Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Legislatíva a etika

Ivan Oravec, Jozef Stanko

KPMG
cutting through complexity™

Úvod

- Ochrana informácií a IKT, prostredníctvom ktorých sa tieto informácie spracovávajú, prenášajú alebo v nich ukladajú, si okrem štandardizácie a technických noriem vyžaduje aj ochranu na úrovni legislatívy ES a zároveň aj na úrovni legislatívy príslušných štátov.
- Vhodný a efektívny právny rámec je prvým nutným a kľúčovým, nie však postačujúcim, predpokladom zabezpečenia primeranej ochrany práv jednotlivca a organizácií, či už súkromného alebo verejného sektora.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Potláčanie kriminality vs. štandardizácia IB

- Až na základe leg. rámca môžeme povedať, že prípadné zneužitie IKT je protiprávne a zároveň môžeme v takomto prípade zasiahnuť a vyvodiť zodpovednosti a príslušné sankcie.
- Práve možné sankcie definované v príslušnom právnom rámci môžu pôsobiť aj ako odradzujúci účinok pre potenciálnych útočníkov od budúcich pokusov o narušenie alebo zneužitie IKT.
- Legislatíva SR však nie je zameraná len na potláčanie kriminality použitím trestného zákona a trestného poriadku, ale definuje tiež konkrétne podmienky štandardizácie informačnej bezpečnosti a riadenia bezpečnosti informačných a komunikačných technológií digitálneho priestoru.
- Tieto podmienky ozrejmujú práva a povinnosti používateľov, prevádzkovateľov a sprostredkovateľov služieb.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Oblasti riadenia IB podľa ISO 2700x

- Bezpečnostná politika
- Organizácia informačnej bezpečnosti
- Manažment aktív
- Bezpečnosť ľudských zdrojov
- Fyzická bezpečnosť a bezpečnosť prostredia
- Manažment komunikácie a prevádzky
- Manažment prístupu
- Obstarávanie, vývoj a údržba informačných systémov
- Manažment incidentov informačnej bezpečnosti
- Manažment kontinuity činnosti spoločnosti
- Súlad

KPMG
cutting through complexity™

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Oblasť „Súlad“ (1/2)

- **A.15.1 Súlad so zákonnými požiadavkami**
- **Cieľ manažmentu:** Vyhnúť sa porušeniam akýchkoľvek právnych, štatutárnych, regulačných alebo zmluvných záväzkov a akýchkoľvek bezpečnostných požiadaviek.

- Identifikácia platnej legislatívy
  - Všetky významné štatutárne, regulačné a zmluvné požiadavky a prístup organizácie na dosiahnutie týchto požiadaviek musia byť explicitne definované, dokumentované a udržiavané v aktuálnej podobe pre každý informačný systém a organizáciu ako celok.
- Práva duševného vlastníctva
  - Musia sa implementovať vhodné procedúry, ktoré by zabezpečili súlad so zákonnými, regulačnými a zmluvnými požiadavkami o používaní materiálu v zmysle práv duševného vlastníctva a použitia značkou chránených softvérových produktov.
- Zabezpečenie záznamov organizácie
  - Dôležité záznamy organizácie musia byť chránené pred stratou, zničením a falzifikáciou v súlade so štatutárnymi, regulačnými, zmluvnými alebo podnikovými požiadavkami.
- Ochrana dát a utajenie osobných informácií
  - Ochrana a utajovanie dát musia byť zaisťované ak sú vyžadované zákonmi a vyhláškami a ak sa to vyžaduje požiadavkami zahrnutými do zmluvy.
- Predchádzanie zneužívaniu prostriedkov spracúvajúcich informácie
  - Používatelia musia byť odrádzaní od použitia prostriedkov na spracovanie informácií na neautorizované účely.
- Regulácia kryptografických opatrení
  - Musia byť zavedené kryptografické opatrenia s cieľom dosiahnuť súlad so všetkými platnými dohodami, zákonmi a vyhláškami.

KPMG cutting through complexity™

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Oblasť „Súlad“ (2/2)

- **A.15.2 Súlad s bezpečnostnými politikami, normami a technický súlad**
- **Cieľ manažmentu:** Zaistiť súlad systémov s bezpečnostnými politikami a normami organizácie.

- A.15.2.1 Súlad s bezpečnostnými politikami a normami
  - Manažéri musia konať s cieľom zaisťovať, aby všetky bezpečnostné procedúry v rámci ich oblasti zodpovednosti sa vykonávali správne s cieľom zaistiť súlad s bezpečnostnými politikami a normami.
- A.15.2.2 Kontrolovanie technického súladu
  - Informačné systémy musia byť pravidelne kontrolované z hľadiska súladu s normami na implementáciu bezpečnosti.

- **A.15.3 Hľadiská auditu systému**
- **Cieľ manažmentu:** Maximalizovať efektívnosť procesov auditu systému a minimalizovať ich negatívne vplyvy, podobne ako aj negatívne vplyvy na ne pôsobiace.

- A.15.3.1 Opatrenia auditu informačného systému
  - Požiadavky na audit a aktivity zahŕňajúce kontroly prevádzkovaných systémov musia byť starostlivo plánované a odsúhlasené, aby sa minimalizovalo riziko prerušení podnikových procesov.
- A.15.3.2 Ochrana nástrojov auditu informačných systémov
  - Prístup k nástrojom auditu informačných systémov musí byť chránený, aby sa predišlo možnému zneužitiu alebo kompromitovaniu.

KPMG cutting through complexity™

Osnova (1/2)

- **Tri základné časti:**
  I. Identifikácia definícií, práv, povinností a prípadných sankcií vyplývajúcich zo všeobecnej legislatívy, týkajúcej sa IB z trestného zákona, trestného poriadku a autorského zákona.
  II. Špecializovaná legislatíva už priamo rieši a štandardizuje IB v jej príslušných oblastiach. Ide najmä o predpisy týkajúce sa ISVS, OOÚ a kritickej infraštruktúry.
  III. Špecifické právne predpisy, ktoré už neštandardizujú problematiku IB ako takú, ale obsahujú určité prvky a požiadavky na používateľov a prevádzkovateľov, či už z pohľadu zabezpečenia IB alebo z pohľadu riadenia IB. Ide o predpisy týkajúce sa EP, ochrany US, elektronického obchodu, elektronických komunikácií a poskytovania zdravotnej starostlivosti.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Osnova (2/2)

- **<u>Ďalšie časti:</u>**
  IV. Prehľad legislatívy EÚ, ktorá ma rovnako vzťah a súvis s IB
  V. Vnútorná legislatíva organizácie v oblasti riadenia IB
  VI. Anonymita a súkromie vs. monitorovanie zamestnancov
  VII. Etika a morálny kódex
  VIII. Verejné obstarávanie IKT
  IX. Forenzná analýza

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

I. časť

TRESTNÝ ZÁKON, TRESTNÝ PORIADOK A AUTORSKÝ ZÁKON

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad všeobecnej legislatívy vzťahujúcej sa na IB (1/4)

Problémy, resp. výzvy dnešného sveta:

- Jednou z komplikácií, ktorú je potrebné riešiť pri vytváraní právnych predpisov v tejto oblasti je definovanie „hmotných“ pravidiel pre akúsi virtuálnu sieť, keďže pojmy používané v informačnej bezpečnosti podliehajú určitej „virtuálnosti“ a teda nemajú charakter fyzického prvku.
- Rovnako pôsobnosť a kompetencie jednotlivých štátov, resp. príslušných orgánov činných v trestnom konaní je geograficky obmedzená, čo vo virtuálnom svete nie je možné zabezpečiť.
- Aj napriek skutočnosti, že napr. §10 ods. 9 Trestného poriadku definuje možnosť vytvorenia spoločného „medzinárodného“ vyšetrovacieho tímu, určiť geografické „miesto činu“ vo virtuálnom svete, a geografické miesto odkiaľ bol tento čin spáchaný a jeho jednoznačné priradenie konkrétnym orgánom konkrétnej krajiny, je v súčasnosti, vo väčšine prípadov, nemožná úloha.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad všeobecnej legislatívy vzťahujúcej sa na IB (2/4)

Internetové právo:

- Najviac definícií pojmov a právnych vzťahov vo všeobecnej rovine možno nájsť v občianskom práve – ale nie je v ňom zvláštna časť, ktorá by vymedzovala konkrétne aktivity na internete.
  - Občiansky zákonník – pojmy ako spôsobilosť k právnym úkonom, ochrana dobrej viery, ochrana práv tretích osôb, alebo tiež zásada, že „všetko čo je dovolené, nie je zakázané“, základné práva a povinnosti, charakteristika občiansko-právnych vzťahov.
- Trestné právo, pod ktoré spadá trestný zákon a trestný poriadok a samostatne stojaci autorský zákon.
  - najmä právne vzťahy súvisiace s počítačovými programami, licenčné zmluvy týkajúce sa softvéru, definícia osoby s právami k rozmnoženine počítačového programu a pod.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad všeobecnej legislatívy vzťahujúcej sa na IB (3/4)

Trestný zákon (zákon č. 300/2005 Z. z.):

- Čo určuje?
  - **Druh a výšku trestov** za (predovšetkým) úmyselné a spoločensky škodlivé činy (ale aj činy z nedbanlivosti).
- Zaoberá sa aj tzv. **hmotným trestným právom**
  - hovorí, **aké konanie je trestné**, **aké sankcie je možné vyvodiť** z takéhoto konania a **aké opatrenia možno použiť** proti páchateľom trestných činov (podmienky pre vyvodenie trestnej zodpovednosti, druhy trestov, druhy ochranných opatrení, ukladanie trestov a definícia skutkových podstát trestných činov)

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad všeobecnej legislatívy vzťahujúcej sa na IB (4/4)

Trestný poriadok (zákon č. 301/2005 Z. z.):

- Čo rieši?
  - Na rozdiel od trestného zákona rieši najmä tzv. **procesný rámec.**
- Čo sa myslí pod procesným rámcom?
  - Definovanie postupov orgánov činných v trestnom konaní pri vyšetrovaní trestných činov a tiež práva a povinnosti osôb, ktoré sa na trestnom konaní zúčastňujú.

KPMG
cutting through complexity™

Trestný zákon (1/6)

- Časová pôsobnosť
  - trestnosť činu sa posudzuje podľa zákona účinného v čase, kedy bol čin spáchaný
  - pokiaľ od času, kedy bol trestný čin spáchaný do času, kedy sa vynáša rozsudok nadobudnú činnosť viaceré zákony, trestnosť činu sa posudzuje podľa toho zákona, ktorý je pre páchateľa priaznivejší
- Územná pôsobnosť
  - iba pre posudzovanie trestného činu spáchaného (alebo aspoň čiastočne spáchaného) na území SR
- Osobná pôsobnosť
  - Jedná sa buď o páchateľa, ktorý je občanom SR, alebo má na území SR trvalý pobyt alebo sa posudzuje trestný čin spáchaný proti SK občanovi (a to aj v prípade, ak je v mieste spáchania činu tento čin trestný a aj v prípade, ak v mieste jeho vykonania nepodlieha žiadnemu postihu vyplývajúcemu z miestneho zákona).

Trestný zákon (2/6)

Druhy trestných činov:

- **Prečin**
  - Čin spáchaný **z nedbanlivosti**. Ide o čin, ktorého trest je podľa tohto zákona ustanovený na odňatie slobody na **menej ako 5 rokov.**
- **Zločin**
  - Bol spáchaný **úmyselne** a je podľa tohto zákona potrestaný odňatím slobody na **viac ako 5 rokov**.
- **Obzvlášť závažný zločin**
  - Za obzvlášť závažný zločin sa považuje taký zločin, ktorý je podľa ustanovenia tohto zákona potrestaný odňatím slobody **s dolnou hranicou sadzby 10 rokov.**

Trestný zákon (3/6)

- Miesto spáchania trestného činu:
  - Každé miesto na ktorom páchateľ konal, nastal v ňom, alebo podľa predstavy páchateľa mal nastať trestný čin.
- Príprava na zločin:
  - Konanie, ktoré spočíva v organizovaní zločinu, zadovažovaní nástrojov na jeho spáchanie, v spolčovaní sa s nebezpečnými skupinami za účelom jeho spáchania aj v prípade, ak k nemu nedôjde.
  - Trestnosť zaniká, ak páchateľ upustil od ďalšieho konania smerujúceho k zločinu, alebo urobil o príprave na trestný čin oznámenie orgánu činnému v trestnom konaní, alebo Policajnému zboru.
- Pokusom trestného činu je:
  - Konanie, ktoré priamo smeruje k jeho dokonaniu, ak k nemu v konečnom dôsledku nedôjde.
  - Je trestný podľa sadzby ustanovenej na dokonaný trestný čin.
  - Ak však páchateľ upustí od trestného činu a odstráni nebezpečenstvo plynúce z podniknutej prípravy, trestnosť prípravy zaniká.
  - Ustanovením o trestnosti pokusu o trestný čin nie je dotknutá trestnosť iného činu, ktorý páchateľ týmto pokusom spáchal.

