[VAŠE POTREBY] [NAŠE RIEŠENIA]

Úvodník

Rok sa presunul do svojho ďalšieho obdobia a leto je už nenávratne za nami. Veľa z nás ho využili na regeneráciu a obnovu svojich síl, aby sa pustili do novej práce. Jeseň je pre mnohých, hlavne poľnohospodárov, bilancovaním svojho snaženia po celý rok. Aj keď nie sme poľnohospodári, môžeme aj my na jeseň bilancovať. Dokončili sme tretiu verziu nášho produktu na zálohovanie dát, **KERBER BackUp Server**, ktorú v týchto dňoch uvádzame na trh. Ide o významný krok vpred a preto sme sa rozhodli uvedenie tejto verzie podporiť šnúrou prezentácií po Slovensku. Pokiaľ by ste mali aj vy záujem zúčastniť sa tejto prezentácie, tak pozvánku na ňu nájdete na konci tohto newsletteru.

RNDr. Daniel Schikor
Produktový manažér

[VAŠE POTREBY] [NAŠE RIEŠENIA]

Zabezpečte si dáta bezpečne

Bezpečnosť v dátovej komunikácii je v dnešnej dobe široký pojem a mnohí sa v tejto problematike strácajú. Neraz nakupujú drahé zariadenia a riešenia, a napriek tomu zaznamenávajú úniky dát a vniknutia do dôležitých systémov. Riešenie nie je ukryté vo vysokej cene, ale v komplexnosti a správnom nastavení procesov. Bezpečnosť dát sa dnes stáva otázkou samotného prežitia.

Dômyselné softvérové nástroje môžu v súčasnom zmätku na všade prítomnom Internete ľahko preniknúť do informačných systémov a bez pozorovania monitorovať informácie ukryté v ňom. Môžete prísť o cenné dáta a tie môžu skončiť v rukách konkurencie. Jedinou ochranou je zabezpečenie vašej lokálnej siete z Internetu a dôsledná kontrola dátovej komunikácie. Tú Vám zabezpečí naše riešenie **Kerber Secure Server**, ktoré plní úlohu bezpečnostnej brány do siete Internet. Jeho úlohou je ochraňovať Vašu sieť a dáta, ktoré plynú medzi vami a Internetom, a v neposlednom rade aj dohliadať na správanie vašich zamestnancov.

Internetom sa šíria rôzne typy vírusov ransomware, ktoré sú schopné zničiť vaše súbory. Snažia sa preniknúť do vašich počítačov, čo sa im často darí za pomoci „neznalého zamestnanca“, ktorý klikne na neznámu prílohu mailu. Tým otvorí vírusu cestu na zašifrovanie súborov nie len na pevnom disku, ale aj na pripojených USB diskoch. Pokiaľ sa takéto niečo udeje, tak už vám neostáva iná možnosť, len zaplatiť výkupné, ktoré niekedy dosahuje hodnotu aj niekoľko tisíc eur alebo obnoviť dáta zo zálohy, ak ju máte. Jednou z možností, ako sa chrániť, je použitie silnej antispamovej kontroly. Tá tvorí súčasť nášho **Kerber Mail Servera,** ktorý predstavuje veľmi účinnú metódu v boji so spam botnetmi. Najlepšou ochranou je ale nezávislé a pravidelné zálohovanie všetkých dôležitých dát z lokálnych počítačov. Tak ako to dokáže náš **Kerber BackUp Server,** ktorý síce neslúži pre ochranu pred vírusmi, ale v prípade ransomware je účinným nástrojom pre obnovenie dát a tým aj pre zamedzenie zámeru „výpalníkov“ získať od vás nemalé prostriedky.

Pokiaľ Vám na Vašich dátach skutočne záleží, tak vám odporúčame zúčastniť sa našej **RoadShow,** kde vám bližšie ozrejmíme vyššie popísané témy. **Registrovať sa môžete tu.**

Buďte pripravení, pretože väčšina bezpečnostných incidentov a rizík vychádza z nepripravenosti!

Bezpečnosť je dôležité vnímať ako proces.

