1. BLOK

Úvod: Ochrana dat a etika v informačních technologiích

Zavedením prostředků informačních technologií (IT) nemusí vždy dojít ke zlepšení úrovně ochrany informací a jiných hodnot - často tomu bývá právě opačně. První problémy znají "pamětníci" z dob, kdy se výplaty začaly počítat na počítači výplaty byly spočítány daleko rychleji a za menšího úsilí, ale případné opravy a nedostatky se také najednou řešily mnohem déle. Často to byla řešení typu "my to nemůžeme opravit, dáme ti chybějící peníze příští měsíc v odměnách". Je tomu dnes jinak? Jaké další problémy lze očekávat? Které z nich se dotknou "jen" firem a vládních organizací a které mohou bolet nás jako soukromé osoby? K jakým nedopatřením při nasazení prostředků IT došlo a dochází, čeho se lze vyvarovat a jak?

Co je DES a jak pracuje? K čemu je digitální podpis a k čemu PGP? Lze zajistit bezpečné obchodování na Internetu a jak? Může se v budoucnu stát, že se budete bát svěřit některé údaje o zdravotních problémech svému lékaři?

Prostřednictvím této části kurzu se pokusím zodpovědět co nejvíce obdobných otázek, a také ujasnit pojmy a techniky, které jsou často zmiňovány povrchně a bez náležitého vysvětlení a uvedení souvislostí.

1.1 Bezpečnost a informační soukromí

Bezpečnost (angl. *Security*) je vlastnost prvku (např. IS), který je na určité úrovni chráněn proti ztrátám nebo také stav ochrany (na určité úrovni) proti ztrátám. V bezpečnosti IT zahrnuje ochranu činností zpracování, úschovy, distribuce a prezentace informací. Pojmem bezpečnost budeme nadále rozumět jen bezpečnost jako "Security", pokud nebude stanoveno jinak.

Stejný český termín bezpečnost označuje totiž i anglické "*Safety*", což je spíše předpoklad, že při specifikovaných podmínkách nedojde ke stavu ohrožení lidského života, zdraví, hodnot a prostředí.

Soukromí (angl. *Privacy*) je v obecném pojetí charakteristikou života jedince a jeho práva a možnosti kontroly informací o sobě a o své činnosti, spolu s ochranou proti nežádoucímu rušení. Informační soukromí se vztahuje především na zmíněnou možnost kontroly informací osobních dat a jiných relevantních citlivých informací. Tento termín se váže na jiná práva jedince, a tak je přesná

definice obtížná. Proto se také termín informační soukromí používá spíše pro neformální motivaci k zajištění ochrany osobních informací, pravidel pro jejich kontrolu a poskytování jiným subjektům atd. Příklady relevantních bezpečnostních funkcí mohou být anonymita, pseudonymita, nespojitelnost a nepozorovatelnost.

Ochrana informačního soukromí nebo jen osobních dat může být důvodem pro zajištění bezpečnosti, stejně jako třeba ochrana firemních dat nebo informací vojenské rozvědky. V žádném případě nelze pojmy (informační) bezpečnost a informační soukromí volně zaměňovat, ale ani oddělovat.

1.2 Hodnota osobních dat

> *Soukromé informace jsou informace, které nechceme sdílet s jinými, nebo u kterých chceme osobně kontrolovat jejich pohyb (tzn. sdílíme je s někým, ale ne s "ostatními").*
>
> *[KC Laudon, Communications of ACM 9/96].*

Roger Needham, profesor University of Cambridge a světově uznávaný odborník v oblasti bezpečnosti, formuloval tuto myšlenku: *rozhodujícím ukazatelem úrovně ochrany je cena osobních dat "na ulici" - na černém či šedém trhu*. U zdravotních dat je cena v Anglii 150-200 liber, v kanadské provincii Quebec podle některých "inzerátů" 20-60 liber. Podle Needhama by měla cena být výrazně nad 500 liber. Pokud bude cena směšně nízká, je nevýznamnou položkou nákladů pojišťovacích firem, které tak mají jednodušší rozhodnutí, jak vysoké splátky pojistného nasadit tomu či onomu jedinci.

Cenu osobních dat a tím i úroveň ochrany ovlivňují tři faktory:

1. výše trestu těm, kdo data jiných řádně neohlídali a spolupodíleli se tak na jejich úniku;
2. výše trestu těm, kdo s nimi neoprávněně manipulují;
3. úroveň ochranných mechanismů.

Čtyřicet let komunistického "pořádku", který neřadil soukromí občana k nejvíce respektovaným hodnotám, u nás vykonalo své - často nevíme, jakou hodnotu mají naše osobní informace pro stát i mnohé firmy a jaká škoda nám může vzniknout jejich únikem mimo naši kontrolu. Pro zajímavost, v Anglii je ke svým osobním datům a zacházení s nimi necelých 20 % občanů totálně lhostejných, stejný počet velmi obezřetných až paranoidních a okolo 60 % je ochotno část svých práv nechat omezit za "přiměřenou úhradu" - finanční, věcnou či nejčastěji v podobě výrazného zlepšení služeb. Co to konkrétně znamená?

