Internetové podvody

Velká příručka anti-spywaru

Dnes jste počestným občanem, ale zítra už můžete být považován za zloděje. Vaše konto by mohlo být již zítra prázdné. Pokud internetoví zločinci ukradnou vaše data, jste v pěkné bryndě. Braňte se!

Daniel Behrense, Michal Bareš

Vymahači inkasa za dveřmi, soudní rozsudek v poštovní schránce a každý den nadávky v telefonu. Jako oběť krádeže identity máte na krku pěkný problém. Pro Marka K. (jméno bylo pozměněno) začala tato noční můra před dvanácti týdny. Telefonovali mu rozzuření uživatelé Ebaye, kteří se úspěšně účastnili aukcí, zaplatili, ale pak žádné zboží nedostali. Jako nabízející byl uveden Marek K. Jenže on žádný účet na Ebay nemá. To mu však podvedení uživatelé nevěří a podávají na něj trestní oznámení. Podvodník, na jehož konto peníze převedli, je dávno za kopečky. Pomocí zfalšovaného průkazu se mu povedlo otevřít si bankovní konto na cizí jméno.

Účet na Ebay na falešné jméno

Jak si mohl založit účet na cizí jméno? Úplně jednoduše: oběť před časem bez většího přemýšlení umístila na svoji webovou stránku životopis - včetně adresy a data narození, jak to bývá běžné. A přesně tato data stačí, aby si člověk mohl na Ebay otevřít konto. Marek K. nebude nakonec muset materiální škody uhradit. Ale celý příběh ho stál velké množství času a nervů.

Stav konta: minus osmdesát tisíc

O mnoho lépe to nedopadlo ani v případě Petra M. (jméno změněno). Nevěřil svým očím, když se na výpisu z jeho konta objevila částka minus 80 000 Kč. Co se stalo? Matně si vzpomínal, že před několika dny dostal od své banky e-mail, ve kterém ho prosili, aby jako dodatečné bezpečnostní opatření vyplnil tajnou otázku pro on-line bankovnictví. Kliknul na odkaz obsažený v e-mailu a zadal požadovaná data, včetně čísla účtu, PIN a jako potvrzení TAN (číslo transakce). Webová stránka vypadala úplně stejně jako ta, kterou používá jeho banka, takže nepojal žádné podezření. Ve skutečnosti se však jednalo o přesnou kopii s velmi podobně znějící webovou adresou, kterou založili podvodníci. Několik minut poté, co Petr M. zadal data, toho jeden z podvodníků využil a vyprázdnil jeho konto - nebál se ani využít celý kontokorent. Když Petr M. krádež objevil a informoval banku, účet podvodníků již neexistoval. Peníze byly pryč.

Jak se v podobném případě zachovat

Co dělat, pokud se stanete obětí takovýchto podvodníků? Jako první byste měli uvědomit provozovatele služby, v prvním případě Ebay, ve druhém vaši banku. Pak byste měli podat trestní oznámení na policii. Kontakt na Ebay najdete na www.ebay.de/kontakt. Zvolte "Sdělení o problémech s ostatními účastníky Ebay, přestupky ohledně kontaktních dat/identita" a poté "Někdo používá moje jméno a mojí adresu". Klikněte na "Dále" a na další stránce na "e-mail". Zde se dostanete k formuláři. Váš e-mail bude zaslán pracovníkům, specializovaným na takovéto případy. Ebay slibuje: "Pokud nám bude hodnověrně nahlášeno zneužití identity, budeme postiženého či postižené v rámci našich možností jako provozovatele aukcí podporovat, jak nejlépe budeme moci". V takových případech se údajně úzce

spolupracuje s vyšetřujícími úřady, kterým se předávají "v rámci právních předpisů" všechny potřebné informace.

Tipy a triky proti on-line podvodu

Abyste zůstali ušetřeni podobných hororových scénářů, nabídneme vám několik tipů, jak se můžete proti podvodům na internetu efektivně bránit. Ať už se jedná o trojské koně, phishing, krádež dat z osobních stránek, z internetové kavárny nebo z firemní sítě - ukážeme vám, v čem spočívá nebezpečí a co proti němu podniknout.

