# Egovernment

elektronizace veřejné správy

## Kyberbezpečnost eIDAS a GDPR nejen osobní ochranný faktor

www.egovernment.cz

č. 2/2017

# Úvodní slovo

Kyberbezpečnost je stále důležitější, protože kyberkriminalita je stále produktivnější.

Není to tak dávno, co jsme zažili patrně jeden z nejrozsáhlejších útoků v rámci kyberprostoru. Pod názvem WanaCrypt byl schován virus, který byl infiltrován do neuvěřitelného množství počítačů, a to ve velice krátké době. Ředitel Europolu Rob Wainwright hovoří o více jak 200 000 počítačů napříč Evropou. Mezi napadenými byly komerční subjekty, jako například automobilka Renault nebo doručovací společnost FedEx, ale rovněž veřejná správa, například britský systém zdravotní péče (NBÚ potvrdilo, že v rámci české veřejné správy žádný problém zaznamenán nebyl). Všichni napadení měli společné to, že používali již nepodporovaný operační systém Windows XP. Dalo by se říci jejich nedbalost. Na druhou stranu se tak stalo údajně díky „díře", o které bezpečnostní služby věděly, ale místo, aby ji nahlásily bezpečnostním expertům, samy ji využívaly k útokům na své protivníky.

Rozhořela se tak diskuze o roli tajných služeb a „korektnosti" takového chování. Protože i u nás se nyní diskutuje o zapojení zpravodajských služeb (vojenského zpravodajství) do oblasti kyberbezpečnosti, připravil magazín Egovernment, dnes již tradiční seminář Kyberbezpečnost víc než zákon. Krátce potom jsme realizovali seminář Elektronická identita pro každého. A protože, alespoň podle našeho mínění, spolu obě tato témata velice úzce souvisejí, předkládáme Vám některé výstupy z uvedených seminářů.

Ing. Michal Jirkovský
šéfredaktor

# Obsah




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

info◆com s.r.o, Na Zatlance 10, 150 00 Praha 5
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:** Mgr. Kristýna Petrů

**Grafika:** PROPAGANDA, Malá Štupartská 7, Praha 1
**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.

# KYBER BEZPEČNOST

## - VÍC NEŽ ZÁKON

Egovernment

GENERÁLNÍ PARTNER

FORTINET

ZLATÝ PARTNER

ICZ

PARTNER

Deloitte.

HUAWEI

FORCEPOINT
POWERED BY Raytheon

www.egovernment.cz

# Stav kyberbezpečnosti v ČR

***Více než 200 000 počítačů v rámci celé Evropy. To je bilance vlastně jen jednoho, velice rychlého útoku na počítače, které provozovaly nepodporované operační systémy Microsoft XP. V rámci ČR jsme zřejmě ve veřejné správě počítače pečlivě a poctivě aktualizovali a provedli upgrade, neboť podle informací NBÚ nebyl žádný takovýto problém v naší veřejné správě zaznamenán. V jiných státech ano a ukazuje to, že uživatelé jsou přece jen za útočníky pozadu. A nemusí se vždy jednat o ledabylost. Technická zastaralost a neschopnost držet krok s vývojem je samozřejmě dána i množstvím financí, které jsou k dispozici. Popravdě nebývala vždy otázka zabezpečení tou, která se řešila jako první a měla vyčleněn nejvyšší rozpočet.***

Kyberbezpečnost více než zákon, to je název dnes již tradičního semináře, který magazín Egovernment, spolu se svými partnery pořádá v Poslanecké sněmovně Parlamentu ČR. I letos na jaře se nám podařilo získat reprezentativní sestavu vystupujících. Ke klasickému složení NBÚ, MV ČR přibylo na straně státu ještě vojenské zpravodajství. To je dáno jeho úlohou v rámci kyberobrany a diskuzí, které se v současné době vedou ve sněmovně právě při schvalování novely zákona o vojenském zpravodajství (momentálně přerušeno ve druhém čtení).

Právě popsaný útok s nasazením viru Wana Crypt ukázal určitý rozkol mezi tajnými službami a IT bezpečnostními experty. Ti totiž tajné služby viní z toho, že o díře, která vedla do systému XP, věděly, ale záměrně neinformovaly. I proto se v naší sněmovně živě diskutuje o tom, kam až při své obraně pustit do svých dat vojenské zpravodajství.

Informace o stavu kyberbezpečnosti ČR a postupu MV ČR v rámci veřejné správy i o záměrech a úloze vojenského zpravodajství naleznete na následujících stranách, nebo na www.egovernment.cz v sekci věnované semináři Kyberbezpečnost víc než zákon.

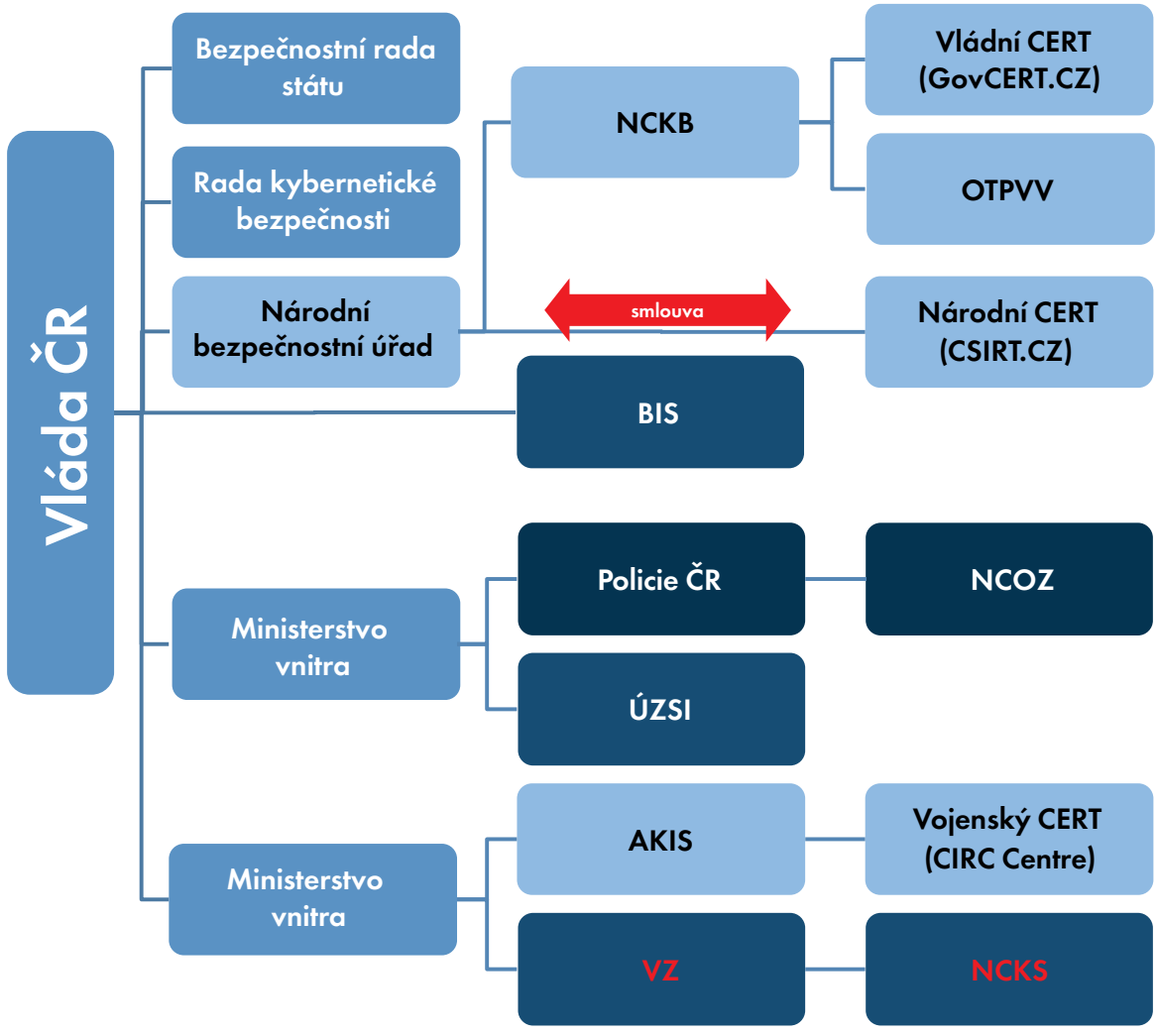
# Zákon o kybernetické bezpečnosti – aktuální situace

***Jaroslav Šmíd, náměstek, NBÚ na začátku svého vystoupení reagoval především na vývoj legislativy v oblasti kyberbezpečnosti a aktuální novinky, které se udály od posledního semináře, který magazín Egovernment v Poslanecké sněmovně pořádal.***

Jaroslav Šmíd na začátku svého vystoupení reagoval především na vývoj legislativy v oblasti kyberbezpečnosti a aktuální novinky, které se udály od posledního semináře, který magazín Egovernment v Poslanecké sněmovně pořádal. Především prezentoval ORGANIZAČNÍ RÁMEC tak, aby bylo zřejmé, jak je nyní tato problematika postihnuta

Ze struktury jsou patrné především dvě věci, že NBÚ nově provozuje Národní centrum kybernetické bezpečnosti (NCKB) a zároveň, že existuje smlouva mezi Národním bezpečnostním úřadem a národním CERTem, který provozuje společnost CZ.NIC. Zároveň došlo i k určitým změnám v rámci vládního CERTu, které náměstek Šmíd postupně v rámci svého vystoupení vysvětlil.

## ORGANIZAČNÍ RÁMEC



## TERMINOLOGIE

Podle Jaroslava Šmída je velice důležité si vyjasnit, co přesně znamenají jednotlivé termíny, jako je kybernetická bezpečnost, kybernetická obrana a kybernetická kriminalita. V této souvislosti zdůraznil, že NBÚ je odpovědno za kybernetickou bezpečnost. Úřad se tedy stará o bezpečnost kritické informační infrastruktury a významných informačních systémů. Jedná se o systémy, které NBÚ určil jako významné a kterých se týká povinnost plnit konkrétní standardy vydané NBÚ.

Kybernetická obrana je naopak oblastí, ve které působí vojenské zpravodajství. Zde jde především o identifikaci útočníků a zásah v případě, že hrozby a útoky v této oblasti dosáhnou míry, kdy je není možné řešit standardním způsobem. I proto náměstek Šmíd upozornil, že se zde nejedná o žádný kompetenční spor v rámci jednotlivých rolí NBÚ a vojenského zpravodajství (NCKB a Národního centra kybernetických sil). Trochu bokem pak podle náměstka Šmída stojí kyberkriminalita, ale rámcově i v této oblasti platí, že spolu všechny zainteresované složky spolupracují.

**BEZPEČNOST** – zastřešující termín pro široké spektrum bezpečnostních oblastí, zahrnuje všechny preventivní a reaktivní aktivity státu v oblasti ochrany dat, informací, systémů, služeb a sítí ve smyslu neustálého navyšování integrity, odolnosti a robustnosti státní informační infrastruktury a infrastruktury pro kritickou informační infrastrukturu.

**OBRANA** – ochrana státu výhradně proti pokročilým, závažným, nepřátelským kybernetickým útokům (tj. proti jakýmkoliv aktivitám, které mohou narušit státní integritu a suverenitu nebo hrozbám působícím proti národním strategickým zájmům a ekonomické prosperitě země). Mezi kybernetickou bezpečností a obranou rozlišujeme v závislosti na:

1. povaze hrozby;
2. typu kybernetického útoku a jeho cíli.

**KRIMINALITA** – trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, tedy veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat.

Novinkou, na kterou náměstek Šmíd upozornil, je skutečnost, že průběžně bylo Národní centrum kybernetické bezpečnosti posilováno, a to natolik, že z jednoho odboru, který byl součástí NBÚ, se stal samostatný útvar se dvěma odbory – vládním CERTem a odborem kybernetických bezpečnostních politik.

## GOVCERT.CZ

Jedná se o pracoviště, které úzce spolupracuje s řadou mezinárodních organizací, jichž je zároveň členem. Stejně tak úzce spolupracuje s národním CERTem (provozováno CZ.NIC). Pracoviště je rozděleno na čtyři základní oblasti – reaktivní oddělení, vývoj a bezpečnostní testování, oddělení síťové analýzy a analytické oddělení. Jeho smyslem je zajistit, pokud dojde k nahlášení kybernetické útoku, pomoc příslušné napadené instituci nejen s okamžitým řešením situace, ale rovněž její obranu do budoucna proti dalším obdobným útokům. Zároveň by mělo poskytovat informace a včasná varování před určitými typy útoků, které by mohly být zaznamenány i v rámci ČR. Tato varování jsou vydávána na základě mezinárodní spolupráce. Zároveň, s ohledem na problematickou úroveň zabezpečení systémů průmyslového řízení, je v této sféře ze strany CERTu nabízeno penetrační testování.

## ODBOR KYBERNETICKÝCH BEZPEČNOSTNÍCH POLITIK

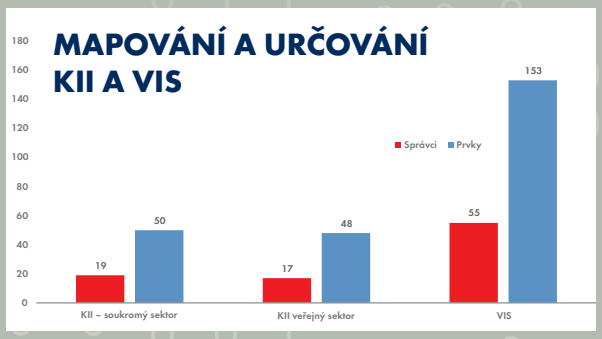
Jedná se o netechnické pracoviště. Tento odbor řeší především oblast kybernetických cvičení, legislativy (například transpozice NIS do národního prostředí) a mezinárodních vztahů. Zároveň zpracovává analýzy kybernetických útoků v různých částech světa. Náměstek Šmíd upozornil na skutečnost, že výsledky tohoto pracoviště byly velice úspěšně prezentovány i na mezinárodním poli. Od loňského roku rovněž toto pracoviště kontroluje, jak jsou standardy, které zákon předepisuje, implementovány.

Hlavní úkolem odboru je však určování prvků a informačních systémů kritické informační infrastruktury a významných informačních systémů. Tuto činnost realizuje dvěma způsoby:

a) v případě veřejného sektoru dává NBÚ návrh na zařazení IS do seznamu, který je následně předkládán vládě. Kritické informační systémy jsou provozovány pouze u prvků kritické infrastruktury. Tyto prvky jsou v kompetenci Hasičského záchranného sboru. I proto je příprava seznamu řešena ve spolupráci

s HZS. Vláda následně usnesením informační systémy určí a tím se dostávají pod dohled NBÚ a musí splňovat příslušné zákonné povinnosti;

b) v případě významných informačních systémů, které nesplňují kritéria pro provoz kritické infrastruktury, zároveň jsou ale pro chod státu podstatné se jedná se o systémy, jejichž znefunkčněním by státu vznikl zásadní problém. Mohou být provozovány pouze OVM a určují se vyhláškou. Proces jejich určení je tedy méně časově i procesně náročný.




## AKTUÁLNÍ TRENDY

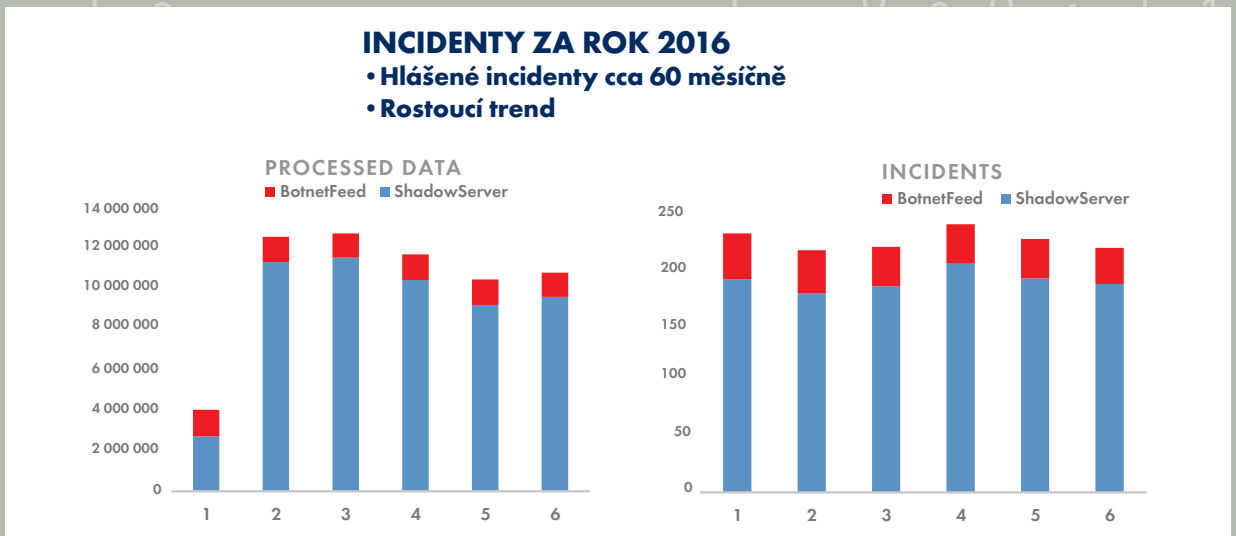
Pokud jde o aktuální trendy v oblasti kybernetických útoků, upozornil Jaroslav Šmíd na stále pokračující phishingové kampaně. Stále častějším, a to nejen v oblasti komerční, ale rovněž státních institucí, je výskyt Ransomware (vyděračský software). Jak upozornil, v těchto případech velmi často není jiná možnost, jak získat svá data zpět, než zaplacení požadované finanční částky. Zároveň připustil, že k něčemu podobnému již došlo i na úrovni ministerstev. Dalším nebezpečím je šíření velkého množství škodlivého kódu (Maelware), přičemž jeho podsunutí do systému bývá podle slov Jaroslava Šmída stále propracovanější.

V této souvislosti náměstek Šmíd popsal skutečnost, jak vznikají informace o jednotlivých incidentech. Povinnost jejich hlášení vznikla institucím, jejichž systémy byly NBÚ určeny jako součást kritické informační infrastruktury, případně významných informačních systémů. Kromě těchto institucí, které mají povinnost dávat hlášení o jednotlivých incidentech, tak mohou ostatní učinit i dobrovolně.

Počty hlášení jsou podle slov náměstka Šmída značné. Měsíčně NBÚ řeší v řádu několika set prokázaných útoků. I proto se nyní pracuje na projektech, které by měly ještě vylepšit činnost vládního CERTu. Byl, mimo jiné, otevřen nový informační portál a zároveň vzniká „zakrytý" portál jako zdroj informací pouze pro oprávněné subjekty. Zároveň jsou připravována nová kybernetická cvičení. Ve spolupráci s Policií ČR je rovněž budována forenzní laboratoř a zároveň jsou nabízeny penetrační testy z vnějšího prostředí.

## ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

Jak uvedl náměstek Šmíd, NBÚ průběžně pracuje na řadě dokumentů. Pravidelně každý rok zpracovává pro vládu zprávu o kybernetické bezpečnosti ČR, řadu analýz v oblasti kybernetické bezpečnosti, a především aktualizaci Národní strategie kybernetické bezpečnosti a akčního plánu. Novelu zákona o kyberbezpečnosti si vynutila evropská směrnice NIS (směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii). Novela je vedena ve dvou liniích. Tou první je transpozice NIS. Druhá je pak



součástí novely zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Díky tomu NBÚ dosáhne nyní nejen na správce IS, ale rovněž na jejich provozovatele. Jak Jaroslav Šmíd upozornil, je totiž velice problematické zajistit bezpečnost systémů, které jsou outsourcovány například na základě špatně uzavřených smluv. Doposud bylo možné pokutovat (v zásadě nízkou pokutou) pouze správce IS, kterými ve většině jsou ministerstva. Sami provozovatelé pak měli možnost se vymlouvat, že některé kroky, které jsou po nich požadovány, nejsou obsaženy ve smlouvě atp. Kromě toho, že bude nyní možné postihovat i tyto provozovatele, bude zvýšena horní hranice pokuty ze současných 100 000 Kč na 1 mil. Kč. NBÚ v této souvislosti připravil i samostatný workshop pro senátory a poslance, kde jim vysvětloval důvody těchto kroků a skutečnost, proč je vhodné, aby byla novela zákona v této podobě přijata.

Jak dále náměstek Šmíd upozornil, směrnice NIS se skutečně z velké části překrývá s tím, jak jsou u nás již definovány prvky kritické infrastruktury. Konkrétně EU touto směrnicí zahrnula mezi poskytovatele základních služeb energetiku, dopravu, bankovnictví, infrastrukturu finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastrukturu a chemický průmysl. Pro nás je tak nové pouze zařazení zdravotnictví. To se nacházelo v ČR mimo kritické systémy. Kritéria pro jeho hodnocení byla totiž nastavena tak, že pod ně žádné zdravotnické zařízení nespadalo. Například kritériem pro nemocnice byla nutnost existence 2500 akutních lůžek. Protože takto vybavenou nemocnici v ČR nemáme, nebylo možné zdravotnictví do kategorie kritických informačních systémů zařadit. Nyní tedy, díky směrnici NIS, toto již možné skutečně je.

Náměstek Šmíd dále uvedl, že kritéria pro určování provozovatelů těchto služeb jsou dosti podobná těm, která byla již obsažena v našem stávajícím zákoně. Připravit novelu tedy v tomto smyslu není žádný problém, neboť více jak 80 % skutečností, které požaduje NIS, máme již v našem zákonu zahrnuto.

