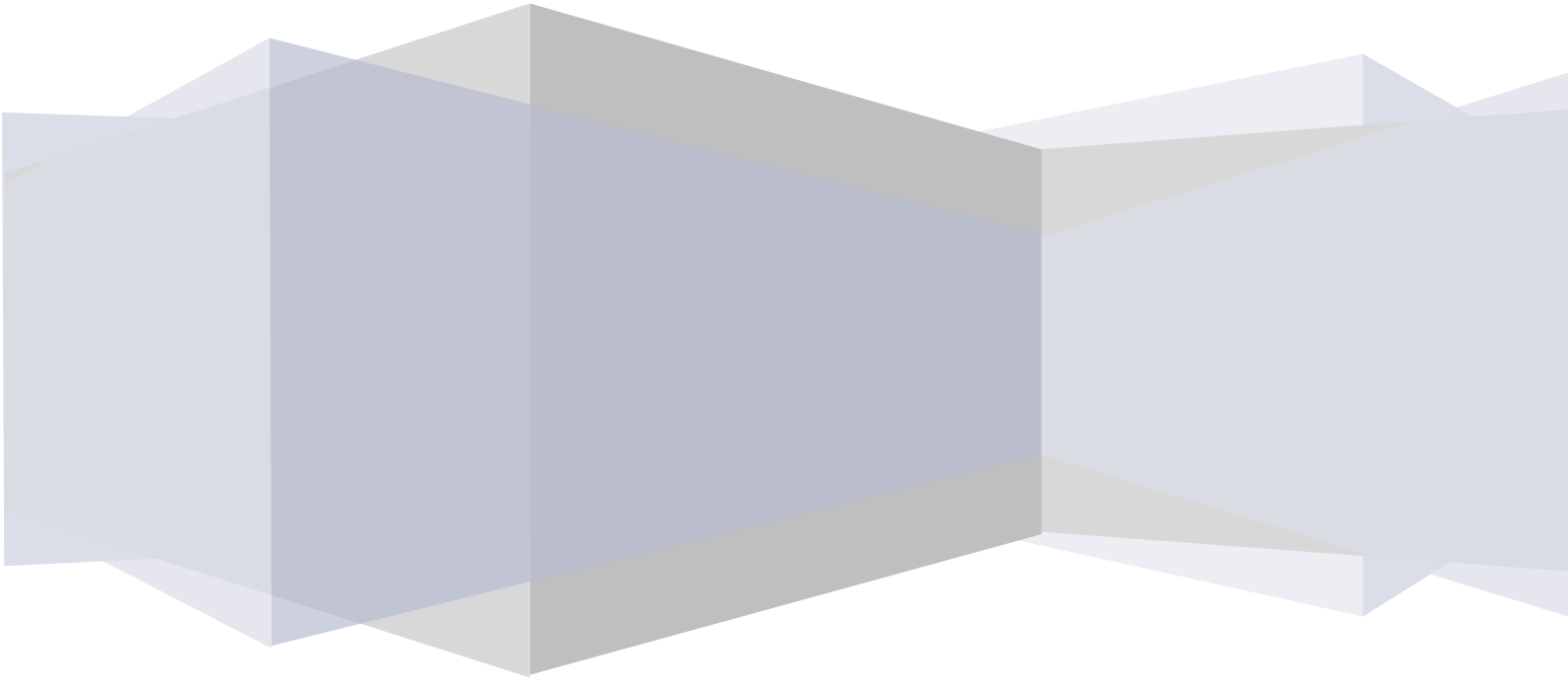
SK-nic
Slovak top level domain registry

Prevádzková správa systému SK-NIC

za obdobie 1. decembra 2008 – 31. mája 2009



Obsah

Executive Summary

- ✓ Doména .SK stále rastie. Počas prvého polroka 2009 počet zaregistrovaných domén rástol priemerne o 6 135 doménových mien mesačne a dosiahol počet viac než 34 domén na tisíc obyvateľov.
- ✓ Počet registrovaných domén prekročil vo februári 2009 hranicu 180 tisíc. Na konci sledovaného obdobia bolo zaregistrovaných 186 709 domén, z toho do zóny .SK je generovaných viac než 179 tisíc domén druhej úrovne.
- ✓ V sledovanom období vzrástol počet oprávnených registrátorov domény .SK o 172. Na konci mája 2009 bolo akreditovaných 3 389 registrátorov.
- ✓ V sledovanom období takisto vzrástol počet užívateľov doménových mien o 3 968 subjektov. Na konci mája bolo v systéme SK-NIC registrovaných 71 654 užívateľov.
- ✓ Mierne sa zvýšilo množstvo špekulatívnych registrácií domén v rámci tzv. domain-tasting obdobia (domény v stave technickej akceptácie, DOM_TA). Kým na začiatku sledovaného obdobia bolo v tomto stave 0,79% domén, na konci obdobia to bolo 0,96%. Medziročne sa však tento počet znížil. Najvyšší počet domén v stave TA v sledovanom období bol 18. januára 2009 – 2 473 domén (1,41% z celkového počtu registrovaných domén). Na konci obdobia to bolo 1 795 domén.
- ✓ V sledovanom období registrátori zaregistrovali 36 814 nových domén. Vymazaných bolo 21 229 domén.
- ✓ Spoločnosť SK-NIC, a.s. je riadnym členom Rady správcov európskych národných domén CENTR.
- ✓ Spoločnosť' SK-NIC, a.s. je riadnym členom Organizácie národných správcov domén (ccNSO), ktorá funguje v rámci Medzinárodnej korporácie pre prideľovanie mien a čísel ICANN. ccNSO je orgánom pre tvorbu politiky ICANN v súvislosti s národnými internetovými doménami najvyššej úrovne.

O dokumente

Spoločnosť SK-NIC, a.s. vydáva každý polrok prevádzkovú správu. Táto správa obsahuje všetky dôležité udalosti, ako aj práce vykonané počas príslušného obdobia, vrátane technického stavu, výkonu systému, a tiež komplikácií, ktoré nastali. Táto správa obsahuje tiež údaje o výkone systému správy domény .SK, najmä celkový počet registračných operácií, počet nových, presunutých, zmazaných a zrušených registrácií v rámci domény .SK, počet akreditovaných registrátorov vrátane počtu registrácií každého z registrátorov.

O SK-NIC, a.s.

Spoločnosť SK-NIC, a.s. je správcom domény .SK a zabezpečuje registráciu domén druhej úrovne pod doménou .SK ako doménou najvyššej úrovne (top level domain, TLD). Spoločnosť SK-NIC, a.s. poskytuje túto službu pre registrátorov, užívateľov a držiteľov domén. Povaha a charakter týchto poskytovaných služieb vyžaduje, aby bola zabezpečovaná v každej krajine centrálne s následným prepojením na technické koordinačné centrum pre Internet ICANN. Spoločnosť SK-NIC, a.s. je jediným subjektom na území Slovenskej republiky, ktorý vykonáva správu domény .SK a registráciu domén druhej úrovne pod doménou .SK. Spoločnosť SK-NIC, a.s. získala toto postavenie na základe poverenia medzinárodnej organizácie The Internet Corporation for Assigned Names and Numbers („ICANN“) a je touto organizáciou riadne akreditovaným správcom na poskytovanie služby takéhoto charakteru.

Spoločnosť SK-NIC, a.s. podpísala 5. júna 2006 Zmluvu o spolupráci s Ministerstvom dopravy, pôšt a telekomunikácií SR. Jej cieľom je správa internetovej domény najvyššej úrovne .SK v súlade so záujmami Slovenskej republiky i internetovej komunity pôsobiacej na Slovensku. Na základe tejto zmluvy je spoločnosť SK-NIC, a.s. povinná zabezpečovať evidenciu doménových mien domén druhej úrovne, vykonávať správu príslušných databáz a príslušných verejných vyhľadávacích a dopytovacích služieb, zabezpečovať prevádzku registračného systému domén druhej úrovne, zabezpečovať prevádzku menných serverov TLD .SK, vytvárať a vykonávať manažment zónových súborov TLD .SK. Spoločnosť SK-NIC, a.s. sa zaviazala, že 5 % z vybraných poplatkov (tržieb za predaj služieb) použije na financovanie projektov v záujme internetovej komunity. Použitie týchto finančných prostriedkov na konkrétne projekty schvaľuje ministerstvo. 31. januára 2007 bol podpísaný dodatok k tejto zmluve, ktorý spresňuje niektoré ustanovenia, najmä v prospech slovenskej internetovej komunity, napr. zvýšil sa počet členov riadiacej komisie zo 6 na 7 v prospech komunity; určili sa jednotlivé zložky, z ktorých by mali pochádzať reprezentanti internetovej komunity; spresnili sa niektoré ustanovenia týkajúce sa lehôt, krízových stavov a podobne. V súčasnosti sa doménou zaoberá Ministerstvo financií SR, z dôvodu presunu kompetencií v záležitostiach informatizácie a následnej delimitácie zmluvy o spolupráci.

Spoločnosť SK-NIC, a.s. je riadnym členom Rady správcov európskych národných domén CENTR. Rozhodlo o tom valné zhromaždenie CENTR, ktoré zasadalo v Paríži 10. októbra 2007. CENTR (Council of European National Top-Level Domain Registries) je asociáciou správcov národných internetových domén najvyššej úrovne (ccTLD). Okrem viac než 40 krajín z európskeho regiónu sú členmi CENTR aj mimoeurópski správcovia, napr. Irán, Japonsko, Nový Zéland a Kanada. CENTR vytvára fórum pre diskusiu o otázkach politík jednotlivých správcov a slúži ako kanál pre komunikáciu s organizáciami riadiacimi internet, ako aj inými entitami spojenými s internetom. Pravidlá a registračné postupy správcov domén sa v jednotlivých krajinách značne líšia. CENTR sa snaží zbierať o nich informácie a dokumentovať ich prax. CENTR tiež podporuje spoločné projekty, ktoré riešia technické, manažérske a právne problémy správcov domén. V súčasnosti reprezentujú členovia CENTR viac než 37 miliónov registrovaných doménových mien. Členstvo v CENTR prispeje k vyššej efektivite systému správy národnej domény .SK. Skúsenosti ostatných členov významne pomôžu pri úpravách systému na Slovensku, ktoré sú po viac než troch rokoch fungovania nevyhnutné.

