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

Modul 12:

Bezpečnosť pri využívaní IKT

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

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.

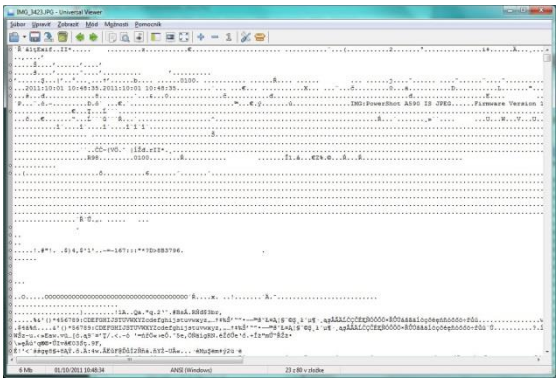
Dopady hrozby sú v podstate následky toho, čo sa stane, ak sa hrozba naplní.

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

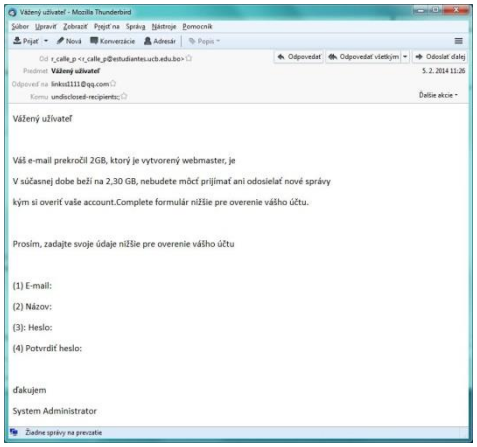
Sociálne inžinierstvo je spôsob získavania dôverných informácií využívajúci manipuláciu osôb za účelom vykonania určitej akcie (napríklad spustenia nejakého súboru) alebo získania určitých informácií. Môže prebiehať osobne, prostredníctvom komunikačného prostriedku (telefón, e-mail, ...) alebo prostredníctvom 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.).

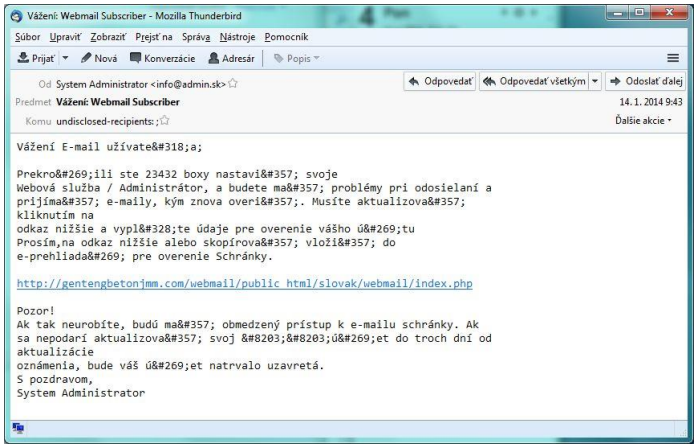
Sociálneho inžiniera môžeme definovať ako človeka, ktorý využíva rôzne manipulačné techniky voči ľudom a snaží sa tak získať prístup k IS, citlivým údajom a pod. V dobe, kedy je Internet každodennou súčasťou života, ľudia sami uľahčujú prácu sociálnych inžinierov. Internet poskytuje ľudom falošný pocit 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).

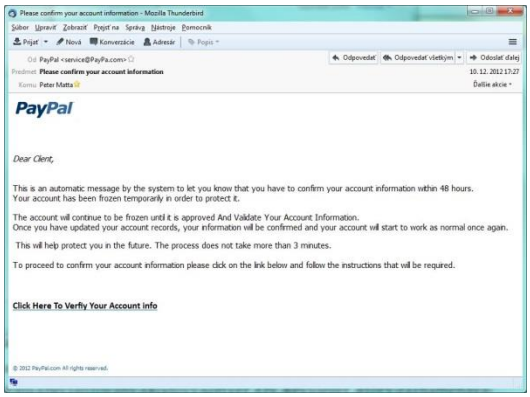


Obrázok 3: Vyžiadanie mena a hesla

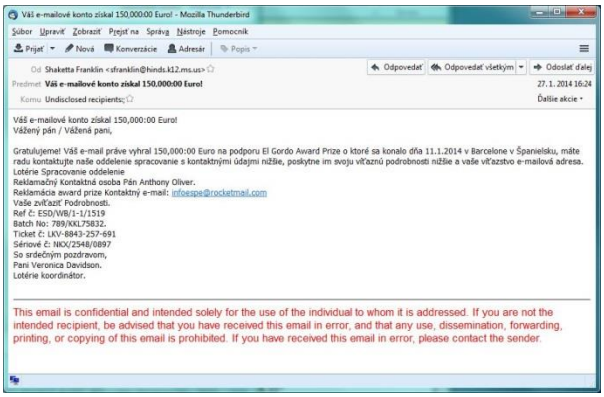


Obrázok 4: Odkaz na falošnú stránku

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.

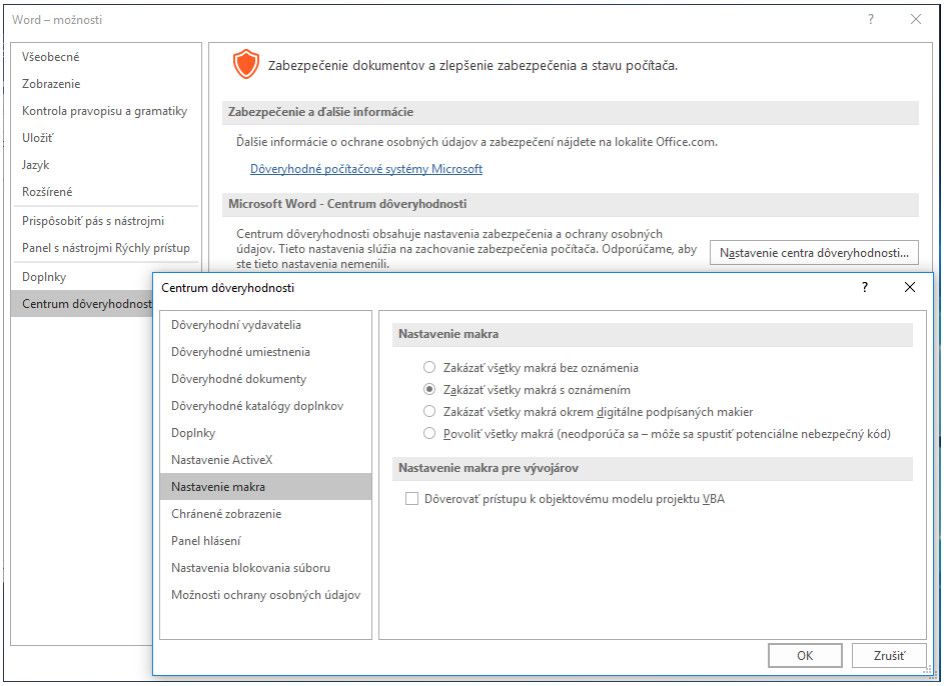
1.4 Bezpečnosť súborov

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

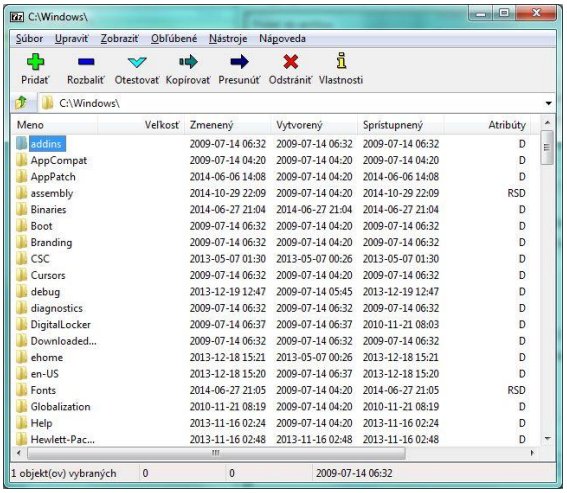
Prístup k informáciám uloženým v súboroch môžeme chrániť ich šifrovaním. Bežne môžeme súbory vytvárané v MS Office ukladať šifrované. Všetky súbory môžeme šifrovať aj bežnými programami pre archiváciu

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".

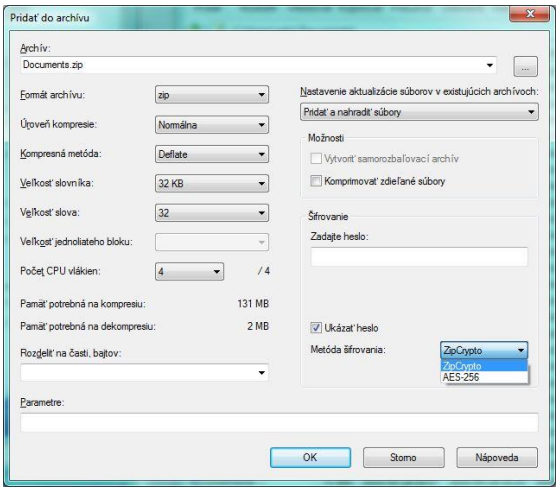
Základným zabezpečením spoločným pre všetky je zašifrovať dokument heslom. V závislosti od konkrétneho programu potom máme možnosť zablokovať dokument (resp. jeho časť) proti zmenám.

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".

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

Modul 12: Bezpečnosť pri využívaní IKT

Škodlivý softvér (malware)

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

2 Škodlivý softvér (malware)

2.1 Typy a metodiky

2.1.1 Čo je škodlivý softvér (malware), rôzne spôsoby skrývania sa škodlivého softvéru (trójsky kôň, rootkit, backdoor)

Malware (z anglického malicious software - škodlivý softvér) je všeobecné označenie pre škodlivý softvéru akéhokoľvek typu, ktoré väčšinou bežia na počítači bez vedomia (a súhlasu) majiteľa počítača. Patria sem napr. vírusy, červy, trójske kone, spyware, adware, ransomware, keylogger, backdoor, rootkit, dialer, spammer. Majú rôzne funkcie, spôsoby šírenia a skrývania sa - malware využíva rôzne spôsoby maskovania aby nebol predčasne odhalený a mohol vykonať svoju úlohu.

Trójsky kôň je škodlivý softvér, ktorý sa maskuje za užitočný. Nerozmnožuje sa. Väčšinou si ho používateľ stiahne alebo nainštaluje dobrovoľne ako užitočný program. Počas jeho používania program okrem užitočných vecí začne vykonávať aj iné, škodlivé činnosti.

Rootkit je sada aplikácií, ktoré maskujú prítomnosť malwaru v počítači. Rootkit upravuje operačný systém (skrýva adresáre, API volania, procesy, sieťové spojenia alebo systémové služby) tak, aby prítomnosť malwaru nebolo možné odhaliť bežnými prostriedkami.

Backdoor (z angličtiny zadné vrátka) je v informatike názov metódy, ktorá umožňuje obísť štandardnú autentifikáciu, ktorá bráni používateľovi neoprávnene využívať počítačový systém. Backdoor je väčšinou zámerne implementovaná funkcia programátorom systému. Môže byť využívaný na legitímnu činnosť (napr. pre servisný účel), ale veľmi často býva zneužitý útočníkmi (a malwarom) na vykonávanie činností, na ktoré nemajú v systéme oprávnenie.

2.1.2 Nákazlivý malware (vírusy, červy)

Vírus je časť kódu, ktorý nefunguje samostatne, ale pripája sa k iným programom a rozmnožuje sa do ďalších programov. Patria tu aj škodlivé makrá v dokumentoch.

Červ je samostatný program, ktorý sa rozširuje rôznymi komunikačnými kanálmi (napr. cez backdoor alebo cez e-maily) do ďalších počítačov.

2.1.3 Formy odcudzenia údajov, typy škodlivého softvéru zameraného na dosiahnutie priameho zisku (adware, ransomware, spyware, botnet, keylogger, dialler)

Adware (z anglického advertising-supported software – reklamou podporovaný softvér) program, ktorý zobrazuje nevyžiadanú reklamu. Väčšinou nie sú priamo nebezpečné, bývajú súčasťou nejakej bezplatne použiteľnej aplikácie a prinášajú takto autorovi aplikácie zisk.

Ransomware (z anglického ransom software – softvér na výkupné) zneprístupní informácie na napadnutom počítači (často ich zašifrovaním) a od používateľa požaduje zaplatenie výkupného za opätovné sprístupnenie (dešifrovanie) informácií.

Spyware z anglického spy software - špionážny softvér) kradne a odosiela rôzne (aj citlivé) informácie z napadnutého počítača útočníkovi.

Botnet (z anglického robots network – sieť robotov) je sieť počítačov infikovaných malwarom, ktorý je riadený z nejakého centra. Takto infikovaný počítač bez vedomia používateľa vykonáva rôzne koordinované činnosti, napr. rozosiela nevyžiadanú poštu alebo realizuje útok na niektoré služby s cieľom vyradiť ju s činnosti. Útočník sám nemusí využívať botnet, môže prístup k nemu predávať iným záujemcom za účelom zisku.

Keylogger (z anglického keystroke logger – zaznamenávač stlačení kláves) je špeciálny typ spyware, ktorý sleduje a ukladá (odosiela) stláčanie jednotlivých kláves - dá sa takto použiť na odchytenie hesla.

Dialer (z anglického dialer – "vytáčač") program, ktorý vytáča audiotextové číslo cez modem alebo softvér na telefonovanie, nebezpečné môžu byť nové klony na mobily.

2.2 Ochrana

2.2.1 Princípy fungovania antivírusového softvéru a jeho obmedzenia

Na ochrane počítača proti malware sa podieľajú tri základné komponenty.

Prvou je samotný operačný systém a jeho nastavenia pre používateľov, ktorý môže eliminovať väčšinu malware. Napr. ak používateľ nemá administrátorské práva, program, ktorý spustí, nemôže zapisovať do oblastí, kde je uložený operačný systém. Dôležitá je pravidelná aktualizácia operačného systému (a aplikačného softvéru), ktorou sa odstraňujú priebežne objavované bezpečnostné diery.

Druhou je samotný používateľ, ktorý by sa mal správať obozretne a neotvárať súbory a nespúšťať programy z pochybných zdrojov.

Treťou je antivírusový softvér, ktorý má úlohu odhaliť a zneškodniť malware, ktorý neeliminoval operačný systém a omylom alebo úmyselne ho aktivoval používateľ. Treba si uvedomiť, že antivírus už z princípu nemôže byť dokonalý a je to len doplnkom k prvým dvom spomenutým komponentom ochrany počítača. Antivírus pre odhaľovanie malwaru využíva niekoľko spôsobov:

- rezidentná ochrana súborového systému (kontroluje súbory pri spúšťaní, otváraní, ukladaní),
- ochrana prístupu na web (kontroluje obsah údajov preberaných z webu, najmä aktívne prvky ako skripty a pod.),
- ochrana elektronickej pošty (kontroluje obsah správ, najmä príloh, prijímanej aj odosielanej pošty),

- kontrola vymeniteľných médií (optické nosiče, USB kľúče, pamäťové karty a pod.),
- kontrola na vyžiadanie.

Antivírusový softvér využíva v princípe dve techniky na detekciu škodlivého softvéru:

- rozpoznávanie vzoriek známeho malware, ktoré má uložené vo vírusovej databáze,
- rozpoznávanie podozrivých aktivít v systéme, na ktoré používa rôzne heuristické metódy a je účinné aj proti neznámemu malware, ale môže spôsobiť falošné poplachy.

2.2.2 Nutnosť inštalácie antivírusového softvéru na počítači a zariadeniach

Antivírusový program nedokáže zo zle nastaveného alebo deravého operačného systému vytvoriť bezpečný systém - je to však užitočný doplnkový komponent ochrany, obzvlášť ak hovoríme o bežných používateľoch počítača.

