POČÍTAČOVÁ BEZPEČNOST A VÝUKA INFORMATIKY

COMPUTER SECURITY AND EDUCATION OF INFORMATICS

Dagmar Brechlerová

EuroMISE centrum, Oddělení medicínské informatiky
ÚI AV ČR,v.v.i.
Pod Vodárenskou věží 2
182 07 Praha 8

Abstrakt
Příspěvek se zabývá významem informací o počítačové bezpečnosti ve výuce informatiky pro lékaře i další zdravotnický personál

Klíčová slova: počítačová bezpečnost, výuka informatiky

Abstract
This paper describes problem of computer security education. It is necessary to include computer security to informatics education for medical students, too.

Keywords: computer security, education of informatics

Úvod

Ve zdravotnictví se dnes běžně používá výpočetní a komunikační technika jako je propojení pracovišť sítěmi různého druhu, zdravotnické informační systémy, využívá se internet, elektronická podpora při léčení pacientů, pro další vzdělávání lékařů a ostatního personálu, stejně tak studentů. Zákon o péči o zdraví lidu (Zákon č. 20/1966 Sb. o péči o zdraví lidu, ve znění pozdějších předpisů) umožňuje za určitých podmínek vést dokumentaci v elektronické podobě, současný technologický pokrok (XML podepisování [1]) umožňuje i výběrové (tj. pouze určité části) digitální podpisování dokumentů. Stejně tak nové pokroky v možnostech v precizně diferencovaném rozdělení přístupu ke zdrojům (dané např. novými bezpečnostními jazyky SAML - Security Assertion Markup Language [2]) a XACML - eXtensible Access Control Markup Language [3])) umožňují přesně diferencovat možnost přístupu k elektronické dokumentaci pro různé skupiny uživatelů (lékař, sestra, laborant atd.). Zdá se, že již nic nebrání tomu, přejít k vedení dokumentace pouze v elektronické podobě. [4] Stejně tak rychlý pokrok v dalších oblastech využití ICT ve

zdravotnictví na první pohled může svádět k nadšení a obrovskému optimismu. Všechny tyto i další prostředky a metody mohou skutečně přinášet mnoho výhod pro lékaře i pacienty, stejně tak ale přinášejí různá nebezpečí. Vzhledem k rychlému rozvoji výše uvedených oblastí si ne každý nebezpečí spojená s těmito technologiemi uvědomuje.

Neměli bychom tedy zapomínat na to, že použití počítačů a dalších prostředků ICT. může naopak přinášet různá nebezpečí. Mezi ně můžeme počítat řadu nebezpečí, která se objevují vždy při použití informačních technologií, jako je podvržení zfalšovaných dat, špatné smazání dat (zejména citlivých), únik dat jak při přenosu přes internet či jinou síť, tak ale i z nepřipojeného počítače při jeho opravě, při užívání neoprávněnou osobou atd. Dále zfalšování webových stránek, útoky na hesla, phissing a mnoho dalších útoků. Ale také běžné chyby jako špatné ukládání dokumentů a dat, opomenutí zálohování, nezajištění systému při výpadku proudu a mnoho dalších.

Počítačová bezpečnost

Celé této oblasti různých bezpečnostních problémů se věnuje specializovaný podobor informatiky tzv. počítačová bezpečnost. Jde o velmi rychle se rozvíjející obor, neboť s každou nově zavedenou technologií také bohužel ihned přijde řada nových druhů útoků. Zatím zejména finanční instituce jako banky, apod. věnují této skutečnosti velkou pozornost. Ale i přes jejich velkou snahu a významné vložené prostředky občas dochází k úniku dat, k jejich napadení, prodeji osobních údajů apod. U finančních institucí se většinou jedná o úspěch vnitřního útočníka, který využije některého zanedbání bezpečnostních pravidel.

Stejně tak ale mohou být napadena data zdravotní. Dá se namítnout, že odpovědnost za zabezpečení sítě nese správce sítě a nikoliv lékař. Za zabezpečení zálohování odpovídá IT oddělení nemocnice atd. Ale existuje řada útoků, které využívají nevědomosti či naivity uživatele a některým těmto útokům se nedá zabránit ani sebelépe propracovanou technologií. Navíc řada lékařů zejména v malých privátních ordinacích neužívá pro správu svého počítače nebo malé sítě žádného profesionála, ale třeba členů rodiny, známých apod. Je nutno si uvědomit, že na rozdíl od ztráty bankovních dat či napadení účtu je v oblasti zdravotnictví poněkud jiná situace. Pokud dojde k prozrazení dat o pacientovi, tak je jednak porušen Zákon o ochraně osobních údajů a je spáchán trestný čin, ale navíc na rozdíl od prozrazení bankovních dat nejde již tuto situaci změnit. Zatímco účet můžeme zrušit, peníze převést jinam, jednou prozrazená zdravotní data již nijak změnit či zrušit nejde. Proto je nutné, aby všechen zdravotnický personál si byl této situace vědom. Stejně tak např. podvržená zdravotní data mohou způsobit poškození zdraví až smrt. Tak jak výpočetní technika do zdravotnictví stále více proniká, tak také tato nebezpečí

vzrůstají. Navíc zástupci různých firem, kteří se snaží prodat zdravotnické informační systémy či podobný software, na tato nebezpečí samozřejmě ve svém zájmu neupozorňují. Vývoj v IT je velmi rychlý a díky tlaku firem, které vyvíjejí nový hardware či software, se do praxe dostávají i ne zatím ověřené technologie. Na oblast léčiv se vztahují přísné mechanismy pro jejich ověřování, ale na použití IT zatím nikoliv.

