Záznam
zo stretnutia Pracovnej skupiny pre bezpečnostné štandardy (PS10)
uskutočneného 26. februára 2013 na MF SR

Zúčastnení:
Peter Bíro (MF SR, predseda), Anna Levčíková (MF SR, člen), Nadežda Nikšová (MF SR, prizvaná), Tibor Karász (MH SR, zástupca), Ondrej Zimen (ÚOOÚ, člen), Radoslav Feďo (NASES, člen), František Tomajko (NASES, zástupca), Petra Hochmannová (CSIRT.SK, člen), Lukáš Hlavička (CSIRT.SK, prizvaný), Peter Belák (ITAS [EMM], zástupca), Štefan Porubčan (ITAS [Soitron], člen), Jaroslav Janáček (Slovenská informatická spoločnosť, člen), Tomáš Zaťko (SOIT, zástupca), Lucia Menkeová (Rowan Legal, člen), Richard Hollý (ITAS, prizvaný)

Ospravedlnení:
Martin Horňák (MŠVVŠ SR, člen)

Neospravedlnení:
Rastislav Machel (nezávislý expert, člen), Erika Slivová (ITAS [Anasoft], člen)

Program zasadnutia

1. Informácia o transformácii náplne pracovnej skupiny.
2. Návrh štandardu „Cloud Ready".
3. Návrh štandardov NASES pre integráciu s Ústredným portálom verejnej správy.
4. Ostatné.

Priebeh zasadnutia:

Zasadnutie Pracovnej skupiny pre bezpečnostné štandardy (ďalej len „PS10" viedol jej predseda P. Bíro.

1. Informácia o transformácii náplne pracovnej skupiny

P. Bíro v krátkosti informoval o zmene pracovnej náplne PS10, ktoré vyplynulo z 13. stretnutia Komisie pre štandardizáciu informačných systémov verejnej správy. PS10 sa má perspektívne zaoberať celým spektrom bezpečnostných štandardov a zároveň sa bude zaoberať aj prvotným spracovaním a pripomienkovaním návrhu štandardov pre oblasť cloud computingu. P. Bíro v tejto súvislosti informoval o rozšírení členského rámca PS10.

2. Návrh štandardu „Cloud Ready"

Zástupca ITAS p. Richard Hollý predstavil návrh štandardu pre oblasť cloud computingu, tzv. „Cloud Ready". V tejto súvislosti uviedol, že pôvodným zámerom predloženého dokumentu bolo nastaviť kritériá pre budúce projekty OPIS, t.j. pôvodne nebol pripravovaný ako štandardizačný dokument.

Ďalej uviedol, že návrh bol vypracovaný na téze, že pre služby eGovernmentu sa v najbližšej dobe bude brať do úvahy iba privátny cloud, inými podobami cloudu sa teda návrh nezaoberal. Najjasnejšou oblasťou návrh je podľa neho taxonomická oblasť, ktorá má zabrániť zbytočné rekapitulácie známych faktov v jednotlivých projektoch, a to navyše pomocou odlišných pojmov. Ďalšími oblasťami sú bezpečnosť (iba rámcovo), referenčná architektúra (vychádza z architektonického modelu NIST) – najnižšia vrstva t.j. dodávanie zdrojov, model vyspelosti (momentálne je najmenej štandardizovateľný, návrh vychádza z modelu CMMI) a služby (rozpracované boli rámcovo iba IaaS, nezaoberá sa PaaS alebo SaaS). Podľa p. Hollého zatiaľ absentuje napr. aj „finančný model“ (finančného alebo nefinančného charakteru). Na Slovensku zatiaľ v oblasti cloud computingu nie je prijatá žiadna vládna stratégia.

P. Bíro k tomuto uviedol, že fáza vydania pre OPIS je podľa neho uzavretá, nakoľko PS10 sa zaoberá štandardizáciu z pohľadu informačných systémov verejnej správy (ďalej len „IS VS“), je však potrebné určiť komu má byť tento štandard určený a čo z neho má byť povinné. Povinné a odporúčané časti sa určia na základe kontextu a určeného rámca, rovnako ako aj presná forma publikácie. Zhodnotil aj, že zatiaľ absentuje predloženie sprievodných kritérií pre posudzovanie štandardov v aktuálnej verzii 4.3.