## URČENÍ

NBÚ připravilo určitý návod, jak je možné předběžně určit, zda konkrétní systém bude spadat mezi nově určené prvky podle evropské směrnice. Nicméně NBÚ v tomto směru neočekává žádné problémy. Podle jeho odhadů totiž bude nad rámec doposud určených prvků těch nových v zásadě velice málo. V energetice by se mělo jednat o maximálně 5 nových prvků, v dopravě či bankovnictví kolem deseti. Samozřejmě největší nárůst bude v oblasti zdravotnictví, které doposud nebylo do určení zahrnuto. Celkově však NBÚ odhaduje, že by se ve výsledku mělo dostat na maximální počet 80 nových prvků při posuzování podle kritérií EU. Kromě samotného odhadu počtů má NBÚ rovněž vytipováno, o které konkrétní společnosti by se mohlo jednat a se všemi těmito subjekty probíhá na uvedené téma diskuze. Neměl by tedy skutečně podle slov náměstka Šmída v tomto smyslu nastat nějaký problém. Stejně tak dopadová kritéria nejsou podle jeho slov nijak překvapivá. Měla by totiž zohledňovat:

1. počet uživatelů, kteří jsou závislí na službě poskytované daným subjektem;
2. závislost dalších odvětví na službě poskytované daným subjektem;
3. možný dopad incidentů, pokud jde o intenzitu a trvání, na činnosti hospodářství a společnosti nebo na veřejnou bezpečnost;
4. podíl daného subjektu na trhu;
5. zeměpisný rozsah oblasti, která by mohla být incidentem dotčena;
6. důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativních způsobů zajištění této služby.

Jaroslav Šmíd ještě upozornil, že diskuze se vedla hlavně kolem chemického průmyslu. Jedná se totiž o oblast, kterou evropská směrnice přímo neurčuje, ale NBÚ i po poradě se Svazem průmyslu a dopravy považuje za vhodné, aby v jeho rámci existovala popsaná a zavedená bezpečnostní opatření. Je tedy žádoucí, aby chemický průmysl byl takto postižen, proto se nyní intenzivně pracuje na konkrétních omezujících kritériích.

Podle náměstka Šmída je podstatné, že přípravy na změnu vyhlášky byly ukončeny a vyhláška byla poslána do připomínkového mezirezortního řízení. Zároveň je nutno připravit tzv. „mazací vyhlášku". Tedy vyhlášku, která pokrývá situaci, kdy outsorcovaný systém ukončí svoji činnost tak, aby provozovatelům vznikala definovaným způsobem povinnost data smazat a předat je správci. Zároveň je nutné připravit vyhlášku postihující provoz systémů ve státním cloudu, a to jak ve státní, tak komerční části. Tedy popsat, kdo spadá do které z těchto částí a jaká bezpečnostní opatření budou muset u těchto systémů být implementována.

# KYBEZ – pohled MV ČR

***Miroslav Tůma chtěl přítomné seznámit především s tím, jakým způsobem se v rámci MV ČR vyvíjí kyberbezpečnost, čeho bylo dosaženo a jaký je směr dalšího postupu. Celé téma kyberbezpečnosti je podle něj velice dynamické a daleko širší, než postihuje zákon. Problematiku kyberbezpečnosti navíc podle jeho slov MV ČR řešilo již dávno před existencí zákona. Kyberbezpečnost byla vlastně velkou součástí celé bezpečnosti ICT, která se měla řešit průběžně. Správně by se měla bezpečnost ICT řešit nezávisle na existenci zákona, ale ve skutečnosti teprve díky němu, respektive sankcím z něho plynoucím, se dostala do popředí zájmu. Alespoň tedy pokud hovoříme o kybernetické bezpečnosti na úrovni systému kritické informační infrastruktury a významných informačních systémů. Z tohoto pohledu je tedy jedině dobře, že zákon o kyberbezpečnosti existuje. Díky němu došlo na řešení některých problémů, přičemž byla odstraněna řada nejasností. Před existencí zákona se totiž velmi často postupovalo dle principu, dokud se nic nestane, tak je všechno v pořádku. Jenže, jak Miroslav Tůma zdůraznil, v této oblasti platí, že když už se něco stane, je pozdě, proto je prevence velice důležitá.***

MV ČR spravuje poměrně velké množství systémů a velké množství dat, která jsou pro stát klíčová. Představa, že tyto systémy někdo učiní nedůvěryhodnými například tím, že zamění některá data, je naprosto nepřípustná. Následky takového zásahu by byly skutečně fatální. Proto je kyberbezpečnosti v rámci MV ČR věnována skutečně zásadní pozornost.

Miroslav Tůma prezentoval dvě základní definice, které by měly napomoci lepšímu vnímání, co vlastně kyberbezpečnost znamená:

Cílem a úlohou kybernetické bezpečnosti resortu MV je zabezpečení kybernetického prostoru proti vnějším a vnitřním kybernetickým hrozbám prostřednictvím organizačních a technických opatření a minimalizace možných důsledků kybernetických událostí / incidentů.

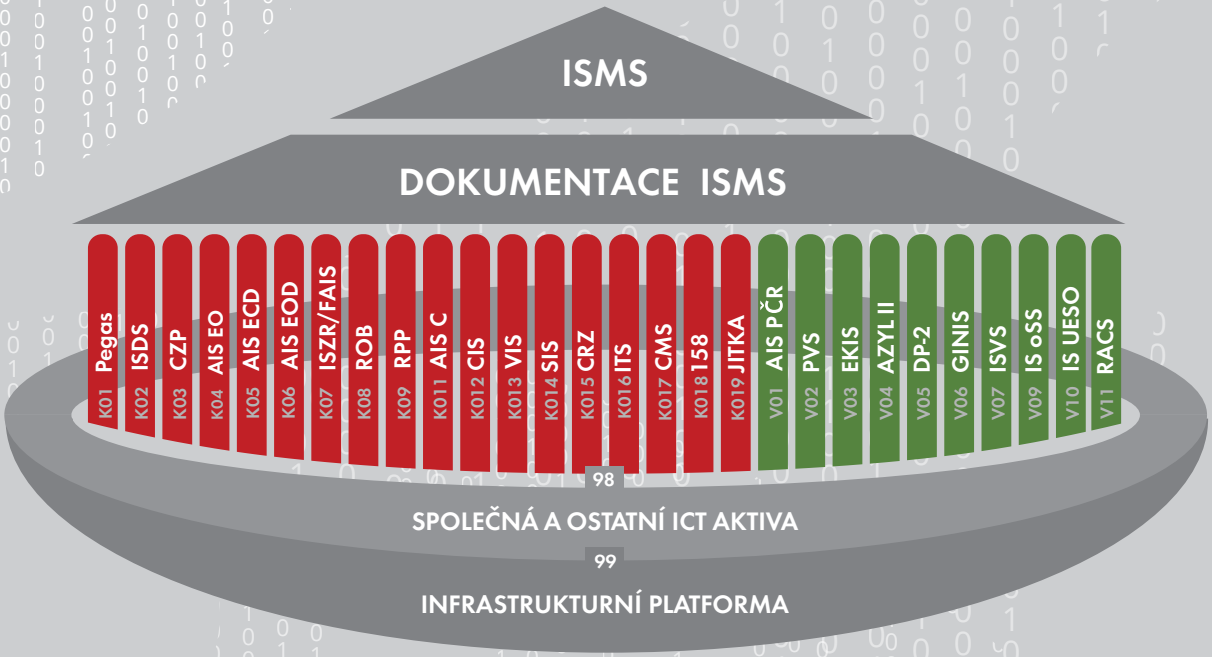
Bezpečnost kybernetického prostoru resortu MV je řízena průběžně zdokonalovaným systémem řízení bezpečnosti informací ISMS.

## KYBERNETICKÁ BEZPEČNOST JE SOUČÁSTÍ CELKOVÉ BEZPEČNOSTI ICT A MĚLA BÝT ŘEŠENA DÁVNO PŘED ZoKB.

Vnímání podstaty kyberbezpečnosti je podle Miroslava Tůmy skutečně ten největší problém. Vychází to z určitého historického přístupu k zabezpečování systémů. Ještě před časem to podle jeho slov vypadalo tak, že byla vyčleněna „parta" na zabezpečení systému. To však spočívalo především ve vytvoření dokumentace, bez konkrétních souvislostí. A ti samotní pracovníci vlastně neměli ponětí, proč tu činnost vykonávají. Jediným důvodem bylo nařízení zákona. Něco vyhodnocovali, ale vůbec si neuvědomovali souvislosti, rozsah výsledku, na němž se podílejí, byť dílčím úkolem. Že se jedná o ochranu resortu MV před vnějšími, ale i vnitřními útoky, to vlastně nemohli ani zaznamenat. Každý se tak v rámci kyberbezpečnosti soustředil na dílčí úkoly a vůbec nevěděl, kam ve výsledku směřují. Uvedené definice by tedy měly vysvětlovat, proč se celá tato činnost realizuje. Vytváření množství dokumentace a spousty výstupů je sice nádherná věc, ale bez konečného cíle, když nevíme, proč to vlastně děláme, tak to děláme jenom proto, aby to vzniklo. A pak je to práce bez potřebného efektu. MV ČR se snaží zpřístupnit kyberbezpečnost tak, aby byla vnímána jako zabezpečení určitého perimetru, určitých systémů důležitých pro stát, nikoli jako povinnost vyplývající ze zákona.

Jak bylo již řečeno, resort MV ČR má na starosti poměrně velké množství kritických systémů, nebo systémů kritické informační infrastruktury a velké množství významných informačních systémů a má povinnost je zabezpečit. Podle Miroslava Tůmy je však podstatné si uvědomit, že zabezpečení těchto systémů nelze udělat separátně. Je tedy nutné se na jejich uspořádání dívat jako na určitý na panteon, alespoň tak si to na Ministerstvu vnitra graficky vyjádřili. Jednotlivé systémy zde tvoří sloupy panteonu.

Nad nimi je umístěn vlastní systém řízení bezpečnosti a informací (tzn. systém řízení kybernetické bezpečnosti jako takový – systém ISMS). Zabezpečovaných systémů




je zde 27, ale kromě nich je nutno uvažovat i zabezpečení infrastruktury, tedy provázání všech těchto systémů. Jedině pak můžeme hovořit o tom, že máme systémy skutečně zabezpečeny. Panteon tedy nenahlížíme pouze jako stavbu shora dolů, ale i zleva doprava. Jednotlivé systémy se zde vzájemně ovlivňují, vzájemně se ovlivňuje samotná architektura.

Právě z tohoto uspořádání je patrné, že není možné řešit zabezpečení jen dílčích elementů, například jednotlivých systémů. Ty mohou být zabezpečeny důkladně, ale bez současného přístupu k jejich propojení není vlastně zabezpečeno vůbec nic. Právě proto je nutný komplexní pohled.

Ve chvíli, kdy takto vznikl uvedený pantheon, bylo zřejmé, že na něj navazuje celá složitá struktura. Podle Miroslava Tůmy bylo v tomto okamžiku důležité si uvědomit, jak vlastně vypadá kyberbezpečnost, kde jsou aktiva, která máme chránit, a co jsou tato aktiva.

## POČET SYTÉMŮ

MV dnes má až 40 % všech určených kritických systémů. A 6 % významných systémů, které jsou v této republice. Má tedy jednoznačně největší záběr. Počet 27 je, podle Miroslava Tůmy, skutečně veliký. Přitom není možné předpokládat, že to, co se naučíme v rámci jednoho systému, můžeme aplikovat v rámci jiného systému. Svým způsobem je každý z nich jedinečným. Právě proto je třeba mít silné metodiky a postupy. A především je důležité tyto postupy dodržovat a neustále optimalizovat. Konkrétně se jedná o:

- Komunikační systém pro IZS
- Informační systém datových schránek
- Informační systém CZECH Point
- Agendový informační systéme evidence osob
- Agendový informační systém evidence cestovních dokladů
- Agendový informační systém elektronických občanských průkazů
- ISZR – Formulářový agendový informační systém
- Registr obyvatel
- Registr práv a povinností
- Agendový informační systém cizinců
- Cizinecký informační systém
- Vízový informační systém
- Schengenský informační systém
- Centrální registr zbraní
- Integrovaná telekomunikační síť MV
- Centrální místo služeb
- Tísňové volání 158
- Jedná systémová informační technologická a komunikační platforma
- Agendový informační systém Policie České republiky
- Portál veřejné správy
- Ekonomický informační systém
- Informační systém pro evidenci udělení azylu

- IS sociálního zabezpečení, výpočet a výplata dávek sociálního zabezpečení
- Informační systém elektronické spisové služby
- Informační systém o informačních systémech veřejné správy
- Informační systém – registr státního občanství
- Informační systém o státní službě
- Systém řízení přístupů do ZR

Tyto systémy e-governmentu mají přesah přes resort MV. Jedná se o významné a skutečně velice důležité systémy podstatné pro chod tohoto státu. Proto je nutná jejich ochrana. Zároveň se ale jedná o živý organismus – například v případě určování kritických a významných systémů se jen v rámci MV ČR stalo, že v průběhu dvou let došlo celkem k 8 změnám. Celkově se tedy systémy 8x vyměnily, dokonce se jeden z kritických systémů dostal do významných, neboť vzhledem k vývoji a struktuře už kritickým přestal být. Postupně systémy přibývají, neustále se objevují nové a není možné považovat jejich uspořádání za definitivní.

MV ČR vyhodnocovalo své systémy hned od začátku. Nejprve byla hodnocena samotná aktiva, z nich pak jejich rizikovost a na základě rizikovosti se hodnotila jednotlivá opatření. Postupně tak v rámci MV ČR bylo identifikováno 12 mil. uživatelů, 776 tisíc technických aktiv a k tomu přes 900 tisíc opatření k jednotlivým aktivům. Takto popsán působil celý systém jako výborně analyzovaný. Bylo však nutné rozhodnout, jak naložit především s oněmi 900 000 opatřeními. Pokud možno, jejich počet zredukovat do rozumné míry. Šlo tedy o to, aby nebyla implementována dílčí opatření v jednotlivých částech systému, ale aby se jednalo o „globální" implementaci. To je záležitost, která se nyní podařila. Je připraven globální projekt pro zabezpečení celého perimetru, celkové infrastruktury a individuální opatření jsou schována v rámci těchto globálních a budou na řadě až v 2. úrovni dat při další aktualizaci celkových analýz.

Podle Miroslava Tůmy problém nyní spočívá v rozdílné úrovni systémů z pohledu zabezpečení, zpracované dokumentace, nastavení, přístupu jednotlivých uživatelů, garantů, správců atd. Nejprve je tedy nutné sjednotit celkové myšlení a přístup, všechny systémy zabezpečit globálně a teprve následně se můžeme věnovat jednotlivostem a jejich specifikům. To je, podle Miroslava Tůmy, výsledný poznatek, k němuž v rámci MV ČR dospěli. Zdánlivě jednoduché konstatování, za kterým se však nachází obrovské množství práce. Nyní má MV ČR k dispozici první základní výstup a určité poučení, stejně tak i upřesněnou metodiku, která usnadní další práce a analýzy. Další práce tedy budou postupovat k cíli rychleji a s menším úsilím.

## DOHLEDOVÉ CENTRUM

Dalším zásadním krokem v rámci resortu MV ČR bylo vybudování poměrně rozsáhlého dohledového centra e-governmentu. To dohlíží na veškeré kritické a významné informační systémy. V režimu 7x24 je zde monitorován jak provoz, tak samozřejmě bezpečnost celého perimetru. Při přípravě tohoto dohledového centra bylo nutné definovat řadu potencionálních problémů a incidentů. Některé z nich se následně rušily či upravovaly, ale nakonec se vše, podle slov Miroslava Tůmy, podařilo vyladit.

Dohledové centrum musí průběžně řešit v rámci provozního dohledu události, jejichž dopady se pohybují v rozměru miliard Kč. Skutečnost, že MV ČR nemuselo platit za návrat svých dat, nemělo doposud problém s ransomware atp., zatím potvrzuje, že bylo nastaveno správně. Pravdou podle Miroslava Tůmy ovšem je, že celkový počet útoků doposud nebyl vysoký.

V minulém roce řešilo MV ČR pouze 2 základní typické kybernetické incidenty, událostí celkově 122, respektive 124 celkově, tedy v průměru se téměř každý druhý den něco stalo a bylo nutno to řešit. Každá z těchto událostí byla zároveň určitým poučením, každá si vynutila určitou změnu, nějakou optimalizaci, a to nejen v rámci opatření. Z každé takové události bylo podle Miroslava Tůmy vypracováno jasné preventivní opatření tak, aby se událost nemohla opakovat a aby jí bylo předcházeno. V této souvislosti je zajímavé rozložení incidentů v jednotlivých měsících. Dokonce existuje analýza, která potvrzuje, že největší počet útoků se objevuje v úterý.

Podle slov Miroslav Tůmy v roce 2016 dospěli na MV ČR k závěru, že celý systém, jak byl nastaven, není úplně efektivní ve vypjatějších situacích. Proto jej bylo nutno výrazně zjednodušit. Šlo mimo jiné o to, aby celá dokumentace byla jednodušší, přístupnější a uchopitelnější. Důvodem byla i skutečnost, že v rámci resortu vnitra existuje 59 organizací. Ty potřebují jednotné prostředí pro sdílení informací. To ale znamená, že v těchto 59 organizacích pracuje v kyberprostoru zhruba 70 tisíc zaměstnanců. I proto MV ČR zvolilo platformu Sharepointu, kde byla celková dokumentace uveřejněna. Zároveň jsou zde prezentovány veškeré vzdělávací materiály, seznamovací materiály a k dispozici jsou jednotlivé posudky k daným dokumentům.

Celý systém bezpečnostních informací byl dokumentován formou dynamického objektového modelu, tedy formou, kdy kdy je „proklikávací" model provázaný s jednotlivými procesními dokumenty. Procesy tedy nebyly popisovány vývojovými diagramy, ale moderními nástroji a moderními metodami na popis procesů. Výsledkem je situace, kdy jednotlivé procesy byly svázány s konkrétní odpovědností, a tak bylo možné určit, kdo a kolik má jakých povinností, kdo spravuje jednotlivé dokumenty atd.

Souběžně byly vypracovány a dány k dispozici i veškeré vzdělávací materiály. Uživatelé tedy mají dostupnou nejen samotnou dokumentaci, ale i základní legislativu, souhrnné a základní školicí materiály atp. Nicméně pořád to bylo příliš mnoho dokumentů. Následovalo proto vytvoření tzv. „Quic Guide", tzn. příručky, kde byly postiženy 3 základní dokumenty, tj. základní souhrn zásad a politik, které vycházejí z celého „ISMS". To jsou nyní podklady pro rychlou orientaci. Vedle toho samozřejmě existují zásady chovaní uživatele – dvoustránkový materiál, který definuje základní pravidla chování - například je zde popsán zákaz používání externích úložišť, zákaz využívat jakékoliv externí vstupy obecně, zákaz zkoušet otevírat neznámé soubory atp. Je to vlastně dokument, který shrnuje, co znamená zabezpečení systémů kritické informační infrastruktury a významných informačních systémů tak, aby byly skutečně kyberneticky bezpečné.

Problém je, že popsané zabezpečení je ve výsledku poměrně finančně náročné. Realizovat všechna potřebná opatření by obnášelo astronomické částky. I proto se postupuje dle priorit, kapacity a prostředků, které jsou dispozici. V tomto případě se tedy nejedná o plošnou implementaci.

## CO MÁME PŘED SEBOU?

Jak bylo řečeno, systém je živý organismus a kyberbezpečnost se stále vyvíjí. I proto je potřeba stále zlepšovat systém, neustále jej zdokonalovat a předělávat. Zatímco v loňském roce MV ČR obdrželo celkově od NCKB zhruba deset upozornění na určitý problém, v letošním roce přišlo do konce března už patnáct takových varování. V loňském roce MV ČR řešilo 122 událostí, letos jen do března 150. Miroslav Tůma nevidí problém v tom, že bychom se chovali nebezpečně, že by naše systémy nebyly zabezpečeny atp. Problém je podle jeho mínění v tom, že počet útoků roste geometrickou řadou.

MV ČR postupuje v rámci cyklu PDCA (plan-do-check-act). V tomto cyklu je neustále vylepšován samotný systém, ale rovněž metodiky a postupy, procesy. A to vše je stále znovu optimalizováno. Jak uvedl, někdy je optimalizace rychlejší a proběhne ještě dříve, než uživatelé začnou tyto procesy dodržovat.

Vedle toho je daný plán zvládání rizik, kterým se celý systém rozvíjí.

**Plán zvládání rizik** vzniká na MV ČR z několika zdrojů v rámci rizikových analýz jednotlivých systémů. Současně je monitorováno prostředí internetu, jednotlivé dostupné zdroje, bulletiny a další podobné podklady. Dochází tak k vyhodnocování potencionálních hrozeb, vytváření katalogu hrozeb a na jeho základě k identifikaci možných opatření. MV ČR samozřejmě prochází pravidelnými audity NCKB a audity v rámci ISO 27001. Všechny tyto výstupy se setkávají v rámci souhrnného plánu zvládání rizik, kde jsou odstraněny duplicity a naplánována opatření a jejich implementace. V rámci plánu zvládání rizik má MV ČR rozpracován cca 5tiletý plán rozvoje bezpečnostního povědomí s jasným cílem konkrétní úrovně, na jakou by se měly dostat jednotlivé role či uživatelé.

