29. 12. 2014

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

7 nejčastějších problémů v bezpečnosti kanceláře

Zásady bezpečného chování v informačních systémech (nejen na internetu) by měly patřit mezi elementární znalosti každého uživatele, ať je již domácím uživatelem, nebo právníkem či notářem. Právě právníci a notáři se však od běžných uživatelů liší zejména v tom, že pracují s velmi hodnotnými a často neveřejnými informacemi. Vnímání toho, co je z pohledu bezpečnosti normální v „běžném" světě je ve světě elektronickém ve velkém porušováno. Je například zcela nemyslitelné, aby návrh zásadní smlouvy obsahující údaje o majetkových poměrech stran byl odeslán poštou v nezalepené obálce nebo formou korespondenčního lístku. Nebo archiv celé advokátní kanceláře byl umístěn v jiné budově s tím, že majitel kanceláře ani netuší, kdo všechno má k archivu přístup a nemá šanci ovlivnit, kdo si které listiny prohlíží. Přitom přesně tyto případy jsou každodenní praxí na internetu.

Je nemožné na složité problémy navrhovat jednoduchá a všestranná řešení. Stejně tak je nemožné v rozsahu tohoto článku nabídnout jednoduchý a přitom komplexní návod, jak se v prostředí internetu chovat bezpečně. Pokusíme se však ne odborným IT jazykem upozornit na několik problémů, o kterých je dobré vědět.

1. **„Největší hrozbou jsme si sami sobě."** – tím, že neznáme alespoň základní pravidla fungování internetu a základy bezpečnostního chování, zvyšujeme riziko toho, že se staneme obětí bezpečnostního incidentu. Ty největší incidenty byly většinou způsobeny souhrou více okolností, zásadním faktorem byla ale vždy – byť nevědomá, přesto – aktivní spolupráce uživatele (klik na odkaz v e-mailu, snadno prolomitelné heslo, instalace podezřelého software, absence bezpečnostních záplat software, nebo odeslání důvěrných materiálů otevřeným e-mailem…). Uvědomme si tuto skutečnost a věnujme alespoň několik minut týdně (dobře, měsíčně) vzděláváním se a vytvářením si bezpečnostních návyků.

2. **„Co jednou na internet umístíme, nikdy se toho nezbavíme."** – v tomto internet nezná žádné limity. Jakmile e-mail, soubor, fotka opustí náš počítač a jsou odeslány, nebo umístěny na sociální síť, neexistuje spolehlivý způsob, jak je z internetu vymazat. Přitom nerozvážně odeslaná informace nás může „doběhnout" i za několik let. Na druhou stranu, sami o sobě svobodně rozhodujeme, které informace internetu poskytneme. Je dobré si také uvědomit, že spolu s e-mailem, souborem, které na internet umisťujeme, vznikají i takzvané elektronické stopy.

3. **„E-mailová komunikace je korespondenční lístek."** – bez e-mailové komunikace si nelze v dnešní době představit práci s klienty a komunikaci vůbec. Je rychlá, efektivní a jejím prostřednictvím lze velmi snadno přenášet různé druhy souborů. Ale pozor, technologie přenosu elektronické pošty ve svém původním návrhu a tak, jak je dnes většinou používána, nebyla navržena pro bezpečný přenos informací. Konkrétní e-mail lze velmi snadno podvrhnout, zkopírovat apod. Zvláště doporučujeme si přečíst podmínky používání služby na veřejných free webových službách. Nezbytným řešením je e-mailovou komunikaci s klienty šifrovat, a to ještě ne jakýmkoli způsobem. U šifrování je podstatné, kdo vlastní šifrovací klíče a kdo k nim má přístup. Ty musí být jen a pouze pod kontrolou daného uživatele.