V minulých dobách bylo na oblast počítačové kriminality pohlíženo jak na celkem neškodnou činnost zejména studentů, kteří z této pseudo „zábavy“ vyrostou a mohou se poté stát vysoce kvalifikovanými speciality právě v oblasti počítačové bezpečnosti. Dnes je ale situace již zcela jiná. Jedná se o výnosné odvětví kriminality (dle některých odhadů dokonce výnosnější než odchod s drogami). Data jsou odcizována na objednávku a černý trh s daty nejrůznějšího typu jen kvete. Ne každý uživatel IT si ale tuto situaci uvědomuje a je na ni připraven.

Výuka počítačové bezpečnosti v kurzech informatiky

Bylo by proto dobré, kdyby se i budoucí lékaři a sestry či další zdravotnický personál během svého studia seznamovali i s touto oblastí a proto by bylo žádoucí do osnov informatiky na všech úrovních také zahrnout přiměřené informace právě o počítačové bezpečnosti. Nejde jen o informace pro studenty medicíny či zdravotních škol, ale i o důležité téma pro další vzdělávání lékařů, neboť zejména lékaři starší generace nemají k počítačům často nijak vřelý vztah. Pokud ovšem informační a komunikační technologie využívají ve své praxi (a tomu se dnes již lze vyhnout velmi obtížně), je nutné zachovávat určitá pravidla, protože jejich nedodržení může vést k velmi závažným důsledkům. Ve vzdělávacích kurzech EuroMISE (jako bylo např. vzděláváni v rámci projektu Síť podpory vzdělávání ve zdravotní telematice a eZdraví - Strukutrální fondy), ale i v dalších jako je výuka pro 1.LF UK a MFF UK, jsou součástí výuky i informace o počítačové bezpečnosti a tyto přednášky vždy vyvolají velkou pozornost. Některé zkušenosti z výuky biomedicínské informatiky jsou shrnuty v [5],[6].

Při výuce počítačové bezpečnosti pro neprofesionály v této oblasti není nutné vysvětlovat do hloubky např. problematiku šifrování, či nastavení firewallu, ale spíše problémy uživatelské bezpečnosti. Samozřejmě samotné informační systémy pro zdravotnictví by měly být vyvíjeny tak, aby se pokud možno různá nebezpečí eliminovala. Jak ale již uvedeno výše, tak zejména útoky pomocí tzv. sociálního inženýrství využívají lidské chyby, určité naivity, podcenění nebezpečí a protože se jedná o zcela novou oblast lidského chování, jde poměrně snadno dosáhnout úspěchu.

Dnes již k výuce mediků stejně tak i sester i dalšího zdravotnického personálu běžně patří základy informatiky. Pod tímto názvem se obvykle na

lékařských fakultách či zdravotnických školách vyučují např. základy použití kancelářských balíků, základní informace o hardwaru, použití internetu, základy databází, vyhledávání informací apod. Tedy v osnovách můžeme najít např: textové a tabulkové zpracování zdravotnických dat, grafické a statistické zpracování zdravotnických dat, úvod do tvorby zdravotnické databáze, počítačové sítě. A někdy, ale ne vždy, také základy bezpečnosti dat ve zdravotnictví

Bylo by tedy žádoucí osnovy jak pro studenty tak i pro další vzdělávání pracovníků ve zdravotnictví (jak lékařů, tak i nelékařů) obohatit i o informace z této oblasti. Protože jde o poměrně speciální problematiku, určitě by se pro tuto oblast hodilo vypracování kurzu v elektronické podobě, který by poté mohli využívat pedagogové z různých škol v různých variantách. Tato oblast se velmi rychle mění a elektronická podoba by umožnila sledovat rychlý vývoj oboru. Stejně tak by řadě malých ordinací mohlo pomoci vypracování určité vzorové bezpečnostní politiky, která by ošetřila možná nebezpečí. Bezpečnostní politika je základní dokument při budování bezpečnosti každé instituce, firmy, organizace atd.

Závěr

Příspěvek se snažil upozornit na nebezpečí spojená s používáním ITC ve zdravotnictví a na potřebu vzdělávat lékaře i další personál i v této oblasti.

Literatura

[1] http://www.w3.org/TR/xmldsig-core/

[2] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[3] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[4] Brechlerova, D., Candik, M., New trends of electronic health documentation, 42nd Annual 2008 IEEE International Carnahan Conference on security technology, Prague, 2008, Conference Proceedings, pp.13-16

[5] Zvárová, J. Education in Biomedical Informatics Using e-Learning Tools, Sborník, International EURASIP Conference, Brno, 2008

[6] Zvárová, J. Education in Biomedical Informatics, CeHR : International Conference, 2007, eHealth, Regensburg, Německo, pp.27-32

Práce je podporována projektem AVČR 1ET200300413 - Informační technologie pro rozvoj kontinuální sdílené péče o zdraví