Čo sa stane s nahlásenými incidentami

Zuzana Duračinská • zuzana.duracinska@nic.cz •
06.08.2013

CZ.NIC | SPRÁVCE DOMÉNY CZ

CZ.NIC z.s.p.o.

- Záujmové združenie právnických osôb
- Prevádzkovanie registru doménových men .CZ
- Prevádzkovanie služby mojeID , Akadémie, Laborátorií
- Dôraz na osvetu a bezpečnosť
- Prevádzkovanie národného bezpečnostného týmu CSIRT.CZ

CSIRT.CZ

- Computer Security Incident Response Team
- Národný CSIRT tým Českej republiky
- Prevádzkovaný združením CZ.NIC od roku 2011
- Status akreditovaný u „TI“(Trusted Introducer)
- Interný bezpečnostný tým združenia CZ.NIC

CSIRT.CZ

- **INCIDENT RESPONSE**
- Osveta, školenia, prednášky
- Proaktívne služby
- Služby: Malicious Domain Manager, Skener webu
- Spolupráca na medzinárodnej a národnej úrovni
- *NEMÁ* výkonné právomoci

Incident response

- Pomoc a spolupráca pri riešení incidentov
- Incidenty týkajúce sa adresového rozsahu prideleného do ČR
- Hlásenie na:

abuse@csirt.cz

- Kontakty na stránkach csirt.cz

Kedy sa incident hlási týmu CSIRT.CZ?

- Bezpečnostný incident **pretrváva**
- Nikto na hlásený incident **nereaguje** (v rámci ČR / mimo ČR)
- Na hlásený incident bola prijatá **odmietavá odpoveď**
- Nedokážete detekovať **zdroj útoku** (sieť/IP adresu)
- Problém by mohol byť **plošný**
- CSIRT.CZ ako **last resort!**

Ako by hlásenie malo vyzerať?

- **Jednoduchý** a **zrozumiteľný** textový e-mail
- Správa by mala obsahovať **IP adresu (URL)** alebo **adresný blok**, ktorého sa to týka
- Typ incidentu (napr. spam, virus, DDOS, phishing, pharming...)
- Časť logu

  - časové známky a časová zóna

  - zdrojová a cieľová IP adresa

  - zdrojový a cieľový port

  - TCP-UDP-ICMP

http://csirt.cz/page/883/hlaseni-incidentu/

Hlášení bezpečnostního incidentu

Předtím, než vytvoříte a do *CSIRT.CZ* odešlete hlášení bezpečnostního incidentu, ověřte si prosím zde, jestli se obracíte na správné místo.

Bezpečnostní incidenty hlašte elektronickou poštou na adresu **abuse@csirt.cz**. Hlášení by mělo obsahovat kompletní popis problému.

Doporučený tvar pro hlášení bezpečnostního incidentu:

- Hlášení by měl být **jednoduchý textový e-mail**, v případě potřeby s přílohou (v příloze by měl být tzv. "důkazní materiál").
- Jedno hlášení by se mělo týkat **jedné ip adresy** nebo **jednoho adresového bloku**.
- **Předmět** zprávy by měl obsahovat **IP adresu** nebo **adresový blok** a **typ incidentu** (spam, virus, scanning, DDOS, hacking, phishing, pharming, porušení autorských práv...).
- **Hlášení o scanování** musí obsahovat část logu obsahující záznamy o útoku:

Čo sa stane s nahláseným incidentom?

- Vykonáme prvotnú analýzu
- Zistíme, či máme dostatok informácií
- Kontaktujeme zdroj problému (držiteľ IP adresy, domény, web hosting, databáza TI, známosti, znalosť infraštruktúry...)
- Skontrolujeme či sa problém medzičasom neodstránil (možné napr. u phishingu)
- Sprostredkujeme odpoveď

Čo sa stane s nahláseným incidentom?

- Každý incident vyžaduje individuálne posúdenie
- Incidenty sa môžu opakovať
- Informujeme aj ďalšie potencionálne obete
- Vytvoríme informačný odkaz na webe, prípadne kontaktujeme média
- V prípade potreby vytvoríme návod na obranu

To: csirt@csirt.cz

Attachment: prikaz0B448E2700528389.zip, 64.7 KBytes

VÝZVA K ÚHRADĚ DLUŽNÉHO PLNĚNÍ PŘED PROVEDENÍM EXEKUCE

Soudní exekutor Mgr. Bednář, Richard, Exekutorský úřad Praha-2, IČ 34506386, se sídlem Kateřinská 9, 194 00 Praha 2
pověřený provedením exekuce: č.j. 19 EXE 499/2014 -22, na základě ustanovení: Příkaz č.j. 036591/2014-685/Čen/G V.vyř.,
vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění označených povinností, které ukládá exekuční titul, stejně ták, jako i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, případně zálohu na náklady exekuce a odměnu soudního exekutora:

