.news 18 2012

Vážení čtenáři,

mezi tímto a předešlým vydáním našeho .newsu uplynulo půl roku a možná se tedy ptáte, proč tomu tak je. Důvod je zřejmý. Naše interní komunikační prostředky, ať už je to .blog, Twitter CZ.NIC atd., bohatě v průběhu doby pokryjí naše potřeby, a tak jsme se rozhodli udělat z .newsu jakousi „kroniku CZ.NIC“, v níž dvakrát do roka najdete to nejzajímavější od nás a z našeho více či méně vzdáleného okolí. Pojďme se tedy podívat na to, co přineslo posledních šest měsíců.

Projektu číslo jedna jsme jako již tradičně věnovali otvírák. S jeho pomocí vás můžeme nasměrovat k dalším informacím o našem vlastním DNS serveru Knot DNS. Jeho první verze byla představena na začátku listopadu loňského roku na mezinárodní konferenci RIPE ve Vídni. Jedná se o teprve třetí DNS server, takže jeho zveřejnění a vývoj vzbuzují patřičný zájem. Jen ještě dodám, že na svědomí ho mají kolegové z našich Laboratoří.

Další významné události spojené s koncem roku souvisejí s DNSSEC. Během posledních měsíců minulého roku se totiž k zavedení této bezpečnostní technologie přihlásily společnosti Vodafone a Telefónica. Gratuluji tímto technickým týmům oběma firem a také jejich zákazníkům k získání většího bezpečí na internetu. Druhá vlna informací týkající se DNSSEC na domácí scéně přišla těsně před koncem starého roku, kdy se do podepisování „svých“ domén pustili registrátoři INTERNET CZ, IGNUM, ONE.cz, GENERAL REGISTRY a AERO Trip PRO. Klobouk dolů i před nimi.

Na závěr zmíním už jen v krátkosti překročení hranice 40 000 mojeID účtů. K jejímu dosažení došlo v polovině prosince a já můžu s radostí dodat, že padesátka není daleko.

Příjemné čtení vám přeje,
Ondřej Filip, *výkonný ředitel sdružení CZ.NIC*

CZ.NIC představil vlastní DNS server

Prohlížení internetových stránek, posílání e-mailů, internetová telefonie... Nic z to-ho by nebylo možné, kdyby správně nefungovaly DNS servery. Pro jejich provoz byly z hlediska velkých doménových registrů k dispozici až do 3. listopadu prakticky pouze dva volně dostupné systémy – BIND a NSD. Zástupci CZ.NIC však v listopadu loňského roku představili na mezinárodní konferenci RIPE 63 ve Vídni vlastní DNS server – Knot DNS. Větší nabídka svobodných implementací je výhodnější například pro zajištění stability provozu důležitých domén, jako je například kořenová zóna nebo domény nejvyšší úrovně jako .CZ, .COM, apod. Další implementace napsaná na zelené louce zvýší diverzitu dostupných řešení a s tím i pravděpodobnost, že v případě technických potíží některého systému bude dál možné poskytovat veškeré on-line služby na globální úrovni.

Hlavními přednostmi serveru Knot DNS jsou výkon, škálovatelnost, rychlost a možnost přidávat a odebírat zóny za běhu bez výpadku v provozu serveru. Knot DNS je také zajímavý svým vícevláknovým návrhem, který téměř nepoužívá zámky. Také díky tomu dosahuje Knot DNS i na běžně dostupném hardwaru o výkonu okolo 200 tisíc dotazů za sekundu.

Cílem bylo navrhnout server flexibilní jako BIND, ale s rychlostí NSD. Řešení vytvořené v Laboratořích CZ.NIC je vhodné především pro ty, kteří potřebují autoritativní DNS server, jako jsou třeba operátoři provozující stovky tisíc domén. Knot DNS je napsaný v programovacím jazyce C, podporuje prakticky všechny unixové systémy a je vydaný pod licencí GPL (verze 3). V současnosti se projekt nachází ve fázi beta verze, zdrojové kódy a další informace jsou dostupné na internetové adrese www.knot-dns.cz.

