Část I:
Základní legislativa týkající se bezpečnosti IT

Osnova

- Zákon o ochraně osobních údajů
- GDPR
- Zákon o kybernetické bezpečnosti a jeho novelizace
- Zákon o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 372/2011 Sb. Zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)
- Vyhláška č. 98/2012 Sb

Zákon o ochraně osobních údajů

RNDr. Dagmar Brechlerová, Ph.D.

Zákon č. 101/2000 Sb., O ochraně osobních údajů a o změně některých zákonů

Mnohokrát měněn, poslední změna 2015

UOOU Úřad na ochranu osobních údajů, www.uoou.cz, velké pravomoce

- **Hlava V: Organizace úřadu**
- § 30
- (1) Zaměstnanci Úřadu jsou předseda, inspektoři a další zaměstnanci.
  (2) Kontrolní činnost Úřadu provádějí inspektoři a pověření zaměstnanci (dále jen "kontrolující").
- **§ 37 Oprávnění kontrolujícího na přístup k informacím**
- **Kontrolující je při kontrole zpracování osobních údajů oprávněn seznamovat se se všemi informacemi v rozsahu nezbytném pro dosažení účelu kontroly, včetně citlivých údajů.**
- **§ 40**
- **Dojde-li k porušení povinnosti stanovené zákonem nebo uložené na jeho základě při zpracování osobních údajů, uloží inspektor opatření k odstranění zjištěných nedostatků a stanoví lhůtu pro jejich odstranění.**

Osobní a citlivé údaje

Pro účely tohoto zákona se rozumí
a) **osobním údajem** jakákoliv informace týkající se **určeného nebo určitelného subjektu údajů**. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu

b) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, **zdravotním stavu** a sexuálním životě subjektu údajů a **genetický údaj subjektu údajů**; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,

Správce, zpracovatel

Správce

j) správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, **provádí zpracování a odpovídá za něj**. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,

Zpracovatel

k) zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona,

Správcem osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. obsažených ve zdravotnické dokumentaci je pak **poskytovatel zdravotních služeb**

§ 9 Citlivé údaje je možné zpracovávat, jen jestliže

- a) subjekt údajů dal ke zpracování **výslovný souhlas**…….
- c) **se jedná o zpracování při poskytování zdravotních služeb**, ochrany veřejného zdraví, zdravotního pojištění a výkon státní správy v oblasti zdravotnictví podle zvláštního zákona nebo se jedná o posuzování zdravotního stavu v jiných případech stanovených zvláštním zákonem,
- …. Toto zpracování tedy probíhá **bez výslovného souhlasu subjektů údajů**.

- f) se jedná o údaje podle zvláštního zákona nezbytné pro provádění nemocenského pojištění, důchodového pojištění (zabezpečení), úrazového pojištění, státní sociální podpory a dalších státních sociálních dávek, sociálních služeb, sociální péče, pomoci v hmotné nouzi a sociálně-právní ochrany dětí, a při zajištění ochrany těchto údajů v souladu se zákonem
- Zdravotnictví: zpracování osobních údajů, **dokonce citlivých**
- Zpracování osobních údajů ve zdravotnické dokumentaci je zpracováním, které probíhá na základě zákonného zmocnění, a v souladu s § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, obsahujícím výjimku pro zpracování osobních údajů bez souhlasu pacienta (subjektu údajů) nebo bez souhlasu jeho zákonného zástupce.

Povinnosti osob při zabezpečení osobních údajů

- § 13
- (1) Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k **neoprávněnému** nebo **nahodilému přístupu** k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. **Tato povinnost platí i po ukončení zpracování osobních údajů.**
- (4) V **oblasti automatizovaného zpracování** osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také
  a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,
  b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
  c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a
  d) zabránit neoprávněnému přístupu k datovým nosičům.

§ 20 Likvidace osobních údajů

(1) Správce nebo na základě jeho pokynu zpracovatel je povinen **provést likvidaci** osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti subjektu údajů podle § 21.

(2) Zvláštní zákon stanoví výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.