[VAŠE POTREBY] [NAŠE RIEŠENIA]

5 dôvodov prečo zálohovať

Vaše dáta nie sú len zhlukom jednotiek a núl, ale sú práve srdcom a dušou Vášho podnikania. Zachovanie týchto dát už dnes nie je otázkou pohodlia, ale stáva sa otázkou samotného prežitia. Strata dát môže nastať mnohými spôsobmi. Poruchy pevných diskov v počítačoch, vyliata káva do klávesnice notebooku alebo neobnoviteľné či náhodné (nechcené) vymazanie súboru sú pomerne časté javy. Ku strate dát môže dôjsť hocikedy i pri malom technickom probléme. Poďme sa teda detailnejšie pozrieť kde vám hrozí nebezpečenstvo.

1. Zlyhanie alebo poškodenie disku

Kvôli opotrebovaniu mechanických súčastí či vplyvom vysokej teploty môžu pevné disky začať zlyhávať. Že niečo nie je v poriadku môžete zistiť z dát, ktoré produkujú. Prístup k údajom na disku sa spomalí a časom nie je možné niektoré súbory už ani prečítať a každým čítaním z disku sa situácia zhoršuje. Údaje na disku sa stávajú pre Vás nepoužiteľné a pokiaľ nemáte urobenú zálohu môžu byť nenávratne stratené. Priemerná miera zlyhania diskov a páskových jednotiek je 100% – všetky jednotky nakoniec zlyhajú. Je to len otázkou času.

2. Zlyhanie ľudského faktoru

Nikto z nás nie je neomylný a týka sa to aj práce s počítačom. Mnohokrát sa stáva, že si človek v návale práce prepíše alebo dokonca zmaže dôležitý súbor, ktorý používa ako mustru. Potom sa musí prácne vracať k pôvodnej verzii. Dosť často sa vyskytujú aj chyby spôsobené chvíľkovou nepozornosťou. Napríklad pri čistení preplneného disku si môžeme zmazať aj to čo sme nechceli. Nie nadarmo sa hovorí, že neznalý alebo zmätený používateľ môže často spôsobiť väčšie škody než útok vírusov.

3. Záškodníctvo

Táto kategória patrí medzi najzákernejšie. Pokiaľ je útok dobre zamaskovaný môže sa na stratu dát prísť až vo chvíli, keď sú potrebné čo niekedy môžu byť týždne, mesiace či dokonca roky. Veľké nebezpečenstvo predstavuje odchádzajúci zamestnanec. Niekto ukončí pracovný pomer spokojný s čistým štítom, iný zabuchne dvere a už túži mať so starým miestom svätý pokoj. A sú takí, ktorí sa nevedia vyrovnať s odchodom a majú pocit, že dáta ktoré vytvorili sú len ich. Preto neváhajú a zmažú ich alebo ich jednoducho ukradnú a poskytnú konkurencii.

4. Vírusová nákaza

Určite už má každý z Vás skúsenosť s rôznymi vírusmi, malewarom či spywarom alebo prinajmenšom vie čoho sú tieto programy schopné. Málokto však čakal taký prístup ako v prípade nových vírusov s názvom “CryptoLocker”, ktoré sa šíria cez webové stránky a emailmi a dostane Vás do pozície, že si môžete vybrať medzi zlým a ešte horším riešením. Buď zaplatíte

alebo prídete o všetky dáta na Vašom počítači. Vírus môže byť ukrytý v pošte od Vášho priateľa, náhodne otvorenom spame, ale aj na akejkoľvek webovej stránke.

5. Prírodné katastrofy

Nemusí to byť zrovna požiar alebo povodeň, ktoré zničia Vaše dáta. Už len taká búrka predstavuje nebezpečenstvo. Blesk počas búrky a následné predpätie v elektrických rozvodoch urobí svoje a Vaše dáta môžu byť nenávratne stratené.

Preto je nie potrebné, ale nutné dáta na počítačoch zálohovať. Táto záloha by mala byť nezávislá od toho, kto na počítači pracuje. Mala by sa diať automaticky, bez nutnosti zaťažovania zamestnanca či správcu siete. Len potom môžete byť kľudný, že Vaše dáta sú zabezpečené a obnoviteľné. Takúto automatickú zálohu dát dokáže realizovať náš systém **KERBER BackUp server**.

