Skener webu pre mestá a obce

Zuzana Duračinská • zuzana.duracinska@nic.cz •
07.04.2014

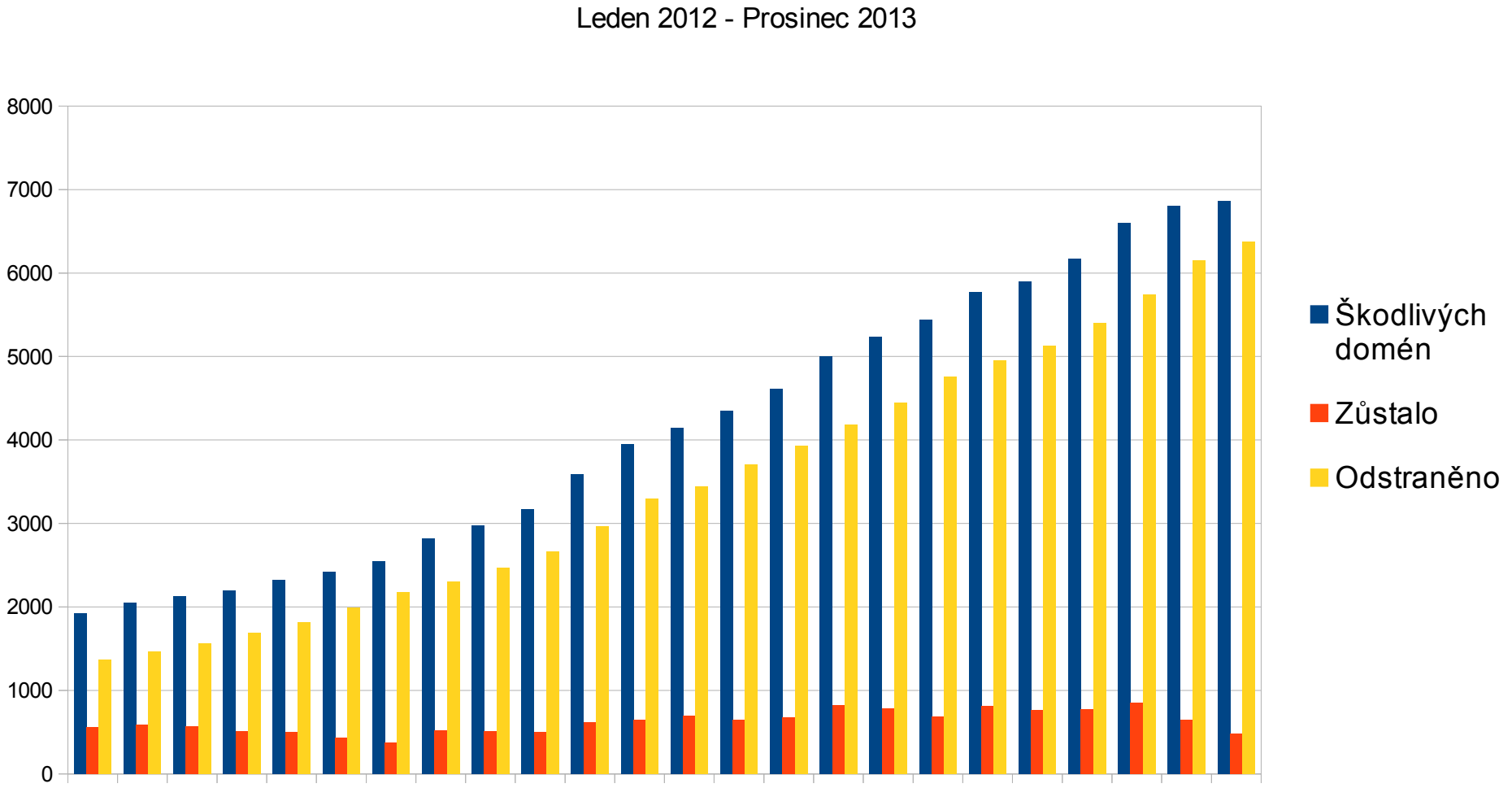
Národný CSIRT tým

- Cyber Security Incident Response Team
- CSIRT týmy na úrovni národnej, vládnej, medzinárodnej, podnikovej
- Prevadzkovaný združením CZ.NIC z.s.p.o.
- Vznik na základe memoranda s Národným bezpečnostným úradom
- Plnenie úlohy „Point of contact“ pre oblasť IT

Aktivity na poli bezpečnosti

- Incident handling
- Vzdelávacie aktivity
- Osveta v oblasti kybernetickej bezpečnosti
- Doplnkové služby napr. „Aktuálně z bezpečnosti“
- Malicious Domain Manager

Malicious Domain Manager



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/
```

Možné dôsledky napadnutia webu

- Zmena (osobných) údajov
- Únik citlivých informácií
- Zneprístupnenie služby
- Nahratie škodlivého kódu na stránky
- ...

Skener webu

- **Bezplatná** služba združenia CZ.NIC a tímu CSIRT.CZ
- Primárne určená pre verejný a neziskový sektor
- Cieľom je nielen identifikovať zraniteľnosti, ale aj nedostatky v oblasti zabezpečenia webu

Skener webu

SKENER WEBU

Chybějící příznak X-FRAME-OPTION

Riziko: informační

V HTTP hlavičkách chybí příznak X-FRAME-OPTION. Tento příznak indikuje, jestli prohlížeč povolí vložení stránky jako <frame> nebo <iframe>. Příznak slouží jako ochrana proti clickjackingu.

Doporučené řešeni: Doporučujeme tento příznak dle potřeby s jednou z možných možností (DENY, SAMEORIGIN, ALLOW-FROM url) vložit do HTTP hlaviček.

Skener webu

- Testovanie podľa OWASP Top 10
- Automatické scany
- Ručné testovanie
- *Výstup pre objednávateľa*: správa s nálezmi a odporúčeniami
- *Výstup pre NIC.CZ:* štatistické údaje a prehľad o zabezpečení webov

Ďakujem za pozornosť

Zuzana Duračinská • zuzana.duracinska@nic.cz