Úvod do informační bezpečnosti, inf. bezpečnost ve zdravotnictví

PV080

Vašek Matyáš

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.

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.

Minimalizace nepřátelské informační dominance

- Pro minimalizaci nepřátelské informační dominance je důležité svěřovat pracovníkům jen nejpotřebnější informace;

- taky tyto pracovníky předem i průběžně prověřovat.

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*).

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.

Ochrana komunikace/dat

- Fyzická ochrana
  - místnosti
  - kabely
  - CD, USB tokeny

  ...
- Kryptografie – umění (mj.) skrýt význam (informační hodnotu) dat
  - Návazná přednáška

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)

- ...

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. ☺)

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.

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 roztříštěné úsilí při tvorbě směrnic a pravidel. (Bezp. 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.