Treba mať totiž na zreteli, že pri práci s počítačom sťahujeme a spúšťame programy aj bez toho, že by sme si to priamo uvedomili (napríklad v podobe makier kancelárskeho balíka, skriptov webových stránok a podobne). Nie vždy máme tiež možnosť overiť integritu a zdroj týchto programov a preto je vhodné mať antivírusový program nainštalovaný, spustený a aktualizovaný.

Aktualizovaná vírusová databáza je u antivírusového programu kľúčový prvok, pretože antivírus bez aktualizácií stráca na efektívnosti detekcie malwaru.

2.2.3 Dôležitosť pravidelnej aktualizácie softvéru (antivírusový program, webový prehliadač, zásuvné moduly, štandardné aplikácie, operačný systém)

Je samozrejmé, že často softvér obsahuje chyby. Neplatí to o všetkých chybách, ale množstvo z týchto chýb je možné zneužiť pre nejaký typ útoku alebo prieniku do počítačového systému (jedná sa o tzv. bezpečnostné chyby). Jedným zo základných kameňov počítačovej bezpečnosti sú aktualizácie softvéru, ktorými sa k používateľom dostávajú opravy známych chýb - a to nielen bezpečnostných (opravy bezpečnostných chýb sa dostávajú k používateľom spravidla s vyššou prioritou a nazývame ich bezpečnostné záplaty/opravy/aktualizácie).

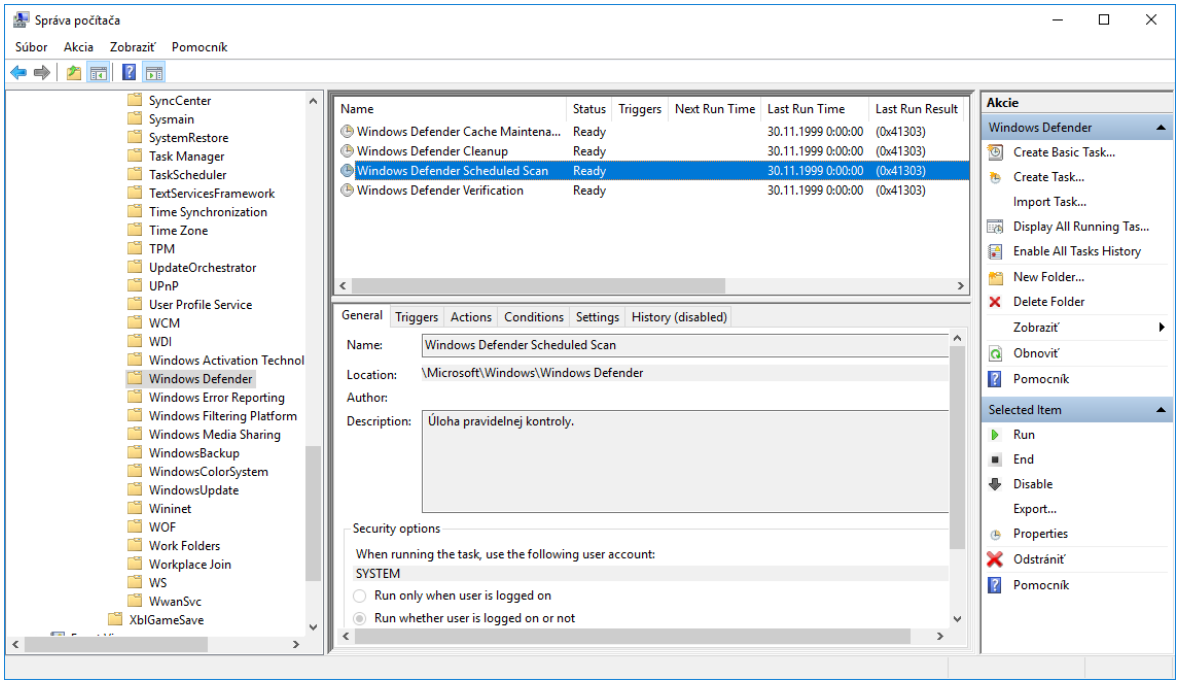
Aj keď nemožno pochybovať o tom, že všetky bezpečnostné opravy sú dôležité, aktualizácie niektorého softwaru v počítači je ešte kritickejšie. Jedná sa hlavne o aktualizácie operačného systému, webového prehliadača a antivírusového programu.

2.2.4 Kontrola konkrétnej pamäťovej jednotky, priečinka alebo súboru pomocou antivírusového softvéru. Naplánovanie kontroly s využitím antivírusového programu

Kedykoľvek si môžeme skontrolovať konkrétny súbor, priečinok, alebo pamäťovú jednotku pomocou antivírusového softvéru priamo cez program Prieskumník. Klikneme

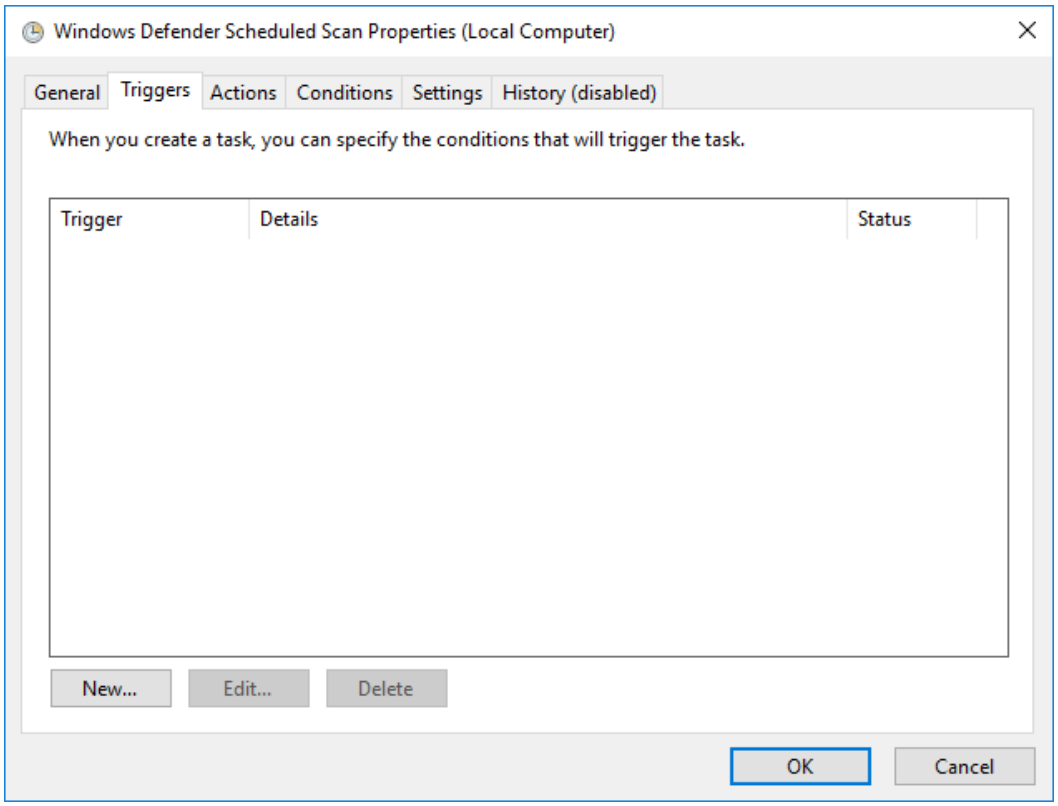
na požadovaný objekt pravým tlačidlom myšky a z ponuky si vyberieme možnosť "Skontrolovať aplikáciou Windows Defender".

Aby sme sa nemuseli starať o pravidelnú kontrolu súborov, môžeme si nastaviť ich kontrolu do tzv. plánovača. Program Windows Defender nemá vlastný plánovač, ale využíva integrovaný plánovač operačného systému (Task Scheduler). V tomto nástroji si v ľavom menu kliknutím otvoríme položku "Task Scheduler Library" a v stromovej štruktúre nájdeme položku "Microsoft/Windows/Windows Defender". Hore v strede máme zoznam úloh - vyberieme Windows Defender Scheduled Scan" (Obrázok 1) a v pravom menu v časti "Selected item" klikneme na tlačidlo "Properties".



Obrázok 1: Nastavenie pravidelnej kontroly súborov pomocou integrovaného plánovača operačného systému (Task Scheduler)

V otvorenom dialógovom okne vyberieme záložku "Triggers" (Obrázok 2). Po kliknutí na tlačidlo "New" je možné pridať rôzne typy "spúšťačov" naplánovaného skenovania. Takýchto spúšťačov môže byť nastavených viacero.



Obrázok 2: Okno pridania spúšťačov naplánovaného skenovania

2.2.5 Riziko pri využívaní zastaraného a nepodporovaného softvéru (zvýšené ohrozenie škodlivým softvérom, nekompatibilita)

Každý softvér má nejakého autora - človeka (alebo tím ľudí, spoločnosť), ktorý daný program naprogramoval, vyvinul. Pri vyvíjaní softvéru vždy dochádza k chybám. Aj keď je dobrým zvykom pri programovaní softvér dôsledne testovať, nie všetky chyby sa vychytajú hneď a k používateľom sa vždy dostane softvér s chybami. Časom sa tieto chyby odhaľujú (nielen autormi softvéru) a v prípade, že sa jedná o bezpečnostnú chybu, skôr či neskôr sa začne táto chyba zneužívať k útokom na daný počítačový systém. Preto je dôležité čo najskôr obdŕžať bezpečnostné záplaty novo objavených chýb.

Aby bol vývoj a používanie softvéru prehľadné, postupne takto vznikajú stále nové a nové verzie konkrétnych programov. Vývoj softvéru je však veľmi komplikovaná vec. V praxi často totiž nastáva situácia, kedy sa nová verzia programu natoľko zmení od predchádzajúcej, že v prípade objavenia chyby, ktorá sa vyskytuje v oboch verziách je natoľko nákladné ju včleniť do staršej verzie programu, že sa autor rozhodne aktualizovať iba novšiu verziu programu - a staršiu takto prestať podporovať. Znamená to, že používatelia sú nútení používať novšiu verziu programu, čo však nemusí byť vždy žiaduce (nová verzia sa napríklad funkčne líši od staršej a je tak pre dotyčného používateľa nepoužiteľná). Preto sa autori snažia podporovať aj staršie verzie softvéru (napríklad operačných systémov) aj nejakú dobu po vydaní novších verzií - prakticky a finančne to však po istom čase prestane byť rentabilné a preto každá verzia softvéru má iba obmedzenú dĺžku podpory. Používanie takej verzie softvéru po uplynutí tejto

doby sa potom stane bezpečnostným rizikom, pretože softvér obsahuje známe bezpečnostné chyby, ktoré sa neopravujú.

Doteraz sme sa na aktualizáciu softvéru pozerali z pohľadu bezpečnosti. Používanie neaktualizovaného a nepodporovaného softvéru má však aj ďalšie negatívum - a tým je kompatibilita. Problém napríklad nepodporovaných verzií operačných systémov je aj to, že ich nie je možné používať na novšom hardvéri, nakoľko aj tento podlieha vývoju a operačný systém sa priebežne musí tomuto vývoju tiež prispôsobovať, meniť (čo sa zo starším systémom už nedeje). Z pohľadu používateľských aplikácií zase staršie verzie programov nemusia korektne bežať na novších verziách operačných systémov alebo kooperovať s novšími verziami a podobne.

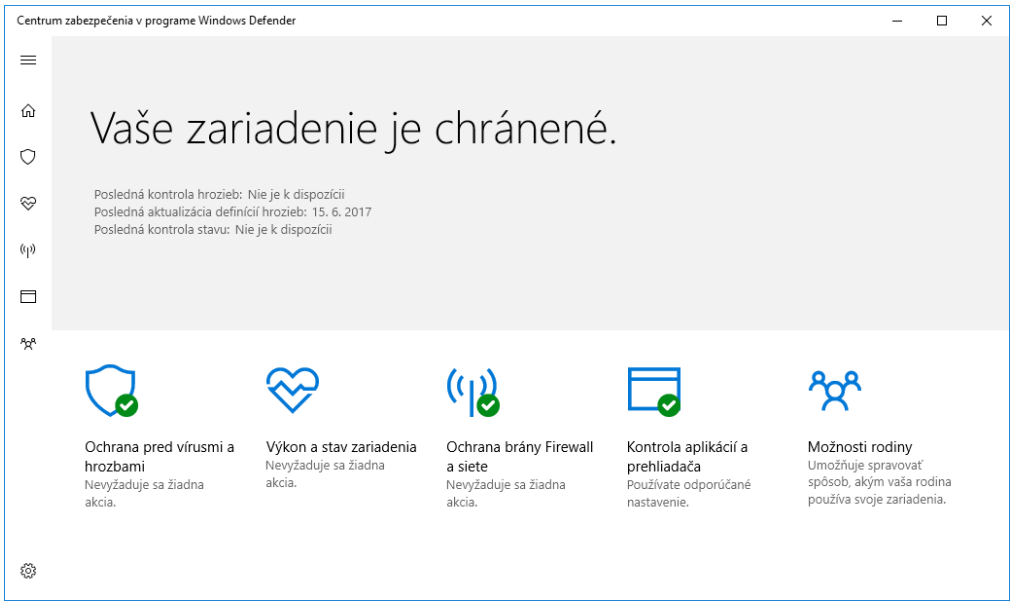
2.3 Vyriešenie a odstránenie

2.3.1 Karanténa a účinok umiestnenia infikovaných alebo podozrivých súborov do karantény

Karanténa je miesto (špeciálny priečinok), kam antivírusový softvér presúva súbory, ktoré detegoval ako nežiaduce. Používateľ má možnosť sa definitívne rozhodnúť či súbory z karantény vymaže alebo obnoví, pričom obnoviť má len súbory, pri ktorých si je istý, že ide o falošný poplach. Ďalšou možnosťou je ponechať si v karanténe súbory, ktoré boli označené len za podozrivé, a po nejakom čase ich skontrolovať znovu. Zaktualizovaný antivírusový softvér a vírusová databáza môžu potvrdiť alebo vyvrátiť podozrenie na infekciu a tým ovplyvniť rozhodovanie o obnove súboru.

2.3.2 Umiestnenie do karantény, vymazanie infikovaných/podozrivých súborov

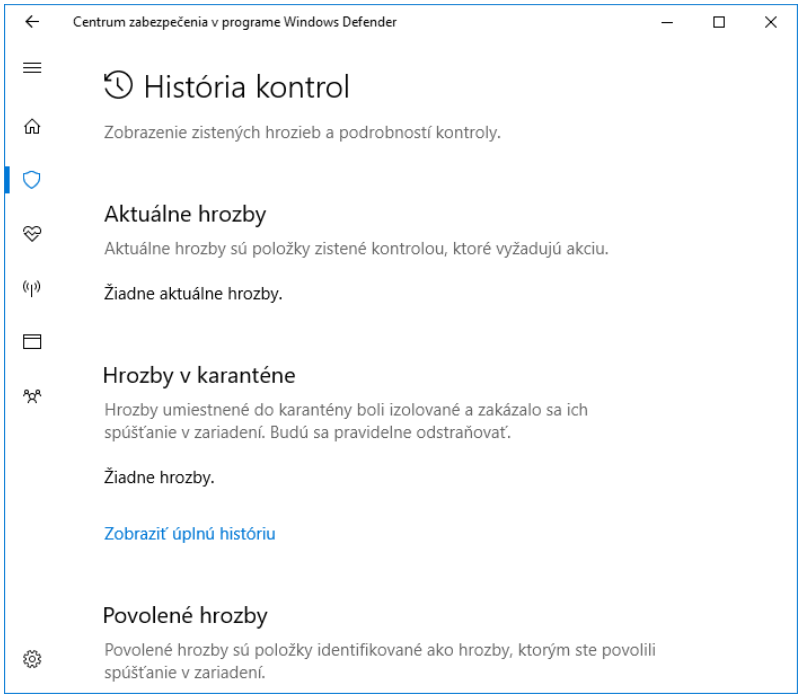
Ak antivírusový systém pri kontrole deteguje nejaký súbor ako podozrivý, presunie ho do tzv. karantény, kde je daný súbor svojim spôsobom izolovaný od zvyšku systému. Ak sa niečo podobné stane, je možné tento z karantény úplne vymazať alebo ho obnoviť (ak sme si istý, že daný súbor určite neobsahuje škodlivý software).



