Egovernment

elektronizace veřejné správy

Úvodní slovo

Vážení čtenáři,

jsem velmi rád, že se nám v posledním roce daří propojovat občany se státní správou, a to prostřednictvím dnes již běžně dostupných elektronických nástrojů. Kromě skutečnosti, že jsme úspěšně implementovali plánované služby v Portálu občana, se také podařilo zapojit některé obce tak, aby byly blíže svým obyvatelům.

Samotný Portál občana dnes ulehčuje kontakt mezi občany a státní správou pro více než 22000 uživatelů a z našich statistik vyplývá, že každý měsíc se registruje asi 2000 nových uživatelů a jejich počet stále stoupá. Mezi nejvyužívanější služby stále patří datové schránky. Jejich prostřednictvím bylo odesláno více než 650 milionů datových zpráv, což znamená, že nemusely být pokáceny další tisíce stromů pro výrobu papíru, ale mohly dále produkovat kyslík.

V průběhu projektu implementujeme také další řešení, abychom přispěli k pohodlnému využívání služeb. Patří k nim spuštění mobilní aplikace pro přihlášení do datových schránek nebo anglická mutace Portálu občana. Snažíme se také dělat prostředí služeb přívětivější, i proto jsme provedli vizuální i funkční redesign datových schránek a vybrali jejich nové moderní logo.
Chceme podpořit využívání všech nástrojů e-governmentu a seznámit občany s cílem celého projektu, souvisejícího s Portálem občana a poskytovaných služeb. Za tímto účelem připravujeme velkou propagační kampaň, která je spolufinancována z evropských zdrojů.

Abychom mohli poskytovat občanům co nejlepší služby, je potřeba také připojovat portály dalších měst a obcí, které dosud nemají kompletní povědomí o výhodách, jaké může poskytování elektronických služeb přinést jim nebo jejich občanům. Připravujeme proto srozumitelné, a přitom podrobné příručky, jak se napojit na Portál občana. Spolupráci obcí v oblasti digitalizace státu totiž považujeme za klíčovou.

Chtěl bych nicméně zdůraznit, že i v oblasti digitalizace platí, že vytvořit jednoduchou věc může být ta nejsložitější práce na světě. Aby vše fungovalo tak, jak má, je zapotřebí mravenčí práce mnoha stakeholderů, která v podstatě není vidět. Aby služby byly jednoduché a naplňovaly sdílený datový fond, je zapotřebí nastavit registr práv a povinností tak, aby vše fungovalo. A právě na tom pracujeme.

Je skvělé, že ostatní resorty pochopily, jak je důležité se zapojit. Obce a ostatní resorty zapojené do Portálu občana jsou ukázkou toho, jak by měla fungovat veřejná správa. Jak by měly informační systémy navzájem fungovat.

Jsem velice rád, že Ministerstvo vnitra je hlavním tahounem celé digitalizace veřejné správy a podílí se velkou měrou na její podobě. I proto jsou součástí tohoto čísla magazínu Egovernment dva články MV ČR informující o napojení měst a obcí a Registru práv a povinností.

JUDr. Jaroslav Strouhal,
náměstek ministra vnitra pro řízení
sekce informačních a komunikačních technologií

Obsah

Redakce	ÚVODNÍ SLOVO	2
	OBSAH, TIRÁŽ	3
KYBEZ	KYBERBEZPEČNOST 90,91:DEBATA NEJEN O VAROVÁNÍ NÚKIB	4–11
	KONTINUITA ČINNOSTÍ Z POHLEDU BEZPEČNOSTI INFORMACÍ	12–14
	BEZPEČNOST SD-WAN MUSÍ BÝT NEJVYŠŠÍ PRIORITOU	16–18
	SPISOVOU SLUŽBU ČEKAJÍ ZÁSADNÍ ZMĚNY	20–21
	WEBOVÉ PORTÁLY: AKTUÁLNÍ ZRANITELNOST A HROZBY	22–25
eIDAS	PROJEKT SONIA	26–27
	PORTÁLY MÍSTNÍCH SAMOSPRÁV	28–29
	CO JE NOVÉHO V RPP	32–33
	eIDENTITA	34–35
	Nařízení eIDAS a bezpečnost	36–37
Konference	ISSS 2019	38–39

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
twitter: @EgovernmentMag
facebook: @EgovernmentMagazin

Šéfredaktor: Ing. Michal Jirkovský
Korektorka: PhDr. Helena Veverková
Asistentka: Martina Maksymovová

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
ISSN 1801-9420

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.

KYBERBEZPEČNOST 90,91: DEBATA NEJEN O VAROVÁNÍ NÚKIB

Magazín Egovernment uspořádal letos další pokračování svého pravidelného semináře s tématem Kyberbezpečnost. Našemu setkání v Malostranské besedě v Praze jsme tentokráte dali podtitul 90,91. Toto zdánlivě, z pohledu kyberbezpečnosti nelogické číselné označení bylo totiž skóre, které Česká republika dosáhla v posledním mezinárodním hodnocení National Cyber Security Index, kde obsadila první příčku (https://ncsi.ega.ee/). Toto ohodnocení bylo vyjádřením skutečnosti, že po formální stránce je v ČR směrem k zajištění kyberbezpečnosti zákonů dost – máme příslušnou strategii, máme příslušné úřady, zákony atp. Otázkou samozřejmě je, do jaké míry se formální a reálná kyberbezpečnost potkávají, či rozcházejí. Na to dalo odpověď, týden před naším seminářem, mezinárodní cvičení NATO – Locked Shields 2019, kde v široké mezinárodní konkurenci obsadila Česká republika 2. místo (https://ccdcoe.org/exercises/locked-shields/). Pod dojmem těchto dvou významných událostí, které dokládají pozici České republiky mezi nejlepšími v oblasti kyberbezpečnosti, jsme vedli naši diskuzi.

IVAN BARTOŠ

Předseda Výboru pro veřejnou správu a regionální rozvoj PS PČR PhDr. Ivan Bartoš, PhD., který našemu setkání udělil záštitu, a proto je zahajoval, uvedl, že je rozhodně dobře, že v České republice máme vybudováno organizační i odborné zázemí v oblasti kyberbezpečnosti. Nejedná se přitom pouze o NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost https://nukib.cz/), ale i řadu neziskových organizací, které pomáhají dohlížet na bezpečnost českého internetu. Jejich dostatečné rozložení a propojení tedy potvrdil Národní bezpečnostní index, v jehož hodnocení, jak bylo řečeno, jsme obsadili první místo. Nicméně je, podle slov Ivana Bartoše, důležité si uvědomit, že toto hodnocení je v zásadě administrativního charakteru. Je to hodnocení existence legislativy. Jedná se o určitou statistiku, v jejímž rámci odškrtané body ukazují, že podle zákonů máme vše správně nastaveno. Ale vedle toho je zde samotná každodenní práce – operativa jednotlivých institucí, jednotlivých expertů, kteří na bezpečnost a na konkrétní incidenty dohlížejí a reagují na ně. V tomto smyslu je velice potěšující právě výsledek cvičení NATO, v němž jsme obsadili druhé místo

Kyberbezpečnost a kyberválka je, dle slov Ivana Bartoše, téma, kterému se budou čím dál tím vážněji věnovat především ty země, které směřují do plně digitálního světa, a to jak v rámci veřejné správy, tak komerčního sektoru (například v oblasti Internet of Thinks). Ivan Bartoš uvedl, že existuje dostatek filmů a knih, kde narušení kyberbezpečnosti je v hlavní roli konfliktu, který alespoň v rámci těchto příběhů může být devastující. Vždy se jedná o fikci, ale je přesvědčen, že společnost je obecně na takové útoky stále více citlivá, úměrně tomu, jak se stává více digitalizovaná. Proto byl rád, že se program semináře nevěnoval pouze onomu statistickému pohledu. Samotná kyberbezpečnost souvisí především s technickou infrastrukturou, přechází přes dobré nastavení procesů a pokračuje přes vzdělávání a sdílení znalostí. Speciálně vzdělávání a sdílení by nemělo být omezeno pouze na jednotlivé instituce, ale mělo by směřovat zejména k samotným uživatelům a hlavně těm, kteří mohou ovlivnit bezpečnost dat uživatelů a systémů.

V této souvislosti vnímá Ivan Bartoš jako pozitivní skutečnost, že nejen v rámci „jeho" Výboru pro veřejnou správu a regionální rozvoj, ale v podstatě v rámci celé Poslanecké sněmovny se objevuje generace politiků, kteří už vyrůstali s internetem. I díky tomu se rozdíl mezi označením politik a odborník u takovýchto témat bude do budoucna stírat, a to nejen v rámci návrhů zákonů, ale třeba i při diskuzích o rozpočtu. I toto téma je z pohledu kyberbezpečnosti zásadní. Máme sice, podle uvedeného hodnocení, skvěle zvládnutou legislativu, ale financování kyberbezpečnosti poněkud zaostává. A pravdou je, že bezpečnostní opatření, která vyplývají z doporučení konkrétních institucí, stojí a budou stát dost peněz. Ivan Bartoš proto postrádá v rozpočtu kapitolu, která by umožňovala zaplatit odborníky nejen přímo v institucích, které mají na starost kybernetickou bezpečnost, ale ve všech úřadech a ministerstvech. Tam všude by měli být lidé, kteří by dohlíželi na lokální úroveň kybernetické bezpečnosti. V současné rozpočtové situaci však bohužel většinou není možné odborníky adekvátně zaplatit. Ivan Bartoš věří, že pokud politické strany, případně i vláda, deklarují vůli tuto záležitost řešit, dojde do budoucna ke změnám v zařazení a ohodnocení pracovníků veřejné správy tak, aby ti dobří nemuseli utíkat do komerčního sektoru. Tedy, že celkové rozpočtování státu bude tuto situaci zohledňovat. Náklady vynaložené do kyberbezpečnosti a vzdělávání jsou, podle slov Ivana Bartoše, investice do naší budoucnosti. Mají ve své podstatě v sobě obranný prvek a není

na místě tuto oblast podceňovat. Financování týkající se kyberbezpečnosti by mělo být rozhodně obsaženo jak v konkrétních krocích vlády, jednotlivých ministerstev, tak i v rámci hlasování o rozpočtu ve Sněmovně.

S předsedou Výboru pro veřejnou správu a regionální rozvoj Ivanem Bartošem jsme se bavili rovněž o návrhu zákona o právu na digitální služby. Připustil, že i v rámci Sněmovny byl odpor proti „digitálu" citelný. Do jisté míry to chápe, neboť ve výsledku se jedná o další peníze a další práci. Jen výběrová řízení kladou nároky na bezpečnost a dodat nebo vybrat něco, co bude levné, rychlé a bezpečné, je skutečně těžká úloha. Nicméně, jak uvedl, vysvětlováním a přesvědčováním se nakonec poda-

řilo získat 137 poslanců, kteří vyjádřili podporu tomuto návrhu. Ivan Bartoš zdůraznil, že je podstatné, že memorandum není svázáno jen s konkrétním zákonem. Obsahuje výhled na období následujících 5 let, kdy se stát má skutečně posouvat do situace, kde občan vždy bude moci (bude-li chtít) řešit svoje potřeby vůči státu digitální cestou. Důležité je, že memorandum k tomuto cíli zavázalo strany jako celky. Podepsali jej současní předsedové klubů a podepsal jej i současný ministr vnitra. To je velice důležité, neboť i když se hovoří o tom, že digitalizace je meziresortní otázka, stále je gestce v této oblasti přisuzována MV ČR. Toto memorandum by tedy mělo být něco, co překoná horizont volebního období, a Ivan Bartoš doufá, že otázka kyberbezpečnosti v souladu s tím, jak se budou jednotlivé služby digitalizovat, bude napříště spojena s každým zákonem a s každou službou, která se toho bude týkat. Doufá, že kyberbezpečnost konečně nebude „chudá příbuzná", která se řeší až jako poslední, pokud zbudou nějaké peníze.

ONDŘEJ PROFANT

Na Ivana Bartoše navázal předseda podvýboru pro e-government PS PČR Ondřej Profant, který se zaměřil na technické záležitosti. Upozornil na skutečnost, že kyberbezpečnost se netýká pouze ochrany konkrétního perimetru. Právě to je totiž, podle jeho slov, určitý zlozvyk, který vychází z klasického pojetí bezpečnosti - zaměřit se na nějaký perimetr a ten si hlídat. V praxi to pak často vypadá tak, že vlastník konkrétní sítě řeší její zabezpečení, ale nedívá se dál za její hranice. To většinou dopadá špatně. Dnešní svět je komplexnější a hrozby musíme vnímat v širším pohledu. Je nutné řešit kombinaci fyzické ochrany, klasické firewall ochrany a rovněž působení lidského faktoru.

Aby zdůraznil určitou absurditu současné doby, byť to vypadá fantaskně, poukázal na skutečnost, že na naše zařízení může dnes zaútočit třeba i amazonský deštný prales. I ten je totiž označen čipem a připojen k nějaké síti a nikde není zaručeno, že se nemůže za určitých okolností propojit s naší sítí. Jako příklad podporující tuto „absurditu uvedl incident v německé továrně, jejíž produkční prostředí „shodil" kávovar připojený do sítě, a to i přes skutečnost, že se jednalo o síť, která byla standardně odpojená od internetu. Samotný kávovar byl totiž krátkodobě v rámci opravy připojen do internetového prostředí. Toto krátkodobé spojení stačilo k tomu, aby do firemní sítě byl zavlečen virus cestou, která nebyla chráněna, a došlo k následnému narušení výroby. Podle Ondřeje Profanta je právě toto realita, proti které se musíme bránit a musíme ji umět odhalit. Máme kolem sebe značné množství „chytrých" zařízení a je nutné s nimi umět pracovat i ve smyslu jejich zabezpečení. Bezpečnost je kvůli tomu mnohem složitější záležitostí než pouhá kontrola toho, zda je, nebo není zapnutý firewall.

Ondřej Profant rovněž upozornil, že toto je mnohdy problém především právě veřejných institucí. Ty mají velmi často tendenci kyberbezpečnost vnímat jako jednoduché vykázání faktur za nákup určitého ochranného vybavení. Chybí však často dohled nad tím, zda je toto vybavení skutečně správně zapojeno, a především správně opečováváno. Pokud ovšem úřad nemá přehled, co se skutečně s jeho kyberbezpečností děje a neděje, nemůže tvrdit, že ji má zajištěnu.

Problém je tedy v tom, že většinou nevnímáme komplexitu problému, kterým kyberbezpečnost je. To rovněž dokazuje skutečnost, že často není v rámci úřadů věnována dostatečná pozornost například reportům o incidentech. V takovém případě pak nemůže úřad adekvátně a včas reagovat.
Obecně tedy máme tendenci se spoléhat na to, že byla instalována jakási bezpečnostní zařízení a ta „přeci" musí fungovat. Ondřej Profant uvedl, že je to něco podobného, jako když usedáme do automobilu a předpokládáme automaticky, že pojede tam, kam zatočíme volantem. Jenže, ve světě IT jsme velmi často v situaci, kdy nám ta kola někdo povolil a vůz zatáčí sám přesně na opačnou stranu, než kam směřujeme. Ještě jednou tedy podtrhl skutečnost, že kyberbezpečnost je komplexní záležitostí, s níž není jednoduché se vypořádat. Jako zásadní v tomto směru vidí především soustavné vzdělávání a znalost vlastní infrastruktury.

VAROVÁNÍ NÚKIB

V rámci semináře a diskuzí o kyberbezpečnosti jsme samozřejmě nemohli vynechat téma varování NÚKIB z prosince 2018. Sice od něj uplynulo už několik měsíců, přesto se, díky jeho jedinečnosti, jednalo o záležitost stále živou. Pro připomenutí NÚKIB vydal koncem roku 2018 varování před použitím některých prostředků spo-

lečnosti Huawei. Nás v této souvislosti především zajímalo nikoli samotné varování, ale to, co by správně mělo po varování takového druhu následovat. Tedy, jak se měly a mají chovat úřady, jaká měly či mají zavádět opatření atp. Do Malostranské besedy s námi na toto téma přišel za NÚKIB diskutovat ředitel odboru regulace Adam Kučínský.

CO JE VAROVÁNÍ?

Jak sám uvedl, kolem varování stále panuje dost zmatků a nejasností. Proto začal tím, že představil institut varování. Varování vychází ze **zákona o kybernetické bezpečnosti** – § 12, který stanoví ... ***„že úřad (NÚKIB) vydá varování, pokud se dozví (vlastní činností, nebo na podnět orgánů v oblasti kybernetické bezpečnosti, které vykonávají takovou působnost v zahraničí) o hrozbě v oblasti kybernetické bezpečnosti".*** Toto je tedy základní zákonný rámec. Druhý odstavec pak stanovuje procesní postup tohoto varování. Zde je popsáno, co musí úřad dodržet, aby varování bylo skutečně varováním podle zákona.