Ano částečnému omezení práv, když finanční informace budou dostupné komukoliv v rámci banky - za možnost skutečně rychlého a nekomplikovaného obsloužení ve kterékoliv pobočce nebo bankomatu.

Ne výraznému omezení práv zavedením jednotného občanského záznamu ve státním informačním systému. Vzhledem k rozsahu a přehmatům státního aparátu snad nikdo nevěří ujišťování o zárukách ochrany dat. Hlavně je ale zájem na zachování práva občana poskytovat aktuální a úplné informace o sobě jen v nutných případech. Pokud občan plní základní povinnosti (neporušuje zákon a platí daně) a nežádá od státu žádné přímé služby, tak má právo být stranou ("*to be let alone*") a kontrolovat pohyb informací o sobě.

1.3 Soukromí

Pokud se na soukromí z technického pohledu týče, zajímají nás mimo ochrany důvěrnosti (informačního obsahu) dat následující vlastnosti, které definují různé pohledy na obecný pojem „soukromí". K důvěrnosti dat jakožto velmi důležitému tématu se budeme věnovat později.

1.3.1 Anonymita

Anonymita je vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému. Jedná se o poměrně samozřejmou součást pojmu „soukromí". Takto se eliminuje např. hrozba profilování uživatelů (angl. *user profiling*).

1.3.2 Pseudonymita

Jedná se o vlastnost vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému *tak, že uživatel je stále zodpovědný za toto použití*. Možnými aplikacemi jsou např. používání služeb s následnými platbami za toto používání bez uvedení vlastní identity při bezproblémových platbách (v případě problémů lze v odůvodněných případech identitu zjistit – např. u banky). Určitá podobnost existuje s poštovními přihrádkami (PO Box), kde pokud nedojde k porušení zákona, tak majitel přihrádky zůstává odesílateli pošty neznámý. Pokud ale dojde ke střetu se zákonem, lze u pošty zjistit skutečnou identitu majitele přihrádky.

1.3.3 Nespojitelnost

Nespojitelnost (angl. *unlinkability*) je vlastnost systému, který zajišťuje možnost *opakovaného* použití zdrojů nebo služeb s tím, že ostatní si tato použití nebudou schopni spojit (spojení ve smyslu vzájemné souvislosti, může se jednat o postupně i současně poskytované stejné i různé služby). Tato vlastnost se výrazně odlišuje předchozích dvou v tom, že nezohledňuje identitu uživatele, ale

rozsah služeb a zdrojů, které byly použity stejným uživatelem. Možnou aplikací je ochrana soukromí uživatele používajícího současně služeb Internetu a určité telefonní přípojky – komunikační partner by neměl mít možnost zjistit, odkud se daný uživatel na Internet připojuje.

1.3.4 Nepozorovatelnost

Nepozorovatelnost (angl. *unobservability*) je vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb tak, že ostatní nemohou zpozorovat používání daného zdroje nebo služeb. Tato vlastnost nemá přímou návaznost na žádnou z předcházejících vlastností. Ochraňovanými hodnotami nejsou informace o uživatelích, ale o použití zdrojů nebo služeb. Příkladem aplikace může být ochrana proti tzv. analýze provozu (angl. *traffic analysis*), tj. např. proti pozorování toho, která strana rozesílá nejvíce zpráv v určité době nebo při výskytu určité události.

1.4 Rozsáhlé databáze osobních informací

Seskupováním osobních dat do rozsáhlých databází dochází k tomu, že takovýmto kombinováním dat o určité citlivosti lze získat informace daleko citlivější, které jinak spadají do kategorie s vyššími požadavky na ochranu. Pro seskupování se také používá termín agregace (z angl. *aggregation*). Představte si, že máte k dispozici kompletní informace o zdravotním stavu a finanční situaci

1. manžela nebo manželky;
2. přímého nadřízeného;
3. všech zaměstnanců organizace, kde pracujete;
4. všech obyvatel města/vesnice, kde žijete;
5. všech klientů určité banky nebo zdravotní pojišťovny.

Cítíte ten rozdíl? Jedná se přitom o stejné informace - jen se mění druh a počet osob, ke kterým se vztahují. A představte si, jaký zájem o tyto informace musí mít třeba banka, která poskytuje úvěry a hypotéky, nebo např. pojišťovací agent.

Pravděpodobnost, že budou informace neoprávněně zpřístupněny, záleží na dvou faktorech:

- *hodnotě informací*,

- *počtu osob, které mají k informacím přístup* (operátoři i uživatelé systému).