Miroslav Tůma nevidí v tomto směru zásadní problém s pracovníky, kteří se skutečně kyberbezpečností zabývají, za problematické však považuje běžné uživatele. Ti jsou podle něj velmi často přesvědčeni, že už toho realizovali dost, a tedy nemusí nic nového podstupovat. Problém je tedy v uvědomění konkrétních uživatelů a i to je podle jeho slov otázka vedení. Nicméně překážky jsou především v legislativě na straně vymahatelnosti. Není například možné uživatele, který nesplňuje určité testy v rámci kyberbezpečnosti, odpojit z kyberprostoru a zamezit mu do něj přístup. Neumožňuje to služební zákon, případně další legislativní záležitosti.

I proto MV ČR považuje, vedle popsaných opatření, práci s uživateli a jejich vedení za velice důležité a podstatné.

# Kyberbezpečnost pohledem vojenského zpravodajství

***Ve svém vystoupení na semináři se ředitel vojenského zpravodajství plk. Ing. Jan Beroun věnoval především tématu kybernetické obrany. Jak uvedl, ta sice vychází z kybernetické bezpečnosti, ale jedná se o samostatnou kapitolu. Kybernetická bezpečnost je orámována příslušným zákonem (č. 181/2014 Sb.) a dalšími dokumenty. Aplikací těchto dokumentů vznikla, podle slov Jana Berouna, určitá analýza a právě ona dala základ přípravě kybernetické obrany.***

## OBRANA A BEZPEČNOST

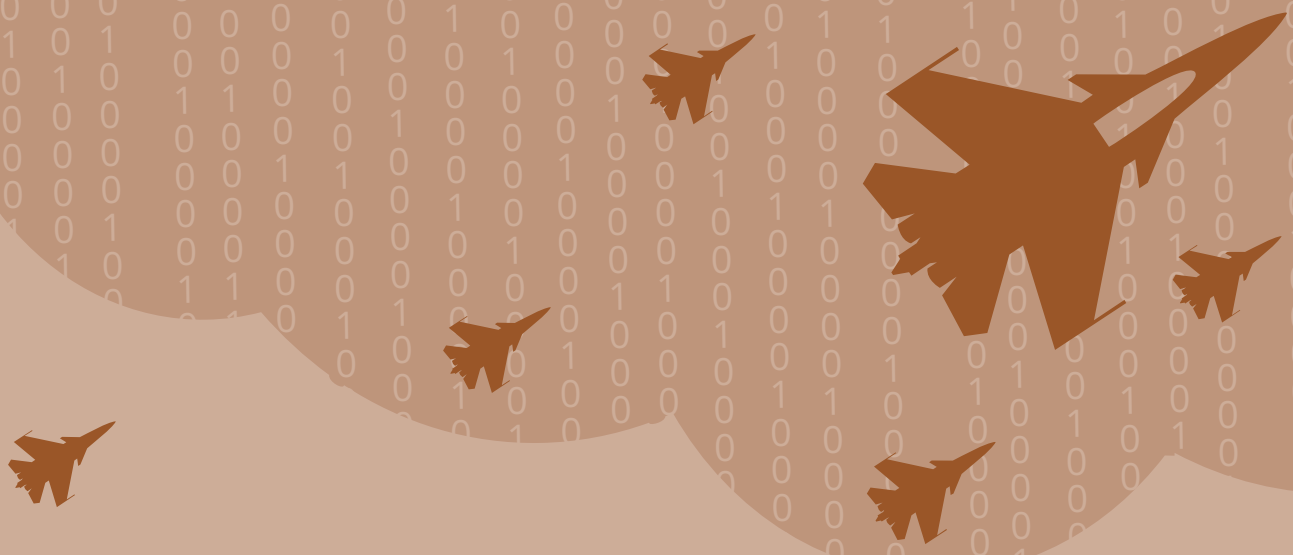
Pro přesné užití termínů kybernetická obrana a kybernetická bezpečnost neexistuje, podle slov Jana Berouna, žádný přesný standard či pravidlo, a to ani na mezinárodní úrovni. Z diskuzí s NBÚ, kterému Jan Beroun poděkoval za iniciaci zákona o kyberbezpečnosti, vzešly rovněž úvahy o potřebě kybernetické obrany. Výsledkem je úkol od vlády pro vojenské zpravodajství, který zahrnuje tyto body:

- v rámci vojenského zpravodajství vytvořit Národní centrum kybernetických sil (NCKS), které bude schopné provádět široké spektrum operací v kyberprostoru a aktivity nutné pro zajištění kybernetické obrany ČR. NCKS bude schopné provádět vojenské operace v kyberprostoru, a to jak na podporu zahraničních operací AČR v rámci NATO nebo EU, tak i v případě hybridního konfliktu za účelem obrany ČR;
- připravit projekt financování a budování NCKS;
- zajistit vhodné prostory a nábor personálu pro NCKS;
- vybudovat kompletní technickou infrastrukturu pro NCKS;
- připravit návrh nutných legislativních změn pro potřeby plné funkčnosti NCKS.

Uvedený krok považuje Jan Beroun svým způsobem za průlomový. Zpravodajské služby měly totiž doposud čistě informační charakter, tedy pouze „sbíraly" informace. Nyní se vnáší do jejich pravomocí aktivní prvek a to je mimo jiné důvod, proč bylo nutné novelizovat zákon.

Podle Jana Berouna je možné aktivity v rámci kybernetického prostoru rozdělit na kybernetickou kriminalitu, kybernetickou bezpečnost, kybernetickou obranu a kybernetické zpravodajství. Význam a podstata kybernetické kriminality a bezpečnosti jsou zjevné. Ve svém vystoupení se tedy zaměřil především na kybernetickou obranu. Podstatné je, že problematika kybernetické obrany byla po celou dobu příprav novely zákona důsledně oddělena od kybernetické kriminality. Kybernetická obrana je obrana státu ve velice specifickém – kybernetickém prostoru. V současné době máme v zákonech a příslušných normách velice přesně popsáno, co se musí stát, jaké jasně definované body se musí naplnit, aby se aktivovala „klasická" – kinetická obrana. Podle mínění Jana Berouna je nutné z této definice odvodit kybernetickou obranu, definovat rozdíly oproti kinetické a stanovit jednotlivé iniciační momenty. Klíčové pro kybernetickou obranu tedy bude zpracování plánu kybernetické obrany, který bude schvalovat vláda.

Plán bude stanovovat veškeré postupy, které mohou být aktivovány v případě projevení určitých indikátorů nebo hrozeb. Právě nastavení těchto indikátorů a definování možného postupu při jejich aktivaci je velice důležité už proto, že vláda z principu jedná jako sbor. Jenže v případě potřeby kybernetické obrany je většinou nutné reagovat okamžitě a není možné čekat na společné jednání vlády. Navíc, oproti klasickému, tedy kinetickému útoku a obraně, je podle Jana Berouna potíž v tom, že kybernetická hrozba přichází zdánlivě z nenadání a bez vnější projevů přípravy – tedy velmi potichu a skrytě. Proto je nutné velice přesně nastavit pravidla pro „spuštění" kybernetické obrany. Je to však, jak upozornil, velice citlivá záležitost, a to i na mezinárodní úrovni. I zde se legislativa stále vyvíjí, ale konkrétní iniciační momenty jsou určovány velice obezřetně. Důvodem je skutečnost, že označení určitého momentu za útok by měl aktivovat kolektivní obranu, a tedy spouštět rozsáhlý mezinárodní mechanismus.



Zákon o vojenském zpravodajství a akční plán předpokládají, že kybernetická obrana bude vybudována vojenským zpravodajstvím jako systém obrany celého státu. Přesto je zřejmé, že některé prvky této činnosti se budou v čase přesouvat do armády. Podle Jana Berouna je to naprosto logické a žádoucí. Je nutné, aby v určitých momentech byly kybernetické jednotky přítomny přímo v místě účasti konkrétních misí. Pouze na základě znalosti prostředí dokáží totiž adekvátně a rychle reagovat. Jedná se o zkušenost, kterou jsme si, podle ředitele vojenského zpravodajství, ověřili při naší účasti v Afghánistánu.

## PROČ VOJENSKÉ ZPRAVODAJSTVÍ?

Podle Jana Berouna právě tato otázka prošla rozsáhlou diskuzí. Jak řekl, je patrně logické, aby obranu státu zajišťovalo Ministerstvo obrany. V tom případě je možné uvažovat právě o vojenském zpravodajství, nebo armádě jako takové. Armáda je však, zatím, díky dosavadnímu vývoji, zaměřena spíše na klasický kinetický styl obrany. V otázce kybernetické obrany nemá ještě žádné předpoklady. Vzhledem k tomu, že se velmi často jedná o realizaci utajených postupů a akvizic, je to záležitost, pro kterou je daleko lépe vybaveno vojenské zpravodajství. Jak ale uvedl, počítá se do budoucna s tím, že některé z těchto činností budou postupně přecházet na armádu. I proto nyní probíhají jednání, která vymezují rámec činnosti obou těchto složek.

## TECHNICKÉ PROSTŘEDKY

Vedle právních záležitostí byly rovněž diskutovány technické prostředky nutné pro zajištění kybernetické obrany. I to je podle Jana Berouna velice citlivá záležitost, a to z několika důvodů. Především technologický vývoj v oblasti IT je značně dynamický. Pokud by zákon uváděl konkrétní prostředky, bylo by nutné je kontinuálně novelizovat. Proto jsou zákonem popsány pouze obecně. Druhým důvodem je zřejmá nutnost jistého utajení. Není nutné potencionálním útočníkům sdělovat, jaké prostředky a v jakém rozsahu je stát schopen nasadit na svoji obranu. Nečiní tak v oblasti „klasické" obrany a není jediný důvod, proč by to měl zveřejňovat v oblasti kybernetické.

Nasazené technické prostředky by neměly podle slov Jana Berouna sloužit ke sběru konkrétních informací. Upozornil však, že se bude jednat o pasivní prostředky určené ke sledování anomálií v rámci běžného provozu. Analýzou těchto anomálií by pak měla být určována konkrétní potencionální rizika.

## NEJKONTROLOVANĚJŠÍ NEJKONTROLOVANĚJŠÍCH?

I proto je ale velice důležitý systém kontroly, který bude, mimo jiné, zahrnut v rámci rozhodování vlády o plánu kybernetické obrany. Vláda tak bude schvalovat finanční prostředky a bude tedy mít související přehled o nasazení a umístění technických prostředků. To je pouze jeden z kontrolních bodů. Je počítáno rovněž s dalšími kontrolními mechanismy na úrovni parlamentní a ministerské. Podle Jana Berouna se bude jednat o nejkontrolovanější činnost zpravodajských služeb. A je to podle jeho mínění logické, protože tato činnost samozřejmě bude v určitém okamžiku pronikat do práv občanů. I proto je i pro samotné vojenské zpravodajství velice důležité, aby zákon popisoval jasně všechna základní pravidla, a zpravodajství bude ve vlastním zájmu dbát na jejich dodržování. Pro stát je totiž tato činnost naprosto klíčová a její případná diskreditace by byla fatální.

# Na kybernetickou bezpečnost koncepčně

***V době, ve které na manažery společností doléhá tlak v podobě evropského nařízení General Data Protection Regulation (GDPR), se vcelku zásadně mění vnímání oblasti kybernetické bezpečnosti. Oproti minulosti jsou firmy daleko více ochotny ztotožnit se s využitím systémů pro správu privilegovaných účtů, potřebou implementovat technologie z rodiny Data Loss Prevention (DLP) a monitorováním přístupů do databází a práci s nimi.***

Až potud je vše v pořádku. Pokud ovšem vlastní návrh není jen souhrnem izolovaných řešení, která nejsou uvedena do kontextu s celkovou situací firemního IT a hlavně s bezpečností celé síťové infrastruktury. Bohužel se v tomto honu na technologie, jež zázračně vyřeší každý problém a zaručeně odzbrojí každou kontrolu z Úřadu pro ochranu osobních údajů, jednotná koncepce často vytrácí. V nejhorším případě se společnost může dostat do situace, kdy bude mít několik výborných technologií, jež se ale vzájemně nijak neovlivňují a nespolupracují. Následná korelace a interpretace výstupů je pak extrémně náročná.

Nejdůležitější je proto vybudovat dobré základy a bezpečnou síť jako funkční celek a až poté přidávat další části, jež pomohou bezpečnost zvýšit i z pohledu ochrany osobních údajů. Bez dobrých základů totiž nemá ani sebelepší technologie šanci plnit plnohodnotně svou funkci a být očekávaným přínosem pro firemní bezpečnost.

## Kde s ochranou začít?

Směr, který při návrhu a implementaci bezpečnostních řešení v ICZ dodržujeme, je vcelku jednoduchý. Síť je potřeba nejprve chránit proti hrozbám z vnějšku a následně zabezpečit interní služby. Je nutné si uvědomit, že začít se musí od perimetru, dále pokračovat přes vnitřní síť a dojít až ke koncovým stanicím.

Ale co je vlastně perimetr? Dříve poměrně jasně definovaná část sítě, kde se umístil firewall, jenž chránil síť před nebezpečím z internetu, je dnes distribuována na různá místa. Každé mobilní zařízení představuje vstupní bod do sítě, tedy jakýsi perimetr. Nad mobilním zařízením není

možné mít úplnou kontrolu, a proto představuje zvýšené riziko při přístupu k firemním datům. Je tedy potřeba vymezit jednoznačné hranice pro firemní data. Segmentace sítě, definice správných politik a kategorizace dat jsou nezbytným základem pro účinnou bezpečnostní strategii.

## Analýza aktuálního stavu

Prvním krokem před návrhem jakékoliv koncepce ochrany by mělo být seznámení se s aktuálním stavem bezpečnosti v síti. Využívá se k tomu například metoda Proof of Concept (PoC), kdy se provádí test technologií přímo v síti zákazníka a následně detailně vyhodnocují slabá místa.

Nedochází při něm k žádným útokům na síť ani služby, data zůstávají uvnitř společnosti a jeho výsledkem je jedinečná analýza, čemu se nepodařilo stávajícím bezpečnostním prvkům zamezit a jaké hrozby se ve firemní síti skrývají. Veškeré výsledky jsou přitom za pomoci moderních vyhodnocovacích nástrojů velmi srozumitelně a přehledně rozděleny pro administrátory i vedení společnosti.

K dispozici je tak komplexní zpráva o zjištěných bezpečnostních událostech, která obsahuje pokusy o průnik a útoky na firemní systémy a služby, regiony, odkud jsou tyto útoky vedeny, aktivitu virů, wormů a botnetů v interní síti s analýzou využití sítě.

Zároveň se sledují i aktivity uživatelů, jako jsou práce s rizikovými aplikacemi (internetová uložiště, anonymizéry, vzdálená administrace systémů), možnosti kompromitace cenných informací (interní dokumenty zasílané na soukromé adresy), používané aplikace, včetně objemu přenesených dat a statistiky navštívených webových stránek.

Test dále hodnotí i způsoby zabezpečení koncových stanic a mobilních zařízení.

## Je testování složité?

Pro testovací účely je většinou využíván monitorovací port v interní síti, do kterého je provoz zrcadlen. Žádným způsobem se nemění topologie ani neovlivňuje chod sítě, vše probíhá v pasivním režimu za pomoci sond v podobě bezpečnostních prvků renomovaných výrobců.
Technici ICZ přivezou dostatečně dimenzované zařízení, provedou fyzické zapojení i potřebnou konfiguraci. Součástí je též zaškolení interních pracovníků, kteří si tak mohou vše vyzkoušet nad reálným provozem, aniž by jej ovlivnili.

## Závěry hodnocení

Po ukončení testu jsou data ze sondy vyhodnocena odborníky ICZ a u vybraných rizikových událostí proběhne hlubší analýza. Závěry shrnuje výsledný report, ve kterém jsou přehlednou formou zobrazeny všechny důležité události a tyto jsou pak předloženy společně s výkladem IT manažerům i vedení společnosti.

## Aplikace výsledků

Na základě výsledků pozorování lze věrohodně a spolehlivě definovat a jasně pojmenovat problematické části sítě a navrhnout koncepci řešení bezpečnosti, buďto se zaměřením na konkrétní technologie, nebo jen definicí nezbytných vlastností. Výstupy mohou být nápomocné i při řešení GDPR, a to jak při analýze stavu souladu (Gap analýza), tak při vlastním rozhodování o technologiích, jež bude nutné nasadit.

ICZ

**Chcete nahlédnout do dění ve své síti zdarma?**

V rámci promo akce nabízí ICZ bezplatné kompletní testování. Máte tak jedinečnou šanci ověřit své zabezpečení a zjistit, zda chování uživatelů a využívání sítě odpovídá Vašim představám. Další informace získáte prostřednictvím e-mailové adresy securitypoc@i.cz.

# K GDPR a ochraně proti kybernetickým hrozbám je třeba přistupovat systematicky

***Masivní technologický rozvoj a nový přístup k IT sice organizacím přinesly nové výhody, jako je provozní pružnost a flexibilita, širší možnosti kontaktu se zákazníky a celkové zrychlení ve všech směrech, zároveň ale vytvořily prostředí pro nové hrozby. Pokud chtějí organizace s neustále se vyvíjejícími kybernetickými hrozbami udržet krok, musí k zabezpečení své infrastruktury přistupovat proaktivně, nikoli reaktivně. Společnost Fortinet nabízí komplexní bezpečnostní řešení, která vynikají nejen špičkovou funkcionalitou, ale i přehledností a jednoduchou správou.***

Společnost Fortinet vyvíjí, vyrábí a prodává portfolio produktů a služeb, které tvoří nejmodernější a nejvýkonnější síťovou bezpečnostní platformu, s jejíž pomocí mohou zákazníci bezpečně budovat a rozvíjet své IT infrastruktury, a to jednodušeji a s nižšími náklady. Díky integraci širokého spektra bezpečnostních služeb v jednom zařízení pomáhá Fortinet zjednodušit celou síťovou infrastrukturu a zajistit pohodlnou centralizovanou správu, lepší kontrolu a ucelený pohled na bezpečnostní situaci v reálném čase.

## Následky bezpečnostních incidentů jsou vážnější než pouhá ztráta dat

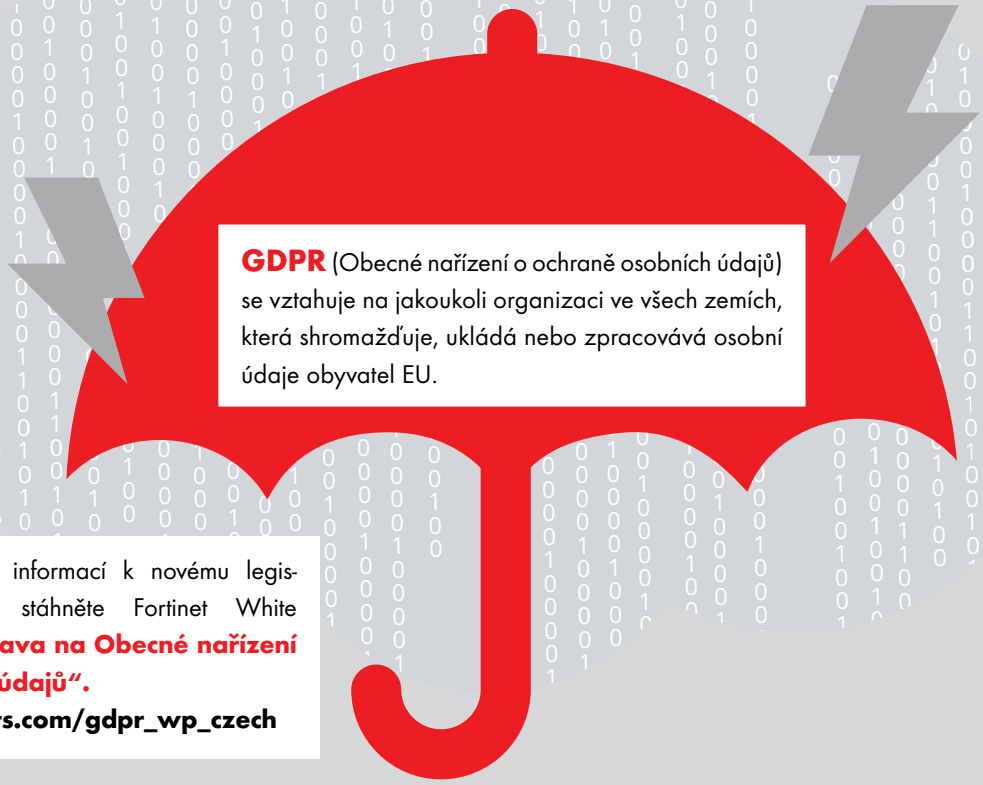
Přestože se kybernetická bezpečnost, i díky schválení kybernetického zákona, dostává do veřejné diskuze stále častěji, jedním z největších problémů současných firem je skutečnost, že mají tendenci kybernetické hrozby podceňovat. S tím, jak se změnily technologie, způsob práce s daty a posunulo se řízení systémů, které zasahují do reálného světa, je třeba adekvátně změnit i způsob ochrany.