Obecné nařízení o ochraně osobních údajů (GDPR)

Důvody

- Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů byla z roku **1995**
- Z toho vznikly národní zákony
- Směrnice přestala vyhovovat novým požadavkům jednotného digitálního trhu, nový vývoj technologií, Internet, předávání dat do zahraničí. Po 4 letech příprav vznikla nová pravidla pro ochranu osobních údajů ve formě **nařízení Evropského parlamentu a Rady, které je přímo použitelné ve všech členských státech.**
- **Nařízení** Evropského parlamentu a Rady (EU) **2016/679** ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- **GDPR vstoupí v plnou účinnost 25. května 2018,** nejvýznamnější změna v oblasti ochrany soukromí a osobních údajů za dvacet let od přijetí původní směrnice

GDPR General Data Protection Regulation

- EU s přijetím obecného nařízení slibuje pevný a soudržnější rámec pro ochranu údajů, **jenž se bude opírat o důrazné vymáhání práva**
- Správcům a zpracovatelům napříč celou Unií nařízení ukládá stejné povinnosti a úkoly, které zajistí důsledné zpracování osobních údajů, přičemž dle vyjádření Evropské komise by mělo dojít také ke snížení administrativní zátěže. Nařízení, které je přímo aplikovatelné ve všech členských státech, má zajistit také účinnou kontrolu jeho dodržování a stejné sankce.
- Forma **přímo účinného nařízení**.
- Členské státy tak normu nemusí transponovat do svých právních řádů, vnitrostátní právní předpisy je potřeba pouze adaptovat tak, aby byly s nařízením v souladu. V případě rozporu vnitrostátního práva s přímo účinným předpisem EU, má pak dle zásady tzv. aplikační přednosti evropského práva **nařízení vždy přednost**.!!!!!!

Ne

- Z působnosti Obecného nařízení jsou **vyloučeny** činnosti fyzické osoby, při kterých jsou zpracovávány **osobní údaje výlučně pro osobní či domácí činnost**.
- Dále je z působnosti Obecného nařízení vyloučeno zpracování prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.
- Právní úpravu však bude aplikovat v každém členském státě nezávislý orgán dohledu a přes jednotnost úpravy se její výklady mohou v jednotlivých členských státech lišit. Nařízení také ponechává více než **50 dílčích otázek k úpravě samotným členským státům**, určitým národním specifikům se proto při přeshraničím zpracování nevyhneme ani do budoucna

Zákon o kybernetické bezpečnosti 181/2014 a jeho novela

Dagmar Brechlerová

KBI FBMI ČVUT

Zákon o kybernetické bezpečnosti

- Vláda České republiky 2. ledna 2014 schválila Návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (tzv. Zákon o kybernetické bezpečnosti)

- Návrh zákona připravil a předložil Národní bezpečnostní úřad.
- Platnost 1.1.2015, 1 rok bylo přechodné období

- Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

NBU

- http://www.nbu.cz/cs/
- 19. října 2011 přijala vláda ČR usnesení č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.
- Přílohou usnesení je Statut Rady pro kybernetickou bezpečnost. Na základě usnesení vzniklo Národní centrum kybernetické bezpečnosti (NCKB), jako součást Národního bezpečnostního úřadu, se sídlem v Brně.

Národní centrum kybernetické bezpečnosti (NCKB)

- http://www.govcert.cz/cs/
- Úkoly:
- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy
- příprava bezpečnostních standardů pro jednotlivé kategorie organizací v ČR
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti

Pojmy…

Kritickou informační infrastrukturou… prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti,

Významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci,

Obě tyto skupiny nemají průnik

§ 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

Kritické …

- Mezi kritickou skupinu tak může patřit např. energetika (výroba, přenos, distribuce, skladování elektřiny, zemního plynu, ropy a ropných produktů). Vodní hospodářství. Potravinářství a zemědělská výroba. **Zdravotnictví.** Doprava (silniční, železniční, letecká, vodní). Komunikační a informační systémy. Technologické prvky pevné sítě elektronických komunikací. Technologické prvky mobilní sítě elektronických komunikací. Technologické prvky pro rozhlasové a televizní vysílání. Technologické prvky pro satelitní komunikaci. Technologické prvky pro poštovní služby. Technologické prvky informačních systémů. Finanční trh a měna. Nouzové služby. IZS. Radiační monitorování. Předpovědní, varovná a hlásná služba Veřejná správa. Veřejné finance. Sociální ochrana a zaměstnanost. Ostatní státní správa. Zpravodajské služby
- Např. http://www.pravniprostor.cz/clanky/ostatni-pravo/jake-povinnosti-vyplyvaji-pro-organy-verejne-moci-ze-zakona-o-kyberneticke-bezpecnosti-ii
- http://www.pravniprostor.cz/clanky/ostatni-pravo/jake-povinnosti-vyplyvaji-pro-organy-verejne-moci-ze-zakona-o-kyberneticke-bezpecnosti-i
- Přednášky prof. Smejkala
- Opět dáno určitými kritérii
- Např. ve zdravotnictví to bylo 2500 akutních lůžek (což není nikde) proto se původní zákon vlastně zdravotnictví nedotkl

Základní služby :

Dále se bude zákon vztahovat na **provozovatele základních služeb**, čímž jsou myšleny především služby, jejichž poskytování je závislé na elektronických sítích nebo informačních systémech a jejichž narušení by mohlo mít významný dopad v některém z důležitých odvětví ekonomiky.