1.4.1 Statistické databáze

Podobné problémy byly poprvé studovány v souvislosti s databázemi údajů ze sčítání lidu v USA. Podobně se také využívají data získaná u nás při sčítání lidu, kdy uvádíte náboženské vyznání i počty televizorů, vybavení mobilními telefony atd. Takové databáze sice obsahují citlivé údaje o jednotlivcích, ale jejich využití má být pouze pro *statistické dotazy* k vytvoření obrazu o celkových potřebách obyvatelstva a formulování vládní politiky - podpora církví, určení vybavenosti domácnosti podle lokalit atd. *Výsledky dotazů v takovýchto databázích nesmějí poskytnout údaje o jednotlivcích.*

V roce 1979 se známé odbornici Dorothy Denningové podařilo prokázat, že prostředky, které využívala americká vláda pro formulaci dotazů a získávání odpovědí ze statistické databáze sčítání lidu, povolovaly konstrukci takových dotazů, které umožnily získat údajně tajné informace o jednotlivci. Podle přesvědčení vládních činitelů byly takové informace opravdu tajné a dobře chráněné - dokud Denninová nezjistila plat svého šéfa sérií legitimních dotazů v databázi.

Konstrukce série takových dotazů nebývá obvykle jednoduchá. Představte si ale zjednodušeně, že se zpřesňováním dotazu až na [kolik je měst s 17-18 000 obyvatel, kde žije jen jeden muž, který je 36letý evangelík slovenské národnosti, jeho 28letá žena žije mimo toto město, 6letá dcera s touto ženou a 15letý syn s oním mužem] dostanete k odpovědi 1. Pak už lze jednoduše zjistit plat tohoto našeho souseda jen doplňováním dotazů o [..., jehož příjem je X-Y měsíčně] a určováním X a Y tak, aby odpověď byla stále 1 a ne 0.

Pokud nám systém spravující databázi pro statistické dotazy umožní podobný postup, pak je to špatný systém. Existují tři druhy protiopatření.

1. *Minimální rozsah dotazu* a to buď s omezením minima

   - celkového počtu záznamů použitých pro tvorbu odpovědí, nebo
   - počtu záznamů použitých pro tvorbu odpovědí na každou automatickou část dotazu.

   Např. první uvedenou techniku využívají databázové systémy novozélandského národního zdravotního systému.

2. *Náhodný výběr* je technika nyní používaná v americké databázi údajů ze sčítání lidu. Každý dotaz je zodpovězen na základě vyhodnocení náhodně vybraných záznamů ze všech existujících záznamů.

3. *Perturbační (zmatečné) techniky* podle některých definic zahrnují i výše uvedený náhodný výběr. Obecně se jedná o přidání pseudonáhodného "šumu" tak, aby odpovědi byly konzistentní, ale získání elementární odpovědi na sérii podobných dotazů nebylo možné. Často jsou používány dvě metody:

   - k záznamům zahrnutým pro vyhodnocení dotazů se přidají další náhodně vybrané podobné záznamy;
   - vypočtená hodnota nebo mezihodnoty jsou zaokrouhlovány nebo mírně pozměněny.

Problém inference (odvození), který jsme diskutovali, je definován jako odvození informací o vyšší citlivosti zpracováním a analýzou skupiny informací o nižší citlivosti nebo také nepřímý přístup k informacím bez přímého přístupu k datům, která tyto informace reprezentují.

1.5 Tři dimenze

I samotné utajení dat je velmi složitým problémem. Když se poprvé objevil AIDS, tak mnohá zdravotnická zařízení ve světě postupovala tak, že záznamy pacientů HIV pozitivních převedla mimo dosah běžných uživatelů zdravotnického informačního systému. Pak je ale jednoduché odvodit, že pacient, jehož záznam nemůže "běžný" lékař získat, je pacientem HIV pozitivním. Opět se jedná o inferenci. A obdobný je i triviální problém u víceúrovňových systémů (viz horizontální členění dále v kurzu), kdy může činnost uživatele na nižší úrovni odhalit fakta odpovídající úrovni vyšší. Téměř klasický případ bývá uváděn při zápisu souboru. Pokud se uživatel na úrovni "Důvěrné" pokusí ve víceúrovňovém systému uložit soubor *DOCS/IRAN/MISSILES/FORM.DOC* a obdrží systémové

hlášení, že soubor již existuje a uživatel nemá právo jej přepsat, pak lze jednoduše odvodit, že soubor již vytvořil a využívá někdo na úrovni vyšší.

Při utajování datové položky je třeba zvážit tři dimenze:

1. zda tato data mají být utajována,
2. zda samotná existence těchto dat je utajována,
3. zda i důvod utajení těchto dat je utajován.

Řešení první dimenze je nejjednodušší - přístup k datům mají jen oprávněné osoby. Technik k realizaci tohoto požadavku existuje několik. Další dvě dimenze vyžadují více zamyšlení a kreativní řešení. Ochrana před inferencí je jedním ze stále ne stoprocentně vyřešených témat při návrhu bezpečných víceúrovňových databází. Pro některé situace vystačí perturbační techniky, jindy zase důsledné vedení auditního záznamu a jeho průběžné hodnocení pro zjištění pokusu o útok na data prostřednictvím inference. Žádné z dosavadních řešení však není všelékem.

