Bezpečnost outsourcingu především?

Může mít rekonstrukce bytového jádra souvislost s ochranou osobních údajů? **Možná Vás to překvapí, ale ano.**

Při čtení zpráv na portálu i-dnes.cz jsem nedávno narazil i na zprávičku, že „Policie prověřuje, zda z počítačů radnice neunikají data“. Jak je v té zprávě dále uvedeno (zde je anonymizovaná citace), „...kriminalisté se budou zabývat tím, zda se e-maily, rodná čísla či údaje o výplatách nemohou dostat z radničních počítačů do nepovolaných rukou. Město i firma, která jeho servery spravuje, to odmítají. Policista, který má o vyšetřování na radnici informace, potvrdil, že krajská hospodářská kriminálka chce prověřit, jaký má servisní společnost přístup k radničním datům. Kriminalisté zjišťují, zda má servisní firma přístup na počítačové servery městského úřadu, za jakým účelem a jaké jsou podmínky tohoto přístupu. Kriminalisté mají podezření, že by se firma mohla dostat v rámci takzvaného vzdáleného přístupu například až k e-mailové korespondenci, datům, se kterými radnice pracuje, či výplatám, zkrátka k osobním údajům, které jsou chráněné zákonem.“

Aniž bych jakkoliv předesílal skutečnou situaci na zmiňované radnici, vždy, když čtu zprávy tohoto charakteru, vybaví se mi nedávná situace, když v našem nájemném bytě majitel prováděl rekonstrukci bytového jádra. My si díky tomu museli na dobu celého měsíce zorganizovat čas tak, aby každý den byl někdo z rodiny doma a byl přítomen práci řemeslníků. Ne že bychom chtěli dělat stavební dozor, ale byli bychom ze zjevných důvodů velice neradi, kdyby se nám řemeslníci toulali po bytě v místech, kde to nepotřebují nebo kde by se nám to nelíbilo.

Možná se zdá divné, jakou souvislost má rekonstrukce bytového jádra s ochranou osobních údajů (a bezpečností informací obecně), ale na úrovni principů a postupů je situace v obou případech stejná. Tak, jako řemeslníci provádějí servisní údržbu bytu, servisní počítačová firma provádí servis počítačů. K oběma činnostem musíme zajistit, aby pracovníci měli odpovídající přístup. Navíc je úplně samozřejmé, že například v případě, kdy potřebujeme pravidelný roční servis plynového kotle, návštěvu servisního technika předem objednáme, domluvíme termín a jsme servisnímu zásahu přítomni. Zkušenosti v oblasti outsourcované správy a servisu výpočetní techniky a informačních systémů jsou však v převážné většině diametrálně odlišné. S jakými nedostatky se potkáváme nejčastěji?

> „Tak, jako řemeslníci provádějí servisní údržbu bytu, servisní počítačová firma provádí servis počítačů.“

Servisní společnost má plný a ničím a nikým nekontrolovaný přístup do informačního systému. Důvodů, proč k takovým situacím dochází, je hned několik. Nejčastěji je to zdůvodněním servisní organizace, že bez takového přístupu nemohou zaručit kvalitu poskytované služby. Jestliže totiž není v servisní smlouvě přesně a detailně specifikován její rozsah a způsob provádění, pro dodavatelskou organizaci je nejjednodušší požadovat (nebo v případě, že servisovanou techniku také dodávala, ponechat si) plný přístup ke všem zdrojům. Takový přístup je nejjednodušší, není potřebné na straně servisní organizace specifikovat a dodržovat žádná další omezení a pravidla, na straně klienta zase není potřebné nic kontrolovat. Důsledky jsou zjevné – nikdo nemá přehled o tom, kdo má k jakým informacím přístup a co s nimi dělá.

Servisní společnost má plný, ale monitorovaný přístup do informačního systému. Situace je sice na první pohled lepší než ta předchozí, zdá se, že je kontrola nad tím, co servisní organizace provádí, avšak plný přístup k prostředkům ICT umožňuje servisní společnosti i přístup k monitorovacím záznamům a tím se monitoring jejich vlastní činnosti stává nefunkčním, protože servisní společnost má možnost tyto záznamy modifikovat.