Adam Kučínský v této souvislosti reagoval na různé nápady, které se po varování objevily, že měl úřad reagovat jinak, neměl vyvěšovat varování na web, měl je poslat přímo a pouze povinným osobám atp. Jak zdůraznil, nic

z toho není možné, protože **institut varování je zákonem nastaven tak, že jej úřad má zveřejnit na svých internetových stránkách** a oznámit orgánům a osobám, které vede v evidenci podle § 3 zákona o kybernetické bezpečnosti (tzv. povinným osobám).

Prostřednictvím varování tedy NÚKIB upozorňuje na konkrétní hrozbu. Důležité je říci, že tento institut je mu dán - je to jeho povinnost. Pokud se tedy NÚKIB dozví o hrozbě a má za to, že je tato hrozba podložená dostatečnými informacemi, musí na ni upozornit. Subjekty, které spadají pod zákon o kybernetické bezpečnosti, jsou následně povinny se touto hrozbou zabývat a zohlednit ji v analýze rizik, neboť hrozba je jednou ze složek výpočtu analýzy rizik. **Samotné varování tedy neznamená bezpodmínečný zákaz** zařízení, na které je upozorněno. Je ale nutné zvážit případné riziko při jejich používání v některých systémech. K onomu zvážení slouží právě analýza rizik. Pokud to výsledky analýzy rizik umožňují, je možné tato zařízení v konkrétních systémech nadále používat.

IMPLEMENTACE OPATŘENÍ

Nejvíce regulovanými jsou dle zákona kritická informační infrastruktura, významné IS a provozovatelé základních služeb. Tyto osoby mají podle § 5 vyhlášky o kybernetické bezpečnosti provádět pro určené informační a komunikační systémy v pravidelných intervalech analýzu rizik. Prostřednictvím této analýzy mají identifikovat rizika a podle jejich závažnosti je mírnit. Uvedené subjekty tedy na základě vyhodnocení rizik zavádějí bezpečnostní opatření, jejichž katalog stanoví vyhláška o kybernetické bezpečnosti. Důležité je upozornit na skutečnost, **že tato opatření by měla být uvedena v rozsahu nezbytném**. Zaváděná opatření mají reagovat přímo a pouze na konkrétní identifikovaná rizika, přičemž minimální penzum bezpečnostních opatření, která na tato rizika reagují, jsou definována vyhláškou.

V souvislosti s řízením rizik se tedy v § 5 vyhlášky, odst.1 písm. H, bod 3 stanoví ... ***„že povinné subjekty musí zohlednit opatření podle § 11".*** Opatřením podle tohoto paragrafu je i varování NÚKIB vydané podle § 12. Z uvedeného tedy vyplývá, že *povinné osoby mají podle vyhlášky povinnost tato opatření minimálně zvážit v rámci analýzy rizik*. Na základě vydaného varování tedy musí povinné osoby realizovat aktualizaci analýzy rizik, ve

které zohlední hrozbu, na kterou NÚKIB upozornil. Pokud bude výsledkem této aktualizované analýzy riziko přesahující přijatelnou úroveň, musí podniknout kroky k jeho snížení. Tyto kroky mohou být různé, od zvýšení monitoringu až po nahrazení konkrétní technologie.

ANALÝZA RIZIK

Obecná definice říká, že **riziko** je možnost či pravděpodobnost, že určitá hrozba využije zranitelnosti aktiva a způsobí nějako škodu. **Řízení rizik** je potom souhrnem činností, které vedou k nalezení a eliminaci rizika. Je nutné však mít stanoven rozsah aktiv, která máme chránit, respektive na která budou tyto aktivity cíleny. Následně je nutné přiřadit a ohodnotit hrozby a zranitelnosti, které se s těmito aktivy pojí.

Aktivum je cokoliv, co má pro danou organizaci jakoukoliv hodnotu. Vyhláška rozeznává **primární a podpůrná aktiva**. **Primární aktiva** jsou služby či informace, které systém poskytuje. **Podpůrná aktiva** je vše, co zajišťuje funkčnost systému. Tedy určitá technická složka (HW či SW), zaměstnanci, kteří s tímto systémem nakládají, a v neposlední řadě i dodavatelé.

Každé aktivum má obecně určitou zranitelnost. Většinou se jedná o více možností – nevhodná architektura, nedostatečná míra kontroly, špatně nastavená přístupová oprávnění atp. Vyhláška proto stanoví určitý minimální **Katalog zranitelnosti a hrozeb**. Ten je možné a vhodné si dále upravit podle vlastních specifik, protože vyhláška obecně dopadá na obrovské množství subjektů rozdílného ražení - od letectví přes energetiku, bankovnictví až po veřejnou správu. Každé z těchto odvětví má samozřejmě úplně jiné potřeby, co se týče domén informační bezpečnosti (důvěrnost, bezpečnost, integrita) a architektury systému a služeb, které poskytují.

Hrozba využívá zranitelnosti konkrétního aktiva a může se jednat například o škodlivý kód, tedy různé viry, mallware atp., zneužití dat či neoprávněnou modifikaci údajů atd. Všechny tyto informace jsou základními vstupy pro analýzu rizik.

Hodnotu aktiva je možné stanovit podle přílohy 1 zákona o kybernetické bezpečnosti. Následně je nutné, buď z katalogu, či expertním odhadem, zjistit **hodnotu hrozeb a hodnotu zranitelností.** Teprve na základě těchto údajů je možné určit míru rizika. Jedna z možných rovnic tohoto výpočtu je popsána přímo ve vyhlášce. Výsledkem výpočtu je pak **HODNOTA RIZIKA**, která indikuje nároky na ochranu. Pokud se tato hodnota pohybuje nad určitou akceptovatelnou úrovní, je nutné přistoupit k opatřením, kterými se jeho úroveň sníží.

Je důležité si uvědomit, že **hodnota rizika nebude nikdy nulová**, ale vždy je možné a vhodné ji minimalizovat. Tato minimalizace by však měla probíhat tak, aby **náklady na bezpečnostní opatření byly vždy přiměřené** ve vztahu ke konkrétnímu riziku. Neměly by například rozhodně převyšovat náklady spojené s realizací rizika.

KONKRÉTNÍ VAROVÁNÍ NÚKIB

Mluvíme-li o současném varování NÚKIB, pak ze skutečností, které jsou v něm uvedené, vyplývá, že hrozba, na kterou upozorňuje (dle klasifikace podle vyhlášky), je hodně pravděpodobnou až jistou, tedy kritickou. Na čtyřčíselné stupnici se tedy jedná o hrozbu na úrovni 4. Tímto vyčíslením NÚKIB stanovil v rámci varování první z možných proměnných uvedeného výpočtu. Ostatní proměnné, tedy hodnotu aktiva a jeho zranitelnost, musí stanovit subjekt sám. Následovat by pak měla analýza prostředí a prošetření, zda se a případně kde technické a programové prostředky, před kterými bylo varováno v rámci konkrétních systémů, používají. Subjekty by se měly snažit dohledat, kde všude mají tyto prostředky nasazeny (mohou zjistit v seznamu podpůrných aktiv, v seznamu majetku atp.). Následně by měly aktualizovat analýzu rizik podle uvedeného postupu. Pokud riziko ani po tomto aktualizačním přepočtu nepřesahuje v rámci organizace akceptovatelnou míru, tzn. jedná se například pouze o okrajové prostředky, jejichž dopady jsou na nízké, nebo na střední úrovni, není nutné provádět žádnou další akci. Pokud se ale bude jednat o nějaké klíčové komponenty, pak se může stát, že aktualizované riziko vyskočí nad akceptovatelnou úroveň. V takovém případě je nutné najít a realizovat bezpečnostní opatření.

REALIZACE NÁPRAVY

Realizace nápravy, tedy zavádění bezpečnostních opatření, není nikdy okamžitým, skokovým krokem. Může se jednat o cestu postupné náhrady (okamžitá náhrada všech prostředků nebývá možná, ani ekonomicky vhodná) a nemusí být k dispozici hned adekvátní prostředky pro náhradu. Je však nutné zvážit hodnotu rizika a postupně zahájit, pokud to analýza rizik vyžaduje, náhradu technických a programových prostředků smysluplnou cestou.

ZÁKON O ZADÁVÁNÍ VEŘEJNÝCH ZAKÁZEK

V souvislosti s varováním NÚKIB se objevilo množství zásadních otázek, které se týkají zákona o zadávání veřejných zakázek především proto, že se v § 36 stanoví, že ... ***„zadavatel nesmí vytvářet při stanovování zadávacích podmínek bezdůvodné překážky v hospodářské soutěži".*** To je velice důležitá formulace upozorňující na základní princip nediskriminace. Důležitým je zde označení „bezdůvodné překážky". Pokud totiž oprávněná autorita (NÚKIB), která k tomu disponuje zákonným zmocněním, vydá určitý akt, který by mohl v určitých případech vést k omezení hospodářské soutěže, **dodržení tohoto požadavku právě při zadávání hospodářské soutěže nemůže být považováno za bezdůvodné překážky.** V takovém okamžiku totiž není bezdůvodné, ale realizované na základě opatření regulátora, tedy na základě zákonného požadavku. Podle názoru NÚKIB v tomto smyslu hospodářskou soutěž omezit lze v rámci stanovení zadávacích podmínek, přičemž se nejedná o porušení zákona. Navíc § 4, odst. 4 zákona stanoví, že ... ***„povinné osoby jsou povinné zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro tyto dané informační systémy, které pod zákon spadají, a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou".*** Toto zohlednění tedy není možné považovat za omezení hospodářské soutěže. Znamená to, že i zákon o kybernetické bezpečnosti dopředu předpokládá, že nastane situace, kdy bude nutné hospodářskou soutěž nějakým způsobem omezit s ohledem na bezpečnost, a reaguje na to uvedeným § 4.

Jak Adam Kučínský připustil, je pravdou, že zatím neexistuje žádný judikát či příklad, že to někdo takto zkusil. To je však důsledkem skutečností, že drtivá většina soutěží je u nás konstruována především na cenu.

KYBER BEZPEČNOST - VÍC NEŽ ZÁKON

OMEZIT VEŘEJNOU ZAKÁZKU – KDY A JAK?

Je samozřejmě nutné zvolit odpovídající postup omezení ve vztahu k tomu, v jaké fázi se konkrétní zakázka nachází.

Může se jednat o tyto tři situace:

A. Zakázka se připravuje – ještě není vypsána. Je to nejjednodušší varianta – v takovém případě by měla být provedena analýza rizik a následně její výsledky zapracovány přímo do zadávací dokumentace;

B. Zadávací řízení probíhá – to se dá rozdělit na dvě podčásti

1. **uplynula lhůta pro podávání nabídek**, to už možné měnit není, jedinou možností je tedy soutěž zrušit,
2. pokud **lhůta ještě neuplynula,** je možné toto zadávací řízení zastavit, aktualizovat a dát dostatečně dlouhý čas uchazečům k podání aktualizované nabídky (nemělo by tedy dojít k žádnému zkrácení lhůty - počítala by se znovu od začátku);

A fáze po skončení zadávacího řízení – v tomto případě není možné příliš měnit. V souladu s § 8 vyhlášky o kybernetické bezpečnosti by ale i tak mělo dojít k řízení rizik spojených s dodavateli. Tzn. měla by být provedena analýza rizik a v případě špatného výsledku by měla být stanovena nějaká další bezpečnostní opatření, která rizika sníží. Pokud není ani toto možné, je nutné v zakázce pokračovat a aktualizaci provést při případném dalším zadávání.

Podle slov Adama Kučínského je nutné mít na paměti, že **vydávání varování nelze automaticky považovat za důvod k vyloučení uchazeče ze zadávacího řízení.** Nadále platí, že zadavatel je oprávněn uchazeče **vyloučit pouze na základě důvodů obsažených v zákoně o zadávání veřejných zakázek,** tedy § 48. Rozdíl je v tom, že zde se bavíme o uchazeči, nikoli o jeho produktech, protože § 48 říká, kdy je možné vyloučit konkrétního dodavatele (osobu právnickou či fyzickou). Dává tedy jasný návod, či informace, podle čeho vylučovat. Problematické je, že bezpečnost v tomto návodu nefiguruje. Znamená to, že § 48 k vyloučení z důvodů bezpečnosti není možné použít.

Vyloučení ze soutěže je tudíž možné pouze na základě nějaké technické specifikace, která je však odůvodnitelná. Potřebné odůvodnění poskytne provedená analýza rizik na základě varování.

ZÁVĚR

Na základě varování a následné analýzy rizik je tedy možné vyloučit konkrétní **technické a programové prostředky,** nikoli ovšem osobu konkrétního účastníka. Bude se jednat o technické podmínky stanovené pomocí odkazu na konkrétní výrobky, přičemž bude využit § 89 zákona o zadávání veřejných zakázek. Není však možné použít požadavky na osobu dodavatele, pouze na konkrétní produkty, které by mohl dodat. Prakticky se tedy dodavatel, před jehož prostředky bylo varováno, může přihlásit do výběrového řízení, ale musí nabídnout jiné technické a programové prostředky, než před kterými bylo varováno. Pokud by nabízel plnění prostřednictvím těch technických a programových prostředků, které byly vyloučeny (bylo před nimi varováno), pak je možné jej vyloučit na základě nesplnění zadávacích podmínek.

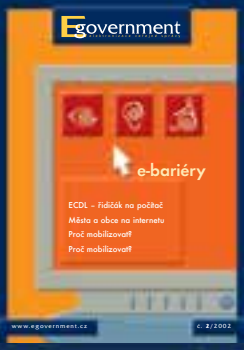
MJ

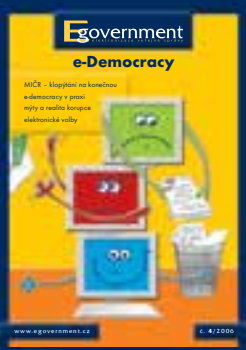
Případné dotazy můžete směrovat na regulace@nukib.cz.

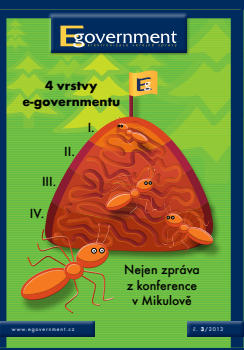
NÚKIB rovněž připravuje další podpůrné materiály, které by Vám v tomto směru měly být k dispozici.

Egovernment

elektronizace veřejné správy







Vše o elektronizaci veřejné správy
- srozumitelně a zdarma:

www.egovernment.cz

ZAJIŠTĚNÍ KONTINUITY ČINNOSTÍ Z POHLEDU BEZPEČNOSTI INFORMACÍ

Nedílnou součástí bezpečnosti informací je i zajištění kontinuity činností, které jsou z pohledu bezpečnosti informací podstatné. Norma ISO 27001 se zabývá kontinuitou bezpečnosti informací v článcích příloha A.17. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, definuje požadavky na zajištění kontinuity v § 15, kde mimo jiné ukládá provedení analýzy dopadů (BIA) a rizik kontinuity činností, stanovení cílů kontinuity, jakož i zpracování, aktualizaci a pravidelné testování plánů kontinuity činností a havarijních plánů. Norma ISO 22301 se věnuje řízení kontinuity v širším rámci a stanovuje požadavky na systémy řízení kontinuity činností (BCMS = Business Continuity Management Systems).

V České republice je zavádění systémů řízení kontinuity činností dost zanedbáváno. Podle mezinárodní organizace pro standardizaci ISO byly v roce 2017 v České republice pouze 4 certifikované organizace, zatímco v Nizozemsku jich bylo 52 a ve Velké Británii rovných 700.

O zajištění kontinuity činností v organizaci obvykle panují mýty. Často můžeme slyšet, že řízení kontinuity se týká jen přírodních katastrof, že plány kontinuity jsou odpovědností IT nebo dokonce, že každá katastrofa je jedinečnou událostí, na kterou se nelze připravit.

Co je zajištění kontinuity

Co to tedy zajištění kontinuity je? Je to soubor opatření, které vycházejí ze strategických a taktických potřeb organizace. Vhodně zvolená opatření zajišťují schopnost organizace poskytovat své produkty nebo služby na přijatelné a předem definované úrovni, a to i když dojde k rušivému incidentu. Proaktivní řízení kontinuity zlepšuje odolnost organizace proti narušení a její schopnosti plnit své cíle, poskytuje ověřené metody pro obnovení poskytování produktů a služeb po narušení, přináší osvědčené schopnosti řídit narušení činností a chránit dobré jméno a značku organizace. Abychom mohli řádně řídit kontinuitu, potřebujeme k tomu vhodné techniky a nástroje. Tento článek není návod k implementaci systému řízení kontinuity činností (BCMS), ale poskytuje prostor, abychom se na některé komponenty BCMS podívali podrobněji.