Trestný zákon (4/6)

- Zavinenie :
  - Trestný čin je spáchaný úmyselne, ak páchateľ chcel spôsobom uvedeným v zákone porušiť, alebo ohroziť záujem chránený týmto zákonom, prípadne vedel, že svojim konaním môže také porušenie, alebo ohrozenie spôsobiť.
  - Z nedbanlivosti, ak si páchateľ uvedomuje, že svojim konaním môže porušiť, alebo ohroziť chránený záujem, alebo ak páchateľ nevie, že svojim konaním môže spôsobiť porušenie, alebo ohrozenie, ale by o tom vzhľadom na svoje osobné pomery a okolnosti vedieť mohol.
  - Pre trestnosť činu je potrebné úmyselné zavinenie, pokiaľ zákon neustanoví inak.
  - Ťažší následok sa považuje za priťažujúcu okolnosť, alebo za okolnosť, ktorá vyžaduje použitie vyššej trestnej sadzby.

Trestný zákon (5/6)

- Páchateľ, spolupáchateľ a účastník trestného činu:
  - Páchateľ je ten, kto trestný čin spáchal sám.
  - Dve, alebo viaceré osoby sa považujú za spolupáchateľov.
  - Účastníkom na dokonanom trestnom čine je organizátor, návodca, objednávateľ alebo pomocník.
    - Organizátor zosnoval spáchanie trestného činu, návodca naviedol iného na spáchanie trestného činu, objednávateľ požiadal iného na spáchanie trestného činu a pomocník poskytol inému pomoc, najmä zadovážením prostriedkov odstránením prekážok, radou, utvrdzovaním v predsavzatí alebo sľubom pomôcť po trestnom čine a pod.
    - Účastník by mal byť potrestaný rovnakým trestom ako páchateľ.

Trestný zákon (6/6)

- Okolnosti vylučujúce trestnú zodpovednosť:
  - Pokiaľ páchateľ nedovŕšil štrnásty rok života, nie je trestne zodpovedný.
  - Rovnako nie je trestne zodpovedný nepríčetný páchateľ trpiaci duševnou poruchou, ktorá mu znemožňuje rozpoznať protiprávnosť trestného činu, alebo ovládať svoje konanie.
- Súhlas poškodeného:
  - Čin inak trestný je akceptovaný ako nie trestný, pokiaľ je vykonaný s vážnym a dobrovoľným súhlasom poškodeného a nie je namierený proti jeho životu, alebo zdraviu.
  - **V prípade informačnej bezpečnosti môžeme toto znenie aplikovať napríklad na spísanie zmluvy alebo protokolu o bezpečnostnom zhodnotení zahŕňajúcom napr. penetračné testovanie informačných systémov.**
  - **V zmluve by malo byť stanovené, do akej hĺbky, v akom rozsahu a v akej maximálnej „agresivite“ môžu byť penetračné testy prevedené.**

Trestný zákon - Počítačová kriminalita (1/3)

- High-Tech Crime:
  - Využívanie informačných technológií, najmä počítačov na páchanie trestnej činnosti.
  - Jedným z nástrojov na jej potieranie je Dohovor o počítačovej kriminalite z 23. novembra 2001. Slovenská republika tento dohovor ratifikovala v roku 2007.
- Počítačová kriminalita v trestnom zákone :
  - § 247 trestného zákona, do ktorého sú premietnuté princípy Dohovoru o kybernetickom zločine CETS č. 185/2001, vydanom Radou Európy.

Trestný zákon - Počítačová kriminalita (2/3)

- Poškodenie a zneužitie záznamu na nosiči informácií (§247)
  - Odňatím slobody sa potrestá ten, kto v úmysle spôsobiť inému škodu alebo inú ujmu alebo zadovážiť sebe alebo inému neoprávnený prospech **získa neoprávnený prístup do počítačového systému, k inému nosiču informácií** alebo jeho časti a jeho informácie neoprávnene použije, alebo také informácie **neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu**, alebo **urobí zásah do technického alebo programového vybavenia počítača**, alebo **vkladaním, prenášaním, poškodením, vymazaním, znížením kvality, pozmenením alebo potlačením počítačových dát marí funkčnosť počítačového systému** alebo **vytvára neautentické dáta s úmyslom, aby sa považovali za autentické** alebo aby sa s nimi takto na právne účely nakladalo.
  - Táto časť zákona upravuje prípady zneužitia informačného systému ktoroukoľvek zo známych foriem počítačovej kriminality. Všeobecná formulácia tohto odseku pokrýva veľký rozsah počítačovej trestnej činnosti od distribúcie nelegálnych kópií softvéru až po sofistikované formy organizovaného hackingu.

Trestný zákon - Počítačová kriminalita (3/3)

- Poškodenie a zneužitie záznamu na nosiči informácií (§247)
  - Zároveň sa, rovnako ako v predchádzajúcom odseku, potrestá ten, kto na účel spáchania činu uvedeného v predchádzajúcom odseku **neoprávnene sleduje prostredníctvom technických prostriedkov neverejný prenos počítačových dát do počítačového systému, z neho alebo v rámci počítačového systému**, alebo **zaobstará alebo sprístupní počítačový program a iné zariadenia alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do celého počítačového systému** alebo do jeho časti.
  - Znenie tejto časti pokrýva sledovanie, odpočúvanie, alebo iné techniky kompromitácie prenosu dát a pokrýva aj oblasť neoprávnených prístupov do informačných systémov.
  - V tejto časti trestný zákon ošetruje predovšetkým neoprávnenú činnosť zneužitia privilégií a neoprávnený prístup k dátam, ktoré sú viazané na dotknutú osobu v zmysle platného zákona č. 122/2013 o ochrane osobných údajov, prípadne majú inak kritický charakter podľa zákona a ich kompromitácia predstavuje riziko finančnej, alebo hospodárskej straty, prípadne straty renomé.
  - Počítače a IKT vo všeobecnosti môžu byť použité na páchanie širokého spektra trestnej činnosti zahŕňajúceho vydieranie, vyhrážanie, rozširovanie detskej pornografie, páchania drogovej trestnej činnosti, podvodu, terorizmu a pod.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Trestný zákon - Neoprávnené nakladanie s osobnými údajmi

- Citlivo vnímaná téma:
  - Na úrovni trestného zákona najmä § 374, ktorý sa venuje neoprávnenému poskytovaniu, sprístupňovaniu a zverejňovaniu osobných údajov a zároveň aj sankciám, ktoré hrozia v prípade porušenia tohto ustanovenia zákona.
  - Ten, kto neoprávnene poskytne, sprístupní alebo zverejní osobné údaje o inom potrestá sa odňatím slobody až na jeden rok. Na dva roky, ak spáchaným činom spôsobí vážnu ujmu.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Trestný poriadok - Rozsah a postup vyšetrovania

- Vyšetrovanie sa vykonáva predovšetkým o zločinoch a v špeciálnych prípadoch aj o menej závažných prečinoch. Ak je potrebné vykonať vyšetrovanie aspoň o jednom z trestných činov, vykoná sa vyšetrovanie o všetkých trestných činoch toho istého obvineného aj proti všetkým obvineným, ktorých trestné činy súvisia.
- Spoločný postup vo vyšetrovaní nariaďuje, že úkony ktoré sa vykonávajú vo vyšetrovaní vykonáva zodpovedný policajt osobne.
- Postupuje vo vyšetrovaní tak, aby čo najrýchlejšie zadovážil podklady na objasnenie skutku v rozsahu potrebnom na posúdenie prípadu a zistenie páchateľa trestného činu. Policajt vykonáva všetky úkony samostatne v súlade so zákonom a včas.
- Zadovažuje dôkazy bez ohľadu na to, či svedčia v prospech, alebo neprospech obvineného.
- Obvinený nesmie byť k výsluchu nezákonne nútený.
- Na vyšetrovanie prečinov je možné pristúpiť k skrátenému vyšetrovaniu

KPMG
cutting through complexity™

Autorský zákon a oblasť duševného vlastníctva (1/3)

- Autorské právo je upravené autorským zákonom č. 618/2003 Z. z. o autorskom práve a o právach súvisiacich s autorským právom v znení neskorších predpisov.
- Autorské právo a majetkové právo :
  - Zreteľne oddeľuje **autorské práva** od **výhradných majetkových práv** (§ 16 autorského zákona).
  - Osobnostných práv sa autor nemôže vzdať, tieto práva sú neprevoditeľné a smrťou autora zanikajú.
  - Dielo možno po smrti jeho autora použiť vždy len spôsobom neznižujúcim jeho hodnotu a uvedením mena autora, pokiaľ nejde o anonymné dielo.
  - Na rozdiel od osobnostných práv, majetkové práva trvajú počas života autora a **ešte 70 rokov po jeho smrti**.
  - **Autor môže dielo používať a udeľovať iným osobám oprávnenie na výkon tohto práva.**

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Autorský zákon a oblasť duševného vlastníctva (2/3)

- Zákon upravuje dva typy autorskej zmluvy:
  - **Zmluva o vytvorení diela** - zaväzuje autora vytvoriť dielo pre objednávateľa, avšak objednávateľovi nevzniká právo dielo použiť.
  - **Licenčná zmluva** - slúži na účel udelenia práv dielo použiť. Udelením licencie je **autor povinný strpieť zásah do svojho práva**. Existuje možnosť licenciu udeliť bezodplatne, napríklad na charitatívne účely. V licenčnej zmluve je potrebné **vyhradiť spôsob**, alebo spôsoby **použitia diela**. Zákon vyslovene vylučuje, aby bola licenčná zmluva vydaná na spôsob použitia, ktorý v čase uzatvorenia zmluvy ešte nie je známy.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Autorský zákon a oblasť duševného vlastníctva (3/3)

- Majetkové práva pre **zamestnanecké dielo** :
  - Majetkové práva k zamestnaneckému **dielu vlastní zamestnávateľ**, ak nie je dohodnuté inak.
  - Zamestnávateľ môže právo výkonu majetkových práv **postúpiť tretej osobe len so súhlasom autora**.
  - Toto neplatí, ak ide o predaj podniku, alebo samostatnej organizačnej zložky podniku.
  - Osobnostné práva sa zamestnancovi ako autorovi zachovávajú, ale jeho majetkové práva vykonáva zamestnávateľ vo vlastnom mene a na vlastný účet, v prípade, že sa zamestnanec a zamestnávateľ nedohodli inak.
  - Napr. **počítačový program**, ktorý nie je spoločným dielom, považuje za **zamestnanecké dielo** aj vtedy, ak bolo celkom, alebo sčasti vytvorené **na základe zmluvy o vytvorení diela**.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Špecifické časti týkajúce sa ochrany duševného vlastníctva v trestnom zákone

- Nájdeme v § 281, 282 a 283 trestného zákona.
- Ide najmä:
  - o porušovanie práv k ochrannej známke, označeniu pôvodu výrobku a k obchodnému menu,
  - porušovanie priemyselných práv a
  - porušovanie autorského práva.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Porušovanie práv k ochrannej známke, označeniu pôvodu výrobku a obch. menu

- Táto časť trestného zákona (§281) ošetruje najmä distribúciu falošne označených kópií originálnych tovarov.
- Ten, kto uvedie do obehu tovar alebo poskytne služby neoprávnene označené označením zhodným alebo zameniteľnými s ochrannou známkou, ku ktorej právo používať ju patrí inému, potrestá sa odňatím slobody až na tri roky.
- Rovnako sa potrestá ten, kto na dosiahnutie hospodárskeho prospechu uvedie do obehu tovar neoprávnene označený označením zhodným alebo zameniteľným so zapísaným označením pôvodu výrobku a zemepisným označením výrobku, ku ktorému právo používať ho patrí inému.

