

Záznam
zo stretnutia Pracovnej skupiny pre vytvorenie Metodického pokynu kategorizácie citlivosti údajov z dôvodu bezpečnosti (PS10)
uskutočneného 28. septembra 2012 na MF SR

Zúčastnení:

Peter Bíro (MF SR, predseda), Tibor Karász (MH SR, zástupca), Róbert Dobrovodský (MS SR, prizvaný), Ondrej Zimen (ÚOOÚ, člen), Radoslav Feďo (NASES, člen), František Boda (ITAS [EMM], člen), Štefan Porubčan (ITAS [Soitron], člen), Ľubor Illek (SOIT, člen), Rastislav Machel (nezávislý expert, člen)

Ospravedlnení:

Martin Horňák (MŠVVŠ SR, člen)

Neospravedlnení:

Erika Slivová (ITAS [Anasoft], člen), Aurel Ugor (MH SR, člen)

Program zasadnutia

1. Informácia o aktuálnom stave pracovného dokumentu na vypracovanie metodického pokynu
2. Diskusia k časti dokumentu o ochrane osobných údajov
3. Klasifikácia jednotlivých IKT na zverejniteľné a nezverejniteľné
4. Ostatné
5. Informácia o aktuálnom stave novelizácie zákona č. 211/2000 Z. z.
6. Závery

Priebeh zasadnutia:

Zasadnutie Pracovnej skupiny pre vytvorenie Metodického pokynu kategorizácie citlivosti údajov z dôvodu bezpečnosti PS10 (ďalej len „pracovná skupina“) viedol jej predseda P. Bíro.

1. Informácia o aktuálnom stave pracovného dokumentu na vypracovanie metodického pokynu

P. Bíro v krátkosti informoval o doplnenom pracovnom dokumente na vypracovanie metodického pokynu (ďalej len „pracovný dokument“) a poďakoval členom pracovnej skupiny za odoslané pripomienky, doplnenia ako aj za návrhy kategorizácie jednotlivých typov údajov o IKT. Ďalej uvítal, že Ministerstvo spravodlivosti SR sa taktiež aktívne zapojilo do činnosti PS10. Následne vyzval členov, aby sa vyjadrili k časti textu pracovného dokumentu o ochrane osobných údajov.

2. Diskusia k časti dokumentu o ochrane osobných údajov

P. Illek poznamenal, že v zásade nevidí problém v takomto texte, len sa obáva toho či vzhľadom na existujúcu právnu úpravu obmedzenia prístupnosti osobných údajov v zákone č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 211/2000 Z. z.“) nebude vznikať chaos. P. Bíro oponoval a povedal, že víta takýto vysvetľujúci text vzhľadom na viaceré existujúce nejasnosti v aplikačnej praxi povinných osôb. Niektorí členovia pracovnej skupiny vyzdvihli užitočnosť demonštratívneho výpočtu príkladov osobných údajov, ktoré majú zároveň aj povahu IKT.

P. Bíro vyzval P. Zimena na doplnenie textu o ďalšie informácie z aplikačnej praxe. Z ďalšej diskusie vyplynulo, že predmetný text by mohol byť doplnený aj výkladom týkajúcim sa IP adries v súvislosti s tým, za akých okolností sa stávajú osobným údajom ako aj vhodnosť rozšírenia počtu demonštratívnych príkladov. P. Zimen zabezpečí doplnenie textu v tejto časti.

V súvislosti s kategorizáciou jednotlivých IKT p. Zimen požiadal členov pracovnej skupiny o zaradenie jednotlivých obsahových súčastí bezpečnostného projektu do konkrétnej kategórie údajov o IKT z hľadiska možnosti ich prístupnosti resp. neprístupnosti. P. Machel v tejto súvislosti upozornil na to, že nový zákon o ochrane osobných údajov, ktorý je v súčasnosti v legislatívnom procese a určité podrobnosti týkajúce sa bezpečnostného projektu bude určovať až vo všeobecne záväznom právnom predpise, ktorý vydá UOOÚ SR. P. Zimen poznamenal, že základné obsahové náležitosti bezpečnostného projektu (bezpečnostný zámer, analýza bezpečnosti informačného systému, bezpečnostné smernice) by sa nemali meniť.

3. Klasifikácia jednotlivých IKT na zverejniteľné a nezverejniteľné

P. Bíro najprv zhrnul zmeny, ktoré v návrhu metodiky nastali a následne prešiel ku konkrétnym pripomienkam týkajúcim sa kategorizácie jednotlivých údajov o IKT. V tejto súvislosti prebehla diskusia ku celémurozsahu identifikovaných údajov o IKT, a najmä k tým, ktoré boli z hľadiska kategorizácie označené viacerými členmi PS10 rozdielne. S odbornými poznámkami sa zapojili hlavne p. Bíro, p. Machel, p. Illek, p. Boda a p. Porubčan.

V priebehu diskusie sa konsenzuálne určila príslušná kategória každému údaju o IKT, pričom otvorená zostala iba otázka kategorizácie troch položiek týkajúcich sa politiky správy aktív, konkrétne "určenie kritickosti aktív", "konkrétne zaradenie údajov podľa citlivosti" a "konkrétne zaradenie IS podľa kritickosti", kde aj pri hlasovaní nastala nerozhodná situácia. Táto časť bude doriešená v blízkej budúcnosti buď elektronickou komunikáciou alebo na ďalšom stretnutí. Niektoré údaje boli pre duplicitu zlúčené, diskutované bolo aj do akej podrobnosti je možné niektoré údaje zverejniť (napr. pre parametre softvéru a hardvéru).