Firmy a instituce si musí uvědomit, že žijeme ve světě, kde většina činností probíhá elektronicky nebo je určitým způsobem na elektronické systémy napojena. Ve světě, kde je většina informací uchovávána a zpracovávána prostřednictvím digitálních systémů, může ohrožení těchto dat způsobit nejen obrovské ekonomické škody, ale reálně i narušit bezpečnost jednotlivců i celých organizací. Ztráta a diskreditace dat je totiž v dnešní době závažným problémem, který může ohrozit konkurenceschopnost firmy, poškodit její jméno a zkompromitovat zákaznická data. Ještě závažnější jsou pak možnosti škod fyzických, způsobených potenciálním útokem na průmyslové a řídicí systémy. Rizika plynoucí z narušení kapacity a kvality výroby může potenciálně pocítit každý z nás.

Navíc je třeba si uvědomit, že cílem hackera se může stát i obyčejná domácnost. Dnes už i velmi malý procesor v pračce nebo v běžném routeru má nezanedbatelný výkon a v době, kdy lze připojit k internetu prakticky jakékoli zařízení, může hacker napadnout celý domácí systém a získat významnou výpočetní kapacitu. Elektřinu platí nic netušící oběť, navíc se vystavuje riziku, že útočník využije informace o jejím životním rytmu k tomu, aby mohl domácnost vykrást.

Zajistit dostatečné zabezpečení firemních sítí v době, kdy se o slovo hlásí nové trendy a technologie, jako je internet věcí, využívání soukromých mobilních zařízení, softwarově definované sítě či cloud, je pro IT oddělení obrovskou výzvou. Častým řešením řady firem je přidat do již tak nepřehledné a přetížené infrastruktury další bezpečnostní řešení. Složitost systému je přitom jednou z největších překážek bezpečnosti. Izolovaná bezpečnostní řešení s vlastní správou nemají šanci zajistit potřebnou komunikaci s ostatními systémy. Místo aby pomáhaly s ochranou infrastruktury, jejich obsluha a optimalizace pouze vytváří zbytečnou pracovní zátěž.

Jako řešení nabízí Fortinet novou bezpečnostní platformu „Fortinet Security Fabric ". Ta integruje kompletní bezpečnostní technologie pro koncové body, přístupovou vrstvu, sítě, aplikace, datová centra, obsah i cloud do jediného bezpečnostního řešení, které lze řídit prostřednictvím jednoho rozhraní. Zákazníci tak získají přehledné a vysoce škálovatelné bezpečnostní řešení s jednoduchou správou, které v sobě integruje špičkové bezpečnostní funkce a využívá pokročilé analytické nástroje pro ještě lepší ochranu proti kybernetickým hrozbám. Pro jednodušší integraci v rámci firemní infrastruktury a maximální využití stávajících zdro-



**GDPR** (Obecné nařízení o ochraně osobních údajů) se vztahuje na jakoukoli organizaci ve všech zemích, která shromažďuje, ukládá nebo zpracovává osobní údaje obyvatel EU.

Pro nalezení klíčových informací k novému legislativnímu nařízení si stáhněte Fortinet White Paper s názvem **„Příprava na Obecné nařízení o ochraně osobních údajů“.**
**www. fortinet-events.com/gdpr_wp_czech**

jů nabízí Fortinet otevřená rozhraní API umožňující technologickým partnerům a řešením třetích stran stát se součástí Fortinet Security Fabric.

## Inovace na prvním místě

Od svého založení v roce 2000 společnost Fortinet vyvíjí technologie vlastními silami a má dokonalou kontrolu nad podobou svých produktů, bez kompromisů v kvalitě, výkonu a spolehlivosti. Za úspěchem Fortinetu stál právě jeho inovativní přístup. V době, kdy se všichni ostatní výrobci snažili na každou funkcionalitu využít speciální zařízení, Fortinet šel cestou all-in-one řešení, což se ukázalo jako správná strategie, která mu zajistila nezanedbatelný vývojový náskok. Ten se promítá nejen do kvality, ale i do cen. Díky vývoji vlastního HW se Fortinet nemusí spoléhat na řešení třetích stran a dosahuje velmi vysoké výkonnosti za zajímavou cenu.

Mimoto je společnost Fortinet jediným dodavatelem síťových bezpečnostních řešení, kterému dodává úplnou analýzu aktuálních hrozeb, a veškeré bezpečnostní a aplikační signatury pro všechny produkty vlastní globální tým, který neustále sleduje bezpečnostní scénu a poskytuje zákazníkům nepřetržitou ochranu před nejnovějšími internetovými hrozbami v reálném čase. Odborný tým v laboratořích FortiGuard čítá přes 200 výzkumných analytiků, techniků a forenzních specialistů rozmístěných po celém světě, kteří poskytují bezpečnostní aktualizace 24 hodin denně 7 dní v týdnu, a to s bezkonkurenční dobou reakce na nové a rozvíjející se hrozby, které ohrožují sítě, obsah a mobilní zařízení zákazníků.

## Nadstandardní zákaznická podpora v českém jazyce

Na českém trhu působí společnost Fortinet již devět let a má zde velice silnou pozici. Technické a asistenční centrum v Praze zaměstnává řadu inženýrů v jednotlivých úrovních podpory, což umožňuje rychle a flexibilně řešit požadavky a dotazy bez ohledu na jejich náročnost. Obrovskou přidanou hodnotou technické podpory Fortinet oproti konkurenci je možnost komunikace v českém jazyce. Zákazníci se tak nemusí obávat zdlouhavé a složité komunikace s technickou podporou v jiných zemích, potažmo dokonce v jiných časových pásmech. Fortinet si zakládá na tom, aby bezpečnost, kterou si firma koupí, nebyla bezpečností jen k datu nákupu, ale po celou dobu životnosti zařízení.

Přesvědčte se sami, jak Vám Fortinet Security Fabric pomůže vyhovět současným požadavkům nařízení GDPR.

FORTINET

# Chování uživatelů v kyberprostoru a ochrana citlivých dat

***V následujícím textu představíme pohled společnosti Forcepoint na nové možnosti v oblasti zajištění ochrany citlivých dat pomocí identifikace potenciálně rizikového chování uživatelů, kteří mají k citlivým datům přístup a které s vysokou mírou pravděpodobnosti předchází úniku dat.***

Na úvod zmíníme několik skutečností. V roce 2016 bylo celosvětově vydáno cca 80 mld. USD na bezpečnostní řešení v oblasti IT, ale dle údajů analytických společností počet bezpečnostních incidentů stále rostl. Dále dle celosvětové studie společnosti Forcepoint z roku 2016 (cca 1 200 respondentů z celého světa) se 80 % odborníků na bezpečnost domnívá, že porozumění chování uživatelů v kybernetickém prostoru je důležité, ale méně než třetina uvedla, že chování svých uživatelů rozumí.

Na základě výše uvedených faktů se v centru pozornosti našich technologií ocitl uživatel jakožto společný jmenovatel většiny bezpečnostních incidentů. Podívejme se na uživatele blíže a na rizika, která může představovat. Vezměme si například pozici generálního ředitele společnosti, což je pravděpodobně jedna z největších výzev pro oddělení bezpečnosti. Je nejvyšší autoritou, má přístup do všech interních systémů, má informace o plánovaných krocích společnosti (např. akvizice) a u některých společností také ovlivňuje a schvaluje bezpečnostní politiku, a jedná se tedy o důvěryhodnou osobu. Je ovšem možné, že se vlivem okolností změní ze dne na den z důvěryhodné osoby na nedůvěryhodnou. U dalších zaměstnanců může dojít k odcizení jejich identity s následkem možného kompromitování firemních systémů. Odpověď na otázku, jak nebezpečným se může uživatel stát, není jednoduchá a záleží na různých faktorech, které ovlivní cíle chování uživatele. Uživatel může být nespokojen v práci, uvažuje o přechodu ke konkurenci nebo pouze udělá chybu a klikne na odkaz v mailu, který jej zavede na webovou stránku, která je infikovaná, a útočník získá přístup do interních systémů – možností je mnoho. A je důležité, jakým způsobem se dostal útočník dovnitř, nebo je důležitý pouze fakt, že ke kompromitaci došlo? Za útoky stojí malware a cílí na nejzranitelnější bod v celém systému – na uživatele.

Uživatelé se nechovají vždy předvídatelně podle předem daných vzorců chování a využívají ke své práci rychle se vyvíjející nové technologie, jako jsou mobilní zařízení, mobilní a cloudové aplikace atd. Reakcí dodavatelů a zákazníků na tyto nové trendy je vývoj a implementace dalších a dalších bezpečnostních technologií, které je mají

chránit před nejnovějšími hrozbami. Dnes mluvíme o umělé inteligenci, machine learning, big datech jako možném svatém grálu, který pomůže nové výzvy v oblasti kybernetické bezpečnosti vyřešit.

Ale najít útočníka v reálném čase, který je důkladně ukryt v IT infrastruktuře, který se může chovat jako kolega v kanceláři, kterému důvěřujete, a který ví, že jej hledáte..., vyžaduje nový přístup. Víme, že nové spotřebitelské technologie a inovace, pokud jsou využívány ve firemním prostředí, mění způsob práce a chování uživatelů. Díky těmto technologiím se dostávají citlivá data mimo chráněný prostor firemního datového centra na mobilní a BYOD zařízení, USB disky, na veřejná cloudová úložiště. A aby byla situace ještě složitější, na mobilních zařízeních máme osobní i firemní aplikace a přenos dat mezi nimi je možný (pokud nemáme perfektně implementováno například MDM). Technologické změny způsobily, že již nemůžeme uvažovat v intencích „starého" světa, kde jsme měli IT pod kontrolou a bylo chráněno za zdmi našeho datového centra.

## Jak můžeme na tuto situaci reagovat?

Jednou z možností je přestat se spoléhat pouze na ochranu, kterou nám poskytují zdi datového centra, a podívat se na bezpečnost z pohledu uživatele, jeho chování a motivaci. Dále předpokládejme, že útočník je v naší síti, a přemýšlejme, jak jej identifikujeme a zastavíme. Vraťme se k otázce big data – každá společnost má milióny záznamů v logovacích souborech o síťovém provozu, koncových zařízeních, ale tyto nám většinou nepomohou, pokud nespojíme chování uživatele při jeho práci s informačními systémy a citlivými daty. To je oblast, ve které vidíme další směr vývoje kybernetické bezpečnosti s cílem rozumět chování uživatelů při práci a rozlišit dobré a špatné chování a úmysly a v ideálním případě rozumět chování uživatelů (zaměstnanců) tak, jako obchodní řetězce rozumí svým zákazníkům. Protože uživatelé jsou jedinou konstantou, která pracuje s citlivými daty a informačními systémy a která může být jednoduše překonána sofistikovanými metodami kybernetických hrozeb.

## Jaké jsou důsledky výše uvedených skutečností?

V historii kybernetických hrozeb jsme se téměř výlučně zaměřili na útočníky vně našich systémů a na ochranu před nimi. V současné době ale může potenciální nebezpečí představovat libovolný uživatel v naší síti svým úmyslným nebo neúmyslným chováním. A tito uživatelé se nacházejí v našich systémech dnes a je důležité rozumět jejich chování.

Pokud se zeptáme osoby zodpovědné za IT bezpečnost (např. CISO), kdo ví o uživatelích společnosti víc, zda Google, Facebook nebo jejich zaměstnavatel, odpověď je v 99 % Facebook. To ale znamená, že spotřebitelé, kteří jsou zároveň uživateli (zaměstnanci), jsou ochotni dobrovolně sdílet informace o sobě a svém chování s třetími stranami výměnou za poskytnutí e-mailu, aplikací, nebo jiných služeb zdarma.

## CISO mohou využít tohoto konceptu a:

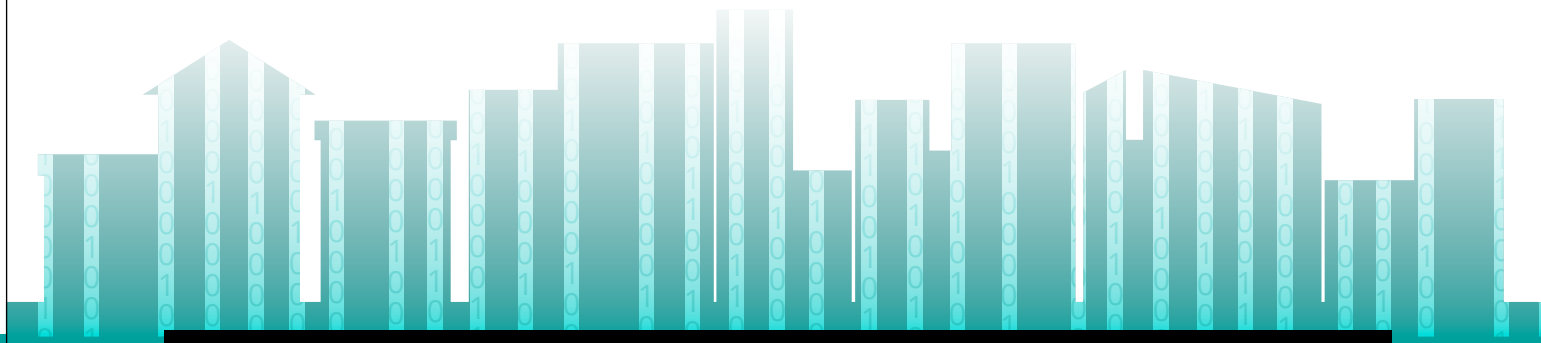
- porozumět chování a úmyslu uživatelů při práci s citlivými daty a informačními systémy;
- identifikovat ty uživatele, kteří představují největší riziko z pohledu kybernetické bezpečnosti;
- pomocí crowdsourcingu vlastních zaměstnanců, jejich přístupu a chování zvýšit odolnost proti kybernetickým hrozbám a zajistit ochranu citlivých dat.

## Na závěr krátké shrnutí:

Každý uživatel firemních systémů je zodpovědný za bezpečnost citlivých dat a zároveň může představovat bezpečnostní riziko. Začněme přemýšlet nikoliv pouze v technologické rovině, ale v rovině chování uživatele a naučme se rozumět uživatelům tak, jak jim rozumí například poskytovatelé sociálních sítí, a budeme schopni identifikovat uživatele s rizikovým chováním dříve, než dojde k bezpečnostnímu incidentu.

FORCEPOINT
POWERED BY Raytheon

**Společnost Forcepoint vznikla v roce 2015 sloučením společností Websense a zbrojovky Raytheon. Websense má desítky let zkušeností v oblasti filtrování webového provozu, ochrany e-mailové komunikace a zabránění únikům citlivých informací. Raytheon díky své divizi Raytheon Cyber Security disponuje unikátními technologiemi pro ochranu před stále sofistikovanějšími typy kybernetických hrozeb.**



## Síťová virtualizační platforma pomáhá zvýšit bezpečnost IT

***Síťovou virtualizační platformu VMware NSX již používá více než 2400 zákazníků z řad firem i institucí a je tak nejrozšířenější platformou svého druhu. Nejnovější verze této platformy jsou plně uzpůsobeny potřebám IT oddělení a nabízejí lepší podporu pro nejdůležitější „use cases", k nimž IT virtualizaci využívá — automatizaci, zabezpečení a zajištění nepřetržitého provozu aplikací.***

Svým uživatelům přináší platforma VMware NSX síťové funkce a zabezpečení zaměřené na aplikace bez ohledu na podkladovou infrastrukturu. NSX je hlavním prvkem strategie společnosti VMware podporovat transformaci sítí.

„VMware NSX je nejrozšířenější, v praxi osvědčená síťová virtualizační platforma," uvádí Milin Desai, viceprezident společnosti VMware pro produkty, sítě a bezpečnost. „Poslední aktualizací pokračujeme ve zvyšování užitné hodnoty platformy NSX s ohledem na nejčastější způsoby jejího využití a zároveň ještě více zjednodušujeme její provoz i v rozsáhlých implementacích. Nadále také investujeme do NSX jako síťové virtualizační platformy, která může sloužit v heterogenních prostředích a umožňuje našim zákazníkům volit mezi novými aplikačními rámci nebo bez obav přejít do veřejného cloudu."

Mezi zákazníky, kteří již implementovali síťovou virtualizační platformu NSX, patří například Burza cenných papírů Praha. Miroslav Prokeš, ředitel odboru technického rozvoje a provozu BCPP, k tomu říká: „VMware NSX umožňuje pražské Burze cenných papírů zajistit spolehlivé a trvalé zabezpečení citlivých informací nejen pro naši společnost, ale i pro ostatní v naší skupině. NSX umožňuje mikrosegmentaci sítě, díky čemuž můžeme přesně naladit bezpečnostní nastavení pro jednotlivé aplikace a výrazně zvýšit celkovou úroveň zabezpečení."

## Příklad z praxe: Progresivní holandské město chrání data svých obyvatel a plní zákonné povinnosti pomoci řešení VMware NSX

***Holandské město Zoetermeer zavedlo kvůli zvýšení bezpečnosti ve svých datových centrech model nulové důvěry s mikrosegmentací pomocí řešení VMware NSX. Zoetermeer tak naplňuje požadavky národního předpisu BIG, který stanovuje základní úroveň bezpečnosti dat holandských měst a obcí.***

Zoetermeer je moderní, rychle se rozrůstající město v provincii Jižní Holandsko. Zajišťuje místní služby, jako je provoz vodovodní a kanalizační soustavy a likvidace domovního odpadu, pro zhruba 125 000 obyvatel. Jako progresivně smýšlející organizace si město Zoetermeer uvědomuje, že stoupající počet kybernetických útoků proti podnikům a organizacím ukazuje na nedostatečnou účinnost tradičních bezpečnostních modelů.

Město proto zavedlo IT řešení, které považuje vše uvnitř sítě za „nedůvěryhodné". Pro zavedení bezpečnostního modelu nulové důvěry město Zoetermeer nasadilo síťovou virtualizaci VMware NSX. Tento model bylo možné zavést díky jedinečné schopnosti řešení NSX mikrosegmentovat síť. Město Zoetermeer nyní člení jednotlivé prvky sítě do oddílů a aplikuje na ně automatizovaná, podrobná bezpečnostní pravidla.

„Město Zoetermeer chce poskytovat svým občanům digitální služby a také svým zaměstnancům digitální nástroje pro co nejefektivnější práci," říká van Gaalen, IT manažer města Zoetermeer. „Na prvním místě však musí vždy být bezpečnost. Díky VMware můžeme správným lidem – občanům i zaměstnancům – poskytovat přístup ke správným datům odkudkoli."

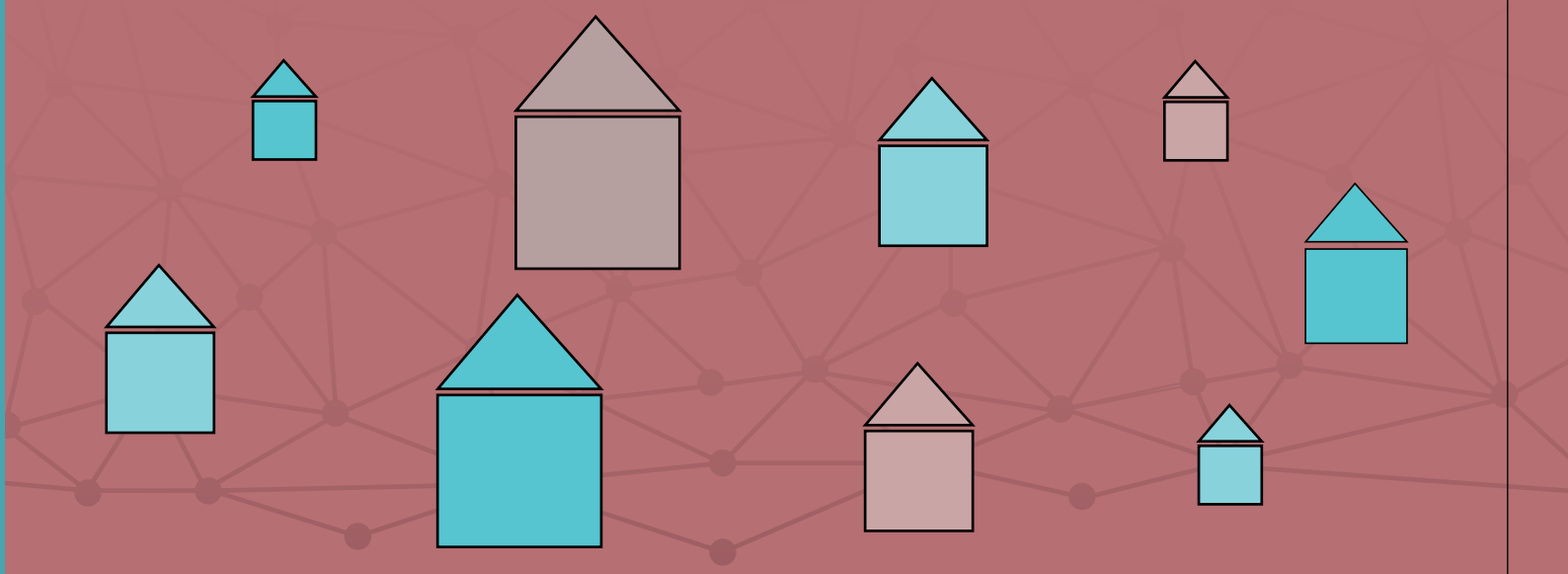
Vedle zajištění vysoké úrovně zabezpečení v datovém centru pomohlo toto řešení městu dodržovat striktní regulatorní požadavky. Řešení VMware NSX městu Zoetermeer fakticky umožnilo naplnit požadavky předpisu BIG, který stanovuje základní úroveň bezpečnosti dat holandských měst a obcí. Pravidla BIG představují soubor bezpečnostních opatření, které zajišťují minimální přijatelnou úroveň informační bezpečnosti v městech a obcích. K naplnění požadavků jsou vyžadovány optimalizované a transparentní IT procesy a bezpečnostní pravidla.

