# Egovernment

elektronizace veřejné správy


www.egovernment.cz

č. 2/2014

**Kyberbezpečnost – víc než zákon?**

Kybernetické hrozby se stávají stále běžnější součástí našeho, vlastně i nekybernetického prostoru. Netýkají se jen počítačů samotných. V současné době je stále větší množství zařízení i běžných domácností připojeno na internet. Je jedno, zda se jedná o televize, lednice, herní konzole, nebo bezpečnostní kamery. Internet tak vstupuje do našeho života i do našich domácností a neustálé připojení on-line považujeme již za samozřejmost.

Zvyšuje se tím naše pohodlí, ale adekvátně tomu se zvyšuje naléhavost toho, jak bychom se měli věnovat zabezpečení těchto kontaktů. Pokud jde o samotné hrozby, které v kyberprostoru na každého z nás čekají, neexistují zde žádné hranice. Pokud máme pocit, že žijeme v malé zemi, která je pro útočníky nezajímavá, je to život v blahé nevědomosti. Útoky co do metod i množství jsou zde stejné jako onde, jen u nás zatím není povinnost zveřejňovat o nich informace. Zrovna tohle by mohl právě čerstvě přijatý zákon o kyberbezpečnosti změnit. Co všechno ostatního může nebo nemůže jeden zákon s poutavým názvem? Snažili jsme se najít odpovědi uspořádáním semináře Kyberbezpečnost – víc než zákon.

Ing. Michal Jirkovský
šéfredaktor

# Obsah


| | | |
|---|---|---|
| **Redakce** | ÚVODNÍ SLOVO | 2 |
| | OBSAH, TIRÁŽ | 3 |
| **Kyberbezpečnost** | PŘICHÁZÍ ZÁKON. A CO ŘEŠÍ? | 4 – 5 |
| | BEZPEČNOST – DŮLEŽITÉ TÉMA | 6 |
| | KYBERBEZPEČNOST – TÉMA PRO VŠECHNY | 8 – 9 |
| | NBÚ – GARANT KYBERBEZPEČNOSTI | 10 – 11 |
| | KROKY NBÚ | 12 – 14 |
| | CESTA ZÁKONA SNĚMOVNOU | 16 – 17 |
| | ZÁKON KYBERBEZPEČNOST NEVYŘEŠÍ | 18 – 19 |
| | KYBERBEZPEČNOST = ARCHITEKTONICKÁ BEZPEČNOST | 20 – 22 |
| | KYBERBEZPEČNOST V PRAXI | 24 – 26 |
| | BOJ S BEZPEČNOSTNÍMI HROZBAMI JE NEPŘETRŽITÝ PROCES | 28 – 29 |
| | BEZPEČNOSTNÍ A PROVOZNÍ STANDARDY IS | 30 – 31 |
| | INTEL: ŘEŠENÍ PRO VIRTUALIZACI A CLOUD | 32 – 33 |
| **Projekty** | PODPORA EGOVERNMENTU V KRAJÍCH | 34 – 35 |
| | KONFERENCE ISSS 2014 | 36 – 38 |
| | ROZVOJ SLUŽEB EGOVERNMENTU V ÚSTECKÉM KRAJI | 40 – 41 |



**V rámci České a Slovenské republiky vydává:**

info◆com s.r.o, Krokova 2, 128 00 Praha 2
www.infocom.cz
IČO: 26426331
zapsána u Městského soudu v Praze
pod č. C – 81357
**tel.:** 241 412 518
**e-mail:** egovernment@egovernment.cz
**http:** www.egovernment.cz
ISSN 1801-9420

**Šéfredaktor:** Ing. Michal Jirkovský
**Korektorka:** PhDr. Helena Veverková
**Asistentka:** Bc. Anna Hosová

**Grafika:** PROPAGANDA, Kafkova 10, Praha 6
**Tiskárna:** A. R. GARAMOND s.r.o., Belnická 758, 252 42 Jesenice
**Registrační číslo:** MK ČR E 11364




## Registrace:

Magazín Egovernment je distribuován, na základě registrace, pracovníkům veřejné správy v České republice a na Slovensku **ZDARMA**. Ostatní čtenáři, kteří nejsou pracovníky veřejné správy zaplatí cenu **100 Kč (4 EUR)** bez DPH**/výtisk, tj. 400 Kč (16 EUR)** bez DPH **ročně**.
S registrací získáte, kromě pravidelného zasílání magazínu, i informace o dalších projektech, které realizuje společnost **info◆com** s.r.o.

# Přichází zákon. A co řeší?

***Poslanecká sněmovna Parlamentu ČR schválila, byť s drobnými doplňujícími návrhy, zákon o kyberbezpečnosti. Stalo se tak v polovině června a mohlo by se zdát, že jsme jeho přijetím udělali logický krok k zajištění našeho bezpečí v době, kdy počítače, respektive propojené počítače, patří k našemu životu asi tak jako sklenka vody, ranní káva, nebo houska s máslem. Ale je tomu tak?***

## KOHO SE TÝKÁ?

Stejně jako sklenka vody není úplnou samozřejmostí pro všechny obyvatele této planety, ani život s počítači není běžný a nevyhnutelný pro všechny obyvatele této země. Ještě dnes jsou lidé, kteří dokáží žít bez bankovní karty, bez internetu i bez mobilu. A jsou někteří, asi jich není mnoho, kteří i na území České republiky vegetují bez dodávky elektrické energie, bez vodovodu a plynovodu. S přihlédnutím k predikcím katastrofických sci-fi filmů a knih bychom mohli tvrdit, že právě oni jsou zárukou přežití lidstva na této planetě. Je ale bezpochyby zřejmé, že těchto obyvatel se zmiňovaný zákon o kyberbezpečnosti netýká, alespoň ne přímo, protože jim je úplně jedno, co se v kyberprostoru děje.

Přímo se tento zákon netýká ani nás ostatních, kteří svůj život už rozdělili mezi skutečný a elektronický svět. Rozhodně se nás netýká přímo. Zákon o kyberbezpečnosti se totiž nijak nezabývá tím, jak ke kyberbezpečnosti přistupuji já osobně na svém vlastním, firemním či jiném počítači. Dokonce zřejmě, dle vyjádření, která zazněla na semináři v Poslanecké sněmovně, není tento zákon namířen ani na města a kraje.

## KRITICKÁ JE KRITICKÁ INFRASTRUKTURA

Zákon je vlastně namířen především na tzv. kritickou infrastrukturu, tedy něco, co spravuje veřejná správa někde na nejvyšší úrovni. Sice asi tušíme, že kritická infrastruktura, bez jejíhož fungování se stát může dostat do značné krize, je patrně něco jako plynovod, ropovod, elektrárny, páteřní datové propojení atp., ale asi úplně přesně neodříkáme, co vše je v ní obsaženo. Kupodivu se to nedočteme ani v samotném zákoně. Kritickou infrastrukturu bude stanovovat teprve jeho tzv. prováděcí vyhláška. Je otázkou, zda to není kritický moment celého zákona.

## ZÁKON NEŘEŠÍ KYBERBEZPEČNOST

Na semináři v Poslanecké sněmovně také zaznělo, že tento zákon vlastně nemůže problém kyberbezpečnosti vyřešit. KyberNEbezpečnost je tak napřed, že ji nemůžeme řešit zákonem. Jestli existuje skutečně nějaká efektivně fungující přeshraniční, respektive mezinárodní spolupráce, pak je to oblast kyberútoků. Všichni, kdož s kyberútoky chtějí jakkoliv bojovat, jsou vždy o krok pozadu a nemohou se zdržovat tvorbou zákonů.

## JAK NA TO?

Vzorem, o kterém se v souvislosti s elektronizací státu často hovoří, je Estonsko, jež začalo eGovernment budovat již krátce po obnovení své nezávislosti v roce 1991, a to jako soustavu zákonů, na kterou byla následně nabalována soustava rozvíjejících se technologických možností. Dnes v Estonsku podává elektronickou cestou daňové přiznání 95 % firem a obyvatel, založit firmu je zde pomocí

čipového občanského průkazu možné trojím kliknutím myši a od října se bude moci kterýkoliv obyvatel planety stát elektronickým obyvatelem Estonska.
Na druhou stranu se Estonsko už v roce 2007 stalo cílem prvního kybernetického útoku. A dnes je zde umístěno sídlo NATO pro kybernetickou obranu. A tak asi není úplně plané tlachání, když Aet Rahe, estonská „ministryně" IT, shodou okolností v Praze říká, že stojíme na prahu informační války (konference Otevřená data březen 2014).

## ČESKÁ CESTA

Pokud jde o elektronizaci, plácáme se pravda po zádech, že propojení eGona, tedy KIVS, datových schránek, Czech POINTu a základních registrů je tak úžasné, že jsme na špici. Ale na rozdíl od Estonska, to vypadá, že u nás začneme nejprve využívat technologie a pak hledáme, jak jim upravit potřebné zákony. A ne vždy se to daří. Datové schránky jsou stále uzavřeným okruhem jen pro komunikaci s veřejnou správou a o sdílení dat ze základních registrů i jiným subjektům než veřejnoprávním (operátorům, dodavatelům energie atp.) tak, aby nám to skutečně usnadnilo život, si zatím můžeme nechat jen zdát. Založení firmy rozhodně neměříme na počet klinutí myší a upřímně i autor tohoto článku, po vlastních zkušenostech, podává daňové přiznání raději v papírové podobě. V České republice nejsou pro elektronizaci ani tak technické, jako především legislativní překážky.

## POCIT JISTOTY A BEZPEČÍ?

A teď najednou, místo toho, abychom upravovali stávající zákony, aby vyhovovaly tomu, co by bylo možné, kdyby nám to umožňovaly zákony, vymýšlíme zákon, který stejně nemůže postihnout to, co nese ve svém názvu. V tomto směru působí dění okolo zákona o kyberbezpečnosti zvláštně. Vybudujeme si nový vládní úřad pro bezpečnost (CERT), přičemž zde již dlouhodobě národní úřad tohoto typu funguje (pod CZ.NIC), vedle samotného zákona sestavuje NBÚ výkladový slovník kybervýrazů, který čítá údajně 600 výrazů a je dvojjazyčný, ale zároveň připouští, že do národního bezpečnostní centra přijímá čerstvé absolventy s rizikem jejich útěku do komerční sféry po té, co získají potřebné zkušenosti.
V případě „bežného" ohrožení se hlavním „ochráncem" státu obvykle stává vláda, respektive premiér. Zákon o kyberbezpečnosti premiérově kybernetické zdatnosti nedůvěřuje, když hlavní a jedinou rozhodující hlavou v případě kyberohrožení státu stanovuje ředitele NBÚ. To začíná být zajímavé v momentě tzv. stavu kybernetického nebezpečí. V takovém momentu totiž ředitel NBÚ může závazně vydávat pokyny například poskytovatelům elektronických komunikací, a tedy zásadně ovlivňovat naši připojenost a propojenost, a NBÚ ví, že bez spojení není velení.

## K ČEMU?

Zákon o kyberbezpečnosti tedy nenařizuje nic samotným občanům, dokonce ani nezavádí nějaké povinnosti městům a krajům. Dokonce na rozdíl od některých zemí s „vlastním" přístupem k věci, nezavádí možnost cenzury a rušení sociálních sítí.
K čemu nám tedy je? Je jen něčím, co jsme byli zvyklí, možná trochu hanlivě zahrnovat pod hlavičku CO (civilní ochrana), nebo je to skutečně důležitý bezpečnostní prvek, který zapadá do bezpečnostní soustavy státu?
Nejen o samotném zákonu, ale především o otázkách kyberbezpečnosti hovořili významní řečníci na semináři Kyberbezpečnost – víc než zákon, který jsme uspořádali v polovině května v Poslanecké sněmovně PČR. K čemu se účastníci v této souvislosti dobrali, můžete posoudit na následujících stranách.

Michal Jirkovský

# Bezpečnost – důležité téma

***Záštitu semináři Kyberbezpečnost, víc než zákon poskytla 1. místopředsedkyně Poslanecké sněmovny Parlamentu ČR paní Jaroslava Jermanová i proto, jak ve svém úvodním slovu uvedla, že považuje za velice přínosné, že se debata na toto téma odehrává právě v Poslanecké sněmovně, tedy místě, kde zákonné normy vznikají.***

Dále připomněla, že žijeme v době, kterou je bezpochyby možné nazývat digitální či kybernetickou. Veškeré důležité procesy se dnes realizují s pomocí či prostřednictvím informačních technologií. Veřejná správa podle jejích slov v tomto smyslu není výjimkou. I když s určitým zpožděním za komerční sférou, postupně i ona se digitalizuje se všemi pozitivními, ale i negativními efekty tohoto procesu. Dnes již podle Jaroslavy Jermanové nemluvíme o tom, že eGovernment, tedy elektronická veřejná správa, je součástí výkonu veřejné správy, ale je zřejmé, že eGovernment je formou výkonu veřejné správy. Bez nadsázky se tedy dá říci, že bez ICT by dnes veřejná správa nefungovala, doslova by se zastavila. A právě proto je, jak Jaroslava Jermanová upozornila, důležité vnímat hrozby, které takový proces sebou přináší. Na jednu stranu je velice příjemné využívat výhod, které poskytuje sdílení dat, zpracování žádostí a podání v reálném čase, možnosti přístupu do systému odkudkoliv a z libovolného zařízení. Jedná se bezpochyby o vyšší uživatelský komfort, pracovní pohodlí i efektivitu. Zároveň se ale zvyšují nároky na zabezpečení dat, která veřejná správa vlastní, někdy výhradně v elektronické podobě, zvyšují se nároky na nutnost identifikace uživatelů, kteří k datům přistupují, či klientů veřejné správy, kteří poskytují svolení s těmito daty nakládat. A samozřejmě se zvyšuje riziko napadení celého systému.

*Ing. Jaroslava Jermanová*

Jaroslava Jermanová zdůraznila, že v rámci semináře se nebude diskutovat pouze o samotném návrhu zákona o kyberbezpečnosti. Předmětem semináře totiž nebylo jeho hodnocení. Diskuze směřovala spíše k tomu, jaké jsou skutečnosti, které pro veřejnou správu z tohoto zákona, po jeho vstupu v účinnost, budou závazné. Podle Jaroslavy Jermanové je proto důležité bavit se o tom, zda jsou dostačující, či zda je vhodné, aby jednotlivé úřady a instituce uvažovaly a jednaly v oblasti kyberbezpečnosti nad rámec tohoto návrhu. Dnešní svět se díky ICT stává pohodlnější, rychlejší a dostupnější. Zároveň ale přináší nové hrozby. Místopředsedkyně sněmovny v této souvislosti připomenula, že informace o kyberútocích, které přerůstají ve skutečné organizované války v kyberprostoru, nejsou dnes již ničím neobvyklým. Hrozba „vypnutí" státu ve smyslu jeho skutečného znefukčnění bez použití fyzického útoku není nic nereálného. Nejedná se ovšem pouze o možné ekonomické škody, ale díky „zasíťování" skutečně o dlouhodobé vyřazení podstatných složek státu – od bezpečnosti přes řídicí složky až po zdravotnictví či energetiku. I proto, jak řekla, je velice ráda, že pozvání k aktivní účasti na tomto semináři přijalo opravdu široké spektrum osobností od zástupců předkladatele zákona, přes zákonadárce, reprezentanty eGovernmentu až po zástupce IT firem, které se na jeho technické realizaci podílejí.

