27. 3. 2007

Kde už vás v Česku s plnicím perem vyhodí

Jak bude nešťastný majitel firmy prokazovat soudu, že elektronickou objednávku zboží za milion on sám skutečně "nepodepsal", ale kdosi zneužil jeho soukromý klíč příslušný k platnému kvalifikovanému certifikátu?

Skóre:	0.71
Název zdroje:	Hospodářské noviny
Datum vydání:	27.03.2007
Nadpis:	Kde už vás v Česku s plnicím perem vyhodí
Strana:	2
Mutace:	komerční příloha
Rubrika:	ICT Revue
Autor:	Ivana Šabatová
Oblast:	Celostátní deníky
Zpracováno:	27.03.2007 05:28
Identifikace:	DCHN20070327010000 cz
Klíčová slova:	Zákon (4x), právem (2x), správa (2x), Sb (2x), soudu, zákonem, novelou zákona, správou, zákona, správě, správy

NADTITULEK: EACCOUNT: ZARUČENÝ ELEKTRONICKÝ PODPIS POPRVÉ POVINNĚ

Jak bude nešťastný majitel firmy prokazovat soudu, že elektronickou objednávku zboží za milion on sám skutečně "nepodepsal", ale kdosi zneužil jeho soukromý klíč příslušný k platnému kvalifikovanému certifikátu?

V první den tohoto měsíce byla v rámci veřejné správy v tuzemsku poprvé spuštěna agenda, která neumožňuje podání jiným způsobem než prostřednictvím internetu s použitím zaručeného elektronického podpisu. Pro nové programovací období strukturálních fondů v ČR v letech 2007 až 2013 se administrátorem velké části Operačního programu Podnikání a inovace stala agentura CzechInvest. Jedná se převážně o přijímání a zpracování žádostí o dotace pro malé a střední podniky z celé České republiky mimo území Prahy. Operační program Podnikání a inovace ve značné míře navazuje na Operační program Průmysl a podnikání z minulého programovacího období z let 2004 až 2006, v jehož rámci v minulých třech letech požádalo o dotace kolem dvou tisíc subjektů. Podle nového programu budou o dotace opět moci žádat podnikatelé, nestátní neziskové organizace i výzkumné a vzdělávací instituce. V prvním pololetí letošního roku bude zahájeno přijímání žádostí do programů Inovace, Eko-energie, ICT v podnicích, ICT a strategické služby, Poradenství, Potenciál, Školicí střediska a Nemovitosti. Od letošního 1. března jsou již přijímány tzv. registrační žádosti o dotace v programech Marketing a Rozvoj. Agentura CzechInvest nově vyvinula a spustila internetový systém eAccount pro podávání a vyřizování žádostí o dotace v agenturou spravovaných oblastech tohoto operačního programu. Vůbec poprvé tak byla v tuzemsku spuštěna veřejnoprávní agenda, která od občanů a podnikatelů vyžaduje vlastnictví kvalifikovaného certifikátu vydaného a používaného v souladu se zákonem o elektronickém podpisu (zák. č. 227/2000 Sb. ve znění

pozdějších předpisů). Podání žádosti o dotaci bez tohoto certifikátu CzechInvest v současné době neumožňuje.