energetika

doprava

bankovnictví

infrastruktura finančních trhů

zdravotnictví

dodávky a rozvody pitné vody

chemický průmysl

veřejná správa

digitální infrastruktura

Zdravotnictví

- Dle sdělení na školení 12.6.2017 MZ (není jasné, zda je to konečné rozhodnutí) se novelizace dotkne nemocnic, které mají bud více než 800 lůžek nebo traumacentrum
- **Mělo by jít o 16 nemocnic**
- Tedy tyto nemocnice budou patřit mezi provozovatele Základní služby

Digitální infrastrukturu

Digitální infrastrukturu budou tvořit výměnné uzly (IXP), poskytovatelé služeb systému doménových jmen (DNS) a registry internetových domén nejvyšší úrovně (TLD).

Pro všechny tyto subjekty bude platit princip minimální harmonizace – to znamená, že povinnosti, které směrnice uvádí, mohou být členskými státy ještě rozšířené.

Národní úřad pro kybernetickou a informační bezpečnost

- Nově
- Brno
- Cílově 400 !!!! zaměstnanců
- Převezme tuto problematiku od NBU

EIDAS

Dagmar Brechlerová

eIDAS

- Zkratka eIDAS se používá pro Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, které bylo publikováno v Úředním věstníku Evropské unie dne 23. července 2014.
- Toto nařízení se plně použilo ode dne 1. července 2016
- 227/2000 zrušen
- 19. září 2016 ve Sbírce zákonů vyhlášený a ihned účinný zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále ZSVDET)
- 298/2016 Sb. ZÁKON ze dne 24. srpna 2016, změnový

eIDAS

- Nařízení eIDAS stanoví, mimo jiné, právní rámec pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek
- http://www.pravniprostor.cz/clanky/procesni-pravo/narizeni-eidas-konecne-adaptovano-do-ceskeho-prava-zakon-o-elektronickem-podpisu-konci
- http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx
- Prezentace: http://www.mvcr.cz/clanek/metodicky-seminar-dopady-narizeni-eidas-po-1-7-2016.aspx

Vyhláška o zdravotnické dokumentaci

Vyhláška č. 98/2012 Sb.

Informace o vyhlášce

- Platnost od 30. 3. 2012
- Účinnost od 1. 4. 2012
- Aktuální znění (květen 2017) od 1. 1. 2016 https://www.zakonyprolidi.cz/cs/2012-98
- + přílohy

Co obsahuje?

- Minimální obsah zdravotnické dokumentace
- Způsob a dobu uchování zdravotnické dokumentace
- Postup vyřazování dokumentace po uplynutí doby uchování

Ve vztahu k IT

- § 2: Součástí zdravotnické dokumentace vedené o pacientovi jsou
  - výsledky vyšetření ve formě písemných popisů, **grafických, audiovizuálních, digitálních nebo jiných obdobných záznamů těchto vyšetření**, operační protokol, anesteziologický záznam,
  - .....
- § 4: Součástí zdravotnické dokumentace zdravotnické záchranné služby jsou
  - **zvukový záznam** o příjmu volání na národní číslo tísňového volání 155 a výzev předaných operačním střediskem jiné základní složky integrovaného záchranného systému (dále jen „tísňové volání"),
  - záznam operátora v **digitální formě,**

Doba uchování

- § 5
- *(1)* Poskytovatel vede a uchovává zdravotnickou dokumentaci v souladu se zásadami stanovenými v příloze č. 2 k této vyhlášce; zajišťuje posouzení potřebnosti zdravotnické dokumentace pro další poskytování zdravotních služeb (dále jen „posouzení potřebnosti") pro účely jejího vyřazení a zničení nebo dalšího uchování. To platí obdobně pro příslušný správní orgán, který podle zákona o zdravotních službách převzal zdravotnickou dokumentaci.
- *(2)* Zdravotnická dokumentace se uchovává po dobu 5 let a označuje se vyřazovacím znakem „S", pokud není jiným právním předpisem nebo v příloze č. 3 k této vyhlášce stanoveno jinak. V případě převzetí zdravotnické dokumentace příslušným správním orgánem se běh lhůt pro dobu uchování podle přílohy č. 3 k této vyhlášce nepřerušuje.
- *(3)* Doba uchovávání zdravotnické dokumentace vedené o pacientovi jedním poskytovatelem počíná běžet dnem 1. ledna následujícího kalendářního roku po dni, v němž byl proveden poslední záznam ve zdravotnické dokumentaci pacienta, pokud není v příloze č. 3 k této vyhlášce stanoveno jinak.
- *(4)* **Pokud zdravotnická dokumentace nebo její části vedené o pacientovi svým zařazením nebo věcným obsahem podléhají několika lhůtám pro její uchování podle přílohy č. 3 k této vyhlášce, doba uchovávání a vyřazovací znak se určí vždy podle nejdelší doby uchování.**

Dokumentace v elektronické podobě (§ 6)

(1) V případě zdravotnické dokumentace vedené **v elektronické podobě** je každý záznam do zdravotnické dokumentace opatřen **elektronickým podpisem**.

