Předmět:	**IS veřejné správy a sociálních služeb**
Téma:	**Bezpečnost ISVS, ochrana osobních údajů**

Vyučující:	dr.Blahuta, dr.Kajzar	Školní rok:2021

Obsah:

1. Základní bezpečnostní legislativa

Základní legislativa k bezpečnosti IS/IT:

- Nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu (eIDAS),
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů (GDPR)
  - GDPR - General Data Protection Regulation,
  - vstoupilo v účinnost 25. 5. 2018,
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů,
- Zákon č. 480/2004 Sb., o některých službách informační společnosti,
- Zákon c. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti,
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti,
- Zákon č. 40/2009 Sb., trestní zákoník.

Technické normy:

- ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky,
- ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací,
- ČSN ISO/IEC 27005:2009 – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.

2. Nařízení Evropské unie „eIDAS“

eIDAS (e-ID And Signature):

- je zkratka pro nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu,
- k nařízení existují Prováděcí nařízení Komise (EU) 2015/1501 a 2015/1502, obě ze dne 8. září 2015,
- požadavky uvedené v eIDAS jsou všechny členské státy EU povinny dodržovat od 1.7.2016.

Nařízení vytvořilo standardy pro:

- elektronické podpisy, kvalifikované digitální certifikáty, elektronické pečeti, časová razítka a další způsoby ověření autentizačních mechanismů,
- tyto standardy umožňují, aby elektronická transakce měla stejné právní postavení jako transakce prováděná na papíře,
- k nařízení existují Prováděcí nařízení Komise (EU) 2015/1501 a 2015/1502, obě ze dne 8. září 2015.

Nařízení vytváří právní prostředí pro:

- zaručený elektronický podpis
  - elektronický podpis se považuje za zaručený, pokud splňuje požadavky směrnice,
  - tj. poskytuje jedinečné identifikační údaje, které ho spojují s podepisující osobou,
  - podepisující osoba má výlučné užití údajů použitých pro vytvoření elektronického podpisu a musí být schopna rozpoznat případnou změnu dat provedenou po podpisu,
- kvalifikovaný digitální certifikát pro elektronický podpis

    - elektronický doklad, který potvrzuje totožnost uživatele a spojuje data, která potvrzují platnost elektronického podpisu s danou osobou,
    - potvrzení o pravosti uznávaného elektronického podpisu, které bylo vydáno kvalifikovaným poskytovatelem důvěryhodných služeb,
- důvěryhodnou službu
    - elektronická služba, která vytváří, potvrzuje a ověřuje elektronické podpisy, časová razítka, pečetě a certifikáty,
    - důvěryhodná služba nadto může ověřovat webové stránky a uchovávat vytvořené elektronické podpisy, certifikáty a pečeti,
    - službu zajišťuje certifikační autorita,
- subjekty pro posuzování shody, tzv. CAB (Conformity Assessment Bodies)
    - organizace, jejichž úkolem je odborné posuzování jednotlivých poskytovatelů služeb vytvářejících důvěru.

Text nařízení eIDAS:

- https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910

3. Ochrana osobních údajů - GDPR

Ochrana osobních údajů:

- Úřad pro ochranu osobních údajů (ÚOOÚ)
    - https://www.uoou.cz/
    - https://lepsi-reseni.cz/ochrana-osobnich-udaju-gdpr/
- původní zákon o ochraně osobních údajů
    - zákon č. 101/2000 Sb., o ochraně osobních údajů,
    - novelizován zákonem č. 432/2004,
    - https://business.center.cz/business/pravo/zakony/oou/
- GDPR - General Data Protection Regulation
    - nařízení Evropského parlamentu a Rady EU č. 2016/679,
    - s platností od 25.5.2018 (!),
    - nahrazuje zákon č. 101/2000 Sb., o ochraně osobních údajů.

