Ministerstvo financií
Slovenskej republiky

EFQM

Návrh zákona o informačnej bezpečnosti
a
Aktuálne výzvy pri riešení bezpečnostných incidentov v digitálnom priestore SR

Kongres ITAPA - október 2013
Bratislava

Jan Hochmann, Ministerstvo financií SR
Petra Hochmannová, CSIRT.SK / DataCentrum

Obsah

1. Návrh zákona o IB
   - Východiská
   - Štruktúra obsahu
2. Aktuálne výzvy pri riešení bezpečnostných incidentov v digitálnom priestore SR
   - CSIRT.SK
   - Riešené bezpečnostné incidenty
   - Aktuálne problémy a možné riešenie

1. Návrh zákona o IB - *východiská I.*

- **Národná stratégia pre informačnú bezpečnosť v SR**

  (uznes. vlády SR č. 570/2008)

- **Akčný plán na roky 2008 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR**

  (uznes. vlády SR č. 46/2010)

  – Budovanie povedomia a kompetentnosti v oblasti IB („Návrh systému vzdelávania v oblasti IB v SR“) *(uznes. vlády SR č. 391/2009)*

  – Zriadenie CSIRT.SK (MF SR / DataCentrum)

  (uznes. vlády SR č. 479/2008)

- **Legislatívny zámer zákona o IB** *(uznes. vlády SR č. 136/2010)*

Zdroj: www.vláda.sk, www.informatizácia.sk, www.csirt.gov.sk

1. Návrh zákona o IB - *východiská II.*

- **Návrh smernice EURÓPSKEHO PARLAMENTU a RADY o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii (2013)**
  - Zavedenie minimálnej úrovne bezpečnosti sietí a informácií v členských štátoch, a tým zvýšenie celkovej úrovne pripravenosti a reakcie na incidenty
  - Zlepšenie spolupráce v oblasti bezpečnosti sietí a informácií na úrovni EÚ v záujme efektívneho boja proti cezhraničným počítačovým incidentom a hrozbám.
  - Vytvorenie kultúry riadenia rizika a zlepšenie výmeny informácií medzi súkromným a verejným sektorom.
- **Ďalšie dokumenty**
  - Stratégia pre kybernetickú bezpečnosť EÚ,
  - smernice a nariadenia EÚ/EK
  - Zákon č. 305/2013 Z.z. o e-Governmente

1. Návrh zákona o IB - štruktúra obsahu 1

- **Legislatívny zámer zákona o IB + niečo navyše (aktualizácia)**
  - Terminológia, kompetencie, štandardy, proces riadenia, kategorizácia/ klasifikácia IS, legislatívne postavenie CSIRT.SK, minimálne znalostné štandardy, minimálne bezpečnostné požiadavky pre el. verejnú správu - eGovernment, minimálne požiadavky pre bezpečnosť internetu,
- **Stratégia kybernetickej bezpečnosti EÚ a návrh smernice EP a Rady**
  - určenie príslušného orgánu zodpovedného za informačnú a sieťovú bezpečnosť, kontaktný bod,
  - vytvorenie funkčného/ných tímov reakcie na počítačové/sieťové incidenty typu CERT/CSIRT, (legislatívne)
  - prijať vnútroštátnu stratégiu a plán spolupráce v oblasti sieťovej a informačnej bezpečnosti, (zjednotenie dokumentov pre IB, ...)