1.6 Síla informací

S příchodem mnohoznačně definované informační společnosti se změní nejen podmínky pro bankovnictví, vzdělávání, obchodování či nakladatelskou činnost, ale také pro armádu a národní bezpečnost. Využití počítačů přináší nesčetné výhody, ale i nová rizika - ve všech oblastech, kam jsou informační technologie zaváděny. Pro zajímavost se podívejme na oblast, která je obestřena nezvykle mnoha "kdyby", "když" a "až" - informační válečnictví (angl. *information warfare*).

Obrana každého pořádného státu závisí nejen na armádě, ale i na tajných službách. Koneckonců i armáda jako taková má své výzvědné služby. Vždy se pracuje na základě dvou nosných principů:

- Dosáhnout vlastní *informační dominance*, tzn. mít správné informace na správném místě ve správný čas.
- Zamezit nepřátelské straně v dosažení informační dominance.

Vzpomeňte jen lekcí z historie. Dávným bitvám snad vždy předcházelo chytání "jazyků", jejichž mučení bylo kruté i na tehdejší poměry. Není snad potřeba příliš rozvádět úspěšnou kryptanalýzu německých šifrovacích strojů Enigma polskými a britskými kryptografy během 2. světové války, která tak podle některých odhadů byla zkrácena o 1-2 roky. A s příchodem radaru se posunulo získávání informací o nepříteli za hranici dohledu oka. Netrvalo ale dlouho a přišlo se na to, že lze vysílat klamavý zpětný signál "od neexistujících letadel". Střely dnes také

nejsou řízeny jen množstvím prachu a orientací hlavně při výstřelu. A copak nelze rušit nebo dokonce "nahradit" řídící signál střely nepřítele signálem vlastním? Moderní války se nevyhrávají zničením co největšího počtu bojových prostředků nebo vojáků v primární fázi. Na to je dost času ve fázi sekundární, kdy vojáci a bojové prostředky nepřítele ve zmatku nevědí co dělat nebo přímo útočí na sebe navzájem. V primární fázi je důležité právě způsobit onen zmatek (maximálně eliminovat příjem a hlavně výměnu informací na straně nepřítele) a přitom si udržet zdroje informací o činnosti a vybavení nepřítele i schopnost dodat informace včas svým jednotkám.

2. BLOK

Co je bezpečnost?

Bezpečnost nemusí pro každého znamenat to samé. Bude jiná pro armádu, jiná pro banky a nemocnice a jiná pro správce rubrik "hezké chvíle" v inzertních časopisech.

Jsou dvě zásadní sféry aplikací bezpečnosti. Ta prapůvodní je vojenská, kde se např. kryptografické techniky (tedy bezpečnostní mechanismy) uplatňují již po tisíciletí, na významu ovšem v posledním desetiletí výrazně nabývá i sféra obchodní či komerční. Požadavky obou se často významně liší a přestože vojenské aplikace daly oboru bezpečnosti IT první uplatnění, dnes se musí i vojenští činitelé často přizpůsobit. Velká přeorganizovanost armády (v určitém smyslu ústící do nepřehlednosti) vytváří potřebu zajistit určitý systém ve zpracování a využití informací. Ten v zásadě spočívá v

- *zajištění vlastní informační dominance* - je třeba mít správné informace na správném místě ve správný čas,
- *minimalizaci nepřátelské informační dominance* - omezit šíření vlastních informací k nepříteli, případně dokonce zajistit dodání špatných (klamavých) informací.

2.1 Hierarchické členění informací

V přeorganizovaných strukturách není systematizace jednoduchá záležitost; částečné řešení přináší hierarchická klasifikace informací. Pro minimalizaci nepřátelské informační dominance je důležité svěřovat pracovníkům jen nejpotřebnější informace (a taky tyto pracovníky předem i průběžně prověřovat). Pak je nasnadě, že *důvěrnost je zásadním požadavkem* v obdobných systémech. *Hierarchické členění* (viz obr.) je jednoduchým modelem vhodným pro tento účel.

Přísně tajná data
Tajná data
Důvěrná data
Citlivá data

Hierarchické členění dat podle citlivosti.

Počet úrovní a klasifikace informací na určitou úroveň záleží na požadavcích organizace. Tomuto tématu budou později věnovány asi dva díly, nyní jen zjednodušeně - uživatel prověřený pro určitou úroveň má obvykle možnost prohlížet informace na úrovni své a všech nižších. Jedna znejčastěji aplikovaných bezpečnostních politik je založena na modelu *Bell-LaPadula:*

- Procesy nesmějí číst data na vyšší úrovni (tzv. jednoduchá bezpečnostní vlastnost, též *NRU - no read up*).

- Procesy nesmějí zapisovat data do nižší úrovně (tzv. *-vlastnost, též *NWD - no write down*).

Tyto dvě základní vlastnosti a formální aparát pro sledování stavu bezpečnosti stroje tvoří podklad pro budování víceúrovňových systémů. Model má drobné nedostatky, přesto je důležitým mezníkem voboru bezpečnosti. Dnes je na základě tohoto horizontálního pohledu hodnocena úroveň bezpečnostních technik a aplikací, celý obor bezpečnosti je tímto pohledem do značné míry ovlivněn.