KPMG
cutting through complexity™

Porušovanie priemyselných práv

- Na prípady najmä neoprávnených zásahov do softvérových patentov, dizajnu, alebo topografie elektronického počítačového systému (patentované elektronické zariadenia, počítače, smartfóny, technológie a pod.) pamätá § 282 trestného zákona.
- Odňatím slobody sa potrestá ten, kto neoprávnene zasiahne do práv k patentu, úžitkovému vzoru, dizajnu, alebo topografii polovodičového výrobku.
- Sankcie odňatia slobody sa pohybujú v rozmedzí jeden rok až päť rokov pri závažných škodách. V prípade škôd veľkého rozsahu alebo ak bol páchateľ člen nebezpečného zoskupenia je možné uložiť trest až vo výške tri až osem rokov.

Porušovanie autorského práva (1/2)

- Paragraf 283 trestného zákona ošetruje problematiku zneužitia a porušovania autorských práv k dielu vo všeobecnosti, najmä umelecké diela, zvukové a obrazové záznamy ale aj softvérové diela, resp. produkty ako také.
- Zároveň sú legislatívne ošetrené aj prípady zneužitia masmédií pomocou IKT pre šírenie potenciálne nebezpečných poplašných správ, ako sme tomu boli svedkami v Českej republike v roku 2007.
- Vtedy mediálna skupina s názvom „Ztohoven“ uskutočnila výstup na jeden z vysielačov používaných Českou televíziou a zneužila jednu z kamier používaných pre živý prenos z Krkonoš.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Porušovanie autorského práva (2/2)

- V rannom vysielaní sa vtedy na ČT2 v relácii Panoráma odvysielal fiktívny výbuch atómovej bomby s panorámou Krkonoš na pozadí.
- Často sa tento akt uvádzal ako „hacking vysielania Českej televízie“. Mnoho divákov bolo šokovaných.
- Bolo podané trestné oznámenie pre šírenie poplašnej správy, ktorý ale sudca nepotvrdil. Za tento skutok bola skupina paradoxne ocenená významnou cenou Národnej Galérie.
- Ak by bol tento skutok spáchaný dnes na území SR, tak by sa páchateľ pravdepodobne trestu nevyhol.
- Klasifikácia tohto činu a aj prípadná sankcia, ktorú je možné za tento čin uložiť, je totižto uvedená priamo v spomenutom § 283 trestného poriadku, podľa ktorého ten, kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, potrestá sa odňatím slobody.

KPMG
cutting through complexity™

Rozmnožovanie a úprava počítačového programu (1/3)

- Na rozmnožovanie a úpravu počítačových programov sa vzťahuje autorské právo v plnom rozsahu.
  - „Právna ochrana počítačových programov, ktoré sú výsledkom tvorivej duševnej činnosti autorov - programátorov, vychádza aj u nás predovšetkým z autorského práva.
  - Predmetom ochrany autorského práva však nemôže byť to, čo objektívne existuje nezávisle od človeka, resp. niečo, k čomu môžu dospieť nezávisle viacerí autori. Predmetom ochrany preto nie je sama myšlienka, ale je to práve tvorivé spracovanie tejto myšlienky.
  - Ak sú pri konkrétnom počítačovom programe splnené pojmové znaky diela v zmysle autorského zákona, autorský zákon mu poskytuje absolútnu ochranu, ktorá pôsobí proti všetkým tretím osobám.“

Rozmnožovanie a úprava počítačového programu (2/3)

- Podľa §35 autorského zákona môže oprávnený užívateľ rozmnoženiny počítačového programu bez súhlasu autora vyhotoviť rozmnoženinu tejto rozmnoženiny počítačového programu alebo vykonať na nej úpravu alebo preklad, ak je takáto rozmnoženina, úprava alebo preklad nevyhnutný na prepojenie počítačového programu s počítačom na účel a v rozsahu, na ktorý bol nadobudnutý, vrátane opráv chýb v počítačovom programe, alebo na nahradenie oprávnene nadobudnutej rozmnoženiny počítačového programu (záložná rozmnoženina).
- V ľudskej reči povedané, ide najmä o vyhotovenie kópie alebo dátového obrazu už vytvoreného počítačového programu na účely jeho používania. Takisto je celkom legálne vyhotovenie záložnej kópie, ktorá zostane vo vlastníctve oprávneného používateľa. Toto právo nemožno vylúčiť v licenčných podmienkach pre jeho používanie.

Rozmnožovanie a úprava počítačového programu (3/3)

- Oprávnený užívateľ rozmnoženiny počítačového programu môže bez súhlasu autora preskúmať, preštudovať alebo preskúšať funkčnosť počítačového programu s cieľom určiť myšlienky alebo princípy, ktoré sú základom akejkoľvek časti programu, a to počas nahrávania, zobrazovania, vysielania, overovania funkčnosti a ukladania programu do pamäte, na ktoré bol oprávnený.
- Táto časť zákona teda dáva priestor potenciálnym pokusom o reverzné inžinierstvo existujúceho softvéru, pokiaľ ho vykonáva oprávnený užívateľ. Takto vyhotovená rozmnoženina však nesmie byť šírená ďalej. Ak sa ďalšie použitie rozmnoženiny počítačového programu stane neoprávneným, každá takáto rozmnoženina, úprava alebo preklad sa musí znehodnotiť.
- Uvedené právo zároveň nemožno zmluvne vylúčiť a v uvedených prípadoch nevzniká povinnosť uhradiť autorovi odmenu.

Spätný preklad počítačového programu (1/3)

- Paragraf 36 autorského zákona definuje podmienky úpravy softvérového produktu pre vlastnú potrebu a reverzného inžinierstva:
  - Súhlas autora sa nevyžaduje na vyhotovenie rozmnoženiny kódu počítačového programu alebo prekladu jeho formy, ak je to nevyhnutné na získanie informácie potrebnej na dosiahnutie vzájomnej súčinnosti nezávisle vytvorených počítačových programov s inými počítačovými programami, ak túto činnosť vykonáva oprávnený užívateľ rozmnoženiny počítačového programu, alebo informácia nevyhnutná na dosiahnutie vzájomnej súčinnosti nebola predtým bežne dostupná osobám oprávneným na rozmnožovanie alebo preklad, alebo sa tieto činnosti dotýkajú iba časti počítačového programu a sú nevyhnutné na dosiahnutie vzájomnej súčinnosti nezávisle vytvorených počítačových programov.

Spätný preklad počítačového programu (2/3)

- Informáciu získanú podľa predchádzajúceho odseku nemožno použiť na dosiahnutie iného cieľa,
  - ako je dosiahnutie vzájomnej súčinnosti nezávisle vytvorených počítačových programov, nemožno ju poskytnúť iným osobám okrem takého použitia, ktoré je nevyhnutné na zabezpečenie vzájomnej súčinnosti nezávisle vytvorených počítačových programov, nemožno ju použiť ani na zabezpečenie vývoja, výroby alebo na obchodovanie s počítačovým programom, ktorý je podobný vo svojom vyjadrení, a rovnako ju nie je možné použiť na činnosť, ktorou by sa porušilo právo autora.
  - Súhlas autora na uvedené činnosti sa vyžaduje na vyhotovenie rozmnožení počítačových programov, ak by takéto vyhotovenie rozmnožení bolo v rozpore s riadnym využívaním počítačového programu alebo by bezdôvodne zasahovalo do právom chránených záujmov autora počítačového programu.

Spätný preklad počítačového programu (3/3)

- Vyhotovenie rozmnoženiny strojového kódu počítačového programu alebo preklad jeho formy nemožno zmluvne vylúčiť.
- Znamená to, že ak pokročilými technikami reverzného inžinierstva odkopírujeme strojový kód aplikácie a budeme schopní jeho časť čiastočne previesť do kódu vyššieho jazyka, neporušili sme tým žiaden paragraf autorského zákona.
- Je však nutné myslieť na odsek 2 písm. c) citovaného paragrafu, v ktorom sa uvádza, že s takto modifikovaným programom nemožno obchodovať a nemožno ho používať, ak účel tohto počínania je v rozpore s platnými licenčnými podmienkami pre používanie tohto softvéru.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Ďalšie práva a povinnosti organizácie podľa všeobecnej legislatívy (1/2)

- Vyšetrovanie trestnej činnosti
  - Základné práva a povinnosti organizácie pri zisťovaní a vyšetrovaní trestnej činnosti, ktorej bola obeťou, alebo takej, ktorú spáchali zamestnanci pomocou IKT prostriedkov organizácie sú definované v § 3 Trestného poriadku.
  - V súlade s §3 ods. 1 Trestného poriadku sú štátne orgány, vyššie územné celky, obce a iné právnické osoby a fyzické osoby povinné poskytnúť súčinnosť orgánom činným v trestnom konaní a súdu pri plnení ich úloh, ktoré súvisia s trestným konaním.
  - Podľa znenia odseku 2 uvedeného paragrafu je organizácia povinná bez meškania oznamovať orgánom činným v trestnom konaní skutočnosti nasvedčujúce tomu, že bol spáchaný trestný čin a včas vybavovať dožiadania orgánov činných v trestnom konaní a súdov.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Ďalšie práva a povinnosti organizácie podľa všeobecnej legislatívy (2/2)

- Použitie ITP prostriedkov:
  - V prípade použitia informačno-technických prostriedkov sú v súlade s §10 ods. 20
    - prevádzkovatelia verejných telefónnych sietí,
    - poskytovatelia elektronických telekomunikačných sietí,
    - poskytovatelia elektronických telekomunikačných služieb,
    - poštový podnik, dopravcovia
    - a iní zasielatelia a ich zamestnanci

    povinní poskytnúť nevyhnutnú súčinnosť pri použití informačno-technických prostriedkov.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

II. časť

ŠPECIALIZOVANÁ LEGISLATÍVA A OBLASTI ÚPRAVY VO VZŤAHU K IB

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Špecializovaná legislatíva a oblasti úpravy vo vzťahu k IB – prehľad

- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
  - Výnos o štandardoch pre ISVS
- Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
  - Vyhláška č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Špecializovaná legislatíva a oblasti úpravy vo vzťahu k IB (1/2)

- Rozvoj a rozšírenie IKT so sebou nesie zvyšujúci sa počet hrozieb a rizík, medzi ktoré patrí najmä narušenie súkromia, vyzradenie osobných údajov, krádež identity, hrozby pre bezpečnosť a spoľahlivosť sietí, rôzne formy kybernetického zločinu (cybercrime) a rozširovanie nelegálneho obsahu.
- V súčasnej dobe prudko sa rozvíjajúcich moderných technológií, kedy dnes už skoro každé zariadenie v domácnosti je „inteligentným“ zariadením s pripojením a možnosťou komunikácie prostredníctvom počítačových sietí a internetu, je potreba ochrany súkromia ešte dôležitejšia.
- Je potrebné jej venovať zvýšenú pozornosť a rovnako je potrebné venovať pozornosť aj zo strany legislatívy, ktorá nás má chrániť.

KPMG
cutting through complexity™

Špecializovaná legislatíva a oblasti úpravy vo vzťahu k IB (2/2)

- Používanie internetu na súkromné, alebo služobné účely so sebou nesie minimálne nižšie definované riziká:
  - spam - nevyžiadaná elektronická pošta, ktorá môže používateľa zavádzať klamnými tvrdeniami na nákup tovaru,
  - spyware - nepovolené monitorovanie činnosti používateľa na internete, napr. odchytávanie stlačených kláves, alebo navštívených stránok a odosielanie týchto dát útočníkovi,
  - phishingu – rozosielanie emailov slúžiacich na presmerovanie užívateľa na útočníkom spravovanú stránku za účelom „vylákania“ jeho prihlasovacích údajov,
  - hijacking – metóda prevzatia kontroly nad sieťovou komunikáciou používateľských aplikácií s počítačom.
- Je preto nevyhnutné legislatívne podporiť ochranu osobných údajov, dodržiavanie bezpečnostných štandardov pri prevádzke systémov na spracovanie osobných a iných citlivých údajov a súvisiace oblasti ochrany kritickej infraštruktúry, utajovaných skutočností, informačných systémov verejnej správy a zákonného rámca na vyvodenie trestnoprávnej zodpovednosti za porušovanie týchto štátom stanovených podmienok.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o ISVS (1/3)

- Informačná bezpečnosť je podľa normy STN ISO/IEC 27001 ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je najmä zaistenie kontinuity obchodných procesov, minimalizácia strát a maximalizácia návratnosti investícií.
- Štandard STN ISO/IEC 27001 vychádza z medzinárodne uznávaného štandardu a definuje požiadavky na systém riadenia informačnej bezpečnosti.
- Je aplikovateľný na každý typ organizácie bez ohľadu na predmet činnosti, alebo jej veľkosť. Jeho cieľom je zlepšovanie informačnej bezpečnosti, ochrana osobných údajov, kontinuita prevádzkových činností, riadenie rizík, súlad s legislatívnymi požiadavkami a požiadavkami štandardov a minimalizácia nákladov.