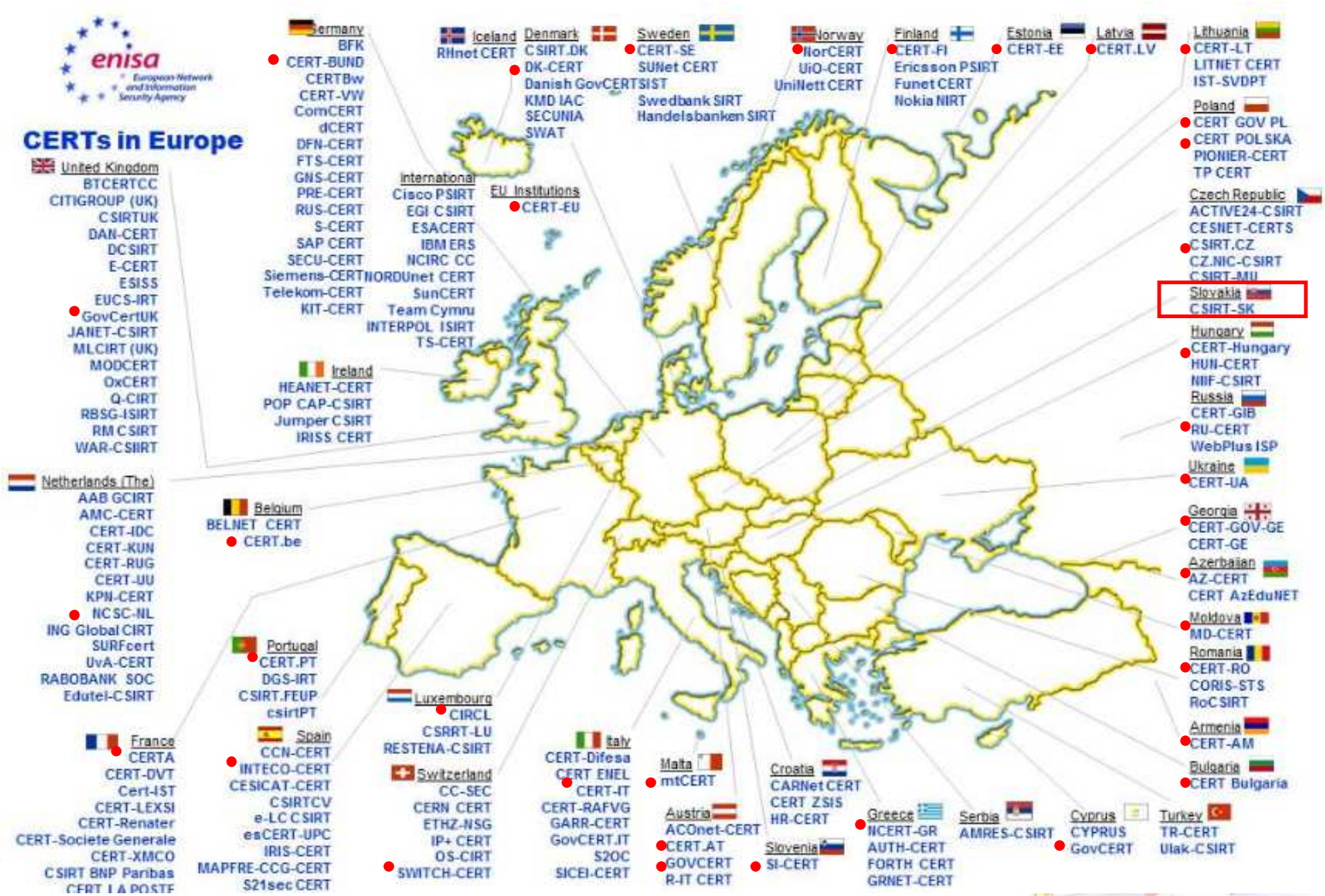
1. Návrh zákona o IB - *štruktúra obsahu 2*

- spolupráca v rámci siete, ktorá umožňuje bezpečnú a účinnú koordináciu vrátane koordinovanej výmeny informácií, ako aj zisťovania a reakcie na úrovni EÚ. Prostredníctvom tejto siete by si členské štáty mali vymieňať informácie a spolupracovať, aby na základe európskeho plánu spolupráce v oblasti bezpečnosti sietí a informácií odvrátili hrozby a incidenty v tejto oblasti,
- zabezpečiť riadenie rizík a výmenu informácií medzi súkromným a verejným sektorom, (pozn.: správa prvkov KII)
- od správcov/gestorov konkrétnych kritických odvetví a inštitúcií verejnej správy vyžadovať, aby posúdili riziká, ktorým čelia, a aby prijali vhodné a primerané opatrenia na zabezpečenie bezpečnosti sietí a informácií.
- povinnosť oznamovať príslušným orgánom všetky incidenty, ktoré vážne ohrozujú ich siete a informačné systémy a majú značný vplyv na kontinuitu kritických služieb a dodávku tovarov.

