8. 11. 2007

Pojem bez nejasností?

Ochrana data

Skóre: 0.72
Název zdroje: Hospodářské noviny
Datum vydání: 08.11.2007
Nadpis: Pojem bez nejasností?
Strana: 10
Mutace: komerční příloha
Rubrika: ICT revue
Autor: (rzh)
Náklad: 60258
Oblast: Celostátní deníky
Zpracováno: 08.11.2007 05:45
Identifikace: DCHN20071108010003 cz
Klíčová slova: Sb (3x), zákony (2x), zákonů, vězení, zákon, zákona, notářských, legislativu, notářská, zákonem, notářské

NADTITULEK: Ochrana data

Pro skórování je zapotřebí zpracovávat průchozí poštu. Ono to vypadá nevinně, ale existují případy, že poskytovatelé pracovali nejen pro adresáty, ale například i pro čínské bezpečnostní služby.

Snad na žádnou jinou oblast IT nejsou tak odlišné pohledy jako na oblast ochrany dat a informací. "Jde o několik úplně odlišných světů. Jen tak namátkou. Srovnejme svět člověka, který řeší ochranu dat na svém osobním PC, a organizací řešících problematiku ochrany dat ve smyslu zákona o ochraně utajovaných informací," říká Marta Vohnoutová, Security Consultant, Siemens IT Solutions and Services, a pokračuje: "K tomu navíc máme svět zákona 101/2000 Sb., o ochraně osobních údajů. Tento zákon je naprosto in, protože hledání sebemenších chyb v ochraně osobních údajů se stalo nejenom mediální posedlostí. Jen drobná námitka proti striktnímu využívání tohoto zákona je totiž považována za novodobé kacířství." Informace se chrání před:

ztrátou,

vyzrazením,

neoprávněnou modifikací,

neoprávněným zpracováním,

"zubem času".

Ztráta dat

Tady asi každý namítne, že jde o triviální záležitost, protože proti ztrátě dat se bráníme jejich zálohováním. Jenže ono se ukazuje, že to není úplně jednoduché. Zatímco domácí data snadno zálohujeme na DVD-R, v případě velkých diskových polí je to trochu problém. Ten spočívá v tom, že kapacita polí dnes často přesahuje kapacitu klasických zálohovacích médií, jako jsou magnetické pásky. Stále častějším řešením je tak on-line zálohování diskového pole na jiné diskové pole. Vypadá to jako dobrý nápad. Druhé pole umístíme do geograficky jiné lokality a problém ztráty dat se zdá být vyřešen.

Takové řešení je jistě skvělé z hlediska vysoké dostupnosti systému, ale z hlediska zálohování (tj. ochrany proti ztrátě dat) toho mnoho nepřináší. Proč? Protože nejčastější příčinou ztráty dat je jejich vymazání chybou programu nebo administrátora. Jedním příkazem může administrátor omylem zrušit celou databázi. A takové zrušení se pak on-line provede i v záložní lokalitě. A jak pak přijdou vhod klasické zálohy, pokud ovšem existují.

Ztráta dat ale může být i fyzická. Třeba při živelních pohromách. Například v Rakousku se poučili a uvědomili si, že ztráty notářských archivů při živelních pohromách se vyrovnají pohromám samotným. Upravili legislativu a všechny notářské listiny pořizují též elektronicky. Rakouská notářská komora pak s firmou Siemens založila společnost, která provozuje důvěryhodný archiv těchto elektronických listin. Stejnou cestou se pak vydali i v Maďarsku a dalších zemích. "Já si jen lámu hlavu, jaká pohroma musí přijít, aby se pohnuly ledy i u nás," podotýká Marta Vohnoutová ze Siemensu.

Vyzrazení dat

Slovní spojení "vyzrazení dat" si každý v prvním okamžiku spojí s armádou či bezpečností. "Ano, právě v této oblasti je ochrana proti vyzrazení dat rozhodně nejpropracovanější. Je specifikována zákonem o ochraně utajovaných informací a navazujícími zákony. Princip této ochrany spočívá v tom, že původce informací je tzv. klasifikuje stupněm utajení (vyhrazené, důvěrné, tajné nebo přísně tajné). S každou takto klasifikovanou informací se pak pracuje odpovídajícím způsobem. To znamená, že mohou s ní být seznámeny jen oprávněné osoby. Prostory i informační systémy s těmito daty musí být odpovídajícím způsobem chráněny, například fyzicky, kryptograficky atd.," připomíná Marta Vohnoutová ze Siemensu.