KPMG
cutting through complexity™

Zákon o ISVS (2/3)

- Samotným riadením IB v organizácii sa zaoberá ďalšia norma z rady 2700x, ktorou je STN ISO/IEC 27002. Jednou zo základných oblastí riadenia definovaných touto normou je aj oblasť súladu s legislatívou.
- Previazanie týchto noriem na legislatívu a legislatívne požiadavky, resp. previazanie informačnej bezpečnosti a legislatívy nezačína a nekončí len pri tejto oblasti súladu ale je zrejmé aj z ďalších oblastí riadenia IB definovaných v uvedenej norme.
- Najmarkantnejším príkladom tohto úzkeho vzťahu je práve zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ISVS“) a najmä príslušný výnos č. 312/2010 Z. z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy (ďalej len „výnos o štandardoch ISVS“).
- Môžeme dokonca tvrdiť, že základom a vzorom pre návrh výnosu o štandardoch bola práve táto norma riadenia IB.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o ISVS (3/3)

- Štandardizácia pomocou týchto noriem prináša lepšiu organizáciu práce, efektívnejšie procesy, bezpečnejší prenos a uchovávanie dát, dôvernejšie vzťahy so zákazníkom a vo všeobecnosti je využiteľná ako referenčný rámec, pokrývajúci všetky aspekty fungujúceho škálovateľného bezpečnostného modelu.
- Informatizácia spoločnosti a s ňou súvisiaca informačná bezpečnosť verejnej správy je vymedzená citovaným zákonom o ISVS.
- Zákon upravuje práva a povinnosti povinných osôb v oblasti ISVS.
- Vymedzuje tiež základné podmienky na zabezpečenie integrovateľnosti a bezpečnosti informačných systémov verejnej správy, upravuje správu a prevádzku ústredného portálu, postup pri vydávaní elektronického odpisu údajov z ISVS a výstupu z ISVS.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o ISVS - Základné práva a povinnosti povinnej osoby (1/2)

- Povinné osoby vypracovávajú koncepcie rozvoja ISVS, zabezpečujú plynulú, bezpečnú a spoľahlivú prevádzku ISVS, sú zodpovedné za predchádzanie zneužitiu IS, sprístupňujú verejnosti údaje z ISVS, zabezpečujú organizačné, odborné a technické zabezpečenie a sú povinné prednostne používať sieťovú infraštruktúru.
- Ministerstvo (rozumej MFSR) na úseku informačných systémov verejnej správy vypracúva národnú koncepciu informatizácie verejnej správy SR, usmerňuje tvorbu a schvaľuje koncepcie rozvoja ISVS povinných osôb s ohľadom na štandardy a súlad s národnou koncepciou informatizácie verejnej správy SR, vydáva štandardy, sleduje stav a hodnotí rozvoj ISVS a o výsledkoch informuje vládu SR. Tiež koordinuje budovanie informačných systémov verejnej správy na národnej a medzinárodnej úrovni a navrhuje časové a vecné viazanie rozpočtových prostriedkov.

Zákon o ISVS - Základné práva a povinnosti povinnej osoby (2/2)

- Ministerstvo tiež zverejňuje vypracované štandardy, rozhodnutia a iné informácie týkajúce sa ISVS. Zároveň kontroluje dodržiavanie povinností ustanovených týmto zákonom, prijíma opatrenia na nápravu zistených nedostatkov a ukladá sankcie za porušenie povinností ustanovených týmto zákonom.
- Medzi dôvody, prečo je dôležité vypracovávať a nasadzovať štandardy patrí lepšia variabilita pri výbere dodávateľa podpory, spravidla lepšia bezpečnosť riešení nasadených podľa otvorených a technologicky neutrálnych súborov pravidiel spojených s vytvorením, rozvojom a využívaním informačných systémov verejnej správy. Integrovateľnosť s inými informačnými systémami je taktiež veľkou výhodou štandardizácie.
- Úrad vlády Slovenskej republiky vykonáva správu, prevádzku a rozvoj Govnetu a ústredného portálu a zabezpečuje úlohy národného prevádzkovateľa centrálnej informačnej infraštruktúry a centrálnej komunikačnej infraštruktúry Slovenskej republiky pre verejnú správu.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o ISVS - Väzba zákona na riadenie IB

- V súlade s § 3 ods. 4 písm. b), c) a i) zákona o ISVS sú jednotlivé povinné osoby povinné:
  - zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, ktoré sú v ich správe, vrátane organizačného, odborného a technického zabezpečenia,
  - zabezpečovať informačný systém verejnej správy proti zneužitiu,
  - zabezpečovať, aby bol informačný systém verejnej správy v súlade so štandardmi informačných systémov verejnej správy (ďalej len "štandardy").
- Na základe uvedeného je jasne vidieť, že pokiaľ chce povinná osoba uvedené povinnosti zabezpečiť, najmä zabrániť zneužitiu a pokiaľ chce dosiahnuť plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, musí sa postarať o patričné riadenie informačnej bezpečnosti vo všetkých jej oblastiach podľa príslušných štandardov, resp. výnosu o štandardoch ISVS.
- Za porušenie týchto povinností týkajúcich sa riadenia IB je možné povinnej osobe udeliť aj sankcie, a to až do výšky 35000 EUR.

KPMG
cutting through complexity™

Výnos o štandardoch pre ISVS (1/2)

- Samotný výnos o štandardoch pre ISVS nerieši len problematiku riadenia IB ale štandardizuje aj ďalšie oblasti. Konkrétne v súlade s § 1 výnosu o štandardoch pre ISVS ide o nasledovné oblasti:
  - technické štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru a programové prostriedky, a to
    - štandardy pre prepojenie,
    - štandardy pre prístup k elektronickým službám,
    - štandardy pre webové služby,
    - štandardy pre integráciu dát,
  - štandardy prístupnosti a funkčnosti webových stránok, vzťahujúce sa na aplikačné programové vybavenie podľa zákona,
  - štandardy použitia súborov, vzťahujúce sa na formáty výmeny údajov,
  - štandardy názvoslovia elektronických služieb, vzťahujúce sa na sieťovú infraštruktúru,
  - bezpečnostné štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru, programové prostriedky a údaje, a to
    - štandardy pre architektúru riadenia,
    - štandardy minimálneho technického zabezpečenia,
  - dátové štandardy, vzťahujúce sa na údaje, registre a číselníky,
  - štandardy elektronických služieb verejnej správy, vzťahujúce sa na údaje, registre, číselníky a aplikačné programové vybavenie podľa zákona,
  - štandardy projektového riadenia, vzťahujúce sa na postupy a podmienky spojené s vytváraním a rozvojom informačných systémov verejnej správy.

Výnos o štandardoch pre ISVS (2/2)

- Oblasť riadenia IB, ktorá vychádza z uvedených medzinárodných a už aj lokalizovaných noriem STN ISO/IEC 27001 a STN ISO/IEC 27002, je definovaná v paragrafoch 28 až 42. Táto oblasť je rozdelená na nasledovné časti:
  - štandardy pre architektúru riadenia (§28-§31) - pokrýva oblasti ako sú napr. samotné riadenie IB, personálna bezpečnosť, riadenie rizík a kontrola riadenia IB,
  - štandardy minimálneho technického zabezpečenia (§32-§42) – pokrýva oblasti ako je napr. ochrana proti škodlivému SW, bezpečnosť sietí, fyzická bezpečnosť, aktualizácia SW, identifikácia a hodnotenie zraniteľností, riadenie bezpečnostných incidentov, zálohovanie a ukladanie dát, riadenie prístupu a prístupových práv, prístup tretích strán a aktualizácia IKT.

Zákon o OOÚ (1/4)

- Národná rada slovenskej republiky schválila a od 1.7.2013 uviedla do platnosti nový zákon č. 122/2013 Z. z. o ochrane osobných údajov, ktorý nahrádza pôvodný zákon č. 428/2002 Z. z. o ochrane osobných údajov.
- Návrh zákona o OOU vychádza z povinností, ktoré nám ukladá európska únia, konkrétne Smernica Európskeho parlamentu a Rady 95/46/ES, záverov a odporúčaní hodnotenia správneho uplatňovania schengenského acquis v Slovenskej republike pre oblasť ochrany osobných údajov a výsledky analýzy súčasne platného zákona z pohľadu aplikácie v praxi.
- Garancia ochrany osobných údajov je zakotvená v ústave, preto musí byť legislatívne zapracovaná. Spoliehať sa na individuálne iniciatívy prevádzkovateľov a sprostredkovateľov nestačí, preto je vo všeobecnosti nutná ochrana osobných údajov na úrovni zákona. Tak je možné stanoviť nie len kvalitatívne parametre pri ich spracovávaní, prenose, ukladaní, sprostredkovávaní a likvidovaní, ale najmä základné opatrenia na ich ochranu.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o OOÚ (2/4)

- Zákon o OOU upravuje ochranu práv fyzických osôb pred neoprávneným zasahovaním do ich súkromného života pri spracúvaní ich osobných údajov. Vymedzuje práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb.
- Zároveň upravuje aj postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov Slovenskej republiky.
- Zákon sa vzťahuje na každého, kto spracúva osobné údaje, určuje účel a prostriedky spracúvania alebo poskytuje osobné údaje na spracúvanie.

KPMG
cutting through complexity™

Zákon o OOÚ (3/4)

- Ako sme uviedli vyššie návrh zákona o OOU vychádza z povinností, ktoré nám ukladá európska únia a tento fakt sa prejavil aj na pôsobnosti zákona.
- Podľa §2 zákona o OOU sa tento zákon vzťahuje aj na prevádzkovateľov, ktorí nemajú sídlo, organizačnú zložku, prevádzkareň alebo trvalý pobyt na území Slovenskej republiky, ale sú umiestnení v zahraničí na mieste, kde sa uplatňuje právny poriadok SR.
- Dokonca môžeme tvrdiť, že zákon v určitých prípadoch nepozná hranice SR a dokonca ani hranice EÚ, pretože ten istý §2 zákona o OOU hovorí, že zákon sa vzťahuje aj na prevádzkovateľov, ktorí nemajú sídlo, organizačnú zložku, prevádzkareň alebo trvalý pobyt na území členského štátu EÚ, ak na účely spracúvania osobných údajov využívajú úplne alebo čiastočne automatizované alebo iné ako automatizované prostriedky spracúvania umiestnené na území SR, pričom tieto prostriedky spracúvania nie sú využívané výlučne len na prenos osobných údajov cez územie členských štátov.

Zákon o OOÚ (4/4)

- Ďalším dôležitým faktom je skutočnosť, že zákon o OOU sa v podstate vzťahuje len na osobné údaje, ktoré sú spracovávané automatizovanými prostriedkami, či už úplne alebo čiastočne, alebo sú spracovávané inými ako automatizovanými prostriedkami spracúvania, ktoré sú súčasťou informačného systému alebo sú určené na spracúvanie v informačnom systéme.
- Zákon o OOU sa nevzťahuje na osobné údaje, ktoré fyzická osoba spracúva sama, alebo na údaje, ktoré boli získané náhodne bez predchádzajúceho určenia, alebo zámeru spracovania.
- Veľmi dôležitou požiadavkou zákona je skutočnosť, že osobné údaje možno spracúvať len spôsobom ustanoveným zákonom o OOU a v jeho medziach tak, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb, najmä k porušeniu ich práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do ich práva na ochranu súkromia.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o OOÚ – Základné práva a povinnosti jednotlivca (1/4)

- Oprávnenou osobou za v zmysle zákona rozumie každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje.
- Fyzická osoba sa stáva oprávnenou osobou dňom jej poučenia prevádzkovateľom.
  - Prevádzkovateľ je povinný poučiť osobu najmä o právach a povinnostiach ustanovených zákonom o OOU a o zodpovednosti za ich porušenie ešte pred uskutočnením prvej operácie s osobnými údajmi.
  - Poučenie by malo obsahovať najmä rozsah oprávnení, popis povolených činností a podmienky spracúvania osobných údajov.
- V prípade, že došlo k zásadnej a podstatnej zmene pracovného, služobného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne pracovných činností, alebo sa podstatne zmenili podmienky, alebo rozsah spracúvaných osobných údajov je prevádzkovateľ povinný opätovne poučiť oprávnenú osobu.

