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)

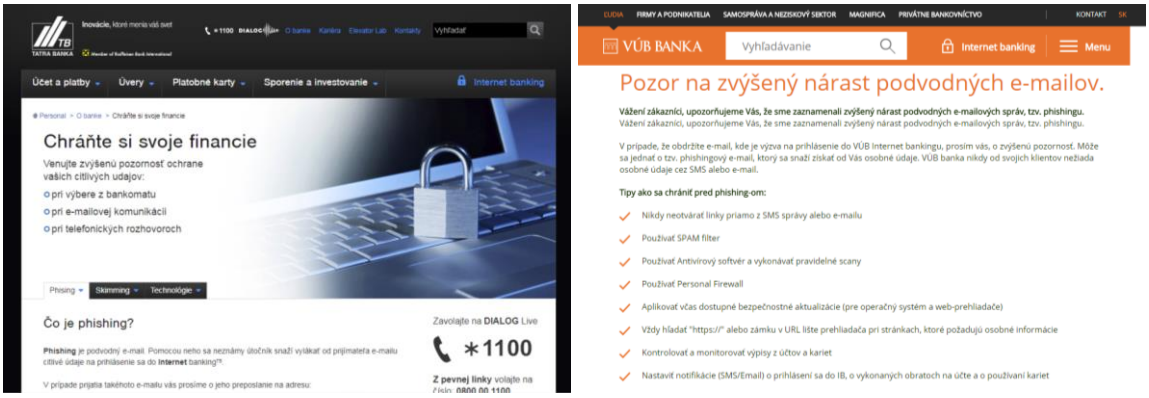
Phishing (z anglického password fishing – doslova rybolov hesiel) je činnosť, pri ktorej sa podvodník snaží vylákať od používateľa prístupové údaje, napr. k elektronickej pošte, do internetbankingu, k platobnej karte a pod.

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).