Trojské koně

Co jsou trojské koně už asi víte: škodlivé programy, které se tváří jako užitečný software. Dříve škodily především ničením dat. Dnes se ale jedná stále častěji o jejich krádeže.

Trojané: ochraňte si počítač

Svůj počítač byste měli co nejvíce izolovat. Jako soukromý uživatel sotva chytíte nějakého specifického trojana (viz strana XX), který by měl jako cíl přímo vás. Existuje však nepřeberné množství nespecifických trojanů, kteří slídí po osobních datech. Tito škůdci se často rádi vyskytují ve spojení s velkými událostmi. Takový byl například mailworm, který předstíral, že pochází od FIFA a tvrdil, že jeho příloha obsahuje důležité informace ohledně nákupu vstupenek. Kupodivu dost lidí, kteří si vstupenky skutečně chtěli koupit, osudnou přílohu otevřelo. Totéž platí pro zfalšované faktury. Kdo dostává účty on-line, dostane nejprve šok, když se ve fingovaném výpisu dočte něco o účtu za několik desítek tisíc. A pokud je neopatrný, otevře údajný důkaz v příloze - netuší, že v tu chvíli zrovna aktivoval mailworm. E-mailoví červi a trojští koni často obsahují keylogger, tedy program, který sleduje a zaznamenává stisknuté klávesy, jež jste zadali v určité aplikaci. Data následně nepozorovaně pošle autorovi. Toho pak zajímají všechna hesla, čísla kreditních karet a osobní údaje.

V každém počítači by tedy měl být nainstalován antivirový program, ať už placený nebo zdarma dostupný na internetu. Kdo za něj nechce platit, může pro soukromé účely využít například Antivir Personal Edition Classic 6.31 nebo AVG Anti-Virus Free Edition 7.

Specifický trojský kůň: malá cílová skupina

Existují i specifičtí trojané, kteří se obrací vždy na určitý okruh osob, například na lékaře nebo advokáty. Na pracovní počítač často proniknou přes e-mail. Při první výzvě se špionážní program nenápadně instaluje a od té doby se spouští společně s Windows. Hledá údaje o pacientech, potažmo klientech na pevném disku a posílá je autorovi trojana, který tyto informace může nejrůznějšími způsoby zneužívat. Jedná-li se o údaje o adrese a datu narození, může si podvodník například otevřít účet na Ebay. Mohl by je prodat i kriminálním organizacím, které si cíleně vybírají především majetné zákazníky.

Nestačí jen ochránit počítač

Trojští koně se mohou zmocnit vaší identity, i když na vašem počítači vládne maximální opatrnost. Především firmy a podnikatelé, kteří spravují data zákazníků, musí dbát na vysokou bezpečnost dat a konfigurovat své systémy tak, aby počítače, z nichž přistupují k datům o zákaznících, nebyly připojené k internetu. V případě specifických trojanů mohou být i antivirové programy bezmocné. Kvůli minimálnímu rozšíření jsou tito škůdci v laboratořích výrobců antivirů většinou neznámí, takže není

možné připravit potřebné popisy. Proti těmto škůdcům nejlépe pomůže heuristika antivirových programů nebo ještě lépe technika, která typické chování trojanů rozpozná a zablokuje (viz vlevo). Vy sami můžete udělat jen jedno: svá data svěřte jen málo firmám. Obzvláště datum narození byste měli držet pod pokličkou, protože s jeho pomocí se například dá otevřít konto ve webové aukční síni.

Phishing

Prostřednictvím phishingu (z anglických slov *password fishing*) číhají datoví špioni taktéž na osobní a tajné informace uživatelů, ale nepoužívají k tomu škodlivý program. Jednoduše oběť donutí vyzradit požadované informace dobrovolně - a často s tím slaví úspěch.

