľúča tretej strane, a teda rizika ohrozenia dôvernosti prenášaných dát. Symetrické šifrovanie sa však bez problémov môže použiť na iné účely, ktorých cieľom nie je výmena dát.

Spomínaný problém symetrickej šifry rieši **asymetrické šifrovanie**. Pri tomto type šifrovania sa využíva tzv. kľúčový pár. Ide o dva unikátne kľúče (súkromný a verejný), ktoré generuje špecializovaný softvér. Jeden z týchto kľúčov (zvyčajne verejný) sa použije na šifrovanie dát, pričom takto zašifrované dáta je možné dešifrovať výlučne

súkromným kľúčom z daného kľúčového páru (nie je možné použiť súkromný kľúč z iného páru).

Ideálne bude ukázať si rozdiel v symetrickom a asymetrickom šifrovaní na hypotetickom príklade. Predstavme si situáciu, kedy chcú spolu komunikovať dve osoby (Janko a Marienka), ale zároveň chcú obsah komunikácie utajiť pred treťou osobou (ježibaba). Keby použili symetrické šifrovanie, musí sa Janko s Marienkou dohodnúť na šifrovacom kľúči tak, aby sa o tomto kľúči nedozvedela ježibaba. Vždy však hrozí riziko, že sa ježibaba daný kľúč dozvie (odpočúva ich súkromný rozhovor alebo telefonát, odchytí kľúč posielaný v maily po sieti a podobne) - toto riziko možno znížiť pri hypotetickej situácií na prijateľné, ale v praxi je to ťažké dosiahnuť (obzvlášť ak Janko s Marienkou nemajú možnosť dohodnúť sa na kľúči osobne). Janko a Marienka však použijú asymetrické šifrovanie. Každý z nich si na svojom počítači vygeneruje svoj vlastný kľúčový pár a potom si navzájom vymenia verejné kľúče. Janko bude teda mať svoj súkromný kľúč a Marienkin verejný kľúč, zatiaľ čo Marienka bude mať svoj súkromný kľúč a Jankov verejný kľúč. Keď bude Janko chcieť poslať nejaké dáta Marienke, zašifruje ich Marienkiným verejným kľúčom - tieto bude možné dešifrovať iba Marienkiným súkromným kľúčom (ktorý má iba Marienka). A opačne - ak bude chcieť Marienka poslať dáta Jankovi, zašifruje ich Jankovým verejným kľúčom - bude ich teda možné dešifrovať iba Jankovým súkromným kľúčom (ktorý má iba Janko). Všimnite si hlavne fakt, že ak by ježibaba v procese výmeny verejných kľúčov odchytila niektorý (alebo oba) verejné kľúče, nebude môcť odpočúvať Jankovu a Marienkinu komunikáciu, pretože sa dáta dešifrujú pomocou súkromných kľúčov, ktoré neopustia počas celého procesu počítače Janka a Marienky a teda ich nie je možné „odpočuť“ (resp. odchytiť).

Dôležitá však je, aby sa obe strany (Janko a Marienka) presvedčili, že pri výmene verejných kľúčov skutočne obdŕžali verejný kľúč druhej strany. Mohlo by sa totiž stať, že tretia strana (ježibaba) odchytí Jankov verejný kľúč a Marienke podvrhne namiesto Jankovho verejného kľúča svoj vlastný a Marienka by tak v nevedomosti šifrovala ježibabiným verejným kľúčom - ježibaba by potom dáta dešifrovala svojím súkromným kľúčom a opätovne ich šifrovala Jankovým verejným - Janko by tak Marienkine dáta dešifroval svojím súkromným kľúčom a nikto (okrem ježibaby samozrejme) by netušil, že dochádza k odpočúvaniu šifrovanej komunikácie (pretože u ježibaby dochádza k dešifrovaniu). Overiť autentickosť verejného kľúča je možné pomocou **certifikačnej autority**, ktorá overí totožnosť vydavateľa verejného kľúča a vystaví na daný verejný kľúč digitálny podpis. Tento podpis potom potvrdzuje pravdivosť údajov uvedených vo verejnom kľúči - a teda, že osoba uvedená vo verejnom kľúči tento kľúč aj skutočne vydala (a je teda držiteľkou príslušného súkromného kľúča). Digitálne podpísaný verejný kľúč sa nazýva pojmom digitálny certifikát. Na základe princípu prenosu dôvery teda možno dôverovať takémuto certifikátu (ak dôverujeme certifikačnej autorite).

Ďalšou dôležitou skutočnosťou je nutnosť poriadneho **zabezpečenia koncových staníc** - teda počítačov Janka a Marienky. Ak by sme napríklad generovali a uskladňovali kľúčový pár na nedôveryhodnom počítači (na ktorý napríklad úspešne zaútočila tretia

strana - ježibaba), môže ľahko dôjsť k úniku súkromného kľúča a tým pádom k ohrozeniu dôvernosti prenášaných dát. Podmienka zabezpečenia a dôveryhodnosti koncových staníc však platí tak pri asymetrickom aj symetrickom šifrovaní.