Pracujeme-li s takto klasifikovanými daty, pak klasifikace musí být někde vyznačena. Podle Vohnoutové dodávají významní výrobci operačních systémů kromě "komerčních" verzí svých systémů též "vojenskou" modifikaci. Ta spočívá v tom, že klasifikovaná data jsou doplněna o tzv. bezpečnostní návěští, v němž je vyznačen stupeň utajení. Klasifikovaná data tak mají jinou strukturu než neklasifikovaná, protože jejich struktura musí být rozšířena právě o toto bezpečnostní návěští.

Operační systémy pak musí zajistit, aby se klasifikovaná data mohla sejít jen s jinými obdobně klasifikovanými daty. Operační systém pak například pro dočasné soubory nemůže mít jeden společný adresář /tmp. Musí jich mít více - pro každou klasifikaci jeden. V malých českých poměrech se běžně takové systémy nepoužívají. Použije se komerční systém a bezpečnostní návěští se nalepí přímo na něj s tím, že celý systém je provozován výhradně pro data odpovídající klasifikace. Pokud se pohybujeme mimo zákon o ochraně utajovaných informací, pak si asi málokdo uvědomuje, že bychom informace také měli klasifikovat. Koneckonců doporučuje to i norma ČSN ISO/IEC 17799. Princip je stejný. Pouze se nehodnotí, jaká případná škoda by byla způsobena České republice, ale konkrétní firmě/organizaci. To znamená, že je dobré si udělat analýzu rizik, z níž by nám vyšlo, která data (informace) jsou pro nás aktivy. A tato aktiva interně klasifikovat.

"Pro klasifikace bychom ale měli použít jiné termíny než vyhrazené, důvěrné, tajné nebo přísně tajné. Důvod je velice prostý. Jako na potvoru totiž získáme nějakou státní zakázku, která pracuje s

klasifikovanými daty. Nepřála bych pak nikomu, aby vysvětloval NBÚ, že tato "důvěrná" data jsou opravdu "důvěrná" a jiná jen interně důvěrná nejsou "důvěrná"," varuje Marta Vohnoutová a pokračuje: "Naše interní klasifikace dat pak nevyžaduje, abychom přímo využívali např. bezpečnostní návěští. Většinou tuto interní klasifikaci postačí zobrazit na aplikační úrovni. Může se tak stát například následujícím hlášením na obrazovce: Zobrazené informace jsou určeny výhradně pro vnitřní potřeby naší firmy!" Každopádně provedení analýzy rizik a klasifikace interních dat donutí firmu, aby si uvědomila, která data jsou pro ni důležitá a která méně. Je to dobrý vstup i pro rozšíření archivačního a skartačního řádu o elektronické dokumenty.

Neoprávněná modifikace

Pro případ ochrany neoprávněné modifikace dat jsme zvyklí používat nepřepisovatelná média (např. DVD-R). Avšak i ta mají svá omezení. Data totiž z nich mohou být zkopírována, modifikována a pak opravená znovu zapsána na jiný kus téhož typu média. Jinou cestou "uzamčení" dat proti jejich modifikaci je podle Vohnoutové softwarové řešení. Asi nejjednodušším řešením je opatření dat časovým razítkem. Časové razítko totiž obsahuje aktuální čas a otisk z dat. A to vše je elektronicky podepsáno nezávislou třetí stranou - autoritou pro vydávání časových razítek. Problémem je jen skutečnost, že časová razítka mají omezenou dobu platnosti. Ale to ani nepřepisovatelná média nemají neomezenou životnost. Docela dobrý způsob je pak kombinace obou metod.