Svůdné e-maily

I přes častá varování se stále někteří uživatelé nechají autenticky působícími e-maily svést ke klikání na linky ve zprávě. Na následujících internetových stránkách pak zadávají osobní údaje. Příkladů lze bohužel najít až příliš mnoho. Často se o pozdvižení starají e-maily, které vypadají, jakoby pocházely od bankovních domů. Paradoxně varují před podvodníky a prosí uživatele, aby klikli na odkaz a zde "vyplnili způsob doplňkové autorizace". Odkaz vypadá na první pohled stejně, jako by vedl k webové stránce opravdové banky. Při důkladném pohledu na URL však zjistíme, že se jedná o trik. Pokud se dostanete na zmíněné stránky, podvod často ani na první pohled nepoznáte. Všechno je podrobně napodobeno - stránka působí autenticky. Ani originální poznámka "pozor na podvodníky!" s varováním před zfalšovanými e-maily zde ironicky nechybí. Do formuláře má zákazník mimo jiné zadat číslo konta, on-line PIN a TAN. Každého by to mělo zarazit hned při přihlašování, nejpozději při zadávání TAN - každopádně při čtení varování "Pozor! Svůj TAN prosím v budoucnu nepoužívejte, vedlo by to k zablokování konta".

Phishingové e-maily chtějí údaje o přihlášení na Ebay

Phishingové e-maily často přicházejí jakoby od Ebay. Většinou jsou v angličtině, někdy ale mohou být i lokalizovány. Vzor je vždy stejný: na základě obskurních událostí, jako spadnutí serveru nebo problémy s databankou, se údajně ztratily informace. Adresát má kliknout na odkaz, který na první pohled vypadá jako adresa Ebay. Na následující (zfalšované) stránce Ebay se má s uživatelským jménem a heslem přihlásit a překontrolovat správnost svých osobních dat. Pokud by to neudělal, bude účastnické konto zrušeno - toto varování vytváří ještě dodatečný tlak. Aby nevzniklo žádné podezření, přesměruje vás hackerská stránka po zadání údajů na skutečnou stránku Ebay - samozřejmě poté, co se zachycená data uživatele uložila do vlastní databáze. Takto získané účty Ebay využívají hackeři k nabídce drahého zboží pod cizím jménem, které si sice nechají zaplatit, ale nikdy jej nedodají.

Efektivní ochrana proti phishingu: neklikat

Nejlepší ochranou proti phishingovým mailům je nedůvěra, pokud jste v e-mailu vyzýváni ověřit zákaznická data u nějaké určité služby. Zásadně byste neměli vyvolávat stránky s přihlášením přes odkaz v e-mailu, nýbrž zadávat adresu služby ručně do adresového řádku prohlížeče (nebo stránku načíst přes záložku, kterou jste sami vytvořili).

Sběrači dat

Říká se, že "Google ví všechno." Trefnější by však bylo tvrdit, že "Google ví příliš mnoho." Tento vyhledávač totiž pročesává vše, co mu přijde pod ruku. Zda se přitom jedná o chráněná data nebo ne, je vyhledávacímu robotu jedno.

Podvodníci využívají vyhledávače

Přes Google a podobné služby se dají zjistit datové pakety milionů lidí: jméno, příjmení, adresa, telefonní číslo a datum narození stačí k získání identity pro kriminální účely. Před několika lety by bylo ještě těžko myslitelné, aby měl někdo problémy z toho, že na webu uvedl své datum narození. Spousta lidí ho naivně dala na svoji vlastní stránku nebo do on-line životopisu. Dnes s těmito údaji lze založit účet na Ebay, který nenechavcům může přinést dost peněz a poškozenému pak řadu nepříjemností. Ebay je však pouze jedním z příkladů, kde mohou podvodníci páchat škody.

Utajte svá data

Na osobních stránkách byste měli zásadně uvádět co nejméně citlivých dat. Objevit by se zde neměla především vaše adresa a hlavně datum narození. Adresa se sice dá získat pomocí služeb jako *www.checkdomain.com* - alespoň však krádež identity ztížíte. On-line životopisy, u nichž se těmto údajům nelze vyhnout, byste měli opatřit heslem, které pak uvedete v odpovědi na inzerát.