P. Boda vo všeobecnosti zdôraznil aspekt ohrozenia bezpečnosti informačného systému v súvislosti so sprístupnením viacerých údajov o IKT. Nasledujúca diskusia zástupcov tretieho sektora potvrdila záver, že je potrebné v súvislosti s ústavným právom na šírenie informácií a jeho zákonným rámcom v zákone č. 211/2000 Z. z. sprístupňovať aj také údaje o IKT, ktoré síce predstavujú hypotetické bezpečnostné riziko, ale toto riziko je vzhľadom na konkrétny údaj o IKT prijateľné, keďže v extrémnom poňatí už samotná informácia o existencii konkrétneho informačného systému predstavuje bezpečnostné riziko.

P. Illek otvoril tému v súvislosti so sprístupňovaním / nesprístupňovaním údajov o IKT, na ktoré sa môže vzťahovať autorské právo jeho pôvodcu. Rozobrali sa niektoré aspekty tejto problematiky. V tejto súvislosti bola skonštatovaná potreba doplnenia informácie, že metodika sa bude zaoberať iba kategorizáciou z pohľadu bezpečnosti a nie z pohľadu autorských práv, obchodných tajomstiev a iných bariér pre zverejnenie, ktoré majú vlastné mechanizmy.

Osobitnou témou bola definícia „neaktuálnosti údajov“, kde vyplynulo, že to musí údaj neaktuálny nielen pre dané IKT, ale aj pre akékoľvek existujúce (používané) IKT. Základ definície zašle p. Fed'ó.

4. Ostatné

P. Karász upozornil na pojem citlivá informácia, ktorý sa používa v pracovnom dokumente v súvislosti so zákonom č. 45/2011 Z. z. o kritickej infraštruktúre (ďalej len „zákon o kritickej infraštruktúre“). Ďalšia diskusia sa týkala informačných systémov, ktoré sú prevádzkované v režime zákona o kritickej infraštruktúre, ktorej výsledkom bolo skonštatovanie, že údaje o IKT, ktoré budú sprístupňované resp. nesprístupňované v režime zákona č. 211/2000 Z. z. majú iný režim ako citlivé informácie v zmysle zákona o kritickej infraštruktúre.

P. Dobrovodský v tejto súvislosti upozornil na nepriamu novelu zákona č. 211/2000 Z. z. zákonom o kritickej infraštruktúre. Z diskusie vyplynulo aj to, že by bolo vhodné použiť iné terminologické označenie pojmu „citlivá informácia“ na účely pracovného dokumentu.

5. Informácia o aktuálnom stave novelizácie zákona č. 211/2000 Z. z.

P. Dobrovodský informoval členov pracovnej skupiny o aktuálnom stave novelizácie zákona č. 211/2000 Z. z. V podstate ide o nevyhnutnú transpozíciu európskej legislatívy, a preto je potreba obmedzenia sprístupnenia údajov o IKT obmedzená iba na novozavádzaný právny inštitút opakovanej informácie, čo je možné hodnotiť ako nedostačujúce, pretože pracovný dokument má ambíciu byť pomôckou pre orgány verejnej správy v celom režime sprístupňovania informácií na základe zákona č. 211/2000 Z. z. P. Bíro a p. Illek uviedli, že pripomienka zo strany MF SR bola k novele v úplnom systémovom riešení a MF SR bude na tejto pozícii trvať aj do budúcnosti.

Ďalej pán Dobrovodský upozornil na rámec zákonnej právnej úpravy, ktorý má priniesť pri obmedzovaní sprístupňovania informácií prebiehajúca novelizácia zákona č. 211/2000 Z. z. v súvislosti s rozsahom pracovného dokumentu. V zmysle Ústavy Slovenskej republiky totiž podzákonný právny predpis nemôže ísť pri úprave práv a povinností nad rámec existujúceho zákona. P. Zimen sa stotožnil s pripomienkou p. Dobrovodského. Vzniknutú situáciu je možné riešiť viacerými spôsobmi, ktoré budú predmetom diskusie najmä medzi MS SR a MF SR. P. Dobrovodský vyzdvihol zloženie pracovnej skupiny, ktorú tvoria aj zástupcovia tretieho sektora resp. zástupcovia žiadateľov o sprístupnenie informácií ako aj zástupcovia orgánov štátnej správy resp. povinných osôb, ako aj odbornosť členov pracovnej skupiny. Tieto

skutočnosti považuje za podstatné pri ďalšom presadzovaní právnej úpravy upravujúcej obmedzenie sprístupnenia údajov o IKT.

6. Závery

1. Záznam zo stretnutia pracovnej skupiny vyhotoví p. Zimen
Zabezpečí p. Zimen Termín: do 5. 10. 2012
2. Zapracovanie pripomienok a záverov k jednotlivým častiam metodiky.
Zabezpečí p. Bíro Termín: do 31. 10. 2012
3. Do časti textu o ochrane osobných údajov sa doplní výklad o IP adresách.
Zabezpečí p. Zimen Termín: 15. 10. 2012
4. V súvislosti s anonymizáciou osobných údajov v režime sprístupňovania sa odkáže na príslušné usmernenie MF SR (bod 6.1 Usmernenia pre konverziu písomných dokumentov na elektronické dokumenty V3)
Zabezpečí p. Bíro Termín: do 31. 10. 2012
5. Prehodnotiť ďalší postup pracovnej skupiny ako aj použitie pracovného dokumentu v intenciách novelizácie zákona č. 211/2000 Z. z.
Zabezpečí p. Bíro a p. Dobrovodský Termín: do 15.10.2012

O hlasovaní o termíne prípadného ďalšieho stretnutia bude informovať p. Bíro členov pracovnej skupiny elektronicky v dostatočnom predstihu.