Obrázok 3: Centrum zabezpečenia v programe Windows Defender

Spustíme rozhranie antivírusového softvéru ("Centrum zabezpečenia v programe Windows Defender" (Obrázok 3).

V ľavom menu klikneme na tlačidlo "Ochrana pred vírusmi a hrozbami" a potom na "História kontrol". V časti "Hrozby v karanténe" je možné manažovať jednotlivé hrozby uložené v karanténe (Obrázok 4).



Obrázok 4: História kontrol programu Windows Defender

2.3.3 Diagnostika útokov škodlivým softvérom a ich riešenie pomocou využitia informácií z online zdrojov (webové stránky operačného systému, antivírusového programu, webového prehliadača a webové sídla zodpovedajúcich autorít)

Na webových sídlach použitého operačného systému, antivírusového programu a webového prehliadača je možné dohľadať informácie o možných útokoch a zraniteľnostiach a riešeniach týchto zraniteľností (resp. následkov útokov). V prípade útoku (prevencie) je možné tieto informácie sledovať a robiť individuálne opatrenia pre zvýšenie bezpečnosti.

Informácie o škodlivom softvéri sa nachádzajú aj na webových stránkach tvorcov antivírusových programov. Na špecifických miestach tvorcov webových prehliadačov môžeme nájsť aj informácie o počítačovej bezpečnosti či kriminalite (https://www.google.com/intl/sk_sk/safetycenter/resources/).

Zdrojmi informácií môžu byť aj stránky jednotlivcov (https://www.viry.cz/), pri ktorých si je potrebné uvedomiť, že nemusí ísť vždy o relevantné údaje.

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

Modul 12: Bezpečnosť pri využívaní IKT

Bezpečnosť počítačových sietí

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

3 Bezpečnosť počítačových sietí

3.1 Počítačové siete a pripojenia

3.1.1 Čo je počítačová sieť, typy počítačových sietí - lokálne siete (LAN), bezdrôtové lokálne siete (WLAN), rozľahlé siete (WAN), virtuálne privátne siete (VPN)

Počítačová sieť je systém vzájomne prepojených a spolupracujúcich počítačov, medzi ktorými môžeme pohodlne a rýchlo prenášať údaje, zdieľať prostriedky a komunikovať medzi používateľmi. Podľa rozsahu môžeme počítačové siete rozdeliť na tri kategórie.

LAN (Local Area Network) je typicky sieť v rozsahu jednej budovy, resp. inštitúcie. Väčšinou sú dobre chránené pred prístupom z vonku. V súčasnosti využíva v podstate dve technológie, a to Ethernet pre káblové (drôtové) prepojenie a WiFi pre bezdrôtové prepojenie - takáto sieť sa tiež nazýva pojmom WLAN (Wireless Local Area Network).

MAN (Metropolitan Area Network) je typicky sieť v rozsahu mesta, ktorá prepája jednotlivé LAN, napríklad siete poskytovateľov pripojenia do Internetu. V súčasnosti využíva najmä optické prepojenia, prípadne špeciálne bezdrôtové prepojenia na väčšie vzdialenosti.

WAN (Wide Area Network) sú rozľahlé siete v rozsahu regiónu, štátu, kontinentu či celého sveta, napr. armádne siete, Internet a podobne.

VPN (Virtual Private Network) - je technológia prepojenia viacerých počítačov pomocou verejnej (nedôveryhodnej) siete tak, akoby boli pripojené na jednu spoločnú súkromnú sieť (dôveryhodnú). Využívajú sa napr. na bezpečný prenos medzi vzdialeným používateľom a vnútornou sieťou organizácie (prístup z domu, počas služobnej cesty), prípadne spojenie medzi pobočkami firmy a podobne.

3.1.2 Vplyv pripojenia sa do siete na bezpečnosť, napríklad na šírenie škodlivého softvéru, na neoprávnený prístup k údajom, na narušenie súkromia

Ak nemáme počítač pripojený do počítačovej siete, útok naň môže byť zrealizovaný len fyzickým kontaktom, teda buď sa útočník dostane k počítaču, alebo používateľ donesie malware na pamäťovom médiu. Únik informácií z takého počítača bez spolupráce používateľa je prakticky nemožný.

Ak počítač pripojíme do počítačovej siete, vystavujeme ho tým možným útokom po sieti (najmä po pripojení do neznámej alebo verejnej siete), ktoré sa väčšinou snažia zneužiť zraniteľnosť nejakej sieťovej služby, prípadne využiť zle nastavenú sieťovú službu, a tak získať neoprávnený prístup k informáciám uloženým v počítači, nainštalovať malware, alebo ovládnuť celý počítač. Rapídne sa zvyšuje možnosť úniku informácií z počítača, či už činnosťou malware alebo chybou používateľa pri využívaní sieťových služieb.

3.1.3 Úloha správcu počítačovej siete v procese riadenia autentifikácie, autorizácie, pri správe používateľských účtov, pri monitorovaní a inštalovaní relevantných bezpečnostných záplat a aktualizácií, pri monitorovaní sieťovej komunikácie, pri riešení nájdeného škodlivého softvéru v rámci spravovanej siete

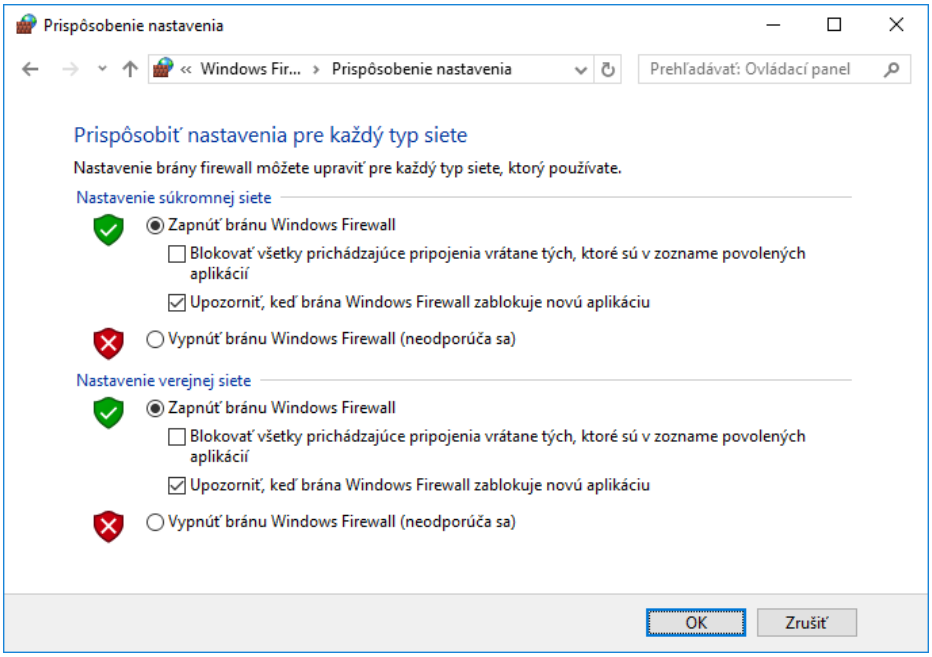
Správca počítačovej siete (administrátor) nastavuje spôsob autentifikácie používateľov v sieti, spravuje používateľské kontá (vytvára a maže), nastavuje pre používateľov oprávnenia (autorizuje ich) pre prístup do lokálnej siete aj do internetu, konfiguruje firewall a sieťové služby, monitoruje sieť, stará sa o inštaláciu softvéru a bezpečnostných záplat a rieši malwarové incidenty.

3.1.4 Funkcia brány firewall, jeho obmedzenia v súkromnom i pracovnom prostredí

Firewall je zariadenie (hardvérové alebo softvérové) pre riadenie sieťovej prevádzky. Zjednodušene sa dá povedať, že slúži ako kontrolný bod, ktorý definuje pravidlá pre komunikáciu medzi sieťami (alebo počítačom a sieťou) a tým povoľuje (resp. zakazuje) komunikáciu podľa vopred definovaných pravidiel.

3.1.5 Aktivácia firewallu, konfigurácia jednoduchých pravidiel

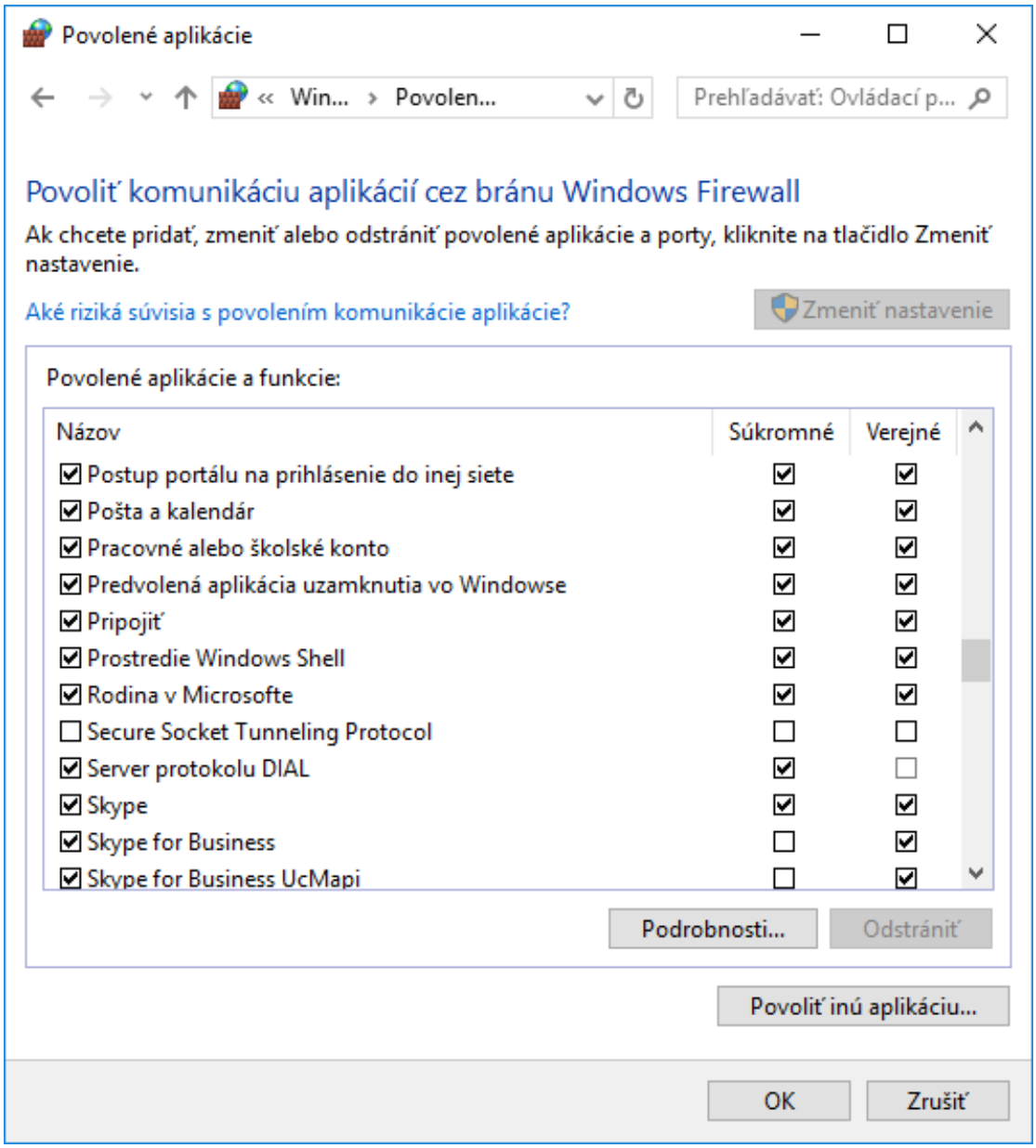
Firewall v systéme Windows môžeme ľahko vypnúť alebo zapnúť. Stačí vojsť do Ovládacieho panela a zvoliť "Systém a zabezpečenie" a ďalej "Windows Firewall". V ľavom menu zvolíme položku "Zapnúť alebo vypnúť bránu Windows Firewall" (Obrázok 1).



Obrázok 1: Zapnutie/vypnutie brány Windows Firewall

Ak v ľavom menu zvolíme možnosť "Povoliť komunikáciu aplikácií cez bránu Windows Firewall" (Obrázok 2) dostaneme sa k dialógu, kde môžeme ručne povoľovať/zakazovať

funkcie a aplikácie firewallu. Tento dialóg obsahuje len veľmi zjednodušené nastavenia firewallu, pre komplexnejšie nastavenia sú potrebné hlbšie znalosti o počítačových sieťach.



Obrázok 2: Povolenie komunikácie aplikácií cez bránu Windows Firewall

Všimnite si, že v oboch spomínaných dialógoch je firewall oddelený do profilov - pre súkromné siete (doma, v práci - na miestach, kde je prehľad o pripojených klientoch) a na verejné siete (hlavne rôzne verejné wifi siete). Dá sa takto nakonfigurovať odlišné správanie firewallu vzhľadom k nastaveniu pripojenej siete.

3.2 Bezpečnosť bezdrôtovej siete

3.2.1 Typy zabezpečenia bezdrôtovej siete - Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) / Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC) filtrovanie, Service Set Identifier (SSID) skrývanie

Komunikáciu realizovanú pomocou bezdrôtovej (WiFi) siete je ľahké odpočúvať. Na rozdiel od (drôtovej) siete sa totiž netreba nikam pripájať, stačí byť v dosahu signálu. Preto je vhodné chrániť prístup k tejto sieti heslo a zároveň takúto komunikáciu šifrovať. Na ochranu bezdrôtovej siete sa využívajú viaceré typy zabezpečenia.

Prístup k sieti sa dá obmedziť **filtrovaním MAC adries**. Využíva filtrovanie pripojených zariadení na základe MAC adresy (Media Access Control), ktorá slúži na identifikáciu sieťového rozhrania v lokálnych počítačových sieťach, ale je ľahko prekonateľná a je to iba ochrana prístupu, nechráni proti samotnému odpočúvaniu.

WEP (Wired Equivalent Privacy) je zastaralé zabezpečenie bezdrôtových sietí. V minulosti bolo prelomené, preto je v súčasnosti toto zabezpečenie považované za nedostatočné.

WPA (Wi-Fi Protected Access) bolo vyvinuté za účelom náhrady WEP. Využíva rovnakú šifrovaciu metódu ako WEP, ale pre správu šifrovacích kľúčov používa protokol TKIP (Temporal Key Integrity Protocol), ktorý mení dočasný kľúč každých 10000 paketov. Pre pripojenie sa využívajú dva spôsoby autentifikácie:

- PSK (Pre-Shared Key) - využíva heslo, ktoré je spoločné pre všetkých používateľov siete,
- Enterprise - využíva autentizačný server a vyžaduje autentifikáciu konkrétneho používateľa (meno a heslo).

WPA a jeho nasledovníka WPA2 je dnes možné prelomiť a preto sa odporúča využiť ich nasledovníka **WPA3**, ktorý je považovaný za bezpečný.