I přesto, že je Knot DNS teprve v beta verzi, tak již nyní obsluhuje některé domény v rámci sdružení CZ.NIC. Zástupci Laboratoří CZ.NIC samozřejmě ocení, pokud se do testování zapojí i odborná veřejnost; toto testování by mělo pokrýt co největší rozsah možných scénářů použití DNS serverů. Pro hlášení chyb je možné využít buď webové rozhraní na adrese https://git.nic.cz/redmine/projects/knot-dns, nebo mailovou konferenci knot-dns-users@lists.nic.cz.

MOJEID MÁ UŽ VÍCE NEŽ 40 000 UŽIVATELŮ

Již 40 tisíc uživatelů má od poloviny prosince uložené své údaje na jednom bezpečném místě, tedy v registru mojeID identit. Jejich správa je tak velice jednoduchá a rychlá. A nejen to!

VÍCE

REGISTRÁTOŘI ZAVEDLI DNSSEC

Pět registrátorů domén .CZ zavedlo na přelomu roku DNSSEC. Bezpečněji se tak teď mohou cítit i zákazníci společností INTERNET CZ, IGNUM, ONE.cz, GENERAL REGISTRY a AERO Trip PRO.

VÍCE

ZMĚNY V DOKUMENTECH CHRÁNÍ PŘEDEVŠÍM DRŽITELE DOMÉN

Smyslem přijatých změn je v první řadě zvýšení ochrany práv a bezpečnosti osobních údajů držitelů domén a současně další posílení zabezpečení databáze proti automatizovanému získávání dat.

VÍCE

VÍTE, ŽE

... CZ.NIC zveřejnil koncepci na další období?

Dokument platí pro roky 2012 až 2015 a hlavními posláními sdružení zůstávají i v tomto období provozování důvěryhodné, bezpečné a stabilní infrastruktury a obecně prospěšných internetových služeb, zejména domény .CZ, ku prospěchu lokální internetové komunity v České republice.

MojeID má už více než 40 000 uživatelů

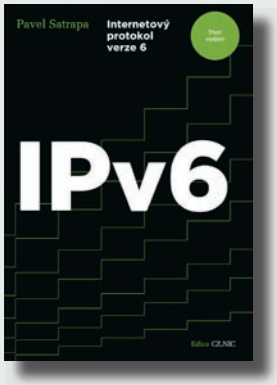
MojeID identitu, která mimo jiné umožňuje spravovat osobní údaje na jednom bezpečném místě a udržovat je stále aktuální, má od poloviny prosince loňského roku více než 40 tisíc uživatelů internetu z České republiky. Své mojeID přihlašovací údaje je možné použít na všech stránkách označených ikonami mojeID či OpenID. V České republice se v současnosti jedná o více než tři tisíce e-shopů, freemailovou službu Volný.cz, komunitní portál Líbímseti.cz nebo internetová média, například Lupa.cz, Živě.cz nebo E15.cz. Zvyšující se počet uživatelů mojeID je jasným signálem pro ty provozovatele webových služeb, kteří s jeho implementací váhají. Zavedením mojeID nejen že usnadní svým zákazníkům život na internetu, ale zároveň mohou získat nové. Spolu s tím budou mít vždy jistotu, že zákazník přihlášený přes mojeID je skutečná osoba s reálnými kontaktními údaji.
Díky mojeID také není potřeba zakládat si vždy nový účet a procházet opakovaně zdlouhavým a složitým procesem registrace. Protože jsou osobní údaje uloženy na jednom bezpečném místě, je jejich správa velice jednoduchá a rychlá.
MojeID je také služba, která od 26. října loňského roku umožňuje uživatelům českého internetu používat pro přihlašování na různé internetové stránky a k různým webovým službám jednotné identifikační údaje (uživatelské jméno a heslo). ■

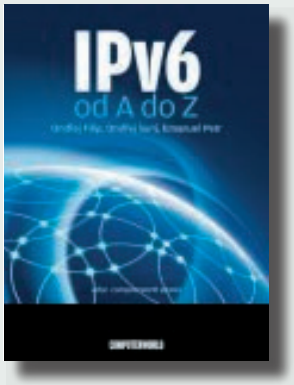
Certifikovaných je už celkem 11 registrátorů