Řešení je ale opravdu jen částečné, poněvadž je umělé a neodráží skutečnou situaci. I v armádě se řeší problémy sohledem na původ protivníka, druh krizové situace apod., nikoliv s ohledem na začlenění informací o protivníkovi do určité kategorie. Např. americká armáda má dnes "nadstavenu" úroveň *přísně tajné* rozšířenou o oborové podúrovně, jako třeba přísně tajné nukleární, přísně tajné chemické, přísně tajné kryptografické atd.

Další problémy mohou souviset se způsobem prosazování takovéto bezpečnostní politiky. To, že nelze zapisovat data do nižší úrovně, je např. u tajných služeb dosti ošemetné - část zpravodajské sítě může padnout díky zrádci na vyšší úrovni, o jehož přístupu kmateriálům na nižší úrovni nejsou správci těchto materiálů informováni. Kdyby se údaje o přístupu (požadavek zodpovědnosti) zapisovaly, pak lze srovnáním těchto údajů u "odstraněných" agentů zjistit, kdo si jejich materiály prohlížel. V praxi se na tyto souvislosti přichází obvykle jen náhodou.

2.2 Případ od případu

V komerční sféře je běžné, že práce se člení podle obchodních případů, rozmístění poboček atd. *Často sice záleží na utajení informací (před konkurencí), nejdůležitějším požadavkem je však integrita dat*. Nemusí se vždy jednat o integritu ve striktním pojetí, ale o *smysluplnost a správnost* využívaných informací. Modelem, který je nejčastěji citován pro komerční bezpečnost, je model *Clark-Wilson*, který formalizuje stoleté zkušenosti zobchodování a účetnictví. Model formalizuje pohled na data a operace nad daty při zachování integrity, ale i pojmy jako auditní záznam a řízení přístupu.

To, že se v komerční sféře řeší problémy sohledem na „téma“ (obchodní partner či případ apod.), vede kodlišnému přístupu ke zpracování informací. Svou roli samozřejmě hraje i menší rozsah drtivé většiny firem a potřeba pružného jednání. Pokud komerční pohled hodně zjednodušíme, pak jej lze shrnout do vertikálního modelu členění informací.

Hrozby vojenským systémům pocházejí primárně od vnějších činitelů, kdežto komerčním systémům hrozí větší nebezpečí od vlastních pracovníků. Vždyť i celý systém podvojného účetnictví je kontrolním systémem proti neúmyslným a často i proti úmyslným chybám (pokud knihu zápisu pro kreditní a debetní pohyby vedly dvě různé osoby/skupiny).

Zaměstnanci mohou, kromě zadávání nesmyslných informací do firemních IS, také informace roznášet „po hospodách" i konkurenci. Tady je pak nasnadě zájem firem, aby zaměstnanci nevěděli více, než je pro jejich práci nezbytně nutné. Informace jsou pro armádu velmi důležité, pro komerční organizace však naprosto nezbytné. Také interakce pracovníků armády s okolním světem je podstatně menší než u pracovníků komerční organizace. Důležitým aspektem pro úschovu a zpracování informací vkomerční sféře jsou právní závazky a do značné míry i *podpora zákazníka.*

K výše uvedenému přistupuje potřeba zajištění bezpečnosti při plně elektronickém obchodování. Téměř vždy je třeba zajistit integritu dat, často i ve spojení se zajištěním důvěrnosti. A to jsme se ještě nedostali k *autentizaci* (ověření původu) dat, zajištění *nepopiratelnosti původu* zprávy nebo jejího *přijetí* atd.

Uvedené zjednodušení vojenského a komerčního pohledu na využívané informace může být v některých ohledech násilné, pro popsání rozdílu v pohledech na různé aspekty bezpečnosti je však výstižné. Svět není černobílý, ale výše popsané rozdíly mohou být pro pochopení mnohých otázek užitečné. Je důležité si uvědomit, že „bezpečnost“ nemusí pro každého znamenat to samé. Bude jiná pro generála, jiná pro šéfa pobočky banky a jiná pro správce databáze Annonce, např. rubriky „hezké chvíle“. Tady se pak dostáváme k trendu posledního desetiletí - *soukromé* bezpečnosti. Není to sice úplně novinka (už César si dopisoval s Kleopatrou šifrovaně), ale je zřejmé, že význam nabývá právě s dostupností počítačů i pro osobní potřebu. Pak lze příliš vtíravému pronikání do osobního života účinně bránit často právě zase počítačem.

Základní pravidlo počítačové bezpečnosti:

Stoprocentní ochrana bývá téměř vždy nemožná a musíme se spokojit s určitým kompromisem.

2.3 Zásadní kroky pro zajištění bezpečnosti

Při prvním pohledu na řešení problémů informační bezpečnosti musíme mít na paměti tři zásadní skupiny úkonů, které je (téměř) vždy potřeba provést:

Analýza hrozeb. V tomto bodě je potřeba zvážit, co všechno by mělo být chráněno, a především vyhodnotit, jaké hrozby hrozí ochraňovaným hodnotám. Tento krok je směrodatný pro další postup, často však nelze než vycházet z analýzy empirických poznatků o problémech v okolí, jiných útocích na podobné hodnoty atd. Chybně provedená analýza hrozeb má za důsledek téměř vždy chybně navržená bezpečnostní opatření. Hodnoty pak mohou být chráněny velmi nákladným, ale naprosto nesmyslným a neúčinným způsobem.