SSID je identifikátor (názov) bezdrôtovej siete. Prístupový bod bezdrôtovej siete pravidelne vysiela tento identifikátor - je však možné nakonfigurovať ho tak, aby tento identifikátor nevysielal, čo môže prispieť k zvýšeniu bezpečnosti bezdrôtovej siete. Pokiaľ je však bezpečnosť siete postavená výlučne len na skrývaní SSID, jedná sa o bezpečnostnú slabinu.

3.2.2 Riziká používania počítačovej siete (odpočúvanie komunikácie, prevzatie sieťového spojenia, odpočúvanie a pozmeňovanie komunikácie)

V nezabezpečenej WiFi sieti sú všetky zariadenia pripojené bez ochrany ich komunikácie, takže nie sú chránené voči útočníkom.

Komunikáciu cez takéto pripojenie môže odpočúvať ktokoľvek v dosahu signálu. Útočník sa môže vydávať za niekoho iného a tak získať prístup k počítačovým systémom. Hroziacim útokom je aj tzv. "Man in the middle" (MITM, človek uprostred), kedy útočník odpočúva sieťovú komunikáciu medzi účastníkmi tak, že sa stane aktívnym

prostredníkom. Na takúto sieť sa môže pripojiť v podstate ktokoľvek a potom hrozia ďalšie útoky súvisiace s prienikom do systému obete.

Ak sa už rozhodnete pripojiť na verejne prístupnú Wi-Fi sieť, skúste sa držať nasledujúcich zásad, ktoré zvýšia pravdepodobnosť, že vaše údaje nezneužije tretia strana. Stránky, kde zadávate chúlostivé informácie (prakticky všade, kde sa prihlasujete menom a heslom) navštevujte iba ak sú zabezpečené dodatočným šifrovaním (URL stránky začína na "https://"). Veľmi dobre môže poslúžiť aj firewall s nastavenými striktnými pravidlami filtrovania prichádzajúcich spojení. Ak je to možné, použite šifrované VPN.

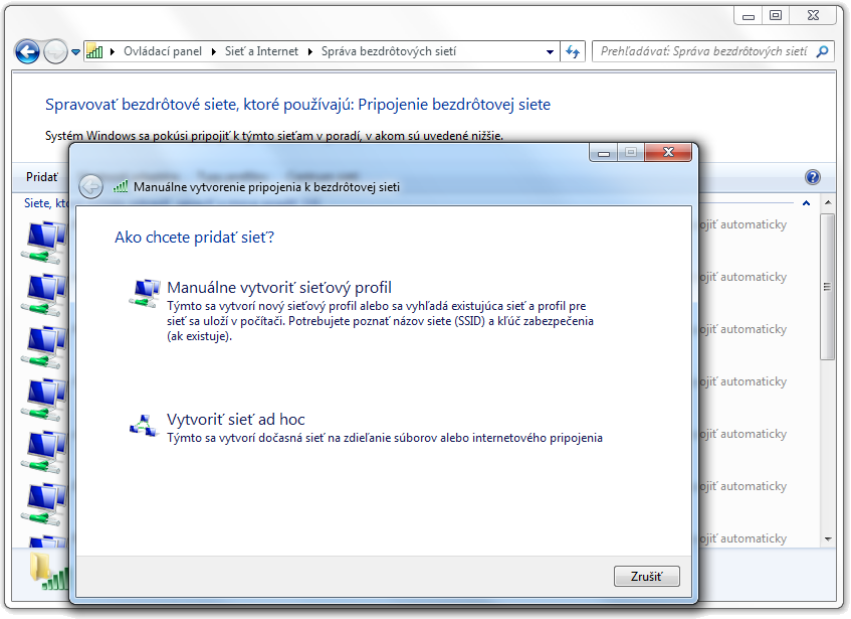
3.2.3 Vytvorenie prípojného bodu (hotspot)

Z bežného počítača vybaveného bezdrôtovým sieťovým rozhraním možno konfiguráciou vytvoriť prípojný bod a takým spôsobom umožniť, aby sa iné počítače pripojili za účelom zdieľania sieťovej konektivity, výmeny dát, využitia nejakých sieťových služieb a podobne.

3.2.4 Vytvorenie osobného hotspotu

Vytvoriť prípojný bod v systéme Windows 7 je jednoduché:

- **`Štart ▶ Ovládací panel ▶ Sieť a Internet`**
- v ľavej časti zvolíme **`Správa bezdrôtových sietí`**
- **`Pridať ▶ Vytvoriť sieť ad hoc`** (Obrázok 3)

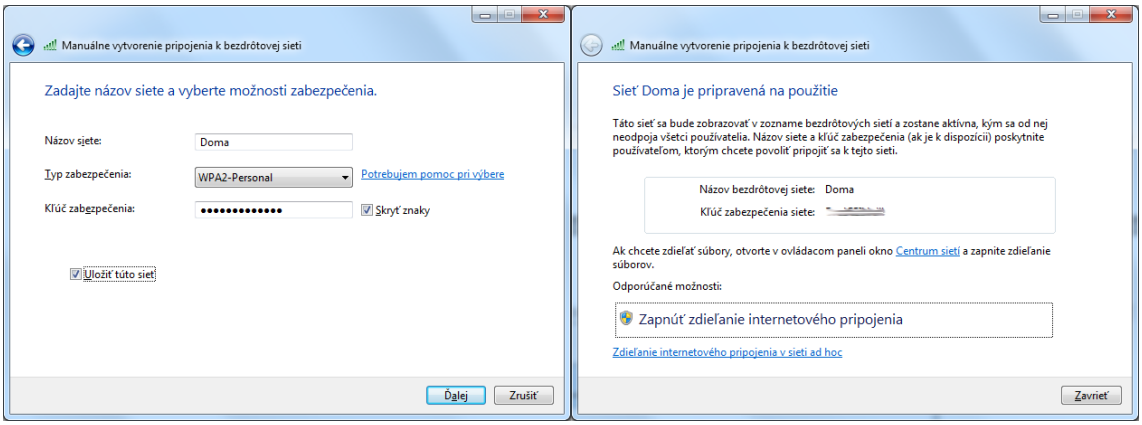


Obrázok 3: Vytvorenie hotspotu vo Windows 7

V nasledujúcej časti nastavíme (Obrázok 4):

- názov siete SSID,
- typ zabezpečenia,
- kľúč zabezpečenia KEY.

Zapnutím zdieľania internetového pripojenia je možné využiť osobný hotspot. Niektoré úkony môžu požadovať administrátorský prístup.



Obrázok 4: Nastavenie siete

Pre Windows 10 vytvoríme nasledovným spôsobom. Otvoríme si príkazový riadok pod administrátorským účtom a nasledovným príkazom vytvoríme ad-hoc sieť:

```
netsh wlan set hostednetwork mode=allow ssid=SSID key=PASSWORD
```

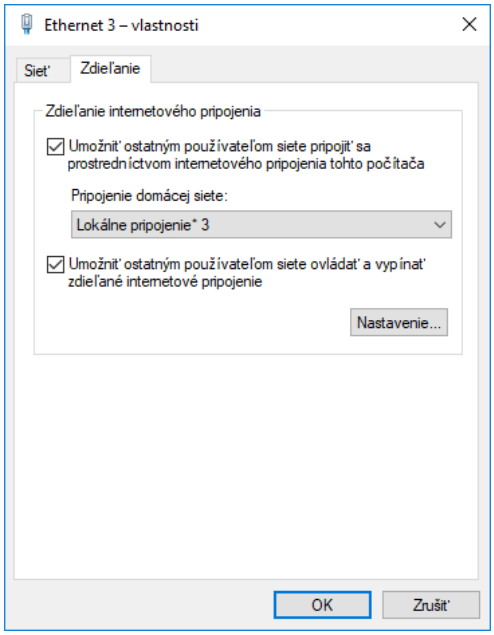
Reťazec SSID nahradíme názvom siete podľa vlastného výberu a reťazec PASSWORD nahradíme heslom. Nasledovným príkazom aktivujeme novovytvorenú sieť:

```
netsh wlan start hostednetwork
```

Tretím krokom povolíme zdieľanie Internetového pripojenia. Otvoríme ovládací panel a zvolíme položku "Sieť a internet" a "Centrum sietí". V ľavom menu klikneme na "Zmeniť nastavenia adaptéra" - otvoríme okno so zoznamom sieťových pripojení.

Klikneme pravým tlačidlom na to pripojenie, ktorým sa počítač pripája na Internet a zvolíme "Vlastnosti" a prejdeme na záložku "Zdieľanie" (Obrázok 5). zaškrtneme možnosť "Umožniť ostatným používateľom siete pripojiť sa prostredníctvom internetového pripojenia tohto počítača" a vo výberovom menu "Pripojenie domácej siete" vyberieme novovytvorenú ad-hoc sieť.

Teraz je možné sa iným zariadením pripojiť k vytvorenej ad-hoc sieti a prostredníctvom nej sa pripojiť na Internet.



Obrázok 5: Zdieľanie sieťového pripojenia

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

Modul 12: Bezpečnosť pri využívaní IKT

Riadenie prístupu

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

4 Riadenie prístupu

4.1 Metodika

4.1.1 Opatrenia na zamedzenie neautorizovaného prístupu k údajom (používateľské heslo, PIN, šifrova-nie, viacfaktorová autentifikácia)

Heslo je všeobecný prostriedok slúžiaci na overenie totožnosti používateľa. Používateľ je považovaný za oprávneného, ak preukáže znalosť hesla.

PIN (z anglického personal identification number - osobné identifikačné číslo) - identifikátor, pomocou ktorého je možné sa autorizovať napr. pri platobnej karte, mobilného telefónu a pod. Najčastejšie sa jedná o štvormiestne číslo, ktoré sa musí zadať pri zapnutí (použití) predmetu a bez jeho znalosti nie je možné tento predmet použiť.

Šifrovanie dát je proces, ktorým sa nezabezpečené dáta prevedú pomocou kryptografie na dáta šifrované (čitateľná iba pre majiteľa dešifrovacieho kľúča).

Viacfaktorová autentifikácia je metóda riadenia prístupu, pri ktorej bude používateľovi udelený prístup na základe úspešného prekonania niekoľkých oddelených bezpečnostných prvkov autentifikačného mechanizmu – typicky minimálne 2 z nasledovných: vedomosť (niečo, čo používateľ vie, napr. heslo alebo PIN), vlastníctvo (niečo čo používateľ má, napr. mobilný telefón s daným číslom alebo platobnú kartu) a fyzický znak (niečo, čo má používateľ vrodené a unikátne (biometrické údaje), napr. odtlačok prsta, sken dúhovky oka).

4.1.2 Jednorazové heslo (one-time password) a jeho využitie

Jednorazové heslá sa používajú väčšinou ako jeden z prvkov viacfaktorovej autentifikácie, prípadne ako prvotné heslo pre prihlásenie do počítačového systému, ktoré je nutné zmeniť po prvom úspešnom prihlásení. Pri viacfaktorovej autentifikácií je to typicky heslo, ktoré potvrdzuje napríklad vlastníctvo mobilného telefónu s istým telefónnym číslom. Takéto heslo má obmedzenú platnosť - dá sa použiť iba raz, čiže v prípade, že by ho útočník odchytil, nie je možné ho použiť znova. Často majú tieto hesla aj obmedzenú časovú platnosť (rádovo niekoľko minút). Napr. v bankovníctve sa využíva zasielanie jednorázového kľúča (PIN) cez SMS pri potvrdzovaní prevodu peňazí.

4.1.3 Účel sieťového účtu

Hlavným účelom sieťového účtu na rôznych sieťových službách je regulovať prístup jednotlivých používateľov k sieti, údajom počítačového systému. Na autentifikáciu k sieti sa používa meno a heslo, prípadne certifikát. Ak nedôjde k úspešnej autentifikácii používateľa, prístup do siete je mu odoprený.

4.1.4 Prístup k používateľskému účtu cez používateľské meno a heslo, nutnosť odhlásenia pri nepoužívaní

K účtu sa pristupuje pomocou mena a hesla. Meno definuje o ktorý účet sa jedná a znalosť hesla autorizuje používateľa k práci s účtom. Ak dotyčný prestane pracovať

s účtom, je dôležité sa odhlásiť z tohto účtu. V prípade kratších prestávok v práci je možné účet na počítači dočasne zablokovať, aby v prípade neprítomnosti nemohol byť účet zneužitý.

4.1.5 Bežné techniky riadenia prístupu k sieti na základe biometrických údajov (odtlačky prstov, obraz dúhovky oka, rozpoznávanie tváre, geometria dlane)

Každý ľudský organizmus je svojím spôsobom unikát a na ľudskom tele sa nachádza niekoľko unikátnych znakov (tzv. biometrických údajov), ktoré možno pomocou dnešnej technológie ľahko digitalizovať a použiť tak k overeniu totožnosti používateľa. Pri autentifikácii pomocou biometrických údajov sa získaná vzorka uloží a priradí k používateľovi a pri prihlasovaní sa načítaný údaj porovná s uloženým a na základe porovnania prihlási používateľa.

Najčastejšie sa využívajú **odtlačky prstov**. Ich snímače sú pomerne lacné a už niekoľko rokov sú súčasťou výbavy niektorých notebookov a nedávno sa dostali aj do mobilných telefónov. U jednoduchších býva chybovosť lepšia ako 1%, v prípade profesionálnych (bezpečnostné firmy a pod.) klesá pod 0,001%.

V súčasnosti sa pripravujú zariadenia pre **skenovanie dúhovky** oka pre nasadenie do mobilných zariadení, kde by mala byť chybovosť do 0,001%. Skenovacie zariadenia používané na niektorých letiskách majú chybovosť pod 0,000001%, čo predstavuje jednu chybu na 100.000.000 pasažierov.

Ďalšími možnosťami zabezpečenia pomocou biometrických údajov sú napríklad **rozpoznávanie tváre** (podľa geometrických charakteristík tváre) a **geometria dlane** (ruka je tiež do istej miery jedinečná - neposkytuje však dostatok informácií a preto sa odporúča používať výlučne v priestoroch s nízkym počtom pohybujúcich sa osôb).

4.2 Správa hesiel

4.2.1 Zásady pre výber hesiel (primeraná dĺžka, zložitosť, nezdieľanie hesla, pravidelná zmena hesla, rozdielne heslá pre rôzne služby)

Na zabezpečenie potrebnej úrovne ochrany používateľských účtov pri prihlasovaní menom a heslom je dôležité stanoviť pravidlá pre tvorbu hesiel.

Základnými parametrami sú dĺžka hesla a povinná kombinácia znakov (veľkých a malých písmen, číslic, prípadne špeciálnych znakov). Takto dosiahneme, že používateľove heslá sú dostatočné pre odolávanie tzv. útoku hrubou silou (útok, pri ktorom počítačový program skúša zaradom všetky možné kombinácie znakov), resp. tzv. slovníkovému útoku (program skúša zaradom všetky heslá z vopred zostaveného slovníku, napríklad bežných slov nejakého jazyka a podobne).

Snáď ani netreba pripomínať, že heslo je tajná informácia, a preto je obrovským rizikom zdieľať prístupové heslo s inými osobami. Na takéto účely slúžia viaceré používateľské účty k jednej službe.

Pri častom používaní hesla sa môže stať, že ho niekto nepovolaný zistí, preto je vhodné heslo po nejakom čase zmeniť. Môže to vykonať používateľ na základe vlastného rozhodnutia, alebo túto požiadavku môže mať jeho organizácia uvedenú v pracovnom poriadku resp. v pravidlách pre používanie siete, prípadne zmenu môže vyžadovať autentifikačný systém. Pre zvýšenie ochrany sa môžu špecifikovať doplnkové pravidlá pre zmenené heslá, typicky napr. nie je možné použiť niekoľko naposledy použitých hesiel, heslo sa musí od predchádzajúceho dostatočne odlišovať (ak mám heslo "Heslo1", nemôžem si nastaviť nové heslo "Heslo2").