Jednodušší, i když méně bezpečné, je donutit vyhledávače, aby určité stránky neiniciovaly. V tom případě si musíte založit textový soubor s názvem *robots.txt* v hlavním adresáři vaší webové stránky.

Do prvního řádku napište "User-agent: *", čímž určíte, že instrukce platí pro všechny vyhledávače. Na dalším řádku následuje příkaz "Disallow: /" s následujícím názvem adresáře, ve kterém jsou uloženy stránky webového serveru, jež nemají být iniciovány. Na konci řádku bude opět lomítko. Pro každý další adresář založíte zvláštní řádek s "Disallow: /".

Pokud chcete celou webovou stránku vyjmout z indikace vyhledávači, nezadávejte za příkazem žádný název adresáře. V následujícím příkladu by měly všechny vyhledávače iniciovat kompletní webovou stránku s výjimkou adresářů "job offer" (nabídka zaměstnání) a "database".

Pokud chcete, aby vyhledávače do indexu nezahrnuly nic, pak musí *robot.txt* vypadat následovně:

Pokud se vaše webová stránka již v indexu Googlu nebo jiných vyhledávačů nachází, musíte chvíli vydržet, než se změna projeví. Vyhledávače zpravidla zjišťují každé čtyři až osm týdnů, zda nedošlo k nějakým změnám. Adresáře pak z indexu vymažou.

Metoda s *robots.txt* je jednodušší, avšak méně bezpečná než ochrana heslem. Vyhledávače totiž nejsou povinné držet se instrukcí v souboru *robot.txt*, i když většina jich to dělá. Kvůli chybám v softwaru se může v určitých případech stát, že soubor *robot.txt* bude ignorován. Určité adresáře lze ochránit heslem zpravidla z konfiguračního menu vaší webové stránky.

Zanechte co nejméně stop

Nad vlastní webovou stránkou máte ještě určitou kontrolu. Těžší je to ale v případech, kdy zadáváte údaje na web tam, odkud je pak již sami nemůžete vymazat. Jedná se například o webová fóra a návštěvní knihy. Mnozí lidé zde zanechají jméno, e-mailovou adresu a možná i další data, aniž by pomysleli na to, že i tyto údaje se dají

pomocí vyhledávačů najít. U Usenet-Newsgroups můžete alespoň zabránit tomu, aby je Google Groups (*http://groups.google.de*) ukládal navěky a byly tak přístupné pomocí vyhledávání. Toho dosáhnete příkazem "X-No-Archive: yes" v prvním řádku zprávy.

Pokud si vedete blog, který je kompletně hostován poskytovatelem, jenž nenabízí přístup přes FTP, nedá se zpravidla zabránit tomu, aby vyhledávače vaše příspěvky neindikovaly. Soubor *robots.txt* zde totiž není možné založit. U některých poskytovatelů blogů se však lze použít heslo pro čtení.

Datové pasti

Chcete anonymně surfovat a použijete k tomu určený speciální nástroj. Přesně tím ale můžete hackerům zprostředkovat svý data. Nebezpečí hrozí i při používání internetu v kanceláři nebo v internetové kavárně.

Proxys: hackeři mohou naslouchat

Je mnoho programů, které by vám měly zaručit anonymní surfování po internetu. Kvůli tomu vedou data přes proxy server (vlevo). Server na druhé straně tak získá pouze IP adresu proxy.

Někteří výrobci prohledávají pravidelně síť kvůli obecně přístupným proxy serverům a vytvářejí seznamy, které pak automaticky nebo ručně ukládají. Otevřené proxy servery - tedy bez přihlašování - mají tu nevýhodu, že vlastně nikdo neví, komu patří a jak jsou konfigurovány. Některé z těchto serverů jsou nastaveny tak, že průběžně ukládají všechny požadované obsahy. Ty se pak při příštím zobrazení musí ukládat pouze v případě, že byly změněny. Když se například chcete dostat ke svým e-mailům přes proxy server webmailu, může se stát, že bude přečtené zprávy průběžně ukládat. Administrátor proxy nebo hacker, který se do serveru naboural, si je může přečíst nebo přímo odposlouchávat datový provoz. Podvodník může vytvořit i vlastní proxy a doufat, že se dostane do seznamů proxy serverů určitého programu, aby mohl odchytávat datový provoz mezi uživateli.

