SECURITY 2014

22. ročník konference o bezpečnosti v ICT

CSIRT.CZ - história, poslanie a poskytované služby

Zuzana Duračinská
CSIRT.CZ

CSIRT

Cyber Security Incident Response Team

- Fyzická bezpečnosť → Kybernetická bezpečnosť
- Viac možností pre tvorbu malwaru
- Narastajúci počet hrozieb = narastajúca obrana
- Bezpečnostné týmy na všetkých úrovniach – medzinarodná, národná, vládna, podniková ...

Úloha CSIRT týmov

- Spoločné ukazovatele:
  - 1. Prevencia incidentov
  - 2. Detekcia incidentov
  - 3. Riešenie incidentov

CSIRT.CZ

- Národný CSIRT tým Českej republiky
- Založený v rámci plnenia grantu „Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky“ (2007-2010)
- V rokoch 2008-2010 bol prevádzkovaný združením CESNET
- Od 01.01.2011 prebralo združenie CZ.NIC provoz národného CSIRT týmu
- Vznik na základe Memoranda s MV ČR, neskôr s NBÚ

Poslanie CSIRT.CZ

- Budovanie a rozvíjanie agendy národného CSIRT týmu ČR
- Riešenie kybernetických incidentov v sietiach prevádzkovaných v ČR (incident response)
- Poskytovanie koordinačnej pomoci pri riešení incidentov (nie pre koncových užívateľov)
- Spolupráca na medzinárodnej a národnej úrovni, výmena skúsenosti a informácií
- Predávanie hlásených incidentov osobám zodpovedným za chod siete/služby, ktorá je zdrojom incidentu

Poslanie CSIRT.CZ

- Zhromažďovanie a vyhodnocovanie dát o ohlásených incidentoch
- Plnenie úlohy národného „Point Of Contact“ pre oblasť IT
- Centrum vzdelávania a šírenia osvety v oblasti kybernetickej bezpečnosti
- Pomoc pri zriaďovaní iných CSIRT tímov v ČR
- NEMÁ VÝKONNÉ PRÁVOMOCI (nedokáže nič vypnúť)

Incident Response

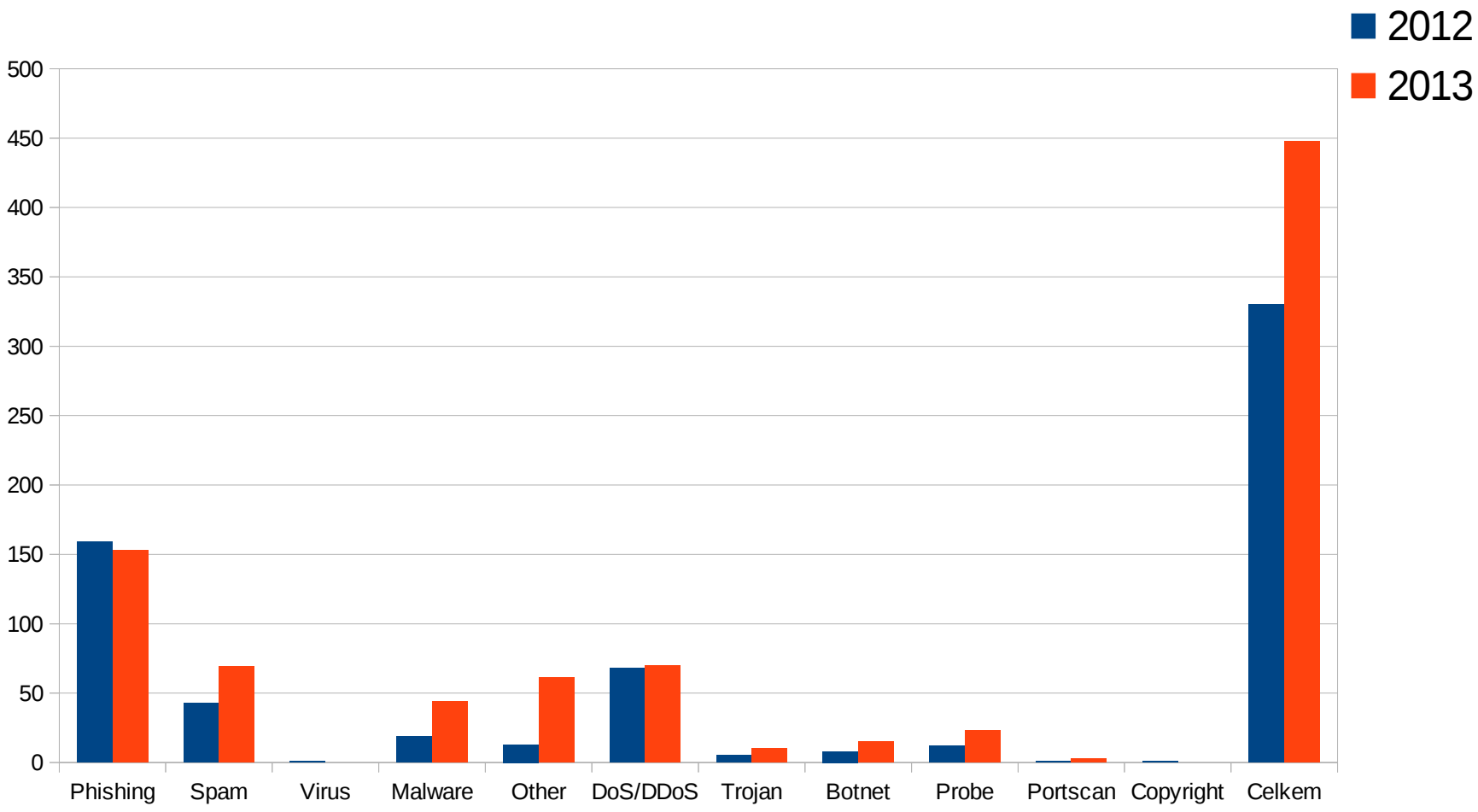
Kedy je bezpečnostný incident hlásený tímu CSIRT.CZ?