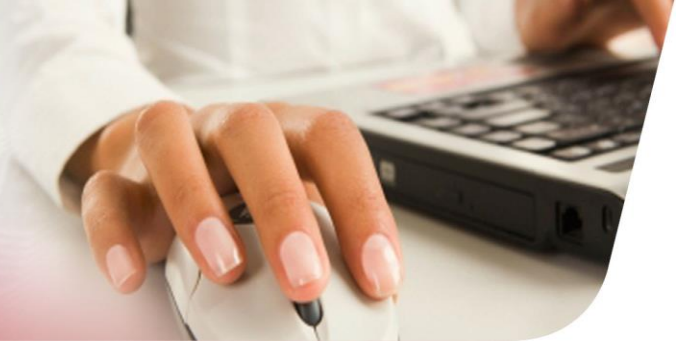
Cloudové služby a osobné údaje

V mesiaci jún Úrad na ochranu osobných údajov vydal viacero metodických usmernení a jedno z nich pod číslom 3/2016 sa týka cloudových služieb. Prinášame Vám zhrnutie z tohto usmernenia.

Cloudové služby v dnešnej dobe prežívajú svoj rozmach a využíva ich čoraz viac firiem. Treba si však uvedomiť aj určité riziká, ktoré musí zákazník cloudovej služby zobrať do úvahy. Jedná sa predovšetkým o riziko straty kontroly nad spracúvanými osobnými údajmi. Poskytnutím údajov do cloudu zákazníci cloudových služieb strácajú výlučnú kontrolu nad poskytnutými údajmi, ktoré sa dostávajú do dispozície poskytovateľa cloudovej služby. Uvedené riziko spočíva predovšetkým v tom, že poskytovateľ cloudovej služby pri prevádzkovaní tejto služby aplikuje vlastné mechanizmy, na ktoré má samotný zákazník len obmedzený dosah (napr. technické a personálne opatrenia, prístup iných strán k údajom a iné). Preto si treba dobre zvážiť výber poskytovateľa služby. Medzi cloudové služby patrí napríklad DCOM (dátové centrum miest a obcí) alebo archivácia školských dát v ASC agende.

Z hľadiska zákona o ochrane osobných údajov je potrebné presne identifikovať postavenie jednotlivých strán. Zákazník cloudovej služby vystupuje ako prevádzkovateľ, ktorý určuje konečný účel spracúvania a rozhoduje o outsourcingu tohto spracovania a delegovaní všetkých alebo časti spracovateľských činností na poskytovateľa cloudovej služby. V tomto kontexte je potrebné zdôrazniť, že je to práve prevádzkovateľ, ktorý nesie primárnu zodpovednosť za spracúvanie osobných údajov v súlade so zákonom o ochrane osobných údajov.

Ďalší subjekt v predmetnom vzťahu je poskytovateľ cloudovej služby, ktorý zastáva postavenie sprostredkovateľa, nakoľko je to subjekt, na ktorý prevádzkovateľ deleguje niektoré zo svojich úloh a povinností. Aj keď sa možno nezdá, že dochádza k spracovaniu osobných údajov, ale treba si uvedomiť, že definícia spracovania je vymedzená v zákone veľmi široko. Pod spracovaním sa rozumie vykonávanie operácie, alebo súboru operácií nad osobnými údajmi.



Rozsah tejto definície pri nakladaní s osobnými údajmi teda s určitosťou pokrýva celý rad spracovateľských operácií vykonávaných v samotnom cloude.

Zákazníka cloudovej služby považujeme za prevádzkovateľa. Poskytovateľa naopak za sprostredkovateľa. Preto je medzi nimi potrebné uzavrieť sprostredkovateľskú zmluvu, ktorá bude mať všetky náležitosti vyžadované zákonom o ochrane osobných údajov. Viac informácií o vzťahu prevádzkovateľ – sprostredkovateľ sa dozviete v článku uverejnenom na našom webe.

Nemenej dôležitou otázkou je aj to, kde sú fyzicky osobné údaje umiestnené. Pri poskytovaní cloudových služieb nie je neobvyklé, že sa dátové úložiská poskytovateľov cloudových služieb nachádzajú v iných štátoch, ako sú štáty, v ktorých pôsobia zákazníci týchto služieb. Podľa umiestnenia rozlišujeme nasledovné prenosy:

Európska únia – zákon o ochrane osobných údajov umožňuje voľný prenos osobných údajov medzi Slovenskou republikou a členskými krajinami únie.

Krajiny zaručujúce primeranú úroveň ochrany osobných údajov – zákon o ochrane osobných údajov spája s takýmto prenosom osobných údajov povinnosť zákazníka cloudovej služby ako prevádzkovateľa informovať dotknuté osoby o tomto prenose. Zoznam krajín s primeranou úrovňou ochrany osobných údajov nájdete na stránke Úradu na ochranu osobných údajov.