Specifikace bezpečnostní politiky a architektury. Bezpečnostní politika stanoví, co mají dosáhnout a zajistit ochranná opatření. Zahrnuje požadavky, pravidla a postupy, určující způsob ochrany a zacházení s ochraňovanými hodnotami. Architektura na vysoké úrovni popisuje strukturu celého komplexu opatření a jednotlivým částem přiřadí bezpečnostní funkce.

Popis bezpečnostních mechanismů. Zde jsou rozepsány techniky pro implementaci bezpečnostních funkcí nebo jejích částí. Účinnost mechanismu musí být v souladu s bezpečnostní politikou a přiměřená odpovídajícím hrozbám.

2.4 Základní cíle

Podívejme se na některé základní prvky bezpečnostní politiky a jejich provázanost s bezpečnostní architekturou (ne vždy jsou potřebné všechny uvedené prvky).

Důvěrnost. Cílem zabránit zjištění sémantického obsahu dat nepovolanými (neautorizovanými) osobami. Můžeme se o to snažit např. obecně utajením existence informací (značně obtížné), kontrolou přístupu k místům, kde se data nacházejí maskováním mezi jinými soubory nebo změnou dat do jiné podoby, kterou nelze změnit zpět bez znalosti patřičné (tajné) informace – klíče. Tento poslední způsob se běžně označuje jako šifrování a budeme se mu věnovat dále v tomto kurzu.

Integrita. Data bez povolení majitele (autorizované osoby) nesmí nepozorovaně změnit svůj stav (tzv. slabá integrita) nebo jej nesmí změnit vůbec (tzv. silná

integrita). Povšimněme si, že pokud bude na dobré úrovni zajištěná důvěrnost, pak je zajištění integrity snazší.

Dostupnost. Autorizovaní uživatelé by měli mít přístup k datům a službám co nejméně komplikovaný. Dobře chráněná data, co se důvěrnosti a integrity týče, která nelze použít při řádné práci, ta nám nebudou příliš platná.

Zodpovědnost. Za veškeré své činy a chování v systému mají uživatelé zodpovědnost vůči majiteli dat. Tato zodpovědnost nemusí být přímá (majitel nekontroluje každého uživatele osobně), ale v případě potřeby musí vždy existovat možnost zjistit, kde a kým (příp. i za jakým účelem) data v určitou dobu byla použita.

2.4.1 Nevhodnost doplňkové bezpečnosti

V praxi se často setkáváme s postupem, kdy se při budování systému nebo tvorbě aplikace těsně před odevzdáním zákazníkovi zjistí, že „by tam mělo být nějaké zabezpečení“. Nejprve je pracně vybudován rozsáhlý systém a teprve dodatečně se přichází na to, že bude potřeba "nějak" zajistit ochranu spravovaných informací. Tak se dodatečně vyčlení několik procent z rozpočtu a začne se doplňovat. Důsledky a výsledky jsou stejné, jako doplňování jedné z pozapomenutých stěžejních funkcí systému těsně před dodáním zákazníkovi.

Doplňková bezpečnost (angl. *add-on security*) v naprosté většině případů neposkytuje stejnou míru ochrany jako bezpečnost budovaná pro začlenění v prvotní specifikaci systému. Důsledkem pozdního doplnění specifikace o zajištění bezpečnosti může být vybudování ochrany na nižší úrovni (než by za stejné peníze poskytla ochrana budovaná plánovitě) nebo překročení rozpočtu, mnohdy obojí.

2.4.2 Co všechno může být bezpečnost

Bezpečnost nespočívá jen v pořízení a nainstalování ochran do systému. I v počítačových systémech hraje významnou roku **fyzická bezpečnost** -- jde o to zjistit, kdo má fyzický přístup k prvkům systému (bez ohledu na hardwarovou či softwarovou ochranu) nebo jaký může být dopad přírodních katastrof. Dokonalá ochrana uživatelských stanic je mnohdy k ničemu, pokud je k systému připojena konzola, ze které operátor může neoprávněně (a nepozorovaně) sledovat informace na uživatelských obrazovkách. A dokonale šifrovaná data na serveru, z něhož někdo bez problémů ukradl celý pevný disk, ta již řešení podnikové strategie asi také nepomohou.

Tady přicházíme k dalšímu aspektu - **bezpečnosti personální** - která je jedním z pilířů dobré ochrany. K ochraně dat nemusí být příliš platné bezpečnostní řešení „na míru“ od renomované firmy, pokud k obsluze systému s přístupem k důležitým datům najmeme špióny konkurence nebo původce krádeží dat z několika bank.