Následne zhrnul aktuálnu situáciu v štandardizácii v tejto oblasti z pohľadu EÚ, kde boli súčasťou podkladov 3. stretnutia PS10 aj závery prvého stretnutia ETSI, ktorého výstupy v oblasti cloud computingu bude potrebné zahrnúť do pripravovaného štandardu.

P. Bírovi chýbalo v návrhu napr. riešenie otázok prenositeľnosti údajov (keďže nepredpokladá, že vo verejnej správe bude existovať jediný cloud), interoperability cloudov (z obdobného dôvodu), reverzibility údajov a servisných licenčných zmlúv (SLAs). Podľa jeho slov je na základe všeobecne akceptovaného súčasného vývoja najkritickejšou témou cloudu bezpečnosť.

P. Hollý zaujal pozitívne stanovisko a skonštatoval, že bezpečnosťou sa je potrebné v službách eGovernmentu zaoberať, a to v podstate nezávisle od toho, či sa jedná alebo nejedná o cloud.

P. Bíro s tým súhlasil a uviedol, že návrh by sa mal zaoberať práve odlišnosťami od už existujúcich bezpečnostných požiadaviek, najmä začlenenie do rámca existujúcich štandardov. Okrem toho každá legislatívna požiadavka musí byť jednoznačná a merateľná, čo v mnohých častiach predloženého návrhu nie je tak. Túto pripomienku uviedol aj p. Zaťko, pričom podľa neho absentovali aj odkazy na normatívne dokumenty.

P. Hollý zhodnotil, že navrhnutý dokument aktuálne nerieši nadväznosť.

P. Zaťkovi chýbal spôsob realizácie a niektoré požiadavky považoval za neodôvodnene silné (napr. certifikáciu voči ISO/IEC 27001, a to bez uvedenia úrovne), ktoré by sa mohli stať blokovacími.

P. Hollý odvetil, že „prisilné pravidlá“ boli nastavené preto, aby dochádzalo k centralizácii resp. zamedzeniu „rozptylu“ Government cloudov na neriadené rezortné riešenia, ktoré nebudú spĺňať potrebnú úroveň.

P. Bíro doplnil, že prísnosť požiadaviek závisí práve od toho, komu má byť navrhovaný štandard určený a zároveň povedal, že mu celkovo v návrhu vo viacerých prípadoch absentuje merateľnosť. Pre dodávateľov je možné napísať odporúčanie, a to aj v osobitnom dokumente.

P. Porubčan podporil, že pokiaľ nebudú definované oblasti a adresáti, veľmi ťažko je možné vytvárať alebo pripomienkovať podrobnosti.

P. Levčíková považovala za potrebný prvý krok vytvorenie scenáru nasadenia cloudu v rámci verejnej správy. P. Bíro súhlasil a zároveň doplnil, že témy sa však dajú identifikovať a popísať v určitom rozsahu aj v súčasnom stave.

P. Menkeová skonštatoval, že návrh popisuje technické pravidlá, ale chýbajú jej právne riziká, napr. vo forme najlepších praktík alebo nejakého odpočítateľného zoznamu, a to najmä vo vzťahu k ochrane osobných údajov. P. Bíro doplnkovo upozornil na ďalšiu legislatívu, ktorá sa chystá zo strany EÚ, ktorá sa dotkne bezpečnostných požiadaviek. V súvislosti s odkazmi na normy poznamenal, že od rozsahu dotknutých osôb závisí aj to, či budú postačovať odkazy alebo bude potrebné požiadavky prepísať do legislatívy.

P. Bíro požiadal upraviť úvod v súvislosti s tým, že neexistuje žiadna spoločne zriadená skupina ITAS a MF SR, ktorá by sa zaoberala vytváraním dokumentu ohľadom cloud computingu, jedinou platformou, ktorou takýto štandard prejde je PS10 resp. Komisia a podľa potreby jej ďalšie pracovné skupiny. Ďalej upozornil na rôzne nejasnosti v navrhovaných požiadavkách a použitých skratkách.