Spoločnosť SK-NIC, a.s. sa v novembri 2007 stala riadnym členom Organizácie národných správcov domén (ccNSO), ktorá funguje v rámci Medzinárodnej korporácie pre prideľovanie mien a čísel ICANN. ccNSO (The Country Code Name Supporting Organization) je orgánom pre tvorbu politiky

ICANN v súvislosti s národnými internetovými doménami najvyššej úrovne. Je vytvorený na základe stanov ICANN. Zodpovedá za rozvoj politík súvisiacich s národnými doménami najvyššej úrovne a je poradným orgánom Rady ICANN v tejto oblasti. Stará sa tiež o vytváranie konsenzu v rámci komunity národných správcov domén a ich aktivít. Má tiež koordinačnú funkciu medzi národnými správcami a ďalšími podpornými organizáciami, výbormi a inými súčasťami organizácie ICANN. V súčasnosti má ccNSO 65 členov.

Získanie členstva v ccNSO a CENTR je súčasťou plánu aktivít, ktorými sa spoločnosť SK-NIC, a.s. snaží priblížiť systém správy národnej domény .SK internetovej komunite.

Z histórie

- 1993 – začiatok prevádzky domény .SK, správcom domény je EUnet
- 1999 – zlúčenie EUnet a GNS – vzniká EuroWeb
- 1999 – databázová aplikácia
- 2002 – platená služba
- 3. november 2003 – deaktivácia nepremigrovaných domén
- 2004 – vzniká Združenie pre správu národnej domény SK
- Apríl 2005 – EuroWeb sa stáva členom skupiny DanubiaTel
- Február 2006 – zmena obchodného mena na SK-NIC, a.s.
- 5. jún 2006 – podpis zmluvy o spolupráci s MDPT SR
- 1. február 2007 – delimitácia Zmluvy na MF SR
- 17. október 2007 – SK-NIC sa stáva členom CENTR
- November 2007 – SK-NIC sa stáva členom ccNSO

Princíp fungovania

Cieľom registrácie domény je jej sprístupnenie koncovému užívateľovi. Spoločnosť SK-NIC, a.s. dňom 13.01.2003 zaviedla nový systém registrácie domén, ktorý je podrobne popísaný v Pravidlách poskytovania menného priestoru v internetovej doméne .SK.

Základné fázy registračného procesu

Doména sa dostáva do **stavu LOCKED** (rezervovaná) vyplnením Formulára 4 (zmluva o doméne uzavretá pred uzavretím rámcovej zmluvy). Návrh podáva registrátor v mene budúceho používateľa. Platí, že zmluva o doméne bola uzavretá s rozväzovacou podmienkou, ktorou sa rozumie márne uplynutie 14-dennej lehoty na platné a účinné uzavretie rámcovej zmluvy, počítanej odo dňa odoslania elektronického návrhu. Doména v tomto stave nie je technicky prevádzkovaná. V prípade márneho uplynutia lehoty na uzavretie rámcovej zmluvy sa považuje rozväzovacia podmienka za splnenú, v dôsledku čoho dochádza k zrušeniu záznamu domény. Ak bola uzavretá rámcová zmluva, SK-NIC to bezodkladne oznámi registrátorovi. Registrátor na základe tohto oznámenia je povinný zaplatiť SK-NIC cenu za prístup k záznamu domény.

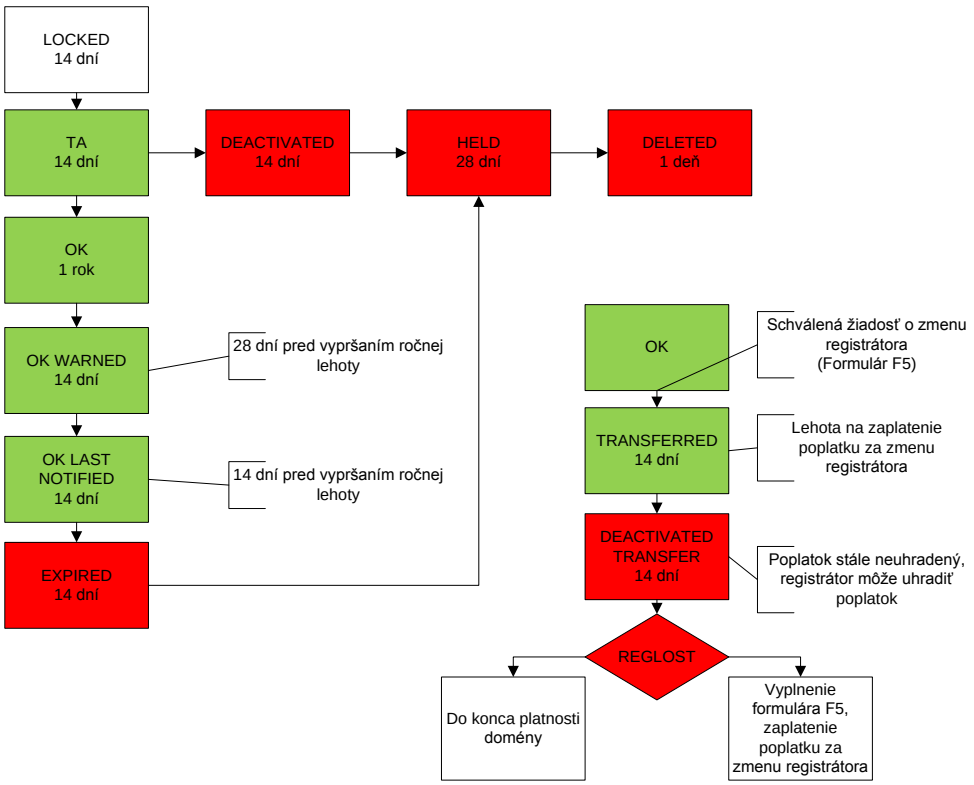
Návrh zmluvy o doméne je podaný doručením riadne vyplneného Formulára 3 (zmluva o doméne uzavretá po uzavretí rámcovej zmluvy) v elektronickej forme SK-NICu, v ktorom uvedie, okrem iného, identifikátor používateľa. SK-NIC akceptuje návrh tým, že používateľovi a registrátorovi zašle elektronickou poštou potvrdenie o registrácii domény. SK-NIC zároveň uvedie doménu do technickej prevádzky – do **stavu TA** (technicky akceptovaná). Registrátor je povinný zaplatiť cenu za prístup k záznamu domény za účelom správy každej domény. Cena sa platí vopred na obdobie jedného roka od začiatku technickej prevádzky domény, a registrátor je povinný ju zaplatiť spravidla do 14 dní od doručenia oznámenia o uzavretí zmluvy o doméne Ak registrátor neuhradí cenu za prístup k záznamu domény v tejto lehote, doména prestáva byť technicky prevádzkovaná a počas trvania ďalšej 14 dňovej lehoty – doména je **v stave DEACTIVATED** (deaktivovaná) – je registrátor oprávnený zaplatiť cenu za prístup do databázy domény, v opačnom prípade sa doména dostáva do stavu HELD.

Do **stavu HELD** alebo **REGLOST** sa doména dostáva v prípade, ak v jej zázname nie je uvedený registrátor. Domény v stavoch HELD a REGLOST nie sú technicky prevádzkované. Do stavu HELD sa dostáva doména v prípade, ak nedošlo k zaplateniu ceny za prístup k záznamu domény, do stavu REGLOST sa dostáva doména spravidla v prípade, ak nebol zaplatený poplatok za zmenu registrátora. Doména v stave REGLOST môže v nezmenenom stave existovať do konca uplynutia lehoty predplateného prístupu k záznamu domény. V stave HELD je držiteľ domény v lehote 28 dní odo dňa jeho vzniku povinný zabezpečiť zmenu registrátora na nového registrátora a zároveň je povinný zabezpečiť, aby sa doména zo stavu HELD nedostala opätovne do stavu HELD, v opačnom prípade má SK-NIC právo odstúpiť od zmluvy o doméne a zrušiť záznam domény.

OK je stav domény, v ktorom existuje záznam domény, je zaplatená cena za prístup do databázy domény, v zázname domény je vyznačený registrátor a doména je technicky prevádzkovaná. Najneskôr 28 dní pred splatnosťou ceny za prístup k záznamu domény na ďalšie ročné obdobie SK-NIC vyzve elektronicky (elektronickou poštou) registrátora na zaplatenie. Doména sa dostáva do **stavu OK WARNED**. Ak registrátor nezaplatí cenu za prístup k záznamu domény v nasledujúcich 14 dňoch, vyzve SK-NIC registrátora na zaplatenie v ďalšej 14 dňovej lehote a zároveň upozorní držiteľa domény, že sa blíži koniec predplateného obdobia – doména sa dostáva do **stavu OK**

LAST NOTIFIED. Ak nedôjde k zaplateniu ceny za prístup k záznamu domény najneskôr v dátume splatnosti, doména prestáva byť technicky prevádzkovaná a počas trvania ďalšej 14 dňovej lehoty – doména je **v stave EXPIRED** – je registrátor oprávnený zaplatiť cenu za prístup do databázy domény, resp. používateľ môže požiadať o zmenu registrátora, v opačnom prípade sa doména dostáva do stavu HELD. Ak v lehote 28 dní od vzniku stavu domény HELD nedošlo k zmene Registrátora, SK-NIC zruší záznam domény a odstupuje od zmluvy o doméne. Na 24 hodín sa doména dostáva do technického **stavu DELETED**, potom je voľná na ďalšie zaregistrovanie.