GDPR (General Data Protection Regulation):

- nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů,
- vztahuje se na všechny subjekty zpracovávající osobní údaje občanů EU,
- části GDPR nařízení se nevztahují na organizace s méně než 250 zaměstnanci v případě, že hlavní činností není zpracování citlivých údajů či velký rozsah zpracování,

Účel nařízení GDPR:

- chránit osobní údaje (soukromí) fyzických osob,
- poskytnout práva fyzických osob rozhodovat o zpracování svých osobních údajů.
- dát možnost významně pokutovat organizace za nedodržení nařízení.

Informace k GDPR:

- https://www.gdpr.cz/gdpr/
- https://lepsi-reseni.cz/ochrana-osobnich-udaju-gdpr/

Fyzická osoba:

- musí být tím, kdo rozhoduje o svých osobních údajích,
- má právo vědět, jaké osobní údaje o ní organizace uchovává a za jakým účelem,
- musí mít právo na výmaz, opravu či přenos svých osobních údajů,
- musí dávat souhlas ke zpracování svých osobních údajů pro konkrétní účely,
- má mít plnou kontrolu nad svými osobními údaji.

Správci a zpracovatelé osobních údajů:

- musí být schopni fyzické osobě sdělit, k jakému účelu jsou její osobní údaje využívané,
- musí reagovat na připomínky fyzické osoby,
- nesou odpovědnost za nedovolené zpracování či únik osobních údajů,
- v případě úniku osobních dat musí včas informovat fyzickou osobu i příslušný dozorový úřad.

Organizace / firma musí:

- vést evidenci účelu zpracování osobních údajů,

- vědět, kde všude má os. údaje (OÚ) uložené,
- být schopna zobrazit uživateli přehled všech jeho evidovaných OÚ,
- zpracovat žádost o opravu či výmaz OÚ,
- zpřístupnit OÚ pro přenos a logovat veškeré přenosy osobních údajů,
- přiřadit příznak omezení zpracování a blokovat OÚ v systému,
- vytvořit a zpětně doložit průběh odsouhlasení, uložení, ochrany a likvidace OÚ.

Možné sankce:

- varování,
- napomenutí,
- pozastavení možnosti zpracovávat osobní údaje,
- pokuta až 10-20 mil. Euro, nebo 2-4% obratu.

Osobním údajem je:

- podle zákona č. 101/2000 Sb., o ochraně osobních údajů
  - jakákoliv informace týkající se určené nebo určitelné fyzické osoby, k níž se osobní údaje vztahují,
- fyz. osoba se považuje za určenou nebo určitelnou
  - jestliže lze fyzickou osobu přímo či nepřímo identifikovat,
  - zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro její fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

ÚOOÚ rozlišuje následující kategorie:

- adresní a identifikační údaje
  - např. jméno, příjmení, datum a místo narození, rodinný stav, rodné číslo,
  - státní příslušnost, adresa trvalého bydliště,
  - telefonní spojení domů, do zaměstnání apod.,
- citlivé údaje
  - údaje vypovídající o národnostním, rasovém nebo etnickém původu,
  - členství v odborových organizacích,
  - o odsouzení za trestný čin, sexuálním životě, genetickém údaji,
  - o politických postojích, náboženství a filosofickém přesvědčení,
  - o zdravotním stavu nebo biometrickém údaji,

- popisné údaje
  - např. vzdělání, znalost cizích jazyků, odborné znalosti a dovednosti,
  - počet dětí,
  - obrazový záznam z kamerového systému,
  - vojenská služba, předchozí zaměstnání, mzda,
  - zdravotní pojišťovna, číslo cestovního dokladu, bankovní spojení apod.,
- údaje o jiné osobě
  - např. adresní a identifikační údaje člena rodiny, manžel/manželka, dítě apod.