(2) Technické prostředky pro vedení zdravotnické dokumentace v elektronické podobě zaručí

- **zabezpečení výpočetní techniky softwarovými a hardwarovými prostředky** před přístupem neoprávněných osob ke zdravotnické dokumentaci a
- vedení **evidence všech přístupů** ke zdravotnické dokumentaci včetně jejich oprav, změn a mazání.

Problémy

- Na jaké medium, doby uchování dost dlouhé
- Jak definovaně likvidovat?
- Jaký dopad GDPR a dalších
- .....

A.

Identifikace, Autentizace, Autorizace uživatele

Identifikace uživatele

- Identifikace je proces zjištění/určení identity uživatele.

1) Udání identity samotným uživatelem.
2) Identifikující systém identitu uživatele určí sám (hledáním v předem daném množství uživatelů). Systém prochází buď databázi těžko podvrhnutelných záznamů všech uživatelů (biometrické informace) nebo databázi tajných informací (například identifikační kód).

Autentizace uživatele

- Autentizace je proces ověření identity uživatele, prokázání identity uživatelem.
- Probíhá obvykle po identifikaci
- Metody:

1) Znalostní faktor (heslo, PIN, bezpečnostní otázka, …)
2) Vlastnický faktor (bezpečnostní token, karta, čip, …)
3) Biometrický faktor (anatomicko-fyziologické charakteristiky, behaviorální charakteristiky)

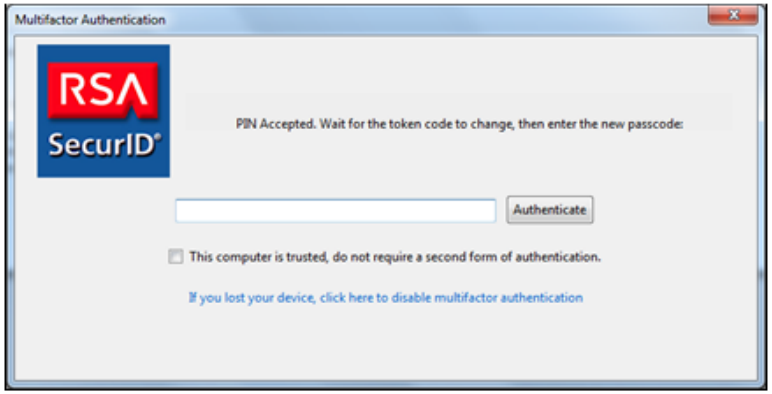
Znalostní faktor

Zásady správného výběru hesla:

- Heslo je bezpečně použitelné pouze tehdy, není-li ostatním uživatelům známé, tj. oprávněný uživatel musí držet heslo v tajnosti.
- Nebezpečné je používat taková hesla, která lze uhádnout s použitím hrubé síly (např. slovníkový útok).
- Heslo by mělo být dostatečně dlouhé a mělo by se skládat z „náhodné" skupiny znaků.
- Známé hlášky, obměny jednoduchých slov, data narození, jména manželů/manželek, dětí, psů aj. jsou pro hesla zcela nevhodná.