- Nie je jasné, kto je za incident zodpovedný
- Nulová reakcia zo strany adresáta sťažnosti
- Nie je snaha incident riešiť
- Jedná sa o závažný incident
- Objaví sa podozrenie, že by určitá množina sietí/zariadení mohla byť cieľom útoku
- Adresa pre hlásenie incidentov: ABUSE@CSIRT.CZ

Štatistiky

	2008	2009	2010	2011	2012	2013	2014	sum
IDS				491	3924	2121	95	6631
Phishing	65	220	209	144	159	175	14	986
Spam	47	28	103	26	43	73	8	328
Virus		121	178	1	1			301
Malware	53	97	42	9	19	44	6	270
Other	1	5	8	62	13	75	9	173
DOS	1	4	2	2	68	72	1	150
Trojan	66	6	26	5	5	12	4	124
Probe		3	14	25	12	26	10	90
Botnet		3	46	5	8	15		77
Portscan	10	4	1	6	1	3		25
Crack	1		4					5
Copyright			1		1			2
sum	244	491	634	776	4254	2616	147	9162

Celkový nárast incidentov



Malicious Domain Manager

- *Open Source* aplikácia vytvorená v Labs CZ.NIC
- Aplikácia získava informácie z verejne dostupných zdrojov o napadnutých webových aplikáciach
- Držitelia domén, ktorých webové aplikácie boli napadnuté sú kontaktovaný so žiadosťou o nápravu

Malicious Domain Manager

Předmět: Škodlivý obsah v doméně priklad.cz

Přiložit soubor

Zpráva:

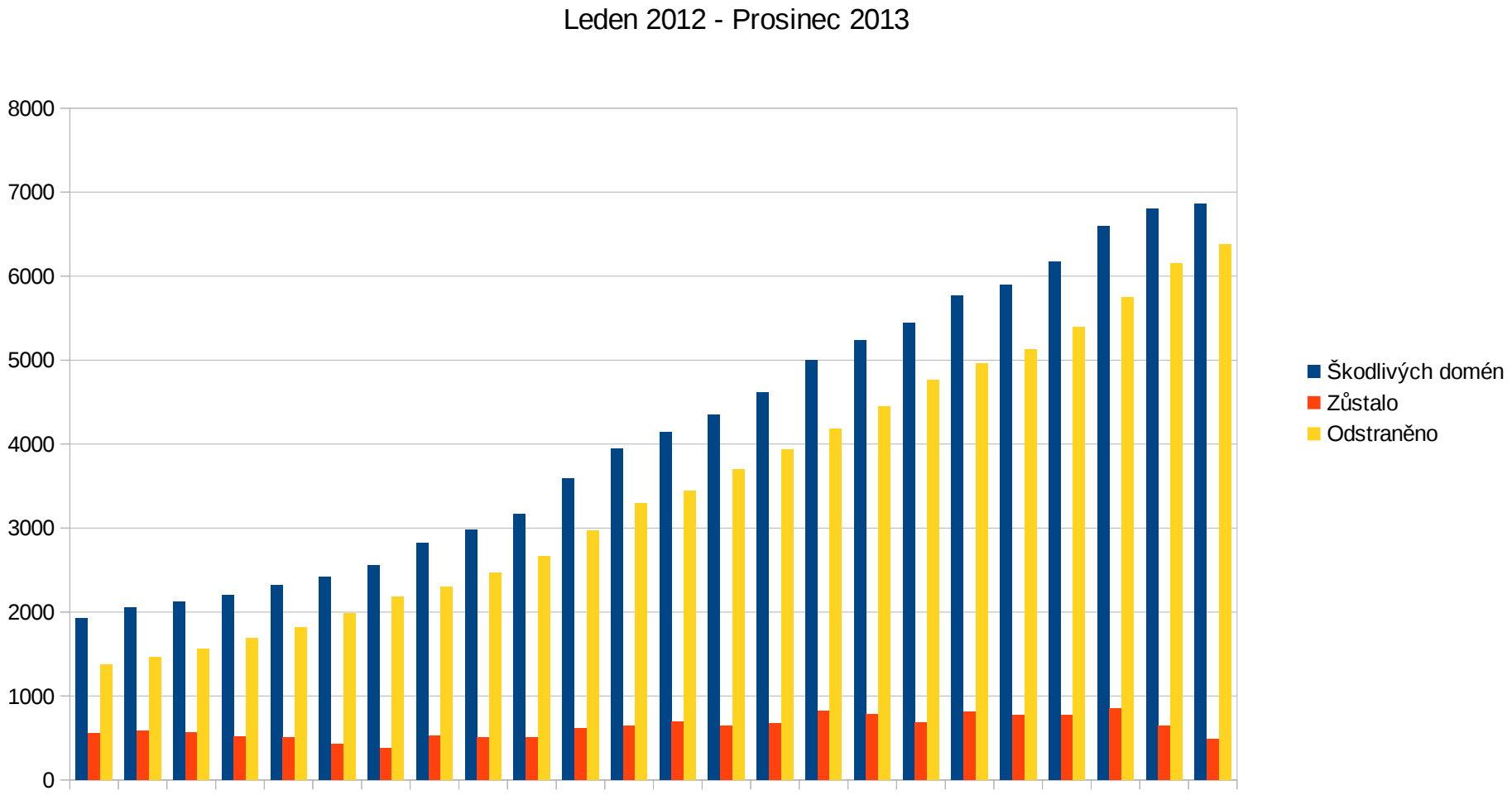
```
Dobrý den,
Vaše doména priklad.cz je vedena v seznamu domén hostujících škodlivý
obsah. Touto zprávou vás chceme požádat o nápravu situace.

Doména je evidována v databázi Phishtank:
http://www.forwifi.cz/libraries/phpinputfilter/fedadministrator/index.htm

Podrobnosti o napadené doméně forwifi.cz:
Adresa:
http://www.priklad.cz/libraries/phpinputfilter/fedadministrator/index.htm
        Více informací:
http://www.phishtank.com/phish_detail.php?phish_id=2115100
        Ověřeno komunitou PhishTank: ano
        Nahlášeno v databázi PhishTank od: 2014-01-28

S pozdravem
Zuzana Duračinská
CZ.NIC-CSIRT
http://www.nic.cz/csirt/
```