Pro anonymní surfování je lepší používat takový software, jehož výrobce garantuje důvěryhodnost používaných proxy serverů. Jedním z nich je například neplacený nástroj JAP 00.05.007 (najdete na našem CD).

Nebezpečí v kanceláři: kolegové čtou také

Zvláště vysoké nebezpečí špionáže hrozí v sítích, kde všichni účastníci sdílejí jeden přístup na internet. Některé neplacené programy (jako *Ethereal 0.10.12* společně s ovladačem *Winpcap 3.0*) stačí k tomu, abyste mohli odposlouchávat, na které aukci na Ebay kolega něco nabízí nebo ve kterém chatu se pohybuje. Jediným předpokladem je síť spojená pomocí hubů. Naštěstí se huby již tolik nepoužívají. Lepší volbou dnes jsou switche. Od hubů se totiž odlišují v jednom zásadním bodě: všímají si, na jakém portu switche je počítač s určitou síťovou adresou připojen. Počítač B tak nepozná - na rozdíl od hubu - když si počítač A vyměňuje data s počítačem C.

Existují způsoby, jak jednotlivé počítače v sítích se switchi odposlouchávat. Program *Ettercap* změní routovací pravidla napadeného počítače tak, že všechna data běží přes mezistanici, kterou je počítač špiona a na níž je tak možné data rovněž přečíst. I bezpečná spojení HTTPS se dají s určitou snahou zmanipulovat tak, aby špion viděl data v nešifrovaném textu. Takovým útokům se jako jednotliví uživatelé nemůžeme

bránit, může nás ochránit pouze síťový administrátor, který vše permanentně hlídá pomocí speciálního softwaru.

Své e-maily však můžete před zvědavými pohledy uchránit: používejte kódovací nástroj jako třeba *PGP Desktop 9.0*. Program je k dispozici i v sharewarové verzi, u niž se po třiceti dnech řada funkcí vypne, ale kódování e-mailů funguje dál.

Datoví špioni číhají v internetových kavárnách

Jisté riziko představuje zadávání přihlašovacích údajů na cizím počítači v internetové kavárně. Jen málo internetových kaváren používá speciální software, který po každé session vrátí systém do předem definovaného základního stavu a smaže přitom všechna osobní data.

Internet Explorer (IE) může být nastaven tak, aby ukládal všechny hodnoty zadané do polí formulářů včetně hesel. Již při zadání prvního písmene se v rámečku s uživatelskými jmény u populárních služeb jako třeba GMX otevře lišta se všemi uloženými identifikacemi, které začínají tímto písmenem. Související heslo je sice maskováno hvězdičkami, log-in ale umožňuje. Všechna uživatelská jména včetně hesel uložená v IE se dají rozšifrovat freewarovým programem *Protected Storage Passview* (najdete na našem CD). Můžete jej vyzkoušet na svém prohlížeči.

U počítače umístěného v internetové kavárně navíc nikdy nevíte, nakolik vážně bere provozovatel bezpečnostní update. Některé z těchto veřejně přístupných počítačů jsou přehlceny spywarem. Často jsou zde i keyloggery, které protokolují všechny stisknuté klávesy. Pokud si nejste jisti, zda se po vašem sezení všechna data smažou, měli byste se vyhnout přihlašování na webové služby.

Ti z vás, kteří se ani na cestách nechtějí vzdát prohlížení e-mailu, si mohou zdarma založit další účet a nechat si na něj zprávy ze své hlavní poštovní schránky převádět. Ne všichni provozovatelé ale tuto funkci nabízejí bezplatně.

Lidé, bděte!