P. Feďo a následne p. Bíro v diskusii informovali ostatných členov o aktuálne pripravovaných ISO normách, ktoré sa týkajú cloudu.

P. Hollý videl problém v popisovaní podrobností ohľadom komponentov a rôznych pohľadov resp. rolí. P. Bíro odvetil, že nezrozumiteľnosť je v legislatíve neprípustná, otázka je skôr hĺbka detailov.

P. Zimen, že asi najprácnejšie podľa neho bude vypracovanie základnému hmotno-právnemu vymedzenia subjektov, najmä v súvislosti k osobným údajom. Problematické vidí napr. dodržanie princípu, že prevádzkovateľ nemôže združovať osobné údaje, ktoré spracováva na viaceré účely v jednom informačnom systéme.

P. Hollý odvetil, že cloud by sa nemal chápať ako informačný systém, avšak p. Zimen oponoval, že zákon o ochrane osobných údajov používa vlastnú definíciu informačného systému, ktorá je braná z iného pohľadu ako IS VS. Následne prebehla diskusia k vlastnej definícii informačného systému vo vzťahu k pojmov v zákone 275/2006 Z. z., resp. ďalších pojmov v legislatíve k osobným údajom, ktorá na stretnutí nebola uzavretá. P. Zimen doplnil, že nie každý model cloudu musí hmotno-právne spadať pod rámec ochrany osobných údajov, pracovná skupina WP29 na úrovni EK preto podľa neho vydala stanovisko, že aj ak poskytovateľ poskytuje iba hardvérovú infraštruktúru, mal by byť braný ako sprostredkovateľ.

Prebiehala aj osobitná diskusia autentizácii, kde sa pripravuje viac predpisov, a to aj na úrovni EÚ.

P. Hollý informoval o existencii wiki, kde sú publikované príslušné materiály. Členovia PS10 prejavili záujem o vytvorenie prístupov. Uvedené bude pre záujemcov organizačne zabezpečené po stretnutí.

P. Bíro upozornil, že do aktuálnej novely výnosu sa dostane iba to, čo sa podarí spracovať do približne júna 2013. V tejto súvislosti skonštatoval, že ak je potrebné stihnúť novelu výnosu, nie je vhodné vytvárať ešte predtým metodiku, ale vytvárať rovno formulácie do výnosu a metodika môže nasledovať v častiach, ktoré majú byť odporúčané, alebo ktoré je potrebné ďalej vysvetliť. Vyjadrenia sú podľa neho nutné

aj pre časti, ktorými sa návrh nebude zaoberať alebo ich nevie popísať. Bezpečnosť cloudu pravdepodobne bude doplnená ako osobitné časti bezpečnostných štandardov.

P. Hollý doplnil, že v rámci wiki sa zameriavajú najmä na obsahovú stránku. P. zhodnotil, že k obsahovej stránke mu z pohľadu bezpečnosti absentujú SLA a plán kontinuity biznisu.

Záverom tohto bodu bolo, že predkladateľ návrhu do 2 týždňov predloží upravenú verziu, a to najmä v súvislosti s jasným zadefinovaním rozsahu a adresátov budúceho štandardu a popisu štruktúry požiadaviek, pričom vlastný dokument sa uvedie na príslušnej wiki a členovia PS10 budú notifikovaní e-mailom. Členovia následne zašlú svoje pripomienky do ďalších 2 týždňov. Ďalšie stretnutie bude približne o mesiac. Prvou časťou ďalšej diskusie bude terminológia.

3. Návrh štandardov NASES pre integráciu s Ústredným portálom verejnej správy

PS10 sa bude zaoberať bezpečnostnou časťou návrhov NASES. PS10 zatiaľ k návrhom pre krátkosť času nezaujala stanoviská, iba pripomienkovala rôzne aspekty návrhov.

