



1.stretnutie pracovnej skupiny „Kybernetická bezpečnosť“

ÚPPVII, 10. júla 2017



Program stretnutia

- Úlohy a otvorené body
- Obsahový a časový rámec
- Pravidlá pre externú komunikáciu
- Členovia pracovnej skupiny
- Predpokladané výstupy a zapojenie členov
- Harmonogram práce
- Iné / diskusia
- Ďalšie kroky



Úlohy a otvorené body

Čas a miesto pre stretnutia PS je zabezpečené, finálny obsah práce je potrebné spresniť dnes

- | | |
|--|-------------------------------|
| 1. Navrhnuť aspoň 2 možnosti pre ďalšie stretnutie PS | splnená |
| 2. Vytvorenie sharepointu
(https://sp.finance.gov.sk/kyberneticka-bezpecnost/SitePages/Domov.aspx) | splnená |
| 3. Rozhodnutie o pracovnej verzii štandardov / ďalší postup | splnená / diskusia o postupe |
| 4. Oslovenie 3 inštitúcií o nomináciu člena | splnená / nezáujem o členstvo |
| 5. Komunikácia s NBÚ – obsahové vyjasnenie pracovných skupín | v procese / doplnenie cieľov |

Otvorené body z posledného stretnutia:

Navrhnuť zmenu kompetencií v zákone o kybernetickej bezpečnosti / zákone o ochrane osobných údajov v prospech ÚPVII (vs NBÚ, vs ÚOOÚ). Spresniť pravidlá pre externú komunikáciu

Návrh vedúceho pracovnej skupiny: zaradiť návrh o spresnení kompetencií ÚPVII v oblasti bezpečnosti IS VS do cieľov pracovnej skupiny na 2H 2017

Obsahový a časový rámec

Obsahovo je práca PS určená 3 dokumentami, z ktorých vyplývajú niektoré aktivity pre druhú polovicu roku 2017

NKIVS

- zjednotenie formálnych požiadaviek
- riadenie rizík pre ISVS
- centralizované riadenie kontinuity činností
- zvyšovanie bezpečnostného povedomia používateľov
- riadenie požiadaviek na bezpečnosť u dodávateľov IT
- inovácia štandardov a riešení
- špecifické systematické riešenia ochrany údajov
- ...

Akčný plán 2015 – 2020 (úlohy pre MF SR, okrem DC)

- systematicky zvyšovať povedomie o aspektoch kybernetickej bezpečnosti
- rozšíriť existujúci projekt vzdelávania zamestnancov verejnej správy o oblasť kybernetickej bezpečnosti a zabezpečiť jeho realizáciu
- ...

OP II PO7, ŠC 7.9 Zvýšenie kybernetickej bezpečnosti

- vytvorenie nástrojov na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov
- zabezpečenie kritickej infraštruktúry
- zavádzanie európskej stratégie pre kybernetickú bezpečnosť
- ...

*Návrh zákona
o kybernetickej
bezpečnosti po MPK –
platný predpoklad?*

Predpokladané témy pre PS (2h2017):

1. Upravenie postavenia ÚPVII v procese riadenia bezpečnosti IS VS a ochrane osobných údajov vo verejnom sektore
2. Vytvorenie minimálnych štandardov pre riadenie bezpečnosti IS VS v súlade s EU stratégiami a návrh na ich implementáciu (vr. rizík / HR, atď)
3. Zvyšovanie povedomia zamestnancov VS v oblasti kybernetickej bezpečnosti
4. Podpora SORO OP II PO7 v oblasti tvorby nástrojov na monitorovanie a riadenie bezpečnostných incidentov



Pravidlá pre externú komunikáciu

Návrh S.D na pravidlá komunikácie mimo skupiny môže byť základom pre definovanie pravidiel pre túto oblasť.

Za Slovensko.Digital navrhujeme mať možnosť informovať ďalej (na našej komunikačnej platforme) nasledovné okruhy informácií:

1. základná informácia o hlavných riešených témach, prístupoch, rozhodnutiach
2. všetky formalizované podklady prezentované v rámci PS, pokiaľ samozrejme nie je dohodnutý ich interný charakter (špeciálne v tejto PS skutočne aj vidím dôvod niektoré informácie/materiály prebrať iba interne a nešíriť ich ďalej) - Tu navrhujem - **VŽDY** požiadať vlastníka informácie /materiálu o súhlas.
3. zápisy z PS, obzvlášť závery, úlohy, zadania a všetky schvaľované veci. Navrhujem až po schválení / akceptovaní vedením úradu.
4. pre spracúvané dokumenty, ktoré majú byť výsledkom činnosti PS ich štruktúru/zadanie (keď bude dohodnuté), následne pred finálnym pripomienkovaním/schvaľovaním zverejniť draft - aby bolo možné mať spätnú väzbu z odbornej komunity. **Toto je nedorozumenie** - ak Úrad bude niečo verejne pripomienkovať, tak sa tak postupuje. My sme len poradcovia úradu, t.j. nebudeme zdvojovať komunikačný tok - keď niečo Úrad da na pripomienkovanie, ide to podľa štandardných postupov.
5. v rámci interného tímu každého zúčastneného subjektu (v našom prípade interný tím za Slovensko.Digital) povolená plná komunikácia o všetkom čo sa v rámci PS rieši, samozrejme členovia interného tímu nemôžu tieto veci komunikovať ďalej