Jaroslava Jermanová zdůraznila, že kyberbezpečnost se stává nedílnou součástí našeho uvažování, nutností, bez které nelze využívat výhod a pohodlí elektronizace. ■


Bisnode

# PROFESIONÁLNÍ INFORMACE O FIRMÁCH

**DATA A INFORMACE MĚNÍME V ODPOVĚDI, KTERÉ FIRMÁM UMOŽŇUJÍ PŘIJÍMAT SPRÁVNÁ ROZHODNUTÍ.**

# Kyberbezpečnost – téma pro všechny

***Zahajovací slovo na semináři měl i další místopředseda Poslanecké sněmovny PČR Jan Bartošek. Podle vlastních slov přemýšlel, jak ozvláštnit dnešní jednání a přiznal se, že uvažoval o tom, zda by nebylo vhodné zkusit nabourat síť Poslanecké sněmovny. Tím chtěl ukázat, jak jsou, nebo nejsou poslanci chráněni od kyberútoků. Chtěl by tím upozornit na skutečnost, že bavíme-li se o nebezpečích, která na nás v kyberprostoru čekají, nejsou to žádné imaginární záležitosti, ale zcela reálné hrozby, které se týkají skutečně každého z nás.***

Jak dále Jan Bartošek uvedl, on sám nepatří mezi IT odborníky. Sám sebe považuje za běžného uživatele, ale sleduje dění kolem sebe a samozřejmě vnímá, co se děje. Jak řekl, reálný obraz toho, co je v kyberprostoru možné, se ukázal docela nedávno a to při řešení krize na Krymu. V této souvislosti si Jan Bartošek myslí, že otázka kyberbezpečnosti je skutečně národní otázkou. Ale není nutné uvažovat hned ve válečných souvislostech. Byly tu rovněž menší útoky, například na naše operátory či bankovní domy. Podle Jana Bartoška je otázkou, kolik toho skutečně o těchto útocích víme, a pokud ne mnoho, pak do jaké míry se jedná o záměrně tabuizované téma a do jaké míry jsou banky skutečně tak profesionální v ochraně svých dat a klientů.

*Ing. Jan Bartošek*

Jako další příklad problematiky nebezpečí kyberprostoru uvedl čin Edwarda Snowdena, který zveřejnil údaje o masívním sledování telefonů a elektronické komunikace. Tím nám ukázal, že naše soukromí je v současné době pojem značně relativní. Jan Bartošek připomněl dnes již legendární film Síť se Sandrou Bullock, který pojednává o odcizení identity. Jak uvedl, je z jeho pohledu velice nadčasový a v současné době možná velice aktuální. Je podstatné, že naše závislost na sítích a internetu vzrůstá každým rokem. Možná by to nestálo za úvahu, pokud by se jednalo o jakýsi módní trend, který postupně opouštíme. Ale ono tomu je zcela naopak, protože každý rok každá instituce a každý občan této republiky zvyšuje svoji závislost na internetu a není tím míněna jejich potřeba „brouzdat" tímto prostorem, ale skutečné využívání připojení do sítě. Jan Bartošek dále uvedl, že jsme se dokonce vzdali tzv. zákonů robotiky, když dnešní moderní roboty – bezpilotní letadla – navádíme k útokům na lidstvo.

Aby nehovořil o zbrojní oblasti, uvedl, že jistá doručovatelská firma testuje tzv. bezpilotní drony, které by měly doručovat domácnostem balíčky. Upozornil, že podle

jeho mínění je to směr, který nepovažuje za dobrý, neboť by mohlo dojít velice snadno ke zneužití pro teroristické útoky a podobné aktivity.

Důvody, proč o takových věcech mluví, jsou podle Jana Bartoška otázky naší bezpečnosti. Nejde totiž jen o naše domácnosti, ale rovněž o zabezpečení energetických zdrojů, zdravotních systémů a dalších záležitostí tzv. kritické infrastruktury, která je podstatná pro chod této země. Občas uvažuje nad tím, jak dalece jsme pohlceni tím, co všechno dokážeme vyrobit, vymyslet a navrhnout, že při tom zapomínáme na samotnou bezpečnost. Připadá mu, že je to podobný model, jako když byla jedna docela nedávná generace zcela fascinována a pohlcena Facebookem, aby následně zjistila, jak není úplně příjemné vystavovat do kyberprostoru veškeré soukromé informace.

Pokud jde o klíčové systémy státu, ani tady není Jan Bartošek přílišným optimistou. Jak řekl, je to i proto, že bylo zjištěno, že jedno z ministerstev mělo více než 20 % počítačů koncových uživatelů infikováno škodlivým kódem. Podle Jana Bartoška je na tom zajímavé a možná znepokojující, že se tento fakt ministerstvo nedozvědělo od svých IT pracovníků, ale od poskytovatele svého internetového připojení. V roce 2011 jsme zase mohli být svědky toho, jak citlivá data občanů této země, kteří byli součástí systémů MPSV, byla volně přístupná z internetu.

To jsou podle Jana Bartoška excesy, které by se neměly stávat, protože základní a primární role státu je zajistit bezpečí obyvatel a v dnešní době i bezpečí jejich dat. Otázkou podle Jana Bartoška zůstává, jak moc se tyto světy, myšleno ten skutečný reálný svět a ten v kyberprostoru, doplňují či ohrožují, kde přesně selhává člověk a kde technika. I proto místopředseda Sněmovny vítá pořádání semináře s názvem Kyberbezpečnost, víc než zákon. ■

# NBÚ – garant kyberbezpečnosti

***Ředitel NBÚ v návaznosti na úvodní slova připomněl, že nabourání sítě znamená znemožnění její dostupnosti, nebo narušení její integrity, tedy pozměnění dat, případně může dojít k narušení její důvěrnosti. To jsou, jak uvedl Dušan Navrátil, základní tři typy hrozeb v prostředí internetu a základní důvody, proč řešit bezpečnost v tomto prostoru.***

Ve svém vystoupení se věnoval především tomu, jak NBÚ postupovalo v záležitostech zákona o kyberbezpečnosti. Jak řekl, v době, kdy se začínal Národní bezpečnostní úřad věnovat problematice zákona o kyberbezpečnosti, byla řada těchto hrozeb spíše teoretická. Dnes už je jasné, že tento problém skutečně existuje a je součástí i našeho života. Jak se prohlubuje elektronizace celé společnosti, tak internet a sítě jako takové jsou určitou nervovou soustavou celé společnosti a státu. Podle mínění Dušana Navrátila je z pohledu státu zásadní, že internet je totálně v soukromých rukou, přitom na něm začíná záviset kritická infrastruktura státu. Původně, jak připomněl, byla kybernetická bezpečnost zařazena pod Ministerstvem informatiky. S jeho zrušením přešla a nepřešla na MV ČR. Tuto otázku bylo nutno, dle slov Dušana Navrátila, diskutovat s tehdejším ministrem vnitra Martinem Pecinou v rámci Bezpečnostní rady státu. Nicméně byla v této době přijata první kybernetická bezpečnostní strategie ČR. V červnu 2011 došlo k dohodě s premiérem, ministrem financí a ministrem vnitra na tom, že garance za kybernetickou bezpečnost přejde pod NBÚ. V této souvislosti bylo přijato usnesení vlády, jehož základním bodem byl zákon o kybernetické bezpečnosti. Zákon, jak Dušan Navrátil uvedl, by mohl být přijat i dříve, ale s ohledem na konání mimořádných voleb se tak děje až nyní.

*Ing. Dušan Navrátil*

Jak ale uvedl, kvituje, že veškeré politické reprezentace, které se během doby příprav vystřídaly, podporovaly tuto problematiku.

Vedle samotného zákona bylo, dle slov Dušana Navrátila, dalším úkolem vybudování Národního centra kybernetické bezpečnosti. To by mělo být plně funkční do konce roku 2015. Už v polovině května byla v Brně slavnostně otevřena budova tohoto centra. Dle Dušana Navrátila v něm v současné době pracuje 22 lidí a příští rok by mělo být dosaženo konečného počtu 34 osob. Personální otázka je podle jeho slov určitým problémem, neboť jsou přijímáni především absolventi, které je nutné vychovat, bohužel s určitým rizikem, že následně odejdou do soukromého sektoru.

Další úkol, který Dušan Navrátil zmínil, nebyl součástí uvedeného vládního usnesení, ale je, podle jeho mínění, nesmírně důležitý. Jedná se o mezinárodní spolupráci. Jak řekl, internet je globální záležitost a bez mezinárodní spolupráce není možné zajišťovat kybernetickou bezpečnost. I proto tým NBÚ postupně objel v Evropě všechny státy, které v této oblasti zaujímají významnou pozici. NBÚ navázal rovněž kontakty mimo Evropu, např. s USA, Koreou a Izraelem. Podle Dušana Navrátila tuto spolupráci dokládá i skutečnost, že při otevírání Národního centra kybernetické bezpečnosti v Brně, byla přítomna řada významných zahraničních hostů. Řada z nich se rovněž účastnila následné konference. NBÚ spolupracuje i s NATO, které je v oblasti kyberbezpečnosti velmi aktivní. NBÚ má svého pracovníka v NATO Cooperative Cyber Defence Centre of Excellence v Estonsku.

Evropská unie sice, podle slov Dušana Navrátila, začala činit kroky v oblasti kyberbezpečnosti, ale její aktivita je o něco těžkopádnější. Minulý rok v únoru navrhla Evropská komise směrnici Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací o Unii, která je v současné době předmětem diskuzí jak v Radě Evropy, tak v Evropském parlamentu. Bohužel při projednávání došlo ke zdržení. Podle původní představy měl být tento materiál dokončen ještě za řeckého předsednictví. To se nestalo a v tuto chvíli není Dušan Navrátil schopen odhadnout, kdy vejde směrnice v platnost. Co je podle jeho slov pozitivní, je to, že prvotní filozofie této směrnice je velice blízká našemu návrhu zákona.

Hrozby v oblasti elektronické bezpečnosti v době, kdy se NBÚ začalo této problematice podrobněji věnovat, sice existovaly, ale rizika jsme mohli vnímat spíše teoreticky. Bohužel podle Dušana Navrátila za těch 2,5 let došlo k tomu, že se bezpečnostní rizika stávají realitou. Jak uvedl, jsou zde zkušenosti, že například státy, na které byla uvalena nějaká sankce, vesměs odpověděly kybernetickými útoky. Vzhledem k mezinárodnímu vývoji lze očekávat, že se takovéto kybernetické útoky, jako určitá forma odvety, budou objevovat stále častěji.

Na závěr ředitel NBÚ Dušan Navrátil uvedl, že Národní centrum kybernetické bezpečnosti bylo vybudováno během zhruba dvouapůlletého období. Zákon o kybernetické bezpečnosti jde nyní do třetího čtení v Poslanecké sněmovně, jsme tedy na konci jakéhosi začátku. Ale je nutné zdůraznit, že cesta ke kybernetické bezpečnosti bude velice dlouhá, respektive nebude nikdy vidět její konec. Stále se budou objevovat nová rizika, kterým se budeme muset věnovat. Podle Dušana Navrátila je důležité, že jsme začali a že ČR v tomto směru zaujímá důstojné postavení. ■

# Kroky NBÚ

***Na ředitele NBÚ navazoval svým vystoupením jeho náměstek pan Jaroslav Šmíd. V prezentaci se věnoval historii internetu, jeho vlivu na naše národní hospodářství a legislativní rámec, především však zdůraznil téma Národního centra kybernetické bezpečnosti.***

V úvodu vystoupení připomenul, že první počítač byl v ČR připojen na internet dne 13. 2. 1992. Jak náměstek Šmíd upozornil, jednalo se v té době spíše o záležitost akademické sféry, nicméně rozvoj fenoménu internetu byl od té doby obrovský. V současné době je podle některých odhadů 3% HDP ČR tvořeno právě v kybernetickém prostředí. Jak Jaroslav Šmíd uvedl, například IT odborníci dnes tvoří v České republice 2,5 % zaměstnanců a obecně internetové prostředí pak nabízí až 6% podíl na celkové zaměstnanosti. Minimálně 1x týdně používá internet pro svoji práci 35 % zaměstnanců, 97% firem v ČR má přístup k internetu, 92 % firem jej využívá pro kontakt s orgány veřejné správy, 40 % jeho prostřednictvím nakupuje a 25 % firem přes internet své produkty prodává. Jak náměstek Šmíd zdůraznil, jedná se sice jen o odhad, ale internet přináší do ekonomiky našeho státu přes 350 miliard korun ročně. Tento souhrn je podle jeho slov dostatečným důvodem, proč bychom měli internet chránit.

Náměstek Šmíd připustil, že jakákoliv pravidla chování na internetu nejsou nijak striktně dána. Sice zhruba od roku 2011 existuje iniciativa mezinárodního společenství pod vedením Velké Británie, která by měla pravidla chování v internetovém prostoru stanovit, zatím se tak však nedaří i proto, že jsou státy, které takové kroky považují za protichůdné vůči zásadám internetu, kterými jsou svoboda a volný přístup k němu. Na druhé straně jsou pak státy, kterým se podařilo prosadit určitou regulaci a omezování internetu, jako Rusko nebo Čína. Tedy v obecném pohledu je přístup k internetu velice roztříštěný.

## JAK VYUŽÍVÁME INTERNET?

Jak dále Jaroslav Šmíd pokračoval, internet je obrovské komunikační médium, které umožňuje komunikaci, přístup k informacím, elektronické obchodování, vzdělávání atp. Ale právě jeho obrovský rozměr a otevřenost sebou nese i hrozbu zneužití a kriminality. Tu je podle Jaroslava Šmída možné rozdělit do několika skupin. Může se jednat o skutečně organizovaný zločin, mohou to být útoky „zevnitř", kdy se například zaměstnavateli snaží škodit jeho vlastní zaměstnanci, může se jednat o špionáž průmyslovou či vojenskou atp. Je možné také registrovat sabotáže a cílené útoky teroristických skupin. V této souvislosti je podle Jaroslava Šmída problematické především to, že v prostředí internetu jsou připojeny i složky tzv. kritické infrastruktury.

*Ing. Jaroslav Šmíd*

I toto jsou tedy důvody, proč se NBÚ zapojil do aktivit v oblasti kyberbezpečnosti. Už v březnu 2012 byl předložen vládě věcný záměr zákona. Schválení jeho paragrafovaného znění bylo, především kvůli politickým změnám, oproti původnímu plánu pozdrženo. Nicméně nyní to skutečně vypadá tak, že zákon bude přijat a 1. 1. 2015 bude účinný.

## ZÁKLADNÍ PRINCIPY

### Důvěra

Především, jak náměstek Šmíd uvedl, je důležité posílit spolupráci všech sektorů společnosti v této oblasti. I proto chce NBÚ koordinovat veškeré aktivity státu, akademické sféry i komerce. Jedním z hlavních pilířů, na kterých stojí kyberbezpečnost, je totiž důvěra a sdílení informací. Prvním úkolem bude nastavit tento model v rámci státní správy, tedy v rámci eGovernmentu.

**Zodpovědnost**

Dalším důležitým faktorem podle náměstka Šmída je individuální zodpovědnost. Je to proto, že nikdo nezná konkrétní informační systém lépe než jeho provozovatel, on je podle náměstka Šmída nejlépe schopen pochopit jeho zranitelnost i cesty, jak minimalizovat škody, které by mohl případný útok způsobit.

**Spolupráce**

Samozřejmě NBÚ navázal spolupráci se všemi dotčenými rezorty, zároveň byla zřízena expertní poradní komise ředitele NBÚ a navázána zahraniční spolupráce.

**Přiměřenost**

Neméně důležitým principem je přiměřenost přijatých opatření. NBÚ nechce podle slov Jaroslava Šmída zavádět přílišné a zbytečné komplikace. I proto je potřeba vycházet z analýzy rizik.

## ZÁSADNÍ PILÍŘE ZÁKONA

- Prvním pilířem zákona je tedy **zavedení bezpečnostních opatření** tak, aby systémy byly dokumentovány, byly přiděleny role a tím rozdělena odpovědnost jednotlivých uživatelů.
- Jako další pilíř se nově objevuje **povinnost hlášení kybernetických incidentů**. Pokud někdo zjistí, že v rámci jeho systému došlo k útoku, bude jeho povinností incident hlásit a popsat tak, aby bylo možné varovat ostatní účastníky a hledat cesty minimalizace dopadů útoku.
- Posledním pilířem jsou **protiopatření**, jistá doporučení ze strany úřadu tak, aby nejen nebylo útočeno na naše systémy, ale aby ani tyto systémy nemohly být zneužity pro útoky směrem ven.

