

## **KNIHOVNÍCI A POČÍTAČOVÁ BEZPEČNOST**

Pavla Kovářová

***Abstrakt:** S připojením knihoven k Internetu a službou poskytování přístupu k Internetu veřejnosti se před knihovnami a knihovníky otevřela otázka počítačové bezpečnosti. Bohužel tato problematika není obecně příliš známá, což způsobuje velké nebezpečí. Přestože v knihovně může být správce počítačů odpovědný i za jejich zabezpečení, knihovník se může dostat do situace, kdy bude muset otázku bezpečnosti řešit sám (nepřítomnost správce, ale i uklidnění rozčileného rodiče, který tvrdí, že se jeho dítě v knihovně dívalo na porno stránky). Proto jsem přesvědčena, že knihovníci by měli disponovat alespoň obecnou orientací v této oblasti a měli by znát hrozby, se kterými se v knihovně mohou setkat.*

Jak dobře víme, veřejné knihovny poskytují **možnost přístupu** k počítači a Internetu **všem bez rozdílu**. To je nepochybně velmi užitečné, přináší to sebou ale i jistá rizika, z nichž některá bych zde chtěla představit.

V první řadě je nutné položit otázku proč by vlastně měli knihovníci měli něco vědět o počítačové bezpečnosti, zda to bude mít pro jejich práci nějaký přínos, když snad každá knihovna má nějak zajištěného **správce počítačů**, resp. počítače. V praxi se můžeme setkat se dvěma situacemi – větší knihovny mají **vlastního správce**, nebo jich mají dokonce víc, ale menší knihovny, které mj. rozpočtem spadají pod obecní nebo městský úřad, se často musí spokojit se správcem počítačů tohoto **úřadu**, což sebou samozřejmě nese problém, že tento správce jim nemůže pomoci hned, když to potřebují, a někdy knihovna musí čekat i několik týdnů, protože nejsou považovány správcem nebo úřadem za prioritní. I v případě, že má knihovna vlastního správce, může se někdy setkat s tím, že je nedostupný – např. díky nemoci, dovolené apod., další příklady Vás jistě napadnou. Tak je nepochybné, že i knihovníci se někdy dostanou do situace, kdy by měli řešit problém s počítači a proto by se měli seznámit alespoň se základy počítačové bezpečnosti.

Ráda bych již přešla k problémům, se kterými se knihovník může setkat, věnovat se chci těmto tématům:

- nevhodné webové stránky
- škodlivý software, zejména „špehovací“

**Studentská konference InfoKon**  
**Filosofická fakulta Masarykovy univerzity**  
**Brno, 24. 11. 2007**

➤ sociální inženýrství

Začneme tedy hned problémem přístupu dětí **k nevhodným webovým stránkám**, zejména pornografii. Knihovny mohou poskytnout dětem prostředek právě k tomuto přístupu. Knihovny tento problém mohou řešit různě – pro knihovníky je asi nejjednodušší metodou instalace programu typu **rodičovské ochrana**, kde jsou nejdříve definovány určité pojmy, a pokud se nachází na zadané webové stránce, není tato stránka zobrazena. Zde se ale většinou znovu objevuje problém financí. Proto se knihovny mohou dostat do situace, kdy snad jedinou možností je, že **knihovník** při procházení kolem počítačů **sleduje**, které stránky si uživatelé prohlíží. Knihovník se v každém případě může dostat do situace, kdy musí vysvětlit, jak je možné, že si nezletilé dítě v knihovně prohlíželo pornografické nebo jinak obsahově nevhodné stránky. Pak by měl být alespoň minimálně znalý v této problematice a měl by přesně vědět, jak knihovní strategie tuto hrozbu řeší nebo chce řešit.