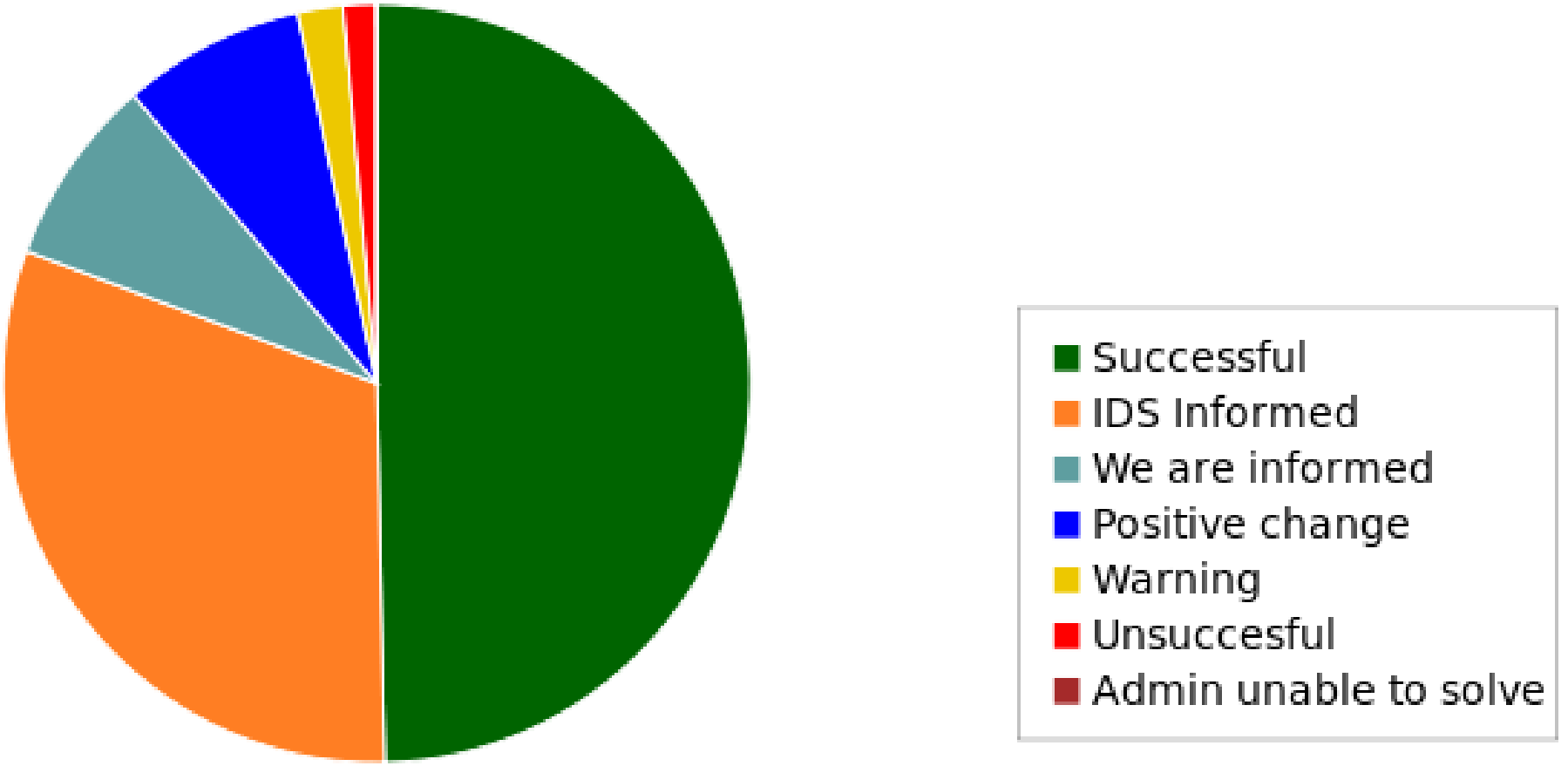
Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 13 427,00 Kč
Záloha na odměnu exekutora (peněžité plnění): 1 549,00 Kč včetně DPH 21%
Náklady exekuce paušálem: 3 833,00 Kč včetně DPH 21%

Pro splnění všech povinností je třeba uhradit na účet soudního exekutora (č.ú. 341719009/5000, variabilní symbol 69665801, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 18 809,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku vymožení povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