Není všechno zlato, co se v kyberprostoru třpytí

Jaké argumenty měl CzechInvest, respektive Ministerstvo průmyslu a obchodu, pro zavedení internetového systému podávání žádostí o dotace eAccount? Hlavním důvodem byl požadavek na snížení administrativní náročnosti přijímání žádostí a zrychlení celého procesu jejich hodnocení a schvalování ze strany agentury. Žadatelům pak agentura prostřednictvím zavedení systému eAccount nabízí zjednodušení a zefektivnění celého procesu přípravy a zpracování žádostí o dotace, úsporu nákladů a zkrácení lhůt od podání žádosti k rozhodnutí o přidělení či nepřidělení dotace. Proč však byla v rámci programu eAccount stanovena povinnost vlastnit kvalifikovaný certifikát a používat jej pro vytváření zaručeného elektronického podpisu při elektronickém podání žádosti o dotaci? A je naše společnost připravena na povinné a plošné používání zaručeného elektronického podpisu ve smyslu zákona o elektronickém podpisu? Rozšiřování počtu agend veřejné správy umožňující dálkovou elektronickou komunikaci občanů a podnikatelů je rozhodně vítanou inovací. Pro bezpečné a správné používání technologií elektronického podpisu je však nutné, aby i uživatelé této problematice dostatečně rozuměli a nevystavovali sebe a své podniky zbytečnému riziku. Veliký krok vpřed byl učiněn novelou zákona o elektronickém podpisu v roce 2004, jež z větší části vyřešila hlavní nedostatky původního znění (viz článek autorky v časopise eGovernment č. 4/2004, lze najít na www.sabi.cz), které především bránily širšímu praktickému využití zaručeného elektronického podpisu. Následně k prvnímu akreditovanému poskytovateli certifikačních služeb, k První certifikační autoritě, a. s. (I.CA), přibyli další dva, a to Česká pošta s akreditovanou certifikační autoritou PostSignum QCA a jen o pár měsíců později eIdentity. Zdálo by se, že bezkonkurenčně nízká cena 190 Kč za kvalifikovaný certifikát od PostSignum QCA prolomí s konečnou platností poslední bariéru v plošném rozšíření důvěryhodné elektronické komunikace nejen s veřejnou správou, ale i v obchodním a občanském styku. Proč se tak ale nestalo? A proč je využití zaručeného elektronického podpisu stále téměř výhradně záležitostí jen několika velkých projektů v rámci budování eGovernmentu a jinak se jedná pouze o pár desítek, maximálně stovek nadšenců, kteří si technologii chtěli spíše vyzkoušet, než by ji plánovali hned používat? Je to snad nedostatek agend, které je možné řešit elektronickou cestou?

Vtíravé paradoxy

Ale ani to už dnes neplatí. V současné době již veřejná správa občanům a podnikatelům poskytuje řadu možností elektronické komunikace s úřady a mnoho klíčových agend pro podnikatele umožňuje jednoduché a uživatelsky příjemné podání elektronickou cestou přes internet pomocí speciálně připravených formulářů. Povinnost zřídit ePodatelny na všech úřadech orgánů veřejné správy, založená už nařízením vlády č. 304/2001 Sb., postupně také došla svého naplnění. Dnes bychom asi těžko hledali úřad, který elektronickou podatelnu veřejnosti neposkytuje. Kupodivu jsme se dostali do situace, která je pro svět informačních technologií poněkud paradoxní. Technologie digitálního podpisu, na níž je celý systém vytváření a ověřování zaručených elektronických podpisů založen, je sice již technologií léty prověřenou a hojně rozšířenou, ale její bezpečné nasazení a využití zdaleka není jednoduchou záležitostí. Záleží totiž i na dalších komunikačních a počítačových technologiích, v jejichž prostředí probíhá vytváření a ověřování zaručeného elektronického podpisu. Prostředí dnešních informačních systémů je značně heterogenní a zejména v malých a středních firmách a v domácnostech je z hlediska informační bezpečnosti velice problematické. Jsme tedy v situaci, kdy společenská poptávka po důvěryhodné elektronické komunikaci existuje a vzrůstá, ale informační technologie poněkud pokulhávají v oblasti standardizace a bezpečnosti.

Jádro e-pudla

Klíčovým problémem je ochrana soukromého klíče (viz autorčin článek "Elektronický podpis - principy a využití" v týdeníku Ekonom č. 45/2005 - příloha Ochrana dat a informací. Lze též najít na www.sabi.cz). Podle zákona o elektronickém podpisu je držitel kvalifikovaného certifikátu povinen sám si zajistit bezpečnost dat používaných pro vytváření zaručeného elektronického podpisu. To znamená, že musí zajistit bezpečnost soukromého klíče, který je párovým klíčem veřejného klíče obsaženého v kvalifikovaném certifikátu, proti zcizení a zneužití. Požadavek zní jednoduše, jeho naplnění ale jednoduché není. Že není radno nechávat své soukromé klíče "pod rohožkou", již prokázala řada případů zcizení a zneužití přístupu k bankovním účtům a dalších informačněbezpečnostních incidentů. Navíc případy, o kterých se z médií dozvíme, tvoří jen špičku ledovce. Úspěšných útoků, o nichž se nedozvíme, je mnohem více. Odborníci na informační bezpečnost doporučují pro vytváření a uchování soukromého klíče použití speciálních hardwarových zařízení. To doporučují i pracovníci agentury CzechInvest v návodu k systému eAccount. V reálném životě však pořízení a používání tzv. hardwarových bezpečnostních předmětů vůbec není jednoduchou záležitostí. Kromě zakoupení hardwarového úložiště soukromého klíče, což může být čipová karta se čtečkou čipových karet nebo tzv. USB token odpovídající požadovanému standardu, musíme také nainstalovat správné ovladače a aplikace pro vytváření zaručeného elektronického podpisu a pro jeho ověřování.