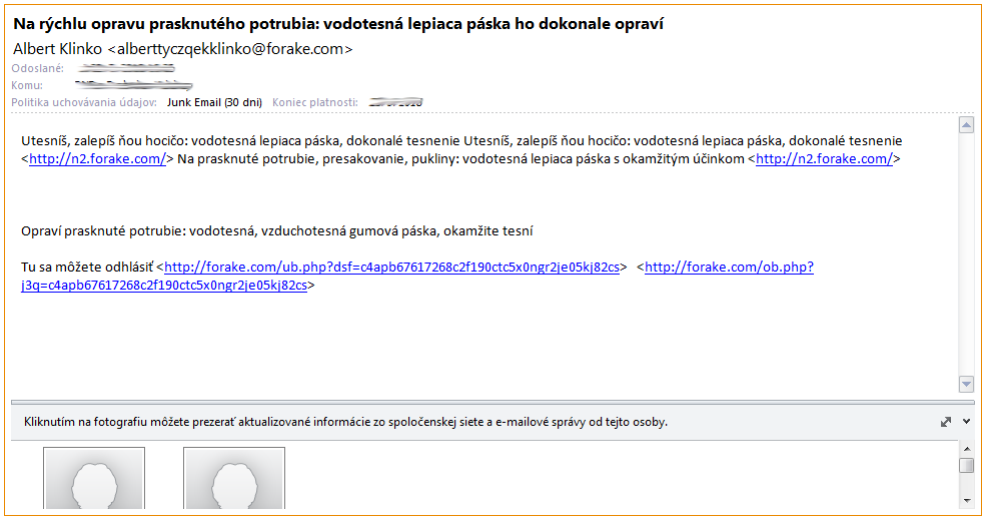
Obrázok 1: Phishing a bankové subjekty

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

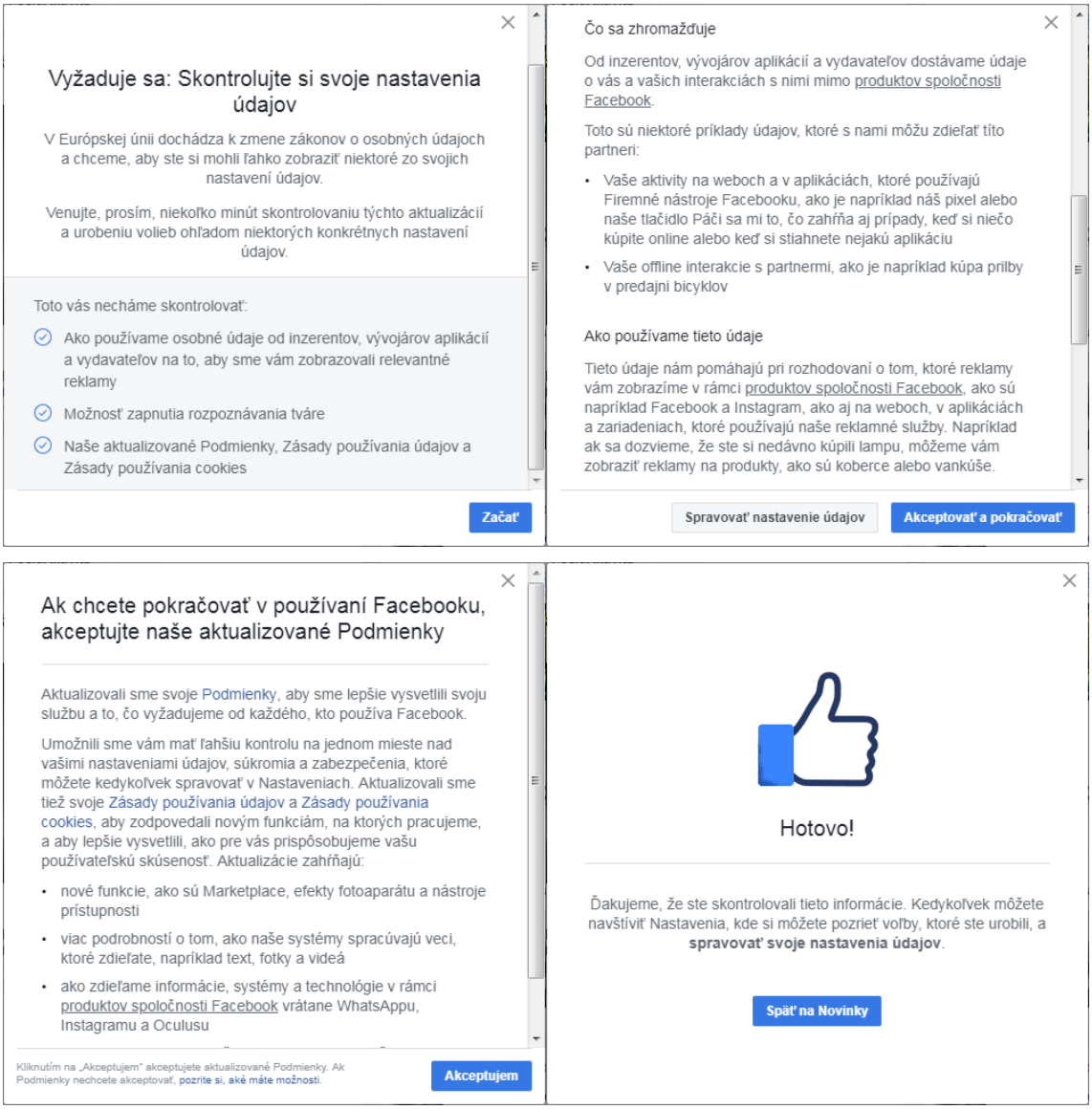
Tak, ako v skutočnom živote človek nezdieľa všetky informácie verejne, ale niektoré len v istom okruhu ľudí, tak isto, možno aj opatrnejšie, by mal narábať s informáciami, ktoré poskytuje vo virtuálnom svete sociálnych sietí. Pri (takmer) každej informácii na sociálnej sieti je možné nastaviť kto si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

