

# Informační bezpečnost ve zdravotnictví

PV080

Vašek Matyáš

# Zdravotnictví a bezpečnost

## SECURITY

- Vlastnost prvku (např. IS), který je na určité úrovni chráněn proti ztrátám nebo také stav ochrany (na určité úrovni) proti ztrátám.

## SAFETY

- Předpoklad, že při specifikovaných podmínkách nedojde ke stavu ohrožení lidského života, zdraví, hodnot a prostředí.

# Ohrožení života „počítačem“ v medicíně?

## PŘÍMO

- Tyto případy jsou velmi výjimečné, spíše extrémní.
- Např. chyba v programu způsobí zvýšení dávek ozáření, kterému pak pacient podlehl.
  - Therac-25 (Wikipedia)
  - Białystok incident

## NEPŘÍMO

- Častější případy.
- Počítač nebo jím řízený přístroj dodají chybné výsledky analýzy, na jejichž základě lékař stanoví chybný léčebný postup.

# Důvěryhodnost a důvěrnost

- Podvržená data – autentizace.
- Rukopis laboranta, razítko ap.
- Digitální podpis – integrita, autenticita dat.
- Prokazatelná zodpovědnost.
- Mlčenlivost – osobní zdravotní informace získané při lékařském výkonu.
- *Lékař, pacient, sestra, vedoucí ústavu, zdrav. pojišťovna.*

# Bezpečnost v klinických informačních systémech

- Víceméně roztráštěné úsilí při tvorbě směrníc a pravidel. (Bezpečnostní politika!)
- "*Security in Clinical Information Systems*", British Medical Association (BMA), 1996

# BMA-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.

# BMA-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.

# BMA-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.



# BMA-4

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

# BMA-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.

# BMA-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.

# BMA-7

- Musí být zavedena účinná opatření proti agregaci osobních 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.

# BMA-8

- Počítačové 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.

# Úvod do informační bezpečnosti

PV080

Vašek Matyáš (část slajdů J. Bouda)

# Bezpečnost (angl. *Security*)

Vlastnost prvku (např. IS), který je na určité úrovni chráněn proti ztrátám nebo také stav ochrany (na určité úrovni) proti ztrátám.

# Bezpečnost

1. Prevence

2. Detekce

3. Reakce



# Informační dominance

1. Cíl: Dosažení vlastní *informační dominance*, tzn. mít správné informace na správném místě ve správný čas.
2. Cíl: Zamezit nepřátelské straně v dosažení informační dominance.

# Minimalizace nepřátelské informační dominance

- Pro minimalizaci nepřátelské informační dominance je důležité svěřovat pracovníkům jen nejpotřebnější informace;
- taky tyto pracovníky předem i průběžně prověřovat.

# Při utajení dat zvažujeme:

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

# Od aktiva k útoku

- **Aktiva** – data, zdroje... – s hodnotou
- **Zranitelnost** (systému) a útočník => **hrozba**
- **Riziko** – pravděpodobnost uplatnění hrozby
- **Útok** je realizací hrozby, **útok může být úspěšný či neúspěšný**
  - Úspěšný únik má dopad na hodnotu aktiv

# Od rizika k bezpečnostní politice

- **Riziko omezujeme**
  - odstranění nemožné či příliš nákladné (častěji)
- **Bezpečnostní opatření** mají omezit rizika
- **Bezpečnostní mechanismy** implementují bezpečnostní opatření
- **Bezpečnostní politika** specifikuje způsoby uplatňování bezpečnostních opatření

# Kde může selhat bezpečnost

- Matematický algoritmus
  - Velmi nepravděpodobné a neobvyklé
  - Může se stát jen při hrubé chybě výrobce systému
  - GSM
- Špatné naprogramování matematického algoritmu
  - Dost neobvyklé, stává se pouze u nekvalitních firem
  - Je důsledkem nedostatečného vzdělání programátorů
  - Nevhodný způsob generování náhodných čísel

# Kde může selhat bezpečnost

- Chyby při implementaci systému
  - Velmi časté
  - Způsobeny snahou firem o minimalizaci nákladů při vývoji
  - Softwarové firmy nenesou odpovědnost za škody způsobené bezpečnostními chybami
  - Škoda na jejich pověsti není tak velká, aby se jim vyplatilo investovat peníze do kvalitního vývoje

# Kde může selhat bezpečnost

- Všechny předchozí důvody zaviňují pouze 5 % všech prolomení bezpečnosti!
- Hlavním důvodem prolomení jsou chyby a úmyslné jednání obsluhy počítačů
  - Snadno zapamatovatelné a tedy i uhodnutelné heslo
  - Použití nevhodných programů, které heslo neúmyslně zveřejňují – nezabezpečený přenos dat po Internetu



# Incidenty způsobeny

- Chybami (neúmyslné): 50-70 %
- Vlivem přírody, zdrojů: 10-15 %
- Škodlivým softwarem: 5-10 %
- Záměrnými útoky (sabotáže) zaměstnanců (i bývalých) : 10-20 %
- Vnějšími útočníky: 1-5 %

# Kde nejčastěji „selže“ bezpečnost

- Úmyslné jednání zaměstnanců
  - Pomsta zaměstnavateli nebo kolegům
  - Snaha obohatit se
  - Zaměstnanec je někým zkorumpován

Absolutně bezpečné systémy v praxi  
NEEXISTUJÍ

# Základní problém bezpečnosti

- Co útočník získá napadením daného systému?
- Kolik peněz, strojů, času a lidí musí nasadit na napadení daného systému?
- Vyplatí se to?
- Hromadné útoky na více systémů!