Vlastnický faktor

- Bezpečnostní token, magnetická karta, čip



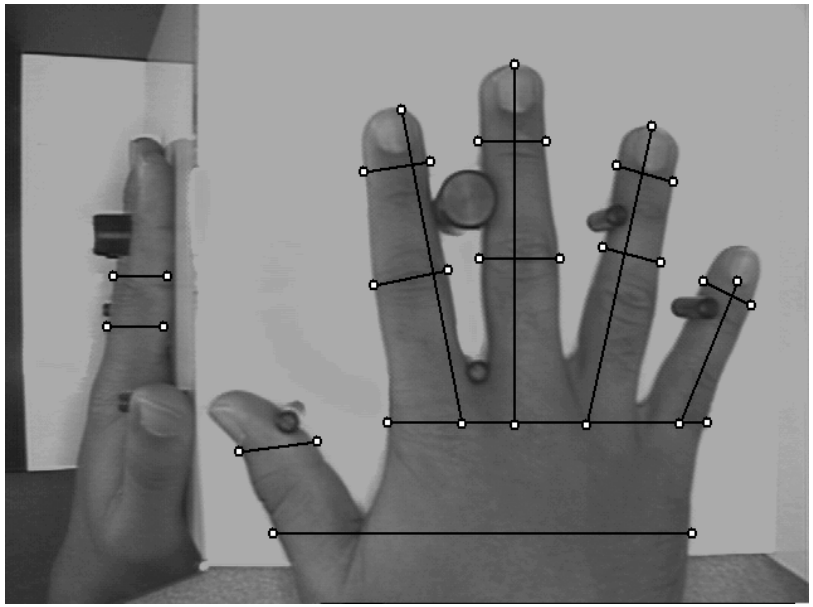
Biometrie

Otisky prstů

- Senzory: kontaktní vs. bezkontaktní

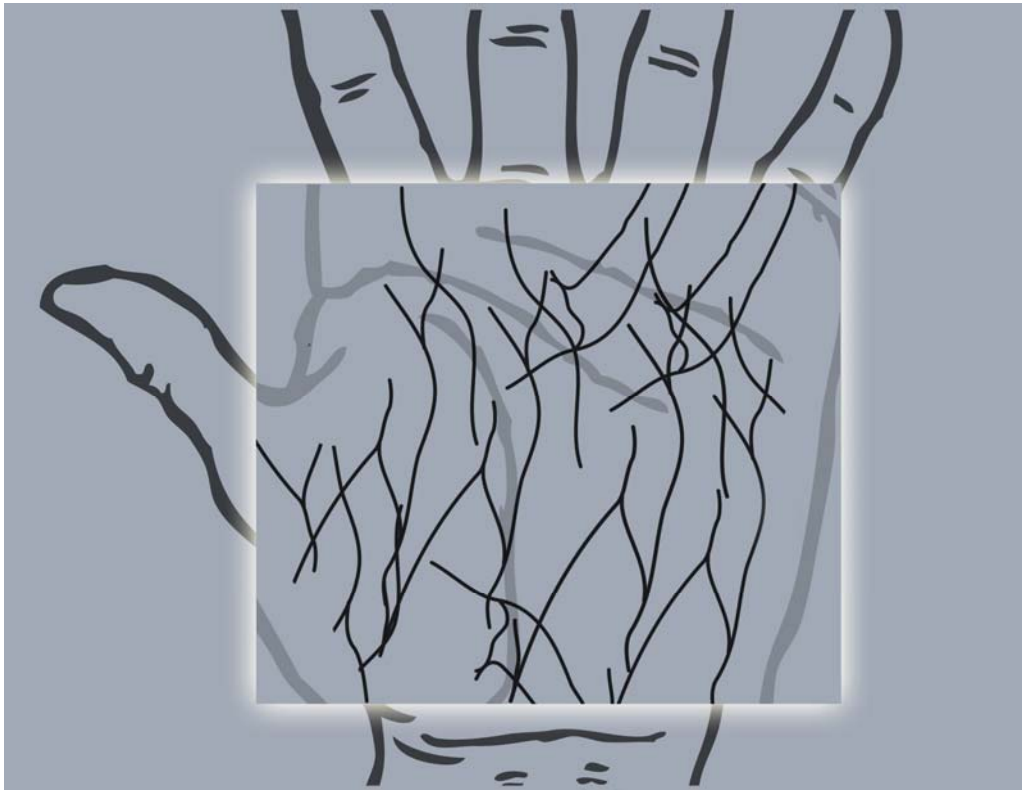
Biometrie

Geometrie tvaru ruky



Biometrie

Snímání krevního řečiště ruky



C.

Bezpečná práce s daty

Šifrování

- Šifrováním se snažíme skrýt obsah komunikace, neskrýváme komunikaci samotnou.
- Šifrou nebo šifrováním budeme označovat kryptografický algoritmus, který převádí čitelnou zprávu neboli prostý text *m* (plaintext, cleartext) na její nečitelnou podobu neboli šifrový text *c* (ciphertext).
- Klíč je tajná informace, bez níž nelze šifrový text přečíst.