Systém řízení kontinuity činností (BCMS)

V roce 2009 přijala mezinárodní organizace pro standardizaci ISO usnesení, podle kterého mají mít všechny normy pro systémy řízení (např. ISO 14001, ISO/IEC 27001, ISO 22301, ISO/IEC 20000 atd.) strukturu, která vychází z normy ISO 9001 (řízení jakosti). Jednotná struktura ISO norem, která se od té doby vyvinula, umožňuje harmonizovat postupy a budovat integrované systémy řízení. A tak systém řízení kontinuity činností zavádí několik klíčových komponent: podporu vedení, politiku, osoby s definovanými odpovědnostmi, řídící procesy (vztažené k zásadám, plánování, implementaci a provozování, hodnocení efektivnosti, přezkoumání vedením a neustálému zlepšování), dokumentaci poskytující auditovatelné důkazy a další procesy specifické pro každou organizaci.

Analýza rizik a analýza dopadů

Správně nastavený systém řízení kontinuity umožňuje organizaci nastavit váhu adaptivních, proaktivních a reaktivních strategií řízení na základě systematického posuzování rizik a analýzy dopadů (BIA = Business Impact Analysis). Rizika, jimž organizace čelí, jsou funkcí interního a externího prostředí, ve kterém organizace působí. Mění se například v závislosti na průmyslovém sektoru/oboru, velikosti organizace i geografickém umístění. Zatímco posouzení rizik řeší oblast identifikace, analýzy a hodnocení rizik, BIA se zabývá analýzou hlavních činností (byznys funkcí) a dopadů, které na ně může narušení mít. A právě identifikace kritických činností klíčových pro-

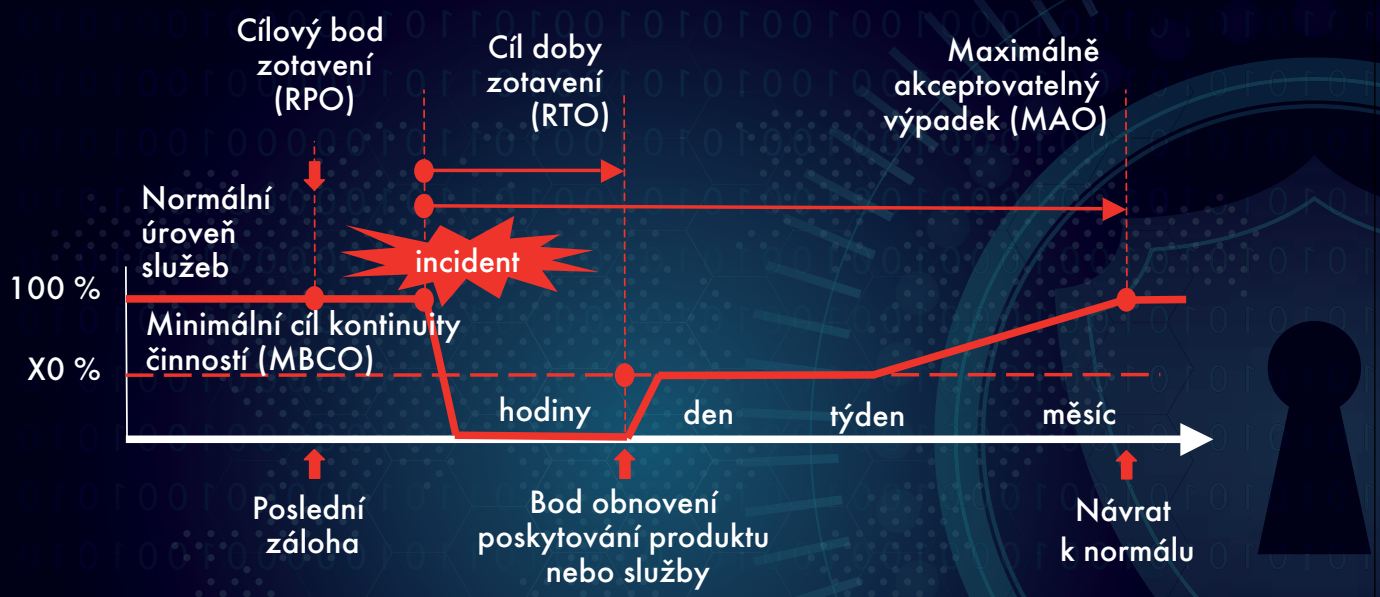
cesů, jejich závislostí a dopadů je nejnáročnějším aspektem analýzy dopadů.
Výsledkem BIA je shromáždění podkladů pro stanovení cílů kontinuity činností, tj. které činnosti musíme udržet v provozu, jaký je minimální cíl kontinuity dané činnosti (MBCO = Minimum Business Continuity Objective), jak rychle musíme provoz obnovit, jaká je cílová doba zotavení (RTO = Recovery Time Objective), k jakému bodu obnovu provádíme (RPO = Recovery Point Objective) nebo jaký je maximální akceptovaný výpadek (MAO = Maximum Acceptable Outage).

Strategie kontinuity činností

Když známe rizika a cíle kontinuity konkrétních činností, můžeme zodpovědně posoudit možnosti a zvolit vhodnou strategii či strategie pro:

- zajištění ochrany prioritních činností před narušením,
- stabilizování, pokračování, obnovení a zotavení prioritních činností po narušení,
- zmírnění, odezvu a zvládání dopadů.

Cíle kontinuity



Při definování strategie zajištění kontinuity činností můžete volit mezi vícero přístupy, od zajištění provozu v nezávislých lokalitách s diverzifikací dodavatelů, přes záložní uspořádání až po přizpůsobení daného procesu. Volba správné strategie bude záviset na chuti organizace riskovat nebo naopak na chuti či možnostech investovat. Nulová strategie, pokud jde o její implementaci, před výskytem ničivé události nic nestojí, ale je to asi ta nejdražší strategie po katastrofě. A naopak, plně vybavená a k okamžitému provozu připravená záložní lokalita je patrně ten nejnákladnější způsob, který však umožní nejrychlejší možné obnovení činností. Většina z nás bude hledat svou cestu někde mezi.

Samozřejmě, některé části strategie nejsou spojeny s investicemi a lze je poměrně rychle realizovat. Příkladem je pojištění, které může zmírnit, i když ne zcela nahradit, finanční dopady narušení. Dalším příkladem je stanovení komunikační strategie, která může efektivně přispět k ochraně dobrého jména organizace i v případě vzniku mimořádné situace.

Ošetření rizik kontinuity

V analýze rizik jsme určili, jakým rizikům čelíme. Musíme se tedy rozhodnout, jakým způsobem existující rizika ošetříme, abychom snížili pravděpodobnost výskytu narušení, zkrátili dobu narušení anebo snížili dopad narušení na schopnost poskytovat klíčové produkty a služby. Zvolený přístup bude opět záviset na ochotě organizace (jejího vedení) riskovat.

Volit můžeme mezi preventivními opatřeními (snižují pravděpodobnost a možný dopad, např. záložní zdroje napájení, instalace systému protipožární ochrany nebo najímání zdatného personálu), detektivními opatřeními (snižují možný dopad, např. detektory tepla nebo kouře, videokamery nebo systém detekce narušení počítačové sítě) a nápravnými opatřeními (zmírňují následky, např. efektivní komunikace, zálohování a obnova dat ze zálohy, plán odezvy na incident). Z podstaty některých opatření vyplývá, že mohou spadat i do dvou nebo dokonce do všech tří skupin, příkladem může být antivirový SW – prevence proti virům, detekce virů, odstraňování virů.

Postupy pro zajištění kontinuity

Nyní víme, které činnosti podporující klíčové produkty a služby musíme chránit, zvolili jsme vhodnou strategii, realizovali jsme nebo jsme naplánovali realizaci potřebných opatření zajišťujících kontinuitu zvolených činností a je před námi další důležitý krok – ustavení postupů kontinuity pro zvládání rušivých incidentů, tedy vytvoření plánu či plánů kontinuity.

Opět závisí na kontextu konkrétní organizace, jak takový plán nebo plány budou obsáhlé a jak detailně budou popisovat postupy reagující na možné incidenty. Existuje více oblastí, které plány kontinuity činností řeší a od toho se také odvíjejí aplikovatelné typy plánů kontinuity.

Metodika implementace

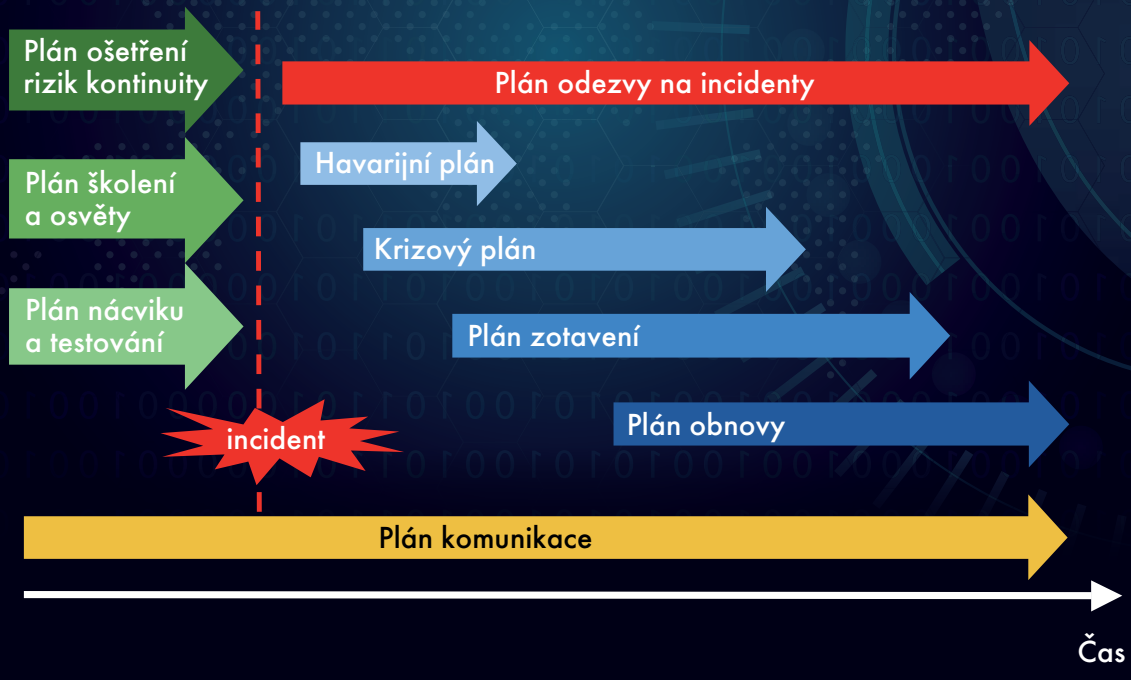
Nyní zhruba víme, co je potřeba udělat, tak si ještě řekněme, jak je možné to udělat. Postupně jsme přijali metodiku pro úspěšnou implementaci a provozování systémů řízení. Tato metodika vychází z PDCA cyklu, který je běžně aplikován v ISO normách pro systémy řízení. Čtyři etapy PDCA cyklu dělíme do 21 kroků, od ustavení projektu BCMS a analýzy existujícího prostředí, přes realizaci všech výše uvedených činností až po interní audit, řízení nápravných opatření a vytvoření kultury neustálého zlepšování.

Závěr

Existuje mnoho zdrojů rušivých incidentů, které mohou výrazně ohrozit nebo dokonce ukončit klíčové činnosti organizace. Od přírodních katastrof, mimořádného počasí, pandemií, výpadků dodávek energií nebo telekomunikačních služeb až po mimořádné události v dodavatelském řetězci, útoky různě motivovaných hackerů nebo chyby či dokonce úmyslné zásahy interních osob. Tak jako se vyskytují černé labutě, vyskytují se i katastrofy. Buďte na ně připraveni, ať nedopadnete tak, jak uvádí Business Continuity Institute – 80 % podniků, které neměly plány kontinuity, nepřežily a opustily své aktivity během 13 měsíců po závažném incidentu.

Ing. Petr Krůček
CEO & Senior Consultant
KRUCEK s.r.o. | Cybersecurity

Plány kontinuity



ROK INFORMATIKY 2019

Magazín Egovernment uspořádal těsně před prázdninami pravidelné setkání všech, pro které je důležitá elektronizace veřejné správy v ČR, především na úrovni obcí, měst a krajů. Ve spolupráci s Jihomoravským krajem a městem Slavkov u Brna jsme pro letošní rok připravili setkání v nádherné „napoleonské" atmosféře zámku Slavkov u Brna.

Tato každoroční akce je již tradičně třídenní a letošní rok nebyl výjimkou. Prvním konferenčním dnem je vždy středa a začíná se odpoledním programem, který je vždy cílen na konkrétní skupinu. Letos se jednalo o setkání ORP s představiteli OHA MV ČR.

Tým OHA vedl jeho ředitel Ing. Petra Kuchař a všichni nejen prezentovali, ale rovněž odpovídali na řadu podrobných dotazů z publika. Účastníci konference mohli své dotazy zasílat v předstihu elektronicky a tak několik zásadních témat, která bylo potřeba vysvětlit, bylo již v prezentacích obsaženo.

Druhý den konference – čtvrtek – je vždy hlavním jednacím dnem. V rámci hodinového bloku zástupci odboru eGovernmentu MV ČR v čele s jeho ředitelem Romanem Vrbou informovali o aktuálních záležitostech, především Portálu občana, RPP, datových schránkách atd. Na jejich prezentace navazoval Michal Pešek, ředitel SZR, s tématem Národní identitní autority a Miroslav Tůma se státním cloudem.

Tradiční součástí konference Rok informatiky je vždy přehled aktuálního dění v oblasti elektronizace krajů, tzv. pětiminutovky. Dopolední program uzavřely informace společnosti CISCO o řešení datových center a GORDIC o technologiích pro SMART regiony.

Odpolední prezentace je většinou přehledem realizovaných projektů a řešení, kde vystupují společně odborníci jednotlivých firem se zástupci a představiteli úřadů, které jejich realizace využívají. Závěrečná část je pak, již rovněž tradičně, vyhrazena společnosti Microsoft a jejich nabídce služeb veřejné správě.

Páteční dopoledne bývá workshopové, letos bylo vyhrazeno živým ukázkám možnosti elektronického úřadování. Petr Špetlík ze společnosti Microsoft zde podrobně ukázal možnosti nasazení Microsoft Teams. Tím odborný program konference sice skončil, ale kdo měl náladu, mohl se ještě vydat na exkurzi do bezpečnostního dohledového centra SOC365 v Brně Slatině, kterou zajistila společnost Visitech.

Jednotlivé prezentace, které v rámci programu zazněly, a fotografie z konference naleznete na: **www.egovernment.cz v sekci ROK INFORMATIKY.**

BEZPEČNOST SD-WAN MUSÍ BÝT NEJVYŠŠÍ PRIORITOU

Softwarově definované sítě WAN získávají na oblibě díky ekonomickým výhodám a přínosům z hlediska výkonu připojení poboček k centrále a u cloudové konektivity. Firmy proto do SD-WAN investují, ale musejí současně řešit otázky bezpečnosti, které jsou s implementací SD-WAN spojené.

Obliba SD-WAN stoupá především díky vysokému výkonu a nenáročnosti správy a je nejlepší variantou pro firmu, která potřebuje síťovou konektivitu mezi podnikovými pobočkami. SD-WAN ale může stejně dobře být vhodným řešením pro společnost, jež prochází digitální transformací a vyžaduje rychlé a výkonné připojení pro softwarové aplikace **poskytované formou služby (SaaS)** nebo pro multicloudové prostředí. V obou případech bude firma očekávat nejen takový výkon WAN, který bude odpovídat garantovaným parametrům jeho aplikací, ale bude také usilovat o zjednodušení připojení WAN a snížení investičních výdajů.

Hlavní problém využití SD-WAN spočívá v bezpečnostních rizicích, které s sebou nese. SD-WAN může obcházet podnikové datové centrum a poskytovat přímé připojení k internetu. To znamená, že příchozí a odchozí komunikace podnikových poboček ztrácí výhody podnikových firewallů a jednotných bezpečnostních pravidel. Typické architektury SD-WAN rovněž rozšiřují prostor pro kybernetické útoky, protože zvyšují počet síťových zařízení, která si útočníci mohou zvolit za cíl. Ještě závažnější problém je, že mnoho samostatných řešení SD-WAN postrádá pokročilé bezpečnostní funkce, například **prevenci průniku (IPS),** analýzu škodlivého softwaru nebo běh v izolovaném prostředí (sandboxing).

Bezpečnost na prvním místě

Celkem logicky je proto bezpečnost nejvážnější obavou uživatelů u sítí WAN. Následně je teprve zajímá výkon sítě a růst nákladů. Podniky si stále častěji uvědomují, že kvůli dodržování zákonných povinností a obchodních požadavků musí jejich SD-WAN řešení zajišťovat také konzistentní zabezpečení a možnosti správy. A právě zde nastupují řešení společnosti Fortinet.