Krajiny nezaručujúce primeranú úroveň ochrany osobných údajov – pri prenose osobných údajov do takejto krajiny sa vyžaduje (buď) súhlas dotknutej osoby, alebo sa prenos môže realizovať na základe zmluvy, ktorá obsahuje štandardné zmluvné doložky.

Využívanie cloudových služieb prináša so sebou okrem výhod aj mnohé riziká. Potencionálni zákazníci by teda mali zvážiť využitie tejto služby predovšetkým s ohľadom na podmienky, ktoré dokážu poskytovatelia tejto služby vytvoriť. Výberom toho správneho poskytovateľa cloudovej služby však proces zabezpečenia ochrany osobných údajov nie je možné považovať za ukončený, nakoľko je nevyhnutné dôsledne zabezpečovať ochranu osobných údajov počas celej doby ich spracúvania.

Celé metodické usmernenie nájdete tu.

[VAŠE POTREBY] [NAŠE RIEŠENIA]

Kamerové systémy – neverejné priestory

Úrad na ochranu osobných údajov vydal nové usmernenie číslo 5/2016, ktoré sa týka monitorovania priestorov verejnosti neprístupných. Prinášame Vám zhrnutie z tohto usmernenia.

Čo je to priestor verejne neprístupný? Je to priestor:

- do ktorého verejnosť nemôže voľne vstupovať,
- v ktorom sa verejnosť nemôže voľne/bez sprievodu zdržiavať, pohybovať, ani vo vymedzenom čase
- súčasne, nie je tento priestor označený ako priestor prístupný verejnosti podľa osobitného zákona

Monitorovanie obydlia

Za obydlie možno považovať súkromný majetok, ktorý je verejnosti neprístupný (za verejnosť sa nepovažujú návštevy a poštový doručovateľ) a nie je využívaný na podnikateľské účely. Pokiaľ sa monitorujú takéto priestory, tak sa naň nevzťahujú ustanovenia zákona na ochranu osobných údajov, nakoľko sa monitorovanie vykonáva pre vlastnú potrebu fyzickej osoby v rámci jej osobných, alebo domácich činností. V tomto prípade nevyplývajú žiadne povinnosti voči Úradu na ochranu osobných údajov.

Monitorovanie podnikateľských priestorov

Ak je priestor využívaný na podnikanie, a do tohto priestoru môžu voľne vstupovať, alebo sa v ňom voľne zdržiavať vo vymedzenom čase, alebo bez obmedzenia času napríklad len zamestnanci prevádzkovateľa, zmluvní partneri, poštár, či návštevy (t.j. nejde o verejnosť a súčasne zamestnanci v tomto priestore spravidla nevykonávajú svoju pracovnú činnosť pravidelne/bežne). V tomto prípade platia ustanovenia zákona 122/2013 Z. z o ochrane osobných údajov. Monitorovanie prebieha na základe §10 ods. 3 písm. g), t.j. ochrana majetku, finančných alebo iných záujmov, alebo zaistenie bezpečnosti. V tomto prípade je potrebné urobiť oznámenie na Úrade na ochranu osobných údajov, ten potom posúdi, či je potrebná osobitná registrácia

Monitorovanie za účelom kontroly zamestnancov

Zamestnancov je možné kontrolovať podľa Zákonníka práce. Zamestnávateľ je povinný túto kontrolu prerokovať so zástupcami zamestnancov a je povinný informovať zamestnancov o jej spôsobe a dĺžke trvania.

Monitorovanie školských zariadení

Školy vo všeobecnosti považujeme za budovy občianskej vybavenosti, do ktorých sa dá voľne vstupovať. Avšak, aj v týchto budovách sú vyhradené priestory, do ktorých má verejnosť vstup zakázaný, respektíve, do ktorých môže vstupovať a pohybovať sa v nich na základe povolenia alebo iba v sprievode personálu/určenej osoby. V školách za takéto priestory možno všeobecne považovať triedy. Pokiaľ sa v triede, alebo v učebni nachádza špeciálne vybavenie, tak je možné použiť §10 ods. 3 písm. g). V tomto prípade je ale potrebné oznámenie na Úrade na ochranu osobných údajov. V prípade tried s bežným vyučovaním nie je možné tento paragraf využiť a je potrebné mať súhlas žiaka alebo jeho zákonného zástupcu. V prípade, ak sa v monitorovanom priestore po ukončení starostlivosti o dieťa pohybujú ďalšie osoby (napríklad údržba, upratovacia služba), nie je možné tieto osoby na základe vyššie uvedeného súhlasu monitorovať, t.j. po skončení vyučovania je potrebné kamery vypnúť.