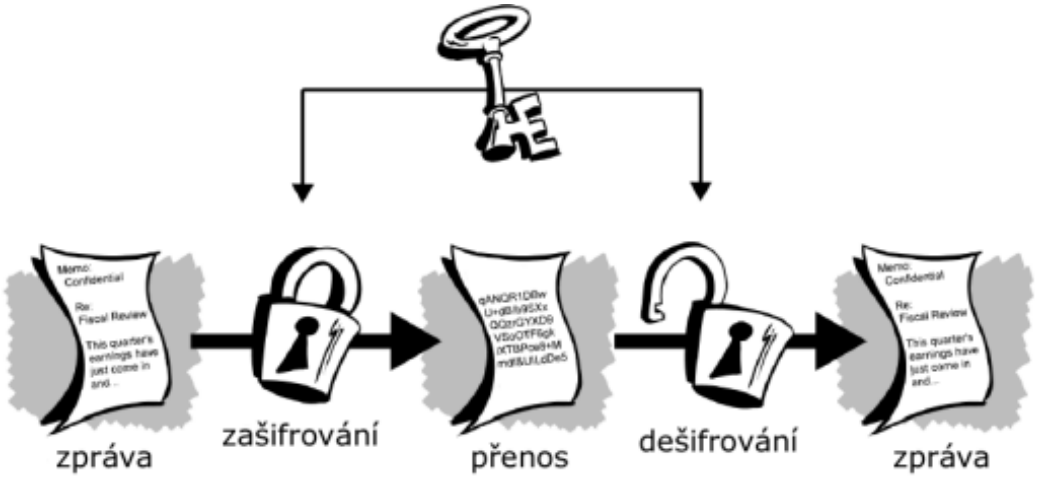
Šifrování

- Symetrická šifra je taková, která pro šifrování i dešifrování používá tentýž klíč.

- Asymetrická šifra používá veřejný klíč pro šifrování a soukromý klíč pro dešifrování.
- Pokud používáme asymetrickou šifru pro podepisování, pak se naopak soukromý klíč podpisujícího používá pro podepsání a jeho veřejný klíč pro ověření podpisu.

Symetrické šifrování

- Symetrické (konvenční) šifrování je založeno na principu jednoho klíče, kterým lze zprávu (data) jak zašifrovat, tak i dešifrovat.



Symetrické šifrování

Výhody:

- nízká výpočetní náročnost

Nevýhody:

- příjemce i odesílatel se musí dohodnout na jednom klíči, který budou znát jen oni dva a který je nutno trvale uchovávat v utajení
- distribuce klíče – jak dostat klíč k příjemci, aniž by se ho chopil někdo nepovolaný
- nutnost velkého počtu klíčů, protože každé dvě komunikující strany potřebují svůj vlastní tajný klíč a počet klíčů ve velké skupině tak neúměrně narůstá

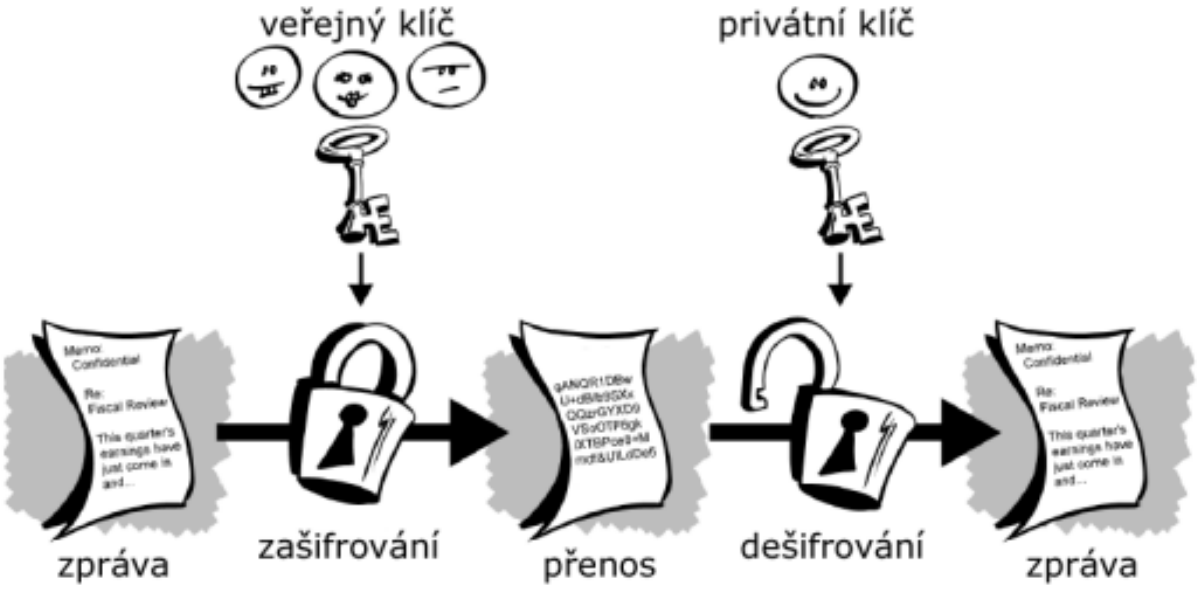
Symetrické blokové šifry

Příklady

Algoritmus	Délka klíče v bitech	Velikost bloku v bitech	Počet rund	Aplikace
DES	56	64	16	SET, Kerberos
Triple DES	112 nebo 168	64	48	PGP, S / MIME
AES	128,192,256	128	10,12 nebo 14	různé
IDEA	128	64	8	PGP
Blowfish	Volitelně do 448	64	16	různé
RC5	Volitelně do 2048	64	Volitelně do 255	různé

Asymetrické šifrování

- Asymetrická kryptografie (kryptografie s veřejným klíčem) je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče.