Podnikání spojené s doménovými registracemi je stále oblíbenější. Od začátku roku 2008 se jen v Česku počet firem, které tuto službu nabízí, téměř ztrojnásobil. To s sebou nese nejen cenový boj výhodný pro zákazníka, ale také zvyšující se nepřehlednost celkové nabídky na trhu. CZ.NIC proto představil projekt certifikace registrátorů. Jeho cílem je poskytnout zájemcům o domény základní přehled o úrovni služeb jednotlivých registrátorů a definovat ideální vlastnosti a funkce registračního systému a souvisejících služeb.
Certifikace je dobrovolná a registrátor ji může kdykoliv podstoupit na základě vlastní žádosti. Při hodnocení jsou zohledněna kritéria jako možnost registrovat domény .CZ, kvalita nápovědy a dokumentace, technická funkčnost systému či doplňkové služby. Podle jejich úrovně může registrátor získat až pět hvězdiček, přičemž od jedné hvězdičky je oprávněn používat označení Registrátor certifikovaný pro maloobchod.
Projekt hodnocení je určen registrátorům zaměřeným na koncového zákazníka. Kritéria hodnocení jsou tudíž definována podle potřeb tohoto typu klienta. V rámci projektu se tak změnila i podoba záložky o registrátorech na adrese www.nic.cz; od této doby se tak pořadí registrátorů domén .CZ řídí výsledky hodnocení. U jednotlivých registrátorů najdou zájemci také ikony IPv6, DNSSEC a mojeID, které symbolizují, že daný registrátor tuto technologii nebo službu podporuje, nebo návod, jak nejrychleji a nejlépe zaregistrovat doménu .CZ. ■

Vyšly dvě publikace na téma IPv6

Na stránkách Edice CZ.NIC je od poloviny prosince k dispozici třetí vydání populární knihy vysokoškolského pedagoga a publicisty Pavla Satrapy s názvem IPv6. Oproti předchozímu vydání, které Edici CZ.NIC zahajovalo, je tato publikace bohatší přibližně o 50 stránek; na nich čtenáři najdou nejen aktuální informace spojené s protokolem IPv6, ale také nová témata, jakými jsou například přechodové mechanismy NAT64 a 6rd nebo směrovací démon BIRD.
Knihu IPv6 je možné si objednat nebo zdarma stáhnout na stránkách Edice CZ.NIC. K dispozici jsou formáty PDF, EPUB a MOBI.
Sdružení CZ.NIC založilo svou edici v roce 2008. První z knih, která byla v jejím rámci vydána, byla publikace Pavla Satrapy z Technické univerzity v Liberci o protokolu IPv6 (2. vydání). Druhou potom kniha Scotta Chacona s názvem Pro Git. Jako třetím přibyla na začátku loňského roku publikace Marka Pilgrima Dive Into Python 3.
Čtvrtým počinem je kniha vysokoškolského pedagoga a publicisty Jiřího Peterky s názvem Báječný svět elektronického podpisu.
Druhým titulem, s nímž je spojený CZ.NIC, konkrétně výkonný ředitel sdružení Ondřej Filip a členové Laboratoří CZ.NIC Ondřej Surý a Emanuel Petr, najdou zájemci na internetových stránkách nakladatelství eReading.cz. Publikace má název IPv6 od A do Z a obsahuje texty, které vycházely v loňském roce ve formě seriálu v tištěné verzi časopisu Computerworld. Dobrá zpráva pro zájemce o problematiku internetových protokolů: celkem devět dílů v „knižní" podobě je možné stáhnout zdarma. ■





Pět registrátorů zavedlo DNSSEC, Česká republika je na špici

Na přelomu roku 2011 a 2012 se pět českých registrátorů domén .CZ rozhodlo podepsat domény spravované na jejich jmenných serverech technologií DNSSEC. Z celkového počtu více než 889 tisíc domén .CZ je tak nyní tímto způsobem chráněno více než 35 procent . V meziročním srovnání to podle statistik sdružení CZ.NIC představuje nárůst o 200 tisíc domén.
35procentní podíl domén chráněných pomocí DNSSEC opět posunul českou národní doménu na nejvyšší příčku žebříčku domén nejvyšší úrovně, které tuto technologii zavedly a využívají ji. Druhá je švédská národní doména .SE, která zavedla DNSSEC jako vůbec první na světě.
Jsme rádi, že si stále více českých registrátorů k tomuto ochrannému opatření nachází cestu, a věříme, že se v budoucnu přidají další.
Registrátoři, kteří v nedávné době podepsali jimi spravované domény, jsou INTERNET CZ, IGNUM, ONE.cz, GENERAL REGISTRY a AERO Trip PRO. Přidali se tak ke společnostem ACTIVE 24, Web4U a ONESolution, jenž DNSSEC nabízejí automaticky již delší dobu.
DNSSEC je rozšíření systému DNS, které zvyšuje bezpečnost služby doménových jmen. Principem DNS je překlad jmenných internetových adres na adresy číselné, kterým počítače rozumějí a s jejichž pomocí dokážou zajistit zobrazování webových stránek, odesílání e-mailů, telefonování po internetu a další běžné internetové služby. DNSSEC zvyšuje bezpečnost při používání DNS tím, že brání podvržení falešných, pozměněných či neúplných údajů o doménových jménech. CZ.NIC zavedl tuto bezpečnostní technologii pro držitele domén .CZ a ENUM a uživatele českého internetu v roce 2008. Více informací na internetové adrese www.dnssec.cz.