Příklady obecných údajů osobních a citlivých:

- (tj. fyz. osoba by měla být informována, že organizace tyto údaje o ní vede),

jméno a příjmení, adresa, pohlaví, věk, datum narození, místo narození, rodné číslo, osobní stav, zdravotní znevýhodnění, fotografie, videozáznamy, audiozáznamy,	e-mailová adresa, obsahuje-li jméno, telefonní číslo, číslo OP, ŘP, pasu, ... údaje o dětech a manželce, mzda, důchod, vzdělání, kulturní profil, ...

Příklady zvláštních údajů, které považujeme za citlivé:

rasový či etnický původ, politické názory, náboženské či filozofické vyznání, členství v odborech, zdravotní stav, sexuální orientace,	trestní delikty a pravomocná odsouzení, genetické informace, krevní skupina, biometrické údaje - snímek obličeje, otisky prstů, podpis, hlas, ...

Uživatel (původce) informací klasifikuje informace do kategorií:

- utajované informace
  - zák. č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti,
- informace zvláštní skutečnosti
  - zák. č. 240/2000 Sb., o krizovém řízení,
- citlivé informace
  - zák. č. 101/2000 Sb., o ochraně osobních údajů,

- obchodní tajemství
    - zák. č. 89/2012 Sb., občanský zákoník.

Pověřenec pro ochranu OÚ:

- tzv. DPO (Data Protection Officer),
- osoba s odbornými znalostmi v oblasti právních předpisů a postupů týkajících se ochrany údajů,
- úkoly DPO
    - monitorování souladu zpracování OÚs povinnostmi vyplývajícími z nařízení,
    - provádění interních auditů,
    - školení pracovníků,
    - celkové řízení agendy interní ochrany dat,
- DPO nenese osobní odpovědnost za nedodržování GDPR,
- funkci DPO je možné vykonávat na základě smlouvy o poskytování služeb uzavřené s jednotlivcem nebo externí organizací,
- při výkonu svých úkolů je DPO vázán mlčenlivostí v souladu s právem EU nebo členských států EU,
- GDPR vyjmenovává případy, kdy je povinnost DPO jmenovat.

4. Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti:

- zákon č. 181/214 Sb., o kybernetické bezpečnosti,
- https://www.nbu.cz/cs/pravni-predpisy/1091-zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/

Účel zákona o KB:

- vynutit plnění požadavků na bezpečnost poskytovaných služeb ze strany poskytovatelů el. služeb.

Zákon o KB obsahuje:

- vymezení subjektů, na které se zákon vztahuje,
- vymezuje bezpečnostní opatření k zajištění bezpečnosti informací,
- definuje pojmy

    - kybernetická bezpečnostní událost (KBU),
    - kybernetický bezp. incident (KBI),
- stanovuje povinnost hlášení KBU a KBI Národnímu bezpečnostnímu úřadu,
- prováděcí právní předpis stanoví
    - typy a kategorie kybernetických bezpečnostních incidentů,
    - náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.

Orgány a osobami, kterým se ukládají povinnosti v oblasti KB, jsou:

- poskytovatel služby elektronických komunikací,
- subjekt zajišťující síť elektronických komunikací,
- orgán nebo osoba zajišťující významnou kom. síť,
- správce a provozovatel IS kritické informační infrastruktury,
- správce a provozovatel komunikačního systému kritické informační infrastruktury,
- správce a provozovatel významného informačního systému.

Kybernetická bezpečnostní událost:

- je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo
- bezpečnosti a integrity sítí elektronických komunikací.

Kybernetický bezpečnostní incident:

- je narušení bezpečnosti informací v informačních systémech,
- nebo narušení bezpečnosti služeb,
- anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

Bezpečnostními opatřeními jsou:

- technická opatření,
- organizační opatření.

Technickými opatřeními jsou:

- fyzická bezpečnost,
- nástroj pro ochranu integrity komunikačních sítí,

- nástroj pro ověřování identity uživatelů,
- nástroj pro řízení přístupových oprávnění,
- nástroj pro ochranu před škodlivým kódem,
- nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,
- nástroj pro detekci kybernetických bezpečnostních událostí,
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- prostředky pro zajištění aplikační bezpečnosti,
- kryptografické prostředky,
- nástroj pro zajišťování úrovně dostupnosti informací,
- bezpečnost průmyslových a řídicích systémů.