Členovia pracovnej skupiny

Na dnešné úvodné stretnutie bolo nominovaných 20 členov pracovnej skupiny

Nevyhnutní nominanti PS	Ministerstvá a ostatné ústredné orgány štátnej správy	Ďalšie subjekty
ÚPVII (2 – štandardy, stratégia) MF SR (2 – MF + CSIRT) MV SR (1) NASES (1)	MO SR (1) MK SR (1) MZ SR (1) MŠVVaŠ SR (1) MPaRV SR (1) ÚGKK (1) GP SR (2) SR SR (1) NR SR (1) MS SR (1) Soc.poist (1)	ITAS (1) Slovensko.Digital (1) SASIB (1) ISACA (1)

Finálny zoznam členov PS bude uzavretý na konci stretnutia (na základe dohodnutých tém a časového rámca – a ich možného zapojenia) a bude vytvorený tzv. dekrét členov



Predpokladané výstupy a zapojenie členov

Závisí od výsledku diskusie nominantov

Ilustrácia

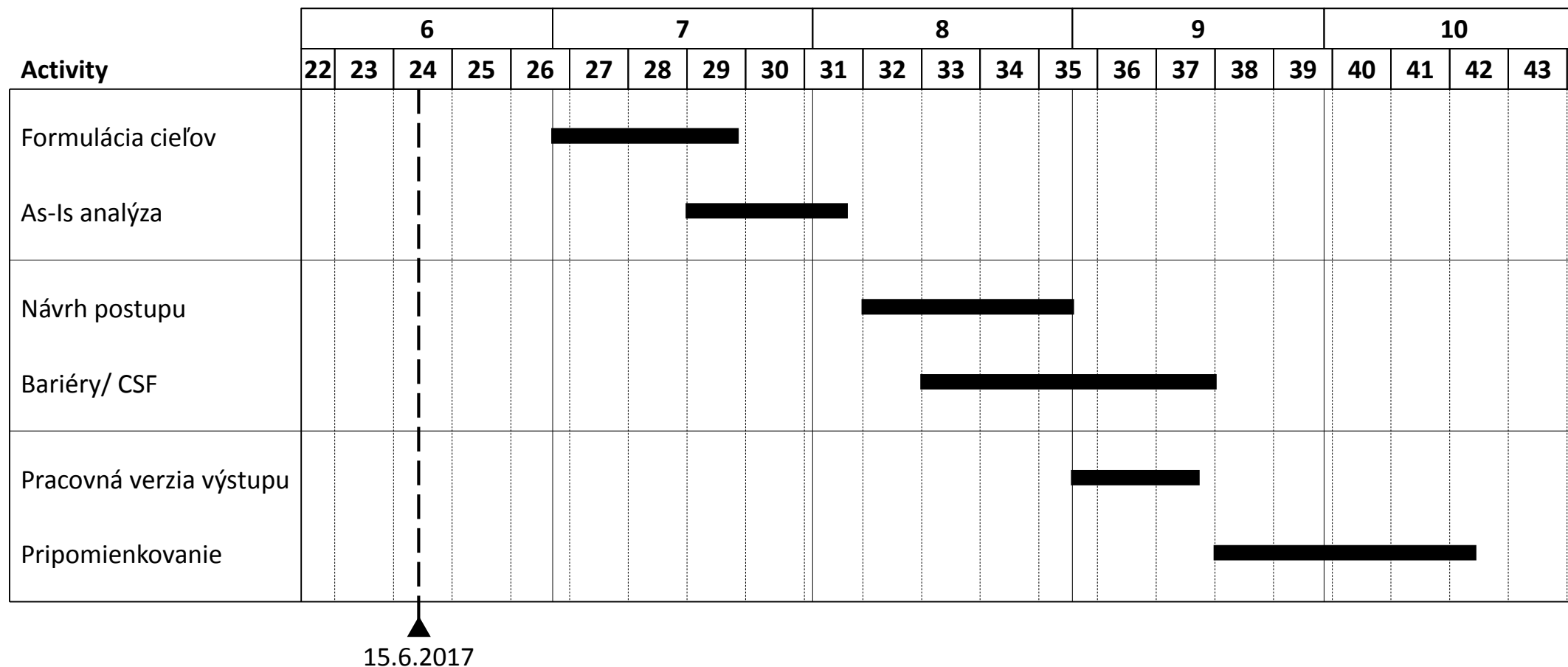
Oblasť č. 1	Cieľ	Predpokladané výstupy	Členovia
Vytvorenie minimálnych štandardov pre riadenie bezpečnosti IS VS			
Oblasť č. 2	Cieľ	Predpokladané výstupy	Členovia
Zvyšovanie povedomia zamestnancov VS v oblasti kybernetickej bezpečnosti			
Oblasť č. 3	Cieľ	Predpokladané výstupy	Členovia
Podpora SORO OP II PO7 v oblasti plnenie ŠC 7.9 Kybernetická bezpečnosť			



Harmonogram práce

Závisí od výsledku diskusie nominantov

Ilustrácia





Ďalšie kroky

Pracovné

Formálne vytvorenie pracovnej skupiny pre Kybernetickú bezpečnosť – ciele, výstupy, harmonogram a členovia (dekrét), podľa dnešného zápisu

T: 6.7.2017

Z: Poliak

Vytvorenie sharepointu pre PS v MetaIS, distribúcia prístupov

T: 6. 7. 2017

Z: Poliak

Zorganizovanie prvého pracovného stretnutia PS – podľa záverov dnešného úvodného stretnutia

T: podľa zápisu

Z: Poliak