Dôležitým aspektom dnešnej doby je nepoužívať rovnaké heslo pre viacero služieb. Môže sa totiž stať, že konkrétna služba neudržuje databázu hesiel dostatočne zabezpečenú a pri útoku na túto službu môže Vaše heslo uniknúť, pričom Vy sa toto väčšinou ani nedozviete. Vaše heslo (aj keď je zložité) je potom v rukách útočníka a spolu s ním aj prístup k ďalším službám.

4.2.2 Softvér na správu hesiel

V dnešnej digitálnej dobe sa denne stretávame s nutnosťou autorizovať sa heslom takmer všade. To so sebou prináša potrebu pamätať si množstvo hesiel, čo sa s pribúdajúcim počtom stáva neúnosným. Situáciu riešia tzv. manažéri hesiel, čo sú špecializované programy slúžiace na ukladanie hesiel - heslá sú uložené v zašifrovanej databáze, čiže relatívne bezpečne. Používateľ si nemusí pamätať všetky heslá, pamätá si iba jedno, ktoré slúži k zašifrovaniu a opätovnému dešifrovaniu databáze. Jednoduché varianty týchto manažérov obsahujú v dnešnej dobe aj webové prehliadače.

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

Modul 12: Bezpečnosť pri využívaní IKT

Bezpečná práca s webom

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

5 Bezpečná práca s webom

5.1 Nastavenie webového prehliadača

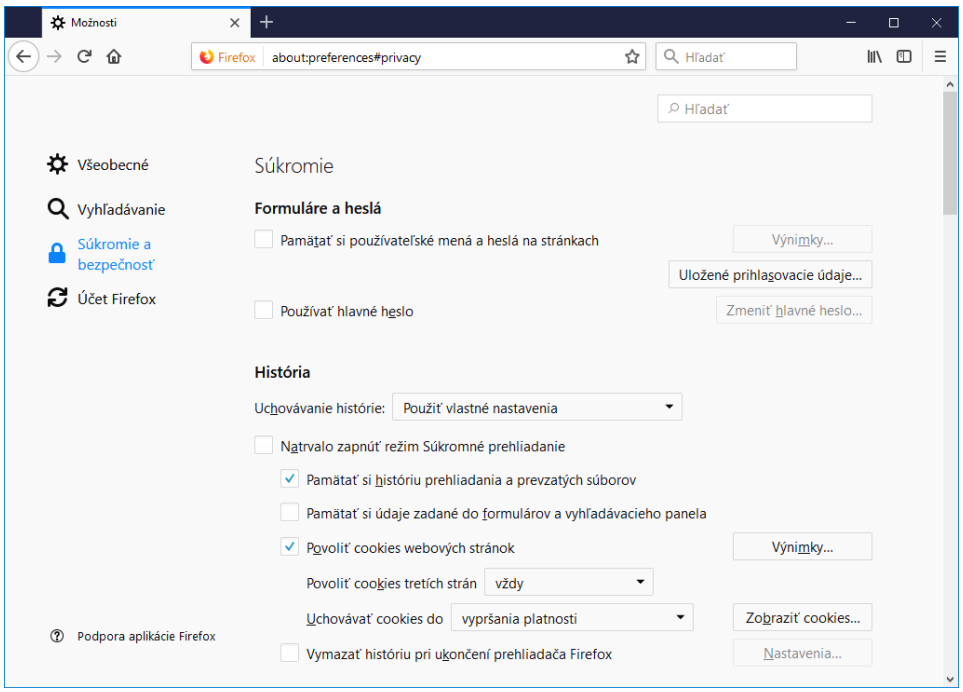
5.1.1 Ako zvoliť vhodné nastavenia pre umožnenie / zakázanie automatického dokončovania a automatického ukladania pri vypĺňaní formulárov a hesiel

Automatické dopĺňanie formulárov na webových stránkach uľahčuje prácu pri častom vypĺňaní rovnakých údajov, ale je vhodné len na vlastnom počítači. Na cudzích alebo zdieľaných počítačoch predstavuje hrozbu - niekto cudzí sa môže dostať k Vašim údajom.

Veľký pozor si musíme dávať na zapamätávanie hesiel. Ak túto funkciu chceme využiť tak jedine v zašifrovanej databáze nejakého spoľahlivého programu na správu hesiel.

Nastavenia automatického dokončovania formulárov sa napr. v prehliadači Mozilla Firefox nachádzajú v nastaveniach pod záložkou "Súkromie a bezpečnosť". V časti "Uchovávanie histórie" nastavíme možnosť "Použiť vlastné nastavenia" a odškrtneme možnosť "Pamätať si údaje zadané do formulárov a vyhľadávacieho panela" (Obrázok 1). Takýmto spôsobom vypneme pamätanie údajov vložených do formulárov.

Ukladanie prihlasovacích údajov môžeme vypnúť v nastaveniach pod záložkou "Súkromie a bezpečnosť" (Obrázok 1). Odškrtneme možnosť "Pamätať si prihlasovacie údaje k stránkam". V prípade, že túto možnosť chceme používať, je dôležité chrániť uložené heslá šifrovaním - to je možné zapnúť zaškrtnutím možnosti "Používať hlavné heslo" a nastavením príslušného hesla.

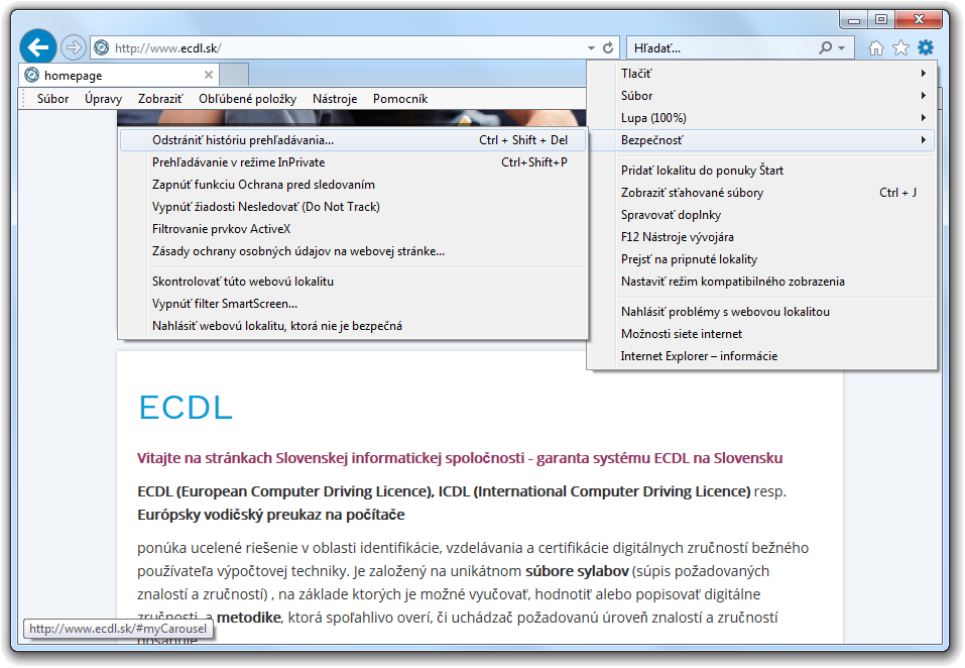


Obrázok 1: Konfiguračný dialóg webového prehliadača Mozilla Firefox

5.1.2 Ako odstrániť z webového prehliadača súkromné údaje, ako sú história prehliadania, pamäť dočasných súborov (cache), heslá, cookies, údaje automatického dokončovania

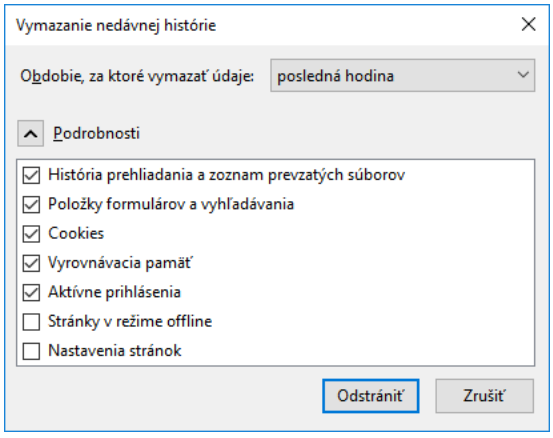
Vymazanie súkromných údajov z prehliadača (cookies, história navštívených stánok, história prevzatých súborov, dočasné kópie navštívených stránok, hodnoty z formulárov) môže byť vhodné najmä na cudzom alebo zdieľanom počítači.

V prehliadači Internet Explorer je možné odstrániť históriu prehliadania cez Nastavenia a časť Bezpečnosť, kde sa nachádzajú aj ďalšie možnosti (Obrázok 2).



Obrázok 2: Nastavenia v prehliadači Internet Explorer

V prehliadači Mozilla Firefox klikneme v menu na tlačidlo "Knižnica", ďalej "História" a "Vymazať nedávnu históriu". V dialógovom okne máme na výber obdobie, za aké je možné súkromné údaje vymazať a v časti "Podrobnosti" je možné vybrať konkrétne údaje, ktoré chceme zmazať (Obrázok 3).



Obrázok 3: Vymazanie histórie vo webovom prehliadači Mozilla Firefox

5.2 Bezpečné prehliadanie webu

5.2.1 Ktoré činnosti na webe by sa mali uskutočňovať iba na zabezpečených webových stránkach

Zabezpečenie komunikácie cez protokol HTTP rieši jeho rozšírenie protokol HTTPS (HTTP over SSL/TLS).

Protokol SSL/TLS využíva asymetrickú kryptografiu a zabezpečuje:

- autentifikáciu servera (aby sme vedeli, že komunikujeme s tým správnym);
- šifrovanie prenášaných údajov (nie je možné získať informácie odpočúvaním);
- kontrolu integrity prenášaných údajov (nie je možné nepozorovane zmeniť prenášané informácie)

Certifikát servera umožňuje webovému prehliadaču vytvoriť zabezpečené pripojenie k serveru.

Všetky aktivity, pri ktorých sa vyžaduje autentifikácia používateľa, by sa mali vykonávať iba na zabezpečených webových stránkach. Patria tu najmä prístup k elektronickej pošte, on-line nákupy, finančné transakcie, práca v informačných systémoch, komunikácia na sociálnej sieti a pod.

5.2.2 Poznať spôsoby ako si potvrdiť autenticitu web stránky (kvalitný obsah, všeobecné uznávaný zdroj, platné URL, prítomné informácie o spoločnosti alebo vlastníkovi stránky, kontaktné informácie, bezpečnostný certifikát stránky, overený vlastník domény)

Existujú viaceré spôsoby ako si potvrdiť, že stránka, ktorú navštevujete je skutočne autentická a nejedná sa o podvrhnutú stránku.

Jedným s kritérií, ktoré môžu potvrdiť autentickosť je kvalitný obsah. Podvrhnuté stránky majú často v obsahu gramatické chyby, nezrozumiteľný text a podobne.

V prípade podozrenia je vhodné zadať názov stránky do vyhľadávača a pozrieť sa na hodnotenie tejto stránky.

Veľmi dobrým pomocníkom je overiť si názov domény v adresnom riadku prehliadača - ak napríklad chcem navštíviť stránku univerzity a v adresnom riadku vidíme niečo ako sk.uni-verzita.ru, je celkom zrejmé, že sa nejedná o stránku slovenskej univerzity.

Na stránkach regulárnych spoločností bývajú uvedené kontaktné informácie (vrátane platného telefónneho čísla).

Ak je stránka dostupná cez šifrované spojenie (https://) je možné vo webovom prehliadači overiť organizáciu/majiteľa certifikátu stránky.

Je tiež možné overiť majiteľa danej domény cez nástroj whois (dostupný aj cez webové stránky - https://whois.sk-nic.sk).

5.2.3 Čo znamená a spôsobuje presmerovanie na podvrhnuté webové stránky (pharming)

Pharming je presmerovanie komunikácie s vybraným serverom na iný server ovládaný útočníkom tým, že sa presmeruje názov webovej stránky na inú adresu. Každej mennej adrese, (napr. www.upjs.sk), prislúcha číselná, tzv. IP adresa (v tomto prípade 158.197.16.80). Presmerovanie takejto adresy môže útočník uskutočniť buď napadnutím servera DNS, ktorý prevádza menné adresy na IP adresy, alebo priamo na počítači používateľa zmenou súboru hosts, v ktorom sú lokálne uložené IP adresy pre vybrané menné adresy.

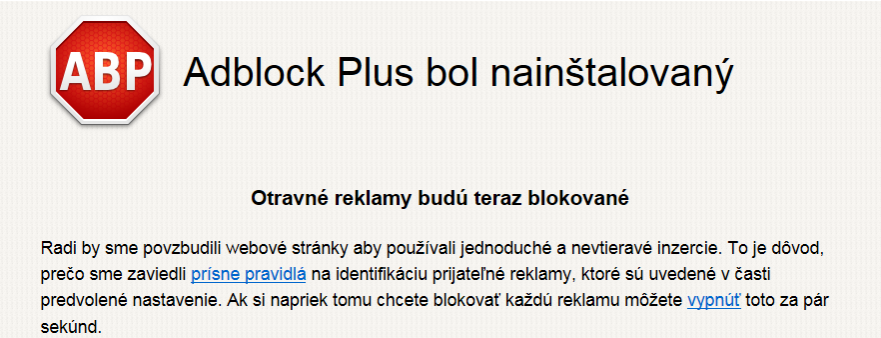
Ak používateľ zadá mennú adresu do internetového prehliadača, namiesto požadovanej stránky (napr. banky) sa zobrazí jej dokonalá napodobenina. Používateľ teda nezistí, že sa nachádza na inej stránke. Po zadaní údajov ich získa neoprávnená osoba, ktorá takúto falošnú stránku vytvorila.

Samotný útok môže prebiehať rôznym spôsobom. Veľmi často sa založí webová stránka, ktorá vyzerá ako presná kópia už existujúcej dôveryhodnej stránky, alebo ponúka nejaké výhody po prihlásení cez ich webovú stránku. Napr. ponúkajú rôzne „skvelé“ služby (napr. vzácne predmety do hier, stiahnutie programov zadarmo po registrácii atď.). Prihlasovacie meno a heslo zadané do falošnej stránky získa útočník, ktorý ich môže priamo zneužiť, prípadne predať ďalším osobám, ktoré o to majú záujem.

5.2.4 Účel, funkcia a druhy softvéru na kontrolu obsahu webových stránok, ako sú softvér na filtrovanie internetového obsahu, softvér na účely rodičovskej kontroly

Antivírusový softvér chráni používateľa pred malwarom ako takým, nechráni však používateľa pred obsahom webových stránok. Softvér na kontrolu obsahu webových stránok slúži na obmedzenie alebo monitoring prístupu k určitému druhu obsahu na webe, prípadne k určitým konkrétnym stránkam.

Podľa účelu a funkcií sa jednotlivé druhy softvéru od seba líšia. Softvér na blokovanie nežiaducej reklamy na internete obmedzí jej zobrazenie vo webovom prehliadači (Obrázok 4). Niektoré webové portály žiaľ žijú prevažne z tejto reklamy.



Obrázok 4: Softvér na blokovanie reklamy

Účelom softvéru na kontrolu obsahu webových stránok je zamedziť používateľovi v prístupe k niektorému typu obsahu (hazard, pornografia a pod.) alebo zamedziť v prístupe ku konkrétnej stránke.

Špecifickú skupinu tvorí softvér, ktorý zabezpečuje tzv. rodičovskú kontrolu. Jednou z najdôležitejších funkcií je filter webových stránok , ktoré môžeme navštíviť. Odporúča sa, aby sme vyplnili zoznam stránok, ktoré nebude možné navštíviť. Ak existuje veľa takýchto adries, môžeme naopak vyplniť "biely zoznam" . Používateľ (dieťa) bude môcť navštíviť iba stránky z tohto zoznamu. V rámci rodičovskej kontroly je možné stanoviť kedy a ako dlho môže používateľ používať zariadenie.