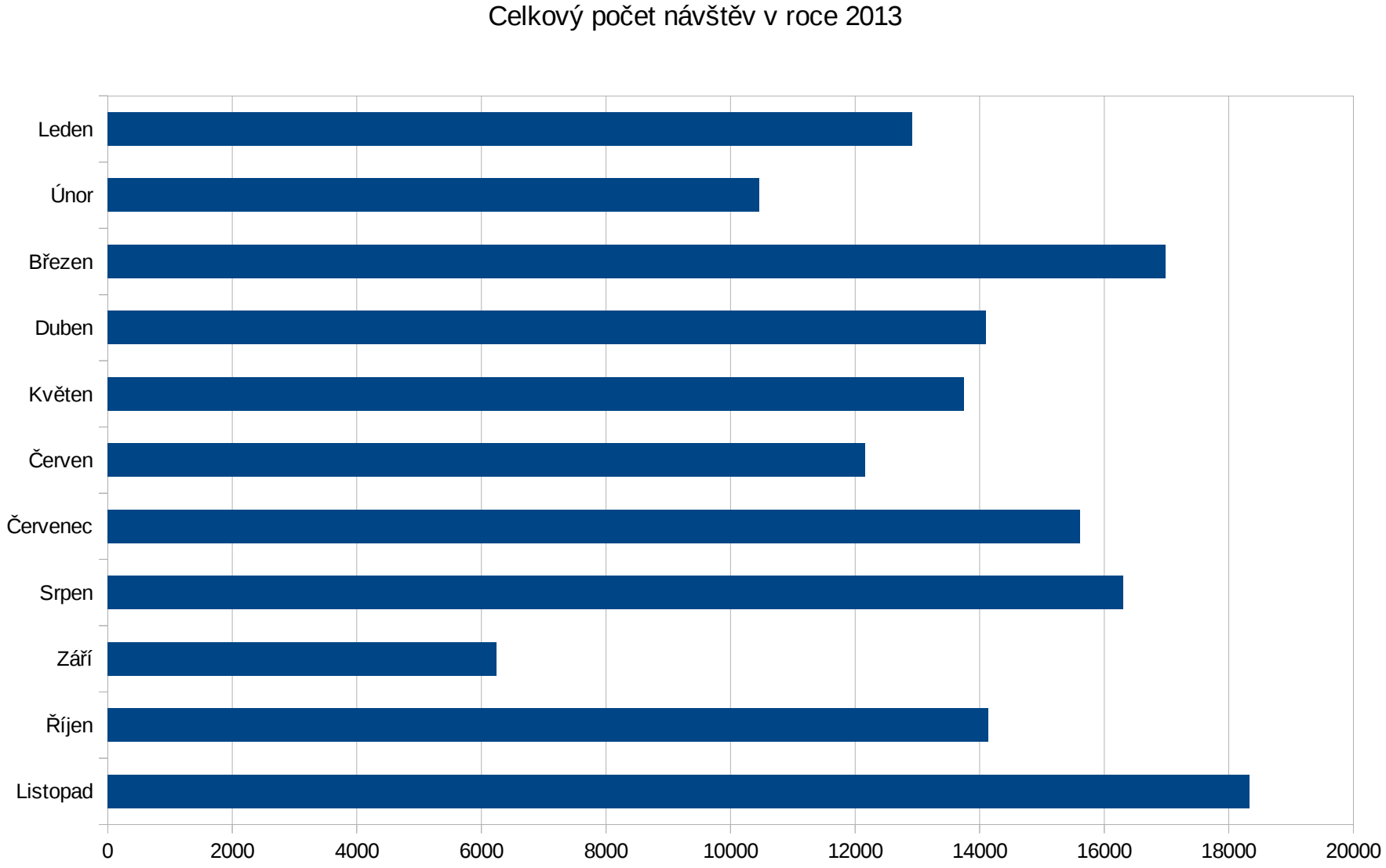
Štatistiky


Leden 2012 - Prosinec 2013
8000
7000
6000
5000
4000
3000
2000
1000
0
Škodlivých domén
Zůstalo
Odstraněno

