Zabezpečenie prostredia a eliminácia následkov spôsobených cieleným útokom

Ing. Petra Hochmannová

CSIRT.SK – DataCentrum, MF SR

26.10.2011

Obsah

- **CSIRT.SK**
- **Koncept cvičení na ochranu KII**
- **Národné cvičenie - SISE 2011**
- **Medzinárodné cvičenia:**
  - **Cyber Europe**
  - **Cyber Atlantic**

CSIRT.SK

Východiska:

- Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, uznesenie vlády SR č. **570/2008** z 27. augusta 2008, MF SR,
- Návrh organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov (CSIRT.SK) v SR, uznesenie č. **479/2009** z 1.júla 2009, MF SR,
- zahraničné materiály.

CSIRT.SK :

- zriadený MF SR ako špecializovaný útvar DataCentra,
- personálne obsadzovanie (od 1. február 2010),
- súčasný stav – IV. etapa vytvárania (finálna etapa - 2012).

Hlavné úlohy:

- riešenie informačno-bezpečnostných incidentov v SR,
- kooperácia so sesterskými organizáciami a reprezentácia SR v oblasti IB na medzinárodnej úrovni,
- kontaktné miesto pre zahraničných partnerov,
- budovanie povedomia v oblasti IB.

Koncept cvičení na ochranu KII

- Cvičenie je nástrojom, ktorý umožní zúčastneným inštitúciám najmä:
  - preverenie pripravenosti,
  - preveriť reakciu na bezpečnostné incidenty,
  - získať skúsenosti v oblasti efektívneho zmierňovania/odstránenia následkov bezpečnostného incidentu,
  - tréning zamestnancov,
  - odhaliť konkrétne zraniteľnosti a slabé miesta v interných postupoch a procesoch,
  - identifikovať vzájomné prepojenia a vzťahy,
  - upevniť medzirezortnú spoluprácu.

Východiská I. – medzinárodné cvičenia

- Smernica Rady č. **2008/114/ES** z 8.12.2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu;

- Uznesenie Rady z 18. decembra 2009 o prístupe Európy k bezpečnosti sietí a informácií založenom na spolupráci **(2009/C 321/01)**, vyzývajúce k tomu, aby sa v Európe v oblasti bezpečnosti sietí a informácií uskutočňovali pravidelné cvičenia, z ktorých by prevádzkovatelia sietí a poskytovatelia služieb, ako aj verejné správy získavali cenné skúsenosti;

- Akčný plán Európskej komisie „Ochrana Európy pred rozsiahlymi kybernetickými útokmi a narušeniami: zvyšovanie pripravenosti, bezpečnosti a odolnosti“ **(KOM (2009) 149)**, v ktorom Európska komisia vyzýva členské štáty k organizovaniu pravidelných cvičení pre zvyšovanie bezpečnosti a odolnosti KII;

- Oznámenie Európskej komisie o „ochrane kritickej informačnej infraštruktúry: úspechy a ďalšie kroky k globálnej kybernetickej bezpečnosti“ **(KOM (2011)169)** z dňa 31.3.2011 vyzývajúce k organizovaniu pravidelných cvičení.

Východiská II. – národné cvičenia

- Národná stratégia pre informačnú bezpečnosť v SR schválená uznesením vlády SR č. **570/2008** z dňa 27.8.2008 definujúca aktuálne priority v oblasti informačnej bezpečnosti v SR;

- Návrh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike schválený uznesením vlády SR č. **46/2010** z dňa 19.1.2010 (podkapitola 3.3.3 Zmierňovanie a obnova);

- Uznesenie vlády č. **479/2009** z dňa 1.7.2009 k návrhu organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov (CSIRT.SK) v SR definujúce úlohy špecializovaného útvaru CSIRT.SK;

- Zákon č. **45/2011** Z.z. z dňa 8.2.2011 o kritickej infraštruktúre definujúci sektory kritickej informačnej infraštruktúry a ústredné orgány zodpovedné za ich ochranu.