Obrázok 5: Rodičovská kontrola v programe Windows Defender

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

Modul 12: Bezpečnosť pri využívaní IKT

Komunikácia

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

6 Komunikácia

V tejto časti sa budeme venovať bezpečnosti dvoch najrozšírenejších spôsobov komunikácie na internete – elektronickej pošte a komunikácii v reálnom čase.

6.1 Elektronická pošta (E-mail)

Elektronická pošta vznikla ešte pred vznikom internetu v druhej polovici šesťdesiatych rokov ako spôsob komunikácie medzi používateľmi veľkých, tzv. mainframových počítačov. Najprv bolo možné posielať správy len medzi používateľmi jedného počítača, no veľmi rýchlo pribudla možnosť poslať správu aj na iný počítač.

Je to tzv. off-line komunikácia, ktorá funguje podobne ako klasická pošta. Odosielateľ odovzdá správu svojmu poštovému serveru („podacia pošta“), ten ju podľa adresy prijímateľa nasmeruje cez sieť poštových serverov až na server, na ktorom má príjemca správy zriadenú schránku („doručovacia pošta“), a ten mu ju doručí do jeho schránky. Príjemca si musí schránku otvoriť, aby videl, či má v nej nejaké správy.

Pre zachovanie kompatibility so staršími systémami elektronická pošta ešte stále využíva textový formát pri prenose informácií. Z tohto dôvodu sú štandardné správy elektronickej pošty z bezpečnostného hľadiska bez:

- ochrany dôvernosti,
- ochrany integrity,
- možnosti overiť si totožnosť odosielateľa (autenticitu).

6.1.1 Účel šifrovania / dešifrovania pri používaní elektronickej pošty

Na zabezpečenie dôvernosti informácií prenášaných správami elektronickej pošty sa používa asymetrické šifrovanie (viď. časť 1.4.3 tohto modulu).

Pre používanie asymetrického šifrovania potrebujeme zabezpečiť dôveryhodnú distribúciu verejných kľúčov. V súčasnosti sú najrozšírenejšie dva systémy:

- S/MIME – používa X.509 certifikáty (ako SSL/TLS pri HTTPS), je podporované väčšinou e-mailových klientov,
- PGP – ľudia si navzájom vymieňajú kľúče, vzniká „ad-hoc sieť dôvery“ medzi používateľmi.

Nakoľko štandardné protokoly pre komunikáciu s poštovými servermi (SMTP, POP3, IMAP) využívajú textový formát, nie je problém pre prípadných útočníkov odpočúvať komunikáciu. Túto otvorenú komunikáciu môžeme chrániť podobne, ako pri HTTP protokole pri webových stránkach, používaním SSL/TLS šifrovania.

6.1.2 Digitálny podpis

Na zabezpečenie integrity a autentickosti správy posielanej elektronickou poštou sa používa elektronický (digitálny) podpis. Digitálny podpis súvisí s asymetrickou kryptografiou (viď. 1.4.3).

Odosielateľ na pripravenú správu použije tzv. hashovaciu funkciu a vytvorí tzv. hash (kontrolný súčet). Ide o reťazec znakov pevnej dĺžky, ktorý je závislý od obsahu dokumentu. Dobrá hashovacia funkcia má tieto dve hlavné vlastnosti:

- je jednosmerná (z výsledného hashu sa spätne nedá odvodiť obsah),
- neexistujú dva rôzne súbory (správy) s rovnakým hashom.

Hash správy sa následne zašifruje súkromným kľúčom odosielateľa a toto celé sa ako jeden súbor pripojí ako príloha k správe. Digitálny podpis je vlastne zašifrovaný hash obsahu pomocou súkromného kľúča.

Príjemca správy spracuje prílohu, pomocou verejného kľúča odosielateľa dešifruje hash a prečíta jeho typ. Následne rovnakým spôsobom, ako odosielateľ, vytvorí hash prijatej správy. Ak sú obidva hashe rovnaké, správa nebola menená, teda jej integrita bola zachovaná.

Dôležité je aj overiť si verejný kľúč odosielateľa, čím sa potvrdí autenticita správy.

6.1.3 Možnosť obdržania podvodnej a nevyžiadanej správy elektronickej pošty

Nevyžiadaná správa (SPAM), je taká, o ktorú príjemca nemá záujem. Môže ísť napr. aj o reklamné letáky v poštovej schránke, nevyžiadané SMS-ky, no v súčasnosti ide najmä o nevyžiadané správy elektronickej pošty obsahujúce spravidla reklamu. Väčšinou ide o hromadne rozosielané správy s takmer rovnakým obsahom.

Hlavnými problémami SPAM-u sú zapĺňanie schránok elektronickej pošty príjemcov, preťažovanie poštových serverov a zbytočné zvyšovanie objemu prenášaných údajov na internete. Podľa odborných odhadov celosvetovo SPAM v súčasnosti tvorí okolo 90% z celkového objemu elektronickej pošty. Ochrana proti SPAM-u je komplikovaná, pretože je veľmi ťažké odlíšiť SPAM od užitočných správ. Najčastejšie sa realizuje na úrovni servera, ktorý SPAM automaticky vyraďuje alebo ich presúva do priečinka SPAM (Nevyžiadaná pošta). Pri tomto systéme sa darí zachytiť väčšinu nevyžiadanej pošty, ale niektoré užitočné správy môžu byť omylom označené za podozrivé alebo SPAM, na druhej strane sa do priečinka Doručená pošta môžu dostať nežiaduce správy. Preto sa väčšinou dá správu v priečinku Doručená pošta označiť ako nevyžiadanú, a naopak, správu v priečinku Nevyžiadaná pošta označiť ako korektnú. Tým môžeme antispamovému systému upraviť pravidlá pre hodnotenie správ a zvýšiť jeho efektivitu.

Nevyžiadanú správu rozpoznáme hlavne podľa odosielateľa (emailovej adresy). Adresy z neznámych domén alebo od neznámych užívateľov sú väčšinou SPAMom. O tom či niečo je alebo nie je SPAM však rozhoduje samotný obsah správy.

Časť z nevyžiadanej pošty tvoria podvodné správy. Podvodná správa je taká, ktorá sa snaží uviesť príjemcu do omylu a tým získať pre jej tvorcu nejaký prospech. Zámerne sme použili výraz tvorca správy, pretože odosielateľ (aspoň ten, ktorý je uvedený v správe) je spravidla falošný. Podvodné správy veľmi často obsahujú malware v prílohách, prípadne sa snažia získať prihlasovacie údaje (tzv. phishing).

6.1.4 Čo je phishing, jeho charakteristické znaky (zneužívanie oficiálnych názvov firiem, osôb, používanie odkazov na falošné webové stránky, zneužívanie zavedených log a značiek, povzbudzovanie k odkrytiu osobných informácií)

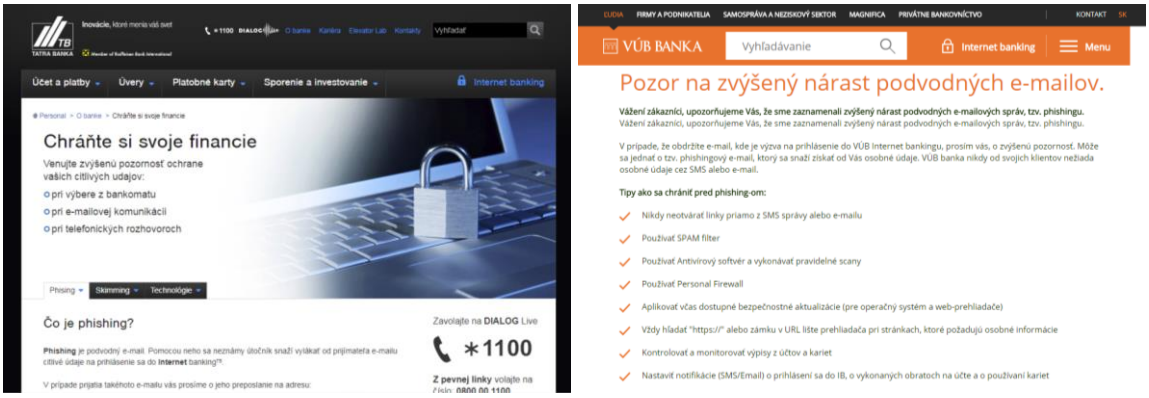
Phishing (z anglického password fishing – doslova rybolov hesiel) je činnosť, pri ktorej sa podvodník snaží vylákať od používateľa prístupové údaje, napr. k elektronickej pošte, do internetbankingu, k platobnej karte a pod.

Väčšinou takéto podvodné správy sa snažia dostať príjemcu do neštandardnej situácie. Napr. správca servera chce riešiť problém s Vašim e-mailovým kontom, banka oznámi zablokovanie Vášho bankového účtu, organizátor lotérie Vám oznamuje výhru a chce Vám ju odovzdať, nešťastná vdova Vás žiada o pomoc pri prevode dedičstva z nejakej rozvojovej krajiny do Európy a pod. Pri snahe o riešenie takejto situácie sa pokúsia získať prístupové údaje buď priamo vyžiadaním v správe (správca servera potrebuje na riešenie problému s Vašim e-mailovým kontom Vaše prihlasovacie údaje), odkazom na falošnú stránku (aby ste sa hneď prihlásili do Vašej banky). V prípade, že zareagujete na správu, napr. o výhre, postupne Vám napíšu čo všetko potrebujú pre odovzdanie výhry, a nakoniec môžu žiadať buď prihlasovacie údaje do Vašej banky, alebo úhradu nejakého poplatku (napr. dane z výhry) aby Vám mohli výhru vyplatiť. Samozrejme, na Vašom účte pribudne len nejaké mínus.

6.1.5 Možnosť ohlásenia pokusov o phishing organizáciám, v ktorých mene útočník pôsobí

Pokusy o phishing je možné nahlásiť organizáciám, v ktorých mene útočník vystupuje. Ideálne je kontaktovať priamo organizáciu a upozorniť ich na danú skutočnosť.

Napr. bankové subjekty, ktoré pôsobia na Slovensku majú prostredníctvom svojich webových sídiel možnosť nahlásenia pokusov o phishing zo strany používateľov prostredníctvom kontaktných formulárov alebo priamo zavolaním na kontaktné telefónne čísla (Obrázok 1).



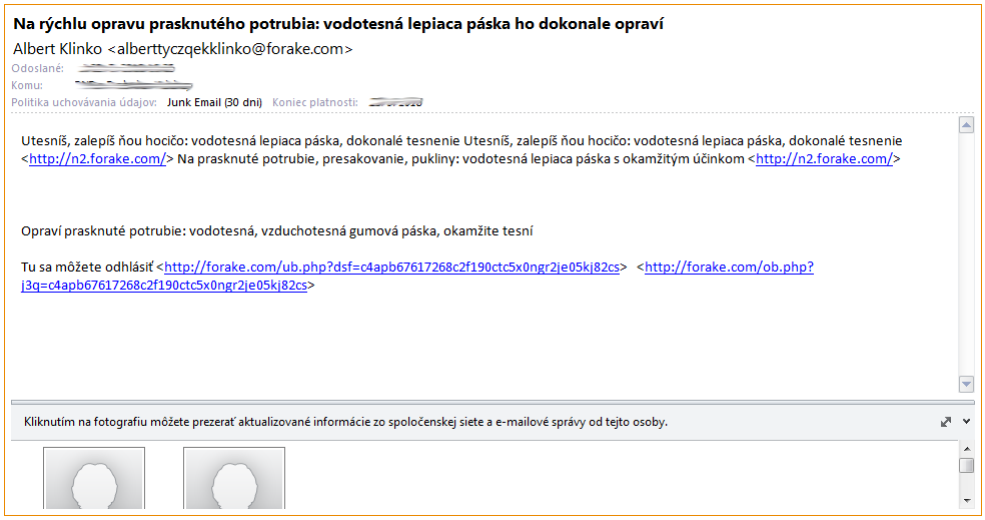
Obrázok 1: Phishing a bankové subjekty

6.1.6 Nebezpečenstvo nákazy počítača škodlivým softvérom pri otvorení prílohy elektronickej pošty, ktorá obsahuje makro alebo spustiteľný súbor

Účelom podvodných správ je často zavedenie malware do počítača príjemcu.

Jednou z možností je použiť v správe odkaz na stiahnutie infikovaného súboru. Typicky to bývajú správy, v ktorých je príjemca upozornený na kritickú chybu nejakého softvéru, a výrobca mu posiela odkaz na aktualizáciu, ktorá túto chybu odstráni. Namiesto aktualizácie si príjemca správy nainštaluje malware.

Druhou možnosťou je poslanie správy s infikovanou prílohou. Bývajú to najmä spustiteľné súbory maskované ako (obrázky a pod.), ale aj dokumenty s makrami (pozvánka, prezentácia, tabuľka s automatickým prepočtom položiek, ...). Najväčšou hrozbou pre používateľa je nastavenie automatického otvárania príloh, keď otvorením správy sa otvorí príloha, čím sa spustí malware a nainfikuje počítač.



Obrázok 2: Nevyžiadaná pošta – možný zdroj nákazy počítača

6.2 Sociálne siete

Európska agentúra pre informačnú a sieťovú bezpečnosť za sociálnu sieť považuje on-line komunitu, ktorá pomocou vytvoreného profilu umožňuje používateľom stretávať ďalších členov siete, komunikovať s nimi, zostať s nimi v kontakte a zdieľať s nimi obrázky a video v rámci zdieľaného priestoru. Iná definícia sociálnej siete je webová služba, ktorá umožňuje používateľom:

1. vytvoriť verejný alebo poloverejný profil v rámci uzatvoreného systému,
2. vytvoriť a editovať zoznam ďalších používateľov, s ktorými udržiavajú spojeniepozorovať a komentovať činnosť ostatných používateľov v rámci systému.

6.2.1 Dôležitosť neuvádzania dôverných informácií na stránkach sociálnych sietí

Ľudia často zverejňujú zneužiteľné osobné informácie, napr. fotografie, časové plány, osobné údaje. Neuvedomujú si, kto všetko k nim má prístup a čo všetko sa z nich dá zistiť a zneužiť.

Príklady sociálnych sietí: Facebook, LinkedIn, XING, Twitter.

Asi najrozšírenejšia sociálna sieť Facebook mala mať skôr súkromný charakter. Napr. už samotný profil v porovnaní s profesionálne zameranými portálmi (napr. LinkedIn) umožňuje zadať množstvo osobných údajov (napr. dátum narodenia, rodinní príslušníci, vzťahy, politická a náboženská príslušnosť), ale súčasne umožňuje zvoliť, kto môže jednotlivé informácie vidieť (verejnosť, priatelia mojich priateľov, len priatelia, ...). Na všetkých portáloch však môžu užívatelia priradiť k svojmu profilu fotografiu, ktorá sa zobrazí verejne.

Facebook Európskej komisii (EK) potvrdil, že obeťami škandálu okolo nepovoleného získavania osobných údajov môže byť aj vyše 2,7 milióna ľudí z Európy. Facebook priznal, že škandál okolo úniku osobných údajov zasiahol 87 miliónov jeho používateľov. Najprv sa hovorilo o 50 miliónoch používateľov, ktorých osobné dáta z Facebooku neoprávnene získala spoločnosť Cambridge Analytica a následne údajne použila na ovplyvnenie amerických prezidentských volieb v roku 2016.