Aktuálně z bezpečnosti

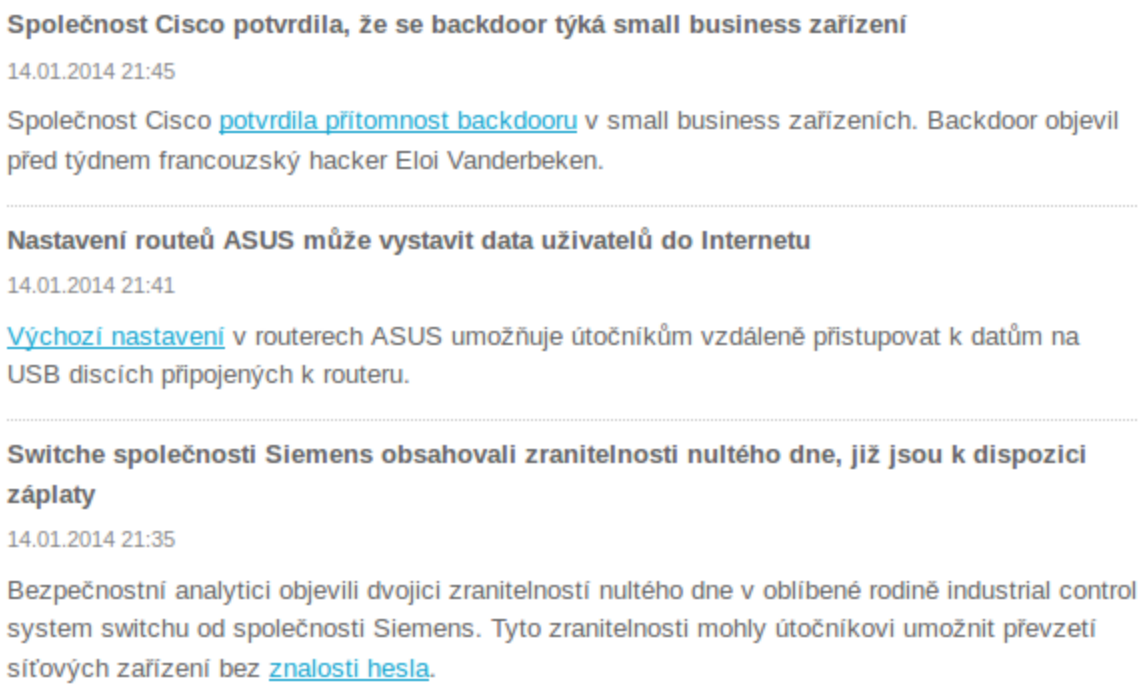
- Pravidelné zverejňovanie noviniek z oblasti bezpečnosti
- Zameriavanie sa na zraniteľnosti, ktoré môžu ohroziť českých užívateľov
- Priestor pre zverejňovanie aktuálnych hrozieb (napr. phishing Českej pošty apod.)
- Postupne sa zvyšujúci počet noviniek
- Priemerne 25 noviniek/mesiac
- Postupne sa zvýšujúca návštevnosť

Počet návštev v rubrike „Aktuálně z bezpečnosti“



Aktuálně z bezpečnosti

- https://www.csirt.cz/news/security/
  - Dostupné v českom a anglickom jazyku



Společnost Cisco potvrdila, že se backdoor týká small business zařízení

14.01.2014 21:45

Společnost Cisco potvrdila přítomnost backdooru v small business zařízeních. Backdoor objevil před týdnem francouzský hacker Eloi Vanderbeken.

Nastavení routeů ASUS může vystavit data uživatelů do Internetu

14.01.2014 21:41

Výchozí nastavení v routerech ASUS umožňuje útočníkům vzdáleně přistupovat k datům na USB discích připojených k routeru.