Hrozí zneužití

Že je to jednoduché? Pro zkušeného správce informačních systémů, který je znalý problematiky, určitě ano. Ve větších organizacích se vytvářejí speciální postupy (směrnice, politiky) stanovující pravidla pro používání elektronických podpisů včetně zaručených elektronických podpisů.

Zavádějí se systémy definující hierarchii pravomocí a odpovědností. Jak se ale s touto výzvou vyrovnají tisíce majitelů a jednatelů malých a středních firem, ve kterých vybavenost a úroveň správy informačních systémů zdaleka neodpovídá ani základním požadavkům na zabezpečení proti útokům a zneužití? Má drobný podnikatel či jednatel malé nebo střední firmy šanci jednoduše a přitom odpovědně získat kvalifikovaný certifikát a zabezpečit svůj soukromý klíč? V naprosté většině případů bude muset požádat o pomoc s instalací svého administrátora informačního systému nebo externí firmu. V každém případě musí přijmout veškerá dostupná opatření k tomu, aby data, za která ručí v některých případech i celým svým majetkem, někdo nezneužil. Problémem asi není, pokud zaručený elektronický podpis používá pro jednání za firmu osoba, která má ze svého pracovního postavení omezené pravomoci. Například pokud se jedná o účetní, která pravidelně za firmu elektronicky zasílá finančnímu úřadu daňová přiznání k dani z přidané hodnoty s připojeným zaručeným elektronickým podpisem. Zneužití soukromého klíče je v takovém případě významně omezeno a v souladu s právem bude případný neoprávněný finanční, majetkový či obchodní závazek prohlášen za neplatný. Jinak tomu bude v případě, že dojde ke zneužití soukromého klíče příslušného ke kvalifikovanému certifikátu jednatele společnosti či osoby samostatně výdělečně činné. Dojde-li ke zneužití soukromého klíče příslušného k platnému kvalifikovanému certifikátu, jak bude nešťastný majitel firmy prokazovat soudu, že elektronická objednávka zboží za několik stovek tisíc či milionový úvěr on sám skutečně "nepodepsal"?

Nenechávejte klíče pod rohožkou

Zatím se bezpečnostních incidentů tohoto typu vyskytuje jen málo, ale víc než vysoká úroveň zabezpečení našich informačních systémů je důvodem spíše malé rozšíření využívání zaručeného elektronického podpisu. Určitým řešením by snad mohlo být omezení využití konkrétního kvalifikovaného certifikátu statutárních zástupců firem na ověřování pouze určitých typů transakcí, například pouze na elektronická podání vůči veřejné správě. Tím by bylo zneužití soukromého klíče pro neoprávněné vytvoření majetkového či finančního závazku znemožněno. Je totiž povinností

protistrany ověřit si rozsah oprávnění podepisující osoby, a to obdobně, jako je tomu u běžného písemného obchodního styku v papírové podobě. Zákon umožňuje takovou informaci v kvalifikovaném certifikátu uvádět, ale něco takového zavést není technologicky jednoduché. Záleží na akreditovaných poskytovatelích certifikačních služeb, zda upraví své postupy a uvádění těchto informací. V tuto chvíli ale není jasné, zda se taková úprava podaří a zda se nevyskytnou jiné komplikace. Jsou možná i kombinovaná řešení s použitím komerčních certifikátů, založených na kvalifikovaných certifikátech. Otázkou je zhodnocení zkušeností z provozu, provedení nutných bezpečnostních analýz a promítnutí těchto aspektů do dalšího rozvoje systému.

Agentura CzechInvest nyní už svůj systém eAccount spustila. Teprve praxe ukáže, zda v navržené podobě dokáže naplnit příslušná očekávání. Podnikatelům a dalším žadatelům o dotace z Operačního programu Podnikání a inovace lze popřát mnoho úspěšně podaných žádostí a šťastně dokončených dotovaných projektů a hlavně důrazně připomenout, aby své soukromé klíče v žádném případě nenechávali pod rohožkou. *

Autorka je konzultantka v oblasti informační bezpečnosti

Zpracovatel: Anopress IT a.s.