6.2.2 Význam vhodného nastavenia úrovne súkromia účtu na sociálnej sieti

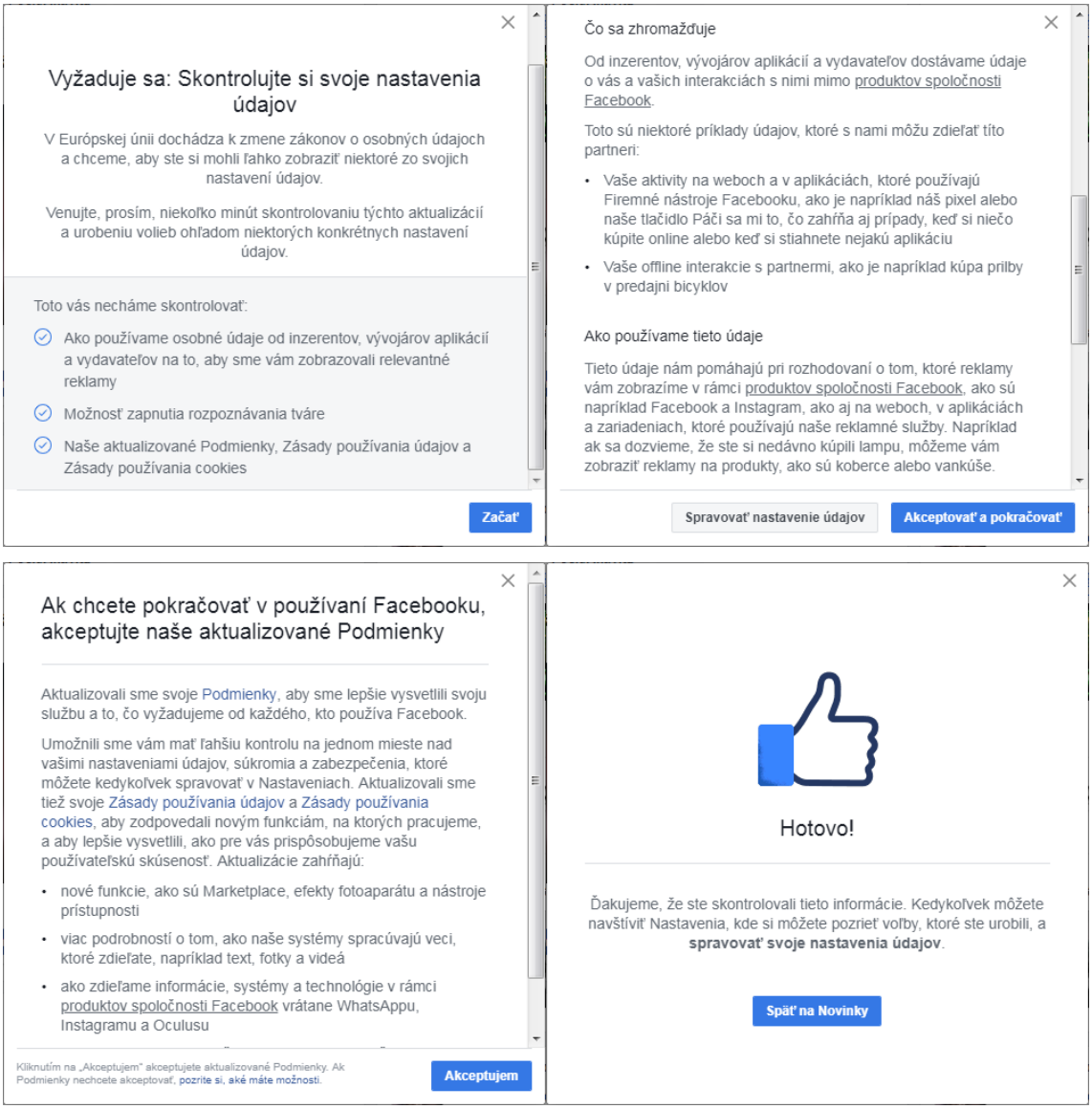
Tak, ako v skutočnom živote človek nezdieľa všetky informácie verejne, ale niektoré len v istom okruhu ľudí, tak isto, možno aj opatrnejšie, by mal narábať s informáciami, ktoré poskytuje vo virtuálnom svete sociálnych sietí. Pri (takmer) každej informácii na sociálnej sieti je možné nastaviť kto si môže zobraziť moje údaje:

- len ja,
- len moji priatelia,
- všetci,
- vlastné nastavenie

Základnou otázkou býva, či sú „moji priatelia“ (na sociálnej sieti) naozaj moji priatelia.

6.2.3 Vedieť na účte sociálnej siete nastaviť úroveň súkromia a lokalitu.

Príchod sociálnych sietí a rozvoj internetových služieb, sprevádzaný marketingovými nástrojmi si vyžiadali zmenu regulácie ochrany osobných údajov aj v IT oblasti. Od 25.5.2018 začal v Európskej únii platiť nariadenie európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR - General Data Protection Regulation). V tejto súvislosti zmenili poskytovatelia pravidlá, ktoré súvisia s nariadením. V súčasnosti (máj 2018) jedna z najrozšírenejších sociálnych sietí Facebook upravuje svoje pravidlá, v ktorých informuje používateľov o zmenách v spracovaní osobných údajov.



Obrázok 3: Nové pravidlá sociálnej siete Facebook (máj 2018)

Prijatie nových pravidiel je zväčša jednorazové, ale používateľ má možnosť na účte sociálnej siete nastaviť si kedykoľvek aj úroveň súkromia. Nastavenia, ktoré majú obmedziť prístup k zverejneným informáciám pre skupiny používateľov či jedincov.

Sociálna sieť Facebook využíva pre zobrazovanie údajov, ktoré môžete zverejniť niekoľko úrovní:

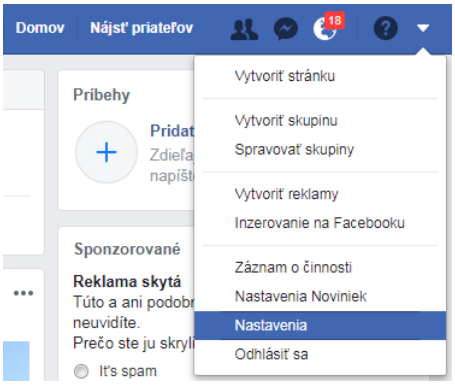
Verejné – pre kohokoľvek s účtom aj bez účtu na Facebooku = žiadne súkromie.

Priatelia, Priatelia okrem ..., Konkrétni priatelia – informácie sú dostupné pre tých, ktorých ste označili za „priateľov".

Iba ja – ochrana súkromia pre používateľov, ktorí si svoje súkromie chránia. Pri tomto nastavení, nemá okrem vlastníka nik iný prístup k zverejneným informáciám.

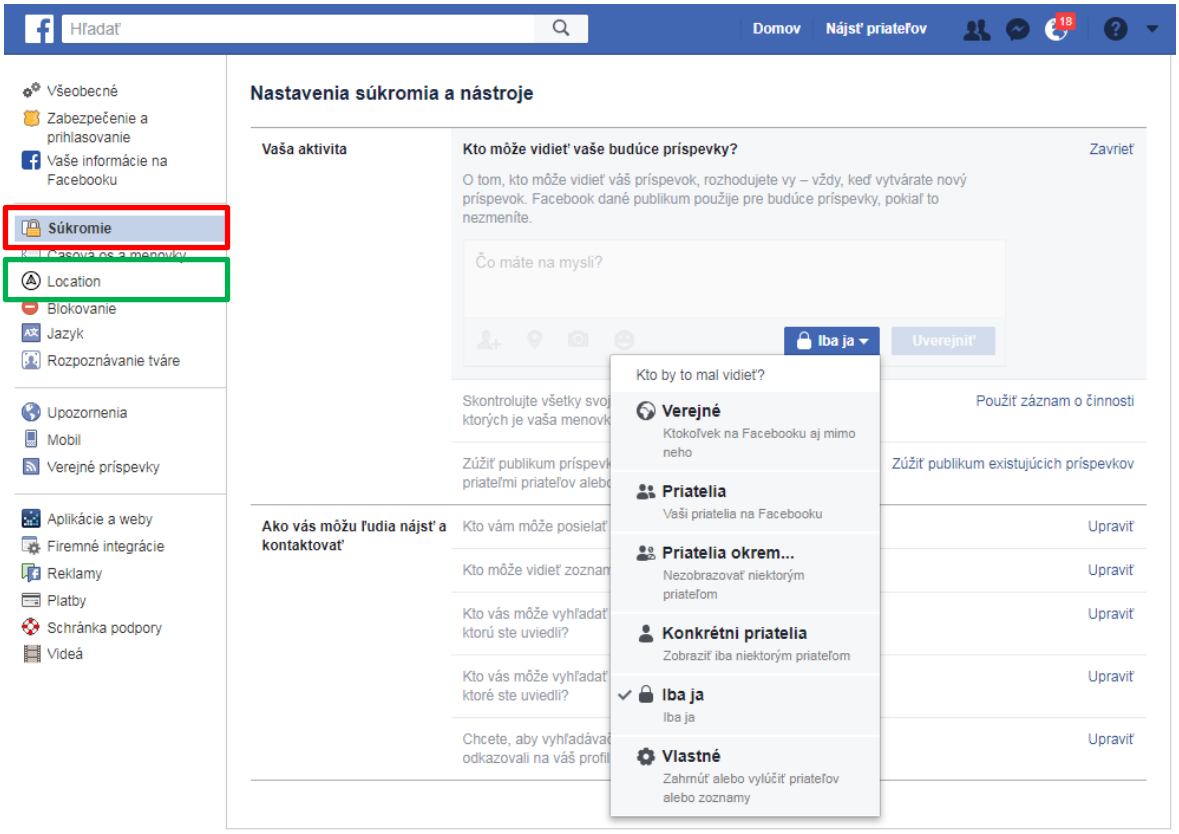
Najzložitejším, ale najlepším riešením je definovanie vlastných pravidiel pre úrovne súkromia – **Vlastné** (pre jednotlivcov, skupiny, ...).

Zmenu úrovne súkromia začneme v pravej časti, kliknutím na položku **Nastavenia** (Obrázok 4).



Obrázok 4: Zmena nastavení v sociálnej siete Facebook

Po zobrazení stránky s rôznymi nastaveniami klikneme v ľavom stĺpci na **Súkromie** (Obrázok 5).



Obrázok 5: Nastavenia súkromia v sociálnej siete Facebook

Služba Facebook vytvára aj históriu presných polôh prijatých prostredníctvom služieb určovania polohy v zariadení. Tieto nastavenia zmeníme v časti **Location**.

6.2.4 Potenciálne nebezpečenstvá spojené s používaním sociálnych sietí, ako napríklad internetové šikanovanie, vytváranie dôverného vzťahu za účelom zneužitia neplnoletej osoby (grooming), podvodným spôsobom odkrytie osobného obsahu, zavádzajúce alebo nebezpečné informácie, falošná totožnosť, podvodné odkazy alebo správy

Kyberšikanovanie (tiež kybernetická šikana, počítačová šikana) je druh šikany, špecifický tým, že je realizovaný prostredníctvom informačných a komunikačných technológií, hlavne prostredníctvom siete internetu a mobilného telefónu. Najčastejšie ide o zasielanie obťažujúcich, urážajúcich či útočných mailov a SMS, vytváranie dehonestujúcich stránok a blogov, prípadne zverejňovanie fotografií a videí s cieľom poškodenia inej osobe.

Grooming je spôsob ako si v on-line prostredí získať obeť pre neskoršie sexuálne zneužitie. Má päť fáz. Počas prvej fázy sa neskorší sexuálny agresor usiluje vybudovať dôveru k dieťaťu a snaží sa ho aj prehovoriť, aby o ich kamarátstve dieťa s nikým nehovorilo. V druhej fáze ide agresorovi o upevňovanie vzťahu, získavanie osobnejších informácií a získanie si dieťaťa prostredníctvom rôznych darčekov – nabitia kreditu mobilného telefónu či posielanie bonusov do hier, ktoré dieťa rado hrá. V tretej fáze sa už začína snaha o vyvolanie emocionálnej závislosti a vyvolanie dojmu, že je jediný, komu sa môže kedykoľvek zdôveriť. Štvrtá fáza nastáva, keď agresor si je istý závislosťou obete na ňom, nebojí sa odhalenia svojej identity pred ňou a pozve ju na lákavé stretnutie, napr. návštevu kina či koncertu. V piatej fáze už dochádza k sexuálnemu zneužitiu aj pod nátlakom (napr. už nebudeme kamaráti, zverejním tvoje fotky či videá, ukážem ich kamarátom, rodičom alebo učiteľom).

Falošná totožnosť/identita na sociálnych sieťach je dnes bohužiaľ bežný jav. Veľkou skupinou sú maloletí, ktorí si chcú vytvoriť účet na sociálnej sieti a nespĺňajú podmienku minimálneho veku. A už keď uviedli iný vek, tak si vymyslia iné meno a naplnia profil nepravdivými informáciami. Ďalšia skupina sú osoby, ktoré potrebujú komunikovať na sociálnej sieti, ale nemajú záujem vyzradiť vlastnú identitu, tak použijú vymyslenú. V oboch prípadoch nastáva problém ak použijú identitu inej fyzickej osoby, prípadne svojou falošnou identitou zavádzajú iných používateľov sociálnej siete.

Falošná identita sa veľmi často zneužíva na šírenie nepravdivých informácií. Ak niekto používa identitu známej a slávnej osoby, môže v jej mene šíriť rôzne informácie, ktoré nemusia mať so skutočnosťou nič spoločné, (napr. vzťahy, obľúbené značky výrobkov, zdravotný stav) a tým oklamať jej priaznivcov. V prípade firiem môže nepravdivá informácia o ich stave ovplyvniť ich obchodných partnerov, prípadne cenu ich akcií na burze. Nebezpečné môžu byť informácie oznamujúce kritické chyby programov, ktoré namiesto na opravy odkazujú na falošné stránky obsahujúce malware.

Poplašné alebo nepravdivé informácie (tzv. hoaxy) sa šíria internetom často v dobrej viere, že neinformovaní používatelia tým pomôžu svojmu okoliu. Tu sú dva príklady poplašného a nepravdivého hoaxu.

Ukážka 1:

VAROVANIE !!!!!!! pošli všetkým

Prezídium Policajného zboru odbor dokladov a evidencií por. Ing. Juraj Solčanský tel: 096Xxxxxxx

Varovanie od firmy AGEM !!!

Prosím, pošlite túto správu každému, kto má prístup k internetu. Môžete dostať na prvý pohľad neškodný e-mail s prezentáciou v Power Pointe pod názvom "Life is beautiful" ("život je krásny"). Pokiaľ ju obdržíte, za žiadnu cenu prezentáciu NEOTVÁRAJTE a okamžite ju vymažte. Pokiaľ ju otvoríte, na vašej obrazovke sa ukáže správa: "It is too late now, your life is no longer beautiful." ("Už je príliš neskoro, teraz váš život už nie je krásny").

Následne STRATÍTE VŠETKO vo vašom PC a osoba, ktorá vám toto zaslala, získa prístup k vášmu menu, emailu a heslu.

Toto je nový vírus, ktorý vstúpil do obehu v sobotu poobede. AOL už potvrdil, že je to vážne a že antivírové programy nie sú schopné tento vírus zničiť. Vírus bol vyrobený hackerom, ktorý si hovorí "life owner".

Prosím, pošlite túto správu všetkým vašim priateľom a požiadajte ich, aby ju čo najrýchlejšie poslali ďalej.