„VMware městu pomáhá splnit náročné požadavky centrální správy na IT bezpečnost a ochranu dat. Díky mikrosegmentaci můžeme v síti lépe řídit bezpečnostní pravidla pro jednotlivé aplikace a výrazně snižovat rizika. Byl to pro nás jednoznačně další krok k vytvoření bezpečného softwarově definovaného datového centra," doplňuje van Gaalen.

Pro Zoetermeer to nebyla první zkušenost s VMware – je dlouholetým zákazníkem a bylo prvním nizozemským městem, které zavedlo platformu VMware Horizon pro virtualizaci desktopů. Na své cestě k mobilní digitalizaci brzy – po otevření nově postavené radnice – poskytne většině svých zaměstnanců digitální pracovní prostory. Nasadí také řešení VMware AirWatch® pro bezpečnou správu služebních mobilních zařízení a pro efektivnější podporu rostoucího počtu mobilních pracovníků.

vmware®


www.egovernment.cz



# eIDAS

***Elektronická identita nabývá v současné době na stále větší důležitosti. A díky zákonu o elektronické identitě a díky novým občanským průkazům se pomalu, ale jistě, přesouvá z oblasti nákupů v e-shopech, komunikace s bankou či operátory i do oblasti komunikace s naší veřejnou správou. Je to k nevíře, ale snad nakonec opravdu dojde k naplnění hesla „Obíhají data, nikoli občané".***

Od poloviny příštího roku se totiž budeme moci, a to nejen v rámci ČR, ale v rámci celé EU, prokazovat a identifkovat vůči veřejné správě na dálku. Budeme moci realizovat něco, čemu se říká úplné elektronické podání. Bez toho, že bychom, s prominutím, zvedli zadek ze židle, bude možné požádat konkrétní úřad o vyřízení konkrétní žádosti přičemž „systému" dáme svolení, aby zkompletoval veškeré potřebné podklady, které vlastní a jež jsou pro takovou žádost potřebné. Představa krásná, která sebou nese pocit luxusu a pohodlí.

Krom toho zdá se, mohla by nám eOP ušetřit i místo v kapse. Nemuseli bychom tahat množství kartiček a průkazů a mohli bychom mít všechno sraženo do jedné jedinné. Konec konců, informační systém základních registrů skutečně většinu zásadních dat o našich osobách už obsahuje. Elektronická občanka se tak může stát klíčem k otevírání této pokladnice informací a usnadnit nám občanům život a úředníkům veřejné správy jejich práci.

Ale nic není zadarmo. Identita takto lehce prokazatelná, je i lehce zcizitelná. Proto budeme muset, rozhodneme-li se využívat možností, které nám bude elektronický občanský průkaz skýtat, daleko pečlivěji než doposud, tuto malou plastovou kartičku hlídat. Oč méně toho na ní bude vidět zvenčí o to větší datové bohatství bude nabízet uvnitř a to bude lákat.

I proto na následujících stránkách předkládáme informace nejen ze semináře na téma ELEKTRONICKÁ IDENTITA PRO KAŽDÉHO, který jsme pořádali v Poslanecké sněmovně Parlamentu ČR, ale i další v souvislosti s GDPR (General Data Protection Regulation – nařízení EU o ochraně osobních údajů). Je totiž dobré vědět, co můžeme a musíme dělat abychom se cítili nejen komfortně, ale i bezpečně.

# Nařízením eIDAS to jen začalo, aneb co nového nás čeká v letech 2017–2018

***Robert Piffl, poradce náměstka ministra vnitra, umístil do své prezentace větší množství slidů, než o kterých bude hovořit tak, aby se účastníci mohli v klidu následně zorientovat jak v problematice elektronické identifikace, tak v dalších aktualitách „e-světa" (prezentace k dispozici na www.egovernment.cz pod odkazem na seminář Kyberbezpečnost víc než zákon). Každopádně za velice důležité považuje zdůrazňovat, že nařízení eIDAS je skutečně závazné v rámci celé EU – má tedy přímou účinnost i v rámci České republiky. MV ČR v této souvislosti vytvořilo dva právní předpisy – zákon o službách vytvářejících důvěru pro elektronické transakce (již realizován) a návrh zákona o elektronické identifikaci (PSP ČR přijala 9. 6. 2017). Krom toho od 25. 5. 2018 vstupuje v účinnost i nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně osobních údajů, které má přednost před národní úpravou.***

## NÁVRH ZÁKONA O ELEKTRONICKÉ IDENTIFIKACI

Novela zákona o občanských průkazech byla schválena Poslaneckou sněmovnou 7. 4. 2017, nyní je v Senátu a předpokládá se její brzké schválení. Jakmile vyjde ve Sbírce zákonů, začnou platit ustanovení v tomto právním předpisu uvedená.

V souvislosti se záměrem elektronických občanských průkazů s čipem byl rovněž zpracován návrh novely zákona o informačních systémech veřejné správy. Zde byl definován přístup se zaručenou identitou do informačních systémů veřejné správy. Jedná se do jisté míry o určitou pojistku, kdyby nebyl přijat zákon o elektronické identifikaci, ale novela o OP ano, bude možné pomocí OP vstupovat do informačních systémů veřejné správy a požadovat například výpisy a další záležitosti. Souběžně byly novelizovány předpisy v oblasti sociálního a zdravotního pojištění, a i zde bude možné činit určité kroky. I kdyby tedy nebyl schválen návrh zákona o elektronické identifikaci (PSP ČR schválila 9. 6. 2017, nyní je v Senátu ČR), bylo by možné použít občanský průkaz alespoň v určitém, limitovaném záběru.

Právní základ máme v současné době vymezen na jedné straně zákonem o archivnictví a spisové službě (vymezeno, jak se zachází s elektronickými dokumenty v rámci veřejné správy) a na druhé straně zákonem o službách vytvářejících důvěru, který upravil určitá specifika v rámci ČR. K dispozici je dvouleté přechodné období, po které se může místo kvalifikovaného podpisu podle nařízení eIDAS používat uznávaný podpis atp. Základ určité „revoluce" i v rámci EU vidí Robert Piffl ve vytvoření jednotného právního základu pro tzv. oznámené systémy elektronické identifikace. Zároveň byly, v rámci celé EU, zavedeny jednotné pojmy v této oblasti tak, abychom si rozuměli a hovořili skutečně o tomtéž.

## ELEKTRONICKÁ IDENTIFIKACE

Přímo v nařízení o elektronické identifikaci byl vymezen samotný pojem elektronická identifikace. Jedná se o postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou, právnickou osobu anebo fyzickou osobu jednající v roli právnické osoby.

Stejně tak jsou zde zavedeny termíny autentizace, bezpečný prostředek, co jsou spoléhající se strany atp.

Jak Robert Piffl připomněl, ani při samotném prezenčním prokázání totožnosti, kdy se občan fyzicky dostaví a identifikuje, nemáme stoprocentní jistotu, že to je skutečně ta

osoba, za níž se vydává. V elektronickém světě je tato nejistota ještě umocněna prokazováním na dálku, které je neosobní, a tedy jakoby vyzývá k pokusům o podvod, neboť riziko odhalení zde je, zdánlivě, nižší než v onom reálném světě. I proto nařízení eIDAS zavádí určitou míru důvěry tohoto ověření, a to ve třech úrovních – nejnižší, střední a nejvyšší. V rámci veřejné správy bude pro řadu úkonů akceptován pouze nejvyšší stupeň důvěry, ale v rámci jednotlivých právních předpisů a systémů, které budou v české veřejné správě nabízeny, může, například pro pořízení určitých výpisů, postačovat střední, nebo nízká úroveň důvěry.
Podstatné je rovněž to, že nehovoříme pouze o eOP, ale o jakémkoliv prostředku, který slouží pro vzdálenou identifikaci. V tomto směru je kritické ono prvotní ztotožnění. Fyzická osoba se dostaví na úřad a bude chtít spárovat svoji fyzickou existenci s elektronickou identitou. Pokud dojde k ověření této identity, je osobě vydán bezpečný prostředek, který se nedá přepsat a má řadu ochran, a díky tomu se může tato osoba prokazovat svojí identitou i na dálku. Vzrušivé diskuze se v tomto směru vedly vzhledem k tomu, že budeme muset této prvotní identifikaci důvěřovat stejně, ať byla provedena v kterékoliv zemi EU.

## PROČ?

Od 1. 7. 2016 je kvalifikovaný podpis na elektronickém dokumentu stejně závažný, jako vlastnoruční podpis na listině, a to napříč Evropou. Pokud tedy disponujeme kvalifikovaným podpisem, je možné elektronicky komunikovat s úřady různých států již nyní. Nicméně pro řadu úkonů bylo a bude požadováno prokazování totožnosti a toto doposud nebylo na dálku možné.
Nyní tedy nastává čas, kdy celá Evropa musí v rámci eIDAS nejpozději od 29. 9. 2018 při jakékoliv on-line službě, kterou ten který stát nabízí, akceptovat v rámci oznámených systémů elektronické identifikace přístup konkrétních fyzických osob i z jiných států EU. Bude tedy možné, aby se kdokoliv přihlásil do systémů veřejné správy jakéhokoliv státu EU a činil zde konkrétní elektronická podání a další úkony.
I proto bylo v rámci našeho právního řádu zavedeno prokázání totožnosti s využitím elektronické identifikace (návrh zákona paragraf 2) a zároveň zavedena povinnost použití, v rámci existujících on-line služeb, elektronické identifikace (pravděpodobně od 1. 7. 2018, kdy se předpokládá podle zákona o elektronické identifikaci nabytí účinnosti zákona o elektronické identifikaci).

Opět zde existuje dvouleté přechodné období tak, aby se veřejná správa mohla připravit, opravit svá portálová řešení atd. Nicméně bude právem občanů nutit veřejnou správu, aby je na dálku identifikovala.
Jak bylo řečeno, eOP bude pouze jedním z těch prostředků, kterými je možné se takto na dálku identifikovat (rovněž mobilem, jinou kartou, případně dalšími prostředky ...). V tomto smyslu záleží především na tom, kdo se stane akreditovaným poskytovatelem identitního prostoru. I proto bylo definováno, co je to národní bod, který bude provozovat Správa základních registrů a který bude sloužit k výměně informací o elektronické identifikaci a identitách napříč EU.

## ÚPLNÉ ELEKTRONICKÉ PODÁNÍ?

Dá se říci, že za touto prací je snaha o naplnění, v souvislosti s e-governmentem již poněkud otřepaného, pravidla – budou obíhat data, nikoli občané. Konkrétně tedy směřujeme k úplnému elektronickému podání. Nyní je možné prostřednictvím e-mailu zaslat úřadu elektronický dokument opatřený kvalifikovaným podpisem. To však není úplně komfortní postup, navíc ne vždy je možné takto obsáhnout všechny agendy. V řadě případů je nutné shromáždit určité údaje a nějak formalizovat zasílaný dokument atp. Naše veřejná správa však už nyní disponuje v rámci backendu řadou informací a dat. Pokud se tedy občan do určité on-line služby přihlásí pomocí elektronické identifikace, měl by právě portál občana zajistit, aby byly všechny potřebné informace, data z veřejných informačních systémů připraveny, sestaveny do určitého formalizovaného podání a občan pak pouze klikáním projeví svou vůli odeslat a předat takové podání konkrétnímu úřadu. Úplné elektronické podání tedy znamená, že občan se identifikuje, vybere si životní situaci, kterou potřebuje řešit, a požádá informační systémy veřejné správy o všechna data, která jsou potřebná k takovému podání doplnit.

## CO NÁM K TOMU CHYBÍ?

Robert Piffl připomněl, že ústava stanoví, že státní moc slouží všem občanům a lze ji uplatňovat jen v případech a mezích, které stanoví zákon. Zdůraznil tedy, že veřejná správa se musí chovat právě podle tohoto ustanovení. I proto byla podle jeho slov věnována velká pozornost propojení informačních systémů veřejné správy. Nyní je nutné, aby jednotlivé resorty byly schopny na základě těchto nástrojů změnit svoje agendové zákony. V rámci MV ČR byla realizována analýza celého právního řádu, která popisuje případy, kde konkrétně právní předpisy znemožňují identifikaci na dálku, nebo obsahují určité ustanovení typu „nutno předložit na formuláři konkrétního formátu a velikosti" atp. Prostřednictvím Rady vlády pro informační společnost bude prezentováno, co je nutné v tomto směru opravit tak, abychom dosáhli plného e-governmentu a fungování veřejné správy elektronicky. Nicméně, beze změn zákonů to skutečně nebude možné, a to ani v případě, že už budeme mít platný zákon o elektronické identifikaci. Proto je nutno co nejdříve začít s jeho úpravami.

## OBČANSKÝ PRŮKAZ S ČIPEM

Občanský průkaz je nyní navržen tak, aby vyhovoval jak současným, tak budoucím požadavkům nařízeni eIDAS. Není zde zohledněna pouze oblast elektronické identifikace. Na občanský průkaz s čipem bude totiž možné umísťovat rovněž „státní" podpisy. Jsou zde tedy zohledněny rovněž požadavky nařízení eIDAS na bezpečný prostředek pro kvalifikované podpisy. Jak bylo řečeno, jedná se o jeden z možných prostředků k prokázání identity. Tento však bude vydáván státem a stát ručí za informace, které obsahuje, a to nejvyšším stupněm záruky.

Pokud bude v rámci našeho právního řádu přijat zákon o elektronické identifikaci a nějaký soukromoprávní poskytovatel projde akreditací, tak jeho identitní prostředek bude zcela rovnocenný s touto elektronickou občankou (například řešení pro mobily jako nástroj identifikace).

MV ČR připravilo tři poměrně závažná usnesení pro jednání vlády - dvě už proběhla loni, jedno je teď na vládě a mělo by projít (usnesení k úplnému elektronickému podání a elektronické fakturaci). Z těchto usnesení vyplývají pro veřejnou správu určité termíny, kdy mají být připraveny systémy spisových služeb, upraveny směrnice atp. Snahou MV ČR je tlačit veřejnou správu, aby otevřela svoje agendové systémy tak, aby občan mohl skutečně fungovat elektronicky.

Pravdou ale je, že v současné době neexistuje na území ČR žádný informační systém, který by byl ztotožněn v souladu s prováděcím aktem pro úroveň vysoké záruky.

## NEDOSTATKY

Největším rizikem je, podle Roberta Piffla, určitá míra počítačové negramotnosti. V rámci populace existuje a bude vždy existovat určitá část, která nebude ochotna či schopna tyto nástroje používat. Platí to bez ohledu na věkové limity. Opačný problém je s mladou generací, kde panuje až přílišná důvěra v elektronický svět. Zde je nutné vysvětlit důsledky právního konání tak, aby bylo zřejmé, že se skutečně jedná o prostředek, který leccos umožňuje, ale je na druhou stranu nutné s ním zacházet s určitou opatrností, protože ztráta identity může mít v tomto směru fatální důsledky.

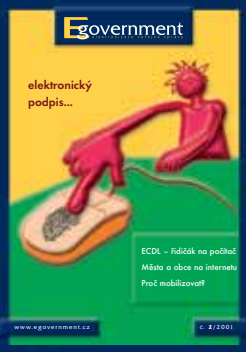
## ČASOVÝ PLÁN

Pokud půjde všechno podle plánu, tak:

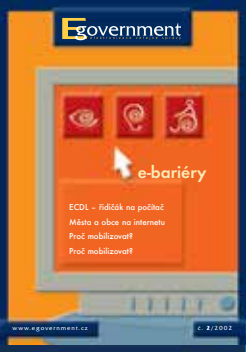
- 25. 5. 2018 vstupuje v účinnost nařízení GDPR;
- v polovině roku 2018 bychom měli mít první eOP s čipem;
- 1. 7. 2018 očekáváme účinnost eID a 29. 9. 2018 bychom měli mít plně účinnou elektronickou identifikaci (to vyplývá z nařízení EU).

# Egovernment

elektronizace veřejné správy

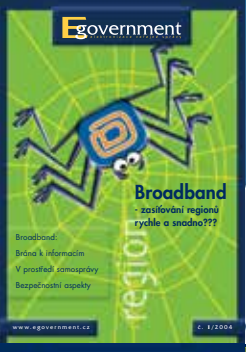




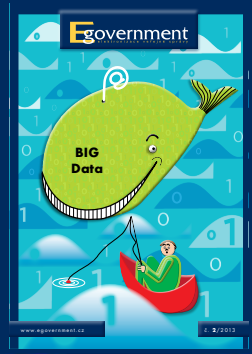








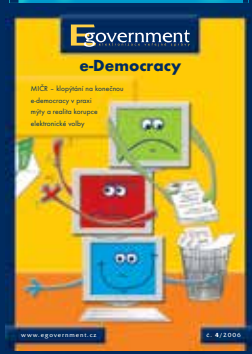


















Vše o elektronizaci veřejné správy
- srozumitelně a zdarma:

**www.egovernment.cz**

# Nejnovější vývoj v oblasti ochrany informačních systémů a dat jimi zpracovávaných

***Tento článek stručně shrnuje základní požadavky na ochranu informačních systémů ve veřejné správě, jakož i dat zpracovávaných těmito systémy, a to se zaměřením na požadavky zákona o kybernetické bezpečnosti, zákona o vojenském zpravodajství, nařízení eIDAS a nařízení GDPR.***

Dramatickému postupu informačních technologií v současném světě nemá právo šanci stačit. Je však žádoucí, aby namísto oněch „dvou kroků pozadu" právo zaostávalo jen o jeden: tedy aby pružně reagovalo a efektivně regulovalo zaváděné technologické novinky, na kterých by slepé uplatnění standardních právních institutů způsobilo nevyhnutelnou škodu. Aby tato ochrana byla komplexní, je třeba, aby splňovala nároky v aspektech bezpečnosti transferu informací, včetně vhodného zabezpečení přenosové infrastruktury, povahy přenášených informací či kvalitní a dostatečné informovanosti zapojených subjektů. Za tímto účelem již bylo přijato množství předpisů; tento článek zamýšlí představit čtyři z nich a upozornit na ně zejména v souvislosti s provozem informačních systémů veřejné správy.

## Zákon o kybernetické bezpečnosti

Již v srpnu 2014 byl s účinností od 1. ledna 2015 přijat na české půdě zákon o kybernetické bezpečnosti. Cílem úpravy bylo zabezpečit Českou republiku a její zájmy před kybernetickými bezpečnostními incidenty. Za tím účelem zákon zavádí minimální standardy pro komplexní bezpečnostní opatření, detekování, nahlašování a reakci na kybernetické bezpečnostní události a související incidenty a také zavádí standardy pro činnost dohledových pracovišť. V tomto smyslu je třeba dodat, že účelem této úpravy není řešit obsahovou složku fungování informační společnosti, nýbrž pouze tuto složku zabezpečit. Zákon dopadá na poskytovatele služeb a sítí elektronických komunikací, osoby zajišťující významnou síť a správce a provozovatele kritických informačních či komunikačních systémů nebo významných systémů.

Kontrolu nad oblastí kybernetické bezpečnosti vykonává NBÚ, který má v souladu s § 25 zákona pravomoc udělovat za zjištěná pochybení pokuty až do výše 100 000 Kč.

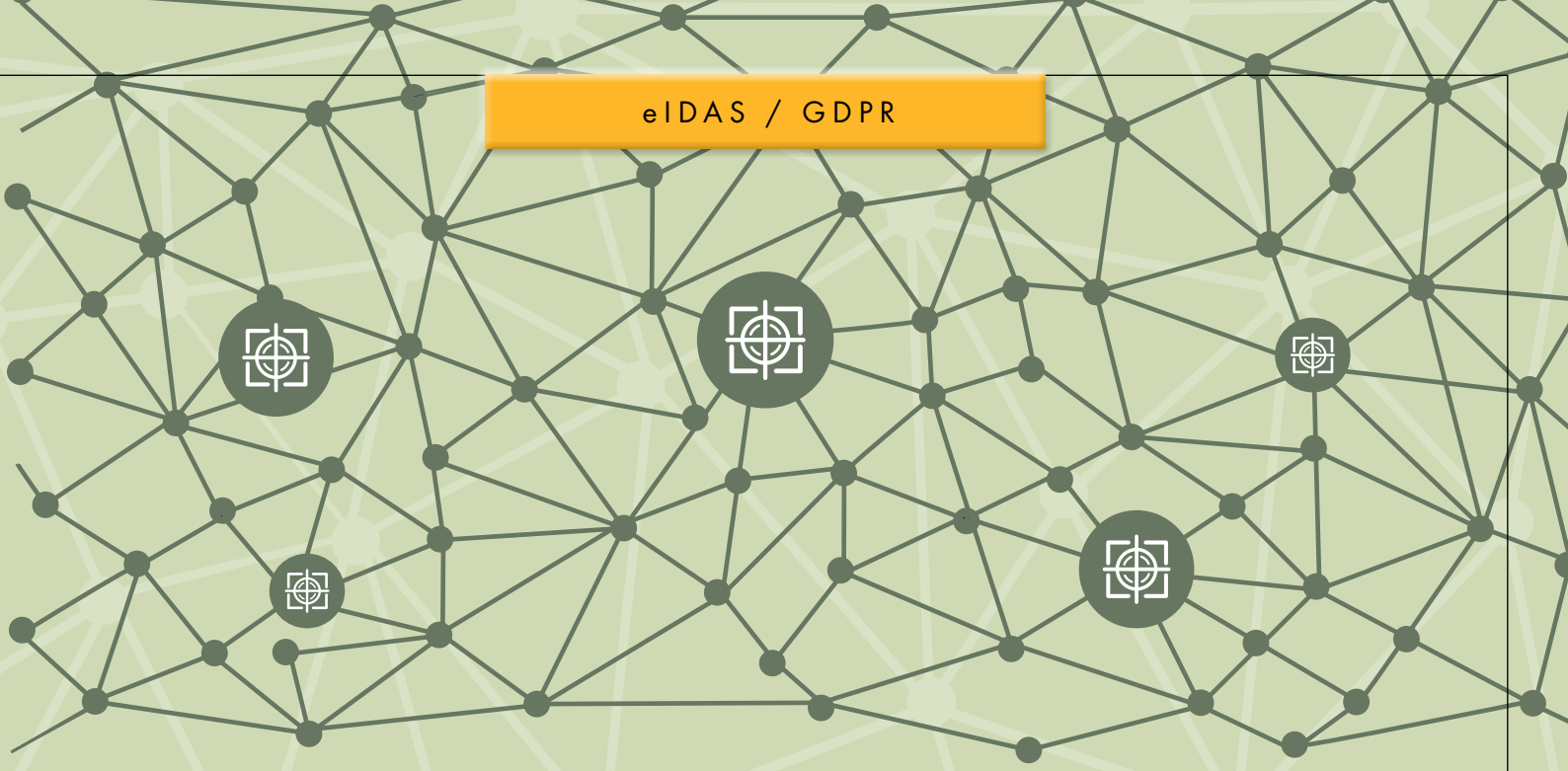
Již dříve byla přijata novela s účinností od 1. 7. 2017, která rozšiřuje působnost zákona na nově definované skupiny provozovatelů/správců IT a dramaticky zvyšuje sankce za správní delikty. NBÚ rovněž bude muset důsledněji kontrolovat splnění zákonných povinností. Poslanecká sněmovna však 12. dubna 2017 přijala další vládní návrh zákona, který má opět rozšířit okruh dotčených osob o poskytovatele a provozovatele některých systémů a služeb a současně upravit hlášení bezpečnostních incidentů. Zákon je momentálně na půdě Senátu a všichni věří, že bude účinný nejpozději na podzim.