Ministerstvo financií
Slovenskej republiky

EFQM

2. Aktuálne výzvy pri riešení bezpečnostných incidentov v digitálnom priestore SR

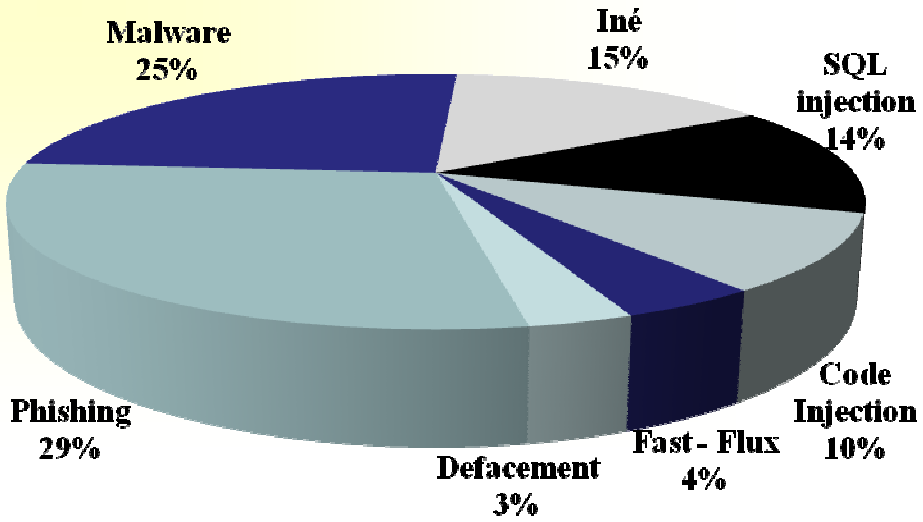


- **Spolupracujúce národné/vládne CSIRT/CERT tímy**

2. Riešené incidenty 2013 - manuálne

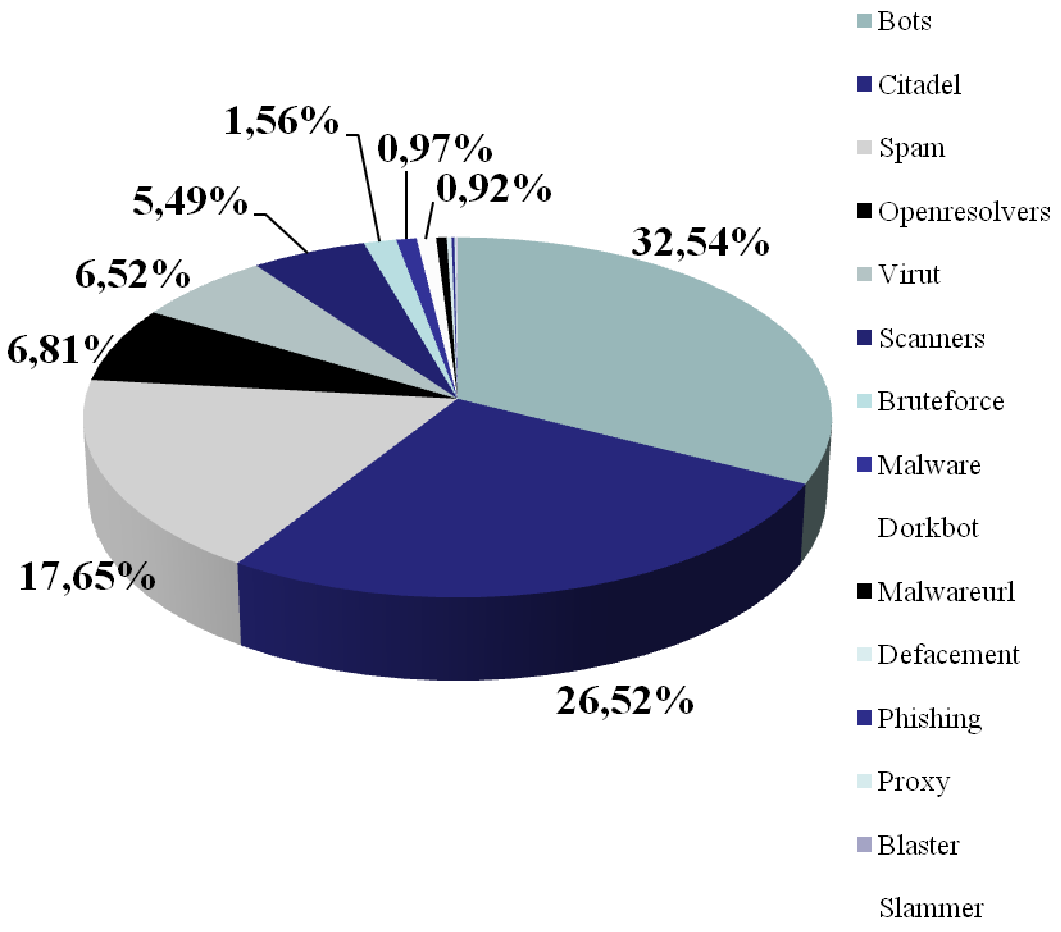
- Zdroje hlásení o bezpečnostných incidentoch:
  - dotknuté inštitúcie doma a v zahraničí,
  - CSIRT/CERT tímy,
  - automatizované systémy na detekciu incidentov (detekcia botnetov, „defacementov“, phishingových stránok, malware url,...).