Jak Jaroslav Šmíd dále uvedl, bezpečnostní opatření, o kterých hovoří, je možné rozdělit na dvě části – organizační a technická. Z pohledu organizačních opatření se jedná o provázanost odpovědných osob v jednotlivých institucích, které jsou, v případě potíží, schopny operativně reagovat, být k dispozici a v kontaktu. Zároveň je nutné mít vybudovaný systém hlášení incidentů, který je schopen fungovat nezávisle na elektronické cestě a NBÚ v této souvislosti považuje za velice potřebné vybudování tzv. dohledových pracovišť na jednotlivých ministerstvech. V této souvislosti rovněž Jaroslav Šmíd vysvětlil, že opatření jsou určité úkony, které vydává NBÚ a jimiž chce varovat systémy. To znamená, že opatření jsou většinou ochranná, zaměřená na preventivní rovinu.

Při přípravě vlastní strategie narazilo NBÚ podle Jaroslava Šmída na skutečnost, že není v této oblasti sjednocená terminologie. I proto nakonec vypracoval vlastní výkladový slovník kybernetické bezpečnosti, který je česko-anglický a obsahuje zhruba 600 termínů.

## KOHO SE ZÁKON TÝKÁ?

Během diskuze, která následovala po jednotlivých prezentacích semináře, jsme dospěli k faktu, že připravovaný zákon o kybernetické bezpečnosti se v podstatě nedotkne měst ani obcí a v zásadě ani krajů. Hlavními ukazateli pro toto posouzení by měly být metriky, podle kterých se onen kritický systém bude posuzovat (např. procento HDP, možný počet obětí při napadnutí systému apod.). NBÚ by měl v současné době úzce spolupracovat především s KISMO a dalšími organizacemi na potřebném ujasnění těchto informací.

*Pozn. redakce:*
*Prezentace ve formátu PDF na www.egovernment.cz/kyber*

## VLÁDNÍ CERT

Vrcholovým pracovištěm v oblasti kyberbezpečnosti by, podle slov náměstka Šmída, měl být vládní CERT (Computer Emergency Response Team). Ten bude provozován v rámci Národního centra kybernetické bezpečnosti (NCKB) Národním bezpečnostním úřadem. Dalším takovým pracovištěm bude národní CERT, který je v současné době již provozován sdružením CZ.NIC, což je správce domény.cz. Podle Jaroslava Šmída je nyní v ČR několik dohledových pracovišť. To nejstarší provozuje CESNET, tedy na akademické půdě, a to od roku 2008. Tím nejmladším je uvedený vládní CERT od listopadu loňského roku. Za zmínku určitě podle slov Jaroslava Šmída stojí vojenský CERT, provozovaný Ministerstvem obrany, který dosáhl zajímavých úspěchů v rámci cvičení pořádaných NATO.

Vládní CERT již provozuje své vlastní webové stránky www.govcert.cz. Zde je možné získat aktuální informace o různých hrozbách a útocích, příslušných opatřeních atp.

## NÁRODNÍ CENTRUM

NCKB je organizační složkou NBÚ. Nejedná se tedy o samostatný úřad, který by s kýmkoliv komunikoval samostatně. Sestává ze dvou základních částí – zmiňovaného vládního CERTu a oddělení teoretické podpory, vzdělávání a výzkumu. Hlavní úlohou národního centra je koordinace a spolupráce jak na národní, tak mezinárodní úrovni, aby bylo předcházeno kybernetickým útokům, případně byla přijímána opatření při řešení těchto incidentů. NCKB tedy provozuje vládní CERT, zastupuje ČR v různých mezinárodních organizacích, připravuje národní bezpečnostní strategie a vydává aktualizace standardů.

NCKB již vydalo 1. kybernetickou strategii a související akční plán. Nyní je, podle slov Jaroslava Šmída, před úkolem zpracovat novou strategii, která bude širší a konkrétnější, protože ta první obsahovala pouze základní nutné kroky.

V další části svého vystoupení Jaroslav Šmíd upozornil na vzdělávací aktivity, v rámci nichž se NBÚ snaží dostat problematiku kyberbezpečnosti nejen do škol, ale rovněž mezi seniory.

Sídlo NCKB bylo slavnostně otevřeno 13. 5. 2014. Nyní již je z části personálně naplněno s tím, že cílového stavu 34 zaměstnanců by mělo být dosaženo do konce příštího roku. V současné době se již NCKB zabývá řešením nahlášených kybernetických incidentů. Podle Jaroslava Šmída se jedná převážně o phishingové útoky. Zároveň probíhají práce na nové strategii, která by měla být do konce června rozeslána k veřejnému připomínkovému řízení. Na tuto strategii navazují práce na akčním plánu, který bude konkretizovat, kdo, co, v jakém případě má dělat a za co je odpovědný.

Kromě uvedeného poskytuje NCKB rovněž metodickou podporu těm, kteří by chtěli budovat obdobná pracoviště.

## VÝZKUM

V oblasti výzkumu participuje NBÚ v současné době na dvou poměrně velkých projektech. Jedním z nich je tzv. kybernetický polygon, který vytváří společně s Masarykovou univerzitou. Jedná se o projekt zaměřený na testování sítí, ohrožených různými typy útoků. Další zajímavý projekt řeší rovněž Masarykova univerzita a jedná se o vybudování systému pro policii, který je orientován na kybernetickou kriminalitu. Další projekty jsou zaměřeny na otázky bezpečnosti mobilních zařízení s ohledem na jejich stále rostoucí popularitu.

Vedle toho se NBÚ podílí na spolupráci na různých úrovních v rámci mezinárodních fór, včetně mezinárodních cvičení v této oblasti. Jak náměstek Šmíd zdůraznil, česká účast a její úroveň bývá vysoce hodnocena.

## BUDOUCNOST

V závěru vystoupení Jaroslav Šmíd uvedl, že bylo by patrně dobré, aby vznikl jakýsi neveřejný informační servis, protože není vždy vhodné okamžitě zveřejňovat úplně všechny informace o zranitelnosti a bezpečnostních dírách. Tyto informace by měly být určeny jen omezenému okruhu uživatelů, především správcům sítí tak, aby měli možnost včas podniknout potřebné kroky k zamezení případných útoků. Jak dále řekl, určitě bude pokračovat začleňování do mezinárodních organizací. Stejně tak je tu plán na vybudování jakéhosi důvěryhodného kanálu na výměnu citlivých a utajovaných informací na národní a mezinárodní úrovni. I v oblasti již zmíněného vzdělávání plánuje NBÚ své zapojení do výuky na vysokých školách a zároveň chce studentům nabídnout možnost podílet se na jeho práci. Výhledově je nejzajímavějším cílem, aby Česká republika byla zahrnuta do transatlantického cvičení. ■

# Informační systém HELIOS Fenix

HELIOS Fenix je ojedinělý **rozsáhlým počtem modulů**, které jsou **vzájemně integrovatelné.** Celé řešení je navrženo tak, aby **nedocházelo k pořizování nadbytečných dat**, resp. aby se **v maximální míře využívaly a sdílely informace**, které jsou v systému již evidovány.

Funkcionality jsou úzce provázané, nicméně systém vazeb a oprávnění umožňuje využívat jednotlivé funkcionality i samostatně, záleží však na konkrétní konfiguraci a potřebách. Maximální důraz při vývoji byl kladen právě na komplexnost řešení a vzájemnou integrovatelnost jednotlivých prvků systému. Produkt je nezávislý na platformě a plně respektuje všechny dosud schválené standardy a normativy pro budování IS veřejné správy.

Informační systém

Spisová služba
Matrika
Základní registry
Registr obyvatel
ePodatelna
Vidimace a legalizace
Fakturace
Smlouvy

Veřejná správa
Volby
Účetnictví
Portál občana
Rozpočet
Schvalování
Fakturace
Outsoursing

ERP
Majetek
Cloudová řešení
CRM
IDM

Moderní řešení a informační systémy pro státní správu, samosprávu, příspěvkové a neziskové organizace, dobrovolné svazky obcí, auditory i pro Vás.

# Spisová služba HELIOS eObec

Moderní, komplexní řešení pro elektronickou komunikaci úřadu s občany a podnikatelskými subjekty.

**Obsahuje** plnohodnotnou **spisovou službu s procesním workflow** pro města, obce a zřizované organizace. Spisová služba zefektivňuje a zpřehledňuje procesy týkající se dokumentu, čímž přináší úsporu produktivního času zaměstnanců organizace. Spisová služba je napojena na lokální systém registru adres tak, aby data pořizovaná do systému byla relevantní. Samozřejmostí je také integrace s IS Základních registrů.

www.helios.eu/fenix
www.helios.eu

HELIOS
Software, který řídí

# Cesta zákona Sněmovnou

***Z pozice zpravodaje uvedeného návrhu zákona v Poslanecké sněmovně PČR byl dalším vystupujícím v programu semináře poslanec Václav Klučka.***

*Ing. Václav Klučka*

Uvedl, že jeho vystoupení se omezí pouze na informaci o tom, jak je ve Sněmovně projednáván zákon o kyberbezpečnosti. Zároveň upozornil, že auditorium semináře bude první, kdo uslyší jeho návrhy a postoje k jednotlivým pozměňovacím návrhům, které jsou připraveny pro druhé a třetí čtení.

Zároveň poslanec Klučka upozornil, že se jedná o první seminář na téma kybernetická bezpečnost, který absolvuje. Je to proto, že se podle svého mínění má diskuse účastnit až tehdy, kdy může komentovat legislativní proces, nikoli že by se vyjadřoval jako odborník na kyberbezpečnost. Pokud jde o samotný zákon, zopakoval poslanec Klučka, že základním cílem návrhu zákona o kyberbezpečnosti je zvýšit bezpečnost kybernetického prostoru a zavést systém dobře fungující spolupráce mezi veřejnou správou a soukromým sektorem, a to za účelem zefektivnění řešení kybernetických bezpečnostních incidentů. V této souvislosti zavádí návrh zákona konkrétní oprávnění a povinnosti vybraným subjektům. Ty mají za cíl zajištění dostatečné bezpečnosti kybernetického prostoru. Návrh zákona přitom nesměřuje k prevenci a eliminaci všech rizik, která se mohou dotknout všech uživatelů kybernetického prostoru, ale zaměřuje se především na ochranu takové části infrastruktury, která je pro fungování státu nezbytná a významná a jejíž ohrožení, nebo narušení by ve svém důsledku mohlo vést k poškození, nebo ohrožení zájmů České republiky.

Jak poslanec Klučka připomněl, pohybuje se ve Sněmovně v oblasti obrany a bezpečnosti. V oblasti bezpečnosti působí především v úseku tzv. kritické infrastruktury, integrovaného záchranného systému a spolupráce složek IZS. Už při prvním čtení zákona o kyberbezpečnosti jasně ve Sněmovně deklaroval, že tento zákon doplňuje pilíře celé oblasti vnitřní bezpečnosti v tomto státě. Nejen bez tohoto zákona, ale ani bez dobře fungujících sítí v systémech a registrech se prostě dnes již neobejdeme. Pokud by došlo k takovému útoku, který by tyto systémy vyřadil z provozu, pak nejsme schopni, v rámci složek IZS, poskytovat účinnou pomoc. Zůstali bychom bez informací, bez spojení, nebylo by možné čerpat potřebné údaje z registrů, které jsou nutné pro zdárnou zásahovou činnost a to by podle jeho slov byla skutečně obrovská pohroma. Nejde zde tedy, jak uvedl poslanec Klučka, pouze o to, abychom změnili v nařízení vlády o kritické infrastruktuře pojmosloví a velikost jednotlivých kritérií, ale abychom kybernetickou bezpečnost dokázali vsunout do jednotlivých ustanovení, a to i do těch, která se týkají kritické infrastruktury. A především, abychom si uvědomovali, že v případě selhání nebudeme schopni tuto záležitost jakkoliv řešit. Václav Klučka připomenul, že nedávno proběhlo v Praze cvičení black-outu. Jak uvedl, přineslo toto cvičení velice zajímavé výsledky. Nejen že si odborníci v praxi ověřili, že v určité době, kdy by byla Praha bez energie, vody a propojení, by došlo ke skutečnému kolapsu. Ale začaly se podle jeho slov také modelovat i situace, kdy nefungují sítě. A zde nastává skutečná beznaděj, z níž v daném okamžiku není, jak uvedl Václav Klučka, východisko. V oblasti krizového plánování je nyní nutno toto vše doplnit. Uvedl, že dříve nebyly parametry, které by zpracovatele strategie nutily k takovému záběru. Je podle něj naprosto zřejmé, že zákon o kyberbezpečnosti je začátek nového procesu, který je před námi, abychom dokázali oblast vnitřní i vnější bezpečnosti ochránit tak, abychom byli schopni skutečně účinných zásahů.

Výbory, které usnesením Poslanecké sněmovny dostaly k projednání zákon o kyberbezpečnosti, jsou rozpočtový, ústavně-právní, pro obranu a výbor pro bezpečnost. Jak referoval poslanec Klučka, je v této chvíli uzavřeno projednávání návrhu zákona ve výboru pro obranu, kde byl přijat pozměňující návrh. Výbor pro bezpečnost už jednal o tomto zákoně dvakrát a měl by toto projednávání dokončit do konce května. Ústavně-právní výbor jednoduchým usnesením doporučil zákon ke schválení v Poslanecké sněmovně a výbor rozpočtový se tímto zákonem prozatím nezabýval a patrně ani nebude zabývat. Tento zákon sám o sobě provádí novelizaci čtyř dalších norem – zákona o svobodném přístupu k informacím, zákona o provozování rozhlasového a televizního vysílání a změně dalších zákonů, zákona o elektronických komunikacích a o změně některých souvisejících zákonů a zákona o ochraně utajovaných skutečností.

Výbor pro obranu, který, jak již bylo řečeno, ukončil projednávání návrhu zákona, přijal pozměňující návrh kolegy Bohuslava Chalupy, který ve své podstatě pouze doplňuje některé ustanovení k paragrafu 17 a 19, tedy Národního CERTU. Nejsou to ale ustanovení, která by měnila původní charakter návrhu zákona tak, jak byl zpracován NBÚ. Tento pozměňující návrh byl navíc takřka jednomyslně ve výboru přijat a jako zpravodaj zákona bude tento návrh poslanec Klučka doporučovat. Jak bylo dále řečeno, výbor pro bezpečnost přerušil projednávání tohoto návrhu především proto, že se ve výboru objevil pozměňující návrh kolegy Matěje Fichtnera. Poslanec Klučka připustil, že to nebylo jednoduché rozhodnutí, očekávalo se totiž, že výbor dokončí projednávání zákona. Bohužel kolega Fichtner kromě toho, že dává ze zákona pryč pojem veřejnoprávní smlouvy a komplikuje záležitost postavení ujednávání se státem, tak se podle slov poslance Klučky pouští do paragrafu 17, kde výrazně mění celou úroveň pravomoci národního CERTu. Poslanec Klučka jako zpravodaj tohoto zákona nebude uvedený pozměňovací návrh doporučovat. Kolega Fichtner bezpochyby návrhne projednání tohoto pozměňovacího návrhu ve druhém čtení. Protože je v rozporu s prvně jmenovaným návrhem poslance Chalupy, patrně se stane, že ve třetím čtení po schválení návrhu poslance Chalupy bude návrh poslance Fichtnera prohlášen za nehlasovatelný. To je pohled na možný přístup očima zpravodaje zákona. Přitom, jak Václav Klučka upozornil, je poněkud mrzuté, že oba autoři těchto návrhů jsou z jednoho politického subjektu a jejich návrhy jsou takto protichůdné.