## Zákon o vojenském zpravodajství

Stávající zákon o vojenském zpravodajství byl přijat v červnu 2005, s účinností od srpna stejného roku. Jeho účelem je zřízení a definice fungování vojenské zpravodajské služby ve snaze zvýšit obranyschopnost České republiky, chránit její ústavní zřízení a významné ekonomické zájmy.

V říjnu loňského roku byl doručen a současně v prvním čtení projednán vládní návrh novely tohoto zákona, dle kterého by mělo být vojenské zpravodajství zodpovědné za zajištění kybernetické obrany a mohlo při ní využívat technických prostředků kybernetické obrany za účelem předcházení, zastavení nebo odvrácení kybernetického útoku. Tento návrh se setkal s nesouhlasem expertů v oblasti kybernetiky, kteří upozorňují na možnost zneužívání a tím i nepřípustných zásahů do soukromí, stejně jako na nekoncepčnost této obrany; zamítavé stanovisko vyjádřila i Česká advokátní komora.

Další projednávání tohoto zákona, který i po čtyřech doplňujících usneseních přináší velmi vzrušenou debatu nad hranicemi zajištění kyberbezpečnosti a případnými konflikty se základními lidskými právy, bude v průběhu léta 2017 a výsledek této debaty bude významně ovlivňovat směřování kybernetické obrany v České republice.



## Nařízení eIDAS

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (...), známé též jako nařízení eIDAS, nastoluje celoevropskou úpravu tzv. elektronických identit a služeb vytvářejících důvěru: elektronických podpisů, elektronických transakcí, digitálních certifikátů a dalších institutů. Evidenci těchto kvalifikovaných služeb a poskytovatelů vede a zveřejňuje Ministerstvo vnitra na svém webu. Nařízení eIDAS dopadá zejména na subjekty spravující systémy elektronické identifikace a tzv. poskytovatele služeb vytvářejících důvěru.

Kromě samotného nařízení eIDAS byl na českém území přijat zákon č. 297/2016, o službách vytvářejících důvěru pro elektronické transakce, který nařízení doplňuje o některé specifické aspekty českého prostředí. V legislativním procesu je navíc vládní návrh zákona o elektronické identifikaci, který v návaznosti na nařízení eIDAS zamýšlí přímo upravit využívání elektronické identifikace a vyjasnit působnost státní správy na tomto úseku vzhledem k tzv. kvalifikovaným systémům elektronické identifikace. Ministerstvo vnitra si od tohoto zákona slibuje tolik potřebné zakotvení institutu elektronické identity, který dosud v našem právním řádu významně chybí.

## Nařízení GDPR

Nařízením, které poměrně zásadním způsobem zpřesňuje a zpřísňuje podmínky pro ochranu osobních údajů, je nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, známé jako GDPR. Toto nařízení dopadá na veškeré správce a zpracovatele osobních údajů, ať už zpracovávají osobní údaje v rámci svých agend (např. evidence žadatelů o dávky apod.), nebo třeba i jen svých zaměstnanců.

Tato reforma v oblasti ochrany osobních údajů přináší množství novinek, např. zavedení povinnosti jmenovat pověřence pro ochranu osobních údajů pro veřejné správce, zavedení nových práv či podrobnější specifikace práv subjektů, jako je např. právo „být zapomenut“ či právo na portabilitu, zpřesnění a rozšíření povinností správců i zpracovatelů osobních údajů, podrobnější vymezení požadavků na návrh informačních systémů a zabezpečení osobních údajů zpracovávaných těmito systémy, zavedení povinnosti nahlašovat některé bezpečnostní incidenty a v neposlední řadě i dramatický nárůst sankcí za porušení nařízení.

Pro veřejný sektor tato příprava znamená nejen nutnost revize klíčových právních předpisů, ale také nutnost zajištění souladu stávajících dokumentů, procesů a informačních systémů s GDPR, včetně zajištění existence fungujících bezpečnostních a organizačních opatření.

Na veškerou přípravu přitom mají správci a zpracovatelé již méně než jeden rok, než začne být GDPR od 25. května 2018 účinné. Jedná se tak o jednu z největších výzev, kterým správci za poslední roky čelili.

JUDr. Josef Donát, LL.M.

ROWAN LEGAL

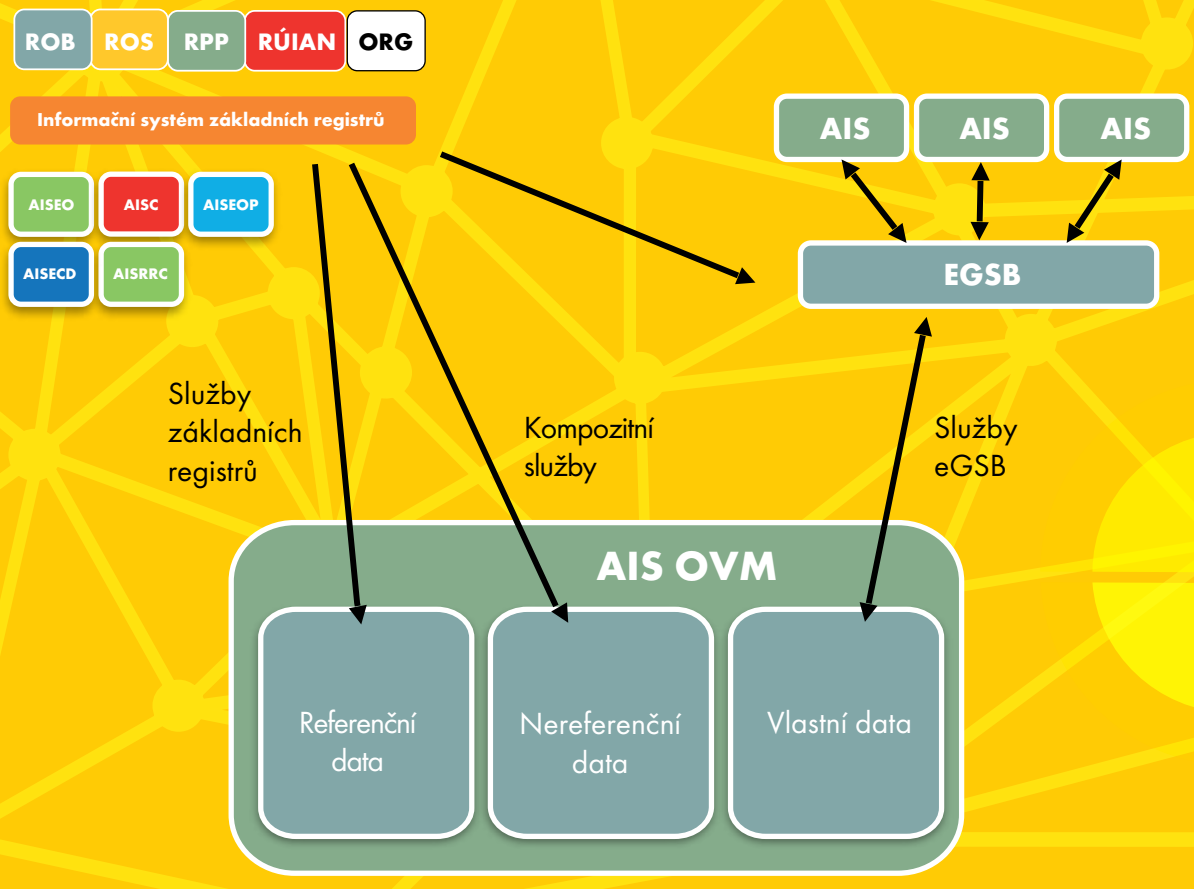
# Základní registry a eIDAS

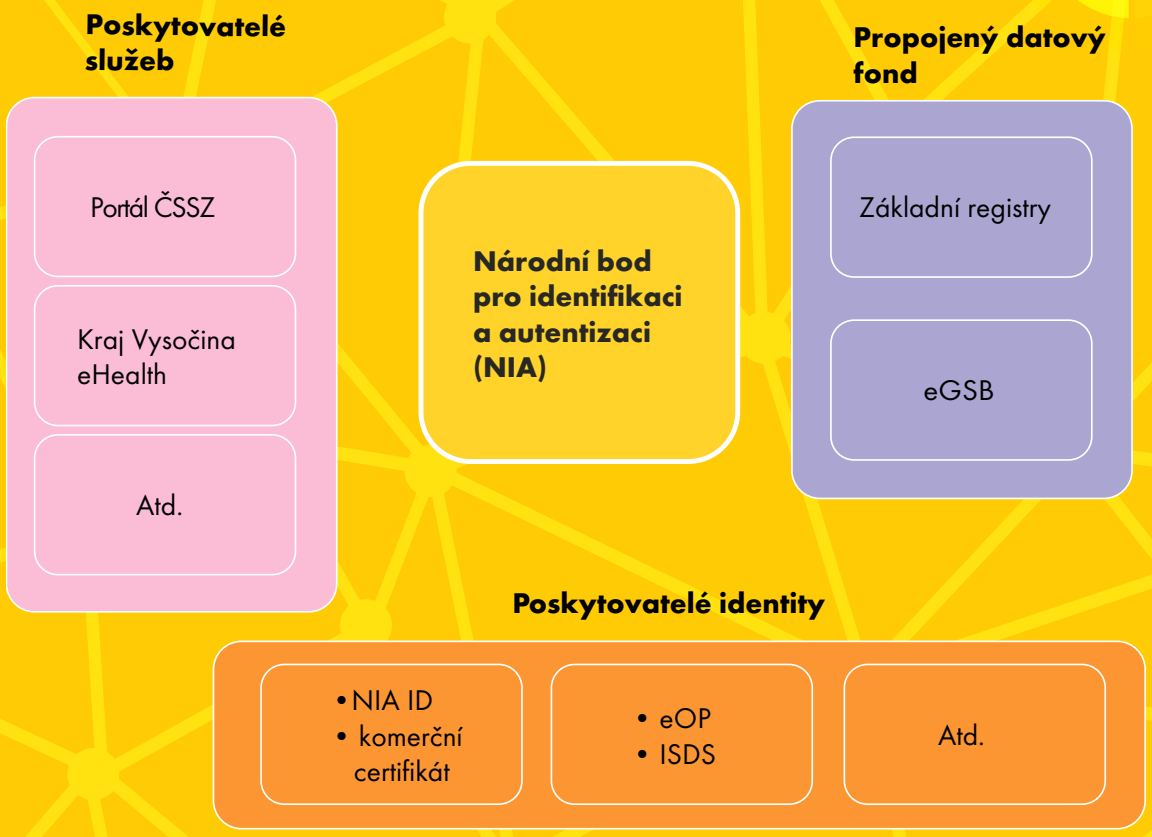
***Situaci eIDAS v souvislosti se základními registry prezentoval ředitel SZR Michal Pešek. Jak uvedl, zhruba poslední dva roky nejde v prezentacích SZR zdaleka tolik o základní registry. Občas je důležité si připomenout, že registry existují a dlouho existovat budou, ale v současné fázi je velice nutným úkolem ostatním vysvětlovat jejich význam tak, aby byli přesvědčeni o možnosti využívání základních registrů pro výkon jednotlivých agend. Jako příklad uvedl využívání již pořízených fotografií občanů například pro řidičské průkazy.***

V rámci samotných základních registrů jsou v současné době tou nejdůležitější záležitostí formuláře a souhlas třetí osobě s poskytováním osobních údajů. Jak řekl Michal Pešek, stále se neposouvá legislativa v oblastech, kdy může druhá strana využívat data základních registrů. Diskuse se v tomto smyslu vedou s Českou bankovní asociací a bankovní sférou obecně o tom, aby příslušní příjemci v soukromoprávní sféře mohli ztotožnit své klienty na základě existujících zákonů. U bank by se jednalo především o zákon o praní špinavých peněz atp. V této souvislosti Michal Pešek ovšem připustil, že je rovněž potřeba posílit marketing v dané oblasti tak, aby o jednotlivých možnostech skutečně existovalo obecné povědomí.

## CO SE POVEDLO

Povedlo se propojit referenční a nereferenční data, což není pouze záležitostí eGon Service Bus. Jedná se o poskytování desítky kompozitních služeb SZR společ-






ně s Ministerstvem vnitra. Nyní se pozornost zaměřuje na dvě služby, které budou poskytovat biometrické údaje (fotografie a podpisy). Tyto služby jsou vždy spojené s výdejem referenčních dat ze základních registrů a k tomu se připojuje informace, která není v základních registrech primárně, například u evidence obyvatel se připojují fotografie a podpisy těchto osob. Jde tedy o to, že v současnosti je možné vytvářet služby, které určitým způsobem skládají data referenční a nereferenční, nicméně je nutná právě ona propagace a určitá míra „přesvědčování", že se jedná o přínos jak občanovi, tak veřejné správě. Pokud jde o určitou statistiku, Michal Pešek uvedl, že základní registry obnášejí v současnosti zhruba 1,2 miliardy vyměněných údajů neboli transakcí. To je samozřejmě velice pozitivní výsledek, ale zároveň upozornil, že v převážné většině veřejná správa využívá data stále přes Czechpoint@office, neboť určitým typům obcí by se nevyplatilo mít vlastní informační systém. Kromě úvah o informačním systému jsou aktuální rovněž diskuze o GDPR, identifikaci CMS2 (nové a bezpečnější připojení pomocí služeb poskytovaných Ministerstvem vnitra). Ve výsledku to pro jednotlivé úřady, které mají vlastní agendové informační systémy, znamená více práce a vyšší investice do těchto služeb.

## CO NÁS ČEKÁ

Elektronická identifikace není z pohledu Michala Peška již pouhá teorie, ale prakticky existuje, máme k dispozici testovací subjekty a čeká se pouze na legislativu. Spolu s Ministerstvem práce a sociálních věcí se podařilo na jejich funkčním portále testování identity datových schránek oproti identitě NIA.Je tedy nutné dobudovat technologie identifikačních certifikátů a podpisové certifikáty. Identifikační budou spojeny s občanským průkazem. Pokud jde o podpisové certifikáty, stát nechce nijak narušovat komerční klima v této oblasti, pouze doplnit tuto službu tak, aby občan skutečně měl možnost využívat podpisový certifikát pro komunikaci se státem. V situaci, kdy si několik stovek tisíc úředníků bude muset pořizovat elektronické podpisy, měl by stát patrně přece jen vlastnit konkrétní technologii.

## SDS (service desk)

Tento systém je podstatný především v situaci, kdy občan má nástroj pro identifikaci, který může být zneužit, a tudíž jej potřebuje okamžitě zneplatnit. V takové chvíli je nutné, aby s ním někdo na tomto procesu spolupracoval. Nebude to ani policie, ani MV, ale právě SZR. V režimu 24x7 by proto měl fungovat Servis Desk pro zneplatňování nikoli samotných OP, ale jeho elektronické části.

## Medializace, dokumentace a příručky

SZR jde nyní především o přípravu podkladové dokumentace a příruček pro orgány veřejné moci a úředníky. Je to zhruba podobný přístup, jaký byl dle slov Michala Peška zvolen v době, kdy se zaváděl Czech POINT a datové schránky. I tehdy museli být proškoleni všichni úředníci v dostatečném časovém předstihu.

## MEZNÍKY:

- v roce 2014 nařízení eIDAS;
- v roce 2016 zákon o službách vytvářejích důvěru pro elektronické transakce;
- posléze usnesení vlády č. 833, ve kterém SZR primárně dostala za úkol vybudovat testovací prostředí - Národní identifikační a identitní autoritu - v souvislosti s OP, protože novela zákona o OP, resp. zákon o OP a o elektronické identifikaci ji vyžaduje.

SZR v roce 2015 společně s Českou poštou, a.s., a OZ, dnes Nakitem, začala budovat strukturu a potřebný systém, který dnes je dokončen. V roce 2016 byla vytvořena detailní funkční specifikace, v říjnu byla vybudována infrastruktura jako podstata pro testovací prostředí národního bodu pro identifikaci a autentizaci. V letošním roce byly připojeny první subjekty - Česká správa sociálního zabezpečení, respektive součást MInisterstva práce a sociálních věcí a Kraj Vysočina.

Nyní SZR spolupracuje s orgány veřejné moci a s poskytovateli služeb, kteří jsou zmíněni v zákoně o elektronické identifikaci, na procesních schématech, jak bude vypadat konkrétní předávání dat. Je téměř dokončeno provozní prostředí, nicméně je nutné počkat, až vyjde zákon o elektronické identifikaci.

## ČEKÁNÍ NA LEGISLATIVU

Michal Pešek v závěru zdůraznil, že vlastně celou dobu hovořil o jednom bodu, který by měl poskytovatelům služeb zajistit, že se k nim přihlašuje skutečně ten konkrétní občan, a jemu naopak zaručit, že služba, které chce využít, patří mezi akreditované poskytovatele služeb.

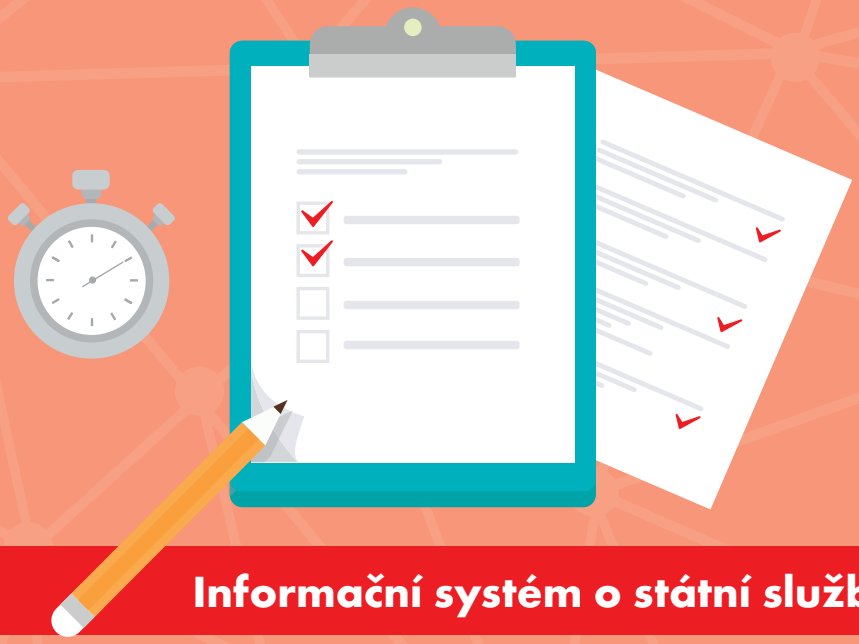
Bude se jednat o jakýsi portál občana, který bude mít na pozadí NIA (národní identitiní autorita). Jejím prostřednictvím se občan přihlásí - identifikuje, otevře se mu konkrétní cesta a pomocí bezvýznamových identifikátorů řekne druhé straně, že toto je skutečně tento člověk. Jedná se tedy o propojení funkcionalit, které již existují, nejsou to žádné nové projekty za stovky miliónů. Jak Michal Pešek zdůraznil, jsme nyní hodně závislí na politické situaci ohledně schvalování legislativy. Pokud vše půjde hladce, budeme si za rok ukazovat, jak je vše připraveno a funguje. Zákon o elektronické identifikaci je navržen s odloženou účinností k 1. 7. 2018. Znamená to, že ještě máme relativně čas. Rozhodně OVM, které chtějí testovat, se mohou obrátit již nyní na stránky eidentita.cz. Bude jedině dobře, pokud přinesou nějaké další služby, které pak lidem zjednoduší život.