Držiteľ domény je oprávnený iniciovať zmenu registrátora v zázname domény, a to tak, že požiada nového registrátora, ktorý už má s SK-NIC uzavretú registrátorskú zmluvu, aby vyplnil a zaslal Formulár 5 v elektronickej forme SK-NICu. Nový registrátor je povinný zaslať SK-NICu Formulár 5 aj v písomnej forme, podpísaný držiteľom domény, a to v lehote 14 dní od odoslania Formulára 5 v elektronickej forme. Tento podpis držiteľa domény sa považuje za jeho súhlas so správou domény novým registrátorom a za vyslovenie nesúhlasu s výkonom správy domény predchádzajúcim registrátorom. Záznam pôvodného registrátora v zázname domény, ak už nebol predtým zrušený z iného dôvodu, bude zrušený SK-NICom a SK-NIC vyznačí zmenu registrátora v zázname domény – doména sa dostáva do **stavu TRANSFERRED**. Nový registrátor je povinný zaplatiť poplatok za zmenu registrátora v zmysle cenníka, v lehote do 14 dní od vykonania zmeny registrátora SK-NICom. Ak nedôjde k zaplateniu poplatku za zmenu registrátora, doména sa dostáva do **stavu DEACTIVATED TRANSFER** (bez technickej prevádzky) a ak nedôjde k zaplateniu poplatku ani v ďalšej 14 dňovej lehote, Doména sa dostáva do **stavu REGLOST** (resp. HELD, ak obdobie na ktoré bola doména predplatená už uplynulo). Doména v stave REGLOST, bez uskutočnenia ďalšej zmeny ostáva až do konca uplynutia lehoty „predplateného" prístupu k záznamu domény. DNS servery sa pri zmene registrátora automaticky nemenia; nový registrátor je povinný nastaviť DNS servery štandardným postupom bezodkladne po uskutočnení zmeny. V týchto prípadoch SK-NIC vykoná zmenu v zázname domény a oznámi túto skutočnosť novému registrátorovi.

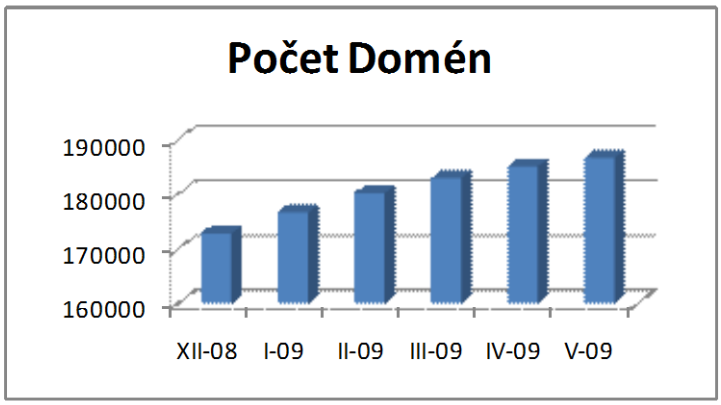


Údaje o výkone správy domény .SK

Počet všetkých registrovaných doménových mien

Tabuľka a graf uvádzajú počet všetkých doménových mien registrovaných v databáze SK-NIC v akomkoľvek stave ku koncu každého mesiaca sledovaného obdobia.

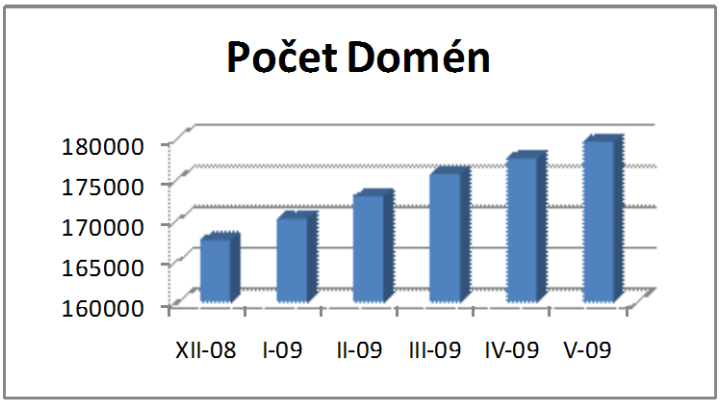
Obdobie	Počet Domén
XII-08	172815
I-09	176661
II-09	180206
III-09	182987
IV-09	185113
V-09	186709



Počet aktívnych doménových mien

Tabuľka a graf uvádzajú počet aktívnych doménových mien generovaných do zóny .SK ku koncu každého mesiaca sledovaného obdobia. Funkčné sú domény v stavoch TA, OK, WARNED, LAST NOTIFIED a DOM_TRAN.

Obdobie	Počet Domén
XII-08	167612
I-09	170220
II-09	172966
III-09	175707
IV-09	177576
V-09	179601



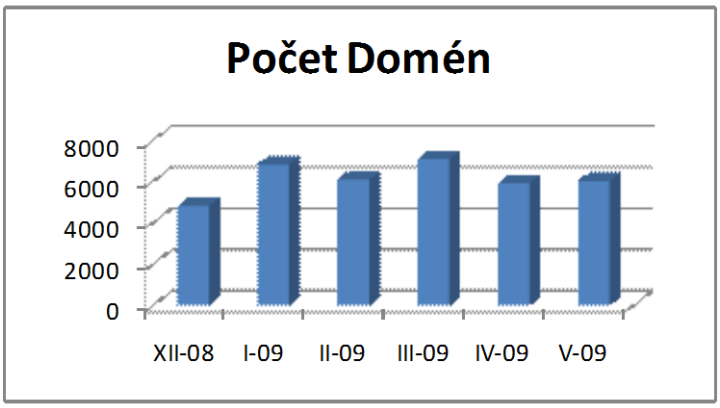
Celkový počet registračných operácií

V sledovanom období (1. decembra 2008 – 31. mája 2009) bolo vykonaných 427 993 operácií v súvislosti s doménami, celkovo 584 570 operácií registračného systému SK-NIC. Oproti minulému sledovanému obdobiu (06/2008 – 11/2008) to znamená pokles o1,15% operácií na doménach, celkovo však nárast o 15%. Medziročne (12/2007 – 5/2008) narástol celkový počet operácií o 13,6 percenta.

Počet nových domén

Tabuľka a graf uvádzajú počet nových registrovaných domén v rámci každého mesiaca v sledovanom období.

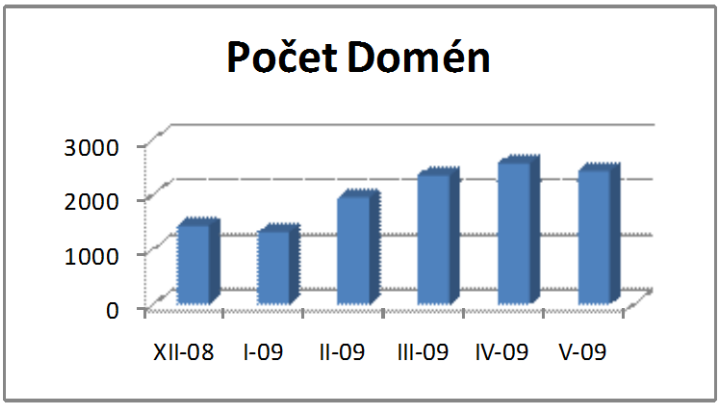
Obdobie	Počet Domén
XII-08	4836
I-09	6834
II-09	6093
III-09	7103
IV-09	5917
V-09	6031
SUMA:	36814



Počet presunutých domén

Tabuľka a graf uvádzajú počet domén presunutých medzi registrátormi v rámci každého mesiaca v sledovanom období.

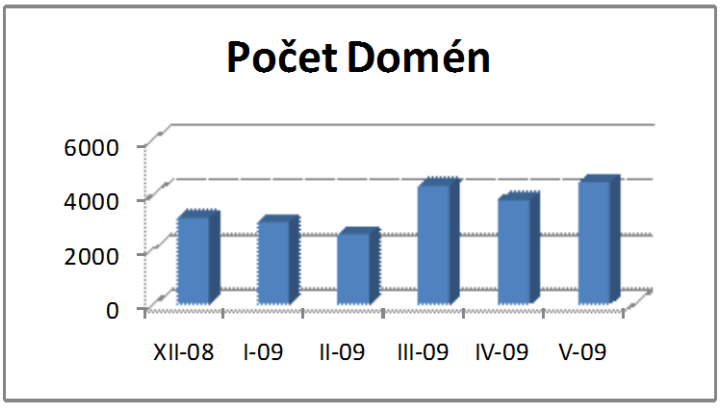
Obdobie	Počet Domén
XII-08	1426
I-09	1311
II-09	1943
III-09	2338
IV-09	2562
V-09	2422
SUMA:	12002



Počet vymazaných domén

Tabuľka a graf uvádzajú počet vymazaných domén zo systému SK-NIC v rámci každého mesiaca v sledovanom období.

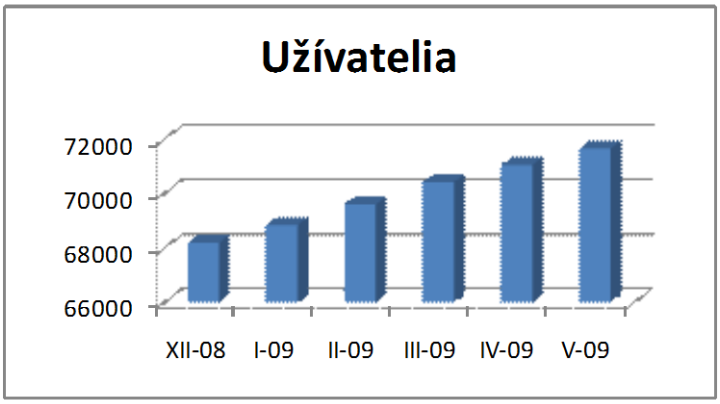
Obdobie	Počet Domén
XII-08	3145
I-09	2988
II-09	2548
III-09	4322
IV-09	3791
V-09	4435
SUMA:	21229



Počet užívateľov

Tabuľka a graf uvádzajú počet registrovaných užívateľov systému SK-NIC ku koncu každého mesiaca sledovaného obdobia.

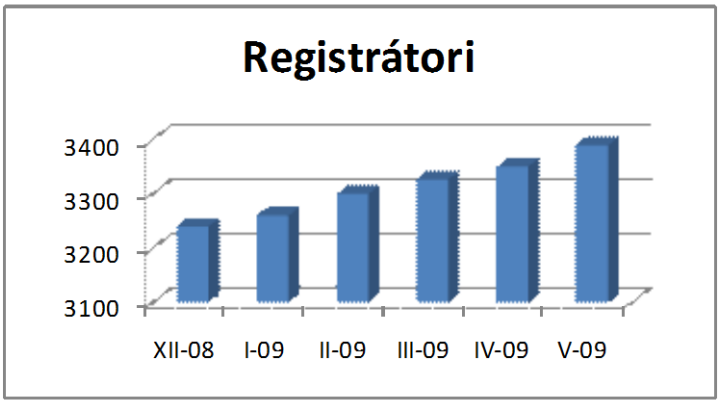
Obdobie	Užívatelia
XII-08	68198
I-09	68838
II-09	69600
III-09	70421
IV-09	71048
V-09	71654



Počet akreditovaných registrátorov

Tabuľka a graf uvádzajú počet oprávnených registrátorov systému SK-NIC ku koncu každého mesiaca sledovaného obdobia.