Několik novinek z našich Laboratoří

Aktuálně největší projekt našich Laboratoří jsme představili v otvíráku tohoto čísla. DNS server KNOT však není jedinou novinkou, kterou se v posledním půlroce prezentovali kolegové z výzkumného a vývojového týmu. Pojďme si představit krátký výběr zajímavých počinů z nedávné doby.
Jedním takovým je IPv6 Laboratoř, která se zájemcům otevřela poprvé v listopadu loňského roku. Její návštěvníci si v rámci tohoto projektu mohou přijít vyzkoušet, jak jsou nebo nejsou jejich zařízení připravena na IPv6. IPv6 laboratoř se skládá z několika experimentálních sítí, ve kterých jsou služby dostupné pouze přes internetový protokol verze 6. Do této sítě je možné přistoupit buď klasickou ethernetovou přípojkou, pomocí bezdrátové sítě nebo prostřednictvím ADSL připojení. K dispozici je několik sítí s rozdílnou konfigurací. Do každé z nich je zapojen jeden nebo více virtuálních serverů určených pro testování aplikací deklarujících podporu IPv6. Více o tomto projektu najdete na stránkách Laboratoří CZ.NIC.
S IPv6 je spojený také webový tester IPv6 widget, jehož první verzi představily Laboratoře na začátku prosince. Widget umožňuje otestovat, zda uživatelův DNS resolver umí používat DNSSEC a jestli je jeho připojení připraveno na protokol IPv6. Software také změří rychlost připojení v obou směrech a na obou protokolech, tedy i na IPv4. Ovládání widgetu je intuitivní. Testy IPv6 konektivity a zabezpečení pomocí technologie DNSSEC se spouští automaticky po zobrazení widgetu na stránce. Test rychlosti připojení spustí uživatel kliknutím na tlačítko.
Dalšími novinkami z nedávné doby jsou dvě aktualizace a to programů Datovka a iDatovka. V případě Datovky došlo kromě změny názvu (do nedávna DSGUI) také na několik novinek týkajících se například portable verze, kterou je možné používat třeba z USB klíčenky, či možnosti snadno importovat data ze zazálohované databáze zpráv. Nové verze se dočkala také populární iDatovka. Tento program umožňující přístup do datových schránek z telefonů iPhone a tabletů iPad obsahuje nově podporu pro autentizaci jednorázovým heslem.