# Klasifikace útočníků I

- Původní klasifikace 1-2-3, dnes nereprezentativní
- **Třída 0** (script kiddies) –útočníci, kteří nedisponují dostatkem znalostí o systému a využívají komukoliv běžně dostupné předpřipravené nástroje a postupy pro útoky na známé zranitelnosti – zkoušením těchto nástrojů metodou pokus-omyl nebo čistě náhodným necíleným zjištěním zranitelnosti (např. reakce zařízení na krátký a intenzivní výboj světla).
- **Třída 1** (chytrí nezasvěcení útočníci) – mnohdy inteligentní útočníci, kteří nemají dostatek znalostí o systému. Využívají cenově běžně dostupných nástrojů nebo služeb s možností zmapování principu fungování přístroje v dohledné době. Obvykle zkouší útočit na známé bezpečnostní slabiny, nevyhledávají nové.

# Klasifikace útočníků II

- **Třída 1.5** – jedná se o osoby nebo skupiny osob s možnostmi na rozhraní mezi 1. a 2. třídou. Útočníci jsou inteligentní, se základními znalostmi systému. Využívají cenově dostupných nástrojů, útočí na známé chyby a snaží se hledat i nové slabiny. Např. specializovaná pracoviště univerzit.
- **Třída 2** (zasvěcení insideři) – zkušení jedinci nebo týmy s nákladným a sofistikovaným vybavením, se kterým jsou schopni provést analýzu systému v dostatečném čase. Mají úzce specializované technické vědomosti a zkušenosti, různě hluboké pro jednotlivé části systému s možným přístupem k většině z nich.

# Klasifikace útočníků III

- **Třída 3** (majetné organizace) – vysoce kvalifikované týmy využívající zařízení, která nejsou běžně dostupná na trhu. Mohou provádět detailní analýzy systému, navrhovat komplexní útoky a využívat nejmodernější analytické nástroje. Příkladem jsou např. vládní organizace (NSA), které mají pro své aktivity značné finanční zabezpečení.

# Ochrana komunikace/dat

- Fyzická ochrana
  - místnosti
  - kabely
  - CD/DVD, USB tokeny
  - ...
- Kryptografie – umění (mj.) skrýt význam (informační hodnotu) dat
  - Návazná přednáška



# Bezpečnost z dřívějšího pohledu

- **Důvěrnost:**

*Cílem je zabránit zjištění sémantického obsahu dat nepovolanými (neautorizovanými) osobami.*

- např. 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.

# Bezpečnostní model 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*).

# Integritní model Biba

- Inverzní k modelu Bell-LaPadula
- Cílem je zajištění integrity dat
- Procesy nesmějí číst data na nižší úrovni – vlastnost *no read down*
- Procesy na dané úrovni nesmí zapsat data do vyšší úrovně – vlastnost *no write up*

# Bezpečnost z více úhlů pohledu

- **Integrita:**

*Data bez svolení majitele (autorizované osoby) nesmí*

- nepozorovaně změnit svůj stav (tzv. slabá integrita)
  - nebo jej nesmí změnit vůbec (tzv. silná integrita).
- Pokud bude na dobré úrovni zajištěná důvěrnost, pak je zajištění integrity snazší.

# Bezpečnost z více úhlů pohledu

- **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.

# Bezpečnost z více úhlů pohledu

- **(Prokazatelná) 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.

# Bezpečnost z více úhlů pohledu

- Autentizace entit: *víme s kým komunikujeme.*
- Řízení přístupu: *přidělování dat/zdrojů kontrolováno.*
- Nepopiratelnost: *aktivitu nelze později popřít.*
  - Odeslání zprávy
  - Přijetí zprávy
- ...

# Zásadní kroky pro zajištění bezpečnosti

1. Analýza a hodnocení hrozeb
2. Specifikace bezpečnostní politiky a architektury
3. Popis bezpečnostních mechanismů



# Analýza a hodnocení hrozeb

- Zvážit, co všechno by mělo být chráněno
- Vyhodnotit, jaké hrozby hrozí ochraňovaným hodnotám.
  - Často 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* – 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 jejich částí.
- Účinnost mechanismu musí být v souladu s bezpečnostní politikou a přiměřená odpovídajícím hrozbám.

# Nevhodnost doplňkové bezpečnosti

- Nejprve je pracně vybudován rozsáhlý systém a pak se přijde na to, že bude potřeba “nějak” zajistit ochranu spravovaných informací.
- 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.

# Další oblasti bezpečnosti

- Fyzická
- Personální
- Dokumentová (bez ohledu na formu)
- ...

# Co je to bezpečnost ICT?

- Bezpečnost při používání systémů ICT obecně
  - Počítačová bezpečnost
  - Mobilní telefony
  - Kreditní karty
  - Internetové bankovníctví

# Příklady zneužití

- Neoprávněné použití cizí kreditní karty
  - Výběr z bankomatu
  - Platba na terminálu (v obchodě)
  - Platba po Internetu (!)
- Zneužití mobilního telefonu
  - Odposlech telefonního hovoru
  - Volání na cizí účet
  - Zneužití falešné identity

# Cíle bezpečnosti ICT

- Zamezit zneužití elektronických zařízení
- Nalézt osobu pokoušející se o zneužití
- Minimalizovat škody způsobené zneužitím
- ...

*Více o praktických aspektech později v semestru...*



# Zajištění bezpečnosti

- jedná se o proces, nikoliv stav či cíl!
  - (Výjimku by mohly tvořit systémy, které se samy vůbec nemění a kde beze změny je i jejich okolí. ☺ )

# Polosemestrální písemka!

6. listopadu

Více informací 30. října