Obdobie	Registrátori
XII-08	3240
I-09	3260
II-09	3300
III-09	3326
IV-09	3350
V-09	3389



Počet registrácií každého z registrátorov

V tejto časti uvádzame tabuľku 25 registrátorov s najväčším počtom domén. Kompletnú tabuľku všetkých registrátorov nájdete v prílohe.

Pč	SK-NIC-ID	Spoločnosť	Domén
1	IPEK-0001	WebHouse, s.r.o.	19080
2	YEGO-0001	Yegon s.r.o.	15900
3	ZONE-0002	Zoner, s.r.o.	11806
4	GLOB-0079	ACTIVE 24, s.r.o., organizacna zlozka	10303
5	ISKI-0001	INTERNET SK s.r.o.	10236
6	EXOT-0004	EXO TECHNOLOGIES spol. s r.o.	8216
7	SLOV-0006	Slovak Telekom, a.s.	7661
8	WEBG-0001	WEBGLOBE, s.r.o.	6396
9	ASYS-0003	Atlantis Systems, s. r. o.	6286
10	WEBS-0001	Websupport, s.r.o.	4811
11	IGNU-0001	IGNUM, s.r.o.	3821
12	NHOS-0001	NIC Hosting s.r.o.	3627
13	WEBY-0002	WEBY GROUP, s.r.o.	3460
14	SLOV-0004	SLOVANET, a.s.	3252
15	TELE-0028	GTS Slovakia, a.s.	2982
16	SWAN-0002	SWAN, a.s.	2467
17	EURO-0005	EuroNET Slovakia s.r.o.	2178
18	SZMI-0001	SZM.com s.r.o.	1490
19	TOHO-0003	TOHOS.NET, s.r.o.	1213
20	ELBI-0002	ELBIA, s. r. o.	1119
21	SULA-0001	Singularity, s.r.o.	1017
22	CROO-0002	crooce.com - the internet company, s.r.o.	1011
23	IRIS-0004	IRISOFT, s.r.o.	743
24	DATA-0076	DATACENTRE, s.r.o.	730
25	MPOR-0001	Milan Poruban	716

Komplikácie

V sledovanom období sa neobjavili žiadne vážnejšie komplikácie v rámci systému.

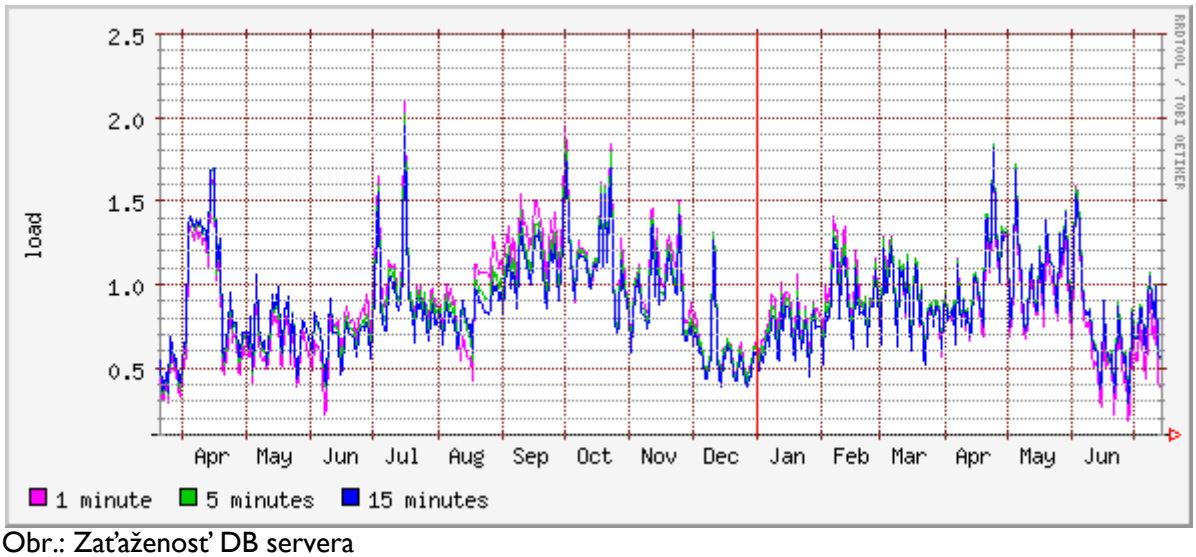
Dňa 04.03.2009 okolo 09:00 nastala chyba vo webovej aplikácii. Dôvodom bol výpadok xen na captcha serveri, ktorý bolo potrebné presunúť na iný server. Systém SK-NIC je ochránený proti podobnému výpadku, ale nebol chránený proti dlhému čakaniu na time-out, t.j. webová stránka nabehla ale po dlhom čakaní na nedošlú odpoveď. Po reštarte služby približne o 11.00 všetky služby bežali opäť v poriadku.

Dňa 14.05.2009 okolo 09:00 bol hlásený výpadok služby whois.sk-nic.sk. Dôsledkom bola interná chyba java/web aplikácie. Po deaktivácii a opätovnom reštarte služieb www.sk-nic.sk a whois.sk-nic.sk bol problém odstránený.

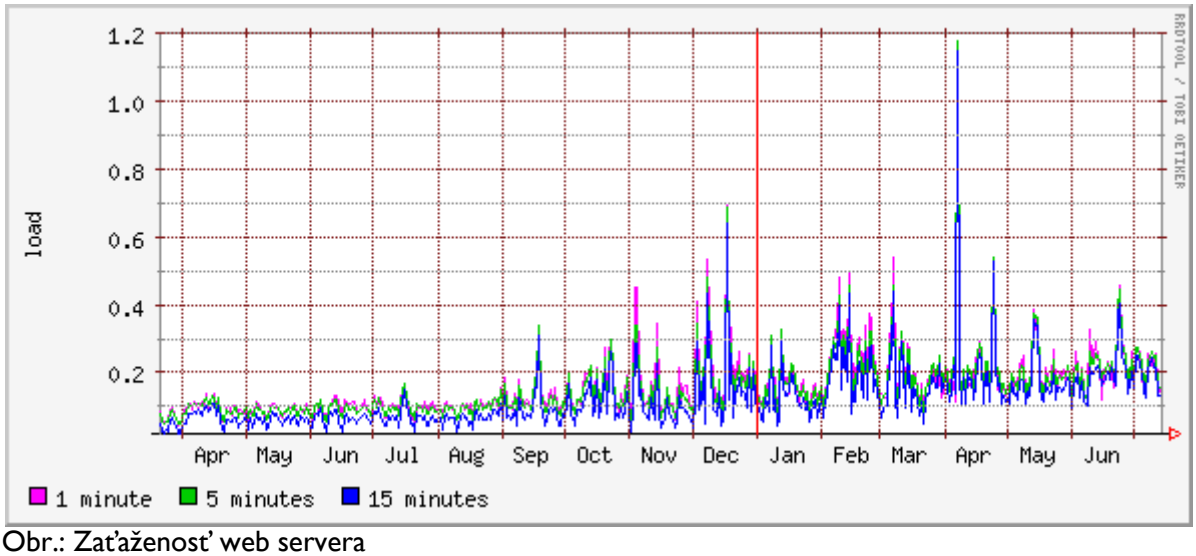
Už dlhodobo zaznamenávame sťažnosti na špekulatívne registrácie domén, keď sú isté domény obsadené už niekoľko rokov bez zaplatenia poplatku registrátora za prístup k záznamu domény. Tento stav je spôsobený modelom poskytovania služby, pretože registrátori platia za prístup k záznamu domény až po jej registrácii. Hoci v minulosti už bola prijatá zmena, že doména sa môže dostať iba dvakrát do stavu HELD bez zaplatenia poplatku, problém to však vyriešilo len čiastočne. Sťažnosti sa týkajú tiež veľkého administratívneho zaťaženia užívateľov pri prvom registrovaní domény a pri zmene registrátora. Situácia sa dá vyriešiť komplexnou zmenou Pravidiel, ktorú schváli riadiaca komisia, zložená zo zástupcov Ministerstva financií SR, spoločnosti SK-NIC, a.s. a miestnej internetovej komunity.

Technický stav

Technický stav systému SK-NIC bol počas sledovaného obdobia vyvážený, okrem viac-menej pravidelných snáh o neoprávnený prístup do systému. Rast databázovej záťaže súvisel s rastúcim počtom domén a počtom užívateľov i registrátorov systému. Pokles záťaže DB servera súvisí s úpravou aplikácie a prístupu k databáze.



Obr.: Zaťaženosť DB servera



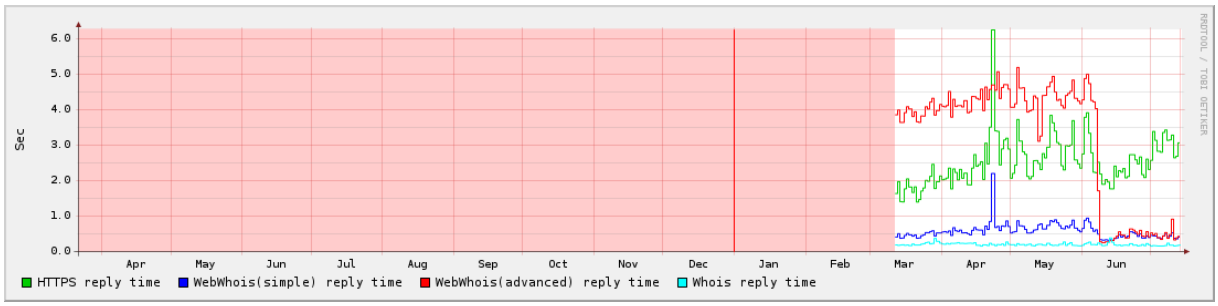
Obr.: Zaťaženosť web servera

Práce vykonané počas príslušného obdobia

V súvislosti s prechodom slovenskej meny na menu euro bolo v systéme SK-NIC vykonaných niekoľko technických opatrení. Obmedzenie systému bolo minimálne. Tatra banka, a.s. nás informovala, že v období od 31. 12. 2008 od 15.00 hod. bude úplná technická odstávka internet bankingu. Keďže systém SK-NIC je napojený na účet vedený v Tatra banke a využíva platobné prostriedky TatraPay a CardPay, upozornili sme všetkých registrátorov , aby si poplatky za domény, splatné v čase 29. 12. 2008 až 07. 01. 2009 uhradili v predstihu, pretože by sa mohlo stať, že o platbe nebude systém SK-NIC zo strany banky informovaný a doména exspiruje, resp. bude deaktivovaná.