Neoprávněné zpracování

S tím, jak se množství uložených dat zvětšovalo, se ukázalo, že jednotlivá data jsou sice zajímavá, ale ve velkém objemu se mezi nimi dají často najít souvislosti. Pan Novák závidí sousedovi vilu. Ale ví jen o této vile. Kdyby ale měl neomezenou možnost vyhledávat v katastru nemovitostí, pak by zjistil, kolik nemovitostí mu patří v sousedním městě a na Moravě, kolik nemovitostí mají jeho příbuzní atd. Neoprávněné zpracování osobních údajů je asi ten nejlepší úlovek inspektora Úřadu na ochranu osobních údajů.

"Já se však se současným způsobem ochrany osobních dat neztotožňuji. Na jednu stranu se bojuje proti zveřejňování rodných čísel. Ta sice mohou být indexem do mnoha databází, ale zveřejněním mého rodného čísla se mnozí dozví onu tajnou informaci - že totiž jsem žena, protože datum narození se nepovažuje za osobní údaj hodný ochrany," diví se Marta Vohnoutová.

Na druhou stranu ochráncům osobních údajů je zcela jedno, že velcí světoví poskytovatelé e-mailových schránek se připravují na zpracování procházející pošty a její skórování. Důvodem je skutečnost, že tito poskytovatelé chtějí část nákladů hradit z cílené reklamy. A právě pro skórování potřebují zpracovávat průchozí poštu.

"Ono to vypadá nevinně, ale máme už případy, že právě tito poskytovatelé poskytli své služby nejenom adresátům, ale i například čínským bezpečnostním službám. Výsledkem pak bylo mnohaleté vězení, a to ještě dobře dopadlo," vysvětluje Marta Vohnoutová ze společnosti Siemens IT Solutions and Services.

Zub času

Zub času hlodá nejenom na starých památkách, ale i na elektronických dokumentech. A to podstatně rychleji. Příčiny jsou v podstatě dvě. První z nich je problém formátu elektronického dokumentu. To poznal asi každý, když si otevřel dokument pořízený nějakým starším programem. Tento problém je nepříjemný, ale pokud je datový formát znám, tak je alespoň teoreticky řešitelný.

Druhý problém je hlubší. Stále častěji totiž elektronické dokumenty opatřujeme elektronickými podpisy a časovými razítky. Tyto nástroje slouží jako indicie pravosti dokumentu a důkazy jeho

existence v konkrétním čase. Problém je v tom, že jak elektronický podpis, tak i časové razítko mají omezenou dobu platnosti. Takže stačí počkat, až jejich platnost vyprší, a dokument lze alespoň teoreticky zpochybnit.

V případě elektronického podpisu používáme právě časové razítko jako důkaz existence podpisu v čase. Sice v delším časovém horizontu, ale i to časové razítko nakonec vyprší. V praxi se pak postupuje ve dvou krocích:

1. V střednědobém horizontu se udržuje platnost elektronického podpisu pomocí časového razítkování tohoto podpisu (nikoliv dokumentu samotného).

2. V dlouhodobém horizontu se pak elektronické dokumenty "zakonzervovávají" zpravidla v celých dávkách. Využije se k tomu tzv. "důkazní záznam" (Evidence Record). O tom, jak by měl vypadat, se vedly deset let diskuse. Letos v srpnu konečně vyšel mezinárodní standard (RFC-4998 Evidence Record Syntax). A tak máme po problému, jak na to.

Nejdřív analýza

"Kdykoliv budeme uvažovat o ochraně dat v rámci firmy či organizace, pak než začneme mluvit o diskových polích a (ne)přepisovatelných médiích, měli bychom mít za sebou analýzu rizik spojených s našimi aktivy, tj. i daty. A na základě této analýzy si doplnit archivační a skartační řád o elektronické dokumenty," uzavírá Marta Vohnoutová ze společnosti Siemens IT Solutions and Services.

U nich by se podle ní mělo kromě skartační doby a skartačního znaku též uvádět:

zda obsahují dokumenty data sledovaná podle zvláštních zákonů (např. o ochraně osobních údajů);

zda je třeba migrovat jejich formát;

zda se musí osvěžovat jejich elektronické podpisy pomocí časových razítek a po jaké době;

zda bude jejich otisk vkládán do důkazního záznamu, případně s jakými jinými dokumenty bude do důkazního záznamu vkládán.

Teprve poté má smysl uvažovat o nových diskových polích, magnetopáskových silech apod.

Zpracovatel: Anopress IT a.s.