Fortinet byl prvním výrobcem **firewallů příští generace (NGFW)**, který do tohoto typu zařízení začlenil nativní podporu SD-WAN. Zatímco mnoho dodavatelů SD-WAN spoléhá na to, že jejich síťové řešení bude doplněno pokročilými bezpečnostními produkty jiných výrobců, bezpečné řešení SD-WAN společnosti Fortinet nativně poskytuje zabezpečení NGFW a správu a řízení využití zdrojů WAN (podkladové vrstvy), a tím umožňuje zajistit garantované parametry připojení pro jednotlivé aplikace. Stejné zařízení, které zajišťuje funkcionalitu SD-WAN, zároveň poskytuje plné spektrum bezpečnostních schopností.

A díky tomu, že se firewally příští generace FortiGate integrují do bezpečnostní architektury Fortinet Security Fabric, automaticky s ostatními bezpečnostními řešeními podniku sdílejí informace o detekovaných hrozbách a reakci na ně. Mají přístup k bezpečnostnímu zpravodajství laboratoří FortiGuard a mohou využívat funkce nástroje FortiSandbox a s jejich pomocí bránit průniku škodlivého softwaru k serverům nebo koncovým bodům firmy.

Proč podniky přecházejí na SD-WAN?

Podle výzkumné společnosti IDC podniky stále větší měrou spoléhají na SD-WAN jako způsob, jak automatizovat směrování aplikačního provozu k pobočkám a vyhnout se tradiční hvězdicovité topologii WAN a vedení internetového a cloudového provozu z poboček přes centrální datové centrum.

Řešení SD-WAN zvyšují výkon aplikací díky inteligentnímu směrování síťového provozu, ale také zlepšují nákladovou efektivitu připojení. Centralizovaná správa této technologie a zprovoznění bez zásahu technika zjednodušují zavádění a průběžnou údržbu síťového připojení. SD-WAN dokáže propojit nové pobočky s ústřední podnikovou sítí metodou „plug-and-play" bez složitého nastavování. Zprovoznění nevyžaduje žádné odborné technické ani bezpečnostní znalosti.

Co je však pravděpodobně nejdůležitější, firewally příští generace FortiGate spolehlivě prokázaly své kvality v reálném provozu. Ve svém historicky prvním skupinovém testu SD-WAN řešení udělila v roce 2018 nezávislá zkušební laboratoř NSS firewallu FortiGate hodnocení „Doporučené". Řešení Fortinet Secure SD-WAN vykazovalo nejlepší nebo téměř nejlepší výsledky v oblasti přenosu hlasu přes IP síť (VoIP), videa a výkonu sítě a nabídlo o 88 % nižší celkové náklady na vlastnictví než nejbližší konkurent.

Obliba SD-WAN stoupá, avšak podniky si začínají rychle uvědomovat, že ne všechna řešení SD-WAN nabízejí srovnatelné možnosti. Implementace flexibilního a přizpůsobitelného řešení vyžaduje úzkou integraci funkcionalit WAN a LAN, podporu vysokokapacitního připojení VPN a integrované zabezpečení, které lze propojit s lokálními a WAN bezpečnostními řešeními, a chránit tak stále složitější komplex síťových, internetových a IoT řešení. Z hlediska ucelenosti, provázanosti, bezpečnosti a jednoduchosti nasazení a správy nedokáže žádný jiný dodavatel konkurovat řešení pro bezpečnou síť SD-WAN od společnosti Fortinet.

TŘI ÚSPĚŠNÉ IMPLEMENTACE SD-WAN OD FORTINETU

Rozsáhlá síť supermarketů

Jeden z největších nizozemských řetězců supermarketů s obratem více než 176 miliard korun a více než 900 prodejnami hledal možnosti, jak snížit provozní náklady na MPLS WAN a zavést konzistentní zabezpečení všech WAN a LAN řešení v každé prodejně. Na straně WAN bylo cílem nahradit původní řešení MPLS řešením SD-WAN, u LAN posílit zabezpečení prodejních systémů (POS) a zajistit provoz a zabezpečení stoupajícího počtu IoT zařízení třetích stran v prodejnách.

Zařízení FortiGate porazilo konkurenci díky integraci bezpečné sítě SD-WAN a pokročilého zabezpečení sítě do jediného řešení. Fortinet dokázal poskytnout Secure SD-WAN jako řešení pro okraj WAN, rozšířit softwarově definovanou pobočku přístupovými body a přepínači a díky úzké technické integraci zařízení FortiGate a FortiSwitch mohl zajistit uplatňování bezpečnostních pravidel na každém portu v prodejně, aniž bylo nutné instalovat zabezpečení koncových bodů na POS a IoT zařízení. To bylo obzvlášť přínosné, protože řada IoT zařízení, jako chladicí pulty a mrazicí boxy, byla ve vlastnictví třetích osob, takže instalace zabezpečení nepřicházela v úvahu. A to vše lze na všech pobočkách řídit pomocí jediného centrálního nástroje pro správu.

Globální energetická společnost

Jedna z největších světových ropných a plynárenských společností s obratem přes 4,4 bilionu korun hledala ekonomicky přijatelný způsob, jak zajistit přímé spojení mezi svými více než 15 tisíci čerpacími stanicemi po celém světě. Cílem bylo snížit objem dat, který k provozu vyžaduje technologie MPLS, a rozšířit strategii upřednostňující cloud do celé infrastruktury.

Společnost hledala řešení, které by poskytlo funkcionalitu SD-WAN, bezproblémovou konektivitu LAN a odpovídající zabezpečení. Po pečlivém posouzení hlavních řešení SD-WAN na trhu byla zvolena společnost Fortinet jako dodavatel projektu zavedení SD-WAN připojení globální sítě čerpacích stanic.

Mezi rozhodující funkce patřilo automatické přepnutí linky na náhradní připojení při výpadku pro Office 365 a pro vlastní aplikace a pokročilé zabezpečení přímého připojení. Společnost Fortinet dokázala tuto funkcionalitu rozšířit i do softwarově definovaných poboček pomocí bezdrátových přístupových bodů a přepínačů Fortinet. Fortinet byl navíc jediným dodavatelem, který dokázal poskytnout centralizované integrované řešení pro správu celé zavádějící sítě.

Maloobchodní řetězec s obuví

Jedna z největších evropských sítí prodejen obuvi s ročním obratem téměř 132 miliard korun hledala novou infrastrukturu LAN a WAN, která by zajistila lepší přehled, bezpečnost a správu celé síťové infrastruktury. Cílem bylo využít funkcionalitu SD-WAN ke směrování datového provozu aplikací, ale společnost potřebovala řešení, které bude mít integrované zabezpečení se SSL.

Firma chtěla také koncentrátor VPN pro datové centrum, který by zvládal 40 000 tunelů VPN při rychlosti 20 GB, podporoval hloubkovou integraci s přístupovými body a přepínači a kvůli nepřítomnosti IT pracovníků v provozovnách také připojení veškerých zařízení bez asistence technika ve všech 4 000 poboček.

V rozsáhlém výběrovém řízení, kde mnozí dodavatelé tvrdili, že spolu s funkcionalitou SD-WAN poskytují také zabezpečení, dokázalo pouze řešení společnosti Fortinet splnit požadavky na bezpečnost. Výsledné řešení pro okraj WAN a LAN zahrnovalo také integrované zařízení pro jednotnou správu hrozeb s veškerými bezpečnostními funkcemi, včetně sandboxingu, pro každou prodejnu spolu se třemi až pěti přístupovými body, okrajovými přepínači a výkonným koncentrátorem VPN pro datové centrum.

FORTINET

info◆com

- Sympozia
- Konference
- Kongresy

Na Zatlance 10, Praha 5 • Tel.: 241 412 518 • infocom@infocom.cz • www.infocom.cz

SPISOVOU SLUŽBU ČEKAJÍ ZÁSADNÍ ZMĚNY

Třetího října loňského roku přijala vláda usnesení č. 630 o provedení analýzy informačních systémů pro správu dokumentů a služeb vytvářejících důvěru pro elektronické transakce ve veřejném sektoru. Cílem projektu mělo být zjištění, v jakém stavu se reálně nachází výkon spisové služby ve státní správě. Ve vzorku 76 vybraných subjektů tak byly zastoupeny všechny kategorie původců: zákonodárci (sněmovna, senát), ministerstva, soudy či správní orgány (například Státní energetická inspekce). Co do rozsahu tak šlo o jednu z nejrozsáhlejších analýz stavu vedení spisové služby od přijetí zákona č. 499/2004 Sb., o archivnictví a spisové službě.

V digitálním světě chybí jednotný postup

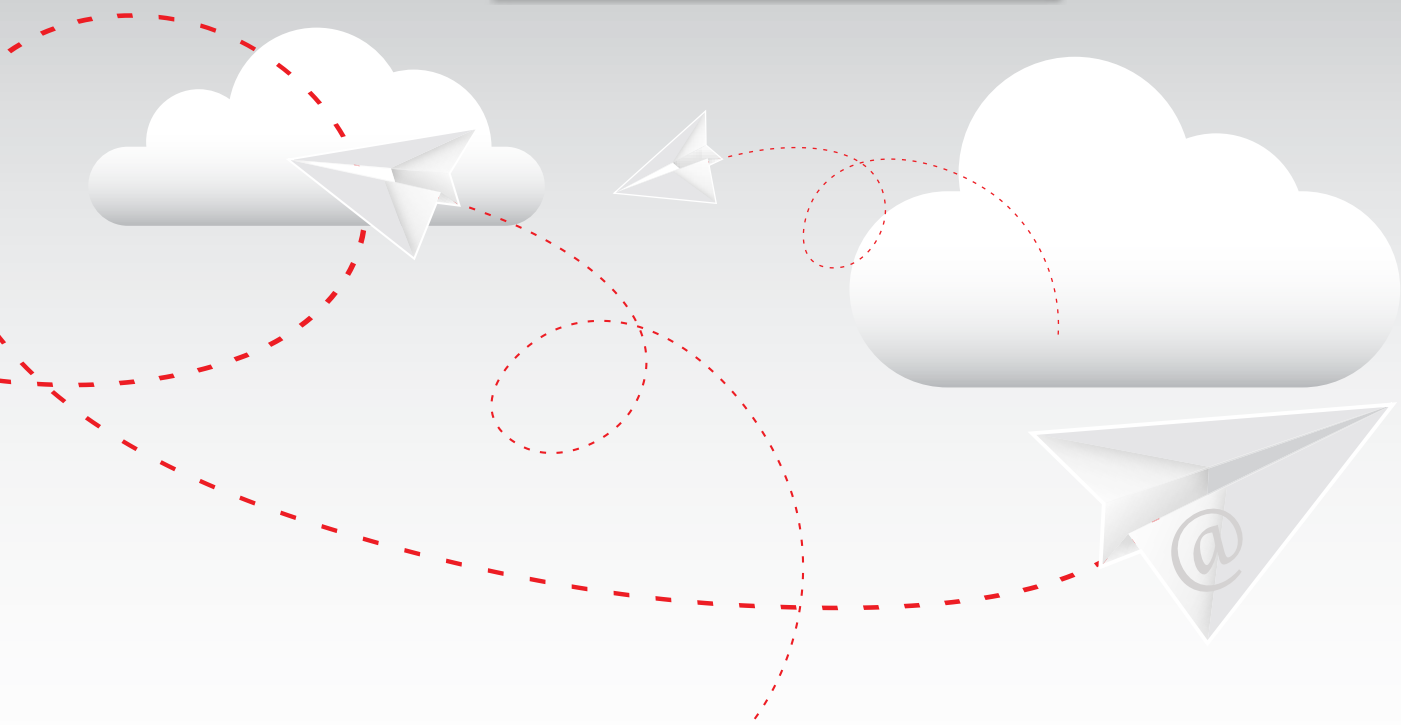
Již samotná příprava tohoto projektu však nebyla jednoduchá. Původní zadání směřovalo ke zjištění, jak jednotliví původci plní své povinnosti či zda informační systémy, podporující vedení spisové služby, splňují požadavky stanovené příslušnými právními předpisy. Nic proti tomu – obě tyto oblasti jsou důležité a již dopředu bylo zřejmé, že ne vždy bude možné původce a jejich dodavatele za reálný stav pochválit. Nicméně stejně tak bylo evidentní, že je třeba dokumentovat i dlouhodobě neřešené střety požadavků jednotlivých právních předpisů s dopadem na výkon spisové služby či výkladovou jednoznačnost metodik a doporučení.

V záplavě předpisů, které přímo či nepřímo výkon spisové služby ovlivňují, se ty správné cesty a postupy hledají velmi obtížně. To, co se dlouhodobě a zvykově realizuje s listinným dokumentem (například vyznačení doložky nabytí právní moci či vykonatelnosti), žel dosud není pro digitální dokumenty právními předpisy jednoznačně definováno. A je nahrazující metodiky ne vždy stačí. A to zdaleka není jediný případ nedořešené odchylnosti listinného a digitálního světa. V praxi to pak vede k tomu, že fakticky identické procesy realizuje každý původce odchylně – a ne vždy správně. Tato skutečnost se pak negativně promítá i do vývoje a provozu elektronických spisových služeb. ICT Unie proto prostřednictvím Hospodářské komory požadovala, aby se analýza zaměřila i na stav souvisejících právních předpisů a identifikaci legislativních překážek.

Ne nepodstatnou oblastí je rovněž zajištění přiměřeného personálního provozu spisové služby. I zde bylo dopředu jasné, že stav u jednotlivých původců zdaleka není ideální – nedostatkem metodiků počínaje přes malý rozsah školení až po nedostatečné finanční ocenění pracovníků podatelen. I tato oblast proto byla zahrnuta do plánovaného zjišťování.

Samotné šetření pak u vybraných původců probíhalo v únoru a březnu. Již první výsledky potvrdily řadu předpokladů zadavatele. Někteří z původců totiž stále spisovou službu vykonávají výhradně v souladu s ustanoveními § 3 a § 63 až § 70 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů a prováděcími právními předpisy, kterými jsou vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby a Národní standard pro elektronické systémy spisové služby, zveřejněný ve Věstníku MV, částka 57/2017. Rozsah legislativního rámce spisové služby, který musí původci i dodavatelé zohlednit, je nicméně výrazně širší a zahrnuje jak vybrané tuzemské právní předpisy (jako např. správní řád, kontrolní řád, zákon o kybernetické bezpečnosti apod.), tak prameny sekundárního práva Evropské unie (nařízení eIDAS, GDPR apod.), případně vybrané technické normy.

Spisová služba je přesto u některých veřejnoprávních původců stále neoprávněně na okraji zájmu a ani ve vědecké oblasti jí není věnován dostatečný prostor. Přitom elektronický systém spisové služby je páteřním (a nezřídka



jediným) informačním systémem veřejnoprávních původců. A především je systémem, jenž umožnuje příjem doručených a odeslání vlastních dokumentů prostřednictvím datových zpráv, zabezpečuje oběh dokumentů v rámci úřadu, jejich dohledatelnost, průkaznost a právní validitu.

Cestou k nápravě budou akční plány

Výčet nedostatků zjištěných analýzou byl tak rozsáhlý, že nebylo možné nereagovat. Počátkem května tak byl vládě předložen návrh opatření zahrnující jak krátkodobé, tak střednědobé cíle. Mezi ty patří zejména příprava nového zákona upravujícího vedení spisové služby v souladu s požadavky a potřebami e-governmentu. Ministerstvo vnitra v této souvislosti uvítalo nabídku spolupráce od prezidenta ICT Unie Mgr. Zdeňka Zajíčka. Na přípravě nové právní úpravy se tak budou moci podílet zkušení metodici a analytici dodavatelských firem. Vedením příslušné pracovní skupiny ICT Unie byl pověřen hlavní architekt elektronické spisové služby GINIS Mgr. Vít Cvrček.

Zároveň je nezbytné zahájit nápravu nejzásadnějších chyb. Usnesení vlády, které bylo k výsledkům analytického projektu dne 13. 5. 2019 přijato, proto počítá s uložením povinnosti všem ústředním správním úřadům zpracovat akční plán rozvoje spisové služby ústředního správního úřadu a předložit ho Ministerstvu vnitra v termínu do 30. září 2019. Aby byly tyto plány srovnatelné, ukládá návrh usnesení Ministerstvu vnitra zpracování pravidel pro definici podoby a minimálního rozsahu akčních plánů v termínu do 31. května. Třetí článek usnesení pak doporučuje vedoucím ostatních ústředních veřejných úřadů nepodřízených vládě postupovat obdobně.