KPMG
cutting through complexity™

Zákon o OOÚ – Základné práva a povinnosti jednotlivca (2/4)

- Jednou z najdôležitejších povinností pre oprávnené osoby je požiadavka na zachovávanie mlčanlivosti. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku.
- Dôležitou skutočnosťou je aj fakt, že tieto údaje nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.
- Povinnosť mlčanlivosti samozrejme platí aj pre iné fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa, či už náhodne alebo úmyselne. Povinnosť mlčanlivosti samozrejme trvá aj po ukončení spracúvania osobných údajov.

Zákon o OOÚ – Základné práva a povinnosti jednotlivca (3/4)

- Okrem základných povinností pre fyzické osoby, zákon o OOU jasne definuje aj základné práva jednotlivcov, o ktorých sa osobné údaje spracovávajú.
- Základným právom je ochrana práv dotknutých osôb. Dotknutá osoba má právo na základe písomnej žiadosti od prevádzkovateľa vyžadovať najmä:
  - potvrdenie, či sú alebo nie sú osobné údaje o nej spracúvané,
  - vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého získal jej osobné údaje na spracúvanie,
  - zoznam jej osobných údajov, ktoré sú predmetom spracúvania,
  - opravu alebo likvidáciu svojich nesprávnych, neúplných alebo neaktuálnych osobných údajov, ktoré sú predmetom spracúvania,
  - likvidáciu jej osobných údajov, ktorých účel spracúvania sa skončil (ak sú predmetom spracúvania úradné doklady obsahujúce osobné údaje, môže požiadať o ich vrátenie),
  - likvidáciu jej osobných údajov, ktoré sú predmetom spracúvania, ak došlo k porušeniu zákona,
  - blokovanie jej osobných údajov z dôvodu odvolania súhlasu pred uplynutím času jeho platnosti, ak prevádzkovateľ spracúva osobné údaje na základe súhlasu dotknutej osoby.

Zákon o OOÚ – Základné práva a povinnosti jednotlivca (4/4)

- Taktiež je dôležité spomenúť aj to, že dotknutá osoba na základe písomnej žiadosti má právo u prevádzkovateľa namietať voči:
  - spracúvaniu jej osobných údajov, o ktorých predpokladá, že sú alebo budú spracúvané na účely priameho marketingu bez jej súhlasu, a žiadať ich likvidáciu,
  - využívaniu osobných údajov na účely priameho marketingu v poštovom styku, alebo
  - poskytovaniu osobných údajov na účely priameho marketingu.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o OOÚ – Základné práva a povinnosti organizácie (1/3)

- Podobne ako pre fyzické osoby, povinnosť mlčanlivosti sa vzťahuje aj na organizáciu, resp. prevádzkovateľa.
- Prevádzkovateľ je rovnako ako oprávnená osoba povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.
- **Kľúčovou časťou zákona z pohľadu informačnej bezpečnosti je určite jeho druhá hlava, ktorá pojednáva o bezpečnosti osobných údajov.**
- Zodpovednosť za bezpečnosť osobných údajov je jednoznačne ponechaná na pleciach prevádzkovateľa.
- Prevádzkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania.
- Za týmto účelom je prevádzkovateľ povinný, z pohľadu informačnej bezpečnosti, prijať primerané technické, organizačné a personálne opatrenia (ďalej len „bezpečnostné opatrenia“) zodpovedajúce spôsobu spracúvania osobných údajov.
- Pri návrhu konkrétnych bezpečnostných opatrní musí do úvahy zobrať najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, a najmä rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému. Inak povedané je potrebné použiť, tzv. „Risk based approach“ prístup, ktorý najskôr vyžaduje vykonanie analýzy rizík, kde na základe jej výsledkov sú prijaté a implementované príslušné bezpečnostné opatrenia.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o OOÚ – Základné práva a povinnosti organizácie (2/3)

- Prijaté a implementované bezpečnostné opatrenia musí prevádzkovateľ zdokumentovať v bezpečnostnej smernici alebo v bezpečnostnom projekte, v závislosti od toho, či spracúva osobitné kategórie osobných údajov a od toho, či je jeho systém prepojený s verejne prístupnou počítačovou sieťou.
- Bezpečnostný projekt vymedzuje rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.
- Jednoznačné previazanie zákona o OOU s informačnou bezpečnosťou a bezpečnostnými štandardmi je vidieť z povinnosti prevádzkovateľa podľa, ktorej musí bezpečnostný projekt vypracovať nie len v súlade s týmito štandardmi, ale aj právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.
- Nakoľko bezpečnostné opatrenia majú taktiež svoj vlastný životný cyklus je potrebné zabezpečiť ich pravidelnú aktualizáciu vzhľadom na aktuálne podmienky a vývoj.
- Za týmto účelom je prevádzkovateľ povinný bez zbytočného odkladu zabezpečovať aktualizáciu prijatých bezpečnostných opatrení tak, aby zodpovedala prijatým zmenám pri spracúvaní osobných údajov, a to až do ukončenia spracúvania osobných údajov v informačnom systéme.

KPMG
cutting through complexity™

Zákon o OOÚ – Základné práva a povinnosti organizácie (3/3)

- Keďže na celkovej bezpečnosti majú svoj podiel aj jednotliví pracovníci prevádzkovateľa je potrebné, aby prevádzkovateľ oboznámil všetky oprávnené osoby s obsahom bezpečnostnej dokumentácie v rozsahu potrebnom na plnenie ich úloh.
- Ide najmä o oboznámenie s ich právami a povinnosťami, ktoré sa od nich vyžadujú pre zaistenie ochrany osobných údajov.
- Oboznámenie oprávnených osôb s obsahom bezpečnostnej smernice je prevádzkovateľ povinný na žiadosť úradu hodnoverne preukázať. Túto povinnosť si navyše musí prevádzkovateľ splniť pri každej zmene bezpečnostnej dokumentácie.
- V prípade, ak prevádzkovateľ spracúva osobné údaje prostredníctvom 20 a viac oprávnených osôb musí písomne poveriť zodpovednú osobu dohľadom nad dodržiavaním ustanovení zákona o OOU.
- Zodpovednou osobou, môže byť iba fyzická osoba, ktorá má spôsobilosť na právne úkony v plnom rozsahu, je bezúhonná a má platné potvrdenie úradu o absolvovaní skúšky z oblasti ochrany osobných údajov.
- Z dôvodov zabezpečenia celkovej bezpečnosti a efektívneho dohľadu Úradu na ochranu osobných údajov podliehajú informačné systémy, v ktorých sa spracovávajú osobné údaje registrácií a osobitnej registrácií. O informačných systémoch, ktoré nepodliehajú registrácii alebo osobitnej registrácii, je prevádzkovateľ povinný viesť evidenciu, a to najneskôr odo dňa začatia spracúvania údajov v týchto informačných systémoch. Zákon samozrejme definuje aj konkrétne podmienky, kedy ide iba o registráciu, a kedy o osobitnú registráciu, a rovnako aj podmienky samotnej registrácie a osobitnej registrácie, ktoré musia jednotliví prevádzkovatelia naplniť.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vyhláška k zákonu o OOÚ (1/2)

- Úradu na ochranu osobných údajov Slovenskej republiky vydal 13. júna 2013 vyhlášku k zákonu o OOU, ktorá pojednáva o rozsahu a dokumentácii bezpečnostných opatrení.
- Ide o vyhlášku, ktorá v rámci ochrany osobných údajov, detailne štandardizuje informačnú bezpečnosť v oblasti vedenia konkrétnej dokumentácie, ktorá napomáha efektívnemu riadeniu informačnej bezpečnosti.
- Vyhláška definuje dokumentáciu prijatých bezpečnostných opatrení, ktorá popisuje celý proces spracúvania osobných údajov od ich získavania po ich likvidáciu.
- Obsah dokumentácie sa musí zhodovať so skutočným stavom implementovaných bezpečnostných opatrení pri spracúvaní osobných údajov.
- Bezpečnostné opatrenia musia byť zdokumentované prehľadne a jednoznačne.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vyhláška k zákonu o OOÚ (2/2)

- Vyhláška popisuje najmä nasledovnú dokumentáciu:
  - písomnú zmluvu, ak prevádzkovateľ poveril spracúvaním osobných údajov sprostredkovateľa,
  - písomné záznamy o poučení oprávnených osôb,
  - písomné poverenie zodpovednej osoby,
  - záznamy o kontrolnej činnosti prevádzkovateľa zameranej na dodržiavanie bezpečnosti informačného systému,
  - záznamy o zistených bezpečnostných incidentoch vplývajúcich na bezpečnosť osobných údajov a záznamy o nadväzných postupoch, ktorými prevádzkovateľ zabezpečil obnovenie bezpečnosti informačného systému,
  - bezpečnostnú smernicu,
  - bezpečnostný projekt.
- Obsah a rozsah posledných dvoch uvedených typov dokumentácie je popísaný detailnejšie v samostatných paragrafoch vyhlášky.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o kritickej infraštruktúre (1/2)

- Kritickú infraštruktúru definuje VÚS nasledovne:
  - **„Koncepcia ochrany kritickej infraštruktúry na Slovensku bola prijatá uznesením vlády SR č. 120 zo 14. februára 2007. V tejto koncepcii je kritická infraštruktúra označená ako tá časť národnej infraštruktúry, ktorej zničenie alebo znefunkčnenie v dôsledku pôsobenia rizikového faktora spôsobí ohrozenie alebo narušenie hospodárskeho a politického chodu štátu alebo ohrozenie života a zdravia obyvateľstva.**
  - Nepretržité vyhodnocovanie rizík v kritickej infraštruktúre na národnej úrovni vytvára predpoklady na lepší odhad možných ohrození a tým na vytváranie efektívnejších postupov a prostriedkov na zvyšovanie bezpečnosti.“

KPMG
cutting through complexity™

Zákon o kritickej infraštruktúre (2/2)

- Môžeme konštatovať, že uvedené požiadavky koncepcie ochrany kritickej infraštruktúry boli premietnuté do zákona č. 45/2011 Z. z. o kritickej infraštruktúre.
- Požiadavka na monitorovanie a vyhodnocovanie rizík v kritickej infraštruktúre je čiastočne riešená prostredníctvom organizácie CSIRT.SK.
- CSIRT.SK je špecializovaný útvar DataCentra (rozpočtovej organizácie MFSR), ktorý má za cieľ zabezpečiť primeranú úroveň ochrany národnej informačnej a komunikačnej infraštruktúry.
- Poskytuje aktívne a proaktívne služby pre klientov definované uznesením vlády č. 479/2009.