	2008	2009	2010	2011	2012	2013	2014	sum
IDS				491	3924	2121	1235	7771
Phishing	65	220	209	144	159	175	177	1149
Spam	47	28	103	26	43	73	99	419
Malware	53	97	42	9	19	44	68	332
Virus		121	178	1	1			301
Other	1	5	8	62	13	75	43	207
DOS	1	4	2	2	68	72	17	166
Trojan	66	6	26	5	5	12	31	151
Probe		3	14	25	12	26	47	127
Botnet		3	46	5	8	15		77
Portscan	10	4	1	6	1	3	14	39
Pharming							19	19
Crack	1		4					5
Copyright			1		1			2
sum	244	491	634	776	4254	2616	1750	10765


Successful
IDS Informed
We are informed
Positive change
Warning
Unsuccesful
Admin unable to solve

Proces Incident Handlingu

- Zaoberáme sa všetkými nahlásenými incidentami
- Workflow je pružné, prípady sú posudzované individuálne
- Zachovávame dôveryhodnosť informácií
- Všetky informácie a štatistiky sú anonymizované

Malicious Domain Manager

- Aplikácia vyvinutá v CZ.NICu
- Získavanie informácií z verejne dostupných zdrojov o napadnutých webových prezentáciach na doméne .CZ
- Držitelia domén sú informovaný so žiadosťou o riešenie

Malicious Domain Manager

MDM - Správce škodlivých domén

Stav databáze

Aktuální počet škodlivých domén	332
Aktuální počet škodlivých URL	2463
Celkem vyřešených domén	7542
Celkem vyřešených URL	102276
Poslední aktualizace	2014-08-05 05:52:10

Předmět: Škodlivý obsah v doméně priklad.cz

Přiložit soubor

Zpráva:

Dobrý den,
Vaše doména priklad.cz je vedena v seznamu domén hostujících škodlivý
obsah. Touto zprávou vás chceme požádat o nápravu situace.

Seznam napadených URL:
http://www.priklad.cz/images/stories/priklad/doc/settings/natwest/NatWest/default.aspx.htm

Podrobnosti k evidovaným adresám můžete zjistit například na diagnostické stránce databáze Google Safebrowsing:
http://www.google.com/safebrowsing/diagnostic?site=http%3A%2F
%2Fwww.hasicikrinec.cz%2Fimages%2Fstories%2Fhasicikrinec%2Fdoc%2Fsettings%2Fnatwest%2FNatWest%2Fdefault.aspx.htm

Pro diagnostiku tohoto incidentu můžete použít například služby urlQuery
http://www.urlquery.net/index.php nebo Sucuri SiteCheck
http://sitecheck.sucuri.net/scanner/

Pro odstranění Vaší domény z databáze Google Safe Browsing, Vám doporučujeme
postupovat podle informací zveřejněných společností Google zde:
http://www.google.com/support/webmasters/bin/answer.py?answer=163633

V případě, že se bezpečnostní problémy s Vaší webovou aplikaci opakují,
doporučujeme Vám využít naší BEZPLATNÉ služby Skener webu. Díky ní se dozvíte,
jaké zranitelnosti se na Vašem webu nacházejí a jak je eliminovat.
http://www.skenerwebu.cz

Skener webu

- Reakcia na výsledky z MDM
- **Bezplatná** služba zameraná primárne na neziskový a verejný sektor
- Penetračné **testovanie webových stránok** cez automatické nástroje a ručné testy

https://www.skenerwebu.cz/

podpora@skenerwebu.cz

Skener webu

- Výstup pre žiadateľa:

  Výsledná správa s nálezmi a doporučenými riešeniami

- Výstup pre nás:

  Anonymizované štatistiky a prehľad o najčastejších bezpečnostných nálezoch na českých weboch

CSIRT.CZ

- Aktuálne z bezpečnosti

  http://csirt.cz/news/security/

- Rady a návody

  http://csirt.cz/page/1971/rady-a-navody/

Akademie CZ.NIC

- kurzy internetových technologií v podání zkušených odborníků
- učebna v Praze a v Brně
- výuka na testovacím HW
- IPv6, protokol BGP, DNS a DNSSEC, IP telefonie, PKI, Bezpečnost webových aplikací, …

Edice CZ.NIC

- odborné knihy
- tištěné i elektronické
- *knihy.nic.cz*

Další informace najdete na:

- *akademie.nic.cz*
- *fb.com/AkademieCZNIC*
- *twitter.com/AkademieCZNIC*

Ďakujem za pozornosť

Zuzana Duračinská • zuzana.duracinska@nic.cz