Při návrhu bezpečnostní politiky je třeba si uvědomit, že mnohé hrozby nelze přímo odvrátit, ale buď jen snížit pravděpodobnost jejich "úspěšné" realizace nebo s minimálními ztrátami (zdržením) zajistit následnou nápravu. Data je možné lehce duplikovat a záložní kopie bezpečně ukládat na vzdáleném místě. Nikdo nemůže zabránit šíření moru a virů, můžeme však udělat hodně pro to, aby nedošlo k nákaze našich dat. Zajištění bezpečnosti nikdy neznamená zajištění úplné ochrany, nýbrž minimalizaci rizik na tolerovatelnou úroveň.

2.5 Příklad z praxe

Pojďme se podívat na skutečný případ budování bezpečnosti v celostátní počítačové síti Národního zdravotního systému (NHS) v Anglii. Předběžný odhad nákladů - pouze na zavedení šifrovacích služeb pro zajištění důvěrnosti dat - je téměř 20 milionů liber, na roční údržbu a provoz padnou zhruba 3 miliony liber. Podle názoru mnohých expertů budou skutečné náklady několikanásobně vyšší, i když se opominou investice na zajištění jiných, pro medicínskou praxi životně důležitých, funkcí spolehlivé počítačové sítě. Dvě zásadní předpokládané hrozby jsou:

- možnost neautorizovaného připojení jedinců (hackerů) k síti a
- možnost odposlechu zasílaných informací.

Kritiku tohoto přístupu lze shrnout uvedením dvou údajů:

- podle posledních údajů z nezávislého auditu Národního zdravotního systému je jen 6 % případů narušení bezpečnosti způsobeno zvenčí,
- podle slov vedoucího oddělení UNIRAS, která je zodpovědná za vyhodnocování incidentů v oblasti bezpečnosti IT v celé vládě, byla v letech 1994/95 jen 2 % případů narušení bezpečnosti způsobena zvenčí.

Zkuste se na základě těchto údajů zamyslet nad tím, zda zajištění důvěrnosti je opravdu stěžejním problémem, případně které jiné hrozby nebyly zohledněny a o jaké prvky by měla být doplněna bezpečnostní politika takové rozsáhlé sítě.

2.6 Informační bezpečnost ve zdravotnictví

Medicína je velmi specifický obor lidské činnosti a rozhodně se jí rozvoj v oboru informačních technologií nedotkl tak, jako třeba žurnalistiky nebo obchodu. (Naštěstí?!) Samozřejmě – s počítači se i v lékařské praxi setkáváme téměř denně, nelze ovšem čekat, že nahradí člověka do takové míry jako třeba v dopravě. Doktor není jen opravář těl, ale často i duší a lidských vztahů. Návštěva lékaře není pro většinu z nás nikdy obyčejným aktem jako třeba koupě piva nebo příjem výplaty.

Pokud chceme hovořit o bezpečnosti IT v medicíně, tak na prvním místě musíme zmínit bezpečnost ve smyslu anglického "Safety" - předpoklad, že při specifikovaných podmínkách nedojde ke stavu ohrožení lidského života, zdraví, hodnot a prostředí. Ano, jde právě o ten lidský život. Kolik přístrojů je dnes v nemocnici obsluhovaných počítačem nebo s jeho zásadní podporou? K ohrožení života může dojít *přímo*, podobné případy jsou ale podle odborné literatury velice výjimečné, spíše extrémní. Jsou např. zaznamenány případy, kdy chyba v programu způsobila zvýšení dávek ozáření, kterému pak pacient podlehl. Lapidárně řečeno - pro počítač je číslo jako číslo. To je také příčinou chyb vedoucích k *nepřímému* ohrožení, kdy počítač nebo jím řízený přístroj dodají chybné výsledky vyšetření/analýzy, na jejichž základě lékař stanoví chybný léčebný postup.

2.6.1 Důvěryhodnost a důvěrnost

Mnohých případů léčby na základě chybných dat se lze vyvarovat zajištěním důvěryhodnosti (např. autentizací) předávaných informací. U informací na papíře lékař obvykle pozná rukopis specialisty z nemocnice nebo alespoň razítko ap. Jak ale pozná

původ digitalizovaných informací? Přece nebude při obdržení výsledků z laboratoře telefonovat, ověřovat a zjišťovat kdo, kdy, jak a koho!? Právě bezpečnostní mechanismy jako třeba digitální podpis by měly lékaři umožnit zodpovězení všech otázek současně s přijetím laboratorní zprávy. S jakou úrovní spolehlivosti, to už závisí na implementaci a také přístupu všech pracovníků, kteří budou takovému systému předávat data nebo jej spravovat. Důležitý je také audit práce s daty (kdo viděl nebo dokonce měnil výsledky testu). Právě důvěrnost zdravotních informací je dnes velice aktuálním a ožehavým tématem.

Pacient má rozhodně právo očekávat, že lékař nikomu nesdělí žádné jeho osobní zdravotní informace, které získal při lékařském výkonu. Morální závazek lékaře je zde jasný, ne vždy však je dobře zakotven i v zákonech. Podle mého osobního názoru by lékař měl mít povinnost střežit takto získané informace stejně, jako kněz střeží informace spadající pod zpovědní tajemství. Bez souhlasu pacienta by pak rozhodně neměl tyto informace žádným způsobem předávat dál, ani pro potřeby soudu nebo policie.