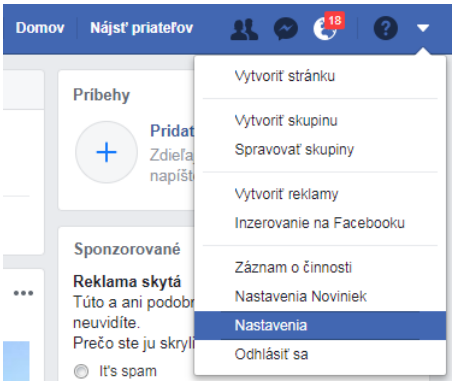
Verejné – pre kohokoľvek s účtom aj bez účtu na Facebooku = žiadne súkromie.

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.

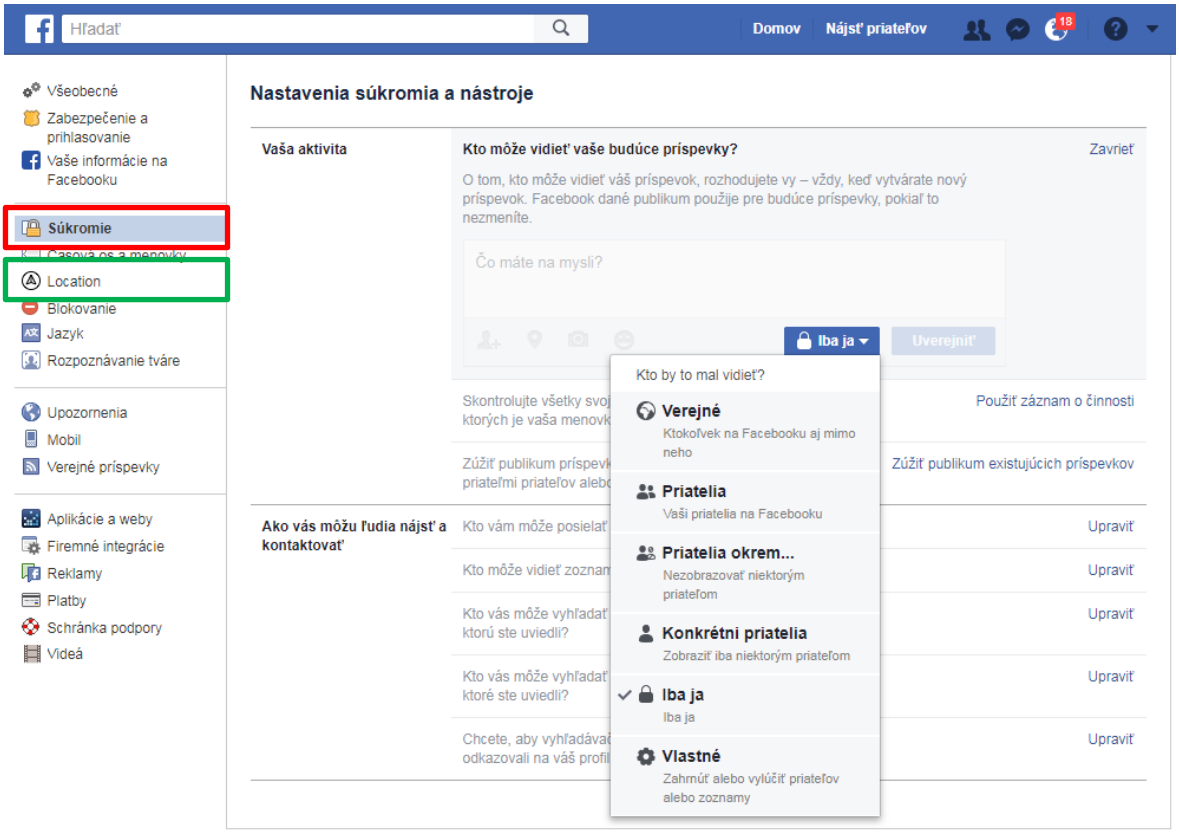
Najzložitejším, ale najlepším riešením je definovanie vlastných pravidiel pre úrovne súkromia – **Vlastné** (pre jednotlivcov, skupiny, ...).