1. marca 2009 sa v systéme SK-NIC spustila prevádzka tzv. systému CAPTCHA. V prípade, že je subjekt registrátorom viac než 10 domén a počet jeho neuhradených domén je vyšší ako počet ním uhradených domén, bude nútený pre registráciu domény použiť overenie prostredníctvom tzv. CAPTCHA kódu. Akýkoľvek automatický nástroj pre prácu s portálom www.sk-nic.sk sa v tomto prípade stáva nefunkčným.

Od marca 2009 bol v systéme SK-NIC nasadený proces pravidelnej kontroly doby odozvy whois, http-whois a sk-nic webového rozhrania. Kontroly prebiehajú pravidelne každých 5 minút a generujú žltý resp. červený alarm v dohľadovom centre systému SK-NIC. Tieto časy sú graficky zaznamenávané a pravidelne vyhodnocované. Zhoršenie odozvy systému je najčastejšie spôsobené novým problémom, ktorý takto dokážeme skôr zachytiť, analyzovať a odstrániť.



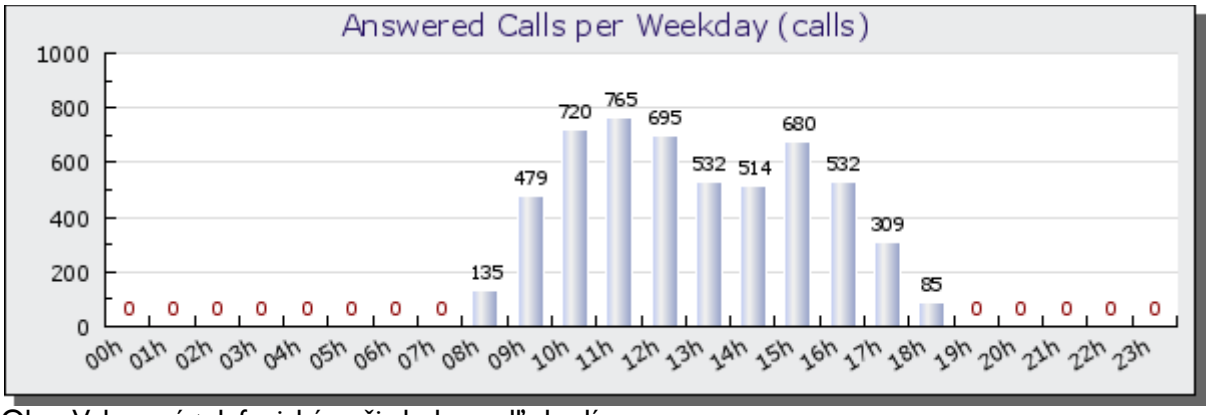
Obr.: SK-NIC plant response (LE6S)

V priebehu sledovaného obdobia sme začali pracovať na zlepšení komunikácie s bankovým informačným systémom. Cieľom je dosiahnuť zlepšenie stavu párovania platieb registrátorov za prístup k záznamu domény so systémom SK-NIC, resp. skrátenie lehoty, počas ktorej sa uhradená platba reálne prejaví na stave domény. Systém by mal začať fungovať v druhom polroku 2009.

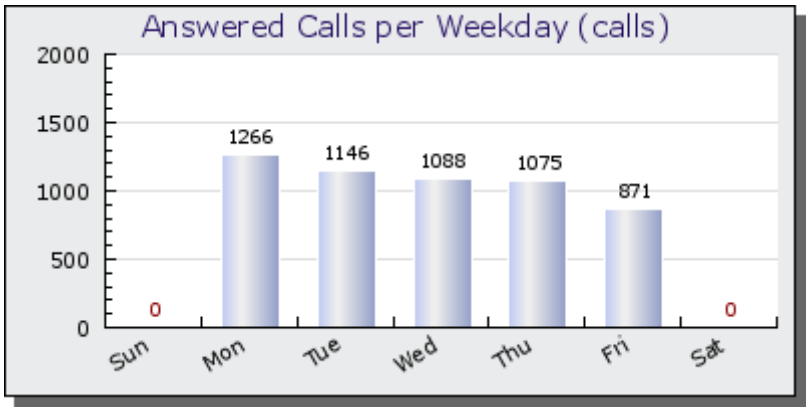
Helpdesk

V čase od 01.12.2008 do 31.05.2009 vybavil náš helpdesk 5 444 hovorov, čo je nárast oproti minulému obdobiu o 9,5 percenta, medziročne sa počet hovorov zvýšil o takmer 24 percent. Najviac hovorov prebiehalo v čase okolo 11:00. Najviac požiadaviek na helpdesk z dní v týždni bolo v pondelok. V tomto období operátori pretelefonovali so zákazníkmi celkovo 12 204 minút.

V čase od 01.12.2008 do 31.05.2009 odpovedali zamestnanci helpdesku na 8 274 e-mailových požiadaviek, čo je oproti predchádzajúcemu obdobiu nárast o približne 60 percent. Medziročne to znamená nárast o približne 29%. Nárast požiadaviek na helpdesk súvisí pravdepodobne so zmenou slovenskej meny na euro a zvýšený záujem registrátorov i užívateľov o informácie pri vykonávaní registračných operácií.



Obr.: Vybavené telefonické požiadavky podľa hodín



Obr.: Vybavené telefonické požiadavky podľa dní v týždni

SK-NIC v médiách

ČR: Pol milióna zaregistrovaných domén

[zive.sk 26/12/2008]

Ivan Kvasnica

Česi majú pol milióna registrovaných domén s koncovkou .cz. Hlási to združenie CZ.NIC, ktoré má správu českých domén pod palcom. Doména s poradovým číslom 500 000 bola obsadená 22. decembra vo večerných hodinách.

Pokorenie jubilejnej hranice sa v decembri stalo len otázkou času, veď počet domén CZ je jeden z najrýchlejšie rastúcich na svete. Od októbra 2007 ich bolo zaregistrovaných viac než dvestotisíc. Údajne aj vďaka vlastnému registračnému systému FRED, ktorý celý proces výrazne zjednodušil.

Počet slovenských domén nie je zatiaľ ani polovičný. Podľa verejných štatistík združenia SK-NIC ich je takmer 173 tisíc.

Swan vlani s celkovými výnosmi 33,65 mil. eur

[www.itnews.sk 11/02/2009]

Autor: SITA

Zisk alternatívneho telekomunikačného operátora Swan, a.s. pred započítaním daní, úrokov, odpisov a amortizácie (EBITDA) predstavoval za vlaňajšok 10,5 mil. eur, čo je medziročne viac o 61,5 %

Alternatívny telekomunikačný operátor Swan, a.s. dosiahol za minulý rok celkové výnosy 33,65 mil. eur, čo v medziročnom porovnaní predstavuje nárast výnosov o 37,9 %. Ako agentúru SITA informoval marketingový manažér operátora Martin Holák, výnosy dosiahla spoločnosť Swan najmä vďaka akvizíciám, vstupu na rezidenčný trh so službou triple play a získaním nových zákazníkov v korporátnom segmente a v štátnej správe.

Zisk operátora pred započítaním daní, úrokov, odpisov a amortizácie (EBITDA) predstavoval za vlaňajšok 10,5 mil. eur, čo je medziročne viac o 61,5 %. Pridaná hodnota vzrástla oproti predchádzajúcemu roku o 3,3 mil. eur na vlaňajších 14 mil. eur. "Hospodárske výsledky Swanu sú odrazom jeho dlhodobého rozvoja a stratégie, ako i nárastu spoločnosti vo všetkých oblastiach telekomunikačnej sféry," uviedol alternatívny telekomunikačný operátor. Investície Swanu do hmotného a nehmotného investičného majetku dosiahli v minulom roku celkovo 8,2 mil. eur, pričom smerovali najmä do rozvoja technológií a na výstavbu optickej siete. Rok predtým spoločnosť preinvestovala 6,4 mil. eur.

Spoločnosť Swan pôsobí na slovenskom trhu ako prevádzkovateľ verejných rádiotelekomunikačných služieb so zameraním na poskytovanie dátových, hlasových, internetových a multimediálnych služieb. Materskou firmou alternatívneho operátora je spoločnosť DanubiaTel, a.s., ktorá vlastní 100 % jeho akcií. Do skupiny patria taktiež firmy GlobalTel, a.s., Viasec, s.r.o., CNC, a.s. a SK - NIC, a.s. Skupina je zároveň vlastníkom 50-percentného podielu spoločnosti Net Slovakia, s.r.o.

Zmätočné názvy webov

[Markíza, 19:20 06/04/2009]

Miriam Kalisová, redaktorka TV Markíza: "Ak chcete vedieť kedy je v Čadci, Podolínci, či Rajeckých Tepliciach otvorená matrika a spoliehate sa na internet, máte smolu. Ak totiž do internetového prehliadača zadáte názov obce a príponu bodka sk, to čo chcete vedieť, sa nedozviete. Na stránkach sú reklamné prezentácie súkromných spoločností a samosprávy s tým nemôžu nič neurobiť."

Jaroslav Krafka, redaktor TV Markíza: "Namiesto slovenskej stránky Čadce nájdete nábytok. Rajecké Teplice vás presmerujú do reštaurácie a na stránke podolinec.sk nájdete informácie o výrobe reklamy. Mestá totiž predbehol v registrácii niekto iný."