Jak dále poslanec Klučka uvedl, v systému Poslanecké sněmovny je dále návrh poslance Valenty, který se týká paragrafu 5. Poslanec Valenta chce, aby orgány a osoby, které jsou uvedeny v paragrafu 3 písm. c–e, měly povinnost volit jako dodavatele služeb elektronických komunikací pro relevantní informační systémy pouze subjekt, který zároveň zajišťuje veřejnou komunikační síť, která má zásadní vliv na bezpečnost příslušného systému. O tomto návrhu se zatím nijak nediskutovalo. Poslanec Klučka však nebude tento návrh podporovat. Dalším je pak pozměňující návrh poslance Jana Birkeho, který v paragrafu 4 doplňuje odstavec 3. Tento pozměňující návrh byl diskutován s NBÚ a tento pozměňující návrh bude poslanec Klučka podporovat i v rámci třetího čtení v Poslanecké sněmovně. A poslední připomínka je od dvou navrhovatelů a má dvě podoby. Nejsou to však lidé z Poslanecké sněmovny. Tito dva navrhovatelé, jak poslanec Klučka uvedl, řeší paragraf 89. Toto řešení v zásadě odporuje základní podstatě, která byla NBÚ do zákona zavedena, a proto zpravodaj zákona souhlasí se zamítavým stanoviskem NBÚ k tomuto návrhu.

Závěrem Václav Klučka uvedl, že výbor pro bezpečnost bude jednat koncem května, Sněmovna pak v polovině června. Nejprve bude probíhat druhé čtení a do 48 hodin pak čtení třetí. Uvedl, že předpokládá, že na tomto jednání bude návrh zákona o kyberbezpečnosti přijat. A pak už jen případné výhrady Senátu by mohly zabránit tomu, aby účinnost zákona byla skutečně od 1. 1. 2015. ■

(Doplňující informace redakce – návrh zákona byl ve třetím čtení projednán a schválen dne 18. 6. 2014.)

# Zákon kyberbezpečnost nevyřeší

***Ivan Pilný upozornil, že nevystupuje na semináři jako předseda Hospodářského výboru, protože tento výbor nemá zákon o kyberbezpečnosti k projednání. Proto zde vystupuje spíše jako poslanec a politik. Připomněl, že při svém vstupu do politiky podepsal výzvu, která mimo jiné upozorňuje na skutečnost, že zde schází devět zákonů. Dnes, po seznámení se s celkovou situací v Poslanecké sněmovně, je podle svých slov přesvědčen, že tady je naopak 99 zákonů, které přebývají. Proto vždy, když se začne hovořit o přípravě nového zákona, se Ivan Pilný ptá, jaký problém tento zákon řeší?***

*Ing. Ivan Pilný*

Podle Ivana Pilného je zcela evidentní, že zákon o kybernetické bezpečnosti neřeší kybernetickou bezpečnost. Není to totiž možné. Jak upozornil, už z prezentace náměstka Šmída bylo zřejmé, že řada činností, které s kyberbezpečností souvisejí, se musí a bude vykonávat mimo tento zákon. Kybernetická bezpečnost je podle Ivana Pilného problém, který začíná prevencí. Je to tedy otázka toho, jak budeme například přistupovat k sociálnímu inženýrství, které je jedním z klíčových vstupů do problematiky bezpečnosti. Je podle něj otázkou, jak budeme definovat nějaké bezpečnostní standardy atp.

Zákon se výrazně orientuje na detekci útoků na kybernetickou bezpečnost. Ty by měly být podkladem pro analýzu tak, aby bylo možné systém neustále zlepšovat, a zároveň by měly být podkladem pro činnost hasičů, protože když vzniknou nějaké útoky, je samozřejmě potřeba se s nimi vypořádat. Pojem kybernetické bezpečnosti se podle Ivana Pilného v žádném případě neomezuje na téma veřejné správy, stejně tak ne jen na toto území. Ohrožení veřejné správy, tedy výkonu veřejné správy, znamená ohrožení bezpečnosti a hospodářství této země. Je to samozřejmě otázka rovněž nějaké trestní odpovědnosti a dalších souvislostí. Jak je vidět, jedná se o velice rozsáhlou problematiku, kterou je potřeba vnímat mnohem šířeji, než je v tom zákoně momentálně definováno.

Ivan Pilný se dále věnoval některým základním premisám, na nichž je zákon vystavěn. Uvedl, že otázka spolupráce je jistě na místě. Zastavil se však u termínu individuální odpovědnosti. Jak řekl, je nutné se zamyslet nad tím, jak ji budeme zajišťovat a jak ji budeme vymáhat. Pokud nebude v tom zákoně obsažena, pak je zmínka o individuální odpovědnosti zbytečná.

Pro něj osobně je tento zákon teprve jakýmsi prvním startem do problematiky a jeho projednávání bude přiměřené expertýze, která momentálně v Poslanecké sněmovně je. Tedy poslanci se podle něj budou bavit o soukromí, o definici incidentů a o tom, které subjekty do problematiky kyberbezpečnosti mohou vstupovat. To je podle mínění Ivana Pilného všechno, co je možné v Poslanecké sněmovně projednat. Jak dále řekl, jsou to sice věci banální, ale Sněmovna s nimi nemůže nic udělat. Protože jak víme, soukromí už dávno neexistuje. Ve chvíli, kdy kdokoliv z nás aktivně vstoupí na internet, zbaví se těch posledních jeho zbytků. To, že budeme muset spolupracovat s veřejnými subjekty, je zřejmé, protože většina veřejných subjektů provozuje například infrastrukturu a vytváří softwarové i hardwarové prostředky, které bezpečnost definují.

Kličkování kolem toho, co je a není bezpečnostní incident, je podle Ivana Pilného hraním se slovy stejně jako problematika nějakého slovníku kybernetických útoků. Je mimo jiné zřejmé, že ten slovník se bude stále rozšiřovat. Nicméně platí, že zákon bude projednán a je možné jej tedy považovat za jakýsi první výkop, ale v žádném případě to nemůže být zákon poslední.

Doporučoval by ovšem výrazné posílení kvantitativního i kvalitativního materiálu a zázemí, které má k dispozici NBÚ. Zatím útoky, které jsou podnikány, jsou spíše v oblasti anekdot. Ale když se podíváme, jak jsou některé naše systémy zabezpečeny, je zřejmé, že by bylo možné veřejnou správu velice snadno paralyzovat poměrně triviálními kybernetickými útoky. A je jedno, jestli pro tyto postupy máme v našich slovnících označení. Podstatné je podle Ivana Pilného i to, že kriminalita v kyberprostoru se vyvíjí a žádné zákony ji nikdy nedoženou. Ale to neznamená, že bychom se o to neměli snažit.

V závěru svého vystoupení Ivan Pilný řekl, je velice rád, že se v Poslanecké sněmovně začal zákon projednávat a že vznikají takovéto semináře. Ponětí, povědomí o tom, co hrozby v kybeprostoru znamenají, je skutečně potřeba zvyšovat a je potřeba úměrně tomu navyšovat zdroje, které jsou v tomto směru k dispozici. ■

# Kyberbezpečnost = architektonická bezpečnost

***Ondřej Felix tématicky navázal na slova poslance Ivana Pilného. Hned v úvodu řekl, že bezpečnost začíná architekturou a to je prazáklad všeho. Ondřej Felix upozornil, že jsme s bezpečností v informačních systémech nezačali ani internetem ani právě diskutovaným zákonem, ale mnohem dříve. V oblasti bezpečnosti se jedná o záležitosti, které mají velkou setrvačnost, jde při tom o stále stejné požadavky a my se musíme učit budovat sdílené služby tak, aby byly bezpečné.***

## SDÍLENÉ SLUŽBY

Jestliže vyhovíme současným trendům a veřejnou správu vybudujeme jako systém sdílených služeb, tak i z bezpečnostního hlediska přidáváme jedno zcela zásadní riziko – sdílená služba implementovaná jednou a poskytovaná homogenním způsobem na území celého státu znamená, že když tato služba vypadne, přestane fungovat příslušná část celého státu. Poskytování sdílených služeb nemůže, respektive nesmí být vybudováno amatérsky, ale musí se jednat o kvalitní inženýrské dílo, které musí být vhodně zabezpečeno jak z provozních, tak bezpečnostních hledisek. Pokud systém nebude vytvořen takto, pak budeme podle Ondřeje Felixe ve stejné situaci jako s centrálním registrem vozidel.

*Ing. Ondřej Felix, CSc.*

## DŮVĚRYHODNÉ

ICT služby veřejné správy musí být důvěryhodné – to je jedna z věcí, na kterou se podle Ondřeje Felixe velice často zapomíná. Proto zákon o kybernetické bezpečnosti není podle něj zdaleka to první, co se týká bezpečnosti. Zákon o elektronickém podpisu v roce 2000 byl vlastně prvním zákonem, který se zabýval tím, jak vyrobit důvěryhodný elektronický dokument a jak mu zajistit určitou dávku bezpečnosti. Zákon o datových schránkách se zabývá tím, jak důvěryhodně doručovat v současném prostředí, aby zásilka byla právně závazná, bezpečná a spolehlivá. Takže zákon o kyberbezpečnosti je jen logickým pokračováním.

## ORCHESTROVANÉ

Třetím požadavkem je orchestrace (automatická koordinace) a to je požadavek náročný na finance. Jak Ondřej Felix upozornil, máme dnes vedle sebe postaveny stovky agendových systémů, které se sice nepřekrývají ve funkčních požadavcích, ale ve všech nefunkčních požadavcích v podstatě ano. Každý z nich totiž znovu zabezpečuje svůj systém pro přístup uživatelů z internetu, každý z nich znova vytváří síťovou infrastrukturu, každý z nich znovu dělá monitoring, service desks a tak dále.

## PROPOJENÉ

Kromě toho, že tyto služby by měly být orchestrované, měly by podle Ondřeje Felixe být také propojené. To znamená, že pokud obsahují data, musíme je používat. Tady ale podle něj opět narážíme na bezpečnost. Jako příklad uvedl skutečnost, že jednou padělaný řidičský průkaz, který se nachází v systému řidičských průkazů, je padělaný navždy pro celou veřejnou správu.

Zásadní riziko, které Ondřej Felix vidí v oblasti informačních systémů veřejné správy, tedy není v tom, že systém někdo „naboura“. Jak uvedl, za dva roky provozu základních registrů došlo pouze ke dvěma výpadkům a oba byly způsobeny skutečně velmi hardwarovými hackery. Jeden totiž převrtal vysokonapěťový kabel a druhý šroubovákem odpálil baterky v zásobním centru a způsobil tak požár.

Propojené tedy znamená, a s tím se setkávají dnes ti, kteří si jdou přihlásit automobil na přepážky, že pokud jeden z asi dvanácti systémů, jež se kontrolují, v momentě přihlašování nefunguje, tak se tento proces přeruší a automobil se v dané chvíli nepřihlásí. Pokud celý systém funguje, je to podle slov Ondřeje Felixe vynikající. Přihlašující nemusí už nic dokládat a má přihlášené vozidlo. Pokud

ale nepracuje byť jen jediný článek toho řetězce, tak automobil prostě nepřihlásí. Problém se samozřejmě zvětšuje úměrně době, po kterou systém nefunguje.
Jednotlivým principům se dále věnoval podrobněji.

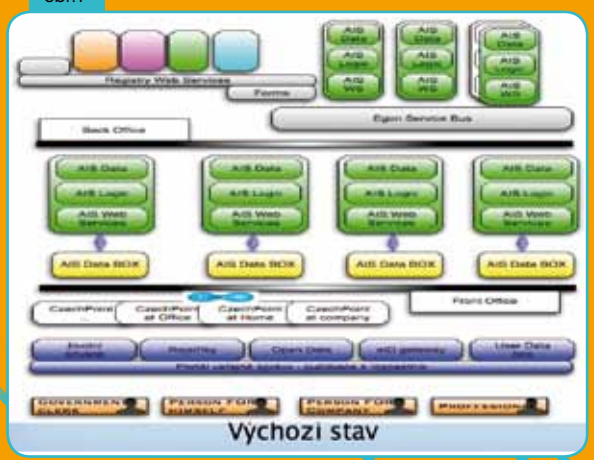
**Propojenost** je podle Ondřeje Felixe dalším rizikem. Jak uvedl, na základní registry je dnes připojeno 2000 informačních systémů veřejné správy. Pokud registry přestanou fungovat, v prvních dnech to patrně nebude nikomu až tak vadit. Ale během týdne se začne situace skutečně zhoršovat, protože veřejná správa se bude zastavovat. Čím víc budeme propojovat a čím více budeme propojení dělat bezprostřední, tím víc budeme, jak Ondřej Felix zdůraznil, senzitivní na jakoukoliv poruchu.

**Přístupnost** – v ní je podle Ondřeje Felixe základní problém. Celá internetová bezpečnost je totiž především bezpečností přístupové sítě. Pokud nebude dobře architektonicky navržená, tak žádný úředník nemůže komunikovat se svým systémem přes internet, protože takový přístup by byl architektonicky špatný. Ale jakýkoliv samoobslužný uživatel samozřejmě musí přistupovat k nabízeným službám přes internet. Jakýkoliv mobilní uživatel jde přes nějakou kombinaci mobilního operátora a internetu. To tedy znamená, že čím víc budeme dělat samoobsluhu, tím víc si žádáme o problém. Ale čím víc budeme dělat samoobsluhu, tím je vše samozřejmě pohodlnější. Pohodlnost a bezprostřednost by měla být vždy vyvažována bezpečností a penězi.

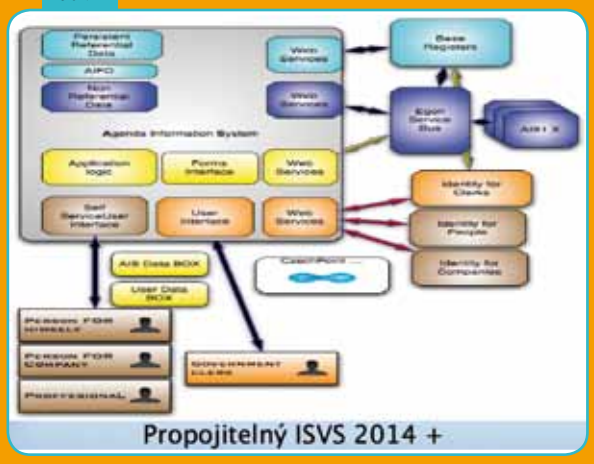
**Dostupnost** – to je další zásadní moment, který je podle slov Ondřeje Felixe nutno správně posuzovat. Velmi často je jako vzor internetových služeb zmiňováno internetové bankovnictví. Ondřej Felix proto upozornil, že nezná internetové bankovnictví, které by své klienty pouštělo do bankovního systému. Bankovní systém je chráněn několika zónami, a pokud dojde k zaúčtování, neproběhne na základě toho, že se někdo připojí přes internet k hlavní knize banky a tam cosi změní v účtu.
Pokud tedy chceme být efektivní, tak budeme podle mínění Ondřeje Felixe pracovat ve sdílené infrastruktuře, ale rozhodně to nemůže být infrastruktura ve veřejné cloudu, umístěném kdesi v dalekém a neznámém zahraničí. Musí se jednat o sdílenou infrastrukturu s regulovatelnými, viditelnými a definovatelnými pravidly podle oboru, ve kterém se pohybujeme.