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:

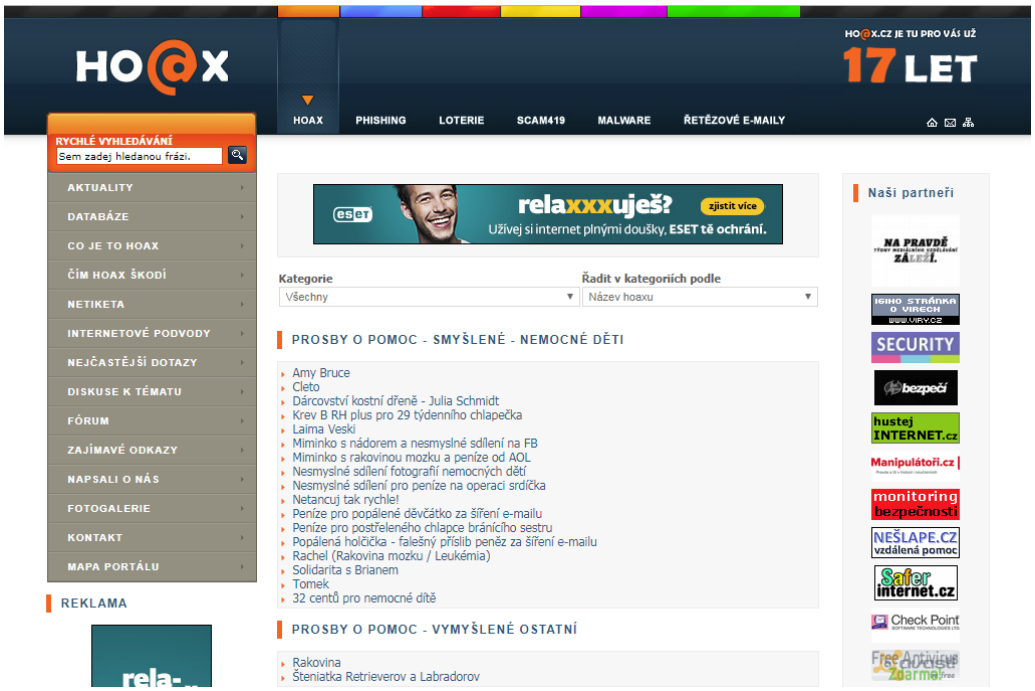
Akonáhle sa ocitnete v situácii, kedy ste prinútení násilníkom a musíte pod nátlakom vybrať peniaze z bankomatu, zadajte svoje PIN opačne: tzn. od konca - napr. ak máte 1234, tak zadáte 4321 a bankomat vám peniaze síce vydá, ale tiež súčasne privolá políciu, ktorá vám príde na pomoc. Tato správa bola 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)



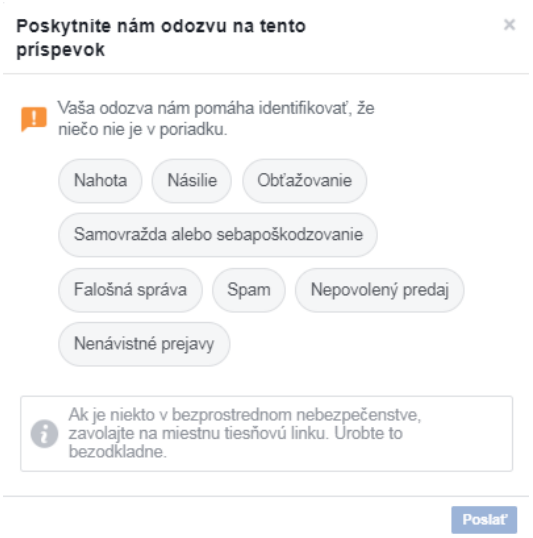
Obrázok 6: Stránka venujúca sa HOAXu

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).