Celé usmernenie nájdete tu.

Zákon 211/2000 Z. z. a osobné údaje

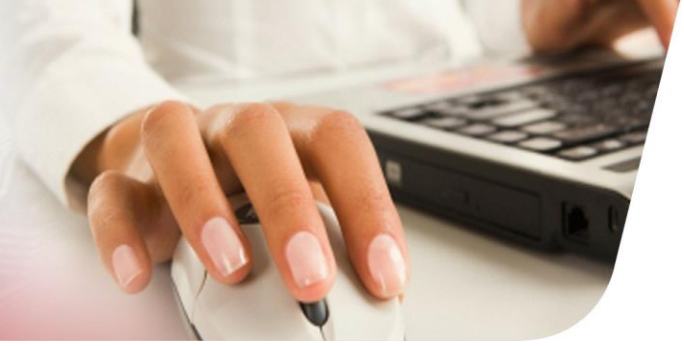
Od roku 2000 platí zákon o slobodnom prístupe k informáciám. Podľa tohto zákona sú mestá, obce, a nimi zriadené organizácie (napr. základné školy) povinné zverejňovať informácie týkajúce sa hlavne ich hospodárenia. Jedná sa o objednávky, zmluvy a faktúry. Často sú súčasťou týchto dokumentov aj osobné údaje. Preto je potrebné zverejňovať tieto dokumenty tak, aby nedošlo k narušeniu práv dotknutých osôb a zverejnenie nebolo v rozpore so zákonom 122/2013 Z. z. o ochrane osobných údajov. Aké osobné údaje je možné v súlade s tými dvomi legislatívnymi normami zverejniť?

Podľa zákona na ochranu osobných údajov možno osobné údaje zverejniť len s predchádzajúcim súhlasom dotknutej osoby, pokiaľ nejaký osobitný zákon neustanovuje inak. Osobitným zákonom v tomto prípade je zákon 211/2000 Z. z. o slobodnom prístupe k informáciám. Podľa tohto zákona je povinné zverejňovať:

Prevod nehnuteľností (§5 ods. 6) vo vlastníctve obce alebo mesta do vlastníctva inej osoby. V tomto prípade platí povinnosť zverejniť dátum prevodu alebo prechodu vlastníctva a právny titul, ako aj informácie o osobných údajoch a iných identifikačných údajoch osôb, ktoré nadobudli tento majetok do vlastníctva, a to v rozsahu:

a) meno a priezvisko, názov alebo obchodné meno,
b) adresa pobytu alebo sídlo,
c) identifikačné číslo, ak ide o právnickú osobu alebo fyzickú osobu – podnikateľa.

Povinne zverejňovaná zmluva (§5a) je písomná zmluva, ktorú uzaviera povinná osoba (obec alebo mesto). Pri zverejňovaní zmluvy sa uvádza identifikácia účastníkov zmluvy. Z osobných údajov sa zverejňuje (§5a od 13) titul, meno, priezvisko, adresa trvalého pobytu a označenie



nehnuteľnosti. Ostané osobné údaje je potrebné anonymizovať. Je to hlavne rodné číslo a podpis na zmluve.

Pri **objednávkach alebo faktúrach** sa zverejňujú nasledujúce osobné údaje:

a) identifikačné údaje dodávateľa objednaného/fakturovaného plnenia
   - meno a priezvisko fyzickej osoby, obchodné meno fyzickej osoby-podnikateľa alebo obchodné meno/názov právnickej osoby,
   - adresu trvalého pobytu fyzickej osoby, miesto podnikania fyzickej osoby-podnikateľa alebo sídlo právnickej osoby,
   - identifikačné číslo, ak ho má dodávateľ objednaného plnenia pridelené,

b) údaje o fyzickej osobe, ktorá objednávku/faktúru podpísala:
   - meno a priezvisko fyzickej osoby,
   - funkciu fyzickej osoby, ak takáto funkcia existuje.