Byť tedy návrh usnesení neukládá přímou povinnost všem určeným původcům, přináší jasný vzkaz: v kontrolách zaměřených na vedení spisové služby se bude pokračovat v zájmu udržení důvěryhodnosti dokumentů spravovaných původci. Ministerstvo vnitra zároveň přislíbilo aktualizaci vydaných metodik a jejich publikaci na jednom místě.

Společnost GORDIC nabídne svým zákazníkům podporu při zpracování akčních plánů i při aktualizaci a rozšíření elektronického systému spisové služby GINIS tak, aby splňoval jak současné, tak již dnes známé funkcionality nezbytné pro vedení plně elektronické spisové služby a realizaci řízení. I nadále pak budeme pro naše zákazníky zajišťovat informační podporu tak, aby na všechny novinky a povinnosti vyplývající z připravované nové právní úpravy byli původci připraveni včas v dostatečném rozsahu.

Mgr. Vít Cvrček
hlavní architekt spisové služby
GORDIC

GORDIC®

WEBOVÉ PORTÁLY: AKTUÁLNÍ ZRANITELNOSTI A HROZBY

O pohled na problematiku ochrany webových portálů proti aktuální zranitelnosti jsme požádali společnost F5 Networks, která je specialistou na vysokou dostupnost aplikací, aplikační bezpečnost, DDoS ochranu, identity management a centralizované řešení SSL na perimetru.

Botnety vládnou internetu

Pouhých 6 minut průměrně trvá, než je aplikace, která byla publikována do prostředí internetu (může se jednat o spuštění nových webových stránek, zákaznického portálu, portálu pro občany, extranetu atd.), „oskenována" hackry. Za necelé dvě hodiny je taková aplikace prolomená v případě, že není chráněna proti zranitelnosti Právě aplikace jsou totiž branou k citlivým datům o zákaznících, zaměstnancích, pacientech nebo občanech.

Prolomit tuto bránu zvládají generátory robotické komunikace na internetu, tzv. botnety. Jedná se o softwarové programy, které spouští automatizované úlohy (skripty). Odhaduje se, že roboty všech druhů představují více než 50% dnešního internetového provozu. Karel Čapek vymyslel jméno robot, ale těžko mohl čekat, jak se může význam tohoto slova změnit vlivem internetu.

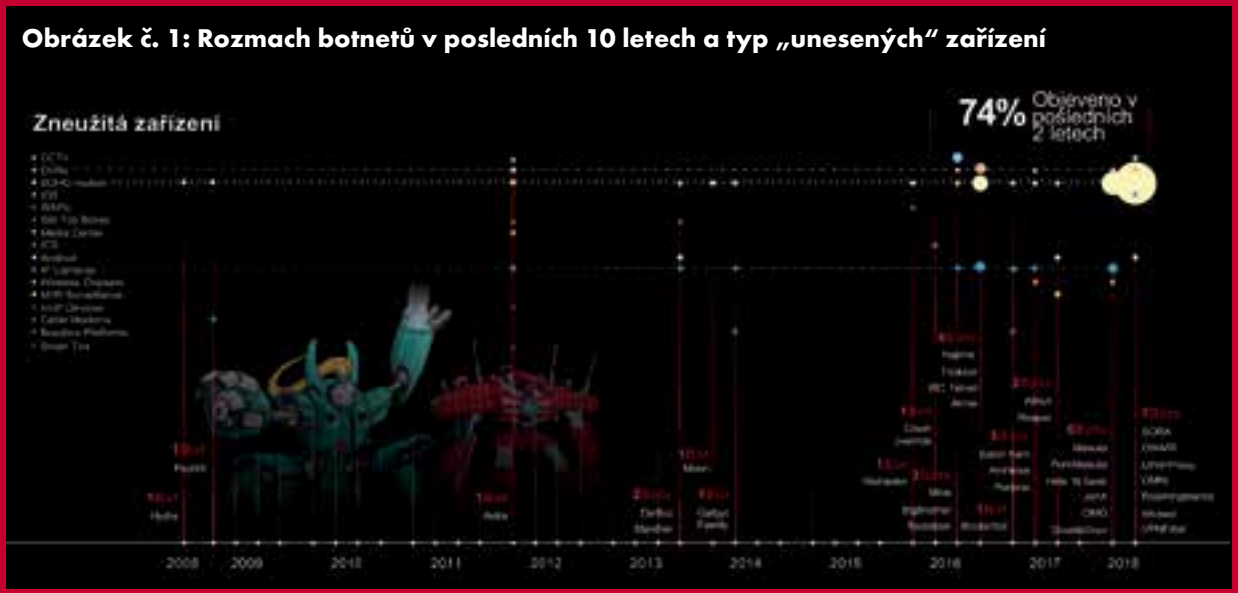
Když jsou Boti dobří

„Dobří" roboti jsou určeni na pomoc podnikům a spotřebitelům. Už od počátku devadesátých let minulého století byly vyvinuty první roboty pro vyhledávače, aby procházely internet a hledaly („indexovaly") informace. Bez nich by neexistovaly společnosti Google, Yahoo a Bing. Další příklady dobrých botů - většinou zaměřených na spotřebitele – zahrnují chatboty (např. Apple Siri) nebo shopboty (např. Aukro).

Když jsou Boti zlí

Všechno, co je určeno pro dobro, bývá zneužito pro zlo a to platí i pro internetové roboty. Pro útočníky spočívá skutečná síla botů v botnetech – miliónech zařízení infikovaných malwarem (tzv. zombie), které řídí útočník z kontrolního centra (C&C – Command and Control Center). Botnety poskytují kolektivní procesní sílu, která je nezbytná pro spuštění rozsáhlých útoků. Speciální kategorií jsou Thingboty, tvořené zařízeními internetu věcí (Internet of Things). Většinou se jedná o IP kamery, domácí routery, herní konzole atd., jež dostaly při výrobě jednoduché uživatelské jméno a heslo typu admin/admin. Útočník pomocí svého stávajícího botnetu „oskenuje" v internetu nově spuštěné zařízení a převezme pod svou kontrolu, aniž bychom o tom věděli. Zlé botnety jsou s námi už celé jedno desetiletí, ale skutečný rozmach nastal v posledních 2 letech, kdy byly objeveny skoro tři čtvrtiny všech známých botnetů (obrázek č. 1).

Obrázek č. 1: Rozmach botnetů v posledních 10 letech a typ „unesených" zařízení



Prakticky všechna počítačová zařízení, která byla „unesena" špatnými roboty, se používají pro škodlivé činnosti, jako např.:

- **útoky DDoS (Distributed Denial of Service)** – Doslova s miliardami zranitelných IoT zařízení jsou útočníci schopni vybudovat masivní botnety a provádět obrovské DDoS útoky, jako byly útoky z Botnetu Mirai ve 2016 na DynDNS a OVH, nebo útok o síle 1.3 Gbps na GitHub v roce 2018. Cílem je vyřadit webové portály nebo infrastrukturu z provozu a znemožnit jejich dostupnost;
- **aplikační útoky** – k takovému útoku není třeba velký botnet, ale stačí pár strojů, někdy dokonce jeden počítač. Často se takový útok skrývá ve velkém volumetrickém útoku, který útočníkům slouží jako zastírací kouřová stěna. Cílem útočníků je získat citlivá data o uživatelích služby, na kterou je útok cílen;
- **použití zcizených uživatelských identit s cílem převzít účet (Credential stuffing)** – útočníci používají roboty ke spouštění automatizovaných útoků. Ukradené databáze s uživatelskými jmény a hesly používají na portálech s cílem získat neoprávněný přístup k účtům s citlivými daty. Zda je konkrétní identita součástí internetových databází zcizených identit, je možné zjistit na stránce https://haveibeenpwned.com/;
- a další, jako je **zneužití platebních karet, využití kapacity napadených zařízení pro těžbu kryptoměn, pro distribuci spamu, nechtěné skenování obsahu na webových stránkách** a mnoho dalších.

Využití botnetů útočníky je zobrazeno na obrázku č. 2.

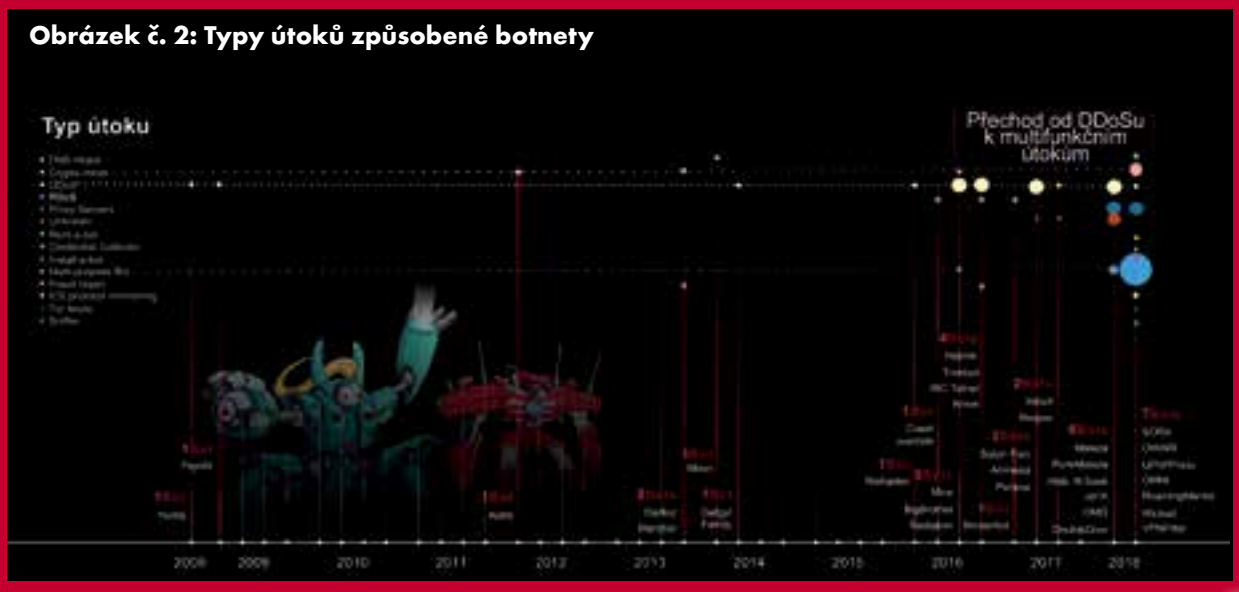
Možnosti botnetů jsou de-facto neomezené a jejich síla se bude do budoucna zvětšovat. Útoky botnetů mají přímý, ale i nepřímý finanční dopad na vaše organizace. Vytvářejí totiž další provoz v síti, který může zpomalit stránky a konzumuje kapacitu zařízení na bezpečnostním perimetru datového centra. Je to také provoz, se kterým je potřeba se vypořádat, když platíme za internetovou konektivitu do privátního cloudu nebo za kapacitu ve veřejném cloudu.

Jak na ně?

Neexistuje jedno univerzální řešení, jak dostat provoz zlých botů z datového centra. Ale kombinace různých nástrojů zajistí účinnou ochranu. Zde jsou příklady takových nástrojů, kterými by měl disponovat Web Aplikační FW (WAF) na bezpečnostním perimetru datového centra:

- **detekce založená na jednoznačných identifikátorech (signaturách)** – Boti mohou být identifikováni pomocí jedinečných nebo specifických vzorců chování, které byly pozorovány v minulosti. Ačkoli detekce botů založená na signaturách je spolehlivá, nemůže detekovat nové neznámé roboty. Pro udržení kroku s novými roboty bude potřeba neustále aktualizovat signatury a vytvářet nové;
- **detekce chování založená na analýze nestandardního chování, tzv. behaviorální analýze** – zahrnuje identifikaci vysokého nebo nepravidelného provozu, pokusy o spuštění nebo zastavení procesů v aplikaci, pokusy o stažení spustitelných souborů nebo přístup k omezeným souborům a vzory robotického surfování;
- **identifikace podvodného robotického uživatele pomocí webového prohlížeče** – prohlížeč každého

Obrázek č. 2: Typy útoků způsobené botnety



jednotlivého uživatele má svůj vlastní podpis, který identifikuje, jak byl vytvořen a konfigurován na konkrétním zařízení a zda se jedná o skutečného uživatele nebo robota;

- **použití CAPTCHA k rozlišení chování člověka od botů na webových stránkách** – CAPTCHA není pro uživatele přívětivé řešení, proto je možné ho vynutit jen v případě, že Web Aplikační FW vyhodnotí chování uživatele jako nestandardní s podezřením na robota;
- **zpětné vyhledávání útočníků podle IP adresy a její následné blokování na Firewallu** – útoky jsou sice často spouštěny ze stovek různých IP adres, ale zpětné vyhledávání může být efektivní způsob, jak identifikovat i ty dobré roboty, jako je např. indexování stránek vyhledávači. A u těch je naopak potřeba zajistit, aby blokovány nebyly, a dát je na „whitelist".

Je uživatelské jméno a heslo mrtvá technologie?

Útočníci mají v zásadě 2 nástroje, jak zcizit přístupová data.

- První možnost je přímo **z webového portálu**, jelikož webová aplikace je branou k citlivým datům. U portálů, které nejsou chráněny proti zranitelnosti, je možné vložením správně formulovaného databázového dotazu do přihlašovacích polí portálu získat např. přístupová data uživatelů. V posledních letech patří mezi hackery tento útok – tzv. injection – k nejoblíbenějším pro získání citlivých dat z aplikací. Během útoku webová aplikace zpracuje neočekávaný příkaz nebo umožní přístup k datům bez řádné autorizace. Potvrzuje to i klasifikace útoků na webové aplikace popsaná nezávislým sdružením OWASP – Open Web Application Security Project (obrázek č. 3).

- Druhý nástroj útočníků je **zcizení dat přímo z koncové stanice, tj. z PC pomocí malwaru**, který se do počítače dostane neopatrným chováním uživatele na internetu – otevřením zavirované přílohy v e-mailu, návštěvou závadných webových stránek, použitím infikované USB klíčenky atd. Při zadávání uživatelského jména a hesla malware „poslouchá" a informace pošle útočníkovi. Alternativně útočník pomocí malwaru zcizí obsah souboru cookie v počítači. V cookie jsou i další citlivé informace, jako např. čísla kreditních karet, které se díky cookies předvyplňují při nákupech v e-shopech. Zcizení obsahu cookies je obecně velkým bezpečnostním problémem, jelikož útočník se pomocí jeho obsahu může vydávat za původního uživatele.

Podle sdružení OWASP je narušení autentizace, jejímž cílem je vydávat se během ověřovacího procesu za skutečného uživatele, druhým nejčastějším útokem na webové aplikace. Útočníci kompromitují hesla, klíče nebo tokeny nebo hledají jiné nedostatky v implementaci autentizačních nástrojů s cílem dočasně nebo trvale převzít identitu legitimních uživatelů. Společným jmenovatelem těchto útoků jsou opět škodlivé botnety. Pomocí automatizovaných operací generují aplikační útoky typu „injection" anebo umí distribuovat malware do koncových stanic, které nejsou proti malwaru chráněné.

Obrázek č. 3: Deset nejčastějších útoků na webové aplikace podle sdružení OWASP v letech 2013 a 2017

Jak na to?

V prvé řadě je nezbytné edukovat uživatele o správném chování na internetu. Zkušenost ale praví, že to zdaleka nestačí. Koncové stanice je potřeba mít chráněny proti virům a malwaru. A v neposlední řadě je potřeba chránit samotnou webovou aplikaci takovými zařízeními, která si umí poradit se všemi deseti nejčastějšími OWASP útoky. A nezapomínejme na ochranu proti škodlivým botnetům, která by dnes měla být samozřejmostí.

Řešením je rovněž implementace řešení Identity Managementu. Jeho součástí je vícefaktorové ověření uživatele **(Multi-Factor Authentication – MFA) v kombinaci s technologií jednotného přihlašování, tzv. single sign-on (SSO).**

- S pomocí SSO si už uživatel nemusí pamatovat desítky hesel, ale pouze jedno, které je použito pro všechny aplikace v organizaci. Stejný koncept je možné použít pro jednotné přihlašování do zákaznických portálů. Je to velká úleva pro IT helpdesky organizací a nakonec i samotné IT administrátory.
- MFA pak ověřuje identitu uživatele za použití dalších nástrojů, které pomáhají zvýšit důvěru v uživatele. Nejčastější je využití dvoufaktorového ověřování, které většinou spočívá v užití kombinace uživatelského jména, hesla a jednorázového hesla (OTP) nebo kódu generovaného např. bezpečnostním tokenem nebo aplikací ve smartphonu, kterým disponuje pouze uživatel. Právě tento druhý faktor znemožní útočníkům, aby neoprávněně přistoupili ke službě s pomocí odcizeného uživatelského jména a hesla.