Množství phishingových e-mailů vzrostlo tak dramaticky hlavně kvůli neodpovědnému a lehkomyslnému přístupu uživatelů, kteří bez přemýšlení vykonají, co se po nich v podezřelém mailu žádá. Autorizační kódy, PIN, uživatelská jména, hesla - to vše důvěřivě svěří webové stránce, na níž je navede phishingový e-mail. Nediví se ani pravopisným chybám a kostrbatým formulacím a dokonce ani tomu, že prohlížeč nenavazuje zabezpečené spojení. Když je to černé na bílém, pak to musí být pravda. Jediná rada zní: buďte zdravě paranoidní, bez určité míry nedůvěřivosti dnes už nelze internet používat.

Nacistická hesla vaším jménem

Trojské koně a červi nemusí způsobovat jen materiální škody. Některé ohrožují vaši dobrou pověst: například e-mailoví červi Sober.P a Sober.Q rozesílají vaším jménem nacistická hesla na adresy, která najdou na pevném disku, například v adresáři. Možní jsou i červi, kteří vystaví vaše dokumenty z Office ve veřejných diskuzních skupinách nebo na webových fórech.

1) pro soukromé použití 2) lze získat i jako shareware, doba platnosti 30 dní 3) v balíku s Panda Titanium Antivirus 2005: 49,95 euro

Aktivní ochrana proti virům

Proti neznámým virům a trojským koním pomáhají nejlépe techniky rozpoznávající jejich typické chování. Takovou používá například antivirus *NOD32* (*www.nod32.cz*, licence na 1 rok stojí 1 500 Kč, update na další rok 600 Kč), balík *Norman Virus Control 5* (56,84 euro,). Panda Software nabízí zase *Tru Prevent Personal 2005* - jako samostatný produkt za 29,95 euro a v balíku s *Panda Titanium Antivirus 2005* za 49,95 euro (*www.pandasoftware.com*).

Pět podlých triků a jak se proti nim bránit

1. Phishing: Podvodníci rozesílají e-maily, které vypadají jako by pocházely od banky nebo od Ebay. Adresáti jsou pod nějakou záminkou vyzýváni, aby kliknuli na uvedený odkaz. Ten je pak zavede na webovou stránku, která vypadá podobně jako ta pravá. Zde mají oběti zadat svoje přihlašovací údaje.

Ochrana: Neklikejte na odkazy v e-mailech, ale zadávejte vám známou adresu služby do prohlížeče ručně (viz strana 65).

2. Trojské koně: Trojské koně neposílají na vaši adresu jen nakažené e-maily. Spolupracují s keyloggery, které zaznamenají heslo a pošlou ho zadavateli.

Ochrana: Nainstalujte si antivirový program a stále ho udržujete v aktualizovaném stavu (viz na této straně).

3. Obsah homepage: Podvodníci cíleně pátrají po osobních stránkách, na nichž autor uvádí adresu a datum narození. Tyto údaje pak využijí při zakládání různých kont a jménem oběti draží věci, které vůbec nevlastní.

Ochrana: Adresu a datum narození zadávejte pouze tehdy, pokud je to bezpodmínečně nutné a pouze v oblasti chráněné heslem (viz strana 66).

4. Krádež dat v internetové kavárně: Na špatně chráněných počítačích v internetových kavárnách číhají bezpečnostní mezery a trojské koně - navíc zde prohlížeč může ukládat identifikační údaje.

Ochrana: Nepoužívejte v internetových kavárnách webové služby, k nimž se musíte přihlašovat (viz strana 70).

5. Odposlouchávání proxy-serverů: Podvodníci napadnou proxy servery, vyhodnocují dočasně uložená data a odposlouchávají datový provoz.

Ochrana: Nezadávejte žádná osobní data a identifikační údaje, pokud používáte proxy například v případě anonymního surfování (viz strana 68).

Phishing - ochrana na Ebay

Ebay eviduje všechny e-maily, které služba posílá uživatelům, a to i v soukromém okruhu zákazníků. Pro ověření, zda se jedná o pravý e-mail, se tedy stačí přihlásit na zákaznické centrum - samozřejmě opět ručním spuštěním prohlížeče, nikoliv přes odkaz v e-mailu.