Zákon o KI – Základné práva a povinnosti organizácie (1/3)

- Zákon o KI ustanovuje organizáciu a pôsobnosť orgánov štátnej správy na úseku kritickej infraštruktúry, postup pri určovaní prvku kritickej infraštruktúry, povinnosti prevádzkovateľa pri ochrane prvku kritickej infraštruktúry a zodpovednosť za porušenie týchto povinností. Môže sa tiež jednať o obrannú infraštruktúru podľa osobitného predpisu.
- Štátnu správu na úseku kritickej infraštruktúry vykonáva vláda SR, Ministerstvo vnútra SR, Ministerstvo hospodárstva SR, Ministerstvo financií SR, Ministerstvo dopravy, výstavby a regionálneho rozvoja SR, Ministerstvo životného prostredia SR a Ministerstvo zdravotníctva SR.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o KI – Základné práva a povinnosti organizácie (2/3)

- Môžeme povedať, že rovnako ako pri zákone o ISVS aj povinnosti definované v zákone o KI vychádzajú z medzinárodných štandardov riadenia IB.
- Organizácia, resp. prevádzkovateľ prvku kritickej infraštruktúry je povinný ochraňovať prvok pred narušením alebo zničením. Na tento účel je prevádzkovateľ povinný najmä:
  - uplatniť pri modernizácii prvku technológiu, ktorá zabezpečuje jeho ochranu,
  - zaviesť bezpečnostný plán, a tento pravidelne prehodnocovať,
  - oboznámiť svojich zamestnancov v nevyhnutnom rozsahu s bezpečnostným plánom,
  - precvičiť podľa bezpečnostného plánu aspoň raz za tri roky modelovú situáciu hrozby narušenia alebo zničenia prvku,
  - postupovať podľa bezpečnostného plánu v prípade hrozby narušenia alebo zničenia prvku.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o KI – Základné práva a povinnosti organizácie (3/3)

- Bezpečnostný plán obsahuje popis možných spôsobov hrozby narušenia alebo zničenia prvku, zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu.
- Bezpečnostné opatrenia na ochranu prvku sú najmä mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné prvky informačných systémov, fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia.
- Rozsah bezpečnostných opatrení na ochranu prvku sa určuje na základe posúdenia hrozby narušenia alebo zničenia prvku.
- Zákon o KI tiež určuje ďalšie detaily v súvislosti s informačnou bezpečnosťou, týkajúce sa najmä:
  - postupov pri určovaní prvku kritickej infraštruktúry (§ 8),
  - postupov pre vypracovanie bezpečnostného plánu (príloha č. 2),
  - označovania citlivej informácie, ktorá musí byť označená slovami „Kritická infraštruktúra – nezverejňovať“ (§ 12),
  - vyraďovania prvku a prvku európskej kritickej infraštruktúry (§ 13),
  - priestupkov pri porušení povinnosti, alebo úmyselnom vyzradení citlivej informácie (§ 14),
  - iných správnych deliktov a s nimi súvisiacich pokút (§ 15).

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

III. časť

INÁ ŠPECIFICKÁ LEGISLATÍVA VO VZŤAHU K IB

KPMG
cutting through complexity™

Iná špecifická legislatíva vo vzťahu k IB (1/3)

- V rámci tejto špecifickej časti si stručne uvedieme prehľad niektorých špecifických právnych predpisov, ktoré už neštandardizujú problematiku IB a riadenia IB ako takú, ale obsahujú určité prvky a požiadavky na používateľov a prevádzkovateľov, či už z pohľadu zabezpečenia IB alebo z pohľadu riadenia IB.
- Môžeme povedať, že tieto predpisy vo väčšej alebo menšej miere aplikujú prvky informačnej bezpečnosti a riadenia informačnej bezpečnosti, ktoré sú štandardizované v rámci špecializovanej legislatívy.

Iná špecifická legislatíva vo vzťahu k IB (2/3)

- Prehľad predpisov:
  - Zákon č. 215/2002 Z. z. o elektronickom podpise
  - Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností
  - Zákon č. 351/2011 Z. z. o elektronických komunikáciách
  - Zákon č. 22/2004 Z. z. o elektronickom obchode
  - Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Iná špecifická legislatíva vo vzťahu k IB (3/3)

- Povinnosti pre organizácie vyplývajúce z týchto právnych predpisov nie sú pre účely týchto študijných materiálov dôležité, nakoľko nejde o všeobecné povinnosti pre všetky inštitúcie verejnej správy ale o povinnosti pre vybrané organizácie (prevažne súkromného sektora), poskytujúce príslušné špecifické služby zväčša na základe špeciálneho povolenia, certifikácie alebo akreditácie.
- Spomenuté právne predpisy uvádzame z dôvodu všeobecného a ucelenejšieho prehľadu legislatívy majúcej vplyv alebo vzťah s informačnou bezpečnosťou ako takou.
- Okrem tohto dôvodu považujeme za nutné ich spomenúť najmä z pohľadu povinností v súvislosti s informačnou bezpečnosťou a ochranou informácií alebo súkromia, ktoré definujú pre jednotlivcov, resp. používateľov príslušných služieb definovaných konkrétnym právnym predpisom.
- Pre používateľov sú zároveň dôležité aj informácie o ich právach, ktoré v určitých prípadoch nepriamo vyplývajú z povinností definovaných pre príslušnú organizáciu.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o elektronickom podpise (1/2)

- Elektronický podpis (EP) je jedným z nástrojov, prostredníctvom ktorého je možné vykonať autorizáciu (podpísanie) elektronického dokumentu konkrétnou osobou.
- Jeho ďalšou nezanedbateľnou bezpečnostnou funkciou, ktorá vychádza z podstaty samotného elektronického podpisu na báze asymetrickej kryptografie, je možnosť kontroly zachovania integrity podpisovaného dokumentu.
- Zákon o EP upravuje vzťahy vznikajúce v súvislosti s vyhotovovaním a používaním elektronického podpisu, práva a povinnosti fyzických osôb a právnických osôb pri používaní elektronického podpisu, hodnovernosť a ochranu elektronických dokumentov podpísaných elektronickým podpisom.
- Uvádza tiež požiadavky na rozsah auditu certifikačných autorít. Rozsah auditu certifikačnej autority je pomerne široký, keďže činnosť certifikačnej autority nespočíva iba v manažmente kľúčov, ale zahŕňa napr. aj dodržanie fyzickej a režimovej bezpečnosti nad špecifickou množinou aktív.

Zákon o elektronickom podpise (2/2)

- Gestorom zákona o EP je Národný bezpečnostný úrad, ktorý vykonáva činnosti kontroly dodržiavania tohto zákona, posudzuje žiadosti o akreditáciu certifikačných autorít na území SR, udeľuje a odníma certifikačným autoritám akreditáciu a vydáva osvedčenia o akreditácii.
- Vydáva certifikáty verejných kľúčov akreditovaným certifikačným autoritám, zverejňuje vlastný verejný kľúč a vydáva certifikát svojho vlastného verejného kľúča, eviduje certifikačné autority pôsobiace na Slovensku, vedie zoznam akreditovaných certifikačných autorít a zverejňuje ho na svojom webovom sídle.
- Zrušuje certifikát akreditovanej certifikačnej autority, ak jej bola odňatá právomoc, alebo ak ukončila svoju činnosť, vedie register zahraničných certifikačných autorít, ktorých certifikáty boli úradom uznané na použitie v SR.

Zákon o EP - Základné práva a povinnosti jednotlivca (1/5)

- Používanie elektronického podpisu (§ 5)
  - V styku s orgánmi verejnej moci sa používa elektronický podpis, alebo zaručený elektronický podpis.
  - Ak sa používa zaručený elektronický podpis, tento musí byť vyhotovený prostredníctvom súkromného kľúč, na ktorý je vydaný kvalifikovaný certifikát, ktorý vydala akreditovaná certifikačná autoritou a tento certifikát musí obsahovať rodné číslo držiteľa certifikátu.
  - Overovateľ overuje elektronický podpis prostriedkami na overovanie elektronického podpisu využitím podpísaného elektronického dokumentu a verejného kľúča patriaceho udávanému podpisovateľovi.
  - Pri overovaní elektronického podpisu overovateľ môže požadovať overenie pravosti verejného kľúča, to znamená toho, že verejný kľúč patrí podpisovateľovi. Na tento účel môže použiť certifikát verejného kľúča podpisovateľa.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EP - Základné práva a povinnosti jednotlivca (2/5)

- Používanie zaručeného elektronického podpisu:
  - Na rozdiel od „obyčajného“ elektronického podpisu, kde overovateľ môže vykonať určité, vyššie uvedené, overenia, pri overovaní zaručeného elektronického podpisu overovateľ už musí overiť určité, zákonom definované skutočnosti.
  - Ide najmä o verifikovanie toho, či verejný kľúč na overenie zaručeného elektronického podpisu patrí podpisovateľovi, ktoré sa musí vykonať na základe kvalifikovaného certifikátu verejného kľúča.

KPMG
cutting through complexity™

Zákon o EP - Základné práva a povinnosti jednotlivca (3/5)

- Povinnosti v prípade vydania „mandátneho“ certifikátu (§7)
  - Jedna z posledných noviel zákona o EP priniesla aj možnosť vydávať, tzv. „mandátne“ certifikáty pre fyzické ale aj právnické osoby. Fyzickej osobe konajúcej v mene inej fyzickej osoby, alebo fyzickej osobe – podnikateľovi, prípadne právnickej osobe môže byť rovnako vydaný kvalifikovaný certifikát, ktorý oprávňuje túto fyzickú osobu konať v mene inej, v certifikáte uvedenej, fyzickej osoby.
  - Z uvedenej skutočnosti však pre takto zastupovanú fyzickú osobu vyplýva minimálne jedna dôležitá povinnosť, ktorou je požiadanie o zrušenie „mandátneho“ certifikátu v prípade, že oprávnenie osoby bolo zrušené alebo zaniklo. V prípade, že zastupovaná osoba zomrela, bola vyhlásená za mŕtvu, zanikla alebo bola zrušená, prenáša sa táto povinnosť o zrušenie certifikátu na samotného držiteľ „mandátneho“ certifikátu.

Zákon o EP - Základné práva a povinnosti jednotlivca (4/5)

- Medzi ďalšie základné povinnosti držiteľa certifikátu vo všeobecnosti patrí podľa §22 najmä:
  - zaobchádzať so svojím súkromným kľúčom s náležitou starostlivosťou tak, aby nemohlo dôjsť k zneužitiu jeho súkromného kľúča,
  - uvádzať presné, pravdivé a úplné informácie vo vzťahu k certifikátu svojho verejného kľúča,
  - neodkladne požiadať certifikačnú autoritu, ktorá spravuje jeho certifikát, o zrušenie certifikátu, ak zistí, že došlo k neoprávnenému použitiu jeho súkromného kľúča, alebo ak hrozí neoprávnené použitie jeho súkromného kľúča, alebo ak nastali zmeny v údajoch uvedených v certifikáte.
- Za škodu spôsobenú porušením povinností zodpovedá držiteľ certifikátu podľa všeobecných predpisov o náhrade škody.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EP - Základné práva a povinnosti jednotlivca (5/5)

- Zrušovanie certifikátov (§ 15):
  - Držiteľ certifikátu by mal zároveň poznať aj povinnosti certifikačnej autority, ktorá mu vydal príslušný certifikát v súvislosti s jeho možným zrušením. Certifikačná autorita je totižto povinná zrušiť certifikát, ktorý spravuje, ak zistí, že neboli splnené požiadavky podľa zákona o EP, alebo ak zistí, že certifikát nebol vydaný na základe pravdivých údajov.
  - Najdôležitejšou podmienkou zrušenia z pohľadu držiteľa certifikátu je ale možnosť, kedy držiteľ, alebo osoba, ktorej údaje sú uvedené v certifikáte, sama požiada o zrušenie certifikátu z akýchkoľvek dôvodov, ktorými samozrejme spravidla bývajú bezpečnostné dôvody, prípadne zmena identifikačných údajov.
  - Taktiež môže o zrušenie certifikátu požiadať súd, prípadne to môže byť certifikačná autorita, ktorá požiada o zrušenie certifikátu, v prípade, ak držiteľ zomrel, alebo v prípade, ak držiteľ certifikátu zanikol ako právnická osoba.
  - Ďalším dôvodom pre zrušenie certifikátu môže byť, že súkromný kľúč patriaci k certifikátu pozná iná osoba, než osoba uvedená v certifikáte.
  - O zrušenie certifikátu môže okrem držiteľa certifikátu zažiadať aj zastupovaná osoba.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EP - Priestupky a správne delikty

- Podľa §26 sa priestupku dopustí ten, kto:
  - zneužije súkromný kľúč podpisovateľa,
  - predloží nepravdivé údaje pri podávaní žiadosti o vydanie certifikátu,
  - poruší povinnosť bezodkladne požiadať o zrušenie certifikátu.
- Za uvedený priestupok podľa prvého bodu možno uložiť pokutu do výšky 33000 EUR a za priestupok podľa posledných dvoch bodov možno uložiť pokutu až do výšky 66000 EUR.
- Rovnako je možné, v súlade s §27, uložiť pokutu aj poskytovateľovi certifikačných služieb, prípadne inej relevantnej právnickej osobe, za porušenie príslušných povinností vyplývajúcich zo zákona, a to až do výšky 332000 EUR.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EP - Základné práva a povinnosti organizácie

- Povinnosti v prípade vydania „mandátneho“ certifikátu (§7)
  - Podobne ako pri povinnostiach jednotlivca v súvislosti so správou „mandátnych“ certifikátov, platia rovnaké povinnosti aj pre organizáciu verejnej moci, v mene ktorej bol príslušný „mandátny“ certifikát vydaný.
  - Kvalifikovaný certifikát môže byť vydaný aj fyzickej osobe, ktorá má oprávnenie na vykonávanie činnosti podľa osobitného predpisu (napr. notárovi, advokátovi, exekútorovi a pod.), fyzickej osobe, ktorá vykonáva funkciu podľa osobitného predpisu (napr. sudcovi, prokurátorovi a pod.) a fyzickej osobe, ktorá je verejným funkcionárom.
  - Z uvedenej skutočnosti pre príslušný orgán verejnej moci, v mene ktorého je „mandátny“ certifikát vydaný, vyplýva povinnosť bezodkladne požiadať o zrušenie tohto „mandátneho“ certifikátu, ak oprávnenie osoby alebo postavenie osoby uvedenej v „mandátnom“ certifikáte bolo zrušené, alebo zaniklo.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EP - Väzba zákona na riadenie IB

- Vzťah zákona o EP s požiadavkami noriem ohľadom informačnej bezpečnosti a riadenia IB je možné vidieť najmä pri povinnostiach kladených na jednotlivé certifikačné a akreditované certifikačné autority.
- Okrem špecifických povinností vyplývajúcich z vydávania, rušenia a celkovej správy certifikátov, definuje zákon o EP (a najmä príslušné vyhlášky NBÚ k tomuto zákonu) aj povinnosti, ktoré sa priamo týkajú IB a riadenia IB.
- Ide napríklad o pravidelné vykonávanie nezávislých bezpečnostných auditov, vedenie bezpečnostnej a prevádzkovej dokumentácie s minimálnym predpísaným obsahom, o požiadavky na audítorov a na samotný rozsah a výkon auditu.