To platí i pro přihlašování do SaaS, jako např. Office 365. Právě s těmito aplikacemi se mění vnímání bezpečnostního perimetru, který je logicky definován napříč jednotlivými aplikacemi nehledě na to, kde jsou instalovány, zda „doma" nebo v cloudu. Někteří výrobci, jako např. F5, umožňují vynucení MFA (případně také vynucení přístupu k aplikaci přes VPN) jen pro konkrétní části aplikace podle citlivosti k přistupovaným datům.

Nechráním, co nevidím

Většina dnešního internetového provozu je https, tedy šifrovaná pomocí protokolu SSL/TLS. Důvodem je zajištění integrity komunikace a eliminace zranitelnosti uživatelů vůči internetovým hrozbám, jako je zcizení citlivých dat ať už privátního nebo komerčního charakteru.

F5 Networks

F5 Networks je specialista na vysokou dostupnost aplikací, aplikační bezpečnost, DDoS ochranu, identity management a centralizované řešení SSL na perimetru. Mezi její zákazníky v České republice patří největší české banky, státní instituce, velké státní firmy, operátoři a komerční firmy. www.f5.com

Šifrování je ale na druhou stranu výzvou pro podniky a státní organizace co se týče ochrany jejich interní sítě. Dešifrování klade nemalé požadavky na výkon bezpečnostních zařízení na perimetru. Proto se některé organizace někdy uchylují k vypnutí dekrypce SSL na perimetru, pokud takové zařízení kapacitně nestíhá, což ale znamená slepé místo v ochraně interní sítě nebo aplikace. SSL/TLS je totiž nástrojem pro útočníky, aby v šifrované komunikaci schovali malware nebo jinou zranitelnost. Navíc pokrok je neúprosný a s rostoucími hrozbami vznikají nové šifrovací algoritmy a protokoly, jejichž podporu je nezbytné zajistit, jako např. nedávno zveřejněné TLS 1.3.

Pro účinnou ochranu je nezbytné, aby všechna zařízení na perimetru dělala dekrypci a inspekci provozu proti zranitelnosti. Pokud výkonově nestačí, nabízí se řešení centralizované správy SSL certifikátů v jednom zařízení, které umí dělat inteligentní směrování provozu (service chaining) na další bezpečnostní zařízení podle typu provozu a závažnosti komunikace – NGFW, DLP, Sandbox, Web proxy atd., které už dekrypci a re-enkrypci nemusí řešit. Takové řešení je také výhodné z provozního hlediska a umožňuje škálovatelnost.

Případné další informace o problematice hrozeb a ochraně aplikací, které přesahují rozsah tohoto článku, je možné najít na stránkách F5 LABS https://www.f5.com/labs.

Výhodou F5 je možnost konsolidace zmíněných bezpečnostních funkcí do jednoho zařízení v datovém centru, nebo do jedné SW instance, která může být volitelně instalována v privátním nebo veřejném cloudu. To výrazně zjednodušuje správu řešení, zvyšuje bezpečnost a v neposlední řadě snižuje TCO, tedy náklady na údržbu v celém horizontu životního cyklu projektu zákazníka.

Filip Kolář , Sales manager F5

PROJEKT SONIA: ELEKTRONICKÁ IDENTITA PRO 5 MILIONŮ ČECHŮ

Představte si, že z pohodlí svého domova za pomocí svých přihlašovacích údajů do internetového bankovnictví zjistíte, kolik vám zbývá „řidičských bodů", zaplatíte poplatek za psa, vyřídíte smlouvu o dodávce plynu či elektřiny, nebo se pojistíte. Vše jednoduše a bez čekání, bez nutnosti skenovat a zasílat kopie dokladů či jinak dodatečně potvrzovat svou totožnost. Takovou vizi přináší projekt SONIA.

Důvěryhodná elektronická identita je dnes nezbytnou podmínkou přístupu ke službám státu i provádění důležitých transakcí se soukromými subjekty. Evropská unie na tuto dlouho pociťovanou potřebu reagovala nařízením eIDAS, stát pak přijetím zákona č. 250/2017 Sb., o elektronické identifikaci, a vybudováním Národního bodu pro identifikaci a autentizaci (NIA). Občanům stát zároveň vydává občanské průkazy použitelné jako prostředek elektronické identifikace.

Řada občanů však nevyužívá možnost aktivovat svůj občanský průkaz pro elektronickou identifikaci a cesta občanských průkazů jako prostředků elektronické identifikace k většímu rozšíření tak bude ještě dlouhá. Současně lze aktivovaný elektronický občanský průkaz využít pouze pro identifikaci ve vztahu ke službám orgánů veřejné moci a těch, kteří ověřují totožnost na základě zákonné povinnosti. Kvůli tomuto omezení, vyplývajícímu z § 2 zákona o elektronické identifikaci, tak zůstává důvěryhodná a univerzální elektronická identita pro většinu soukromého sektoru nedostupná.

Právě na potřeby široce dostupného prostředku pro elektronickou identifikaci, využitelného pro stát i soukromý sektor, reaguje projekt SONIA. S ohledem na přísnou regulaci v oblasti platebních služeb i na prostou potřebu řídit vlastní rizika a předcházet podvodům banky již nyní ověřují velmi důsledně totožnost svých klientů při každé elektronické transakci. Pro tyto účely mají banky vybudovány robustní systémy elektronické identifikace, zpravidla založené na dvoufaktorovém ověření totožnosti. Možnost přístupu do elektronického bankovnictví pomocí těchto vysoce důvěryhodných prostředků elektronické identifikace má přitom v České republice více než 5,5 milionu klientů. Po vzoru zahraničních příkladů se Česká bankovní asociace rozhodla tento obrovský potenciál robustní a důvěryhodné identity společným úsilím zpřístupnit veřejnému i soukromému sektoru. Smyslem projektu SONIA proto není konkurovat NIA, vybudované státem, ale zpřístupnit v ní prostředky elektronické identifikace klientů bank a vedle NIA vybudovat systém pro zpřístupnění bankovní identity soukromému sektoru – takový systém již úspěšně funguje například ve Švédsku.

Prakticky si lze představit umístění tohoto řešení na Portálu občana. Po spuštění projektu SONIA a napojení bank do

NIA zde vedle stávajících možností přibude také možnost přihlásit se pomocí bankovní identity spolu s možností zvolit si konkrétní zapojenou banku. Po zvolení konkrétní banky bude uživatel přepojen na její webové stránky, kde se přihlásí stejným způsobem, jako by se přihlašoval do internetového bankovnictví. Po přihlášení bude uživatel vyzván, aby odsouhlasil předání své identifikace a dalších požadovaných údajů Portálu občana a potvrdil jej stejně jako jinou transakci (např. pomocí autorizačního kódu zaslaného přes SMS nebo pomocí aplikace ve svém mobilním telefonu). Po tomto potvrzení bude uživatel přepojen zpět do Portálu občana, kde bude moci využít jeho služby.

Cesta k takovému cíli však není bez překážek – nezbytnou podmínkou je úprava současné legislativy. V cestě stojí v prvé řadě zákon o bankách, který bankám nedává jednoznačné dovolení, aby v rámci své bankovní licence poskytovaly služby elektronické identifikace. Tento stav je třeba napravit úpravou tohoto zákona. Změny jsou však nezbytné také v dalších předpisech.

Současná podoba NIA totiž neumožňuje bankám zapojení s ohledem na jejich povinnosti v oblasti řízení rizik. Jakkoli je NIA potenciálně přístupná jen omezenému okruhu subjektů ze soukromého sektoru, přesto poskytování identity takovým subjektům představuje pro banky riziko, které v NIA nelze efektivně řídit – využití bankovní identity přes NIA nelze podmiňovat uzavřením smlouvy, okruh transakcí nelze omezit. Z toho důvodu je před zapojením bank do NIA a zpřístupněním bankovní identity orgánům veřejné moci nezbytné legislativně ošetřit omezení spojená s využitím bankovní identity ostatními subjekty.

S projektem SONIA je také spojeno dlouho opomíjené téma přístupu bank do základních registrů, po kterém volá Finanční analytický úřad jako dozorový orgán v oblasti předcházení legalizace výnosů z trestné činnosti a financování terorismu. Legislativně je tento přístup ošetřen pro pojišťovny, banky však dosud zůstaly opomenuty. Cílem projektu je tuto situaci napravit a zajistit bankám bezpečný a technicky robustní přístup do základních registrů, aby mohly efektivněji plnit své úkoly v oblasti AML/CFT.

Tyto potřebné legislativní změny zpracovává pracovní tým České bankovní asociace spolu s externími poradci a předkládá je příslušným orgánům k projednání, aby podmínky pro vznik SONIA a zpřístupnění bankovní identity byly vytvořeny co nejdříve. Cíl všech členů projektového týmu je přitom stejný – zpřístupnit prostředky důvěryhodné elektronické identifikace vůči státu i soukromému sektoru 5 milionům Čechů. Na tomto místě je třeba zdůraznit, že bankovní identita je od počátku zamýšlena jako bezplatná pro klienty i pro stát. Její využití bude pro klienty dobrovolné, žádná jejich data nebudou sdílena bez jejich výslovného dovolení.

Projekt SONIA však nepřinese benefity jen občanům. Pro stát znamená bankovní identita potenciál 5 milionů uživatelů jeho elektronických služeb, který nepochybně zvýší smysluplnost a motivaci k veškerým investicím do e-governmentu. Spolu se zákonem o právu na digitální službu tak v dlouhodobém horizontu povede k výraznému rozšíření portfolia online služeb státu. Pro soukromý sektor pak projekt přinese způsob, jak důvěryhodně ověřovat totožnost zákazníků online tam, kde to dříve nebylo možné. Tím se otevře cesta pro elektronizaci řady transakcí, které jsme dosud zpravidla nuceni provádět osobně na pobočce příslušného subjektu – ať už jde o otevření účtu v jiné bance, sjednání pojištění či uzavření smlouvy na dodávku energií.

Všechny tyto přínosy projektu SONIA z něj činí skvělou ukázku, jaké benefity může přinášet spolupráce soukromého a veřejného sektoru. Pro jeho uskutečnění je však nezbytná úzká koordinace bank a dotčených státních orgánů nad podobou potřebné legislativy i následným technickým řešením napojení bank do NIA a základních registrů. Nezbývá tedy než doufat, že všem zúčastněným stranám se podaří co nejdříve najít shodu nad všemi potřebnými aspekty, aby se projekt mohl stát skutečností a „nést své ovoce“ v co nejkratší době.

JUDr. Josef Donát, LL.M.,
ROWAN LEGAL,
advokátní kancelář s.r.o.

PORTÁLY MÍSTNÍCH SAMOSPRÁV A POSKYTOVÁNÍ PERSONALIZOVANÝCH SLUŽEB KLIENTŮM VEŘEJNÉ SPRÁVY

Základním předpokladem úspěšné elektronizace státu je kromě digitalizované veřejné správy s efektivní výměnou dat a kvalitními on-line službami také zapojení místních samospráv. Spolupráce obcí s velkými centrálními projekty, jakými jsou Národní bod pro identifikaci a autentizaci (dále též „NIA") nebo Portál občana, je nepostradatelná pro celkový rozvoj elektronických služeb veřejné správy na místní i celostátní úrovni. V průběhu loňského a letošního roku připojily města Chotěboř, Pelhřimov nebo Říčany k NIA své samostatně spravované samoobslužné portály pro on-line komunikaci mezi klienty veřejné správy a městským úřadem. Tato města tak patří mezi první, která se aktivně zapojila do digitalizace a elektronizace veřejné správy na centrální úrovni. Portály obcí jsou v principu obecně navrženy tak, aby občanovi pasivně poskytly informace k životním situacím/událostem a následně ho aktivně dovedly k jejímu úplnému nebo částečnému on-line vyřešení. V neposlední řádě je zásadním prvkem portálů obcí také jejich propojení s centrálními informačními systémy, jako je NIA, Informační systém datových schránek (dále též „ISDS") nebo Portál veřejné správy (dále též „PVS"), včetně své transakční části, Portálu občana. Propojení centrálně spravovaného Portálu občana integrujícího sdílené služby e-governmentu s lokálními portály měst a obcí tak naplňuje cíl zajistit občanovi on-line komunikaci a možnost vyřízení životních událostí a služeb na úřadech s lokální i celostátní působností.

Co portály obcí jsou a jak se přihlásit

Již spuštěné portály uvedených obcí jsou architektonicky podobně navrženy jako Portál veřejné správy s transakční částí Portál občana, spravovaný centrálně Ministerstvem vnitra. Stejný koncept samoobslužného portálu spočívá v tom, že portál obce je ve valné většině případů rozdělen na dvě části, veřejnou a neveřejnou.

Veřejná část portálu obsahuje přehled životních situací/událostí, jako je například registrace vozidel, řidičské a občanské průkazy, stavební povolení, živnostenské podnikání, matrika nebo odpady. Každá životní situace/událost obsahuje kromě podrobného návodu, jak při jejím řešení postupovat, také kontakty na pracovníky úřadu a odkazy na konkrétní formulář.

Na druhé straně neveřejná část je občanovi přístupná až po jeho identifikaci a autentizaci s využitím elektronické identity. Zásadním rozdílem mezi Portálem občana spravovaným státem, který má celorepublikovou působnost, a portálem obce je zachování místní věcné příslušnosti při řešení agend týkajících se konkrétního města a v některých případech nutnosti dodatečné registrace pro úspěšnou identifikaci a autentizaci uživatele. U Portálu občana, spravovaného státem, není registrace pro úspěšné přihlášení nutná. Občan je při přihlášení pomocí elektronického občanského průkazu s aktivovaným čipem vydaným po 1. 7. 2018 úspěšně identifikován a autentizován pomocí NIA. Stejnou možnost nabízí přihlášení pomocí datové schránky zřízené na žádost. Naopak registrace je nutná pouze při založení a aktivaci uživatelského účtu NIA sloužícího též jako identitní prostředek.

Dalším důležitým atributem je přímá propojenost portálů obcí s Portálem občana. Oba typy portálů využívají společné výše uvedené nástroje ověření elektronické identity. Pokud má obec portál (obvykle dostupný z webových stránek obce), který svému občanovi umožňuje přihlásit se prostřednictvím služeb portálu NIA, může pak jako service provider (poskytovatel služeb) umístit svou „dlaždici" také na Portál občana. Na Portálu občana mají obce napojené na NIA svou vlastní dlaždici s odkazem umožňujícím přihlášenému uživateli přesměrování

na portál své obce. Po kliknutí na tuto dlaždici je uživatel přesměrován na portál své obce, kde bude moci přistoupit k jejím službám, aniž by se musel znovu přihlašovat. Zároveň portál zapojeného města může umožnit uživatelům přesměrování na Portál občana. Výhodou tohoto propojení pro občany je, že mají vše případně pod kontrolou v rámci jednoho profilu na Portálu občana, který je možné následně využít jako rozcestník služeb a „přenést" odsud svoji identitu na portály dalších subjektů.

Co portály obcí a měst umějí a nabízejí?

Hlavním cílem konceptu portálů obcí je zajistit elektronické vyřízení co největšího množství životních situací/událostí a poskytovat přehled o stavu zpracování požadavků či žádostí od klientů. Webová aplikace by navíc měla umožnit občanovi vést elektronickou komunikaci s úřadem, která zčásti nahradí osobní nebo poštovní kontakt. V praxi tak bude mít fyzická, podnikající fyzická nebo právnická osoba možnost např. učinit podání pomocí dostupných elektronických on-line formulářů i mimo úřední hodiny.

Ve vybraných případech mohou uživatelé po přihlášení do neveřejné části dále stáhnout potřebné formuláře, automaticky předvyplněné údaji, které úřad zná. Přihlášená fyzická osoba nebo podnikatelský subjekt může poté předvyplněný elektronický formulář vytisknout, vyplnit a on-line nebo poštou doručit na podatelnu města a sledovat stav jeho vyřízení spolu s historií všech formulářů či požadavků odeslaných dotyčnému úřadu. Uživatel má možnost také s využitím platební brány portálu hradit některé platby, jako jsou např. poplatky za psa či svoz odpadu. Portály obcí v neposlední řadě nabízejí také on-line rezervace návštěv úřadu nebo užitečnou funkcionalitu v podobě tzv. „hlídacího psa", který umožňuje nastavit e-mailovou notifikaci s upozorněním např. na končící platnost dokladu či blížící se termín úhrady poplatku.

Obec jako service provider vůči NIA

Jak již bylo zmíněno, Portál občana jako takový není k dispozici pouze občanům, ač tato věta zní možná jako protimluv. Využít portál a připojit se k němu prostřednictvím NIA jakožto service provider1 mohou mj. územní samosprávní celky, tedy obce a kraje. Pokud má obec vlastní portál s vlastním systémem přihlašování, ale nevyužívá služeb NIA, tedy není ze zákona service providerem, je možné se takovým poskytovatelem stát. Podrobný návod, včetně technických specifikací, je dostupný na webu https://www.eidentita.cz/Home/Ovm. Po splnění podmínek a registraci může obec využívat přihlašování prostřednictvím portálu NIA. Obec tak umožní svým uživatelům přihlásit se prostřednictvím služeb stejného kvalifikovaného poskytovatele identity jako v případě přihlašování do Portálu občana. Z tohoto důvodu se již nebude muset uživatel v Portálu občana při kliknutí na dlaždici obce či kraje znovu přihlašovat.