Kde všude jste se mohli setkat s CZ.NIC

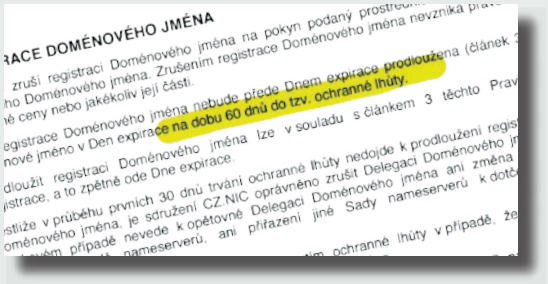
S logem CZ.NIC, mojeID nebo DNSSEC jste se mohli v druhé půlce loňského roku setkat nejen na řadě konferencí, ale i na stránkách internetových a tištěných médií. Co konkrétně jste tedy mohli vidět a kde?
Začneme úspěchem, který nás potkal při vyhlašování výsledků letošního ročníku soutěže Internet Effectiveness Awards. V té se do finále dostala naše kampaň Dvojníci upozorňující na význam a potřebu technologie DNSSEC při ochraně záznamů uložených v DNS. Z pražské Lucerny jsme si nakonec odnesli druhé místo za nejlepší mediální kampaň a ještě dvě další uznání - za nejlepší použití videa a nejlepší použití virálního marketingu a sociálních sítí.
CZ.NIC, respektive projekt mojeID, kterému byl nedávno jeden rok, se představily mimo jiné na loňském Webexpu, konferenci E-Business Fórum nebo inShop Festivalu. Setkat se s mojeID mohli také návštěvníci Czech Internet Fóra, které se uskutečnilo 10. listopadu, nebo Křišťálové lupy konající se o týden později.
Ani v médiích nepřestáváme být vidět. Za zmínku stojí mimo jiné seriál o programovacím jazyku Go, který vychází na AbcLinuxu.cz od ledna loňského roku a má už sedm dílů; další se připravují.
Pozadu nezůstává ani DNSSEC, o němž se čtenáři mohli setkat v každém loňském vydání Securityworldu. Poslední informace je věnována relativně nové záložce na našich stránkách. Ta má název Výstupy v médiích a evidujeme v ní všechny naše relevantní výstupy za poslední roky.

Společnosti Telefónica a Vodafone zavedly DNSSEC

Na konci listopadu a v polovině prosince oznámily zavedení DNSSEC dvě klíčové společnosti – Telefónica a Vodafone.
Tyto významné počiny umocňuje fakt, že společnost Telefónica patří k největším poskytovatelům připojení k internetu v této zemi, takže DNSSEC mohou v jejím případě využívat jak majitelé mobilních telefonů v síti O2, tak i klienti připojení prostřednictvím ADSL či pevných linek.
Aby byla ochrana DNSSEC plnohodnotná, je potřeba ji zavést nejen na straně držitelů domén, ale zároveň u poskytovatelů služeb a připojení k internetu. Zavedení technologie DNSSEC v sítích společností Telefónica a Vodafone tak pomůže zvýšit bezpečnost zákazníků těchto významných hráčů na trhu. Je na místě ocenit práci technických týmů, které velmi rychle DNSSEC ve svých sítích otestovaly a poté nasadily do běžného provozu.
Uživatelé internetových služeb obou firem se o zabezpečení DNSSEC mohou přesvědčit dvěma způsoby. Na stránkách www.dnssec.cz je k dispozici automatický test, který zobrazením zelené nebo červené ikony klíče uživatelům ukáže, zda jejich připojení je, resp. není bezpečné. Druhou možnost nabízí doplněk pro prohlížeč Firefox, který lze stáhnout zdarma ze stránek www.dnssec-validator.cz. Ten umožňuje kontrolovat, zda je či není aktuálně navštívená doména chráněná, a to opět zobrazením ikony klíče, tentokrát přímo v adresním řádku okna prohlížeče. ■

Přijaté změny chrání především držitele domén

Ke konci roku 2011 vyšly nové verze Pravidel registrace, Obchodních podmínek pro registrátory a Ceníku.
Největší změny se týkají plánovaného snížení velkoobchodní ceny domény .CZ a prodloužení ochranné lhůty před zrušením domény. Cílem většiny přijatých úprav je v první řadě zvýšení ochrany práv a bezpečnosti osobních údajů držitelů domén a současně další posílení zabezpečení databáze proti automatizovanému získávání dat.
Velice důležitou změnou je tedy prodloužení ochranné lhůty: zatímco dosud byla doména zrušena po 45 dnech od data, do kterého byla zaplacena (tedy do data expirace), v současnosti dochází k jejímu uvolnění až po dvou měsících. Smyslem je poskytnout držitelům, kteří mají o své domény zájem, více času a omezit tak případy, kdy o ně přijdou, neboť z nejrůznějších důvodů nestihnou prodloužení registrace zajistit. Další podstatná úprava dokumentů souvisí s pravidly činnosti registrátora: obchodní podmínky nyní ještě přesněji určují, jakým způsobem lze použít data z centrálního registru, čímž je dále zvyšován důraz na ochranu soukromí držitelů domén. Poslední, v současnosti již také účinná změna, se týká zpoplatnění nadlimitních dotazů registrátorů do registru domén .CZ. ■