Magazín Egovernment spustil přihlašování do nového ročníku soutěže o nejsympatičtější dámu ve veřejné správě. Jste sympatická a komunikativní, nebo máte kolem sebe takové kolegyně? Stačí vyplnit on-line formulář.


# ŠANCE PRO SYMPATICKÉ DÁMY Z VEŘEJNÉ SPRÁVY!

**Více na WWW.EGOVERNMENT.CZ**

Přihlásit se mohou jak přímo samotné dámy, nebo je mohou přihlásit jejich kolegové. Podrobné informace a registrační formulář naleznete na **www.egovernment.cz**

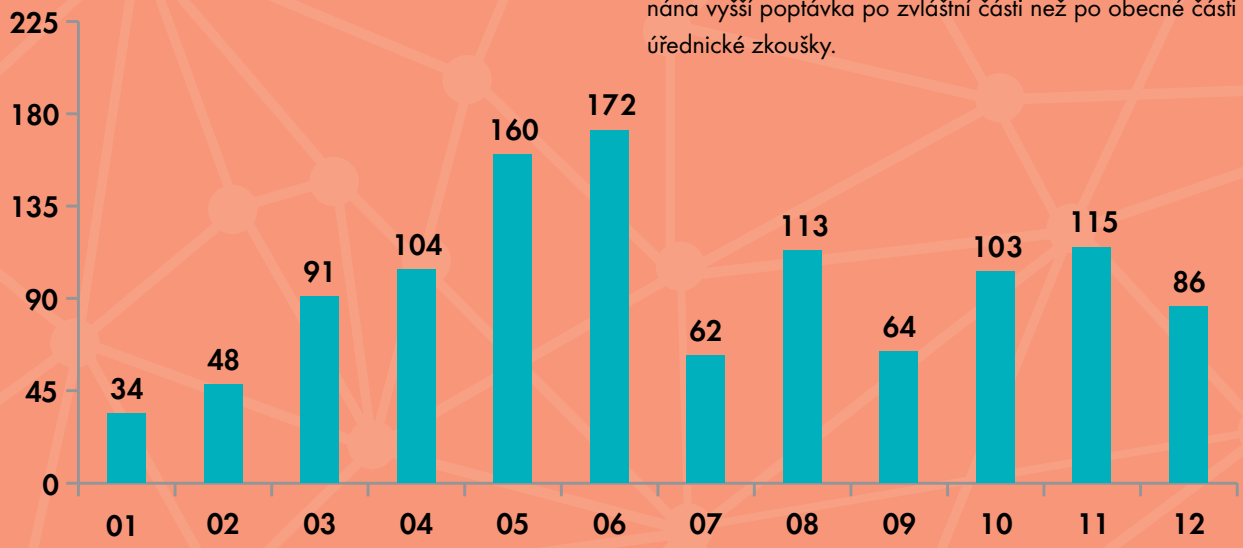


# Informační systém o státní službě

***Informační systém o státní službě (ISoSS) má za sebou již 2 roky provozu, které byly využity pro jeho naplnění informacemi, další rozvoj a zvyšování uživatelského komfortu, ale také např. pro masivní organizaci úředních zkoušek.***

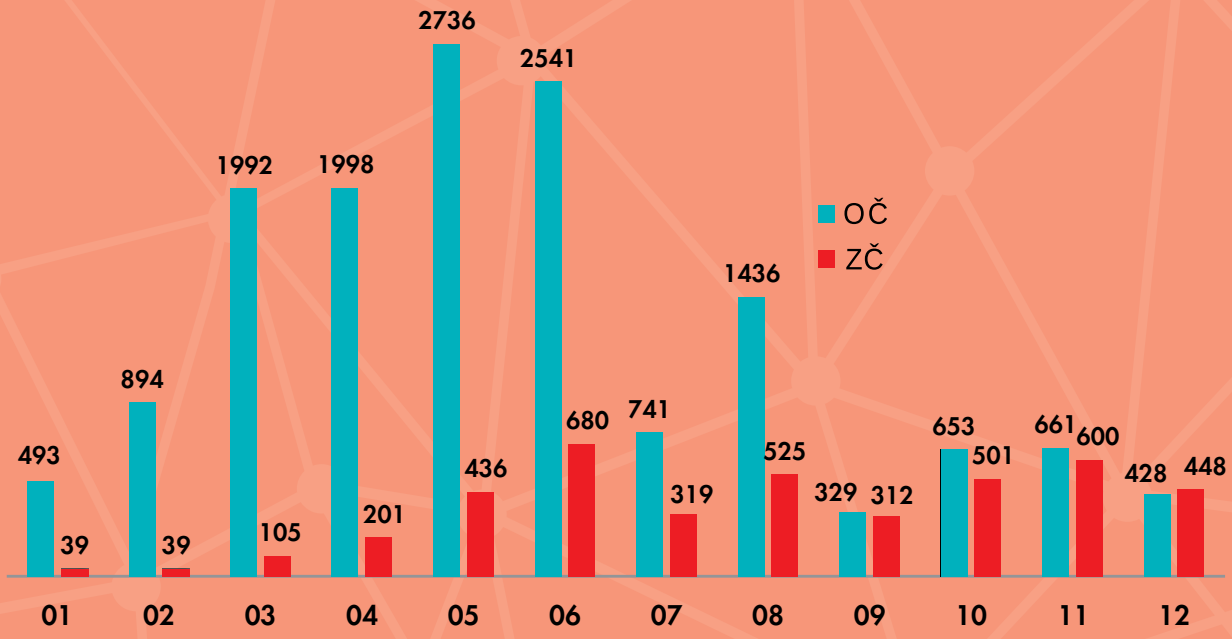
Jen v roce 2016 bylo vypsáno 1 152 termínů pro konání úředních zkoušek. Obecnou část úřednické zkoušky konalo 14 900 osob a zvláštní část 4 205 osob, což ukazují níže uvedené grafy.

Během 1. poloviny roku 2016 byla poptávka ze strany státních zaměstnanců především po obecné části úřednické zkoušky (OČ). Pokles zájmu o obecnou část nastal v průběhu září, kdy byla zveřejněna nová sada 300 zkušebních otázek. Od září se poměr obecných a zvláštních částí (ZČ) značně vyrovnal a v prosinci byla poprvé zaznamenána vyšší poptávka po zvláštní části než po obecné části úřednické zkoušky.




Mimo portál pro přihlašování na úřednickou zkoušku a modul pro evidenci provedených úřednických zkoušek, přes které se realizují úřednické zkoušky, tvoří ISoSS od počátku své existence další dva moduly - rejstřík státních zaměstnanců a evidence obsazovaných služebních míst. Do konce roku 2016 bylo v ISoSS evidováno na 64 tisíc státních zaměstnanců a uveřejněno bylo 22 670 výběrových řízení.

Na začátku roku 2016 byl potom zahájen vývoj nového modulu, nazvaného organizační struktura a systemizace služebních a pracovních míst, zkráceně OSYS.
Modul OSYS zahrnuje osm různých procesů pro řízení předkládání, posuzování a schvalování návrhů změn a aktualizací organizační struktury a systemizace služebních a pracovních míst zařazených ve služebních úřadech dle zákona o státní službě a jeho prováděcích předpisech.




Podstatnou součástí systému OSYS jsou automatické kontroly, které probíhají ve dvou úrovních – jako on-line kontroly na povinné systemizační atributy systemizovaných služebních a pracovních míst a organizačních jednotek a dále následné kontroly při uložení dávky dle pravidel stanovených zákonem, nařízením vlády č. 92/2015 Sb. a služebním předpisem náměstka ministra vnitra pro státní službu č. 3/2017.

OSYS tak představuje sofistikované technické řešení, které je možné plnohodnotně využívat od 1. ledna 2017. Toto datum nebylo stanoveno náhodně, ale vychází z data účinnosti systemizace na rok 2017, která byla vládou České republiky schválena dne 21. září 2016. Po 1. lednu 2017 se veškeré návrhy a oznámení týkající se systemizace a organizační struktury a jejich změn předkládají výhradně prostřednictvím modulu OSYS.

Spuštění produktivního provozu modulu OSYS předcházela komplexní a velmi intenzivní příprava věcného i technického řešení, která zahrnovala také četné prezentace pro zástupce vedení, personálních a IT útvarů služebních úřadů i dodavatele jejich personálních systémů. Zvláštní pozornost byla věnována zaškolení koncových uživatelů ze služebních úřadů, celkem bylo vypsáno jedenáct termínů školení. Personalisté na nich byli zevrubně seznámeni jak s konkrétními principy ovládání a práce v portálové aplikaci, tak s metodikou přípravy systemizace a organizační struktury služebních úřadů. Zároveň zde byl věnován významný prostor přípravě migračního souboru, který slouží k přenosu iniciálních dat systemizace a organizační struktury do OSYS. Stejně jako u ostatních modulů byly i pro uživatele modulu OSYS připraveny uživatelské příručky, které mají usnadnit další orientaci v systému a jeho používání, technické manuály a další dokumentace.
Neodmyslitelnou součástí přípravy na spuštění provozu nového modulu OSYS bylo testování připravené funkcionality, které se zúčastnily úřady zařazené v resortech Ministerstva vnitra, Ministerstva práce a sociálních věcí, Ministerstva kultury a Ministerstva financí. Nutno poznamenat, že role Ministerstva financí byla mnohem širší, protože plní také úlohu spoluposuzovatele předkládaných návrhů a hodnotí návrhy z hlediska jejich dopadů na státní rozpočet. Proto byla pro Ministerstvo financí vyvinuta zvláštní funkcionalita, na základě které může posuzovat předkládané návrhy systemizace a ukládat v OSYS svá vyjádření.

Na začátku roku 2017 byla ještě ze strany sekce pro státní službu Ministerstva vnitra dokončována kontrola předložených migračních dat, ale zároveň už probíhala příprava na přijetí prvních návrhů na změnu systemizace a jejich následné předání ke schválení vládě. Proces předložení a následné zpracování těchto návrhů je v modulu OSYS realizován plně elektronicky. Zároveň také průběžně dochází k drobným úpravám portálové aplikace, a to zejména jejímu rozšíření o některé analytické a kontrolní nástroje pro usnadnění práce jednotlivých uživatelů s návrhy organizační struktury a systemizace služebních úřadů.

Ing. Kateřina Vojtová, MPA
sekce pro státní službu MVČR

# Realizace změn v informačním systému RPP v souvislosti s novelizací zákona č. 111/2009 Sb.

***Prvního července 2017 proběhne 5. výročí od spuštění základního strategického nástroje veřejné správy k automatizovanému sdílení svých údajů, tedy od spuštění základních registrů. Základní registry, které jsou definovány výčtem v § 3 zákona č. 111/2009 Sb., o základních registrech (dále ZZR), jsou výsledkem dlouhodobě hledaného konceptu, které údaje a jakým způsobem je sdílet mezi úředníky veřejné správy v České republice. Nad oborovou koncepcí, tj. sdílet údaje v rámci věcně souvisejících agend a kompetencí, zvítězil koncept sdílet jen ty vybrané údaje, které potřebuje každý úředník bez ohledu, na které úrovni vykonává působnost orgánu veřejné moci. Jedná se tak zejména o adresní a identifikační údaje obyvatel, osob a územních prvků, které nejčastěji potřebují úředníci při výkonu činností, ve kterých vystupují jako orgán veřejné moci vůči klientům české veřejné správy. Tyto údaje mají podle dikce zákona referenční postavení, jednoduše řečeno, za jejich správnost odpovídá stát a jednotliví úředníci se při vyřizování agend veřejné správy a) na ně mohou spolehnout, b) musí je využívat a nevyžadovat je po klientech. Za dobu pěti let se implementace tohoto konceptu postupně penetrovala do celé veřejné správy jak prostřednictvím centrálních agendových informačních systémů (dále AIS), tak prostřednictvím AIS jednotlivých orgánů veřejné moci (dále OVM).***

Počet těchto AIS, připojených k rozhraní Správy základních registrů a využívajících pravidelně údaje základních registrů, se v roce 2017 blíží k hranici 4 tisíc (přičemž je využívá cca 5 500 OVM). Vedle toho nelze opomenout, že významnou část sdílení referenčních údajů ve veřejné správě zajišťují formuláře implementované v prostředí Czech POINT. Počet transakcí v rámci automatizované komunikace mezi základními registry se v roce 2017 celkově blíží k hranici 1,5 miliardy a měsíčně dosahuje několika desítek milionů.

Registr práv a povinností (který se podle dikce novelizace ZZR provedené zákonem č. 192/2016 Sb., jmenuje „základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností") v tomto systému hraje klíčovou úlohu – nastavuje a kontroluje oprávnění přístupů k údajům základních registrů. Z tohoto pohledu nejenže jeho údaje automatizovaně využívá rozhraní Správy základních registrů (ve spolupráci s autentizačním systémem Ministerstva vnitra) k reálnému zamezení tomu, aby úředníci bez zákonného zmocnění nemohli vidět, natož shromažďovat, osobní údaje občanů, případně neměnili bez zmocnění sdílené údaje, ale zároveň slouží k veřejné kontrole ze strany občanů, kteří se z výpisů základních registrů mohou přesvědčit, kdo a na základě jaké působnosti s jejich osobními údaji pracoval, nebo je měnil. Třetím, poněkud upozaděným, ale neméně významných přínosem základního registru práv a povinností (dále RPP) je vznik přehledové mapy výkonu veřejné správy. Do doby RPP existovaly různé studie a analýzy organizační struktury veřejné správy, které vždy časem postupně díky legislativním změnám ztrácely vypovídací schopnost a relevanci. V současnosti RPP poskytuje aktualizovaný výčet OVM (k červnu 2017 cca 7 550), jejich společnou kompetenci v právních předpisech v rámci tzv. souhrnných kategorií (v červnu 2017 cca 130), dále počet agend (rozuměj oblastí regulací stanovených zákonem), ve kterých mají OVM působnost (v červnu 2017 cca 340), dále činností, které v rámci agend vykonávají (v červnu 2017 cca 7 100), a v neposlední řadě strukturované oprávnění k jednotlivým referenčním údajům. Všechny OVM tak zároveň získaly přehled o zákonech, které se na ně vztahují, a o agendách a činnostech, které v jejich rámci vykonávají.

Strategická vize, že obíhat mají data a ne občané, však není zdaleka naplněna, zejména proto, že potřeba sdílet údaje veřejné správy je daleko širší. V další etapě je nutné dobudovat sdílení celého datového fondu veřejné správy. Státní správa i Ministerstvo vnitra jsou k tomu významně

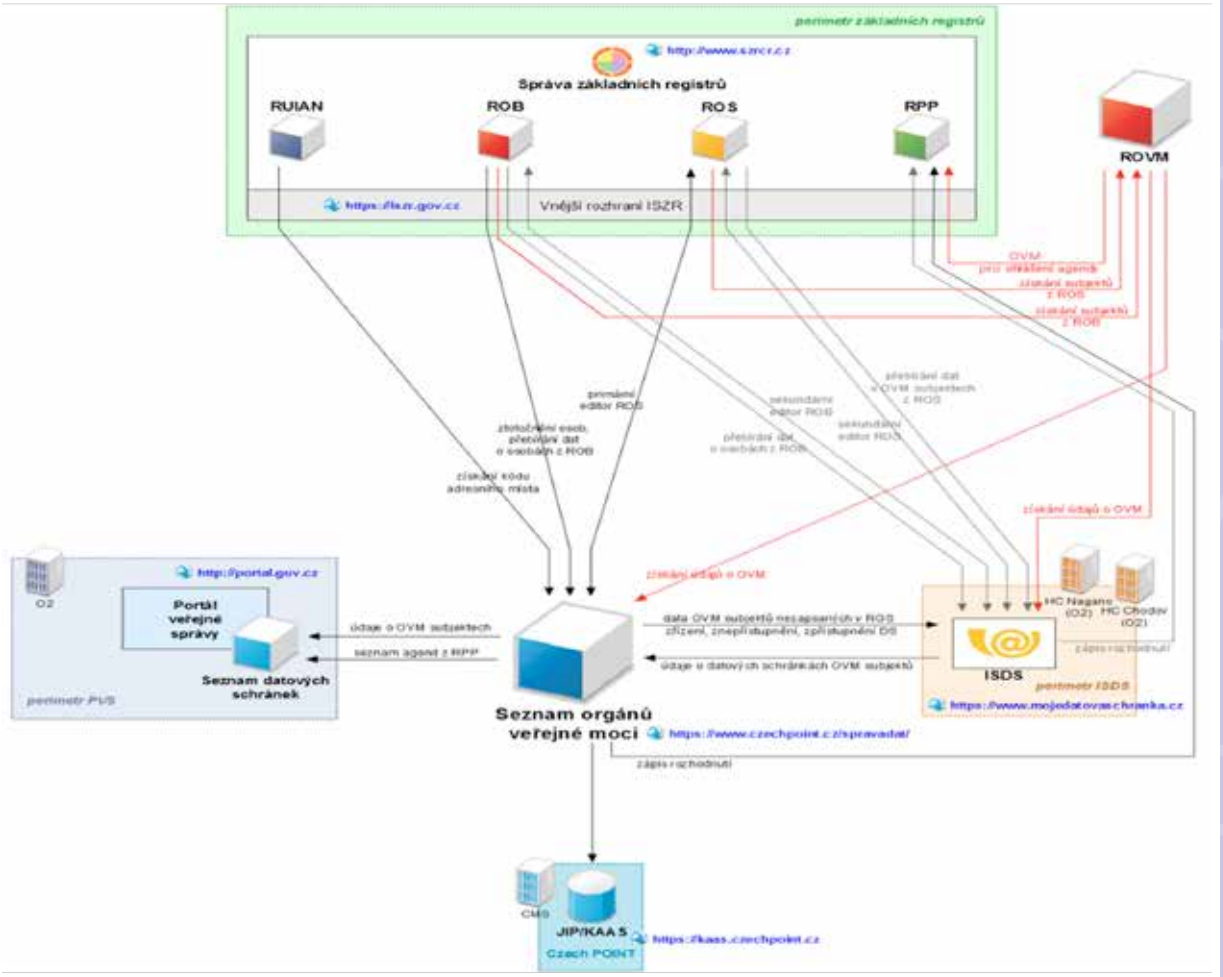
připravenější, než tomu bylo u rozjezdu základních registrů. Existuje vybudovaná infrastruktura a „komunikační dálnice" eGON Service Bus, jsou přijata zákonná zmocnění pro Správu základních registrů k propojování AIS mezi sebou a dle novely ZZR nově i zmocnění pro Ministerstvo vnitra shromáždit evidenci všech údajů, které vede veřejná správa. Vzhledem k tomu, že se princip centrální odpovědnosti za přístup k údajům základních registrů osvědčil, bude implementován i při propojování AIS navzájem, a to zejména těch, jejichž správci jsou správní úřady a v rámci těchto procesů tak musí zahájit změny nejprve RPP. Jaké jsou tedy zásadní změny v RPP, které přinesla novela ZZR a které v roce 2017 proběhnou?