KPMG
cutting through complexity™

Zákon o ochrane utajovaných skutočností (1/3)

- Zákon o ochrane utajovaných skutočností sa v podstate skoro celý venuje bezpečnostným požiadavkám, avšak požiadavkám nad špecifickým typom aktíva, ktorým sú utajované skutočnosti.
- Ochrana utajovaných skutočností (povinnosť postúpená z EÚ a NATO) bola dôvodom vzniku NBÚ v roku 2001.
- Vytvorenie optimálneho systému ochrany utajovaných skutočností je preto jeho primárnou úlohou.
- Samotný zákon chápe ochranu utajovaných skutočností ako súbor opatrení, ktorý pokrýva všetky základné oblasti, ktorými je personálna bezpečnosť, administratívna bezpečnosť, šifrová ochrana informácií, fyzická bezpečnosť, objektová bezpečnosť, bezpečnosť technických prostriedkov a priemyselná bezpečnosť.

Zákon o ochrane utajovaných skutočností (2/3)

- Môžeme konštatovať, že najdetailnejšie rozpracovanou oblasťou, resp. oblasťou, ktorej je venovaný najväčší dôraz je jednoznačne oblasť personálnej bezpečnosti, v rámci ktorej sa vykonávajú bezpečnostné previerky na preverenie bezpečnostnej spoľahlivosti osoby, ktorá sa bude oboznamovať s utajovanou skutočnosťou. Samozrejme pozornosť je venovaná aj zvyšným uvedeným oblastiam.
- Motiváciou pre kladenie dôrazu na oblasť personálnej bezpečnosti boli pravdepodobne praktické skúsenosti a nepísané pravidlo, ktoré hovorí, že najslabším článkom v informačnej bezpečnosti je vždy „ľudský faktor“.
- Zákon č. 215/2004 o ochrane utajovaných skutočností a o zmene a doplnení neskorších predpisov teda upravuje podmienky na ochranu utajovaných skutočností, najmä práva a povinnosti právnických osôb, obcí a fyzických osôb pri ich ochrane.
- Zároveň upravuje a definuje pôsobnosť NBÚ a pôsobnosť ďalších štátnych orgánov zaoberajúcich sa utajovanými skutočnosťami.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o ochrane utajovaných skutočností (3/3)

- Pôvodcom utajovanej skutočnosti je právnická osoba alebo fyzická osoba, ktorá je oprávnená rozhodnúť, že informácia alebo vec je utajovanou skutočnosťou, určiť stupeň utajenia a rozhodnúť o zmene alebo zrušení stupňa jej utajenia.
- Oprávnenou osobou je právnická osoba alebo fyzická osoba, ktorá je určená na oboznamovanie sa s utajovanými skutočnosťami, alebo ktorej oprávnenie na oboznamovanie sa s utajovanými skutočnosťami vzniklo zo zákona.
- Nepovolanou osobou je fyzická osoba, ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami, alebo ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami nad rozsah, ktorý jej je určený.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o US - Základné práva a povinnosti jednotlivca

- Základné povinnosti oprávnenej osoby sú najmä:
  - zachovávať pred nepovolanou osobou a pred cudzou mocou mlčanlivosť o informáciách a veciach obsahujúcich utajované skutočnosti počas utajenia týchto skutočností, a to aj po zániku oprávnenia oboznamovať sa s utajovanými skutočnosťami,
  - dodržiavať všeobecne záväzné právne predpisy upravujúce ochranu utajovaných skutočností,
  - oznámiť neodkladne vedúcemu neoprávnenú manipuláciu s utajovanými skutočnosťami a záujem nepovolaných osôb o utajované skutočnosti a spolupracovať s úradom na objasnení príčin neoprávnenej manipulácie s utajovanými skutočnosťami,
  - oznámiť neodkladne vedúcemu skutočnosť, ktorá by mohla mať vplyv na jej oprávnenie oboznamovať sa s utajovanými skutočnosťami, ako aj každú skutočnosť, ktorá by mohla mať vplyv na takéto oprávnenie inej oprávnenej osoby.
- Medzi základné povinnosti všetkých „bežných“ občanov, resp. nepovolaných osôb, patrí povinnosť neodkladného odovzdania získanej alebo nájdenej utajovanej skutočnosti NBÚ alebo útvaru Policajného zboru. Príjemca takto odovzdanej utajovanej skutočnosti je zároveň na požiadanie povinný vystaviť odovzdávajúcemu potvrdenie o jej prevzatí.

KPMG
cutting through complexity™

Zákon o US - Základné práva a povinnosti organizácie (1/2)

- Povinnosti vedúceho (§ 8):
  - Ochranu utajovaných skutočností je povinný zabezpečiť v štátnom orgáne štatutárny orgán, v obci starosta, vo vyššom územnom celku predseda a v inej právnickej osobe štatutárny orgán (ďalej len "vedúci").
  - Vedúci najmä určuje základné vymedzenie utajovaných skutočností, lehoty, zmeny a zrušenia stupňa utajenia. Určuje tiež koncepciu ochrany utajovaných skutočností a **vytvára podmienky na jej zabezpečenie**.
  - Zabezpečuje poučenie osôb, ktoré sa majú oboznamovať s utajovanými skutočnosťami stupňa utajenia vyhradené postúpenými SR cudzou mocou.
  - Medzi ďalšie jeho povinnosti patrí napr. vedenie evidencie a zoznamov oprávnených osôb a osôb, ktorým toto oprávnenie zaniklo, oznamuje úradu zmenu rozsahu oboznamovania sa s utajovanými skutočnosťami, informuje úrad o začatí plnenia úloh výskumu, vývoja, projekcie a výroby, oznamuje vopred úradu prípravu a uzatvorenie medzinárodnej zmluvy a vykonáva ďalšie opatrenia na úseku ochrany utajovaných skutočností vyplývajúce zo zákona o US.
  - Z pohľadu informačnej bezpečnosti môžeme povedať, že medzi najdôležitejšie povinnosti patrí povinnosť neodkladne oznamovať NBÚ neoprávnenú manipuláciu s utajovanými skutočnosťami a pokusy narušenia ochrany utajovaných skutočností a povinnosť vypracovať ročnú správu o kontrole ochrany utajovaných skutočností, v ktorej je potrebné uviesť najmä údaje o počte vykonaných kontrol, zistených nedostatkoch a prijatých opatreniach na ich nápravu.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o US - Základné práva a povinnosti organizácie (2/2)

- V súvislosti s ochranou utajovaných skutočností, medzi ďalšie povinnosti organizácie patria najmä povinnosti v oblasti ochrany objektov a chránených priestorov, systémových prostriedkov, technických prostriedkov a šifrovej ochrany informácií.
- Môžeme povedať, že všetky tieto povinnosti vyplývajú z medzinárodných štandardov IB, avšak v rámci tohto zákona sú definované špecificky pre ochranu aktív, ktorými sú utajované skutočnosti.
- Detailné požiadavky a popis konkrétnych opatrení je definovaný v príslušných vyhláškach NBÚ k zákonu o US.

KPMG
cutting through complexity™

Zákon o elektronických komunikáciách

- Zákon č. 351/2011 Z. z. o elektronických komunikáciách upravuje podmienky na poskytovanie elektronických komunikačných sietí a služieb, podmienky na používanie rádiových zariadení, reguláciu elektronických komunikácií, práva a povinnosti podnikov a užívateľov elektronických komunikačných sietí a služieb, ochranu elektronických komunikačných sietí a služieb a efektívne využívanie frekvenčného spektra a čísel.
- Zahŕňa tiež paragrafy týkajúce sa ochrany súkromia a ochrany spracúvania osobných údajov v oblasti elektronických komunikácií a ochrany telekomunikačného tajomstva.
- Netýka sa však obsahu služieb, ktoré sa poskytujú prostredníctvom elektronických komunikačných sietí.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EK - Základné práva a povinnosti jednotlivca

- Užívateľ je osoba, ktorá používa, alebo požaduje poskytovanie verejnej služby. Za užívateľa sa považuje aj účastník a koncový užívateľ. Koncový užívateľ je osoba, ktorá používa verejnú službu, alebo požaduje jej poskytovanie a túto službu ďalej neposkytuje a ani prostredníctvom nej neposkytuje ďalšie služby. Koncovým užívateľom je spotrebiteľ, alebo v prípade rozhlasových a televíznych programov aj poslucháč a divák.
- Najdôležitejšou povinnosťou pre jednotlivca z pohľadu informačnej bezpečnosti je povinnosť zachovávať telekomunikačné tajomstvo.
- Telekomunikačné tajomstvo je povinný zachovávať každý, kto príde s jeho predmetom do styku, či už pri poskytovaní sietí a služieb, pri používaní služieb, alebo náhodne, prípadne akýmkoľvek iným spôsobom.
- Telekomunikačným tajomstvom sa rozumie:
  - obsah prenášaných správ,
  - súvisiace údaje komunikujúcich strán, ktorými sú telefónne číslo, obchodné meno a sídlo právnickej osoby, alebo obchodné meno a miesto podnikania fyzickej osoby (podnikateľa) alebo osobné údaje fyzickej osoby, ktorými sú meno, priezvisko, titul a adresa trvalého pobytu,
  - prevádzkové údaje a
  - lokalizačné údaje.
- Predmetom telekomunikačného tajomstva nie sú údaje, ktoré sú zverejnené v telefónnom zozname.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EK - Základné práva a povinnosti organizácie (1/5)

- Zákon definuje podnik, ktorým je každá osoba, ktorá poskytuje sieť, alebo službu. Poskytovanie siete, alebo služby v oblasti elektronických komunikácií pre tretiu osobu je podnikaním. Zákon ďalej vymedzuje pôsobnosť orgánov štátnej správy v oblastiach, ktoré zákon upravuje. Orgány štátnej správy v oblasti elektronických komunikácií sú Ministerstvo dopravy, výstavby a regionálneho rozvoja SR a Telekomunikačný úrad SR.
- Organizácia, resp. v zmysle definície zákona podnik, **je povinný prijať zodpovedajúce technické a organizačné opatrenia na ochranu bezpečnosti svojich služieb**, a ak je to nevyhnutné, aj v súčinnosti s poskytovateľom verejnej siete. **Prijaté opatrenia musia zabezpečiť takú úroveň bezpečnosti služieb, ktorá je primeraná existujúcemu riziku s ohľadom na stav techniky a náklady na ich realizáciu**.
- Zákon pamätá aj na ochranu osobných údajov, pretože podniku dáva aj povinnosť informovať účastníka o tom, aké osobné údaje sa získavajú a spracúvajú, na základe akého právneho dôvodu, na aký účel a ako dlho sa budú spracúvať. Túto informáciu musí podnik poskytnúť najneskôr pri uzavretí zmluvy o poskytovaní verejných služieb.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EK - Základné práva a povinnosti organizácie (2/5)