RACE DOMÉNOVÉHO JMÉNA

zruší registraci Doménového jména na pokyn podaný prostřed
ho Doménového jména. Zrušením registrace Doménového jména nevzniká
né ceny nebo jakékoliv její části.
egistrace Doménového jména nebude před Dnem expirace prodloužena (článek
nové jméno v Den expirace na dobu 60 dnů do tzv. ochranné lhůty.
dloužit registraci Doménového jména lze v souladu s článkem 3 těchto Pra
istrace, a to zpětně ode Dne expirace.
stliže v průběhu prvních 30 dnů trvání ochranné lhůty nedojde k prodloužení regis
oménového jména, je sdružení CZ.NIC oprávněno zrušit Delegaci Doménového
méně případě nevede k opětovné Delegaci Doménového jména ani změna
nameserverů, ani přiřazení jiné Sady nameserverů k dotč
ochranné lhůty v případě, že

V Praze se konal mezinárodní workshop o internetové bezpečnosti

Pražský hotel Jalta hostil 3. a 4. října mezinárodní workshop o internetové bezpečnosti, který zorganizoval EUROPOL a sdružení ENISA ve spolupráci s bezpečnostním týmem CSIRT.CZ (Národní CSIRT České republiky). Workshopu se účastnili členové evropských národních a vládních CERT/CSIRT týmů a zástupci orgánů činných v trestním řízení z celé Evropy.
Tento workshop byl teprve šestý v pořadí a protože se v takových případech jedná o jednu z mála příležitostí k osobnímu setkání, byl pro pracovníky bezpečnostních týmů řešící kybernetickou bezpečnost velice důležitý. Jsme rádi, že si sdružení ENISA vybralo pro takovouto akci právě Prahu a my se mohli podílet na pořádání takovéhoto workshopu. Cílem setkání evropských bezpečnostních špiček byla především výměna zkušeností. Pro náš poměrně mladý bezpečnostní tým CSIRT.CZ je každá taková příležitost velice důležitá.
Slovem CSIRT je obecně označován bezpečnostní tým, které si vytváří jednotlivé organizace pro svoji potřebu. Takový tým potom odpovídá za řešení bezpečnostních incidentů v organizací definovaném poli působnosti, typicky v konkrétní síti, AS nebo například doméně. Týmy mají také svoji neformální hierarchii. V úrovni nad týmy jednotlivých organizací jsou potom CSIRT týmy národní a/nebo vládní, které nemají moc výkonnou (možnost odstranit problém přímým zásahem), ale jejichž role je koordinační a vzdělávací. V rámci České republiky plní roli národního CSIRT tým CSIRT.CZ. Více informací na www.csirt.cz. ■

Vybráno z .blogu

Větší bezpečnost obsahu domén v zóně .cz

autor: Pavel Bašta
bezpečnostní analytik
publikováno: 19. prosince 2011

Nedávno jsem zde psal o proaktivitě týmu CSIRT.CZ. Dnes bych vám chtěl ukázat, že ani náš interní tým CZ.NIC-CSIRT, jehož jsem také členem, v této oblasti nijak nezaostává. Ti, kteří byli na letošní konferenci IT 11, si možná pamatují na prezentaci, kterou měl kolega Michal Prokop, a která se točila kolem nové aplikace našich Laboratoří a proaktivního informování o bezpečnostních incidentech na doménách v zóně .cz. Jedná se o aplikaci, která z veřejně dostupných zdrojů získává informace o doménách v zóně .cz, na nichž je umístěn škodlivý obsah. Následně o incidentu prostřednictvím e-mailové zprávy informujeme držitele těchto domén a v případě potřeby se jim snažíme poradit, jak se s problémem vypořádat. Fáze testování a nastavování pravidel pro práci s touto aplikací a incidenty v ní obsaženými se pomalu blíží k závěru, a tak bychom vás rádi informovali o novinkách, které se kolem této aplikace chystají.

V první řadě bych rád uvedl, že v současné době se nám podařilo dostat se na úroveň, kdy již zpracováváme pouze aktuálně detekované příchozí incidenty. Databáze obsahovala po stažení velké množství domén, které byly v jednotlivých veřejných zdrojích evidovány již delší dobu a jejichž držitelé o tomto problému vůbec neměli tušení. Během předchozích měsíců se nám podařilo rozeslat informaci všem držitelům těchto přibližně 800 domén. Z toho již více jak 280 domén je vyčištěno.