Anti-Phishing-Toolbar

Dodatečnou bezpečnost slibuje *Netcraft Toolbar* (najdete na našem CD). Když zobrazíte webovou stránku, nástroj se zároveň zeptá příslušného registru domén, kdy

a u jakého poskytovatele byla doména registrována a ve které zemi se webová stránka nachází. Nedávno založená doména by měla být podezřelá. Malý proužek, který je obvykle zelený, se zbarví v různé délce červeně podle toho, nakolik důvěryhodnou se stránka jeví. Netcraft Toolbar je k dispozici pro Internet Explorer od verze 6.0 a pro Firefox od 1.0.

Riziko potvrzovacích e-mailů

Nejlepší šifrování dat u objednávkových a registračních formulářů nepomůže, pokud provozovatel uživateli vzápětí pošle jako potvrzení nezabezpečený e-mail se všemi zadanými údaji, včetně těch bankovních. Je to sice spíše výjimkou, ale bohužel nemůžete nikdy předem vědět, jak odpovědně bude poskytovatel s vašimi daty zacházet. Zpravidla se sice dá spolehnout na to, že si nešifrovaný mail nikdo cizí nepřečte, ale garantováno to není.

Jak hlídá stát své občany

Stát může střežit své občany před trestnými činy na internetu jen v rámci velmi omezených hranic. Vyšetřovatelé mohou něco podniknout pouze v případě, pokud existuje konkrétní podezření. Evropská komise požaduje pečlivé ukládání dat. Provozovatelé internetových služeb by pak byli povinni ukládat všechna data o místech a spojeních svých zákazníků po přesně stanovenou lhůtu několika měsíců. Není ještě jisté, zda by se jednalo jen o IP adresu uživatele a adresy serverů, na které měl přístup, nebo zda by se uchovávala všechna uživatelská data, tedy e-maily, webové stránky, hovory přes VoIP a podobně. Vzhledem k tomu, že uživatelská data by jistě zlikvidovala ukládací kapacitu poskytovatele, takto daleko vše asi nedojde. Již dnes musí mít poskytovatelé elektronické pošty s více než tisícem zákazníků odposlouchávací zařízení, které orgánům činným v trestním řízení na základě soudního povolení umožní cíleně nahrát e-mailovou komunikaci podezřelého. Poskytovatelé kvůli tomu musí investovat do nákladného softwarového a hardwarového vybavení. Takový postup však asi nic nepřinese, protože profesionální pachatelé již dlouho šifrují svoji komunikaci pomocí programů jako PGP, které používají velmi bezpečné algoritmy.

Informace o phishingu

Anti-Phishing Working Group () na své webové stránce uvádí obecné informace k tématu a informuje o aktuálních a předchozích phishingových mailech v anglickém jazyce.

Proxy servery

Proxy slouží jako mezistanice. Pokud svůj prohlížeč řádně nakonfigurujete, nenapojuje se přímo na požadovanou webovou stránku, ale posílá požadavky přes proxy. Tím zjistí pouze vaší IP identifikaci, přes níž se dají zpětně sledovat připojení k internetu. Proxy nabere data na požadovaném webovém serveru a pošle je vašemu prohlížeči. Na internetu je spousta proxy serverů, ale některé jsou kvůli chybě v konfiguraci volně přístupné a ze sítě jsou odebrány v okamžiku, kdy si administrátor chyby všimne.

Anonymně na internetu?

I když si myslíte, že se na internetu pomocí nějakého nástroje pohybujete anonymně, nemusí to být pravda. Řada těchto programů včetně aplikace JAP (vpravo) umožňuje pouze anonymní surfování. Jakmile ale děláte jiné věci, například čtete e-maily pomocí klienta, stahujete soubory přes FTP nebo využíváte internetové aukční síně, dáváte tím k dispozici svoji skutečnou IP identifikaci. Pro maskování kompletního internetového připojení se hodí například placená služba .

Man in the middle attack

Doslovný překlad "útok muže uprostřed" popisuje celkem přesně, o jaký typ napadení se jedná. Počítač se chová v síťové komunikaci PC jako mezistanice.

obrázek vpravo, popisek: Protected Storage Passview: tímto freewarem se na internetu dají zobrazit hesla, uložená Internet Explorerem.