Jak má však lékař dodržet takové závazky, když musí zdravotní pojišťovně sdělit jaké zákroky provedl? Jaké závazky pak mají pracovníci pojišťovny? Na jaké úrovni pak lze udělat smysluplný kompromis? Podobné otázky je vždy nutno řešit při tvorbě *administrativních* dat, která v medicíně jsou v 90 % založena na datech *klinických*. České zdravotnictví se ale v současné době potýká s řadou existenčních problémů, takže lze očekávat, že důsledné řešení obdobných otázek zůstane až na další století.

2.6.2 Bezpečnost v klinických informačních systémech

V medicínské informatice bývá sice požadavek na ochranu dat často explicitně zmiňován, obvykle však bez podrobnější specifikace bezpečnostní politiky. Objevilo se donedávna jen několik návrhů k principům bezpečnostní politiky. Zásadní význam má až publikace "*Security in Clinical Information Systems*", kterou vydala British Medical Association (BMA) v lednu 1996. Zásadní přínos tohoto výsledku práce specialistů BMA a zvláště Rosse Andersona (Cambridge University) je ve stanovení devíti základních principů bezpečnostní politiky pro klinické informační systémy. Přístup, který vyžaduje BMA i od vedoucích činitelů ministerstva zdravotnictví a Národního zdravotního systému, se často kříží s některými "představami" o jednotném zdravotním záznamu - který by byl přístupný např. i pracovníkum ministerstva. Jejich zájem je zřejmý, ale nebude asi ani vzdáleně podobný představě pacienta. Také model práce zdravotnictví v Británii je rozdílný od českého -- přesto -- podívejme se na jednotlivé principy:

Každý identifikovatelný klinický záznam musí mít seznam řízení přístupu s vyjmenováním lidí nebo skupin lidí, kteří mohou záznam číst a přidávat k němu data. Systém musí zamezit přístupu kohokoliv, kdo není na tomto seznamu.

1. Doktor může otevřít nový záznam, kde je uveden jen on a pacient na seznamu řízení přístupu. Pokud je pacient jen na speciálním vyšetření, pak může doktor na seznam zařadit i jeho ošetřujícího lékaře.

2. Právě jeden z lékařů na seznamu řízení přístupu musí být označen jako odpovědný a pouze on může seznam měnit a může k němu přidávat jen odborné zdravotnické pracovníky.

3. Odpovědný lékař musí pacientovi sdělit, kdo je na seznamu řízení přístupu při vytvoření nového záznamu, při jakýchkoliv změnách a kdykoliv je odpovědnost za záznam předávána jinému lékaři. Pacientův souhlas musí být výslovný, s výjimkou řešení nouzových stavů a specifikovaných statutárních případů.

4. Nikdo nesmí mít možnost smazat klinické informace, dokud neuplynula předepsaná doba pro jejich úschovu.

5. Všechny přístupy ke klinickým záznamům musí být zaznamenány s udáním informací kdo a kdy se záznamem pracoval. Auditní záznam všech mazání musí být neustále udržován.

6. Informace ze záznamu A mohou být připojeny k záznamu B tehdy a jen tehdy, když seznam řízení přístupu záznamu B je obsazen v seznamu pro A.

7. Musí být zavedena účinná opatření proti agregaci osobích zdravotních informací. Pacienti, k jejichž seznamu řízení přístupu má být přidána další osoba, musí být zvlášť upozorněni, pokud již tato osoba má přístup ke zdravotním informacím velkého množství lidí.

8. Počítacové systémy, které pracují s osobními zdravotními daty, musí mít subsystém, který efektivně prosazuje výše uvedené principy. Účinnost tohoto subsystému musí být podrobena hodnocení nezávislými experty.

2.6.3 Požadavky lékařů?

Při využití počítačů jsou lékaři velmi vnímaví uživatelé. Trpí sice obvyklou "nemocí" požadavku na jednoduchost obsluhy atd., ale jsou si jasně vědomi možností, které jim počítače přinášejí. Je to do jisté míry dáno kvantem informací, které během svého vzdělání a každodenní praxe musejí lékaři vyhledávat, zpracovávat a využívat. Vědí, do jaké míry je spolehlivost (důvěryhodnost) informací zásadní pro jejich práci a také vědí, že jejich pacientům záleží na tom, aby ne každý (úředník) věděl o jejich nejniternějších problémech.

Dva zásadní požadavky - důvěryhodnost a důvěrnost informací - jsou zásadní charakteristiky lékařské praxe po tisíciletí. Osobně si myslím, že právě tento fakt dodává spolupráci lékařů a odborníků na bezpečnost IT hodně na zajímavosti. Ať už to budou aplikace na ochranu důvěrnosti informací o pacientech, na zajištění důvěryhodnosti laboratorních výsledků a zpráv o nových léčebných postupech a šetřeních nebo anonymizace dat pro výzkum a výuku nových adeptů oboru, popř. i pro plánovače ministerstva zdravotnictví.