Andrea Jančíková, vedúca kancelárie primátora: "Keď sme mali ešte záujem o koncovku sk, Spišská Nová Ves.sk, tak v tej dobe už bola doména s touto koncovkou obsadená."

Jaroslav Krafka, redaktor TV Markíza: "Preto museli oficiálnu prezentáciu mesta presunúť na európsku doménu bodka eu. Paralelne s ňou funguje aj jej slovenská obdoba, ktorá je na predaj. Samozrejme za vyššiu cenu. S tou istou situáciou sa stretli aj v bratislavskej mestskej časti Čunovo."

Gabriela Ferenčáková, starostka MČ Bratislava- Čunovo: "Sme zistili, že už je obsadená, že ju má nejaký súkromný vlastník, ktorý by ju nám bol teda predal za istú finančnú čiastku."

Jaroslav Krafka, redaktor TV Markíza: "Podľa slovenských pravidiel mestá nemajú v registrácii domén pred súkromníkmi prednosť."

telefonuje Patrik Krauspe, riaditeľ slovenského národného registrátora domén SK-NIC: "Geografické názvy nie sú chránenými názvami, chránenými názvami v rámci internetovej domény sk sú iba ochranné známky."

Jaroslav Krafka, redaktor TV Markíza: "Ojedinelé nie sú ani oficiálne stránky, ktoré si mestá prenajímajú od súkromníkov."

Juraj Grešš, poskytovateľ internetových služieb: "Za účelom nejakého zisku alebo nejakého zvýšenia príjmu."

Jaroslav Krafka, redaktor TV Markíza: "Odborníci na weby hovoria, aby mestá zbytočne nepreplácali stránky so slovenskou koncovkou, ak ju niekto ponúka za vysokú cenu."

Daniel Duriš, odborník na webové štandardy: "Vo väčšine prípadov možno je lepšie sa sústrediť na kvalitný obsah, rozvíjať ten obsah, rozvíjať tú stránku."

Jaroslav Krafka, redaktor TV Markíza: "Pretože stránky miest a obcí by mali byť najmä o informáciách, ktoré sú prehľadné, ľahko čitateľné pre slabozrakých a najmä aktuálne."

Jaroslav Krafka, TV Markíza.

Karta warta po roku prevádzky

[PC Revue 02/04/2009]

Zriadenie webovej stránky vo forme karty warta funguje už viac ako rok. Zopakujeme, že karta warta umožňuje zaregistrovať si vlastnú doménu napr. v tvare www.mojafirma.sk a prevádzkovať ju na dobu 12 mesiacov, všetko bez zmlúv a faktúr. Okrem toho máte k dispozícii priestor 1 GB na webovú lokalitu a elektronickú poštu, originálne účty elektronickej pošty napr. vo forme riaditel@mojafirma. sk. K tomu patrí ešte prevádzka webovej lokality s podporou skriptovacieho jazyka PHP, možnosť vytvorenia FTP účtov, podpora databázy MySQL a servisná podpora napr. aj

diaľkovým ovládaním vášho počítača, pokiaľ to dovolíte. Nás zaujímalo, čo sa stane po roku prevádzky, teda ako vo všetkých vytvorených službách pokračovať. Dobrá správa je, že cena pri pokračovaní služieb sa nemení, predĺženie o ďalší rok prevádzky vás bude stáť takú istú sumu ako zriadenie a prevádzkovanie novej domény. Najjednoduchšie sa to dá realizovať nákupom novej karty warta, ktorú možno kúpiť pomerne jednoducho, špecialitou je nákup na pošte, prípadne zakúpenie karty warta cez internet (tzv.

virtuálna karta). Odporúčaná cena je 39, 50 eura / 1189, 98 Sk, v cene sú zahrnuté všetky poplatky vrátane poplatku za registráciu domény . sk na obdobie ďalších 12 mesiacov. Prevádzkovateľ vás pritom 14 dní pred exspiráciou domény vyzve na pokračovanie v službách. Od tejto chvíle máte 28 dní na to, aby prevádzkovateľ mohol zabezpečiť pokračovanie služieb v pôvodnej doméne. Žiaľ, zatiaľ si nemožno zakúpiť naraz viac kariet warta a takto si dopredu predplatiť doménu na dlhšie obdobie. Problémom je to, že registrátor domén SK-NIC nateraz neumožňuje zakúpiť si doménu na viac ako jeden rok. Existuje však možnosť prejsť na fakturačný systém platieb, čo sa dá realizovať pomocou kontaktovania úseku služieb zákazníkom. Predĺženie služieb sa realizuje napr. pomocou stránky www. warta. sk výberom položky aktivácia karty warta, pričom v následne vzniknutom okne vyberiete ako typ aktivácie predĺženie služby na ďalšie obdobie. Po zadaní aktivačného kódu a sériového čísla z karty warta sa vaša žiadosť zaregistruje a spracuje. O úspešnej aktivácii služieb na ďalšie obdobie ste následne informovaní pomocou rekapitulácie služieb. Od tejto chvíle pokračuje poskytovanie služieb na dobu ďalších 12 mesiacov.

Bezpečnosť TLS na slovenských serveroch

[www.itnews.sk 15/01/2009]

Juraj Bednár

Po mnohých bezpečnostných problémoch v protokole TLS a predovšetkým v procesoch vydávania certifikátov, na ktoré upozorňujú bezpečnostní analytici, sme sa rozhodli pozrieť na certifikáty TLS internet bankingov a chránených zón finančných a iných inštitúcií na Slovensku.

O aké problémy ide? V roku 2001 autor tohto článku poukázal na nie dostatočne bezpečné procesy pri vydávaní certifikátov v časopise 2600. Išlo o zneužitie procesných chýb na získanie platného certifikátu od certifikačnej autority bez toho, aby mal žiadateľ na tento certifikát právo. Na získanie certifikátu stačil internetový prehliadač, e-mailový klient a fax. Začiatkom tohto roka sa objavili ďalšie podobné problémy.

Od roku 2006 však už zďaleka neplatí, že všetky certifikáty sú si rovné. Povieme si o základných vlastnostiach certifikátov. V tomto prieskume sa nebudeme zameriavať na bezpečnosť šifier, hashovacích funkcií či podpisových algoritmov. Tie boli vo všetkých prípadoch podľa dostupných štandardov dostačujúce.

Certifikačná autorita

Na to, aby bol internetový prehliadač (prípadne e-mailový klient) schopný overiť identitu druhej strany, je potrebný certifikát, ktorý je súhrnom informácií o druhej strane a obsahuje predovšetkým dátum platnosti, meno servera (common name) a verejný kľúč servera. Tieto informácie sú digitálne podpísané. Na to, aby bol prehliadač schopný overiť identitu, musí sa certifikačná autorita nachádzať v prehliadači. Mnohé certifikačné autority spĺňajúce bezpečnostné požiadavky tvorcov prehliadačov sú predinštalované. Toto je jediný spôsob, ako získať prístup pomocou protokolu HTTPS bez varovného okna o nezabezpečení a zároveň úplne základný predpoklad zabezpečenej stránky.

Okrem predinštalovaných certifikačných autorít existuje veľa iných a mnohé z nich majú zmysel. Predovšetkým ide o interné certifikačné autority, používané vo firemnom prostredí, a o certifikačné autority pracujúce v súlade so zákonom o elektronickom podpise. Tieto certifikačné autority však nie sú predinštalované v prehliadačoch a na použitie ich treba nainštalovať. Inštalácia často závisí od nezabezpečeného protokolu HTTP, ktorý je náchylný na rôzne druhy útokov. Predovšetkým pri certifikačných autoritách pôsobiacich v rámci zákona o elektronickom podpise vidíme, že väčšinou neposkytujú celú cestu od koreňovej certifikačnej autority Národného bezpečnostného úradu. Keby tak robili, stačilo by nainštalovať koreňový certifikát NBÚ a všetky akreditované certifikačné autority by boli okamžite overené. Je nám doteraz záhadou, prečo tak nerobia.

Koreňový certifikát NBÚ na tom však nie je o nič lepšie - poskytuje sa cez nezabezpečené spojenie. Už len keby NBÚ investoval do jedného CA zahraničnej predplatenej komerčnej CA, bola by bezpečnosť oveľa vyššia. Môže sa tvariť, že zahraničné CA, ktoré poznajú prehliadače, neexistujú, lebo neoperujú v súlade so slovenským právnym poriadkom, no poskytovaním koreňového certifikátu bez zabezpečenia robia situáciu ešte horšou. Podobne funguje väčšina komerčných akreditovaných certifikačných autorít. Neexistuje tak (jednoduchý) bezpečný spôsob ich inštalácie a overenia. Najlepšie, na čo sme prišli, je zatelefonovať do certifikačnej autority, aby nám nadiktovali tzv. odtlačok certifikátu. Je to praktické?

Z bankových inštitúcií túto zásadnú požiadavku nespĺňa len ČSOB, ktorá navyše používa českú certifikačnú autoritu. Na telefonickej linke ČSOB nám poradili, aby sme si odtlačok certifikátu pozreli na webe. Cez nezabezpečené spojenie.

Z iných inštitúcií, na ktoré sme sa rozhodli pozrieť, túto základnú požiadavku nespĺňa ani SK-NIC - monopolný národný registrátor domén. Využíva služby Prvej Slovenskej Certifikačnej Autority, ktorá tiež neposkytuje koreňový certifikát cez zabezpečené spojenie.

Overenie držiteľstva domény

Certifikačná autorita držiteľstvo domény kontroluje dvoma spôsobmi: poslaním e-mailu na adresu, ktorú si certifikačná autorita vygeneruje, a tým, že certifikačná autorita požiada držiteľa domény, aby na konkrétnu cestu umiestnil konkrétny dokument. Certifikačná autorita teda overuje držiteľstvo domény spôsobom, ktorý je náchylný na útoky, ktorým sa celá certifikácia snaží brániť. Na druhej strane útočník musí byť schopný spraviť útok presne v čase vydania certifikátu. Má však možnosť o certifikát aj kedykoľvek požiadať. A tu je kameň úrazu - certifikát, ktorý overuje iba držiteľstvo domény, a certifikát overujúci do istej miery aj identitu sa nedá na prvý pohľad rozlíšiť. Treba sa pozrieť na podrobné informácie o certifikáte.