Poslednou (logickou) nutnosťou pri asymetrickom šifrovaní je nutnosť generovať kľúčový pár sám. Nie je možné poveriť vygenerovaním páru pre vlastné použitie inú osobu ako seba samého - s Marienkiným súkromným kľúčom by nemal totiž manipulovať nikto iný okrem Marienky. Ak by Marienka poverila niekoho iného vygenerovaním kľúča, bolo by to ako keby požiadala niekoho iného, aby vymyslel pre ňu heslo (napríklad pre prístup do internetového bankovníctva) - dotyčný by potom samozrejme mal k Marienkinmu bankovému účtu tiež prístup.

1.4.4 Nastavenie hesla pre súbory, ako sú dokumenty, komprimované súbory, výpočtové tabuľky

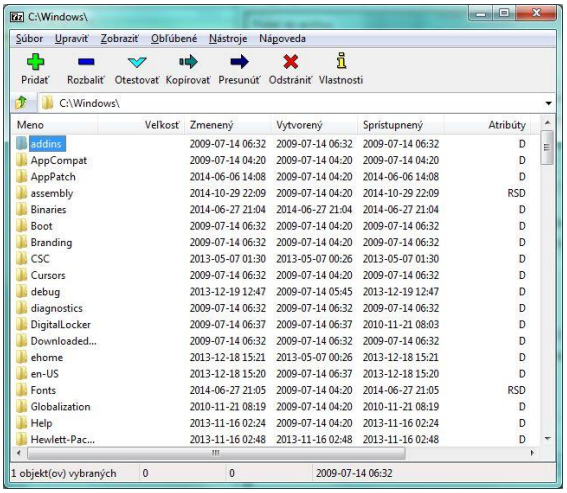
Prístup k informáciám uloženým v súboroch môžeme chrániť ich šifrovaním. Bežne môžeme súbory vytvárané v MS Office ukladať šifrované. Všetky súbory môžeme šifrovať aj bežnými programami pre archiváciu

V MS Office vieme nastaviť ochranu heslom v programoch Microsoft Access, Excel, PowerPoint a Word, pričom v každom máme trochu iné možnosti nastavenia. V každom z programov prejdeme na záložku "Súbor" a vyberieme vľavo položku "Informácie", kde máme tlačidlo "Zabezpečiť dokument".

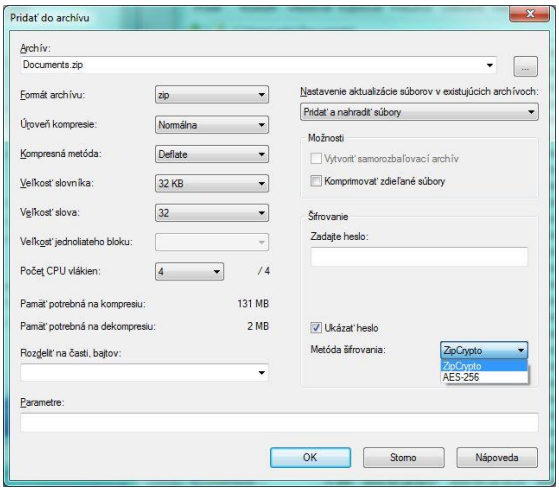
Základným zabezpečením spoločným pre všetky je zašifrovať dokument heslom. V závislosti od konkrétneho programu potom máme možnosť zablokovať dokument (resp. jeho časť) proti zmenám.

Šifrovanie archívov si ukážeme v programe 7-zip. Spustíme program 7-zip File Manager (Obrázok 8), vyberieme si v ňom súbory a/alebo priečinky, ktoré chceme vložiť do archívu a klikneme na ikonu "zelené plus" vľavo hore. Otvorí sa nám okno Pridať do archívu (Obrázok 9), v ktorom si zvolíme typ archívu a ďalšie možnosti.

V strede pravej časti okna máme okienko pre heslo.



Obrázok 8: 7-zip File Manager



Obrázok 9: 7-zip okno Pridať do archívu

Ak chceme archív zašifrovať, musíme zadať heslo. Pozor, nie každý typ archívu podporuje šifrovanie. Je možné tiež zvoliť metódu šifrovania (kvôli kompatibilite sa odporúča nechať prednastavenú metódu pre daný typ archívu).

Pri prezeraní zašifrovaného archívu si bez hesla vieme pozrieť názvy súborov a priečinkov, rozbaliť môžeme šifrovaný archív až po zadaní hesla. Toto správanie je možné zmeniť pri vytváraní archívu položkou "Zašifrovať mená súborov".