Switche společnosti Siemens obsahovali zranitelnosti nultého dne, již jsou k dispozici záplaty

14.01.2014 21:35

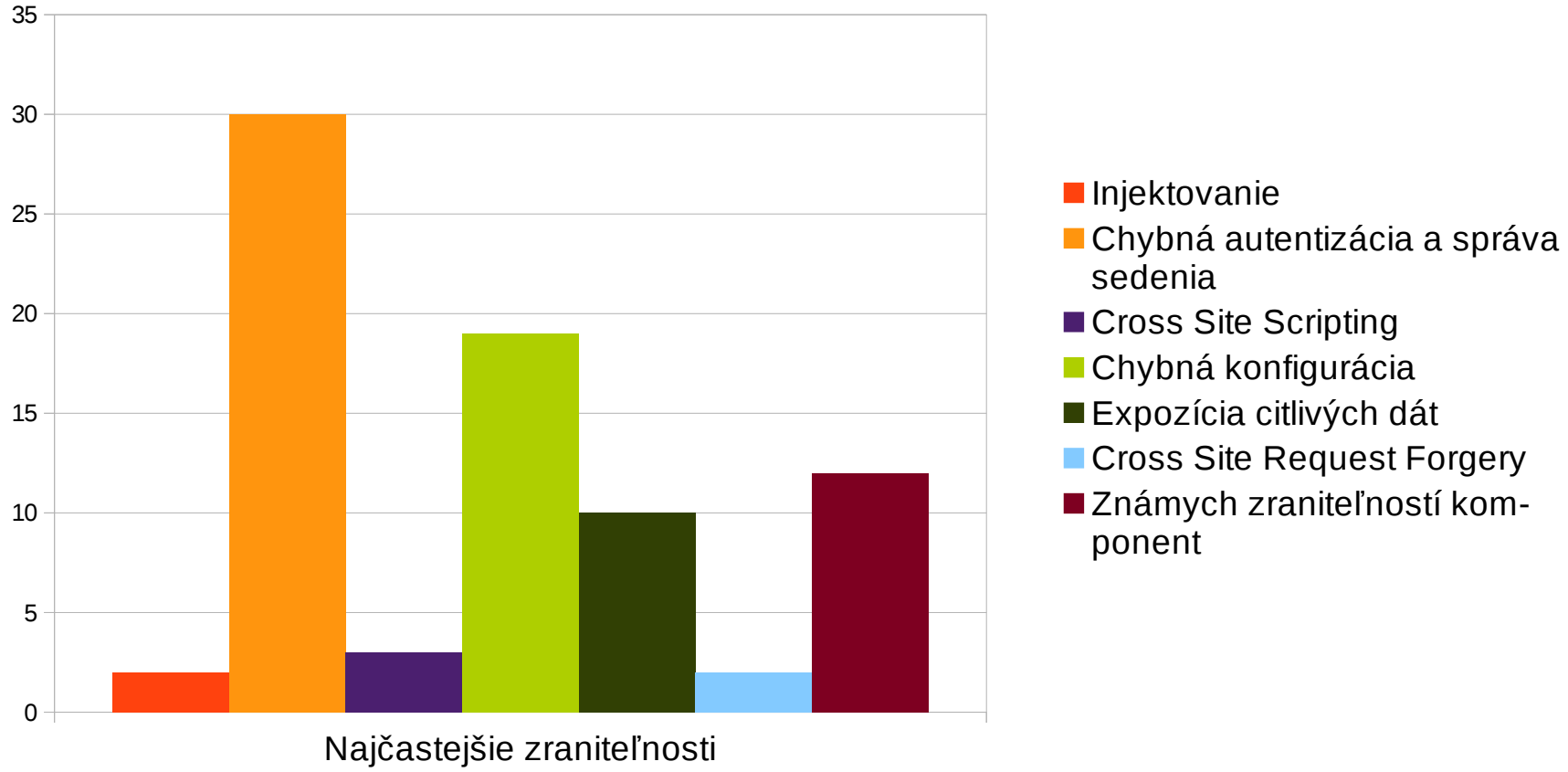
Bezpečnostní analytici objevili dvojici zranitelností nultého dne v oblíbené rodině industrial control system switchu od společnosti Siemens. Tyto zranitelnosti mohly útočníkovi umožnit převzetí síťových zařízení bez znalosti hesla.