4. **Nezabezpečená data na disku počítače** – bezpečnostní otázka, zda má smysl šifrovat data na počítači, má být postavena přesně naopak – existuje nějaký důvod, proč nešifrovat? A to nejen pro případ krádeže počítače (nikdy se mi to nestalo, proč být paranoidní…), ale třeba i pro případ technické závady na datovém nosiči, kdy servis provede výměnu vadného disku za nový. Co se děje následně s tím vadným? Víte, že se data dají s vysokou úspěšností získat i z vadného datového nosiče? Dnes je na trhu několik velmi efektivním technologií pro šifrování dat, vždy se ale stejně jako u e-mailu ptejte, kdo má přístup k šifrovacím klíčům? Je to jen uživatel? Kde jsou klíče uloženy?

5. **Otevírání přístupu k datům třetím stranám** – zde nejde jen o ukládání dat na cloud v otevřené či pseudošifrované podobě (opět – ptejte se – kdo vše má k dispozici klíč…), ale i ošetření situací, kdy dodavatel informačního systému má v rámci zajištění servisní podpory k dispozici vzdálený přístup do informačního systému. Je nezbytně nutné vědět, kdo z jeho zaměstnanců má přístup, jak přistupuje, jak se autentizuje a jaká má v systému oprávnění. Většinu systémů lze navíc i nastavit tak, že o těchto přístupech vznikají automaticky záznamy – auditní stopy. Archivujte si je.

6. **Podcenění bezpečnostních aspektů správy sítě** - u menších subjektů (advokátních nebo notářských kanceláří), pro které není výhodné zaměstnávat vlastního IT specialistu, je obvyklé, že starost o své počítače a informační systém svěřují externím správcům sítě. Mimo již výše uvedené zásady je nutné mít k dispozici platnou základní bezpečnostní dokumentaci k informačnímu systému. Zejména jde o administrátorská hesla (ověřeně platná) uložená v trezoru, kopie základních nastavení systémů. Umíte si představit situaci, kdy váš „ajťák“ odjede na dvoutýdenní dovolenou do Alp bez dostupnosti mobilního signálu a váš informační systém se zhroutí? V tomto případě je znalost administrátorských hesel doslova k nezaplacení.

7. **Nepůjčujte služební počítače rodinným příslušníkům** - tato rada se možná zdá samozřejmá nebo naopak příliš přísná, ale její dodržování už tak běžné není. Nejen, že uživatel, ale i sám počítač v internetu za sebou zanechává elektronickou stopu (nikdy se jí nezbavíte), ale děti jsou navíc velmi vynalézavé v instalaci a užívání software, který lze jednoduše tzv. stáhnout. Přitom však absolutně nelze mít pod kontrolou, co tak nevinně vypadající hra skrytě v počítači provádí a k jakým datům přistupuje a případně exportuje třetím stranám.

Jakákoli bezpečnost přináší snížení komfortu užívání a požadavky na vyšší uživatelskou kázeň. Na internetu je k dispozici mnoho velmi názorných a dobrých doporučení, jak se chovat bezpečně. Jako poslední přijměte toto doporučení – zachovejte zdravý rozum, ale buďte si vědomi toho, že pracujete s informacemi, které mohou mít vysokou hodnotu.

Ing. Vladimír Lazecký,
konzultant pro bezpečnost aplikace pro správu spisu SingleCase,
předseda představenstva VIAVIS a pedagog VŠ CEVRO Institut

Další články:

- Vybrané otázky poskytování zdravotních služeb na dálku
- DEAL MONITOR
- „Za každou kauzou je živý příběh“
- Ombudsman na Maltě – základní parametry a role. A v čem bychom se mohli poučit i my v

Česku?
- DEAL MONITOR
- DEAL MONITOR
- Rozhovor s JUDr. Veronikou Janoušek Rudolfovou, samostatnou advokátkou specializující se na sportovní právo
- DEAL MONITOR
- DEAL MONITOR
- DEAL MONITOR
- Fotbaloví agenti vs. FIFA ve světle stanoviska generálního advokáta Soudního dvora Evropské unie