Ve skutečnosti to byl ovšem pro útočníky mnohem větší zásah, na řadě domén bylo totiž nakaženo hned několik URL a některé evidované domény sloužily k poskytování freehostingu na doménách třetího řádu. Po upozornění většina provozovatelů freehostingových služeb okamžitě zneužité účty blokuje či maže. Na jedné takovéto freehostingové doméně bylo dokonce přes 1100 domén třetího řádu, které si útočníci buď sami registrovali nebo které se jim podařilo nějakým způsobem zneužít. I na dalších napadených doménách v zóně .cz byly počty útoků v řádu stovek domén třetího řádu, mnohdy opět obsahujících více než jednu URL. A to už je opravdu veliké množství zneškodněných útočných stránek.

V současné době nám každým dnem ve vyřešených případech přibývá mezi 5 až 10 doménami. To znamená, že postupně další a další držitelé domén reagují na naše upozornění. Většina zneužitých stránek obsahovala malware, útočné javascripty a menší část byla zneužívána pro phishing. Z e-mailové korespondence s těmi, kteří se na nás obrátili s žádostí o radu, vyplynulo, že na počátku značné části útoků stála kompromitace PC, ze kterého úpravy stránek prováděli. Tento malware pak získal uložená jména a hesla k FTP přístupům a odeslal je útočníkovi. V jednom extrémním případě uživatel opravil stránky, změnil heslo k FTP přístupu, ale protože nevěděl o malware na jeho PC, byl javascript na stránce do hodiny zpět.

Druhou zásadní novinkou je, že naše Laboratoře celý software upravují tak, aby bylo možné uvolnit jej jako open-source program pro využití dalšími doménovými registry. To vyžaduje přepsání rozhraní aplikace a umožnění jejího individuálního nastavení tak, aby si jej každý registr mohl nastavit dle svých potřeb. Aplikaci plánujeme uvolnit koncem tohoto, nebo začátkem příštího roku. Nasazení a aktivní využívání aplikace v dalších registrech by určitě znamenalo přínos pro bezpečnost dané zóny. Doufáme, že tato ukázka proaktivity druhého z CSIRT týmů provozovaného v CZ.NIC naznačuje jeden z možných přínosů zřizování týmů typu CSIRT i pro jiné organizace. Kromě proaktivity je samozřejmě nejdůležitějším prvkem práce CSIRT týmu reagování na vzniklé bezpečnostní incidenty.

O tom ale raději až v případném dalším článku. ■

Akademie CZ.NIC v novém roce

Akademie

První kurzy v tomto roce startují doslova za pár dnů. Právě teď je tedy ideální čas se na některý z nich přihlásit. Z čeho si můžete vybírat? Nabídka zahrnuje školení věnovaná IPv6, DNSSEC, IP telefonii, BGP nebo DNS. Kapacita jednotlivých školení je vyčerpána různě, proto si krátkou anonci vysloužila jen ta setkání, jejichž obsazenost zatím „netrhá rekordy".

Kurz na téma BGP seznámí posluchače s vlastnostmi a principy tohoto směrovacího protokolu, popíše jeho nejběžnější konfigurace, metody implementace směrovací politiky a možnosti zabezpečení BGP. V průběhu kurzu si také účastníci v praxi vyzkouší konfiguraci a troubleshooting BGP. Cílem kurzu je, aby účastník porozuměl vlastnostem a principům BGP a aby získal praktické zkušenosti v této oblasti.

Školitel, který povede kurz věnovaný DNSSEC, podrobně seznámí jeho účastníky s touto bezpečnostní technologií a s její návazností na systém DNS. Součástí kurzu budou i informace o použitelnosti dostupných nástrojů pro podepisování zónových souborů a návrh jednoduchého systému na podepisování včetně rotace DNSSEC klíčů.

Nejbližší kurzy v Akademii CZ.NIC

Implementace IPv6
2. února 2012, přednášející: Petr Černohouz
DNSSEC – zabezpečení DNS
16. února 2012, přednášející: Ľuboš Slovák
IP telefonie – protokol SIP
5. března 2012, přednášející: Petr Hruška
Směrovací protokol BGP
13. března 2012, přednášející: Petr Černohouz

Více informací o těchto a dalších kurzech, stejně jako přihlašovací formulář, jsou na internetové adrese www.nic.cz/akademie. ■