Ostatné osobné údaje je opäť potrebné anonymizovať. Ide hlavne o podpis. Anonymizovanie musí byť urobené takým spôsobom, aby bolo nevratné, t.j. nedalo sa opäť dostať k osobným údajom. Je nepostačujúce zmeniť farbu textu na bielu, alebo farbu pozadia na čiernu. Aj napriek zmene farby tam pôvodný text ostáva a jeho zverejnením sa môže dostať do vyhľadávača Google. Najlepšie je príslušný text úplne vymazať a až potom umiestniť na webovú stránku, alebo do centrálneho registra zmlúv.

Zverejňovanie osobných údajov (§9 ods. 3) verejných funkcionárov, poslancov obecného a mestského zastupiteľstva, a vedúcich zamestnancov obce alebo mesta je možné v rozsahu:

a) titul, meno, priezvisko
b) funkcia a deň ustanovenia alebo vymenovania do funkcie,
c) pracovné zaradenie a deň začiatku výkonu pracovnej činnosti,
d) miesto výkonu funkcie alebo pracovnej činnosti, a orgán, v ktorom túto funkciu alebo činnosť vykonáva,
e) mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie, alebo za výkon pracovnej činnosti, ak sú uhrádzané zo štátneho rozpočtu, alebo z iného verejného rozpočtu.

Pokiaľ by niekto požadoval osobné údaje nad rámec tohto rozsahu, tak je potrebný súhlas dotknutej osoby, napr. aj primátora alebo starostu. V rámci zákona 211/2000 Z. z. rieši ochranu osobných údajov §9, ktorý v odseku 1) hovorí:

Informácie, ktoré sa dotýkajú osobnosti a súkromia fyzickej osoby, písomnosti osobnej povahy, podobizne, obrazové snímky, obrazové a zvukové záznamy týkajúce sa fyzickej osoby alebo jej prejavov osobnej povahy povinná osoba sprístupní len vtedy, ak to ustanovuje osobitný zákon, alebo s predchádzajúcim písomným súhlasom dotknutej osoby.

[VAŠE POTREBY] [NAŠE RIEŠENIA]

Pozvánka na SOMI Roadshow

Zabezpečte si dáta bezpečne

Ako jedna z uznávaných spoločností v oblasti ochrany dát a zabezpečenia dátovej komunikácie, si Vás dovoľujeme pozvať na

SOMI RoadShow

kde Vás oboznámime s úskaliami, ktoré Vás pri dátovej komunikácií môžu postretnúť a tiež s riešeniami, ako týmto úskaliam predchádzať.

Pozývame Vás na našu **bezplatnú prezentáciu**, kde Vám ukážeme ako majú problematiku bezpečnosti v dátovej komunikácii vyriešenú naši zákazníci a ako to reálne funguje. Možno budete prekvapení, že jednoduché a cenovo prijateľné riešenia v súčinnosti so správne nastavenými procesmi dokážu zabezpečiť Vaše dáta **naozaj bezpečne**.

PREDSTAVÍME VÁM:

Bezpečnostný projekt na ochranu osobných údajov – legislatívna nutnosť a reálny výsledok bezpečnostného auditu z pohľadu organizácie.

Kerber 3.0 – produkt na komplexné riešenie bezpečnej a manažovateľnej správy komunikácie z a do internetu.

KBS – Kerber Backup Server – komplexné a automatické riešenie pre obnovu a archiváciu dôležitých firemných dát, riešenie problematiky ransomwarov (vydieračské vírusy).

Moderná WiFi infraštruktúra – zabezpečený a manažovateľný prístup na internet pomocou moderných WiFi zariadení.

SOMI Roadshow uskutočníme postupne v šiestich mestách Slovenska:

Topoľčany 11.10.2016, Bubbles club, Hollého 6 - registrácia
Prešov 12.10.2016, Coop Jednota Prešov, Konštantínova 3 - registrácia
Nitra 13.10.2016, Agroinštitút Nitra, Akademická 4 - registrácia
Poprad 25.10.2016, MsÚ Poprad, Nábrežie J. Pavla II. 2802/3 - registrácia
Michalovce 26.10.2016, Hotel Družba, J. Hollého 698/1 - registrácia
Košice 27.10.2016, SBD II Košice, Bardejovská 3 - registrácia

Tešíme sa na Vašu účasť.

SOMI Systems a.s., Lazovná 69, 974 01 Banská Bystrica

Tel: 048/414 67 59, web: www.somi.sk