Podle Ondřeje Felixe stále zapomínáme na jednu strašně důležitou věc. S technologiemi, kterým říkáme internet, se provozují tři roviny úloh. Jedna je tzv. open internet, kde publikujeme informace a chceme, aby byly svobodně dostupné. Druhou rovinou jsou služby, které nejsou otevřené a na nich se stejný standard nemá co objevovat (jedná o služby bankovní, zdravotních pojišťoven atp.),. A třeti rovinu tvoří otázka privátnosti, tedy našeho soukromí.
Jenom pro připomenutí uvedl Ondřej Felix projekty státní informační politiky z roku 1999. Na základě této politiky byla vytvořena první dávka informatických zákonů, v nichž někde je i soustava on-line služeb eGovernmentu a jeho důvěryhodné a bezpečné transakce. Už v roce 1999 jsme se tedy zabývali otázkami bezpečnosti. Realizovala se však jen určitá část a nyní děláme další krok. Zákon o kybernetické bezpečnosti je podle jeho mínění nastavením minimálních standardů především v oblasti přístupů ke službám veřejné správy. Rozhodně to nejsou všechny standardy a rozhodně nikdy nebudou všechny. Stále nás čekají další a další.
Ondřej Felix dále demonstroval (obr. 1), jak vypadá současná architektura veřejné správy. Uvedl svůj oblíbený příklad – když v ČR není v registru obyvatel zaznamenáno za 24 hodin narození dítěte, tak to neznamená, že vymíráme, ale znamená to, že evidence obyvatelstva se přestala aktualizovat. To se mohlo stát z mnoha různých důvodů, jeden z nich je, že nefunguje připojení k základním registrům. Jak Ondřej Felix řekl, tvoříme propojené systémy, ale zároveň děláme systémy, ve kterých internet nemá co dělat. Síťové propojení musí být podle jeho slov od internetu oddělené, to je jedna ze zásad architektonické bezpečnosti.

obr.1



obr.2




Druhý obrázek (obr. 2) demonstruje, jak by mohly vypadat informační systémy ve velmi krátké budoucnosti. Byly by propojeny klíčovými integračními body se službami okolo nich. Jak ale řekl, každá z těch šipek na tomto obrázku znamená bezpečnostní a provozní riziko, protože bez kterékoliv z těchto šipek nebude celý systém fungovat. To znamená, že místo systémů, které fungovaly v blahé izolaci od okolního světa a díky tomu přežívaly, teď začínáme stavět systémy, které jsou s okolním světem propojené, a to mnoha vazbami.

Jak řekl, je-li naším cílem skutečně učinit AISy propojitelnými a realizovat 85% podání propojitelnými AISy, tak s bezpečností podle Ondřeje Felixe skutečně jenom začínáme a zákon, o kterém hovoříme, vytváří jen minimální standard. V rámci tohoto celého procesu nás čeká ještě mnoho navazujících kroků.

obr.3


Poslední poznámka Ondřeje Felixe se týkala struktury architektury veřejné správy (obr. 3). Tak jak by měla vypadat, včetně toho, že klíčová architektura vedle těch čtyř vrstev je architektura bezpečnostní. Potom by podle jeho slov měl národní architektonický plán vypadat, jak ukazuje obrázek 4.

obr.4


Ondřej Felix závěrem uvedl, že při celkovém pohledu to znamená postavit eGovernment a správu národní architektury systému ve veřejné správě tak, že klíčovou bude architektura bezpečnostní. Pod tuto bezpečnostní architekturu budou spadat některé, nebo možná všechny požadavky zákona o kybernetické bezpečnosti. Z pohledu Ondřeje Felixe je to totiž jeden z dalších základních informatických zákonů upravujících průřezová pravidla pro fungování informačních systémů ve veřejné správě. Je na stejné úrovni jako zákon o informačních systémech veřejné správy či jako zákon o datových schránkách, nebo o základních registrech. Před námi je zásadní úkol – představit si, jak jsou systémy propojeny mezi sebou z bezpečnostních i funkčních hledisek tak, abychom dobře a bezpečně postavili sdílené služby veřejné správy.

Podle Ondřeje Felixe je kyberbezpečnost základní komponenta národního architektonického plánu, ale zdaleka ne jediná. ■

*Pozn. redakce:*
*Prezentace ve formátu PDF na www.egovernment.cz/kyber*

# Finále 9. 9. 2014, Mikulov
# www.egovernment.cz/miss

Jedná se dnes již o tradiční soutěž, která je určena pro sympatické dámy pracující ve veřejné správě.
Mohou to být referentky, přepážkové pracovnice, vedoucí odborů, matrikářky, starostky, náměstkyně... Mohou se přihlásit samy, nebo je mohou přihlásit jejich kolegové prostřednictvím www.egovernment.cz/miss.
Fotografie a stručné profily jednotlivých dam budou vystaveny na tomto webu a jeho návštěvníci hlasováním rozhodnou o tom, kterých deset dam postoupí do finále.

Vítězky obdrží hodnotné ceny. Pro Miss Egovernment 2014 je pak připraven **víkendový wellness pobyt pro dvě osoby** se snídání a kvalitním vínem v hotelu Galant v Mikulově.

V dosavadní historii vedou reprezentantky veřejné správy v počtu vítězství 3:2 nad kolegyněmi z České pošty. Vyrovná letos pošta počet vítězství, nebo bude královnou českého eGovernmentu opět zástupkyně úřadů? **Pokud jste sympatická a komunikativní, neváhejte a přihlašte se, i Vy to můžete změnit!**

# Kyberbezpečnost v praxi

***Miroslav Krejčík své vystoupení zahájil konstatováním, že Česká pošta je již dlouho strategickým partnerem státu při budování eGovernmentu a to je postavení, které je pro poštu velkou výzvou. V současné době Česká pošta provozuje nejen vlastní komunikační a informační systémy, ale rovněž je provozovatelem některých informačních systémů veřejné správy.***

Připustil, že je velice pravděpodobné, že zákon o kybernetické bezpečnosti bude přijat s účinností k 1. 1. 2015, a proto je možné si dovolit určitou prognózu. V důsledku zákona o kybernetické bezpečnosti se stanou některé současné informační systémy veřejné správy tzv. kritickými nebo významnými informačními systémy. To znamená, že ve velmi krátké době budou muset tyto systémy splňovat určité podmínky, které jsou stanoveny právě zákonem a prováděcí vyhláškou. Určitým reprezentantem informačních systémů je v této souvislosti Informační systém datových schránek.

Veřejná správa se snaží přibližovat občanům a podnikatelům, takže jí nezbývá nic jiného než využívat internet. Je to cesta logická, ale zároveň se jedná o slabé místo celého systému. Informační systém datových schránek funguje od roku 2009 a od té doby jsme v situaci, kdy vlastně ani nepochybujeme o existenci tohoto systému a bereme jej jako samozřejmost. Datové schránky znamenaly skutečně přelomový krok, kterým veřejná správa definitivně přešla od papírových k elektronickým dokumentům.

Podle dat k 17. 5. 2014, tedy k datu těsně před konáním semináře, je počet datových schránek zhruba 590 tisíc. Z tohoto počtu je 523 tisíc datových schránek aktivních. Počet odeslaných datových zpráv činí 191 milionů za rok, což znamená 250–280 tisíc odeslaných datových zpráv denně. Jak upozornil Miroslav Krejčík, i s těmito vysokými čísly systém bezproblémově funguje, což považuje za velice důležité. Důvodem, proč o tom mluvit, je skutečnost, že Česká pošta v případě Informačního systému datových schránek zastává několik rolí. Předně, protože je držitelem poštovní licence a poskytovatelem univerzální služby, je prostředníkem pro doručování, adekvátně jako tomu je v papírovém světě. Zároveň je provozovatelem Informačního systému datových schránek, tedy zajišťuje chod některých součástí IS a souvisejících služeb.

*Ing. Miroslav Krejčík*

Pokud se bavíme o kybernetické bezpečnosti, položil si Miroslav Krejčík několik otázek, na něž nabízel i odpovědi:

**Mohou se stát datové schránky cílem kybernetického útoku?**

S velkou pravděpodobností ano, protože se jedná o informační systém, který je přístupný prostřednictvím internetu.

**Dá se tato hrozba na 100 % eliminovat?**

Taková možnost se stoprocentně vyloučit nedá. 100% eliminace žádného potenciálního rizika není v reálném světě možná – lhostejno, o jaký obor lidské činnosti se má jednat.

**Mohlo by se tedy stát, že datové schránky nebudou několik hodin, nebo dokonce několik dní dostupné?**

Rozhodně to možné je.

**Poslední otázka je, zda jsme na takovou situaci připraveni?**

Na krátkodobý výpadek patrně ano, u dlouhodobého výpadku už to tak jisté není.

Že není předchozí obava úplně lichá, dokládá incident z 8. ledna 2014, kdy byly datové schránky nedostupné 110 minut. Přitom nešlo o žádný hackerský útok, ale jen o technický výpadek jednoho technologického prvku, který je však z pohledu provozu velice podstatný.
Pro názornější představu Miroslav Krejčík předestřel pro datové schránky výběr tří možných scénářů bezpečnostních incidentů.

## Scénář číslo 1 – zneužití identity a následné zablokování datové schránky oprávněného uživatele

Aby oprávněný uživatel mohl využívat služeb jeho datové schránky (přijímat a odesílat zprávy), musí se nejprve úspěšně přihlásit. Hovoříme o dostupnosti služby. Ta může být odepřena v případě, kdy se někdo neoprávněný pokusí přihlásit k datové schránce přes zcizenou identitu jejího oprávněného uživatele. Poté může útočník opakovaným logováním docílit zablokování účtu oprávněného uživatele. Ten to většinou zjistí až v momentě, kdy se snaží ke své datové schránce přihlásit. Většinou v takovém okamžiku iniciuje nápravu.
Této situaci se podle Miroslava Krejčíka zabránit nedá. Výskyt tohoto typu bezpečnostního incidentu je samozřejmě možné předpokládat i po nabytí účinnosti očekávaného zákona o kybernetické bezpečnosti. Ten pro uvedený případ nenabízí žádné nástroje, jak hrozbu eliminovat. Jen zakládá oznamovací povinnost provozovatele významného nebo kritického informačního systému veřejné správy (poznámka – lze předpokládat, že se takovým Informační systém datových schránek stane) vůči Národnímu bezpečnostnímu úřadu.

## Scénář číslo 2 – pokus infiltrovat Informační systém datových schránek škodlivým kódem

Útočník se v tomto případě snaží dostat do Informačního systému nějaký škodlivý pozměňující kód, který by narušoval činnost a chod datových schránek. Snaží se tedy poslat infikovanou datovou zprávu a její pomocí, nebo pomocí infikované přílohy, modifikovat funkcionalitu Informačního systému datových schránek. Takový postup je velmi těžké detekovat okamžitě, většinou k odhalení podobných praktik dochází s velkým zpožděním.
Nicméně prostředí datových schránek je vlastně jen tranzitním prostředím. To znamená, že Informační systém datových schránek nevstupuje do kontaktu s obsahem zpráv. Je proto jisté, že negativní následky tohoto útoku ponese jen adresát infikované zprávy. Kterému po vyzvednutí a případném otevření infikované zprávy dojde k zavirování počítače. Informační systém datových schránek v tomto případě není ohrožen.
Jestliže by takový útočník například ovládl datovou schránku některého z orgánů veřejné moci a současně by disponoval podobným nebezpečným kódem, mohl by se pokusit ohrozit i poměrně velký počet potenciálních příjemců datových zpráv. Naštěstí právní předpisy České republiky na takovou situaci pamatují a to umožňuje uložit správní pokutu. Riziko se tak částečně přenáší na odesílatele, tj. toho, z jehož datové schránky by byly podobné zprávy odeslány.

## Scénář číslo 3 – záměrné přetěžování Informačního systému datových schránek (DDOS „flood“ útok)

Jedná se o známou a poměrně hojně rozšířenou formu útoku na informační systém, jehož cílem je způsobit zahlcení vstupu (například tzv. DDOS „flood“ útokem). Výsledkem úspěšného útoku je pak nedostupnost služby, kterou oprávněný uživatel informačního systému požaduje a očekává. V tomto případě je velice důležité, jak přesně je nastavena bezpečnostní politika informačního systému pro identifikaci a řešení bezpečnostních incidentů. V praxi totiž jde zpravidla o minimalizaci časové prodlevy od chvíle, kdy je bezpečnostní incident zaregistrován a následně odstraněn. Jinými slovy, jak dlouho musí uživatel čekat.

Prezentace třetího scénáře měla za cíl především to, abychom si uvědomili, kam se posunula veřejná správa. Úřední záležitosti už dávno nevyřizujeme jen tužkou a papírem. A jestliže průměr odeslaných datových zpráv prostřednictvím Informačního systému datových schránek činí každý den 250 tisíc, je na místě otázka, zda v momentě nějakého skutečně dlouhodobějšího výpadku jsme schopni zajistit náhradní řešení. Miroslav Krejčík náhradních variant moc nevidí, v praxi se nabízí jen jedna – dočasný návrat k listovní formě doručování zpráv. I tak je nezbytné zaměřit pozornost na zajištění bezpečnosti Informačního systému datových schránek proti podobnému typu útoku, nejen technicky ale i organizačně.

Ochrana informačních systémů před kybernetickými hrozbami je nikdy nekončící proces. Základní diskuse je zpravidla vedena v trojúhelníku dostupnost, integrita a důvěrnost. Zatímco u integrity a důvěrnosti je situace docela přehledná a relativně snadno řešitelná, u dostupnosti se jedná o problém, který je stále diskutován. Hrozby v tomto směru neubývají, naopak jich přibývá. Samozřejmě by bylo ideální, aby dostupnost činila 100 %, tzn., že kdykoliv nějakou službu potřebujeme, máme ji k dispozici. Reálné to však není. Reálné je zajištění dostupnosti na 99 a více procent. Musíme si ale uvědomit, že je to oblast, která nejvíce prodražuje informační systémy a zároveň evokuje potenciálně největší nespokojenost na straně uživatelů. Z pohledu provozovatele informačního systému se pak jedná o neustálé balancování nad tím, co jsou ještě účelně vynaložené prostředky a co již nikoli. Pro jasnější ilustraci uvedl Miroslav Krejčík následující čísla:

Dostupnost 99 % znamená v průběhu roku výpadek 3,65 dne, za den se může jednat o 14,39 minut. IS datových schránek má dostupnost cca 99,9 %, to už garantuje výpadek v průběhu roku maximálně 8,76 hodiny a denně maximálně 86,33 sekund.

Pokud jde o Informační systém datových schránek, pak z očekávaného zákona o kyberbezpečnosti pro něj vyplývá celá řada změn a úprav. Pro každého provozovatele informačního systému by bylo patrně jednodušší stavět nový systém tzv. na zelené louce. Platí to i pro Informační systém datových schránek. To ale v současné situaci samozřejmě možné není, takže je nutné veškeré požadavky zákona zapracovat a aplikovat na stávající systém. V daném případě se jedná zatím pouze o odhady, ale pokud by měly být zapracovány všechny změny požadované zákonem a prováděcími předpisy a současně zachována dostupnost 99,9 %, pak mohou jednorázové náklady dosáhnout několika desítek miliónů korun.

Posledním momentem, kterým je v souvislosti se zákonem o kyberbezpečnosti Miroslav Krejčík znepokojen, je praktická aplikace případně uplatněného institutu vydání opravného a reaktivního opatření ze strany Národního bezpečnostního úřadu v případě, kdy shledá potřebu sjednání nápravy významného nebo kritického informačního systému veřejné správy. Jak Miroslav Krejčík uvedl, problém právního postavení státního podniku, který by byl provozovatelem takového typu informačního systému, spatřuje v tom, že má-li na něco reagovat a upravit, pak to většinou znamená projít procedurou zadávání veřejných zakázek, výběrového řízení a následné implementace. To podle jeho zkušeností rychlou reakci a okamžitou úpravu stavu příliš neumožňuje. ■

*Pozn. redakce:*
*Prezentace ve formátu PDF na www.egovernment.cz/kyber*

# Egovernment

elektronizace veřejné správy







Vše o elektronizaci veřejné správy – srozumitelně a zdarma:

**www.egovernment.cz**

# Boj s bezpečnostními hrozbami je nepřetržitý proces

***Nový portál kybernetické bezpečnosti KYBEZ chce zvyšovat informovanost o problematice bezpečnosti, upozorňovat na nebezpečí jejího podceňovaní a poskytovat řešení pro splnění povinností úřadů, které přináší nová legislativní úprava.***

Žijeme ve společnosti, která se spoléhá na informační systémy a začíná být na nich závislá. Ohrožení jejich funkčnosti může způsobit ohrožení fungování základní infrastruktury potřebné pro život. Nepříjemné je, že v důsledku vývoje ICT se neustále vyvíjí také bezpečnostní hrozby a vznikají nové.

Jako reakce na nová rizika pro chod státu a jeho institucí je v těchto měsících přijímán **zákon o kybernetické bezpečnosti,** který představuje nový právní rámec pro řešení velkých bezpečnostních incidentů. Tedy těch, jež přímo ohrožují kritickou síťovou infrastrukturu České republiky a její informační systémy. Prosazení připravovaného zákona o kybernetické bezpečnosti je zásadním počinem pro řešení bezpečnosti informačních systémů, a to nejen v oblasti organizací veřejné správy. Obchodní korporace a organizace, které budou podle tohoto zákona osobami povinnými, se musí včas seznámit, důsledně prostudovat a včasně realizovat požadavky v tomto zákoně uvedené.