Skener webu

- Doplnková služba CSIRT.CZ
- Cieľ: zvýšenie bezpečnosti na strane webových aplikácií
- Penetračné testovanie webových aplikácií
- Služba zameraná primárne na verejný a neziskový sektor
- Služba je poskytovaná ZDARMA
- Odmena pre CSIRT.CZ: užitočné štatistiky:)

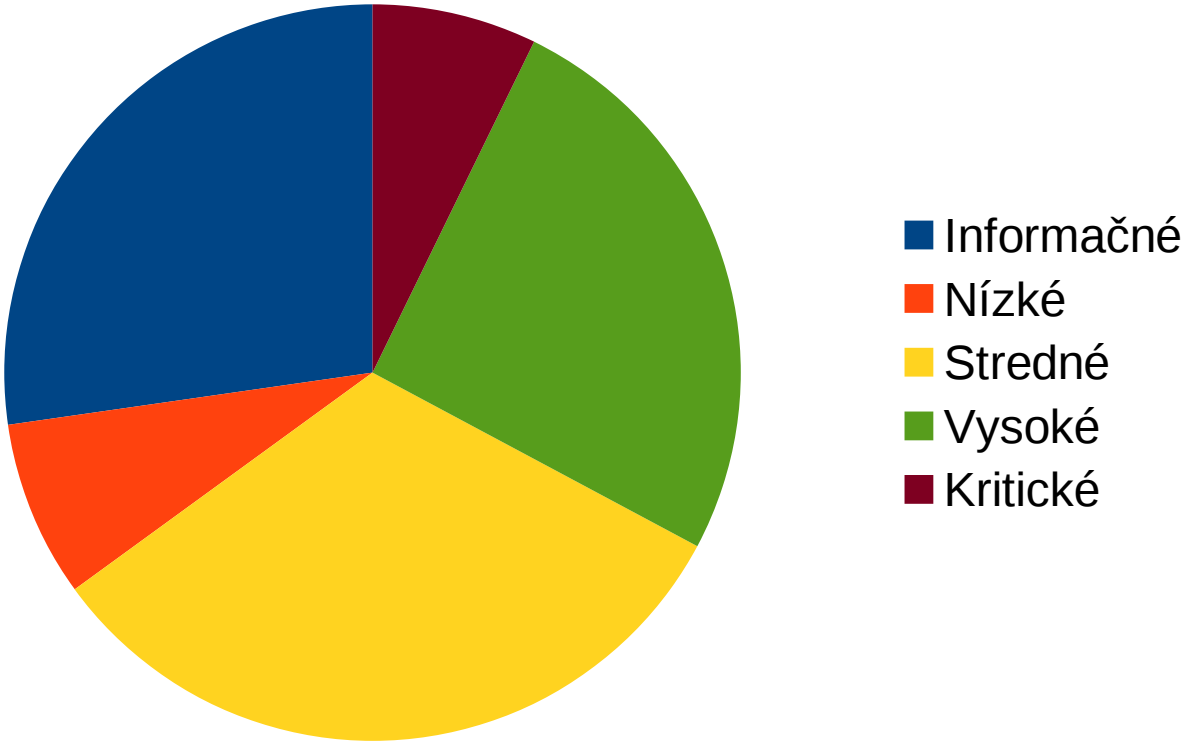
Skener webu

- Počet otestovaných aplikácií: **51**



Skener webu

- Počet nájdených zraniteľností: **774**



Kybernetické cvičenia

- Účasť a príprava celoeurópskych kybernetických cvičení
- Budovanie medzinárodnej spolupráce
- Cvičenie krízových scenárov
- Cvičenie komunikácie spolu s inými bezpečnostnými týmami

Vzdelávacie aktivity

- Usporiadávanie vzdelávacích akcií a kurzov
- Vedenie workshopov
- Vydanie knihy „Buď pánem svého prostoru“
- Účasť formou prednášiek na vzdelávacích akciách
- Spolupráca na tvorbe seriálu “Jak na Internet“

Plánované činnosti

- Ďalší rozvoj už existujúcich služieb
- Väčší dôraz na vzdelávacie aktivity
- Zracionalizovanie analýzy príchodzích dát zo širších zdrojov, ktorý umožní globálny pohľad na incidenty – pomoc pri odhaľovaní „problematických IP adries“, nových typoch útokov, nových botnetoch

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Ďakujem za pozornosť.

Mgr. Zuzana Duračinská
CZ.NIC
zuzana.duracinska@nic.cz