P. Bírovi rámcovo vo všetkých návrhoch absentoval ich účel.

K návrhom 01-1 a 01-3 (SAML token a SAML)

P. Zaťko pripomienkoval, že úrovne autentifikácie by podľa neho mali byť riešené samostatne.

Podľa p. Bíra okrem účelu použitia absentujú aj vzťahy k SAML 1.0 a 1.1, t.j. povolenosť či nepovolenosť použitia a interoperabilita.

P. Hollý upozornil, že na úrovni EÚ boli definované určité úrovne autentifikácie, kde je potrebné zabezpečiť párovanie a pri nastavovaní úrovní aj popis príslušných rizík a ich znižovania, pričom pre jednotlivé služby by mali byť úrovne nastavované adekvátne a nie zbytočne vysoko alebo nízko, čo v rámci návrhu federácie identít absentuje. Podľa neho by malo byť definovaných niekoľko samostatných úrovní federácie a zodpovedajúcich úrovní autentifikácie, a to najmä v súvislosti s požiadavkami na prechod na vyššiu úroveň bezpečnosti. SAML je z tohto pohľadu v širšom kontexte veľmi dôležitým štandardom pre zabezpečenie ochrany údajov.

Členovia PS10 nevyjadrili žiadne pochybnosti ohľadom vlastného návrhu používať protokol SAML 2.0, p. Bíro informoval, že pripomienkou zo strany PS4 bolo, že tento štandard nie je v návrhu dostatočne popísaný (najmä z pohľadu interoperability). Ďalej informoval, že v niektorom legislatívnom predpise bude nutné popísať úrovne autentifikácie podľa európskych metodík, aby boli všetky úrovne napárovateľné, pričom problém je najmä s vágnosťou popisu úrovní 2 a 3.

P. Hollý odporučil úrovne spojiť s analýzou rizík (t.j. „čo sa stratí prechodom na nižšiu úroveň“), p. Bíro odvetil, že sa očakáva, že každá služba verejnej správy bude mať popísanú svoju úroveň bezpečnosti (autentizácie), pričom v súčasnosti sú mnohé služby prehnane identifikované a prehnane autentizované, t.j. majú zbytočné vysoké požiadavky. P. Bíro prisľúbil zaslať členom PS10 rozpracované návrh prebratia úrovní autentizácie podľa európskej metodiky.

Podľa p. Zaťka neboli vyriešené ani aspekty ohľadom federácie, napr. kto za čo ručí, čo sa deje v prípade kompromitácie alebo životnosť single-sign-on relácie. V súvislosti s popísanými certifikátmi nebol podľa neho v návrhu úplne jasný vzťah k zaručenému elektronickému podpisu. P. Hollý v súvislosti so single-sign-on upozornil, že niektoré služby potrebujú mať token validný 24 hodín a niektoré niekoľko mesiacov, čo bude takisto potrebné vyriešiť.

P. Bíro upozornil aj na nesúlad návrhu s katalógom dátových prvkov podľa platného výnosu o štandardoch pre informačné systémy verejnej správy.

K návrhom 08-1 a 08-2 (štandardy pre formáty dlhodobého uchovávania)

Podľa p. Bíra bude k diskusii k tejto téme potrebná účasť aj relevantného zástupcu Ministerstva vnútra SR ako predpokladaného gestora Identifikačného a autentifikačného modulu Ústredného portálu verejnej správy a zároveň gestora legislatívy pre registratúry (vrátane štandardov). Zároveň upozornil, že formáty pre podpisovanie sú určované už existujúcou legislatívou, ktorú je potrebné v návrhu zohľadniť.

P. Zaťko pripomenul, že zatiaľ nie sú štandardizované procesy – formátová normalizácia a formátová migrácia, pričom k samotným formátom by sa mala vyjadriť aj PS4.

K návrhu 10-1 a 08-2 (štandardy pre chat)

P. Bíro skonštatoval, že aj keď tento návrh je principiálne technický, v praxi je to väčšinou bezpečnostná otázka. Ďalej opätovne zhodnotil, že mu chýba komu má byť tento štandard určený a na aké účely.