## Jak a před čím se chránit?

**Smyslem kybernetické bezpečnosti je ochránit tzv. informační aktiva** – tedy prvky informačního systému (hardwarové komponenty, aplikační a systémový software, datové struktury atd.), které mají pro funkčnost IS a jeho provozovatele nezastupitelnou hodnotu. Na základě analýzy aktiv a jejich zranitelných míst musíme identifikovat možné bezpečnostní hrozby, které mohou napadnout konkrétní zranitelné místo konkrétního aktiva. To znamená popsat možnou hrozbu, včetně možného zdroje hrozby, případně úmyslnost a motivaci útočníka, vliv hrozby na jednotlivé atributy informační bezpečnosti aktiva (dostupnost, integritu, důvěrnost). Součástí analýzy hrozby by měl být i odhad pravděpodobnosti, případě možné frekvence hrozby.

***„Přínosem realizace projektu kybernetické bezpečnosti je dobrý pocit, že náš informační systém je provozován řádně, že pro dostupnost, integritu a důvěrnost informačního systému bylo uděláno vše potřebné.“***

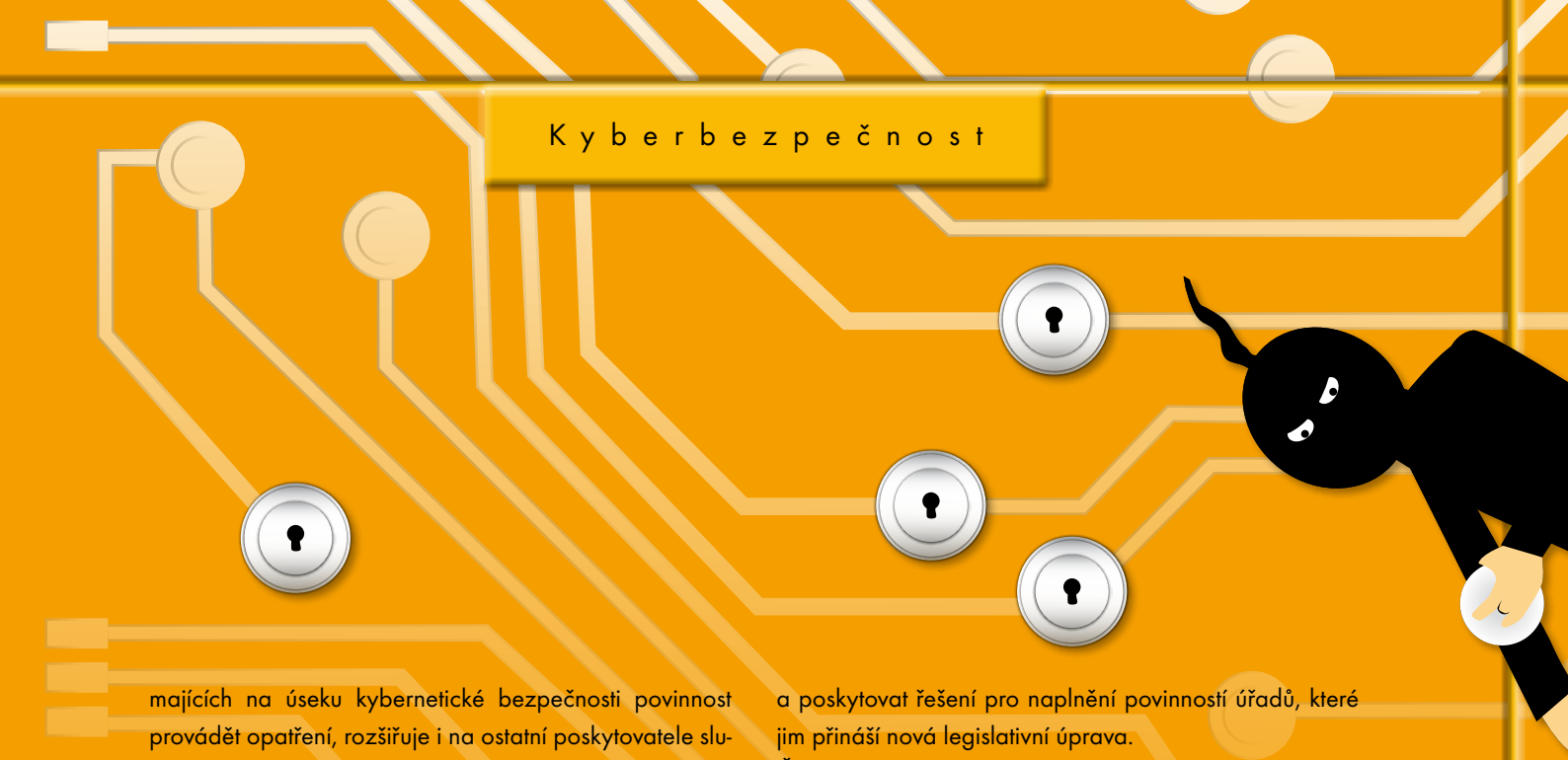
Situaci, kdy se hrozba pokusí působit na zranitelné místo s cílem ohrozit informační bezpečnost aktiva, se **říká bezpečnostní událost**. Pokud se působením hrozby naruší vlastnosti aktiva natolik, že dojde k narušení informační bezpečnosti, vzniká **bezpečnostní incident**. Bezpečnostní incident je tedy stav aktiva a bezpečnostní událost aktivita, která k tomuto stavu vede.

Pro pochopení tohoto rozdílu můžeme uvést tento příklad: neoprávněné otevření dveří do datového centra považujeme za bezpečnostní incident a činnosti, které k němu mohou vést (například útok hrubou silou, manipulace se zámkem, neoprávněné použití klíčů, uvedení oprávněné osoby v omyl atd.), budeme chápat jako bezpečnostní události.

## Týká se to i mě?

Zákon o kybernetické bezpečnosti označuje ***dotčené subjekty*** jako povinné osoby. Těmi jsou v tomto případě subjekty spravující specifické **informační a komunikační systémy**. Jde tedy jen o takové subjekty, které se podílejí na významné elektronické komunikaci či provozují kritickou infrastrukturu. Těmto organizacím budou za standardní situace ukládány konkrétní povinnosti k zavedení bezpečnostních opatření. Hlášení kybernetických bezpečnostních incidentů a provádění opatření se uloží pouze těm subjektům, jejichž systémy, sítě nebo služby mají zásadní význam pro fungování státu nebo informační společnosti.

Nejedná se tedy o poskytovatele obsahu, jednotlivé uživatele ani provozovatele jiných služeb. Pouze při vyhlášení stavu kybernetického nebezpečí se okruh subjektů,



majících na úseku kybernetické bezpečnosti povinnost provádět opatření, rozšiřuje i na ostatní poskytovatele služeb a správce systémů a sítí.

Co pro mě tedy znamená zavést kybernetickou bezpečnost? V první řadě zjistit, jaké slabiny má námi provozovaný informační systém, jaká mu hrozí rizika, a navrhnout, jakými opatřeními a do jaké míry chceme tato rizika eliminovat. Potom je třeba navržená opatření realizovat, sledovat jejich dopady a snažit se dosažený stav udržet a dále zlepšovat. Optimální variantou je zavedení systému řízení bezpečnosti informací podle norem řady ISO 27000.

***„Při vyhlášení stavu kybernetického nebezpečí se okruh dotčených subjektů rozšiřuje."***

Přínosem zavedení je vědomí, že náš informační systém je provozován řádně, že pro dostupnost, integritu a důvěrnost informačního systému bylo provedeno všechno, co bylo potřeba udělat. Zavedením bezpečnostních opatření chráníme nejen sebe a náš informační systém, ale díky našemu zodpovědnému přístupu chráníme i informační systémy jiných provozovatelů dostupné v internetu. A v neposlední řadě splníme požadavky zákona o kybernetické bezpečnosti.

## KYBEZ nabízí pomoc

Snad více než v jiných oblastech platí pro sféru kybernetické bezpečnosti doporučení nechat si zpracovat analýzu rizik, návrh bezpečnostních opatření i jejich realizaci od odborníků, kteří se danou problematikou léta zabývají. I proto vznikl projekt KYBEZ (www.kybez.cz). Jedná se o volné sdružení komerčních firem z oblasti informačních technologií a akademických institucí, jehož cílem je zvyšovat informovanost o problematice kybernetické bezpečnosti, upozorňovat na nebezpečí jejího podceňování a poskytovat řešení pro naplnění povinností úřadů, které jim přináší nová legislativní úprava.

Členové sdružení jsou připraveni pomoci orgánům veřejné moci i dalším zainteresovaným subjektům, jež to myslí s bezpečností vážně, ve splnění požadavků, které na ně zákon o kybernetické bezpečnosti klade.

## 10 důvodů, proč se obrátit na sdružení KYBEZ?

- Známe IT prostředí ve více než 6000 organizacích veřejné správy i komerčních organizací.
- Disponujeme zkušenostmi s realizací projektů s vysokými nároky na bezpečnost (MO ČR, MV ČR).
- Máme více než 20 let praxe s poradenstvím v oblasti informační bezpečnosti.
- Vytvořili jsme metodiku postupu zavádění systému řízení informací (ISMS) dle ISO/IEC 27001.
- Dokážeme zajistit komplexně celou realizaci kybernetické bezpečnosti ve Vaší organizaci.
- Disponujeme odborníky ze soukromé i akademické sféry.
- Jsme schopni důsledně analyzovat Vaše informační aktiva, zranitelná místa a identifikovat případné hrozby.
- Nabízíme pouze špičkové, odzkoušené a přitom cenově dostupné komponenty.
- Máme široké zkušenosti se vzděláváním IT specialistů i běžných uživatelů v oblasti informační bezpečnosti.
- Jsme schopni Vám pomoci i s administrací projektů, podklady pro výběrová řízení a žádostmi o finanční zdroje.

Vladimír Přech

GORDIC®

# Bezpečnostní a provozní standardy informačních systémů

***ICT UNIE přistupuje aktivně k formování strategie informační společnosti a ke strategickému rámci 2014+ uplatnila řadu námětů, mimo jiné v oblasti informační bezpečnosti. Přispívá k vytváření povědomí o důležitosti zajištění bezpečnosti informací – podílí se na pořádání odborných akcí a spolupracuje s dalšími organizacemi tak, aby podpořila vznik kvalitní, odolné a bezpečné informační infrastruktury České republiky. Příkladem může být spolupráce na semináři zabývajícím se tématem elektronické identity (bližší informace o této akci viz rámeček).***

Náměty, které ICT UNIE předložila vládě ČR ke zvážení, míří zejména do oblasti bezpečnostních a provozních standardů informačních systémů, které na jednu stranu podstatně ovlivňují odolnost jednotlivých segmentů infrastruktury, na druhou stranu znamenají nezřídka náklady, jež je třeba odůvodnit z celospolečenského hlediska.

V deklaraci se praví, že občané se nebudou aktivně účastnit elektronické komunikace s veřejnou správou, pokud nebudou mít jistotu, že se na sdílené služby mohou plně spolehnout a že jejich data budou v bezpečí před různými formami počítačové trestné činnosti i dalšími kybernetickými hrozbami. Orgány veřejné moci i komerční společnosti potřebují pro poskytování sdílených služeb prostředí, které je postavené na bezpečnostních standardech a které má jasně stanovená bezpečnostní a provozní pravidla.

Cílem je prosadit taková opatření a pravidla, jež odpovídají rizikům a specifikům dané sdílené služby na dané vrstvě architektury a umožní dosažení odpovídající úrovně důvěrnosti, integrity a dostupnosti sdílené služby z pohledu jejího užití (uživatele).

**Návrh bezpečnostních a provozních standardů bude vycházet zejména z těchto dokumentů:**

- Strategie pro oblast kybernetické bezpečnosti ČR na období 2012–2015 (Strategie a Akční plán pro tuto strategii), schválená usnesením vlády č. 364/2012;
- Zákon č. 101/2000 Sb., o ochraně osobních údajů, č. 365/2000 Sb., o informačních systémech veřejné správy (ISVS) a vyhláška č. 529/2006 v oblasti požadavků na bezpečnost ISVS;
- připravovaný zákon o kybernetické bezpečnosti;
- dokumenty EU-ENISA, připravované nařízení EU „General Data Protection Regulation" a připravovaná směrnice EU „Network and Information Security";
- aplikovatelné standardy v oblasti bezpečnosti informačních systémů (řada ISO 27000) a dále doporučení průmyslových asociací v oblasti ICT služeb;
- zajištění bezpečnosti sdílených služeb v jiných zemích EU a příklady hodnocení dopadu ztráty důvěrnosti, integrity a dostupnosti služby na výkon veřejné správy, občany i soukromou sféru.

Na základě analýzy rizik sdílené služby bude stanoveno několik úrovní možných dopadů (Impact Levels – IL) na výkon funkce úřadu při selhání nebo kompromitaci dané sdílené služby na dané vrstvě architektury. Každá sdílená služba bude začleněna do některé úrovně možných dopadů (IL). Jednotlivé úrovně IL budou mít definovanou sadu povinných bezpečnostních požadavků a opatření (většího nebo menšího rozsahu dle IL). Rozsah požadovaných bezpečnostních opatření tedy bude odstupňovaný podle úrovní dopadů (IL) vyplývajících z možné ztráty důvěrnosti, integrity a dostupnosti dané sdílené služby. Vyšší úrovně požadavků budou kompatibilní s požadavky připravovaného zákona o kybernetické bezpečnosti (jedná se o systémy klasifikované do kategorií „významné" či „kritické informační infrastruktury", pro ty stanoví zákon a jeho prováděcí vyhláška vlastní požadavky).

Dokumenty „Strategie pro oblast kybernetické bezpečnosti ČR na období 2012–2015" a „Akční plán" pro tuto strategii budou aktualizovány po přijetí zákona o kybernetické bezpečnosti. Cílem strategického rámce 2014+ je umožnit konkrétním příjemcům předkládat projekty, které vycházejí z výše uvedené strategie kybernetické bezpečnosti. Tyto projekty by mohly zahrnovat jak možnost nákupu technického vybavení souvisejícího s realizací strategie, tak zajištění výukových a školicích programů v ČR i v zahraničí.

Při projektování a implementaci změn nastíněných ve strategickém rámci tak budou důsledně zohledňovány specifické úkoly v rámci veřejné správy plněné složkami působícími v oblasti zajišťování vnitřní i vnější bezpečnosti státu, veřejného pořádku apod., jako je policie, zpravodajské služby, Generální inspekce bezpečnostních sborů a obecně soustava orgánů činných v trestním řízení, celních orgánů či obecní policie.

**Odborné kolokvium Elektronická identita:**

Asociace AFCEA společně s Fakultou bezpečnostního managementu Policejní akademie ČR zorganizovala 23. dubna letošního roku seminář o přístupu občanů k personalizovaným službám. Hlavním cílem akce bylo posouzení a vyjasnění strategie elektronické identity osob v České republice ve vztahu k požadavkům chystaného nařízení Evropské unie eIDAS a ve vazbě na koncepci eGovernmentu v ČR.

Úvodní projev přednesla náměstkyně ministra vnitra pro veřejnou správu a legislativu Adriana Krnáčová na téma významu, posledního vývoje a očekávaných dopadů evropského „nařízení o elektronické identifikaci a službách vytvářejících důvěru na vnitřním trhu", kterému se ve zkratce říká eIDAS. Následoval příspěvek vymezující oblast elektronické identity s vyšší úrovní důvěryhodnosti, který přednesl člen pracovní skupiny Kybernetická bezpečnost AFCEA Zdeněk Jiříček. Vizi elektronické identifikace pak představil digitální šampion a hlavní architekt eGovernmentu v ČR Ondřej Felix. Obsahem jeho vystoupení byla především problematika pokrytí požadavků na ověřenou elektronickou identifikaci na bázi základních registrů jak uvnitř veřejné správy v ČR (ze zákona), tak i vůči soukromému sektoru a přeshraničním službám (na přání a se souhlasem subjektu dat).