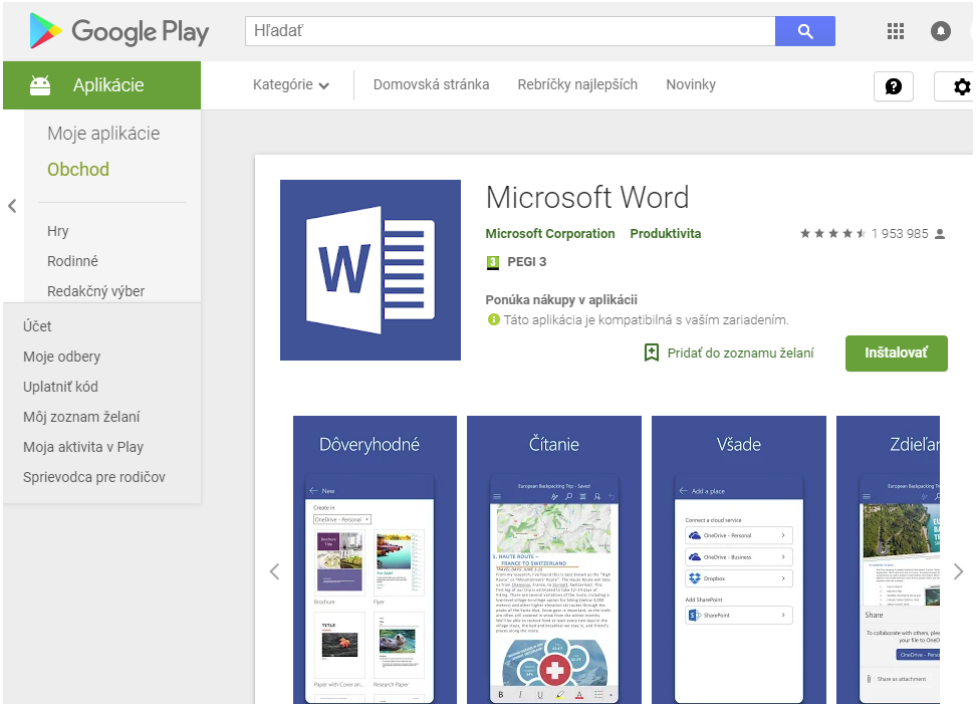
6.4.2 Oprávnenia aplikácií

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

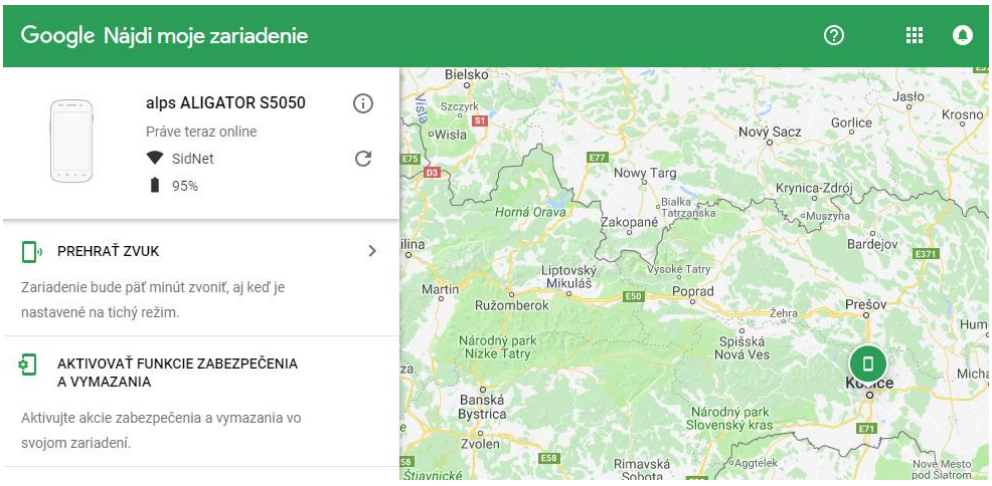
bez vedomia používateľa. Pri inštalácii aplikácie si preto všímajme k akým údajom chce inštalovaná aplikácia získať prístup.



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