P. Hollý v súvislosti s eHealth uviedol, že v rámci telemetrie bol obdobný štandard diskutovaný až na úroveň videa t.j. multimédií a položil otázku, kde by sa mali takéto témy vecne preberať, kde XMPP nepovažoval za vhodný štandard. Dodal aj, že štandard SAML takisto môže byť pre takúto komunikáciu výraznou prekážkou.

P. Bíro doplnil, že generické (prierezové) štandardy pre informačné systémy verejnej správy patria do gescie Ministerstva financií SR, teda týchto pracovných skupín. Špecifické rezortné požiadavky patria do gescie príslušných rezortov.

Uviedol, že otázkou z pohľadu administratívnej bezpečnosti je aj úroveň klasifikácie údajov, pri ich preberaní cez chat.

K návrhu 11-1 (formulár pre zastupovanie)

P. Bíro uviedol, že vzhľadom na to, že neexistuje nejaká generálna úprava či zoznam rolí v rámci možných splnomocnení (najmä v oblasti súkromného práva), táto téma nie je vôbec jednoduchá a všeobecný generický štandard, ktorý by bol použiteľný v elektronickom prostredí pre všetky typy splnomocnení automatizovane pravdepodobne nie je možné vytvoriť. Je ho však možné vytvoriť pre niektoré typizované role, ako napr. notári. P. Bíro upozornil aj na existujúcu národnú legislatívu (mandátne certifikáty) a pripravovanú európsku legislatívu, ktorou vznikne elektronická pečať (podpis právnickej osoby). Podpis elektronickej podateľne podľa návrhu je nepoužiteľný.

P. Zaťko doplnil, že v súvislosti s formulármi je potrebné dodržať formát pre elektronické formuláre (podľa PS6), popis štandardu v návrhu je nedostačujúci, otázkou je aj, či ten formulár vystavuje ten, kto je zastupovaný alebo Ústredný portál verejnej správy. Formát XAdES má zase problém na európskej úrovni.

P. Hollý rozšíril predložené informácie o fakt, že takáto otázka v súvislosti s ÚP VS nebola diskutovaná, ani nie je riešená v projektoch OPIS, kde napr. ESO1 (eHealth) túto tému riešil odlišných spôsobom.

K návrhu 11-2 (SK-TALK)

P. Zaťko uviedol, že návrh neobsahuje žiadne bezpečnostné požiadavky, ani na dôvernosť, ani na identitu, vzťah so ZEP.

P. Bírovi chýbal spôsob výmeny šifrovanej správy, pretože mnoho údajov vymieňaných v prostredí verejnej správy má minimálne citlivý charakter.

Záverom diskusie bolo, že predkladateľ návrhu doplní v zmysle pripomienok a opätovne ich predloží na ďalšie rokovanie, inak sa PS10 nebude ďalej návrhmi zaoberať.

4. Ostatné

P. Zaťko požiadal, či by bolo možné v pozvánke indikovať predpokladanú dĺžku stretnutia. P. Bíro odvetil, že štandardná dĺžka trvanie je do 12:00 až 12:30, ale takúto informáciu je možné dopĺňať.

Ďalšie stretnutie PS10 sa bude konať o približne mesiac, t.j. najskôr v 13. týždni roku 2013.

5. Závery

1. Upraviť návrh štandardu „Cloud Ready“ v zmysle pripomienok a zaslať ho všetkým členom PS10.
   Zabezpečí: ITAS Termín: do 12. 3. 2013

2. Upraviť návrh štandardov NASES v zmysle pripomienok a zaslať ho Ministerstvu financií SR.
   Zabezpečí: NASES Termín: do 25. 3. 2013

3. Podľa možnosti spracovať a zaslať pripomienky k návrhu podľa bodu 1.
   Zabezpečí: členovia PS10 Termín: do 25. 3. 2013

4. Zaslať predbežnú verziu návrhu prebratia úrovní autentizácie podľa európskej metodiky.
   Zabezpečí: P. Bíro Termín: do 1. 3. 2013