Asymetrické šifrování

- Asymetrická kryptografie je založena na tzv. jednocestných funkcích = operace, které lze snadno provést pouze v jednom směru: ze vstupu lze snadno spočítat výstup, z výstupu však je velmi obtížné nalézt vstup.
- Nejběžnějším příkladem je násobení: je velmi snadné vynásobit dvě i velmi velká čísla, avšak rozklad součinu na činitele (tzv. faktorizace) je velmi obtížný. *(Na tomto problému je založen algoritmus RSA.)*

D.

Digitální podpis

Digitální podpis

- Digitální podpis zprávy je číslo, které je závislé na samotné zprávě a na nějaké tajné informaci (tajemství) známé pouze podepisujícímu.
- Základním požadavkem na digitální podpis je ověřitelnost podpisu, tedy nezaujatá třetí strana, která musí být schopna rozhodnout, kdo zprávu podepsal a to bez znalosti oné tajné informace (v asymetrické kryptografii je to tzv. privátní klíč).
- Digitální podpis má v informační bezpečnosti celou řadu aplikací: např. v autentizaci, ověření integrity dat, neodmítnutelnosti, certifikace veřejných klíčů v rozsáhlých sítích, tj. potvrzení identity držitele veřejného klíče.

Zaručený digitální podpis

- Zaručený digitální podpis je aplikací asymetrické kryptografie (tj. kryptografie s veřejným klíčem).
- Principem běžného digitálního podpisu je zašifrování dokumentu soukromým klíčem a jeho následné dešifrování odpovídajícím veřejným klíčem.
- Z praktických důvodů se místo celého dokumentu šifruje pouze jeho hash.
- Algoritmus RSA lze snadno využít pro digitální podpis. Základním principem takového využití je „opačné" použití klíčů než při zašifrování pro utajení.

Zaručený digitální podpis – příklad

- Pokud Alice chce poslat Bobovi podepsanou zprávu, připojí k ní číslo získané zašifrováním haše své zprávy pomocí svého soukromého klíče.
- Bob poté „dešifruje“ podpis pomocí Alicina veřejného klíče a porovná výsledek s hašem zprávy.
- Pokud zpráva nebyla změněna, vyjde stejná hodnot haše.
- Jelikož jediný, kdo zná tajný klíč Alice, je Alice, je tím zaručeno, že ho zašifrovala Alice.

Část III:
Specifika zdravotnických informací z hlediska bezpečnosti a hrozby

Osnova

- Rizika úniku dat
- Zálohování
- Cloudové služby
- Zdravotnická data na Internetu
- Rizika mobilních a bezdrátových technologií
- Internet věcí

Specifika zdravotnických informací

- Jde o důvěrná data podléhající povinné mlčenlivosti (právní i etické)
- Dochází ke zpracování osobních údajů
- Ztrátou nebo narušením integrity dat může dojít k závažnému poškození pacienta

- Související právní úpravy, zákony
  - č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování
  - č. 101/2000 Sb. o ochraně osobních údajů (od 05/2018 + nařízení EU GDPR)
  - č. 181/2014 Sb. o kybernetické bezpečnosti
  - č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce
- Zpřísnění právních úprav a posílená práva pacientů -> atraktivnější podmínky pro útoky na zdravotnická zařízení -> finanční náklady pro poskytovatele péče (náklady na zvyšování zabezpečení, sanaci následků, platby pokut nebo výkupného)

Ochrana poskytovaná ICT

- Řízení přístupu k datům, audit práce (nejen) se zdravotnickou dokumentací
- Zabezpečená nemocniční síť – firewall, antivirus, filtrování webu a aplikací, proaktivní dohled, sondy pro detekci podezřelého provozu
- Kontrolované a šifrované vzdálené připojení – pokud je personálu poskytováno
- DLP (Data Loss Prevention) - kontrola a omezení způsobu nakládání s daty
- Zálohování a replikace, schopnost reálně uskutečnit Disaster Recovery
- Udržování programů a operačních systémů up-to-date
- Vzdělávání zaměstnanců využívající prostředky ICT, kvalifikovaná IT podpora

Rizika úniku dat
Škodlivý software (Malware)

- Existuje pro účely vniknutí do nebo poškození počítačového systému
- Vybrané kategorie:

  - **RANSOMWARE**: znepřístupní data (zašifruje) a požaduje výkupné
  - **SPYWARE**: sbírá data a odesílá je z PC bez vědomí uživatele (Keylogger, …)
  - **BACKDOOR**: umožňuje vzdálené převzetí kontroly nad PC
  - **TROJSKÝ kůň**: navenek neškodný SW, uvnitř obsahující skryté škodlivé funkce
  - **BOTNET agent**: vytváří sítě „zotročených" PC k provádění škodlivé činnosti (rozesílání spamů, odstavení internetových služeb – DoS útoky)

- **Malware, který obtěžuje, ale jinak obvykle neškodí: SPAM, ADWARE, …**

Rizika úniku dat
Sociální inženýrství

- Aneb proč se obtěžovat s používáním brutální síly na prolamování hesel, nebo plýtvat jinou invencí k získání potřebných informací…
- … když nejslabším článkem zabezpečení je člověk
- Existuje řada dobrých důvodů, nad kterými uživatel prakticky nepřemýšlí a udělá to, co po něm útočník chce, zvláště když je pod tlakem

Jeden z nejznámějších hackerů Kevin Mitnick:
„Když jsem získával od firem hesla a jiné citlivé informace, představil jsem se jako někdo jiný a prostě jsem o ně požádal.“

Rizika mobilních a bezdrátových technologií
Odposlech a šifrování

- Nezabezpečené sítě je možné snadno odposlouchávat
- Sítě zabezpečené pomocí WEP šifrování lze snadno prolomit, v řádu minut
- Na odposlech i prolomení šifrování existují volně dostupné programy a popsané postupy, útočník nemusí disponovat zvláštními IT znalostmi

Prevence:

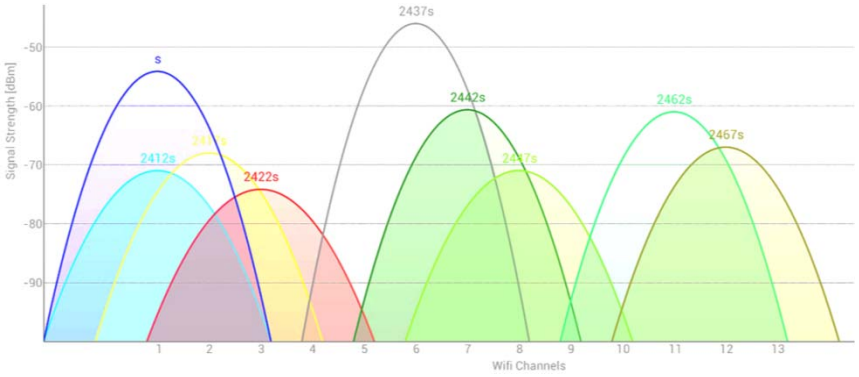
- Eliminace připojení k nezabezpečeným sítím
- Šifrovaná komunikace – https, VPN, …
- Použití zabezpečení WPA/WPA2 s dostatečně složitým klíčem

Rizika mobilních a bezdrátových technologií
Rušení v ISM pásmu

- Standardy Wi-Fi, Bluetooth nebo ZigBee pracují ve volném pásmu 2,4 GHz, kde může docházet k vzájemnému rušení různých technologií i provozovatelů
- Rušení se obvykle projevuje snížením propustnosti v důsledku chybovosti a následného opakování přenosu, nebo nestabilitou

Prevence:

- Průzkum radiového okolí a vhodné frekvenční plánování
- Ve velkých zařízeních použití profesionálních technologií s centrálním řízením
- **Použití bezdrátových zařízení jen tam, kde to má skutečně smysl !**



Internet věcí

- Rozšíření možností běžně využívaných věcí za pomoci připojení k Internetu nebo vzájemnou komunikací s jinými zařízeními
- Vývoj HW - levné, miniaturní a dobře dostupné řídící a komunikační moduly (Arduino apod.)
- Tato zařízení však s sebou nesou také zvýšenou zranitelnost
- Příklady využití:

Intelegentní domácnosti (chytrá elektroinstalace) - adaptivní systémy a vzdálené ovládání domu (vytápění, klimatizace,ventilace, osvětlení), zabezpečení, reporting

Využití pro koncept Smart Cities – zastávky MHD, parkoviště, kontejnery, měření kvality ovzduší, lampy, monitorace elektrických i vodovodních sítí,…

Internet věcí
Využití v nemocnici – chladnička na léky

- Požadavek - skladování léků v teplotně stabilním prostředí, s kontrolovaným přístupem a automatickým měřením teploty s možností alarmování
- Využití běžné (levné) chladící vitríny
- **Internet věcí:**
  Rozšíření o řídící a komunikační jednotku
  - komunikace se serverem a integrace s personálním SW
  - přístup na čipovou kartu (RFID) - ovládání zámku
  - měření teploty v pravidelných intervalech