Následné diskusní panely moderoval Jaroslav Pejčoch, člen Řídícího výboru pro informační společnost ICT UNIE a současně místopředseda pracovní skupiny Kybernetická bezpečnost AFCEA. První panel se věnoval zejména celkové koncepci interoperability elektronických identit v rámci eIDAS a právních důsledků jeho implementace v prostředí České republiky. Druhý panel se zaměřil na příležitosti související s ověřenou elektronickou identifikací pro soukromý sektor. Aktivními účastníky diskuse byli kromě již zmíněného Ondřeje Felixe také např. ředitel odboru bezpečnostní politiky Ministerstva práce a sociálních věcí Aleš Špidla, zástupce České bankovní asociace Pavel Kolář nebo místopředseda představenstva ICT UNIE Zdeněk Pilz.

# Intel: neobyčejně všestranné bezpečné řešení pro virtualizaci a cloud

## ...aneb začněte řešit bezpečnost již na hardwarové úrovni

***Oddělení IT dnes často musejí provádět více úkonů s méně prostředky: starat se o více uživatelů, širší škálu zařízení a větší objemy dat. Díky platformě založené na procesorech Intel® Xeon® řady E5-2600 v2 dokážete ve svém datovém centru virtualizovat jakoukoli pracovní zátěž a současně vytvořit flexibilnější, odolnější a bezpečnější prostředí pro efektivnější a celkově méně nákladnou podporu širokého spektra klíčových firemních aktivit. Procesory Intel® Xeon® řady E5-2600 v2 tvoří základ flexibilní a efektivní infrastruktury datového centra. Jsou navrženy pro dosažení nejlepší kombinace výkonu, vestavěných funkcí a nákladové efektivity. Více jader, více paměti, vyšší míra integrace a větší šířka pásma – to jsou vlastnosti, které tyto procesory nabízejí a které lze využít v datových centrech nové generace.***

### Procesory Intel Xeon řady E5-2600 v2 umožní:

- **posílit bezpečnost a zajistit shodu** pomocí důvěryhodné platformy integrující celé Vaše datové centrum, ochrany dat a aplikací s využitím bezpečnostních technologií, které jsou připraveny pro virtualizaci, a s využitím rychlého šifrování dat s minimálními nároky na výkon systému;
- **snížit náklady na IT konsolidací** pracovní zátěže na malý počet serverů založených na procesorech Intel Xeon řady E5-2600 v2 a přechodem na unifikovanou síť Ethernet 10 Gigabit. Využití serverů lze zvýšit z 5–15 procent až na 60–80 procent a současně lze výrazně snížit požadavky na síťové adaptéry, switche a kabeláž;
- **optimalizovat výkon a energetickou účinnost** v široké škále podnikových aplikací a umožnit tak řešit i ty nejkomplexnější problémy a současně snížit provozní náklady;
- **zajistit nepřerušenou dostupnost IT prostředků** pomocí vysoce spolehlivých serverů, jednoduchého, plně automatizovaného sledování stavu infrastruktury a systému pro převzetí služeb při havárii a následné obnovení činnosti. Funkce Intel Flexmigration v kombinaci s virtualizačním softwarem umožňuje provést živou migraci a přitom nevyžaduje sdílené úložiště, takže můžete odstranit i plánované odstávky pro údržbu hardwaru přesunem pracovní zátěže na jiné servery;
- **zlepšit kvalitu programového vybavení** testováním nových aplikací, aktualizací a záplat před nasazením

do ostrého provozu v izolovaném prostředí (sandboxu) virtuálního stroje. Pracovní prostředí můžete naklonovat téměř okamžitě, což umožňuje provádět testování v reálných podmínkách a vyhnout se tak problémům se softwarem, které by jinak mohly způsobit selhání klíčových podnikových aplikací.

Podívejme se ovšem blíže na jednoho ze zákazníků společnosti Intel a konkrétní nasazení Intel technologií. Společnost Cloud4com byla založena na jaře roku 2010 s cílem poskytovat cloudová řešení středním a velkým firmám v České republice. Jejím stěžejním produktem je služba Virtual Private Data Center*. Ta vychází z konceptu poskytování infrastruktury formou služby (IaaS), kdy zákazníci získávají podle svých potřeb vzdálený přístup k prostředkům, které by v klasickém řešení musely být součástí jejich vlastních datových center. Společnost Cloud4Com si již od samého počátku uvědomovala, že potřebuje jasnou představu o tom, co podniky od cloudových služeb vyžadují, aby tak mohla připravit z obchodního hlediska atraktivní nabídku a opatřit si pro své datové centrum odpovídající technologii, díky které bude schopná takové služby poskytovat. Pro implementaci bylo vybráno řešení Cisco Unified Computing System s 12 procesory Intel Xeon řady E5-2600. To umožnilo vybudovat efektivní, plně automatizovanou infrastrukturu datového centra, která představuje výkonnou, robustní a flexibilní platformu potřebnou pro služby virtuálního privátního datového centra. Procesory Intel Xeon řady E5-2600 jsou vybaveny vestavěnou podporou virtualizovaných prostředí, a proto je řešení pro cloudové služby s jejich využitím výkonnější a jednodušší. S využitím referenční architektury z programu Intel Cloud Builders společnost vybudovala systém podle konceptu Unified Networking založený na technologii 10 GbE, čímž dále zvýšila celkovou výkonnost infrastruktury svého datového centra.

## Bezpečnost infrastruktury díky správné volbě hardware

Společnost Cloud4com jako první Cloud Provider v České republice využívá klíčové technologie Intel Trusted Execution Technology (TXT) a HyTrust Appliance pro zajištění důvěryhodného (Trusted) prostředí systémů na platformě Intel Xeon. Může svým zákazníkům garantovat, že prostředí, kde provozují své virtualizované systémy a aplikace, splňuje přísné požadavky na zabezpečení konfigurace prostředí, dále je zajištěna jeho ochrana proti útokům a dodržování certifikovaných procesů při správě tohoto prostředí kvalifikovanými pracovníky.

Díky technologii Intel® Trusted Execution Technology (Intel® TXT) lze provést kontrolu softwaru pro správu virtuálního stroje ihned při jeho spuštění a ověřit ho na základě pravidel uložených v modulu Trusted Platform Module (TPM). Místo odrážení jednotlivých stále dokonalejších pokusů o napadení systému pomáhá tato strategie zajistit, že systém vždy nabootuje do určeného funkčního stavu a zabrání tak neoprávněným zásahům, ať už v důsledku nesprávné konfigurace, nebo útoku. Tuto technologii důvěryhodné platformy podporuje více než desítka předních dodavatelů řešení v oblasti zabezpečení a zajištění shody. Stává se tak výrazným vylepšením prostředí správy, řízení rizik a zajištění shody.

Další bezpečnostní technologie integrované do procesorů Intel Xeon řady E5-2600 zahrnují Supervisor Mode Execution Protection, která pomáhá chránit proti sofistikovaným útokům směřujícím k získání vyšší úrovně systémových oprávnění, a dále Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), která umožňuje rychlé šifrování s nízkými nároky na výkon systému. Technologie Intel AES-NI dokáže urychlit šifrování až desetinásobně, takže můžete šifrovat citlivá data a komunikaci v celém datovém centru, aniž by došlo ke zpomalení běhu aplikací nebo zvýšení nákladů. Lze také zajistit zjednodušenou antivirovou ochranu s nízkými nároky na výkon systému a umožnit rychlé klonování pracovního prostředí pro potřeby testování záplat a aktualizací v reálných podmínkách.

Pokročilé funkce, které cloudové výpočetní prostředí nabízí, můžete využívat již nyní. Pomohou Vám poskytovat lepší a spolehlivější služby, zvýšit produktivitu a snížit náklady. Poskytnou Vám také kompatibilní základ, který Vám umožní reagovat na vývoj modelů cloudových výpočetních prostředí v budoucnu.

Kontakt pro více informací:
Petr Ulvr, petr.ulvr@intel.com

# Podpora eGovernmentu v krajích

***V měsíci květnu byl ukončen projekt „Koordinační centrum pro zavádění eGOV v územní veřejné správě", financovaný z prostředků Operačního programu Lidské zdroje a zaměstnanost. Smyslem projektu byla podpora a zajištění jednotného přístupu při implementaci eGovernmentu v jednotlivých krajích, vytvoření sdíleného znalostního centra a realizace přímé podpory zástupcům krajských organizací při implementaci eGovernmentu.***

Vlastní projekt byl rozdělen do čtyř aktivit, jejichž logická návaznost umožnila vzájemně provázat jednotlivé výstupy. V úvodu realizace projektu byly se zástupci krajů – na základě provedené analýzy aktuálního stavu a workshopů – definovány minimální, optimální a maximální požadavky na strukturu eGovernmentu v krajích. Tyto požadavky byly vtěleny do podoby koncepčních dokumentů pro oblast řízení a koordinaci eGovernmentu v předem definovaných oblastech. Výstupem této fáze projektu jsou koncepce pokrývající oblast bezpečnosti dat a informací, nakládání s majetkem, principů nakládání s daty (problematika autorského zákona), architektury řízení v návaznosti na IT systémy, procesní model řízení a rozvoje eGovernmentu a metodiky řízení implementace eGovernment projektů pro kraje.

V návaznosti na vytvořené koncepční dokumenty byla dále zpracována interní řídicí dokumentace pro jednotlivé kraje, kdy strategické a koncepční cíle a výstupy (definované a vytvořené v předchozí etapě projektu) byly přeneseny do konkrétních činností a procesů. Výsledkem je sada praktických návodů, manuálů a příruček pro posouzení kompatibility eGovernment strategie kraje, akční plány implementace eGovernmentu a checklisty, směrnice projektového řízení, příručka kvality a kontroly projektů a služeb eGovernmentu, příručky pracovních postupů, relevantní směrnice, návrh komunikačního plánu, definice postupů pro zjišťování spokojenosti klientů služeb eGOV a vzorové dokumenty a formuláře pro sledování stavu implementace eGovernmentu v rámci kraje.

Průběžně byla poskytována odborná podpora ve vazbě na centrální koordinaci projektů realizovaných ze strany jednotlivých krajů prostřednictvím workshopů a sdíleného znalostního centra zveřejněného na webových stránkách Asociace krajů ČR na adrese **www.asociacekraju.cz/akcr/projekty/egov/**, kde je možné rovněž získat veškeré výstupy projektu.

*Radek Polma, ředitel kanceláře Asociace krajů*

*Mgr. Bohdan Urban, ředitel odboru veřejné správy a eGovernmentu MV ČR*

*Ing. Rostislav Mazal, MMR*

Na závěr projektu se konala odborná konference pro zástupce krajů, jejímž cílem bylo nejen prezentovat výstupy projektu jako takového, ale zhodnotit také míru dosažení původních představ o realizaci eGovernmentu na úrovni krajů i veřejné správy obecně a představit zástupcům krajů vize Ministerstva vnitra ČR a možnosti čerpání finančních prostředků v novém programovém období. Za účasti zástupců Ministerstva vnitra, Ministerstva pro místní rozvoj, Ministerstva práce a sociálních věcí, Správy základních registrů, ale i Svazu měst a obcí ČR a samozřejmě Asociace krajů ČR vystoupili např. **Mgr. Bohdan Urban**, ředitel odboru veřejné správy a eGovernmentu MV ČR, **Ing. Rostislav Mazal** z MMR ČR nebo **Mgr. Zdeněk Zajíček**, duchovní otec centrálních eGovernment projektů.

V závěrečné panelové diskuzi byly představeny požadavky krajů, měst a obcí na centrální projekty eGovernmentu a ze strany zástupců MV ČR byla přislíbena vyšší míra informování a spolupráce s územní veřejnou správou. Projekt bude dále rozvíjen v rámci další činnosti Asociace krajů a koordinačního střediska složeného z pracovníků asociace a členů komise rady AK ČR pro informační technologie ve veřejné správě.

*Mgr. Zdeněk Zajíček*

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
OPERAČNÍ PROGRAM LIDSKÉ ZDROJE A ZAMĚSTNANOST
ASOCIACE KRAJŮ ČESKÉ REPUBLIKY
PODPORUJEME VAŠI BUDOUCNOST
www.esfcr.cz
Projekt je financován z prostředků Evropského sociálního fondu prostřednictvím Operačního programu Lidské zdroje a zaměstnanost a jiných národních veřejných finančních prostředků

# Konference ISSS 2014 – návštěva z Bruselu, zájem o přednášky, absence jasnějších vizí ...

***Sedmnáctý ročník konference ISSS/V4DIS – jedné z největších akcí zaměřených na informatizaci a reformu veřejné správy v celém regionu střední a východní Evropy – je od úterý 8. dubna minulosti. Během dvoudenního programu konference, která se jako obvykle konala v královéhradeckém kongresovém centru Aldis, se uskutečnilo přibližně 200 přednášek, prezentací a diskusních setkání, ve výstavní části se představilo přes 100 dodavatelů technologií a služeb, institucí a dalších subjektů. Počet registrovaných hostů konference opět překročil 2 tisícovky. Mezi hosty letos zářili vysocí představitelé Evropské unie – místopředsedkyně EK a komisařka pro digitální agendu Neelie Kroes a místopředseda Evropského parlamentu Oldřich Vlasák. Akce se konala pod osobní záštitou předsedy vlády ČR Bohuslava Sobotky, vicepremiéra Pavla Bělobrádka, který byl z přítomných politiků nejaktivnější a absolvoval prakticky celý pondělní program a zapojil se do řady diskusí a jednání, ministra vnitra Milana Chovance, ministryně pro místní rozvoj Věry Jourové a Asociace krajů ČR. Visegrádskou konferenci V4DIS zaštítil místopředseda Senátu Parlamentu ČR Přemysl Sobotka a jedním z významných hostů byla i ředitelka Mezinárodního visegrádského fondu (IVF) Karla Wursterová.***

Nejsledovanější částí programu bylo jako obvykle pondělní dopolední slavnostní zahájení ve Velkém sále, jehož **moderátorem byl opět Jakub Železný**. **Po úvodních zdravicích vystoupili s klíčovými projevy Neelie Kroes, Oldřich Vlasák a Pavel Bělobrádek.** Šéf poradců premiéra Vladimír Špidla pak přečetl krátkou zdravici předsedy vlády **Bohuslava Sobotky**, který se kvůli pracovnímu vytížení nemohl slavnostního zahájení zúčastnit. Oficiální část zahájení uzavřel první náměstek ministra vnitra **Jan Sixta**.

V oblíbené „kavárenské" diskusi, která vyplnila následující hodinu, zazněly názory řady osobností, mezi nimiž nechyběla ministryně pro místní rozvoj **Věra Jourová**, náměstci ministra vnitra **Adriana Krnáčová** a **Jaroslav Strouhal**, první náměstek ministra financí **Lukáš Wagenknecht**, náměstek ministra zdravotnictví **Tom Philipp**, náměstkyně ministra práce a sociálních věcí **Iva Merhautová**, hejtman Královéhradeckého kraje **Lubomír Franc**, předseda ČÚZK **Karel Večeře**, předseda ČTÚ **Jaromír Novák**, digitální šampion ČR a architekt

*Zahájení konference ISSS 2014 sledoval tradičně nabitý Velký sál*

*Hlavní hvězdou programu byla místopředsedkyně EK Neelie Kroes*

českého e-governmentu **Ondřej Felix**, místopředseda PS Parlamentu ČR **Jan Bartošek**, poslanci **Milada Halíková** a **Ivan Pilný** nebo nový generální ředitel České pošty **Martin Elkán**. Podnikatelský sektor zastupovali prezident ICT Unie **Svatoslav Novák**, ředitel úseku komunálního financování České spořitelny **Milan Hašek**, generální ředitelka Microsoft ČR **Biljana Weber**, generální ředitel IBM **Branislav Šebo**, generální ředitel Cisco ČR **Jiří Devát** a ředitel konference ISSS/V4DIS **Tomáš Renčín**.

