



**Využití BI
a datové analytiky
pro komunikaci se zákazníkem**

**CRM systémy
a potřeby projektově
orientovaného byznysu**

**Lead Management
CRM jako generátor
obchodních příležitostí**

**Data Governance
Jsou čistá data nutnost
nebo zbytečný luxus?**

**Spása jménem Big Data?
aneb Když běžné databázi dochází dech**

**Příloha
IT pro výrobní
podniky 2015
je součástí vydání
pro předplatitele**



Problémy veřejných zakázek v IT • Rozvoj eHealth v ČR vážne • Běžný život s eIDAS • Digitální transformace bankovníctví • Odhalování praní špinavých peněz • Kvalitní data pro úspěšné řízení firmy • Konec režimu bezpečného přístavu • Jak legálně spravovat a vyvážet osobní data?

Chráníte své informace?

Jaroslav Lubas

Každý z nás čím dál častěji přijímá, používá a předává dokumenty v elektronické formě. Předáváme si dokumenty různými cestami, stále častěji využíváme mobilní zařízení a internetové služby. Dokumenty jsou běžně přenášeny v nezabezpečené podobě, nejčastěji prostřednictvím e-mailu, a následně ukládány v informačních systémech, cloudových úložištích, personálních počítačích a mobilních zařízeních. V současnosti nestačí řešit jen otázku uchování a digitální kontinuity elektronické formy dokumentu ve vhodném DMS systému, chráněném v důvěryhodném prostředí firmy. Musíme řešit i způsob, jakým můžeme dokumenty předávat tak, abychom si byli jisti, že náš protějšek skutečně obdrží dokument nejen v nezměněné podobě, ale i s dostatečnou zárukou, že informace v něm obsažené nebudou na komunikační cestě ani koncovém zařízení zneužity.

Nic není úplně zadarmo

Dokázali byste si potvrdit následující tvrzení? „Vím zcela bezpečně, že dokumenty, které potřebuji chránit, nikdo jiný, kromě mne či jiné oprávněné osoby nečetl.“ Pokud dobře odhaduji, 95% z nás nebude schopno toto tvrzení s jistotou potvrdit. Často opravdu nevíme, jakou cestou jsou data předávána, často si vůbec neuvědomujeme, že „v cestě“ může stát někdo, kdo se o mé informace zajímá a my o něm nevíme. Díky snadnosti elektronické komunikace a naší pohodlnosti předáváme často data v nechráněné podobě. Nemůžeme se však následně divit, že jsme například neuspěli v konkurenčním boji o zajímavou zakázku.

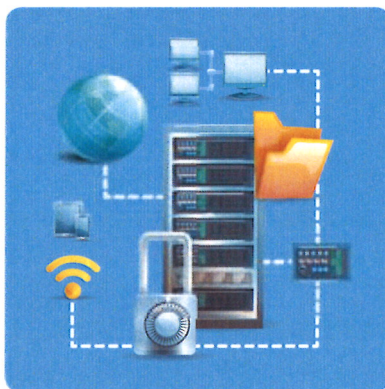
Často jsme k využívání této snadné komunikace motivováni tím, že je to pohodlné a „je to zadarmo“. Pravdou je, že při používání kvalitních, užitečných a masově používaných služeb pro komunikaci, spolupráci a sdílení na internetu o sobě nebo o své společnosti přímo či nevědomě prozrazujeme značné množství informací. Každá informace takto předaná však má svou cenu a svého kupce. Nic není úplně zadarmo.

Rovnoprávnost elektronických dokumentů

Nemůžeme však pominout fakt, že i státní správa přechází již (konečně) na elektronickou „verzi“ komunikace, která je námi vítána a která nás zbavuje nezbytnosti osobně navštěvovat úřady. Děje se tak i na základě tlaku EU. Jedním ze zajímavých a velmi důležitých dokumentů je nařízení evropského

parlamentu a rady (EU) č. 910/2014 ze dne 23. července 2014, nazývané též eIDAS.

V článku č. 46 – Právní účinky elektronických dokumentů – najdeme velmi důležitou větu: „Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu.“



Řešení bezpečné komunikace

Na jedné straně potřebujeme elektronicky komunikovat, na druhé straně to může být i nebezpečné. Existuje řešení? Ano, existuje. Známe je i poměrně dlouho. Je to využití kryptografie pro komunikaci mezi zúčastněnými stranami. Z počátku byla využívána zejména ve vojenské oblasti. První zmínky o jejím využití pochází z dob ještě před naším letopočtem, z dob Řecko-Perských válek. Mimochodem není neobvyklé, že rozvoj té, či oné technologie byl nastartován právě vojáky. Současný Internet, tak jak jej známe, vznikl

de facto na základě zadání ministerstva obrany USA, které potřebovalo vybudovat robustní síť bez centrálního uzlu, která by fungovala i v případě, kdy některé její části byly zničeny (ARPANET).

Co nám přináší využití kryptografie pro elektronické dokumenty? Přináší nám zejména zajištění důvěrnosti, kontrolu integrity a autenticity zprávy, důvěryhodné spojení s časem, nebo autorizaci přístupu. Kryptografie nám umožňuje zajistit důvěrnost dokumentů (informací) šifrováním. Dokumenty jsou „uzamčeny“ pomocí klíče a kryptografického algoritmu. V moderní kryptografii je veškeré tajemství soustředěno v klíči, kryptografický algoritmus je známý a prověřený. Klíče můžeme efektivněji chránit před neoprávněným přístupem, než data mnoha dokumentů libovolné délky.

Kryptografie sama nemůže zajistit neporušitelnost integrity, ale může zajistit její kontrolu. Pro kontrolu integrity je možné použít algoritmy symetrické či nesymetrické kryptografie, v kombinaci s hashovacími funkcemi. Pro současnou kontrolu integrity a autenticity dat nebo dokumentů se používají zejména elektronické podpisy a digitální certifikáty v rámci PKI nebo i jiné metody pro důvěryhodné svázání veřejných klíčů s identifikací subjektu, který provedl autentizaci dokumentu.

Moderní aplikace šifrují za vás

Dobře si uvědomuji, že se jedná o velmi specializovanou terminologii. Některé moderní aplikace, jak na mobilních platformách, tak na stolních, ale zejména přenosných počítačích, dokáží využít kryptografii bez znalosti odborného pozadí a zabezpečit důvěru při zpracování, ukládání i přenosu informací. ■

Ing. Jaroslav Lubas



Autor článku je vedoucím konzultantem společností OKsystem a.s.