Dále bych se chtěla zabývat škodlivým softwarem, se kterým se jistě setkal každý uživatel počítače s přístupem na Internet. Škodlivý software, neboli **malware**, zahrnuje mnoho různých kategorií – viry, červi, trojské koně, spyware, dialer a mnoho dalších. Vysvětlování těchto pojmů by zabralo několik hodin, proto se jim zde nebudu věnovat, v případě zájmu odkazuji na množství publikací, které se malwaru věnují. Abychom se vrátily ke knihovnám, samozřejmě i ty se musí potýkat se škodlivým softwarem. Největší nebezpečí představují **špehovací programy**, jejich cílem je získat uživatelská jména a hesla. Knihovny jsou totiž velmi atraktivním cílem – vystřídá se zde mnoho uživatelů a často i těch, kteří se nutně rychle potřebují podívat na svoje účty elektronického bankovníctví. Jak je patrné, v současnosti je Internet spojen se stále větším množstvím peněz – ať myslíme zmíněné internetové bankovníctví, nebo nákupy přes internet, platby kreditními kartami apod. Proto by se knihovny a knihovníci měli mít před takovými problémy na pozoru. Vzhledem k možnostem se ale často knihovníci musí spokojit s antivirovými **programy** a to pouze těmi, na které opět stačí finanční prostředky. Dále je možné využít antispysware, z nichž některé jsou zdarma, proto by alespoň nějaký měl být nainstalován, důležité je i pravidelně záplatovat operační systém a programy. Popsaný problém i jeho konkrétní řešení by opět knihovník měl důvěrně znát, aby uživateli mohl vysvětlit, jak je počítač ochráněn, případně se mohl hájit, pokud by si uživatel myslel, že právě v knihovně došlo k úniku jeho uživatelského hesla.

Posední oblastí, kterou bych zde chtěla představit, je **sociální inženýrství**, které není pouze počítačovým problémem, můžeme se s ním setkat kdekoliv. Jedná se v podstatě o

**Studentská konference InfoKon**  
**Filosofická fakulta Masarykovy univerzity**  
**Brno, 24. 11. 2007**

„obelhání“ někoho pro získání něčeho, k čemu by jinak tento člověk nemohl přijít – ať už jde o získání informace, přístup nebo cokoli jiného. V knihovně takto může být např. získán přístup k ovládnutí zapojených počítačů. Abych uvedla pro lepší vysvětlení **konkrétní případ** – představme si, že knihovníkovi někdo zavolá, představí se jako správce počítačů v knihovně (získat jeho jméno není tak těžké) a žádat knihovníkovo heslo pro přístup k počítačům, z důvodu kontroly bezpečnosti. Pokud knihovník nikdy neslyšel o sociálním inženýrství, může prozradit opravdu důležité a tajné informace. Zde by navíc mohlo vzniknout podezření, že sám knihovník je útočníkem, nebo jeho spolupracovníkem. Sociotechnické útoky jsou obtížně rozeznatelné, nejlepší **ochranou** je využití zdravého rozumu a především ověřování všeho, co by mohlo být nebezpečné. Pro bližší informace odkazuji na knihu Umění klamu Kevina Mitnicka, který je zřejmě nejznámějším sociotechnikem, existuje i mnoho časopiseckých článků, které stručně tento problém popisují.

Ve svém příspěvku jsem popsala nebezpečí, která podle mého názoru představují nebo mohou představovat největší hrozby pro knihovny a knihovníky. Naznačila jsem také některé důvody, proč by se knihovníci v této oblasti měli orientovat alespoň na základní úrovni. V budoucnosti bude jistě nutné, aby toto problematiku knihovníci nejen znali, ale aby byli schopni také poradit svým uživatelům, proto se domnívám, že by bylo dobré zahrnout orientaci v počítačové bezpečnosti i do vzdělání knihovníků.

Pro podrobnější informace o počítačové kriminalitě odkazuji na svou bakalářskou práci, která se věnuje zejména oblasti, která odpovídá názvu - KOVÁŘOVÁ, Pavla. *Problematika získávání dat z cizího osobního počítače s OS Windows XP s přihlédnutím k situaci v ČR*. Brno : Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, 2006. 76 s., 11 s. příl. Vedoucí diplomové práce Mgr. Petr Škyřík. Tato práce také zahrnuje bohatý poznámkový aparát, který může posloužit jako zdroj pro získání konkrétních informací, právě z materiálů uvedených v tomto příspěvku jsem vycházela, proto neuvádím použitou literaturu – šlo by o seznam delší než samotný příspěvek.