Overenie identity

Overenie identity umožní držiteľovi certifikátu mať na ňom okrem domény napísané aj obchodné meno spoločnosti. Procedúra na overenie obchodného mena sa často líši v závislosti od autority (a znova pripomíname, že bežný používateľ na prvý pohľad nezbadá, kto certifikát vydal, musí sa na to špeciálne pozrieť). Neraz na overenie identity stačí tzv. business license, čo je výpis z obchodného registra. Slovenský súd vydá výpis z obchodného registra akejkoľvek spoločnosti bez overenia identity. Ten potom stačí odfaxovať, prípadne počkať na telefonické overenie.

Rozšírené overenie identity

Práve na boj proti takýmto praktikám niektoré certifikačné autority vymysleli spôsob overovania s názvom Extended Validation. Ten je už v najnovších prehliadačoch implementovaný. V prípade, že stránka tento spôsob podporuje, prehliadače to indikujú väčšinou zeleným pásikom s URL (adresou), vedľa ktorej sa nachádza meno spoločnosti, ktorej bol certifikát vydaný, prípadne certifikačná autorita.

Používateľ môže tento fakt vizuálne overiť, a ak stránka jeho banky alebo iná citlivá stránka zrazu nemá zelený pásik s adresou, prípadne je na ňom napísané meno inej inštitúcie, bude opatrnejší a nezadá stránke nijaké prihlasovacie údaje. Je to jediný spôsob, ako na prvý pohľad odlíšiť úroveň overovania zákazníka. Procedúra na vydanie certifikátu s rozšíreným overením identity je oveľa presnejšia a zložitejšia.

Rozšírené overenie je pomerne nové, ale aj napriek tomu sme očakávali častejšie využívanie hlavne pri bankových inštitúciách. Zo 16 inštitúcií, na ktoré sme sa pozreli, sa o proces rozšírenej validácie úspešne pokúsili len štyri. Pri zvyšných inštitúciách sa teda musíme uspokojiť so štandardným overením a pri spomínaných dvoch inštitúciách prakticky so žiadnym overením, hoci teoretická možnosť overenia existuje.

Prechod na euro odstaví internetové bankovníctva i obchody

[zive.sk 20/12/2008]

Ivan Kvasnica

Príchod eura prináša aj komplikácie. Na ktoré veci si dať pozor, čoho sa vystríhať.

Vaša téma Hoci prechod Slovenska zo slovenskej koruny na euro je skôr záležitosťou ekonomickej obce, nevyhne sa samozrejme ani ostatným. Priamo sa dotkne aj ľudí pracujúcich v IT odvetví.

Každá zmena znamená, že sa musia vykonať príslušné úpravy rôznych systémov. Nová mena nie je výnimkou. Najviac zainteresované budú azda banky a ich internetové bankovníctvo, platobné systémy a karty.

Internet banking len v pasívnej forme

Výpadok hlásia všetky banky približne od 1. do 4. januára roku 2009, kedy budú pre bežné platobné príkazy nedostupné aj pobočky. Obmedzenia sa týkajú aj telefónneho bankovníctva. Platobné príkazy zadané v tomto období sa zrealizujú až 5. januára.

O podobnej nedostupnosti služieb musia banky informovať aspoň mesiac pred zavedením eura v pobočkách a na internetových stránkach. Túto povinnosť im ukladá Zákon o zavedení meny euro v Slovenskej republike.

Náš rýchly test neodhalil prakticky žiadne pochybenia. Ukážkové informácie poskytuje napríklad Tatra banka, ktorá priamo na stránkach internet bankingu zverejnila konkrétne termíny a obmedzenia, na ktoré sa musia klienti začiatkom roka pripraviť. Už 31. decembra nebude dostupné internetové bankovníctvo, počas prvých štyroch dní nového roka sa sprístupní pasívna verzia. Klienti si tak môžu skontrolovať stav účtov k poslednému decembrovému dňu. Ďalšia úplná odstávka prebehne 4. januára. Nasledujúci deň by mali byť dostupné všetky služby.

Slovenská sporiteľňa odkazuje na euroinformácie na svojej hlavnej stránke, v internetovom bankovníctve nie. Klientom taktiež ponúkne pasívnu verziu od 1. do 4. januára.

ČSOB a VÚB hlásia výpadok od 31. decembra do 5. januára. Druhá menovaná banka bude mať kompletnú odstávku od posledného dňa aktuálneho roku od 21. hodiny do popoludňajších hodín prvého januárového dňa. Odstávku zažije aj internetová mBank, a to od 8. hodiny posledného dňa roku 2008. Systém bude prijímať platobné príkazy 2. januára, následne sa však opäť zneprístupní až do 4. januára.

Dexia banka sprístupnila detailné informácie na prihlasovacej stránke internet bankingu. Príkazy sa budú spracovávať do 9:30. Poštová banka prijme platobné príkazy maximálne do 12. hodiny silvestrovského dňa. Na stránkach OTP Banky sme žiadne informácie o odstávkach nenašli, hoci inak poskytuje k euru podrobné informácie. Prinášame prehľadnú tabuľku s odkazmi na detailné údaje jednotlivých bánk.

O polnoci si peniaze nevyberiete

Zaujímavé sú aj informácie o obmedzení funkčnosti bankomatov a platobných kariet. Niektoré banky upozorňujú na ich krátkodobý výpadok. Slovenská sporiteľňa hlási len minimálnu nedostupnosť. Tatrabanka je konkrétnejšia - bankomaty a platobné karty nevyužijete na prelome rokov približne od 23. do 2. hodiny.

Odstávku bude mať aj VÚB. Platobné karty môžu mať problémy medzi 23. hodinou a polnocou. V rovnakú hodinu sa pripravte na nedostupnosť bankomatov ČSOB.

Platobné karty mBank môžete používať bez obmedzenia. Internetová banka ale upozorňuje na fakt, že z bankomatov nemusíte hneď po polnoci dostať hotovosť v eurách. Stane sa tak až po výmene meny v konkrétnom bankomate.

Vo všeobecnosti platí, že s výberom hotovosti alebo platbou kartou môžete mať s blížiacou sa silvestrovskou polnocou problémy ako s posielaním SMS správ. Detailné informácie nájdete po navštívení vyššie uvedených odkazov. Jednotlivé časy uvádzame opäť v tabuľke.

Výpadok platobných systémov bude mať za následok aj nedostupnosť niektorých internetových obchodov. Medzi tradične najobľúbenejšie patria e-shopy mobilných operátorov. Výpadky sú väčšieho rozsahu než služby internetového bankovníctva. Telefónica O2 doručuje objednávky prijaté po 23. decembri až od 7. januára 2009, pričom účtované budú už v eurách. Orange dokonca deklaruje nefunkčnosť všetkých svojich portálov (orange.sk, orangeportal.sk, e-shop a orangeclick.sk) od 31. decembra 22. hodiny do 2. januára 7. hodiny. T-Mobile žiadne informácie neuvádza.

Detailnejšie sa mobilným operátorom a prechodu na euro venujeme v samostatnom článku na MobilMania.sk.

Pozor na nezaplatené domény

Pozor by ste si mali dávať aj v prípade, ak vlastníte niektorú slovenskú doménu, ktorej v nasledujúcom období vyprší platnosť. Správca domén SK-NIC na stránkach upozorňuje na nedostupnosť služieb TatraPay a CardPay od 31. decembra od 12. hodiny do 4. januára. Platiť nebude možné, ako sme už písali, ani inými spôsobmi.

V systéme SK-NIC sa to prejaví tým, že si klienti nebudú môcť vytvárať proforma faktúry od posledného dňa tohto roku (od 12. hodiny) do obeda 2. januára. Podľa riaditeľa spoločnosti Patrika

Krauspeho to nie je príliš veľký dôvod na pozastavovanie expirácie domén. Navyše, systém na podobné zásahy nie je pripravený.

Registrátori boli na uvedené skutočnosti vopred upozornení aj s podrobným časovým harmonogramom e-mailom. "Veľkí registrátori budú môcť uhrádzať domény takmer bez prestávky," dodáva.

Internetoví používatelia by sa mali z dôvodu výpadkov platobných systémov bánk pripraviť aj na výpadky iných internetových obchodov či služieb. Napríklad internetová peňaženka Moneybookers rozosiela svojim používateľom informačný e-mail. Korunové účty sa zmenia na eurové až 12. januára.

Prechod na euro už ale stihol priniesť aj príjemnejšiu skutočnosť. Tretí mobilný operátor O2 totiž zlacnil o niekoľko halierov volania, SMS a MMS správy až do 16 percent. Orange nové paušály uviedol priamo v zaokrúhlených eurových cenách.

Desiatky slovenských domén aktívne distribuujú malware

[www.itnews.sk 07/01/2009]

Rastislav Turek

Asi pred pol rokom som sa začal trošku zaujímať o slovenské domény. Vtedy som napísal článok so štatistikami, ktorý som mienil písať každý mesiac. Dodnes ma to nepustilo, akurát som sa rozhodol pre ne urobiť celý web, nech to nemusím robiť ručne.

Keďže mám toho dosť veľa, moc sa mi nedarí dokončiť tento web a tak som sa rozhodol podeliť sa s vami aspoň o niekoľko veľmi zaujímavých informácií. Jednou z vecí, ktoré kontrolujem na doménach je aj to, či nerozširujú malware (vírusy, trojany, atď.). Táto informácie je pre mňa veľmi dôležitá hlavne preto, že na väčšine týchto domén existuje zraniteľnosť v podobe RFI (Remote File Inclusion), resp. persistant XSS.

Samozrejme mi to dáva aj iné informácie. Napríklad, aké skupiny infikujú tieto weby, aký malware distribuujú, akou metódou, ako sa dostali na web, atď. Tieto informácie mi slúžia k lepšiemu poznaniu ich správaniu a potom samozrejme aj k lepšej prevencii. Tieto informácie zdieľam aj s Davidom Vorelom z projektu HoneyNet, ktorý ich analyzuje a získava z nich ďalšie užitočné dáta.

Ako to celé funguje

O malwari distribuovanom cez XSS som písal už mnohokrát, ale skúsim vám priblížiť postup, akým sa malware dostane na konkrétny web a čo znamená nielen pre návštevníkov, ale aj majiteľa webu.