Typ incidentu	Počet
Phishing	27
Malware	23
Iné	14
SQL injection	13
Code Injection	9
Fast - Flux	4
Defacement	3
Celkom	**93**

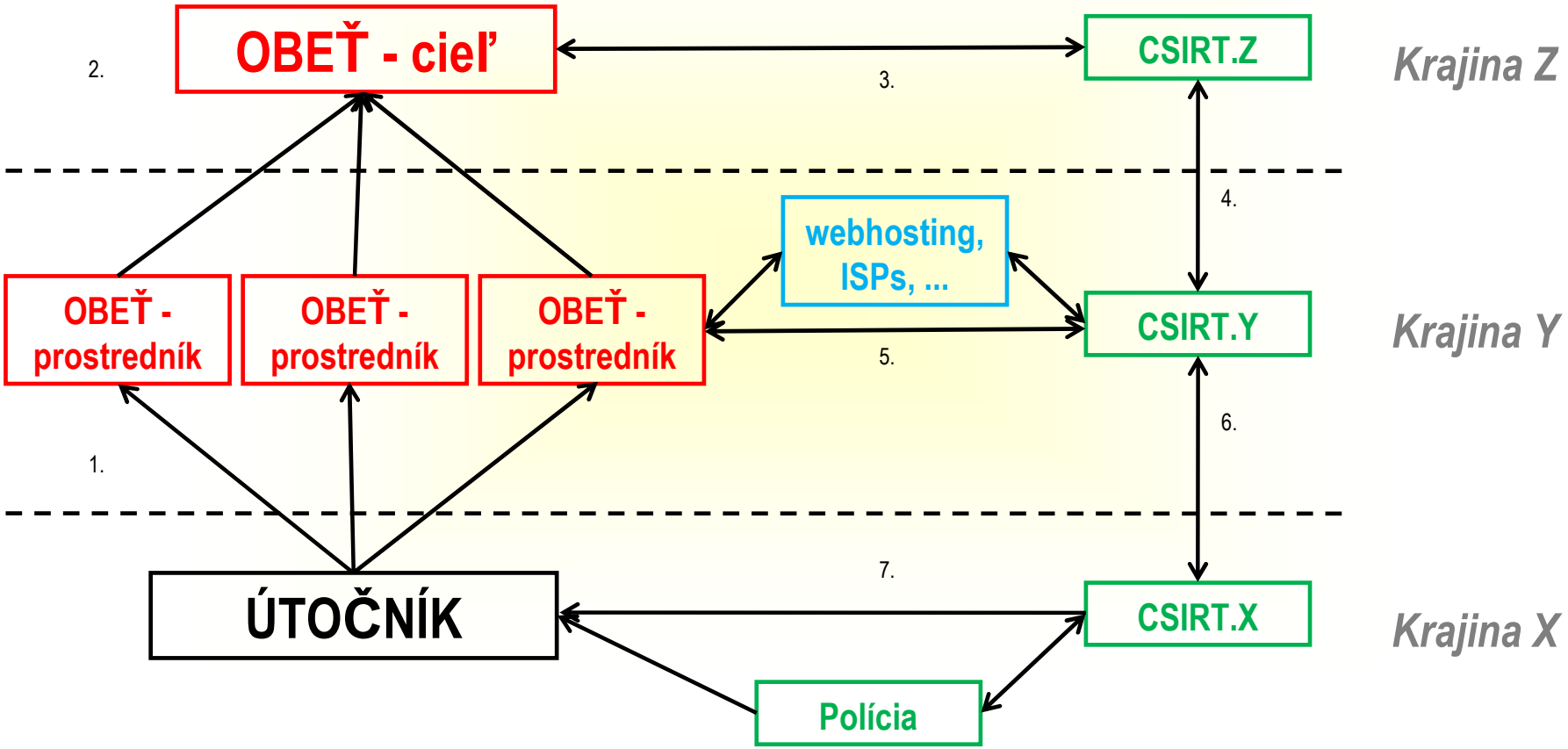


2. Riešené incidenty 2013 - automatizovane

Typ incidentu	Počet
Bots	61,327
Citadel	49,980
Spam	33,255
Openresolvers	12,832
Virut	12,297
Scanners	10,356
Bruteforce	2,938
Malware	1,822
Dorkbot	1,737
Malwareurl	953
Defacement	435
Phishing	248
Proxy	150
Blaster	80
Slammer	55
Celkom	**188,465**



2. Príklad komunikačnej schémy



Ministerstvo financií
Slovenskej republiky

EFQM

Ďakujeme za pozornosť

Jan Hochmann
Petra Hochmannová