Organizačními opatřeními jsou:

- bezpečnostní politika (dokument),
- organizační bezpečnost,
- stanovení bezpečnostních požadavků pro dodavatele,
- systém řízení bezpečnosti informací,
- řízení rizik,
- řízení aktiv,
- bezpečnost lidských zdrojů,
- řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,
- řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,
- vývoj a údržba kritické informační infrastruktury a významných informačních systémů,
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- řízení kontinuity činností,
- kontrola a audit kritické informační infrastruktury a významných informačních systémů.

5. Dopady těchto předpisů na IS organizací

GDPR - IS organizací musí být schopné:

- zajistit ochranu osobních údajů podle nařízení EU a návazných předpisů,
  - aplikace pro evidenci účelu zpracování osobních údajů fyz. osob,
  - tj. zaměstnanců, zákazníků, ...
- po obdržení žádosti fyzické osoby
  - zpracovat přehled osobních údajů fyzické osoby a účel jejich zpracování,
  - provést výmaz osobních údajů fyzické osoby,
  - zpracovat výstup osobních údajů fyzické osoby pro jejich přenos jinému zpracovateli,
  - aplikační podpora uvedených úkonů (!)
- umožnit úkony pověřence pro ochranu OÚ
  - aplikace pro podporu práce Pověřence.

KB – požadavky na řízení IS:

- provedení revize nastavení (konfigurace) všech komponent IS
  - síťové prvky, aplikační servery, databázové servery, OS,
- rekonfigurace komponent IS,
- nasazení systémů pro detekce kybernetických útoků,
- monitorovací systémy stavu provozovaných IS/IT,
- auditní systémy – sledování činností uživatelů v IS,
- systémy pro analýzy a vyhodnocování událostí v IS.

Nasazení systémů IDS/IPS:

- Intrusion Detection System / Intrusion Prevention Systems,
- systémy pro detekci a prevenci průniků,
- monitorují provoz systému (počítačová síť, operační systémy),
- snaží se odhalit (detekovat) podezřelé a neobvyklé aktivity,
  - např. pokusy o průniky do podnikové sítě, podnikového IS, ...
- zaznamenávají průběh neobvyklých aktivit,
- zasílají oznámení (hlášení, poplach) výskytu těchto činností,

- blokují podezřelé aktivity,
- jsou považovány za druhou ochrannou linii podnikových IS,
- v podnikové síti jsou umístěné za firewally,
- rovněž na kritických místech sítě – tj. před klíčovými podnikovými IS.

Napojení podnikových IS na SIEM:

- SIEM (Security Information and Event Management),
- viz https://cs.wikipedia.org/wiki/SIEM,
- jde o management bezpečnostních informací a událostí v prostředí podnikových IS/IT,
- řešení SIEM je postaveno na bázi aplikace, která
  - stahuje z jiných aplikací (jejich alert či audit logů) informace,
  - nad takto získanou databází pak provádí analýzy a generuje reporty,
- SIEM v reálném čase provádí analýzu bezpečnostních alertů, které generují komponenty podnikových IS/IT
  - monitorování činnosti zařízení či konkrétního uživatele, ...
  - analýzy provozu IS a nalézání vzájemných vztahů událostí (korelace),
  - zasílání varování (alerting),
  - informační panely, přehledové sestavy (dashboards),
  - reportování shod (compliance),
  - zachování, ukládání historických dat (logů).