Prajem pekný deň

Ukážka 2:

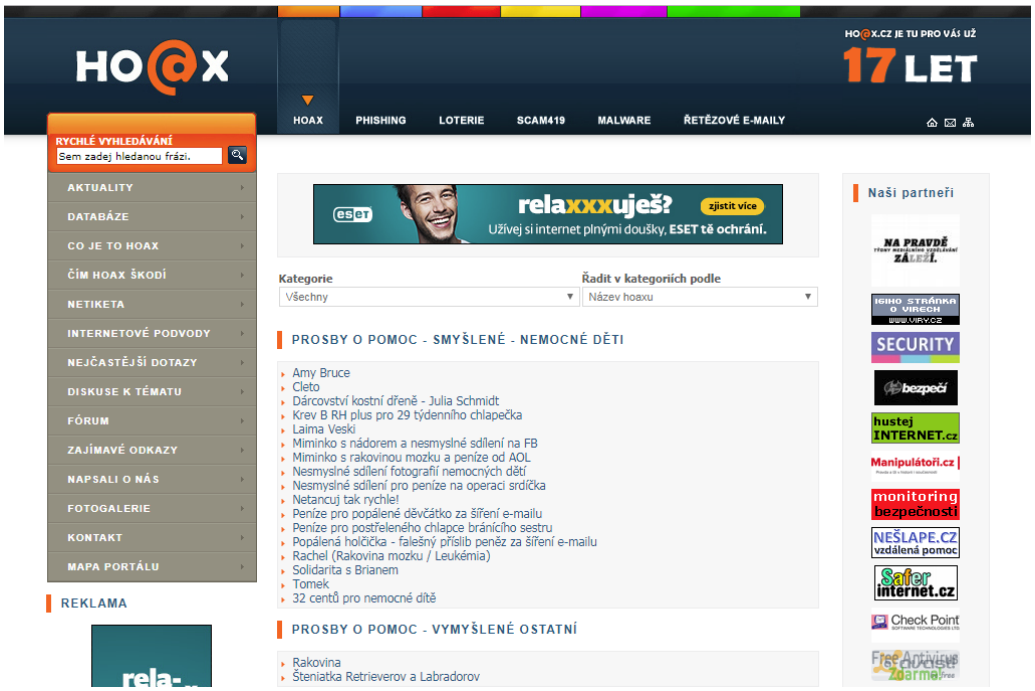
Akonáhle sa ocitnete v situácii, kedy ste prinútení násilníkom a musíte pod nátlakom vybrať peniaze z bankomatu, zadajte svoje PIN opačne: tzn. od konca - napr. ak máte 1234, tak zadáte 4321 a bankomat vám peniaze síce vydá, ale tiež súčasne privolá políciu, ktorá vám príde na pomoc. Tato správa bola prednedávnom vysielaná v TV, napriek tomu ju využili doposiaľ len 3 ľudia, pretože sa o tejto skutočnosti medzi ľuďmi nevie. Prepošli to čo najviac ľuďom.

Ukážka 3:

Subject: FW: Dôležité upozornenie

V týchto dňoch koluje na internete vírus, ktorý sa aktivuje otvorením prílohy. Nesie meno " Bobak", " Bobačik a pod." Prosím upozorni aj ostatných, ak príde správa s takýmto obsahom neotvárajte prílohu a okamžite ju vymažte ! Pri otvorení mailu sa program dokáže v počítači aktivovať za cca 1 min. a vymaže všetky súbory. Nakoniec sa na obrazovke zobrazí foto Bin Ladina čím je všetko vymazané. Pravdepodobne ide o nový druh vírusového pirátstva na ktorý sú ochranné systémy počítačov málo odolné. Verím, že si zachránite aj Vaše počítače. Mnoho ich už dnes na Slovensku padlo.

V súčasnosti je vhodné overiť si dôveryhodnosť správy a neprispievať k šíreniu SPAMu na internete. Hoaxové správy jednoducho skontrolujete na českej stránke hoax.cz (Obrázok 6)



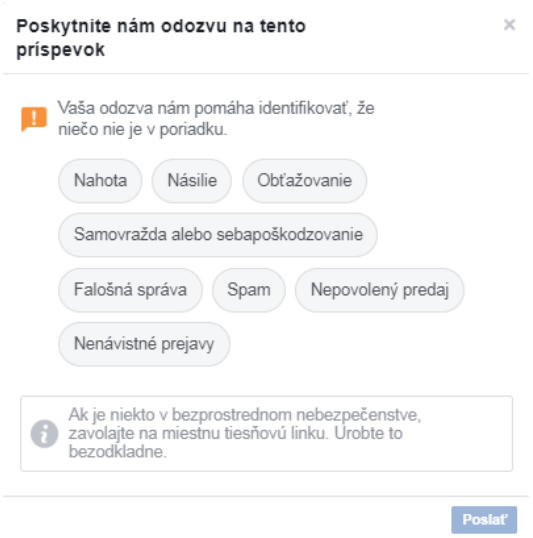
Obrázok 6: Stránka venujúca sa HOAXu

6.2.5 Možnosť ohlásenia nevhodného využívania sociálnej siete alebo nevhodného správania sa poskytovateľovi služby alebo zodpovedajúcim úradom

Nevhodné využívanie sociálnej siete je možné nahlásiť priamo prevádzkovateľovi (viď. pravidlá prevádzky konkrétnej sociálnej siete). Takisto je možné nahlásiť túto skutočnosť úradom, nakoľko je však internet geograficky neobmedzená sieť, je veľmi ťažké zvoliť vhodný úrad konkrétnej krajiny.

Napr. sociálna sieť Facebook obsahuje časť, ktorá umožní ľuďom nahlásiť príspevky a konverzácie, ktoré porušujú štandardy komunity. Reaguje tým na požiadavky používateľov (Obrázok 7).

Zaujímavou položkou je Nepovolený predaj, ktorý poukazuje na rastúce využitie nástrojov sociálnych sietí na nelegálne transakcie tohto charakteru.



Obrázok 7: Facebook - Odozva na príspevok

6.3 VoIP a komunikácia v sieti v reálnom čase (Instant Messaging, IM)

Na rozdiel od elektronickej pošty, kde sa nepredpokladá súčasné pripojenie komunikujúcich osôb, sa to v prípade komunikácie v reálnom čase zväčša vyžaduje, hlavne ak ide o multimediálnu komunikáciu (hovor alebo videohovor). Medzi najznámejšie služby patrí Skype (Microsoft), Telegram, Whatsapp (Facebook) a ďalšie.

6.3.1 Bezpečnostné hrozby pri komunikácii v sieti v reálnom čase (instant messaging, IM) a komunikácii Voice over IP (VoIP)

Jedným z možných problémov pri používaní IM je úroveň zabezpečenia komunikácie medzi klientskym programom a serverom. Mnohé z nich používajú vlastné komunikačné protokoly, u ktorých môže byť problematické posúdiť úroveň ochrany komunikácie a možnosti prípadného odpočúvania.

Vzhľadom na množstvo rôznych systémov pre IM je pomerne veľké riziko výskytu chýb, ktoré môžu byť zneužité, napr. pre neoprávnený prístup do počítača. V prípade útoku typu „zadné vrátka“ sa útočník môže dostať k údajom uloženým na počítači.

Podobne, ako pri ohrození infikovanou prílohou v správe, môže byť ohrozený používateľ IM pri prijatí infikovaného súboru. Nebezpečnejšie je to v tom, že súbor v IM väčšinou posiela dôveryhodná osoba, ktorú má používateľ vo svojom zozname kontaktov, takže príjemca má voči odosielateľovi súboru väčšiu dôveru než voči neznámemu odosielateľovi správy elektronickej pošty.

6.3.2 Spôsoby zabezpečenia dôverných informácií pri komunikácii v sieti v reálnom čase a pri VoIP

V IM, podobne ako v sociálnych sieťach, sa môžu do používateľského profilu zadať aj citlivé informácie. Našťastie, podobne ako v sociálnych sieťach, aj tu si pri informáciách zadávaných do profilu môžeme vybrať komu sa môžu zobraziť.

Aby sme zabezpečili dôvernosť citlivých informácií, mali by sme použiť šifrovanie. Napríklad stačí súbory s citlivými informáciami skomprimovať, komprimovaný súbor zabezpečiť heslom, a heslo poslať príjemcovi iným informačným kanálom (napr. v SMS-ke).

Ideálne by bolo mať šifrovanú celú komunikáciu, nie len súbory. Z vyššie uvedených (a asi najrozšírenejších) IM systémov jedna polovica nepodporuje šifrovanú komunikáciu, druhá polovica to deklaruje, ale neposkytuje informácie o použitom type šifrovania.

6.4 Mobilné zariadenia

Dnešné mobilné telefóny (tzv. smartfóny) majú bližšie k počítačom, ako k niekdajším mobilným telefónom. Tak ako počítače, aj telefóny sa pripájajú na sieť, inštaluje a spúšťa sa na nich softvér tretích strán a teda k nim treba pristupovať tak ako počítačom aj čo sa týka bezpečnosti.

6.4.1 Dôsledky používania aplikácií z neoficiálnych obchodov (mobilný škodlivý softvér, zbytočné vyťažovanie zdrojov, neoprávnený prístup k osobným údajom, nízka kvalita produktu, skryté náklady počas využívania produktu)

Tak ako aj pri bežnom počítači, aj pri mobilných aplikáciách je dôležité neinštalovať aplikácie z neoficiálnych zdrojov ale z overených obchodov mobilných aplikácií. Problémom je však to, že na mnohých obchodoch nedochádza k dôslednej kontrole softvéru a nakoľko do týchto obchodov nahrávajú softvér tretie strany (v zmysle nie výrobca telefónu alebo operačného systému), aj aplikácia z oficiálneho obchodu môže obsahovať malware. Pri riešení tohto problému môžu pomôcť užívateľské recenzie na daný softvér.

Špecifickým problémom spojeným s používaním mobilných aplikácií (ale nie len) môže byť aj to, že aplikácia sa dá nainštalovať bezplatne, ale rôzne finančné výdavky sú spojené s jej používaním.

Ďalším problémom, ktorý sa rozšíril s príchodom smartfónov a ktorý pomaly prestupuje aj svetom osobných počítačov je to, že aplikácie často pre svoj beh vyžadujú prístup k niektorým dátam (aj keď by sa to na prvý pohľad nemuselo zdať potrebné).

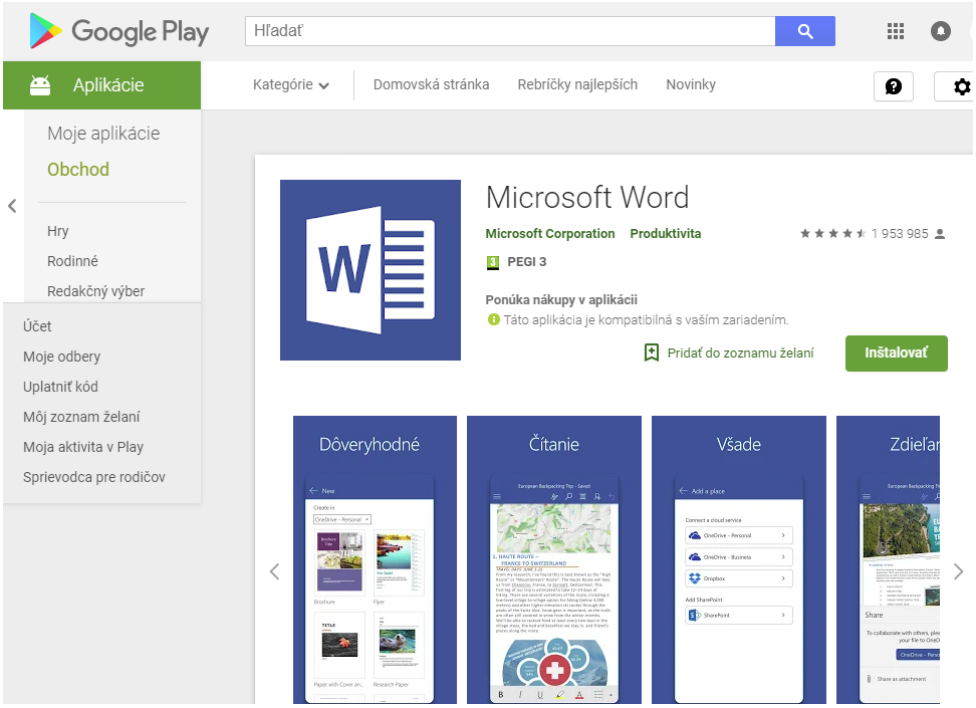
6.4.2 Oprávnenia aplikácií

Veľký problém, ktorý sa rozšíril s príchodom smartfónov a ktorý pomaly prestupuje aj svetom osobných počítačov je, že aplikácie často pre svoj beh vyžadujú prístup k niektorým dátam, aj keď by sa to na prvý pohľad nemuselo zdať potrebné. Pri inštalácií mobilných aplikácií by mal byť používateľ vopred upozornený na tieto požiadavky a má teda možnosť si premyslieť, či takúto aplikáciu chce alebo nie. V prípade inštalácie takýchto aplikácií hrozí, že aplikácia získa prístup k dátam ako detaily kontaktov, história prehliadača, fotografie a podobne.

6.4.3 Získavanie osobných informácií z mobilného zariadenia pomocou aplikácií (detaily kontaktov, história pohybu v lokalitách, a podobne)

Mobilná aplikácia by nemala zhromažďovať žiadne osobné údaje o používateľovi. Pre skvalitnenie dostupných informácií môže zhromažďovať iba neadresné štatistické dáta, napríklad ktoré kategórie používatelia preferujú, alebo ktorý operačný systém mobilného zariadenia je najviac používaný. Tieto štatistické dáta môžu byť využité pri ďalšom vývoji aplikácie, ale používateľ by mal byť vždy informovaný čo a na aký účel sa získava. Získané osobné informácie nesmú byť poskytované žiadnym iným subjektom

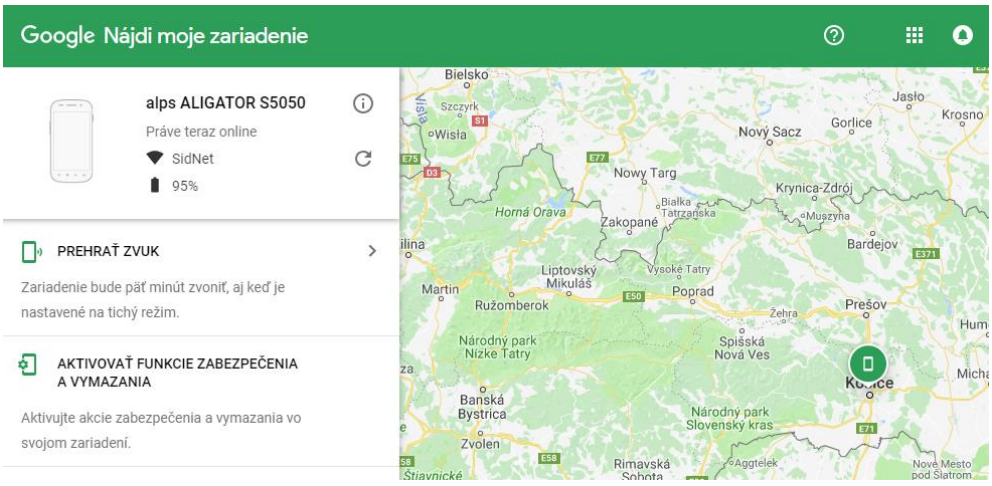
bez vedomia používateľa. Pri inštalácii aplikácie si preto všímajme k akým údajom chce inštalovaná aplikácia získať prístup.



Obrázok 8: Obchod Google Play

6.4.4 Núdzové bezpečnostné opatrenia pri strate zariadenia (deaktivácia zariadenia na diaľku, vymazanie údajov zo zariadenia na diaľku, lokalizácia zariadenie)

Výrobcovia niektorých operačných systémov pre mobilné zariadenia implementovali do týchto systémov možnosť na diaľku telefón uzamknúť, vymazať všetky dáta (uviesť systém do továrenského nastavenia) alebo lokalizovať zariadenie. Tieto funkcie fungujú však iba ak je cieľové (stratené) zariadenie pripojené na Internet - možnosti týchto nástrojov sú teda obmedzené - napriek tomu však táto funkcia môže byť užitočná (Obrázok 9).



Obrázok 9: Lokalizačná služba Google

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.