Národné cvičenie - SISE 2011

Slovak Information Security Exercise 2011:

- prvé národné cvičenie zamerané na ochranu kritickej informačnej infraštruktúry v SR,
- medzirezortné s medzinárodným aspektom,
- predstavuje kombináciou operačného a komunikačného cvičenia (table-top),
- vo finálnej fáze prípravy,
- plánované na november 2011.

Životný cyklus cvičenia:

SISE 2011 - ciele

Scenár:

- simulovaný rozsiahly kybernetický útok na vybrané informačné systémy štátnej správy.

Roly:

- organizátor – CSIRT.SK, MF SR
- plánovač – CSIRT.SK
- účastníci – orgány štátnej správy, zahraničné útvary typu CSIRT/CERT
- pozorovatelia

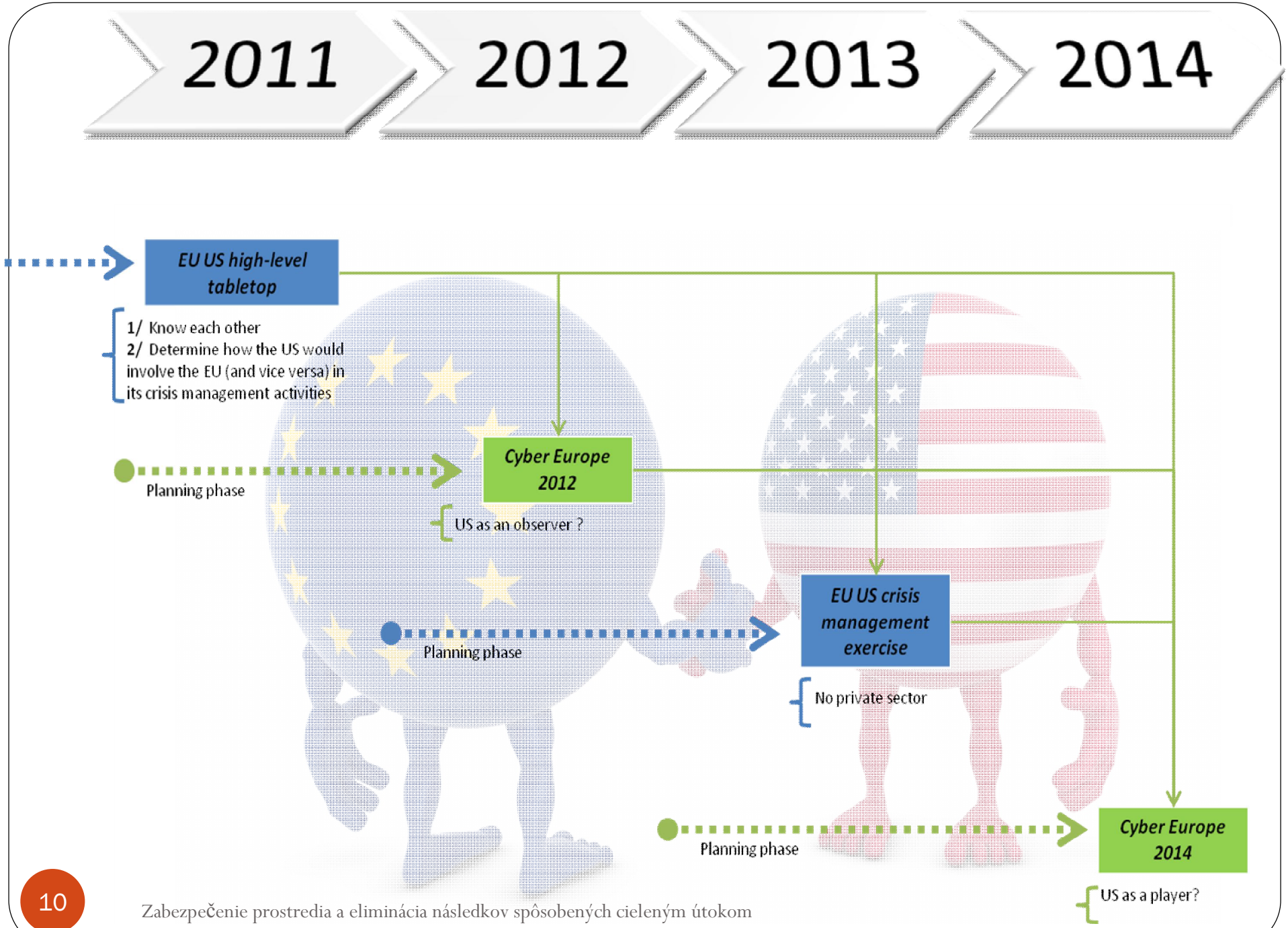
Primárny cieľ:

- preverenie reakcie zúčastnených inštitúcií na rozsiahle IKT incidenty.

SISE 2011 - ciele

Sekundárne ciele:

- preverenie efektívnosti medzirezortnej komunikácie a výmeny informácií;
- oboznámenie sa s rôznymi prístupmi jednotlivých inštitúcií k riešeniu rozsiahlych bezpečnostných incidentov majúcich dopad na IKT;
- preverenie funkčnosti interných procesov a postupov (havarijné plány, plány obnovy činnosti po rozsiahlom IKT incidente, eskalačné postupy, a pod.);
- preverenie schopností špecializovaného útvaru CSIRT.SK ako kontaktného bodu a národného koordinátora riešiť rozsiahly KII incident;
- budovanie dôvery a posilnenie spolupráce na národnej úrovni;
- získanie informácií potrebných pre vypracovanie vnútroštátneho plánu riešenia krízových situácií (National Contingency Plan - NCP), ktorého vypracovanie vyplýva z odporúčaní Európskej komisie;
- získanie skúseností pre prípravu a realizáciu ďalších cvičení riešenia rozsiahlych bezpečnostných počítačových incidentov.


2011
2012
2013
2014
EU US high-level tabletop
1/ Know each other
2/ Determine how the US would involve the EU (and vice versa) in its crisis management activities
Planning phase
Cyber Europe 2012
US as an observer ?
Planning phase
EU US crisis management exercise
No private sector
Planning phase
Cyber Europe 2014
US as a player?

Cyber Europe

Cyber Europe 2010:

- cvičenia zamerané na ochranu KII organizované pod záštitou agentúry ENISA a JRC,
- scenár: rekcia na simulované cielené kybernetické útoky majúce za následok ochromenie internetového prepojenia a kritických on-line služieb v Európe,
- účastníci cvičenia za SR: MF SR (CSIRT.SK), MDVRR SR, MV SR, TÚ SR
- **Ciele cvičenia:**
  - budovanie dôvery,
  - preverenie efektívnosti komunikácie,
  - riešenie incidentov v Európe,
  - overenie kontaktných bodov.

Cyber Europe 2012:

- potreba vytvorenia jednotného mechanizmu na výmenu informácií,
- príprava dokumentu „European Standard Operating Procedures (SOPs)“ – v podobe pracovnej verzie,
- cieľ: navrhnúť proces, kt. umožní efektívnu výmenu informácií medzi členskými štátmi počas obdobia krízy.

Cyber Atlantic 2011

Východiská:

- Summit EU-USA v novembri 2010 v Lisabone,
- založenie pracovnej skupiny EU-USA pre kybernetickú bezpečnosť a zločin (EU-US WG).

Ciele:

- identifikácia oblastí možnej vzájomnej EU-USA spolupráce,
- výmena informácií a overených postupov z oblasti reakcie na bezpečnostné incidenty a krízov manažmentu.

Scenár:

1. Advanced Persistence Threat (APT)
- únik a následné zverejnenie citlivých informácií na simulovanom portáli „Euroleaks“,
- USA sa cíti byť ohrozené a žiada EÚ o pomoc.

2. SCADA
- útoky na veterné elektrárne v EÚ,
- využitie existujúcej zraniteľnosti mikropočítača systému SCADA,
- EÚ žiada o asistenciu USA.

CSIRT.SK

DataCentrum

Cintorínska 5, 814 88 Bratislava

www.csirt.gov.sk

tel: 02 59 278 502

e-mail: info@csirt.gov.sk

incident@csirt.gov.sk