Komisařka Neelie Kroes ve svém projevu zdůraznila potřebu sladění české informatizace veřejné správy s hlavními trendy Evropské unie a mimo jiné poznamenala: *„Využijte možností, které vám EU nabízí, zvláště pak příležitosti investovat do budoucnosti – do lepších služeb na mezinárodní úrovni, do veřejných zakázek, elektronizace zdravotnictví apod. Existuje řada programů, z nichž lze financovat další rozvoj – například Horizont 2020 pro oblasti výzkumu a inovací nebo nový program Connecting Europe Facility určený pro online služby."*

Další program konference se tradičně věnoval především aktuálním otázkám rozvoje e-governmentu a významnou roli zde hrály prezentace Ministerstva vnitra ČR. První náměstek Jan Sixta už v úvodním projevu zdůraznil hlavní koncepci ministerstva: *„Abychom dosáhli lepší, přívětivější a rychlejší veřejné správy, musíme se zcela pevně držet základních bodů. Tedy vycházet z toho, že moderní technologie jsou pouze prostředkem, ne cílem. Zprovoznit pouze ty systémy, které přímo a bez oklik povedou ke zjednodušení komunikace občanů a firem s veřejnou správou i mezi úřady. Provozovat pouze takové systémy, které budou prospěšné pro občany, přebujelou veřejnou správu zjednoduší a dále nezatíží."*

V následujících prezentacích se zástupci MV zaměřili hlavně na nejdůležitější stávající či budoucí projekty tuzemského e-governmentu, jako jsou systém základních registrů, úplná elektronická podání, e-identita v mezinárodním měřítku, eSbírka a eLegislativa, procesní modelování agend, přístupnost informací pro hendikepované či další strategie rozvoje.
V programu konference ale zaujala i další témata, jako například e-government v evropském kontextu, elektronizace zdravotnictví a sociálních služeb, opendata, problematika veřejných zakázek, digitalizace a archivace dokumentů, strategie 2014+ a veřejná správa, dopady zákona o kybernetické bezpečnosti nebo systémy GIS a související problematika.


*Do diskusí se zapojoval i ředitel konference Tomáš Renčín*

Během dvou dnů konference se tradičně uskutečnilo několik dalších doprovodných akcí, jako například ICT summit zástupců ICT průmyslu a státního sektoru, zaměřený

*Mezi doprovodnými akcemi nechyběl ani tentokrát ICT Summit*

na konkurenceschopnost tohoto segmentu i aktuální problémy. Letos byl jedním z důležitých bodů podpis společného memoranda o spolupráci ICT Unie a České bankovní asociace. Dále proběhlo setkání poslaneckých klubů, zasedání komisí Rady Asociace krajů ČR a Gremia ředitelů krajských úřadů, diskuse zástupců akademické obce a odborníků zaměřená na lepší sepětí vědy, výzkumu a na spolupráci s veřejnou správou či setkání Sdružení tajemníků obecních a městských úřadů.

## Soutěže

V průběhu nedělního večera a pondělního programu byly tradičně vyhlášeny výsledky populárních soutěží a předána na ocenění. Ocenění Český zavináč letos získalo sdružení CZ.NIC, a to za osvětovou činnost v oblasti internetu a elektronických služeb. Do mezinárodní části konference patřilo vyhlášení soutěže Eurocrest a svoji chvíli slávy si prožili vítězové letošního ročníku soutěže JuniorErb, kteří měli možnost téměř hodinu diskutovat s komisařkou Neelie Kroes a poté převzali z jejích rukou a za přítomnosti ředitelky Mezinárodního visegrádského fondu Karly Wursterové pamětní listy. Během pondělního galavečera pak přišla řada na vítěze soutěže Zlatý erb a Biblioweb (kompletní výsledky všech soutěží jsou k dispozici na www.isss.cz) a náměstkyně ministra vnitra pro veřejnou správu Adriana Krnáčová předala zvláštní cenu ministra vnitra za přínos k rozvoji informačních a komunikačních technologií ve veřejné správě za rok 2013. Držitelem ceny se stal Liberecký kraj, a to za „podporu otevřených dat na Portálu veřejné správy".

*Zájem byl letos i o expozice dodavatelů ...*

## Organizátoři a partneři

Hlavním pořadatelem konference ISSS/V4DIS byla jako obvykle společnost Triada, spolupořadateli pak sdružení Český zavináč, společnost Ponca a časopis Obec a finance. Na organizaci visegrádské konference se významně podílel Kraj Vysočina. Mezi spolupracujícími subjekty byly ICT Unie, Hradec Králové, Kladno, Královéhradecký kraj, Calendarium Regina, STMOÚ – Sdružení tajemníků městských a obecních úřadů a jako analytický partner společnost IDC CEMA.

Generálním partnerem konference byla Česká spořitelna, hlavními partnery společnosti ATOS, CISCO, Česká pošta, IBM, ICZ a VITA software, hlavním odborným partnerem Microsoft, partnery pak Accenture, Asseco, AutoCont, AV Media, Citrix, Fujitsu, Gordic a HP. Partnery odborných bloků se staly ČIMIB (Český institut manažerů informační bezpečnosti), T-Mobile, T-Systems a VEEAM, na jejím programu se pak podílela řada ministerstev a státních organizací i samospráv.

## Za rok nashledanou

Osmnáctý ročník konference ISSS/V4DIS se uskuteční ve dnech 20.–21. dubna 2015 opět na stejném místě. Doufejme, že bude ještě otevřenější – alespoň z pohledu průhlednějších vyjádření a většího odkrytí karet politiků. To byla snad jediná výhrada účastníků k letošnímu ročníku. Přes kvalitní program a dobrou organizaci chyběly zřetelnější obrysy toho, kam se bude český e-government dále ubírat. Veřejná správa totiž potřebuje konkrétní informace a jasně definované kroky. Absenci toho nenahradí ani nejatraktivnější návštěva z Bruselu.

**Více informací včetně kompletního archivu minulých ročníků lze najít na www.isss.cz.**

Prokop Konopa

isss
Internet ve státní správě a samosprávě
LOCAL AND GLOBAL INFORMATION SOCIETY

Egovernment

elektronizace veřejné správy

# THE BEST 2014

Přehled nejzajímavějších projektů elektronizace veřejné správy v ČR.


Nový partner = nová soutěžní kategorie, více informací na **www.egovernment.cz/best**

# Projekt „Rozvoj služeb eGovernmentu v Ústeckém kraji I., II., III., IV. a VI.“

***Ústecký kraj od 23. 4. 2010 do 31. 7. 2014 realizuje projekt „Rozvoj služeb eGovernmentu v Ústeckém kraji I., II., III., IV. a VI.“, registrační číslo CZ.1.06/2.1.00/08.07230, který je financován v rámci integrovaného operačního programu prioritní osa 6.2 Zavádění ICT v územní veřejné správě – cíl konvergence, oblast podpory 6.2.1 Zavádění ICT v územní veřejné správě, výzva 08. Hlavním cílem projektu je vytvoření technologického centra, které má posílit infrastrukturu Ústeckého kraje pro bezpečné zpracování, uchování a přenášení dat, zefektivnění a zkvalitnění procesů interních i externích, transparentnost výkonu a modernizaci chodu veřejné správy. Projekt se skládá ze dvou větších celků, a to z Digitální mapy veřejné správy (DMVS) a samotného Technologického centra Ústeckého kraje (TCÚK).***

Část DMVS realizoval dodavatel T-Mapy spol. s r.o. Pro realizaci DMVS, části účelové katastrální mapy (ÚKM), uzavřel Ústecký kraj dohodu o spolupráci s Katastrálním úřadem pro Ústecký kraj, kde byly stanoveny technické a organizační podmínky při pořizování, správě a aktualizaci ÚKM Ústeckého kraje. Ústecký kraj nechal zpracovat účelovou katastrální mapu za vybraná území a předal ji Katastrálnímu úřadu pro Ústecký kraj. Dále byl dne 13. 8. 2013 spuštěn produkční provoz Geoportálu ÚAP, který obsahuje mapové projekty pro různá témata, a to povodňové plány, krizové řízení, dopravu, životní prostředí, cestovní ruch apod., a nástroje pro tvorbu a údržbu územně analytických podkladů. Geoportál **geoportal.kr-ustecky.cz/gs** má veřejnou nezabezpečenou část, kde jsou tematické mapy a veřejně dostupné informace, a zabezpečenou část pro registrované uživatele, kde jsou aplikace územního plánování, výdej dat a georeporty. Geportál ÚAP je již téměř rok v produkčním provozu, přičemž Ústecký kraj průběžně aktualizuje a rozšiřuje obsah webových stránek.

Část TCÚK realizuje dodavatel scanservice a.s. s hlavními subdodavateli CDL System a.s. a ICZ a.s. Realizace Technologického centra ÚK se skládá z části Technologické centrum (TCÚK), což zahrnuje výstavbu primárního a sekundárního datového centra, části Integrace úřadu (INT), části Elektronická spisová služba (SSL), části Digitalizace a ukládání (DA), která se skládá z podčástí Krajská digitalizační jednotka (KDJ), Krajský digitální repozitář (KDR) a Krajská digitální spisovna (KDS). Realizace TCÚK byla zahájena 18. 3. 2013.

*Knižní skener*

**V 1. etapě TCÚK** byl pořízen HW a systémový SW pro výstavbu hlavního a záložního datového centra, včetně Identity managementu. Datová centra byla převzata do provozu ke dni 30. 8. 2013 a byl zahájen zkušební provoz. V rámci zkušebního provozu byl proveden komplexní disaster recovery test simulující možné stavy technologického centra vzniklé při výpadcích jednotlivých komponent. Na vybudovaném datovém centru byla implementována a spuštěna do ostrého provozu hostovaná spisová služba e-Spis LITE pro 138 organizací zřizovaných Ústeckým krajem.

**Ve 2. etapě TCÚK** byl pořízen HW a SW pro část Digitalizace a ukládání (DA). Dne 5. 12. 2013 byly dokončeny úpravy místnosti č. 0024 pro Krajskou digitalizační jednotku. Postupně byl dodán knižní skener, instalovány PC, notebook pro zpracování dat pořízených v KDJ, 3D skener a velkoplošný skener. Dne 17. 1. 2014 bylo Ústeckým krajem převzato funkční digitalizační pracoviště. Od převzetí techniky

do zkušebního provozu poskytuje Ústecký kraj techniku pořízenou pro využití organizacemi zřizovanými Ústeckým krajem. Knižní skener využívá především Severočeská vědecká knihovna p.o. v Ústí nad Labem k digitalizaci svého knižního fondu. 3D skener si v první fázi zapůjčil Ústav archeologické a památkové péče Severozápadních Čech v.v.i. pro naskenování třírozměrných objektů. Současně s vybudováním KDJ byl pořízen SW pro realizaci Krajského digitálního repozitáře a Krajské digitální spisovny, což jsou garantovaná úložiště dat pořízených především v rámci digitalizačního pracoviště a spisových služeb.

*Velkoformátový skener*

**Ve 3. etapě TCÚK** byly realizovány a spuštěny do zkušebního provozu veškeré integrace nově pořízených i stávajících informačních systémů. Především se jedná se o integraci Identity managementu s personálně mzdovým systém FLUX, spisovou službou úřadu EZOP, hostovanou spisovou službou e-Spis LITE a ekonomickým systémem MS Navision, dále se jedná o synchronizaci agend a činnostních rolí z registru práv a povinností (RPP) a synchronizaci uživatelů do jednotného identitního prostoru (JIP). Byla provedena integrace Krajské digitalizační jednotky s Krajským digitálním repozitářem, což reprezentuje produkt DESA edice DER a systém Kramerius pro prezentaci monografií a periodik. Byla realizována integrace hostované spisové služby e-Spis LITE a spisové služby EZOP s Krajskou digitální spisovnou, což reprezentuje produkt DESA edice DES. Zkušební provoz systémové integrace všech subsystémů technologického centra bude dokončen k 18. 7. 2014.

*3D skener*

Projekt **„Rozvoj služeb eGovernmentu v Ústeckém kraji I., II., III., IV. a VI.“** bude dokončen 31. 7. 2014 a k tomuto datu dojde i k naplnění všech indikátorů projektu. Implementace projektu splnila očekávání Ústeckého kraje ve smyslu významného posílení infrastruktury a zrychlení s tím souvisejících interních a externích procesů. Do projektu byly dle studie proveditelnosti zapojeny plánované cílové skupiny, především Ústecký kraj, Krajský úřad, včetně jeho organizačních složek, krajem zřizované a zakládané organizace, obce Ústeckého kraje, úřady územního plánování, poskytovatelé údajů o území a stát. Výstupy projektu jsou přístupné veřejnosti. Na webových stránkách Ústeckého kraje **www.kr-ustecky.cz/** je uvedena sekce eGovernment – Rozvoj služeb eGovernmentu v Ústeckém kraji (CZ.1.06/2.1.00/08.07230) s aktuálními informacemi o tomto projektu. Jsou zde uvedeny podrobnější informace o realizovaných změnách v projektu a o průběhu veřejných zakázek.

Dále uvádíme odkaz na webové stránky strukturálních fondů – **www.strukturalni-fondy.cz/iop**, jejichž dotační program nám umožnil tento projekt realizovat.

Bc. Jan Jelínek
vedoucí odboru informatiky
a organizačních věcí
Krajský úřad Ústeckého kraje

Ústecký kraj

INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

# e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

**MIKULOV • 9. - 10. 9. 2014**

ODBORNÝ PARTNER

Česká pošta

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

PLATINOVÝ PARTNER

CISCO

GENERÁLNÍ PARTNER

GORDIC®

Telefónica

VITA SOFTWARE

ZLATÝ PARTNER

Atos

CITRIX

dns

era jednoduše

FUJITSU

hp

ICZ

KOMIX

Microsoft

software602

vmware

STŘÍBRNÝ PARTNER

AutoCont

information and records management society CZECH REPUBLIC GROUP

TECHNI Serv TECHNISERV IT

sas

TECHNOLOGICKÝ PARTNER

AV MEDIA komunikace obrazem

intel

PARTNER

HELIOS

ict unie

IBM

MARBES CONSULTING

NESS

NEWPS.CZ

AVERA

VÍTKOVICE VÍTKOVICE IT SOLUTIONS

## ... v září opět v Mikulově!

Více naleznete na **www.egovernment.cz/mikulov**



I letos si Vás dovolujeme pozvat na konferenci **e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně.** Konference, kterou pořádá magazín Egovernment, proběhne tradičně na zámku Mikulov a to v termínu **9. - 10. 9. 2014**.

Opět pro Vás bude připraven bohatý dvoudenní program stejně jako společenský večer.

Součástí večera bude volba **Miss Egovernment**

- přihlašování soutěžících je již možné

(více na www.egovernment.cz/miss)

## Vstupné na konferenci se mění v čase:

**VEŘEJNÁ SPRÁVA (uvedené ceny jsou bez DPH):**

registrace do 25. 5. 2014 ..... 400 Kč
registrace do 25. 6. 2014 ..... 500 Kč
registrace do 25. 7. 2014 ..... 1 000 Kč
registrace do 30. 8. 2014 ..... 1 200 Kč

**KOMERČNÍ SFÉRA (uvedené ceny jsou bez DPH):**

registrace do 25. 5. 2014 ..... 2 500 Kč
registrace do 25. 6. 2014 ..... 3 300 Kč
registrace do 25. 7. 2014 ..... 4 500 Kč
registrace do 30. 8. 2014 ..... 8 000 Kč







... v září opět v Mikulově!

Přihlašování na konferenci je možné na **www.egovernment.cz/mikulov**

Česká pošta


# Na poště ověříme také Váš podpis a listiny

Navštivte kterékoliv z 1000 kontaktních míst Czech POINT na poště, kde na počkání úředně ověříme Váš podpis i dokumenty. A navíc můžete právě ověřené dokumenty ihned odeslat zamýšlenému adresátovi. **Vše na jednom místě.**