1) Je to již zmíněná evidence všech údajů vedených veřejnou správou podle všech právních předpisů. Ministerstvo vnitra již v průběhu legislativního procesu na tuto povinnost připravovalo ústřední správní úřady jako ohlašovatele a po nabytí platnosti novely provedlo koncem roku 2016 i jejich praktické zaškolení. Ve vzájemné koordinaci přijaly ústřední správní úřady ambici Ministerstva vnitra (zákon nestanovil termín) dodat tyto údaje do dotčených agend (poskytujících údaje) do poloviny roku 2017. V RPP tak vznikne jedna centrální evidence o údajích vedených veřejnou správou.
2) Následná etapa do konce roku 2017 se již týká všech ohlašovatelů a agend a bude obsahovat doplnění rozsahu oprávnění OVM k údajům sesbíraným v etapě prvé. V RPP tak vznikne jedna centrální evidence o oprávněních přístupu k údajům vedených veřejnou správou.
3) Třetí změnou je povinnost připravit RPP na vedení oprávnění v případě přístupu soukromoprávních uživatelů údajů. Je tím vyjádřena vůle zákonodárce umožnit využití údajů ze základních registrů těm subjektům, které zajišťují služby občanům a právnickým osobám a ke komunikaci potřebují jejich korektní adresy. Přístup soukromoprávních uživatelů údajů je ovšem podmíněn zákonným zmocněním a pouze prostřednictvím AIS orgánu veřejné moci.
4) Došlo i k technickým změnám, jedná se např. o vhodnější řešení pro zapojení správců jak základních registrů, tak AIS do schvalování přístupů. V zákoně bylo původně nastaveno, že stanovisko k jednotlivým oznámením působnosti zaujímaly OVM v agendě správci (na správce ZR zákon nemyslel vůbec) až po registraci agendy. Vzhledem k tomu, že se ve většině případů jednalo o jednotnou kompetenci v rámci souhrnného označení (nově kategorie), docházelo jednak k zavalení správců požadavky na de facto totéž stanovisko (např. u nejčastěji užívané kategorie obce šlo o 6 254 stanovisek), jednak v případě jejich nesouhlasu k přeregistraci agendy a opakování registrace OVM. Umocněno to bylo nastavením automatického souhlasu v případě nečinnosti do 10 pracovních dnů, čímž docházelo ke kuriózní situaci, že ve stejné působnosti byla část registrace OVM zastavena správcem a část již byla zaregistrována. Vzhledem k tomu, že individuálních působností je v RPP vedeno celkem téměř 300 tisíc, nebylo myslitelné tyto případy řešit individuální komunikací. Nově je proces nastaven tak, že stanovisko poskytuje příslušný správce před registrací agendy a OVM (většinově se jedná o územně samosprávní celky) již nejsou případnými rozpory zatěžovány. Lapidárně řečeno - kontrola je ústředními správními úřady prováděna na vstupu, nikoliv až na výstupu. Nemálo zbytné komunikace prostřednictvím datových zpráv bylo vyvoláno ustanovením dnes již neplatné dikce zákona, že při veškerých změnách v podkladech registrované agendy ať již legitimně vyvolaných legislativní změnou, či potřebou změnit pro korektní přístup k základním registrům nevhodnou dekompozici právního předpisu (nemluvě o opravě chyb způsobených lidským faktorem) je nutné opakovat znovu všechny registrační procesy. Bez registrace nové působnosti pak vznikal problém s přerušením přístupu příslušného OVM k základním registrům. Nově jsou dle dikce zákona i procesy informačního systému RPP (dále AIS RPP) nastaveny tak, že je možné doplnit údaje agendy bez její úplné přeregistrace a rovněž opravit nezávisle údaje o výkonu agendy ze strany OVM. V každém případě nedojde k odpojení dotčených AIS od základních registrů. Lapidárně řečeno – „registrace jednou a dost". Z těchto změn rovněž vyplynulo omezení zbytných informací o krocích procesů, které byly pro OVM značně zatěžující.
5) Vznikl nový nástroj – rejstřík orgánů veřejné moci. Jedním z problémů dekompozice a strukturace údajů právních předpisů je nejednotné používání definic OVM. Zejména panuje nejednota v užívání souhrnných označení OVM (nově kategorií). V právních předpisech byly uvedeny dvě různé definice OVM, jedna v ZZR a druhá v zákoně č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ta druhá slouží pro odlišení druhu datové schránky (dále

DS) na DS typu OVM a ty ostatní. Praktickým důsledkem bylo, že se vyskytly subjekty, které měly povýšenou DS na typ OVM, ale zároveň nebyly registrovány jako OVM. Obdobná nejednota panovala v pojmech souhrnných označení, která měla odlišný rozsah, často i obsah v závislosti na znění různých právních předpisů. Rovněž většinou nebyla v předpisech za aktualizaci obsahu souhrnných označení stanovena konkrétní odpovědnost. Rejstřík OVM bude schopen takové problémy průběžně řešit a bude primárním zdrojem číselníků pro Informační systém datových schránek (dále ISDS) i Czech POINT. Navíc bude rejstřík obsahovat údaje o soukromoprávních subjektech, pokud jim speciální zákon umožní sdílet údaje základních registrů.

6) Integrace RPP a údajů ISDS. Rejstřík OVM bude primárním zdrojem DS typu OVM pro ISDS, datové výměny mezi stroji obou systémů zajistí automatické založení nebo zrušení DS typu OVM. AIS RPP zároveň omezí datové zprávy o krocích procesů registrace zajišťované ISDS.

## Integrace RPP a údajů ISDS




7) Využití údajů RPP k nahrazení identifikace AIS k automatizaci certifikačního řízení Správy základních registrů. Stávající procesy certifikace k připojování AIS k rozhraní Informačního systému základních registrů (dále ISZR) postrádají plnou automatizaci procesů aktualizace a reklamace při sdílení údajů mezi RPP a ISZR, zejména strukturované údaje o vazbě AIS/agenda/OVM/role (tj. rozsah oprávnění).

PhDr. Jan Tretera
oddělení registru práv a povinností,
odbor eGovernmentu, MVČR

# Teorie a praxe

***eIDAS, GDPR, Kybernetická bezpečnost a další zaklínadla naplňují v současnosti diskuse lidí kolem ICT. Každý se bojí, že něco poruší, ale málokdo dělá něco pro to, aby se tak opravdu nestalo. Chybí procesy, osvěta, technologie, lidi, a hlavně nějaká branná cvičení a testy. Branná cvičení?***

Uvedu příklad: Kamarád na nejmenovaném ministerstvu ze své pozice hlavního „bezpečáka" rozeslal všem varovný mail, že NIKDY NEMAJÍ KLIKAT NA ODKAZY V NEOČEKÁVANÉM MAILU. Počkal pár dní a pak jim rozeslal z jakési adresy cosi s odkazem. A kolik si myslíte, že „kliklo"? VÍCE JAK 60%! Trvající útoky s Ransomware (škodlivý program, který znepřístupní počítač obvykle zašifrováním veškerých dat a útočník žádá následně výkupné) ukazují, že taková osvěta a opatření proti hlouposti nejsou jen samoúčelnou paranoiou. A není to jen o hlouposti uživatelů, ale i hlouposti správců systémů. Opět jeden konkrétní příklad. Jistá komerční firma nezabezpečila vzdálený přístup ke svým serverům, a tak se na jeden útočníci dostali. Protože byli na serveru, tak měli vysoká práva a zvládli zašifrovat nejen VEŠKERÁ PROVOZNÍ DATA, ALE I VEŠKERÉ ZÁLOHY! Ano, správně se ptáte: Jak to, že byly zálohy dostupné i pro zápis? No prostě byly, a tak byly zašifrovány. Firma přišla o veškerá data, a nakonec zaplatila výpalné ve výši mnoha milionů korun! JSTE SI JISTI, ŽE U VÁS TOMU TAK NENÍ? Opravdu takové ztráty nehrozí? Jiné ministerstvo zase mělo nakaženo škodlivým software více jak 50% počítačů a zjistilo to až když jejich poskytovatel připojení do internetu hlásil, že se děje cosi nekalého. Samozřejmě měli drahé řešení firewallů, a to fungovalo a logovalo a logovalo, ale logy nikdo nečetl, nikdo a nic je nevyhodnocovalo, a tak to bylo celé k ničemu. Kolikrát jste již obdrželi nějaký nevyžádaný nebo nakažený mail od člověka, kterého znáte? Ono to samozřejmě nebylo od něj, ale útočník ukradl kontakty Vám nebo někomu z okruhu Vašich přátel a použil je na rozesílání něčeho nekalého. Třeba nenastala škoda. Nikdo nikam neklikl, maily chytil nějaký štít proti nevyžádané poště apod. Ale co až bude v účinnosti nařízení EU komise GDPR (nařízení o ochraně osobních údajů)? Nedělá Vás takový únik osobních údajů a následné pokuty? Kde vede Vaše organizace data povahy osobních údajů a jak je chrání? Máte je v CRM, Outlooku, ERP, KMS a tisících Excelových tabulek? Ano? A co nakládání s takovými daty? Povolujete BYOD (používání vlastních zařízení „od Ježíška" typu telefon, tablet, domácí PC)? Ano? Sdílí Vaši zaměstnanci data přes OneDrive, Google Drive, Dropbox, Úschovnu, ...?

Jak jste připraveni na případný úspěšný útok? Například jedna banka testovala své systémy a při cvičení, co dělat po identifikovaném průniku do systému, zjistila, že nemá lokálně právo vypnout nebo omezit clearing (zpracování mezibankovních transakcí). Máte ošetřeny a skutečně nacvičeny krizové situace?

Jako znalecký ústav CETAG máme zkušenost, že znalecký posudek je používán až v situaci, kdy problém již nastal a je třeba jej zdokumentovat, nalézt příčiny a viníky a stanovit odškodnění.

Pro účely prevence proto doporučujeme využít specializovanou laboratoř ( www.cyberlab.cz ), která hodnotí zejména technickou a procesní stránku existujících řešení s cílem nalézt případné slabiny a navrhnout řešení a omezení rizik. Součástí služeb této laboratoře je i zajištění odpovídajícího certifikátu.

Jan Vojtěch Binder

CETAG – znalecký ústav v oboru kybernetika – výpočetní technika a v oboru ekonomika – oceňování HW a SW

*P.S. Použité příklady nejsou smyšlené, ale jakákoliv podobnost s Vaší organizací je čistě náhodná*

# eOP s kontaktním čipem – klíč k elektronické identitě

***STÁTNÍ TISKÁRNA CENIN, státní podnik, vyrábí občanské průkazy na plastových kartách od roku 2012, a to ve dvou provedeních – bez čipu a s kontaktním čipem. Občan má právo si vybrat, jaký typ dokladu si zvolí. Vzhledem k tomu, že dnes čip nepředstavuje pro držitele průkazu žádnou zajímavou přidanou hodnotu, je množství vydaných občanských průkazů s čipem velmi malé. Zároveň tento čip nesplňuje některé požadavky vyplývající z nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (nařízení eIDAS). To by se však mělo brzy změnit.***

## Elektronická identita

V nedávné době byl prezidentem České republiky podepsán návrh novely zákona č. 328/1999 Sb., o občanských průkazech, který zavádí plošné vydávání elektronických občanských průkazů. Senát Parlamentu České republiky aktuálně projednává další důležitý zákon, a tím je vládní návrh zákona o elektronické identifikaci.

Obě tyto legislativní normy lze považovat za základní stavební kameny systému elektronické identity v České republice.

Návrh zákona o elektronické identifikaci zavádí princip prokázání totožnosti s využitím elektronické identifikace. V souladu s návrhem zákona o elektronické identifikaci je možné elektronicky prokázat totožnost osoby jen tehdy, pokud se osoba elektronicky identifikuje prostřednictvím kvalifikovaného systému elektronické identifikace.

Kvalifikovaným systémem elektronické identifikace je systém, v rámci kterého je, mimo jiné, vydáván prostředek pro elektronickou identifikaci, který je spojen s osobou, kterou identifikuje, a který splňuje požadavky nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (nařízení eIDAS) a jehož součástí je i tzv. národní bod, což je systém veřejné správy, podporující proces elektronické identifikace a autentizace.

## eOP – prostředek pro elektronickou identifikaci

Zmiňovaným prostředkem pro elektronickou identifikaci, který bude vydáván v rámci kvalifikovaného systému elektronické identifikace, bude nový občanský průkaz s elektronickým kontaktním čipem. Bude se jednat o státem garantovaný důvěryhodný prostředek pro elektronickou identifikaci splňující požadavky nařízení eIDAS na vysokou úroveň záruky a současně se bude jednat o kvalifikovaný prostředek pro vytváření kvalifikovaných elektronických podpisů, tzv. QSCD zařízení.

Na čipu nového občanského průkazu bude uložen tzv. identifikační certifikát, chráněný kódy IOD/DOK, prostřednictvím kterého se občan bude moci autentizovat k národnímu bodu a vzdáleně a důvěryhodně tak prokázat svou totožnost.

Vybudováním národního bodu a zahájením vydávání nových občanských průkazů s kontaktním elektronickým čipem bude zajištěna garantovaná identita občana a k ní existující důvěryhodný technický prostředek pro bezpečnou autentizaci.

S využitím nových občanských průkazů tak získají občané ČR bezpečný a důvěryhodný přístup k elektronickým službám státu.

## Služební průkaz a nařízení eIDAS?

A nejedná se jen o občanské průkazy, existuje celá řada dalších dokladů a průkazů, které by mohly splňovat požadavky nařízení eIDAS. Domníváme se, že by bylo například vhodné o tuto funkcionalitu rozšířit rovněž připravovaný služební průkaz podle zákona o státní službě č. 234/2014 Sb. Pro zaměstnance státní správy by tak mohl tento průkaz, obsahující kvalifikovaný elektronický podpis, založený na kvalifikovaném certifikátu pro elektronický podpis, plnit funkci důvěryhodného prostředku pro autentizaci a identifikaci. V současné době probíhají diskuze ohledně detailní technické specifikace služebního průkazu a jeho využití v rámci státní správy. Definitivní vzhled a funkcionalitu služebního průkazu stanoví Ministerstvo vnitra vyhláškou.

## Garance důvěryhodnosti

Z pohledu nařízení eIDAS je důležité, že kvalifikovaný elektronický podpis, založený na kvalifikovaném certifikátu, vydaném v jednom členském státě EU, se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech. Jedná se tudíž o důvěryhodnost dokumentu podepsaného tímto elektronickým podpisem, a to nejen v rámci ČR, ale celé Evropské unie.

## Přechodné období

Přestože v České republice platí dvouleté přechodné období, stanovené zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v rámci kterého je možné po dobu dvou let ode dne nabytí účinnosti zákona používat v ČR zaručený elektronický podpis, založený na kvalifikovaném certifikátu pro elektronický podpis, máme již dnes připravené řešení, které je plně kompatibilní s požadavky eIDAS.

## Zavádíme eIDAS do praxe

V současné době probíhá pilotní provoz tohoto řešení, které je založené na plastové kartě s designem vytvořeným dle požadavků zákazníka, obsahujícím ochranné prvky, s personalizací formou plnobarevného digitálního tisku a s kontaktním čipem, vystupujícím jako kvalifikovaný prostředek pro vytváření důvěry dle nařízení eIDAS. Vedle kontaktního čipu jsou tyto průkazy osazeny i bezkontaktním čipem, sloužícím k zajištění autorizace držitele průkazu pro přístup


do interních systémů zákazníka. Takto koncipovaný průkaz umožňuje sjednotit několik samostatných karet (např. vstupní průkaz, karta s čipem pro elektronický podpis, průkaz zaměstnance) do jediné čipové karty.

Zkušenosti z této etapy bychom následně rádi nabídli státu při zajištění výroby služebního průkazu podle zákona o státní službě č. 234/2014 Sb. STÁTNÍ TISKÁRNA CENIN má dlouholeté zkušenosti s výrobou čipových karet, které poskytují funkcionality elektronického podpisu, elektronické autentizace a identifikace a je připravena i v budoucnu vyrábět moderní čipové karty splňující požadavky evropské i národní legislativy. To je předpoklad pro to, abychom se stali partnerem státu rovněž při vývoji a výrobě služebního průkazu.

## STC jako spolehlivý partner

Profesionální přístup při realizaci zakázek, použití špičkových materiálů a technologií, které jsou mnohdy dostupné jen ceninovým tiskárnám, a 100 % zabezpečení výroby v průběhu celého výrobního procesu činí z STC vysoce důvěryhodného a spolehlivého partnera. Jsme držitelem mnoha certifikátů, mezi jinými i certifikátu ISO 27001:2013 osvědčujícím bezpečnost informací mimo jiné při personalizaci dokladů, včetně personalizace plastových karet a jejich výroby.

Bc. Karel Kohout, projektový specialista
Ing. Petr Mikš, produktový specialista

# ISSS 2017 – jubilejní ročník renomované konference

***V Hradci Králové se po prvním dubnovém víkendu uskutečnil již dvacátý ročník konference ISSS, jenž jako obvykle doprovodila visegrádská konference V4DIS. Opět se zde setkali vrcholní politici, ministři a šéfové státních úřadů se stovkami zástupců měst a obcí, informatiky krajských či městských úřadů, odborníky, hosty ze zahraničí i manažery firem, které do tohoto segmentu dodávají technologie a služby. Počet registrovaných účastníků v posledních letech pravidelně překračuje číslo 2300 a ani letošní ročník nebyl výjimkou, kongresové centrum Aldis bylo opět nabito k prasknutí.***

Akci každoročně poskytuje záštitu celá řada osobností tuzemského politického života. Přímo na konferenci nechyběl předseda vlády ČR Bohuslav Sobotka, který svým vystoupením otevřel celý pondělní program. V bloku, jenž předcházel tradičnímu hodnocení rozvoje e-governmentu z pohledu MV, mu sekundovali poslanci PSP Věra Kovářová a Ivan Pilný, hejtman Kraje Vysočina Jiří Běhounek a prezident ICT Unie Zdeněk Zajíček. Na dopoledním slavnostním zahájení se pak představilo několik členů vlády, včetně místopředsedů Andreje Babiše a Pavla Bělobrádka či nového ministra průmyslu a obchodu Jiřího Havlíčka. Do diskuse se zapojili i poslanci obou komor Parlamentu, šéfové státních organizací, náměstci ministerstev, představitelé asociací a svazů nebo zástupci největších dodavatelských firem.


Oficiální část slavnostního zahájení uzavřel jménem nepřítomného ministra vnitra jeho náměstek Jaroslav Strouhal, poté následovala oblíbená „diskusní kavárna"...

Premiér Sobotka prakticky zahajoval celý pondělní program a po svém vystoupení ještě chvíli diskutoval s kolegy i novináři...

V celém dvoudenním programu dominovalo několik klíčových témat, mezi nimiž nechyběl ani odborný blok věnovaný elektronizaci zdravotnictví, na němž se jako obvykle výrazně podílel Kraj Vysočina, nebo přednášky a diskuse týkající se konceptu „chytrých měst" či internetu věcí. Hodně často se hovořilo i o problematice kybernetické bezpečnosti a o dopadech nového nařízení EK k ochraně osobních dat, které zasáhne od května příštího roku doslova celou veřejnou správu.

Nedílnou součástí programu jsou každoročně setkání a jednání, která těží z mimořádné koncentrace politiků, odborníků a zástupců veřejné správy. Jako obvykle se uskutečnilo jednání komisí Svazu měst a obcí ČR a komise Rady Asociace krajů ČR pro informatiku s poslanci Parlamentu ČR či setkání Sdružení tajemníků městských a obecních úřadů. V letošním roce se navíc konal i neveřejný diskusní panel České bankovní asociace zaměřený především na elektronickou identitu a rozvoj bezhotovostního styku.

Na konferenci se také setkali vítězové oblíbených soutěží, jako jsou například Zlatý erb, Biblioweb či JuniorErb a udělena byla i cena Český zavináč. Ve spolupráci s organizátorem soutěže Zlatý erb, jímž je od letošního roku spolek Český zavináč, vyhlásila Iniciativa 202020 rovněž „nejoblíbenější online službu e-governmentu".

**Podrobné informace, včetně podrobného programu, audio- a videozáznamů, výsledků soutěží, kompletního archivu posledních ročníků i přehledu partnerů a spolupracujících subjektů jsou dostupné na www.isss.cz.**

Prokop Konopa, ISSS

Ocenění Český zavináč letos získal Integrovaný záchranný systém ČR.

# ROK INFORMATIKY 2017

***Magazín Egovernment pořádal počátkem června další ročník již tradiční konference ROK INFORMATIKY. Tentokrát jsme se sešli v malebném Šternberku u Olomouce. Záštitu našemu letošnímu setkání dal hejtman Olomouckého kraje Ladislav Okleštěk a naše diskuze byla, jako vždy, rozložena do tří dnů.***

Ve středu odpoledne jsme se sešli na workshopu věnovaném problematice SmartCity. Jakkoliv je to téma komplexní a města se stávají „chytrými" až v okamžiku, kdy jsou nasazeny smart projekty v širším měřítku a hlavně provázaně, diskutovali jsme o dílčích projektech zaměřených především na dopravu. Je to dáno skutečností, že ta bývá pro většinu měst nejpalčivějším problémem a zde je i řešení smart většinou nejviditelnější. Ucelenější pohled na to, jak začít s chytrým městem, nám dal Pavel Smolík ze společnosti Cisco Systems.

Večerní program prvního dne bývá v rámci ROKU INFORMATIKY tradičně „sportovnější". Vyvezli jsme účastníky konference do sportovního areálu Véska, kde mimo jiné svedli líté boje v turnaji petanque.



Čtvrtek je vždy hlavním jednacím dnem konference, a proto je zahajován slavnostním aktem – šerpováním praporu ROKU INFORMATIKY. **Starosta města Šternberk Stanislav Orság** slavnostně připnul šerpu svého města na vlajku konference a zahájil její jednání. Hlavní částí dopoledního bloku bylo vystoupení zástupců MV ČR – ředitele odboru e-governmentu **Romana Vrby** a pánů Jana Tretery a Jiřího Kárníka z uvedeného odboru. Ti všichni kromě připravených prezentací museli odpovídat na dotazy přítomných. Po živé diskuzi následovala série krajských pětiminutovek - stručných aktuálních informací z krajů. Letos poprvé měli možnost účastníci tyto pětiminutovky hodnotit a s drtivou převahou v tomto hodnocení zvítězil **Jiří Šafránek z Olomouckého kraje**.

Odpolední část je pak tradičně vyhrazena prezentaci realizovaných projektů, a to většinou v podání realizátorů i provozovatelů, tedy samotných firem i úřadů. O závěrečnou část programu se postarala společnost Microsoft se svými partnery v rámci **Microsoft wokna**.

Druhý večer konference mívá společenštější charakter. Raut jsme tentokráte umístili do kulturního domu Šternberka, kde jsme měli zázemí podbarvené výborným hudebním vystoupením. Na „výlety" mohli účastníci v průběhu večera vyrazit na **hrad Šternberk**, nebo do **Expozice času**. Obě tyto trasy byly kapacitně více než vytíženy.
Pro páteční dopoledne jsme tentokráte zvolili jinou, méně konferenční formu. V rámci jakýchsi **laboratoří** zde společnost Microsoft vysvětlovala a hlavně ukazovala, co vlastně znamená a k čemu může být internet věcí a virtuální realita.

Prezentace a fotografie z konference naleznete na **www.egovernment.cz** v sekci ROK INFORMATIKY.
**Příští rok si Vás dovolíme pozvat do Liberce.**

# e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

**MIKULOV • 5. - 6. 9. 2017**

**ODBORNÝ PARTNER**

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

SPCSS

**PLATINOVÝ PARTNER**

CISCO

**GENERÁLNÍ PARTNER**

Česká pošta

GORDIC®

... vše podstatné o eGovernmentu najdete v Mikulově.

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