Jak se napojit?

Dle příručky a zákona č. 250/2017 Sb., o elektronické identifikaci, je NIA definována jako *„informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému"*. Na základě toho NIA „udržuje vazbu mezi základní elektronickou identitou fyzické osoby (záznam v registru obyvatel) a instancemi elektronické identity této osoby u poskytovatelů důvěryhodných služeb identifikace a autentizace".

Service provider je definován dle příručky a zákona č. 250/2017 Sb. jako *„kvalifikovaný poskytovatel on-line služeb nebo jiných činností, při nichž umožňuje prokázání totožnosti s využitím elektronické identifikace"*. Neboli *„právní subjekt poskytující služby fyzické osobě vzdáleným přístupem a využívající Národní identitní schéma pro identifikaci, autentizaci a autorizaci této osoby"*.

Dále je nutné na stránkách eidentita.cz provést registraci a konfiguraci service providera. K provedení registrace je potřeba přihlášení statutárního zástupce města s využitím přihlašovacích údajů do datové schránky města. Následná konfigurace služby, kterou chce obec jako service provider poskytovat (službou se v tomto případě míní konkrétní portál nebo aplikace, které jsou na NIA napojovány, nikoli jednotlivé služby dostupné na těchto portálech či v aplikacích), se řídí následujícími parametry:

- IČO subjektu;
- název kvalifikovaného poskytovatele (SeP);
- popis kvalifikovaného poskytovatele;
- URL adresa odkazující na úvodní webové stránky;
- URL adresa pro odeslání požadavků;
- adresa pro příjem vydaného tokenu (URL);
- URL adresa, na kterou bude uživatel přesměrován při odhlášení z portálu města;
- načtení certifikátu;
- adresa pro načtení veřejné části šifrovacího certifikátu z metadat (URL);
- logo kvalifikovaného poskytovatele.

Po úspěšné konfiguraci a technickém zajištění napojení má obec možnost si pro větší komfort uživatele nechat vytvořit dlaždici s odkazem na svůj portál v Portálu občana. Pro vytvoření dlaždice v současné době stačí kontaktovat Ministerstvo vnitra (na adrese portalobcana@mvcr.cz), které je správcem Portálu občana, a následně vyplnit krátký formulář zahrnující název dlaždice, krátký popis služby, logo a URL adresu na danou službu. Proces vytvoření dlaždice s následným testováním a zavedením do produkce již není technicky ani časově náročný.

Výhodou služeb NIA pro service providery je kromě využití společného nástroje pro ověření elektronické identity uživatele také možnost nastavení více úrovní ověření identity uživatele během přihlašování, odpovídající nařízení eIDAS (tzv. Level of Assurance, LoA). Tyto úrovně jsou tři: nízká, značná a vysoká. Poslední z těchto úrovní odpovídá přihlašování s využitím elektronického občanského průkazu. Rozhodne-li se obec stát service providerem, pak může zvolit pro přihlašování ke službám, které bude poskytovat občanům, všechny tyto úrovně, včetně té nejvyšší. NIA dále přináší poskytovatelům služeb následující výhody:

- vazba na základní registry, tedy referenční údaje o uživateli;
- další údaje poskytnuté uživatelem;
- správa souhlasů poskytnutí údajů uživatelem;
- sada údajů o uživateli pro ověření a předvyplnění ve formulářích.

Jaké jsou problémy a jejich případná řešení?

Proces napojení obcí na NIA a Portál občana se potýká stále s několika praktickými nedostatky. Prvním je nízké povědomí obcí o možnosti stát se poskytovatelem online služeb pomocí NIA. Tento stav podtrhují aktuální počty obcí, pohybující se v řádu jednotek, které tuto službu využívají a zároveň jsou napojeny na Portál občana. Řešení nepomáhá ani obsáhlá příručka pro poskytovatele služeb na webu eidentita.cz, která pro případné zájemce z řad menších obcí postrádající kvalitní IT zázemí může působit složitě až těžkopádně. Problémem dokumentu je, že neposkytuje zájemci stručné a srozumitelné informace o výhodách a možnostech při poskytování služeb pomocí NIA, ačkoli stručnější popis registrace a konfigurace nového poskytovatele služeb již existuje, a to v závěru uživatelské příručky. Další překážkou může být absence popisu s návodem pro napojení již registrovaného poskytovatele služby na Portál občana s následným vytvořením dlaždice, ačkoli tento proces

není vůbec po technické stránce náročný. Plánovaným řešením je vytvoření on-line aplikace v podobě modeleru dlaždic, který tento proces časově urychlí. Podobným problémem je i absence jednoduchého návodu pro obce se zájmem publikovat či čerpat data pomocí centrální sdílené služby eGSB.

Jedním z klíčových problémů je skutečnost, že některé portály vyžadují i po připojení k NIA registraci uživatelů na svých stránkách. Teprve poté existující účet spárují s profilem uživatele přihlášeným přes NIA, toto jde však proti principu „once only", který by měl klientovi veřejné správy po přihlášení zaručit volný pohyb mezi portály a webovými aplikacemi. Detailněji je napojení popsáno v příručce na stránkách Správy základních registrů zde: https://info.eidentita.cz/download/SeP_PriruckaKvalifikovanehoPoskytovatele.pdf.

Závěr

Přestože napojení portálů měst a obcí na NIA a Portál občana v současné době čelí problémům především informačního charakteru, nejedná se o problémy ryze technické, které by zásadně bránily snahám obcí stát se service providery a využívat na svých obecních portálech služeb NIA. Samosprávy nemusí mít úplnou představu o výhodách poskytování on-line služeb pomocí NIA a propojení s Portálem občana a zároveň si nejsou jisté, jak přesně a nejefektivněji postupovat při integraci svého obecního portálu. Nedostatečná informovanost obcí o možnostech a postupech, jak se stát poskytovateli on-line služeb pomocí NIA, je řešitelná například pomocí stručnějších, uživatelsky přívětivějších příruček, které jsou snadno dostupné a lépe zasazené do celkového kontextu.a Vyřešení těchto nedostatků s celkovým zlepšením propagace může rozšířit participaci obcí v digitalizaci státu s užíváním centrálních elektronických služeb státu.

Zdroje:

https://www.eidentita.cz/Resources/SeP_p%C5%99%C3%ADru%C4%8Dka_1v5_20181127.pdf
https://info.eidentita.cz/download/UzivatelskaPriruckaPortalNB.pdf
https://www.vera.cz/-/chcete-propojit-portal-mesta-s-portalem-mvcr-chotebor-vi-jak-na-to
https://info.ricany.cz/mesto/portal-obcana-c23786
https://www.egovernment.cz/soubor/magazin-egovernment-c-1-2019/
http://www.mestopelhrimov.cz/mesto-pelhrimov-obdrzelo-dotaci-na-rozvoj-informacnich-technologii/d-22755

Mgr. Tomáš Musil,
vrchní ministerský rada,
odbor eGovernmentu MVČR

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

CO JE NOVÉHO V REGISTRU PRÁV A POVINNOSTÍ

Nejvýznamnější novinky v registru práv a povinností (RPP) od roku 2017 jsou trojího typu – na jedné straně je to snaha prohloubit inventarizaci veřejné správy, na straně druhé podpořit rozvoj propojeného datového fondu, aby obíhala data a nikoli lidé, a konečně obsah RPP zpřístupnit dalším zájemcům.

Inventarizace veřejné správy

Z hlediska aktuálního rozvoje RPP je nejdůležitějším dokumentem zákon č. 251/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci. Novelou byla do RPP zavedena evidence pracovišť orgánů veřejné moci (OVM), evidence úkonů OVM vykonávaných na žádost subjektu (služeb), evidence míst poskytování služeb a v této souvislosti evidence převodu výkonu agendy na jiný subjekt.

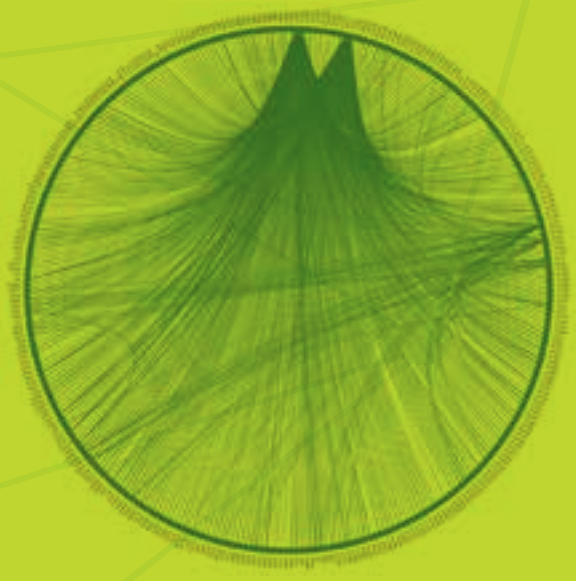
Sběr údajů o pracovištích má význam zejména tam, kde je úřad umístěn ve více budovách či kde se služby reálně poskytují v pobočkách daného OVM. K jednotlivým službám jsou postupně přiřazována místa poskytování a pro klienty veřejné správy je vytvářen zdroj informací, kde je možné službu řešit. Pokud OVM konkrétní úkon neposkytuje, jelikož jej cestou veřejnoprávní smlouvy převedl na jiný OVM, je tato informace do RPP také zaznamenána. Tímto způsobem vzniká otevřený katalog veřejných služeb, který bude chybějícím inventářem nabídky české veřejné správy.

Sběr údajů o službách veřejné správy považuje Ministerstvo vnitra (MV) za prioritní úkol a jeho splnění věnuje značné úsilí, zejména v oblasti metodické podpory a kontroly sbíraných dat. MV si velmi váží vysoké vstřícnosti ze strany jednotlivých ohlašovatelů agend a snahy o poskytnutí kvalitních údajů.

Po provedení legislativních změn bude v rámci registru práv a povinností sjednocena správa informačních systémů veřejné správy, která bude provázána s informacemi o agendách veřejné správy, orgánech veřejné moci a datovém fondu souvisejícím s výkonem agend.

V rámci tohoto konceptu byla provedena integrace informačního systému o informačních systémech veřejné správy (ISoISVS) do RPP. Údaje o informačních systémech tak jsou nyní vedeny jako jeden z vnitřních modulů registru práv a povinností. Veřejný přístup s možností základního vyhledávání je zajištěn na adrese: https://rpp-ais.egon.gov.cz/AISP/verejne.

Schéma mapující propojení jednotlivých agend v RPP



V rámci výše uvedené úpravy byl také automatizován přenos identifikátoru ISVS z RPP do registrační autority základních registrů (RAZR). Tímto opatřením byla významně snížena rizika z důvodu časové prodlevy a chyby způsobené ručním zadáváním údajů.

Podpora propojeného datového fondu

Dosud v realizaci je projekt, jehož ambicí je odstranit technické bariéry bránící výměně dat napříč veřejnou

správou. Nově tak v RPP bude evidována technická struktura údajů evidovaných v agendě a bude přidána funkcionalita pro podporu tvorby, verzování a publikace XML schémat těchto údajů.

Že jsou snahy akcelerovat rozvoj propojeného datového fondu nezbytné, dokládá schéma mapující propojení jednotlivých agend v RPP. Ústředním bodem (na schématu „na dvanácti hodinách") jsou dnes čtyři základní registry. K ostatním agendám se přistupuje v zásadě pouze sporadicky, jak je patrné z grafu níže.

Poskytování OpenDat

V souladu s nařízením vlády č. 425/2016 Sb., o seznamu informací zveřejňovaných jako otevřená data, byly v RPP připraveny denní exporty datových sad obsahující údaje o agendách, orgánech veřejné moci, soukromoprávních uživatelích údajů, výkonu agendy orgány veřejné moci, údajích předávaných mezi agendami, úkonech orgánů veřejné moci vykonávaných na žádost subjektu a další.

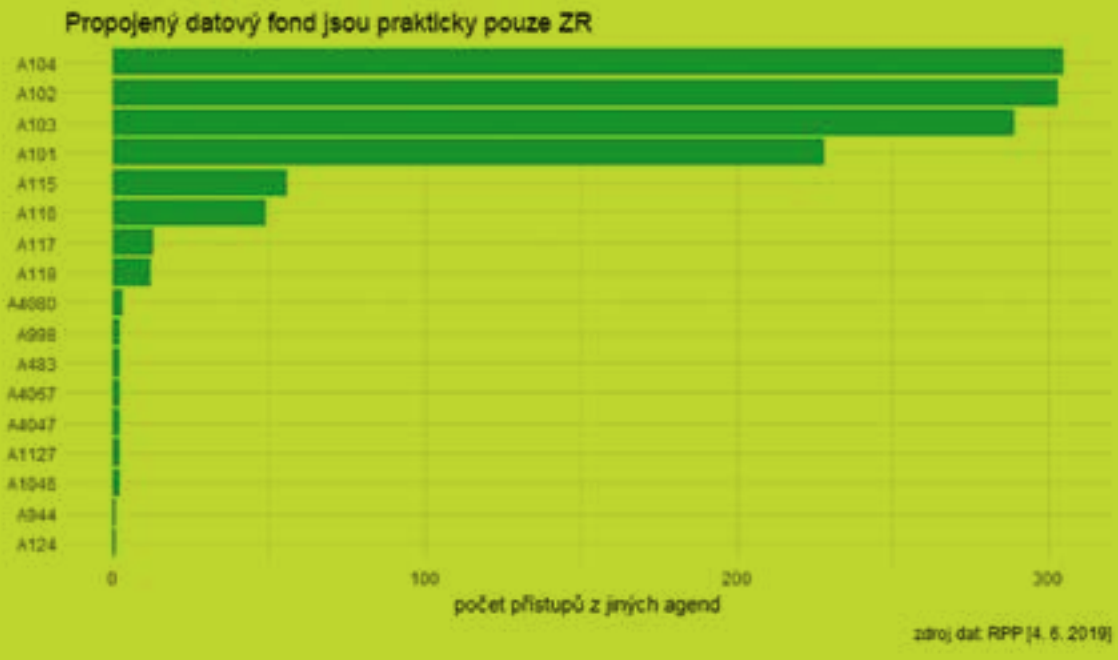
Od dubna 2019 bylo v Národním katalogu otevřených dat zpřístupněno 22 nových datových sad z RPP. Ve srovnání s ostatními ministerstvy se tak Ministerstvo vnitra posunulo na druhé místo za Ministerstvo pro místní rozvoj. Z celkových 67 datových sad v gesci Ministerstva vnitra připadá 22 sad na registr práv a povinností. Datové sady jsou publikovány v nejvyšším, pátém stupni otevřenosti (tzv. 5ti hvězdičková konvence) ve formátu JSON a JSON-LD.

OpenData RPP jsou přístupná na adrese https://data.gov.cz/datové-sady?klíčová%20slova=registr%20práv%20a%20povinností.

Mgr. Šimon Trusina,
oddělení projektů
eGovernmentu MVČR

Mgr. Tomáš Musil,
vrchní ministerský rada,
odbor eGovernmentu MVČR

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



eIDENTITA

V Malostranské besedě v Praze uspořádal na jaře magazín Egovernment setkání k tématu elektronické identity. Pod názvem eIDAS 2019 a pod záštitou PhDr. Ivana Bartoše, PhD., předsedy Výboru pro veřejnou správu a regionální rozvoj PSP ČR a Ondřeje Profanta, předsedy Podvýboru pro e-government PSP ČR, jsme se zaměřili na otázky plnění povinností eIDAS, zákona č. 297/2016 Sb. a 250/2017 Sb., na služby vytvářející důvěru, elektronickou identifikaci, národní certifikační autoritu, PSD2 a další související témata.

IDENTITA

Vstupní prezentaci zajistil Ing. Petr Tiller z OHA MV ČR. V souvislosti s legislativními otázkami připomenul, že podle §2 zákona č. 250/2017 Sb., o elektronické identifikaci, platí, že „vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace". Přechodné období tohoto nařízení je dvouleté, tedy do července 2020. Znamená to, že po tomto datu bude nutné přestat používat lokální přístupové údaje.