Servisní společnost má specifikovaný, monitorovaný a omezený přístup do informačního systému. Tato situace je pravděpodobně optimální pro tento typ služby, avšak aby tomu tak skutečně bylo, je nutné, aby:

- existovala přesná specifikace rozsahu oprávnění, které má servisní společnost k dispozici; k tomu musí existovat přesná evidence informačního systému, aplikací, datových úložišť, databází, souborových systémů a síťových prvků tak, aby při přidělování specifických přístupů byl přesný přehled o přidělených oprávněních a aby přidělené přístupy plně vyhovovaly požadovaným servisním činnostem;
- monitorovací systém přesně sledoval veškeré činnosti, které jsou servisní organizací prováděny, a aby nebylo možné do těchto záznamů zasahovat jak servisní organizací, tak interními pracovníky;
- monitorovací informace byly vyhodnocovány v (téměř) reálném čase.

Právě okamžité vyhodnocování monitorovacích informací (tzv. logů) je jedinou z důležitých podmínek zajištění dobré kontroly činnosti servisní organizace. Podle vyhodnocení monitorovacích záznamů lze přesně určit rozsah a četnost servisních zásahů a tím i objem prací, které byly provedeny a jsou fakturovány. To však postačí vyhodnocovat jednou měsíčně, avšak vyhodnocování monitorovacích informací v (téměř) reálném čase je důležité z pohledu bezpečnosti informací. Jestliže totiž dochází k nelegálním aktivitám, je důležité to vědět nejlépe okamžitě. Mnohdy se po měsíci ani nedá přesně určit, k čemu a v jakém rozsahu došlo. Můžeme sice mít informaci o tom, že před měsícem někdo něco nelegálního prováděl, avšak jestliže je informační systém intenzivně měsíc využíván, další stopy po takové nelegální činnosti mohou být dávno ztraceny. Je to jako s těmi řemeslníky při rekonstrukci bytového jádra; bez on-line dozoru bychom sice věděli, že nám někdo z nich něco v bytě provedl, ale to už je pozdě.

> „Na hlídání bezpečnosti informací je potřebné mít vhodné nástroje a kvalifikované lidi, takže konec konců je to otázka dostatku prostředků a kalkulace, zda tuto specifickou činnost vykonávat vlastními silami, nebo si ji nechat také outsourcovat.“

Na rozdíl od řemeslníků je zajištění bezpečnosti informací poněkud složitější, nejedná se o fyzické hlídání fyzických osob ve fyzickém prostoru. Na hlídání bezpečnosti informací je potřebné mít vhodné nástroje a kvalifikované lidi, takže konec konců je to otázka dostatku prostředků a kalkulace, zda tuto specifickou činnost vykonávat vlastními silami, nebo si ji nechat také outsourcovat. V každém případě však jiným subjektem než organizací, která nám outsourcuje servis a údržbu informačních technologií. Není to nic neobvyklého, bezpečnost objektu nám také obvykle zajišťuje nějaká agentura, tak proč by bezpečnost informací nemohla zajišťovat také třetí strana. Avšak i takovýto typ outsourcingu je potřebné monitorovat, kontrolovat. Konečnou odpovědnost za bezpečnost informací totiž nelze delegovat nebo outsourcovat, proto konečné kontrolní mechanizmy musí vždy zůstat v rukou organizace, vlastníka informací.

Ing. Marián Svetlík

Od ukončení vysokoškolského studia v roce 1983 pracoval v různých oblastech IT/IS, byl vedoucím specializované laboratoře počítačových expertíz Kriminalistického ústavu Praha, lektorem Interpolu a zástupcem ČR v CyberCrime výboru Rady Evropy. Od roku 2000 je vedoucím konzultantem a vedoucím znaleckého ústavu digitálních forenzních analýz společnosti Risk Analysis Consultants, s.r.o., prezidentem celosvětové iniciativy Digital Forensic Forum a předsedou výkonného výboru Akademie forenzních věd.