6. Podpůrné komunikační prostředky v ISVS

Elektronický podpis:

- umožňuje ověřenou komunikaci občana s úřadem,
- ekvivalent podpisu vlastnoručního,
- jednoznačný údaj spojený s datovou zprávou a jejím odesilatelem,
- je určen pouze pro fyzické (nikoliv právnické) osoby,
- prakticky se jedná o určitý řetězec znaků,
- související pojmy
  - privátní a veřejný klíč, certifikát, certifikační autorita,
  - otisk (hash) datové zprávy, šifrování,
- podpis obyčejný (komerční certifikát) a zaručený (kvalifikovaný certifikát).

Elektronický podpis zaručuje:

- autentičnost
  - dokument podepsala daná jednoznačně identifikovatelná osoba,
- integritu zprávy
  - nedošlo k následné změně zprávy,
- nepopiratelnost zprávy
  - podpis zprávy jako vědomý akt podepsaného.

Komerční certifikát:

- certifikáty, které nejsou spjaty se zákonem o elektronickém podpisu,
- vystavuje je certifikační autorita, která ověří žadatele dle svých vlastních směrnic,
- nemusí striktně splňovat náležitosti zákona o elektronickém podpisu,
- je jen na dané certifikační autoritě jaké si stanoví podmínky,
- velmi široké uplatnění - šifrování e-mailů, zajištění autentizace či k elektronickému podepisování zpráv,
- komunikující strany musí však být za jedno s důvěrou danému certifikátu dané certifikační autority.

Kvalifikovaný certifikát:

- má náležitosti podle §12 zákona č. 227/2000 Sb., o elektronickém podpisu,
- jsou určeny výhradně pro elektronické podepisování (nikoliv například pro šifrování),
- určen pro oficiální komunikaci se subjekty státní správy, pojišťovnami apod.,
- vydává tzv. kvalifikovaná certifikační autorita,
- bezpečnost a důvěryhodnost těchto certifikačních autorit je kontrolována a standardizována příslušnými úřady.

Elektronická značka:

- elektronické časové razítko,
- založená na systémovém certifikátu vydaném akreditovanou certifikační autoritou,
- je obdobou el. podpisu, ale pro právnické osoby,
- spojení datové zprávy s časovým okamžikem a právnickou osobou,
- důkaz, že daný dokument existoval v daný časový okamžik,

- je poskytnuté důvěryhodným subjektem (třetí strana) – jehož certifikát a nastavení času respektujeme.

Elektronická podatelna:

- pracoviště pro příjem a odesílání zpráv občan-úřad,
- jednotný komunikační bod s orgánem veřejné správy,
- vazba na spisovou službu organizace – evidence, uložení, archivace, skartace.

Podrobněji k tématům bezpečnostních technologií:

- šifrování, elektronický podpis, ...
- zálohování dat,
- viz předmět Bezpečnost informačních systémů.

7. Shrnutí k tématu

Hlavní body tématu:

- základní bezpečnostní legislativa ISVS
- nařízení EU eIDAS – standardy pro el. transakce (el. podpis, certifikáty, ...),
- ochrana osobních údajů a GDPR - práva a povinnosti plynoucí z GDPR,
- zákon o kybernetické bezpečnosti (KB),
- dopady uvedených předpisů na IS organizací,
- podpůrné komunikační prostředky v ISVS.

8. Otázky k procvičení

1) Vyjmenujte aspoň tři zákony ČR či nařízení EU vztahující se k bezpečnosti IS/IS.
2) Co je to eIDAS a která témata zahrnuje?
3) Co rozumíme pod pojmem osobní údaj? Uveďte příklady.
4) Vysvětlete cíle nařízení GDPR.
5) Jaká práva plynou z GDPR pro fyzické osoby?
6) Jaké povinnosti plynou z GDPR pro zpracovatele osobních údajů?
7) Co je účelem zákona o kybernetické bezpečnosti?
8) Jaké vidíte dopady GDPR na podnikové IS?
9) Jaké požadavky na IS organizací mohou plynout ze zákona o KB?
10) K čemu slouží elektronický podpis, elektronická značka a elektronická podatelna?

11) Co je to certifikát a jaký je rozdíl mezi komerčním a kvalifikovaným certifikátem?