Aby mohol byť malware umiestnený niekam na web, musí mať útočník možnosť zmeniť kód webu. Na to existuje niekoľko možností, väčšinou sa jedná o využitie bezpečnostnej zraniteľnosti. Keby som chcel rozdeliť tie najzákladnejšie postupy, akým sa dostávajú útočníci k deravým webom, bolo by to asi takto:

Automaticky, robotom

Ručne, hľadaním náhodnej zraniteľnosti

Ďalej sa dajú tieto pokusy o získanie prístupu rozdeliť podľa miesta, na ktoré sa útočí.

FTP, SSH, RPC

WEB (napríklad XSS, SQL injection, RFI, remote upload)

SQL

Sociálne inžinierstvo, slabé a často používané heslá

Aby mohol útočník spustiť akéhokoľvek robota, musí vedieť, akú zraniteľnosť bude hľadať. Preto sa najčastejšie zameriavajú na tie najrozšírenejšie systémy, ako napríklad blogovací systém Wordpress, či rôzne fóra.

Niektoré staršie systémy bez ochrany umožňujú vložiť do komentárov odkazy, ktoré útočníci nahradzujú napríklad iframom, takže sa nejedná tak úplne o hackerský spôsob. Výsledok je však úplne rovnaký.

Keď útočník pozná zraniteľnosť daného systému, často využíva tzv. Google Dorks pre nájdenie patričného systému. Napríklad, ak hľadá Wordpress konkrétnej verzie, stačí do Google zadať

"<meta name=generator content=WordPress 2.0.3"

Samozrejme, ide to aj inak, ale to nie je podstatou tohoto článku. Keď robot získa výsledky z Googlu, začne ich prehľadávať a skúšať otestovať, resp. použiť danú zraniteľnosť. Ak je potvrdená, buď tento web označí a hľadá ďalej, alebo vykoná dopredu pripravené úkony. Na takúto činnosť bývajú používané aj samotné botnety a nie je ich málo. Takto vedia útočníci infikovať doslova tisíce webov behom niekoľkých dní. Ručne sa hľadajú zraniteľnosti na weboch len veľmi zriedka a to hlavne v prípadoch, keď je záujem infikovať konkrétny web. Dôvodov môže byť veľké množstvo, napríklad vysoká návštevnosť, prestíž webu, atď.

Weby sa dnes infikujú najčastejšie za pomoci iframov a JavaScriptu a to hlavne kvôli možnosti udržiavať ich dlhodobo živé. Tento kód býva vždy schovaný tak, aby ho nebolo jednoduché rozoznať pre bežného laika. JavaScripty majú veľmi často morfovaný (maskovaný) kód, aby nebolo možné poznať jeho obsah voľným okom. Používať vzdialené načítavanie stránok má svoju logiku. Za prvé si majiteľ webu nevšimne žiadny vyšší traffic, ktorý by tam mohol vzniknúť, ak by návštevníci sťahovali malware priamo z jeho servera. Taktiež je možné udržiavať takýto kód "živý" oveľa dlhšie. Ak je doména, ktorá distribuuje malware označená, je jednoducho vymenená za inú. Tento úkon sťažuje identifikáciu infikovaných domén, ktoré distribuujú malware. Aktuálne pridávajú útočníci aj niekoľko ďalších ochranných techník, ako napríklad overovanie IP adries, či referera. Ak potencionálna obeť používa IP adresu, ktorú má vo svojom "portfóliu" Google, pravdepodobne sa jedná o jeho testovacieho robota, ktorý sa snaží odhaliť takéto weby. Kód teda zostane neaktívny a robot ho neodhalí. Príklad červa, ktorého som našiel na jednom webe si môžete pozrieť na našom fóre.

Hneď ako je web úspešne infikovaný, začne pôsobiť samotný malware. Tu sa tiež využíva niekoľko techník pre distribúciu. Tou najpoužívanejšou je samozrejme sociálne inžinierstvo. Najčastejšie vám vyskočí hláška, že ak chcete vidieť nejaké video, potrebujete stiahnuť kódek a ponúkne vám ho na stiahnutie. Sofistikovanejší útočníci po stiahnutí softvéru prehrajú žiadané video a tak obeť nemá žiadne pochybnosti. Druhým veľmi častým spôsobom je skúšanie rôznych bezpečnostných chýb samotných prehliadačov. Táto metóda je v mnohých prípadoch úspešná, keďže podstatná časť užívateľov si neaktualizuje svoje softvérové vybavenie (často so slovami: "Veď mi slúži dobre, tak načo"). Prehliadač je dnes jednou z najzraniteľnejších častí.

Určite ste si spomenuli na antivírusovú ochranu. Áno, aj tá vám čo to pomôže, no veľmi sa spoliehať na antivírus nemôžete. Anti-vírus vás chráni pred tým, čo pozná. Pre šikovných útočníkov je otázkou

niekoľkých málo minút upraviť kód malwaru tak, že ho antivírus už neodhalí. Najsofistikovanejší malware využíva rôzne techniky automatického morfovania kódu tak, že ho mení pri každom pokuse o infikáciu obete. Na tieto účely býva veľmi často používaný práve JavaScript. Žiadny antivírus na svete vás nedokáže ochrániť pred takýmto malwarom, aj keď vám spoločnosti nasľubujú hory-doly. Ak sa chcete skutočne chrániť, určite nezabudnite na svoj prehliadač a zdravý, chladnokrvný rozum. To, že ste aktuálne na dôveryhodnom webe neznamená, že sa vás nesnaží infikovať. Ak používate Firefox, odporúčam okamžite nainštalovať rozšírenie NoScript. Toto rozšírenie vám automaticky blokuje všetky pokusy o spustenie škodlivého kódu a to aj pri povolení spúšťania globálnych skriptov.

Aké dôsledky má infikovanie webu

Dôsledky pre obeť sú jasné. Na 95% sa stanete súčasťou botnetu. Vaše súkromné dáta budú pravdepodobne nazdielané na servery útočníkov a začnete zasielať obrovské množstva spamu.

Pre majiteľa webu je v prípade odhalenia infikácie dôsledkom zablokovania webu v novších prehliadačoch so zapnutou ochranou ako aj zakázaný prístup z Googlu. Prístup na infikovaný web zabezpečuje aj Google Toolbar, ak ho máte nainštalovaný. To či je web infikovaný sa zisťuje z dvoch zdrojov. Prvým je databáza, ktorú plnia samotní ľudia. Rovnako je tomu aj pri phishingu. Druhým spôsobom je tzv. Honeyclient, ktorý sa pripája spolu s Google robotom na skúmaný web a čaká, či sa objaví nejaký malware, ktorý sa pokúsi o infikáciu. Ak sa tak stane, Google robot označí web za infikovaný a ten je potom blokovaný z vyššie popísaných miest.

Google sa pri tejto službe inšpiroval dlhšie fungujúcim projektom honeynet. Nám najbližší je práve český honeynet.cz, ktorý takýmto spôsobom prechádza rôzne infikované weby a následne skúma daný malware. Davidovi sa doteraz podarilo niekoľko veľmi zaujímavých objavov botnetov, ktoré podrobne popísal na webe. V jeho databázy môžete nájsť aj konkrétne weby, ktoré úspešne infikovali klienta a ako postupovali pri prvom spustení na počítači.

Slovenské domény

Bohužiaľ, aj na u nás na Slovensku máme niekoľko webov, ktoré sú infikované a snažia sa nakaziť príchodzích návštevníkov. Domén s funkčným malwarom je dnes u nás až 100. Tieto domény som po ich objavení zahlásil do databázy, aby bola aspoň časť užívateľov chránená pred nimi. Ďalších vyše 350 domén bolo, alebo stále je infikovaným dnes už nefunkčným kódom. Napriek tomu však väčšina týchto domén obsahuje rovnú zraniteľnosť a tak je to len otázka času, kým budú opätovne infikované.

Informácie o infikovaných doménach môžete získať aj priamo do Googlu, ak do url zadáte konkrétnu doménu:

http://www.google.com/safebrowsing/diagnostic?site=blog.synopsi.com

Google vám poskytne niekoľko informácií o tejto doméne.

Ochrana

V súvislosti s týmito doménami mi napadol jeden spôsob, ako by bolo možné chrániť všetkých užívateľov a to nielen tých, ktorí majú aktualizovaný a dobre ošetrený prehliadač, resp. systém. Celé riešenie spočíva v tom, nechať každý slovenský web prehľadávať robotom, ktorý bude kontrolovať, či sa na tomto webe nenachádza žiaden nebezpečný kód. Ak by sa našiel, bol by web označený za nebezpečný a kód by bol porovnaný s už existujúcou databázou, ktorú ponúka v rámci spolupráce

český honeynet. Ak by bol kód potvrdený aj z tejto databázy, bol by web zablokovaný na úrovni SK-NICu, pričom by sa zobrazovala varovná hláška. Ak by kód overený nebol, doména by šla na preskúmanie odborníkovi, ktorí by ju skontroloval a v prípade potreby zablokoval.

Určite budú niektorí namietať, že je to príliš drastické riešenie a ja súhlasím. No musíte brať do úvahy aj fakt, že tieto domény (resp. weby) poškodzujú svojich návštevníkov a je to vo väčšine prípadov ich chyba (občas za to môže aj hostingová spoločnosť), že je ich web deravý a že bol infikovaný malwarom. Po zablokovaní má samozrejme majiteľ webu možnosť kód odstrániť a doména bude opäť sfunkčnená. Je potrebné si uvedomiť, že tu nejde o desaťtisíce domén, ale o niekoľko stoviek. To pri súčasnom počte cca. 170 000 slovenských domén a cca. 500 infikovaných predstavuje približne 0,3%. Takáto ochrana však môže ochrániť tisícky návštevníkov pred infikovaním škodlivým kódom.

Nebránim sa však ani iným nápadom, ak poznáte lepší spôsob ako zaručiť čo najvyššiu mieru bezpečnosti ľuďom na Slovensku.

Mne je samozrejme jasné, že pri súčasnom stave SK-NICu sa o niečom takomto ani len nedá uvažovať, ale ja pevne verím, že sa tento stav čoskoro zmení, ale o tom zase inokedy.