Jako určité povinné opakování Petr Tiller shrnul, že zatímco identita je pouze jedna a je definována záznamem v ROB, identifikačních prostředků může být neomezeně mnoho. Každý z nich má pak určitou úroveň ztotožnění (LoA), a to nízkou, střední nebo vysokou. Protože elektronická identita slouží především k možnosti využívat on-line služby ze strany státu, uvedl také seznam aktuálně připojených poskytovatelů on-line služeb:

1) Portál občana (obcan.portal.gov.cz);
2) Portál NIA (eIdentita.cz);
3) Portál eRecept (pacient.erecept.sukl.cz);
4) ePortál ČSSZ (eportal.cssz.cz);
5) Portál Finanční správy (adisepo.mfcr.cz);
6) ISDS (mojedatovaschranka.cz);
7) Portál živnostenského rejstříku JRF (www.rzp.cz/jrf/web/);
8) Portál Oborové zdravotní pojišťovny OZP (ozp.cz/vkol);
9) Portál města Pelhřimov (obcan.mupe.cz/obcan);
10) Portál města Říčany (obcan.ricany.cz/obcan);
11) Portál města Chotěboř (portal.chotebor.cz/portal/mujportal.html).

Předpoklad je, že tento seznam se bude neustále rozšiřovat, jak se budou připojovat poskytovatelé s nabídkou dalších služeb. Každé takové řešení je pak „zviditelněno" v rámci Portálu občana samostatnou „dlaždicí".

POSKYTOVATELÉ IDENTITNÍCH SLUŽEB

Ověřit totožnost uživatele je nyní, z pohledu státu, možné dvěma cestami:

A. elektronickým občanským průkazem – úroveň záruky LoA je vysoká. Tyto eOP si od data, kdy začaly být vydávány, tedy 1. 7. 2018, aktivovalo zhruba 135 tisíc držitelů. Identifikační aplikace je obsažena přímo v eOP. Je nutné ji aktivovat, a to buď při převzetí, nebo kdykoliv následně. Zdánlivě nepohodlná může být potřeba zadávání číselných kódů a instalace Middleware, který je v současné době již k dispozici pro všechny platformy, včetně mobilních. Nezbytností je také čtečka eOP, kterou je nutné zakoupit (cca 150 Kč);

B. UPS – User Name Pasword (jméno, heslo, SMS) – zde je úroveň záruky LoA pouze střední. Jedná se o určitou alternativu k eOP, kdy místo čtečky můžeme použít jakýkoliv mobil. Stačí pak založit uživatelský účet v NIA (www.eidentita.cz/ProfileRegistration). Potvrzení tohoto účtu je nutné a možné učinit na každém Czech POINTu, případně prostřednictvím datové schránky FO, nebo eOP. Ověřování je zde dvoufaktorové, tedy prostřednictvím kódu ze zaslané SMS.

NÁRODNÍ UZEL eIDAS

Národní uzel eIDAS zajišťuje propojení národních identitních prostorů napříč EU. Umožňuje tak čerpání on-line služeb států na území jiného státu. Náš Národní uzel eIDAS je v produkčním prostředí od září 2018 a zatím podporuje v ostrém provozu jediný tzv. notifikovaný stát, kterým je Německo. Nicméně v procesu notifikace jsou další země a naopak koncem ledna bylo v rámci Cooperation Network Meeting v Bruselu představeno naše eID schéma.

Od 1. 2. 2019 tak běží proces našeho hodnocení – Peer Review. S ohledem na jednotlivé lhůty je možné očekávat, že nejpozději v srpnu 2020 by mělo dojít k povinnému uznávání našich eOP pro přístup občanů ČR k on-line službám veřejného sektoru ostatních členských států.

NÁRODNÍ IDENTITNÍ AUTORITA

Na Petra Tillera navázal svým vystoupením ředitel SZR Ing. Michal Pešek. Jak uvedl, je to SZR, která zajišťuje provoz, informační a technickou podporu, zprostředkování elektronické identifikace mezi poskytovateli prostředků a poskytovateli on-line služeb, a to včetně napojení na další ohlášené systémy v rámci EU právě pomocí zmiňovaného mezinárodního uzlu.

Národní identitní bod je pak tím, kdo zajišťuje federaci identit mezi poskytovateli identity a poskytovateli služeb, řeší proces přihlášení v režimu Single Sign on (tedy pouze jednou), zajišťuje vazbu mezi daty základních registrů a poskytovatelem služeb a zajištění služby mezinárodní brány, tedy federaci identit v rámci zemí EU.

Michal Pešek informoval přítomné, že byl zahájen přechod na novou verzi CMS a rovněž v této souvislosti probíhá průběžná obnova HW jednotlivých součástí systému. Připravuje se také nová generace systému základních registrů (ZR 3.0), která bude aktuální od roku 2020 a byl vybudován nový nástroj na řízení přístupu k systému základních registrů – RAZR (Registrační autorita základních registrů – https://razr.egon.cms2.cz). Důvodem byla náhrada již zastaralého řešení RACS.

I díky uvedeným kroků platí, že denně se v rámci ZR realizuje 1 600 000 transakcí a jejich počet od 1. 7. 2012 dosáhl již 2,2 mld. V závěru vystoupení se Michal Pešek věnoval ještě tématu Národní certifikační autority. Jak řekl, NCA znamená, že SZR bude kvalifikovaným poskytovatelem a správcem jednotlivých částí NCA a služeb související infrastruktury. Vznikne tak systém certifikačních autorit pro vydávání:

- kvalifikovaných certifikátů pro elektronický podpis;
- kvalifikovaných certifikátů pro elektronické pečetě;
- kvalifikovaných certifikátů pro autentizaci internetových stránek;
- kvalifikovaných elektronických časových razítek.

Podle slov Michala Peška jde o strategický projekt, který bude určen omezenému počtu státních odběratelů.

Nařízení eIDAS a bezpečnost

Nařízení eIDAS klade u každého aspektu, jehož náležitosti upravuje, mimořádnou pozornost na bezpečnost. To se týká jak elektronické identifikace, požadavků na poskytovatele služeb vytvářejících důvěru, zejména ty kvalifikované, tak samozřejmě i na jednotlivé služby.

Je zřejmé, že zajištění bezpečnosti je základním prvkem vytváření důvěryhodnosti online prostředí, a to jak pro podnikatelské prostředí, tak pro komunikaci v rámci e-governmentu a konečně i pro komunikaci jednotlivců. Pokud uživatelé nebudou mít důvěru v bezpečnost elektronické komunikace, bude její využívání na nízké úrovni, resp. bude užívána pouze tam, kde to bude podle požadavků právních předpisů zcela nezbytné. Jistě však není bezpečnost jediným faktorem, který využívání online služeb ovlivňuje, za všechny další lze jmenovat uživatelskou přívětivost aplikací, počítačovou gramotnost, finanční nároky, které jsou s využitím služby spojené, a řadu dalších.

Nařízení eIDAS oproti směrnici Evropského parlamentu a Rady EU 1999/93/ES, kterou nahradilo, výrazným způsobem rozšířilo počet služeb, jejichž náležitosti upravuje. Cílem bylo vytvořit celý rámec pro bezpečné, důvěryhodné a snadno použitelné elektronické transakce.
Požadavky na bezpečnost můžeme najít v obou základních oblastech, které nařízení eIDAS upravuje, tj. elektronickou identifikaci a služby vytvářející důvěru, především tedy certifikační služby.

Elektronická identifikace, tj. možnost prokázání totožnosti v elektronickém prostředí, je v řadě států EU běžnou záležitostí. Problémem byla skutečnost, že každý stát volil vlastní způsob a nebylo myslitelné, aby způsob prokázání totožnosti v jednom státu byl použitelný i za jeho hranicemi. Proto si nařízení eIDAS dalo za cíl odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci, které se v členských státech používají k autentizaci. Důraz je kladen především na přístup k veřejným službám, tj. přeshraniční komunikaci s orgány veřejné moci. Rozšíření použití na služby soukromého sektoru je nejen možné, ale i vítané, zejména z hlediska posílení přístupu ke službám vnitřního trhu.

V České republice je prostředkem pro elektronickou identifikaci s vysokou úrovní záruky podle nařízení eIDAS elektronický občanský průkaz s čipem (eOP) vydávaný od 1. 7. 2018. Je zřejmé, že nezůstane jediným. První certifikační autorita, a.s., (I.CA) připravuje na uvedení do rutinního používání rovněž čipové karty Starcos. Jak eOP, tak i čipové karty Starcos jsou již dnes způsobilé pro vytváření kvalifikovaného elektronického podpisu, tj. jsou zároveň kvalifikovanými prostředky pro vytváření elektronických podpisů (QSigCD) a je v nich uložen soukromý klíč a k němu příslušný kvalifikovaný certifikát pro elektronický podpis.

Elektronická identifikace prostřednictvím eOP je určena především pro využívání online služeb veřejné správy. Čipová karta Starcos jako nástroj elektronické identifikace cílí především na bankovní sektor. Aktuálně je ve fázi testování napojení na NIA (Národní bod sloužící jako nástroj pro bezpečné a zaručené ověření totožnosti uživatele online služeb). Protože nároky na bezpečnost jsou i v tomto případě mimořádně vysoké, audit, který je podmínkou pro akreditaci udělovanou Ministerstvem vnitra, je prováděn ve dvou fázích – nejprve je sledován nástroj jako takový a následně bezpečnost komunikace, tj. činnost celého systému. Audit mohou provést pouze osoby, které k tomu ministerstvo určilo.

Pokud jde o přeshraniční používání nástrojů elektronické identifikace, je na rozhodnutí každého členského státu, zda oznámí své systémy elektronické identifikace Evropské komisi pro přeshraniční používání, nebo je ponechá pouze pro vnitrostátní použití.

Zatímco služby elektronické identifikace ve smyslu eIDAS jsou v České republice novinkou, některé služby vytvářející důvěru už za sebou mají téměř 10 let používání – pokud tuto dobu počítáme od vydání původní evropské směrnice. To se týká především vydávání kvalifikovaných certifikátů pro elektronický podpis, u nichž se mění pouze to, že stále více uživatelů dává přednost uložení soukromého klíče v kvalifikovaném prostředku pro vytváření elektronických podpisů, tj. v případě I.CA čipové karty Starcos, a to buď jako klasické čipové karty, nebo tokeny s vylamovacím čipem. Tyto prostředky zajišťují, že soukromý klíč se generuje v čipu a nelze jej exportovat. Přístup ke klíči je chráněn PINem a pochopitelně jsou marné občasné požadavky klientů, aby jim poskytovatel služby PIN uchoval a následně sdělil v případě, že ho zapomenou. Informativní seznam těchto prostředků zveřejňuje Evropská komise na URL https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

Uživatelé mají zpravidla jeden ze dvou důvodů, proč volí toto řešení – jedná se o veřejnoprávní podepisující, kteří jsou povinni takto postupovat při právním jednání, a pak ti, kteří používání těchto prostředků shledávají jako praktické – například lékaři, kteří potřebují vytvářet elektronický podpis na různých počítačích. K těmto dvěma důvodům lze přidat ještě jeden zásadní – pouze kvalifikovaný elektronický podpis, tj. vytvořený pomocí QSigCD, je podle nařízení eIDAS rovnocenný vlastnoručnímu podpisu a především musí být akceptován v rámci celé EU bez ohledu na to, ve kterém členském státu byl příslušný kvalifikovaný certifikát vydán.

Z hlediska bezpečnosti jsou pro poskytovatele mimořádně náročné na zajištění bezpečnosti další dvě služby – kvalifikovaná služba ověřování kvalifikovaných elektronických podpisů a pečetí (např. I.CA QVerify) a služba vytváření elektronických pečetí na dálku (např. I.CA RemoteSeal). Obě služby jsou ve velké míře využívány subjekty zpracovávajícími velké objemy dokumentů.

Po náročném vývoji obou služeb a před uvedením do rutinního provozu v letech 2017 a 2018 zajistila v obou případech I.CA provedení auditu, subjektem k tomu pověřeným, a následně požádala o posouzení Ministerstvo vnitra. Služba I.CA QVerify získala kvalifikovaný status, u služby I.CA Remote Seal ministerstvo neshledalo rozpor s relevantními právními předpisy. Z formálního hlediska nemůže tato služba získat status „kvalifikovaná“, neboť je z hlediska eIDAS považována za „doplňkovou“ službu ke kvalifikované službě vydávání kvalifikovaných certifikátů pro elektronické pečetě a eIDAS ji nedefinuje jako samostatnou kvalifikovanou službu.

O bezpečnosti v souvislosti s eIDAS by bylo možné uvést mnoho dalšího. Především je však nutné přivítat skutečnost, že autoři nařízení rozhodně nepodcenili bezpečnostní aspekty, ale na druhou stranu nezatížili povinné subjekty nadbytečnými požadavky.

Mgr. Dagmar Bosáková
První certifikační autorita, a.s.

ISSS 2019 – LETOS V POZITIVNÍM DUCHU

Dvaadvacátý ročník konference ISSS/V4DIS se letos odehrál v pozitivní atmosféře nebývalé shody prakticky na všem, co tuzemský e-government v následujících měsících čeká. Hlavních důvodů bylo několik – tím nejdůležitějším byl asi fakt, že současná politická reprezentace napříč celým spektrem se dokázala domluvit a podpořit návrh zákona o právu na digitální služby, který ovlivní většinu procesů ve veřejné správě. K celkové spokojenosti pak určitě přispěla i masivní prezentace MV ČR, jasné výstupy i otevřené diskuse. A konečně, renomé podtrhla reprezentativní účast špičkových politiků – eurokomisařky Věry Jourové, několika členů vlády v čele s premiérem Babišem, desítek poslanců a senátorů, šéfů státních organizací, hejtmanů, primátorů a stovek dalších zástupců veřejné správy. Během dvou dnů se registrovalo téměř 2200 hostů, v programu se odehrálo zhruba 200 prezentací a diskusí a ve výstavní části se představilo přes 100 firem a institucí. Letošní ročník konference oficiálně zaštítili premiér Andrej Babiš, 1. místopředseda vlády a ministr vnitra Jan Hamáček, ministryně pro místní rozvoj Klára Dostálová, vládní zmocněnec pro IT a digitalizaci Vladimír Dzurilla, hejtman Kraje Vysočina Jiří Běhounek a Asociace krajů ČR.

O dosahu a dobré pověsti akce svědčí i slova premiéra Andreje Babiše: „Tuto konferenci už ani nemusíme představovat, nosné téma ISSS patří do vládních priorit. Digitalizaci řešíme a chceme s ní pohnout a to je podle mě hlavní přínos akce. Nejen možnost slyšet, co se aktuálně na poli e-governmentu děje a šance jednoduše se potkat s odborníky, ale je to také prostor pro sdílení poznatků a výměnu zkušeností."

A právě digitalizace řady nejrůznější oblastí dění ve veřejné správě a elektronizace procesů, které by měly zjednodušit a zefektivnit jak řízení státu, tak komunikaci státní správy i samospráv s občany, patřily k hlavním tématům celého dvoudenního programu. Jeho nedílnou součástí byly jako obvykle i workshopy, panelové diskuse a různé doprovodné akce za účasti poslanců a senátorů Parlamentu ČR, členů AKČR a SMO ČR. Během

konference došlo i na vyhlášení výsledků oblíbených soutěží, jako jsou Český zavináč, Zlatý erb, JuniorErb nebo Biblioweb.

Hlavním organizátorem byla společnost Triada, na realizaci konference se tradičně podílel Kraj Vysočina, Český zavináč, časopis Obec a finance a společnost Ponca. Generálním partnerem byla jako v minulých letech Česká spořitelna, hlavními partnery pak společnosti ATOS, CISCO, ICZ, MICROSOFT a VITA software, partnery ALEF, ASSECO, AUTOCONT, AV MEDIA, CITRIX, DISK Systems, FORTINET, GORDIC, ORACLE a PALO ALTO Networks. Poděkování patří i partnerům odborných bloků (DELL EMC a SEFIRA) a spolupracujícím subjektům veřejné správy, mezi nimiž nechybělo Ministerstvo vnitra, Ministerstvo spravedlnosti, Ministerstvo pro místní rozvoj, Ministerstvo životního prostředí, Ministerstvo průmyslu a obchodu, Královéhradecký kraj, město Hradec Králové, fond Regina, ČTÚ, ČÚZK, ICT Unie, Sdružení tajemníků městských a obecních úřadů či analytický partner konference, společnost IDC CEMA.

Více informací, včetně audio a videozáznamů, televizního zpravodajství, prezentací a aktualit lze najít na www.isss.cz.

Prokop Konopa

V rámci slavnostního galavečera byly jako obvykle vyhlášeny výsledky soutěže Zlatý erb.

e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

MIKULOV • 3. - 4. 9. 2019

ODBORNÝ PARTNER

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

NAKIT
Národní agentura pro komunikační a informační technologie, s. p.

PLATINOVÝ PARTNER

CISCO

GENERÁLNÍ PARTNER

GORDIC

ZLATÝ PARTNER

A10

AUTOCONT

ČSOB

FORTINET

CERTIFICATION AUTHORITY

ICZ

Microsoft

... vše podstatné o eGovernmentu najdete v Mikulově.

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