- Okrem tejto povinnosti sú definované aj kroky, ktoré musí podnik, ktorý poskytuje verejné služby, vykonať pri porušení ochrany osobných údajov. V takomto prípade musí podnik:
  - bezodkladne oznámiť Telekomunikačnému úradu SR porušenie ochrany osobných údajov,
  - bezodkladne informovať dotknutých účastníkov a užívateľov o porušení ochrany osobných údajov,
  - na požiadanie úradu informovať dotknutých účastníkov a užívateľov o porušení ochrany osobných údajov, ak porušenie ochrany osobných údajov môže mať negatívny vplyv na dotknutých účastníkov a užívateľov,
  - viesť zoznam prípadov porušení ochrany osobných údajov, ktorý obsahuje podstatné skutočnosti spojené s týmito porušeniami, ich následky a prijaté opatrenia na nápravu.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EK - Základné práva a povinnosti organizácie (3/5)

- **Špecificky sa bezpečnosťou zaoberá § 63 o Telekomunikačnom tajomstve a piata časť o „Ochrane sietí a zariadení“ (§64).**
- Telekomunikačné tajomstvo možno sprístupniť úradu, účastníkovi a užívateľovi, ktorého sa týka, jeho oprávneným zástupcom alebo právnym nástupcom.
- Samozrejme zákon pamätá aj na výnimky, ktoré sú taxatívne vymenované, a za ktorých je možné telekomunikačné tajomstvo postúpiť napr. inému orgánu štátu.
- Takáto výnimka musí byť spravidla odobrená súdom alebo vykonaná na príkaz súdu. Ide najmä o prípady kedy sú údaje, ktoré sú predmetom telekomunikačného tajomstva, potrebné napr. pre pátranie po nezvestných osobách a odcudzených motorových vozidlách alebo mobilných zariadeniach.
- Zákon aj v tomto prípade pamätá na bezpečnosť a ochranu telekomunikačného tajomstva, pretože v takomto prípade, pokiaľ podnik tieto informácie poskytuje v elektronickej forme, musí ich poskytnúť len v zašifrovanom tvare.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EK - Základné práva a povinnosti organizácie (4/5)

- Zákon zároveň ošetruje a definuje základné podmienky na bezpečnosť a integritu verejných sietí a služieb.
- Podnik, ktorý poskytuje verejné siete alebo verejné služby, je povinný prijať zodpovedajúce technické a organizačné opatrenia na ochranu bezpečnosti svojich sietí a služieb, ktoré s ohľadom na stav techniky musia zabezpečiť úroveň bezpečnosti, ktorá je primeraná existujúcemu riziku.
- Opatrenia sa prijímajú najmä s cieľom predchádzať bezpečnostným incidentom a minimalizovať vplyv bezpečnostných incidentov na užívateľov a vzájomne prepojené siete. Z definície môžeme vidieť, že samotná implementácia opatrení by mala byť založená, podobne ako pri zákone o ochrane osobných údajov, na tzv. „Risk based approach“ prístupe, ktorý najskôr vyžaduje vykonanie analýzy rizík.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EK - Základné práva a povinnosti organizácie (5/5)

- Okrem uvedeného prístupu by sa mali použiť aj opatrenia z oblasti zabezpečenia kontinuity podnikateľských činností, pretože zákon priamo od podniku, ktorý poskytuje verejné siete, požaduje udržiavanie integrity svojich sietí s cieľom zaručiť kontinuitu poskytovania služieb prostredníctvom týchto sietí.
- Rovnako je na úrovni zákona ošetrená aj oblasť riadenia bezpečnostných incidentov, nakoľko podnik, ktorý poskytuje verejné siete alebo služby, je povinný bezodkladne informovať úrad o narušení bezpečnosti alebo integrity, ktoré mali významný vplyv na prevádzku sietí alebo služieb.
- Zároveň, ak ide o osobitné riziko ohrozenia bezpečnosti siete, poskytovateľ verejných služieb je povinný informovať dotknutých účastníkov o tomto riziku a možnostiach nápravy vrátane pravdepodobných nákladov potrebných na odvrátenie ohrozenia.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o elektronickom obchode

- Zákon č. 22/2004 Z. z. o elektronickom obchode upravuje vzťahy medzi poskytovateľom služieb informačnej spoločnosti a ich príjemcom, ktoré vznikajú pri ich komunikácií na diaľku, počas spojenia elektronických zariadení elektronickou komunikačnou sieťou a spočívajú na elektronickom **spracovaní, prenose, uchovávaní, vyhľadaní, alebo zhromažďovaní dát vrátane textu, zvuku a obrazu.**
- Zákon o EO tiež upravuje dohľad nad dodržiavaním zákona a medzinárodnú spoluprácu v elektronickom obchode.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EO - Základné práva a povinnosti jednotlivca

- Služby informačnej spoločnosti môže poskytovať každá fyzická osoba a právnická osoba bez povolenia, alebo registrácie. Toto sa vzťahuje aj na poskytovateľa služieb, ktorý poskytuje služby informačnej spoločnosti z členského štátu.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EO - Základné práva a povinnosti organizácie (1/2)

- Poskytovateľ je povinný príjemcovi služby na elektronickom zariadení poskytnúť informácie o svojom názve, obchodnom mene a sídle, daňovom identifikačnom čísle, adrese elektronickej pošty a tel. čísle a pod.
  - Tieto musia byť príjemcovi ľahko a trvalo prístupné.
- Zľavy a dary musia byť od bežnej komunikácie ľahko rozlíšiteľné a podmienky pre ich získanie musia byť prístupné, zrozumiteľné a jednoznačné.
- **Poskytovateľ nesmie zasielať nevyžiadanú elektronickú poštu.**

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o EO - Základné práva a povinnosti organizácie (2/2)

- Ak poskytovateľ služieb uskutočňuje komerčnú komunikáciu v mene alebo na účet inej osoby, musí byť táto osoba identifikovaná. Zákon ale ďalej nerieši a nehovorí akým spôsob má byť táto identifikácia zabezpečená.
- Ak poskytovateľ služieb poskytuje služby informačnej spoločnosti, nie je povinný sledovať informácie ani oprávnený vyhľadávať informácie, ktoré sa prenášajú alebo ukladajú.
- Ak sa však dozvie o protiprávnosti takých informácií, je povinný odstrániť ich z elektronickej komunikačnej siete alebo aspoň zamedziť k nim prístup. Súd môže nariadiť poskytovateľovi služieb ich odstránenie z elektronickej komunikačnej siete aj vtedy, ak sa poskytovateľ služieb o ich protiprávnosti nedozvedel.
- Ďalšie paragrafy sa týkajú najmä:
  - **zmlúv uzatvorených pomocou elektronických zariadení (§ 5),**
  - **vylúčenia zodpovednosti poskytovateľa služieb (§ 6),**
  - **dohľadu (§ 7),**
  - **medzinárodnej spolupráce v elektronickom obchode (§ 8).**

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o zdravotnej starostlivosti

- Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov upravuje poskytovanie zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti, práva a povinnosti fyzických osôb a právnických osôb pri poskytovaní zdravotnej starostlivosti, postup pri úmrtí a výkon štátnej správy na úseku zdravotnej starostlivosti.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o ZS - Základné práva a povinnosti jednotlivca (1/2)

- Zákon o ZS priamo nedefinuje povinnosti pre jednotlivca ako takého z pohľadu informačnej bezpečnosti ale prináša minimálne niekoľko opatrení, ktoré sa týkajú jednotlivca, resp. zdravotnej dokumentácie vedenej o konkrétnom občanovi.
- Priamo §20 zákona o ZS definuje formy vedenia zdravotnej dokumentácie a zároveň zavádza aj niekoľko základných opatrení pri jej vedení.
- Zdravotná dokumentácia sa historicky vedie primárne v písomnej forme. Pokiaľ však poskytovateľ zdravotnej starostlivosti chce viesť zdravotnú dokumentáciu v elektronickej forme, môže, ale musí byť opatrená elektronickým podpisom.
- Zákon ale zároveň ustanovuje aj výnimky a obmedzenia kedy, resp. ktorý typ zdravotnej dokumentácie nemôže byť vedený elektronicky, ale len výlučne písomnou formou.
- Otázkou pre právnikov podľa nás zostáva fakt, či skutočne ani takto definované typy zdravotnej dokumentácie nemôžu byť vedené elektronicky, pretože §40 Občianskeho zákonníka hovorí, že písomná forma je zachovaná vždy pokiaľ je podpísaná zaručeným elektronickým podpisom.
- Ďalším podľa nás, tak trochu paradoxom, je fakt, že zákon jasne nešpecifikuje koho elektronický podpis má byť na zdravotnej dokumentácii, v prípade jej vedenia v elektronickej forme, použitý.
- Minimálne by malo ísť o elektronický podpis poskytovateľa zdravotnej starostlivosti, ale určite by bolo vhodné použiť aj elektronický podpis príjemcu zdravotnej starostlivosti, čiže vlastníka zdravotnej dokumentácie, ktorým by zároveň bolo potvrdené poskytnutie a prijatie deklarovanej zdravotnej starostlivosti.

KPMG
cutting through complexity™

Zákon o ZS - Základné práva a povinnosti jednotlivca (2/2)

- Základné požiadavky na vedenie zdravotnej dokumentácie sú:
  - zdravotná dokumentácia v elektronickej forme s elektronickým podpisom sa vedie na záznamovom nosiči v textovej forme, grafickej forme alebo v audiovizuálnej forme,
  - zdravotnú dokumentáciu možno viesť v elektronickej forme s elektronickým podpisom, len ak:
    - *bezpečnostné kópie dátových súborov sa vyhotovujú podľa štandardov zdravotníckej informatiky najmenej jedenkrát za každý pracovný deň,*
    - *o vytvorených záložných kópiách dátových súborov sa vedie presná evidencia a tie sa ukladajú na mieste prístupnom len osobám oprávneným vyhotovovať záložné kópie,*
    - *pred uplynutím doby životnosti zápisu na archívnom médiu je z archivovaných dát vyhotovená kópia a údaje zo starého nosiča sa odstránia,*
    - *archívne kópie sa vytvárajú najmenej jedenkrát za rok, pričom spôsob vyhotovenia archívnych kópií znemožňuje vykonať v nich dodatočné zásahy.*

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zákon o ZS - Základné práva a povinnosti organizácie

- Medzi základné povinnosti organizácie, poskytovateľa zdravotnej starostlivosti, ktorý vedie zdravotnú dokumentáciu patria požiadavky ohľadom zabezpečenia a uchovávania zdravotnej dokumentácie.
- Zákon o ZS jasne definuje zodpovednosť, podľa ktorej za zabezpečenie zdravotnej dokumentácie zodpovedá poskytovateľ. Poskytovateľ je povinný ukladať a ochraňovať zdravotnú dokumentáciu tak, aby nedošlo k jej poškodeniu, strate, zničeniu alebo k zneužitiu.
- Pokiaľ chce poskytovateľ túto požiadavku naplniť, nezostáva mu nič iné len implementovať opatrenia príslušných štandardov z oblasti informačnej bezpečnosti.
- Okrem základných bezpečnostných opatrení sú definované aj požiadavky na jej archiváciu. Zdravotnú dokumentáciu, ktorú vedie všeobecný lekár, uchováva poskytovateľ 20 rokov po smrti osoby. Iná zdravotná dokumentácia sa archivuje 20 rokov od posledného poskytnutia zdravotnej starostlivosti príslušnej osobe.
- Poskytovateľ je zároveň povinný zabezpečiť, aby k osobitnej zdravotnej dokumentácii nemali prístup iné osoby ako ošetrujúci lekár a v nevyhnutnom rozsahu oprávnení zdravotnícki pracovníci.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

IV. časť

PREHĽAD RELEVANTNEJ LEGISLATÍVY EÚ VZŤAHUJÚCEJ SA NA RIADENIE IB

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad relevantnej legislatívy EÚ vzťahujúcej sa na riadenie IB (1/5)

- Legislatíva EU zlepšuje globálne podmienky pre dôveru a bezpečnosť medzi členskými krajinami.
- Zavedením všeobecne záväzných pravidiel vo forme zákonov vytvára prostredie pre efektívnu medzinárodnú spoluprácu v potláčaní kybernetického zločinu a súvisiacich rizík.
- Medzinárodné právo upravuje autorské právo a ochranu duševného vlastníctva.
- OSN tiež vydalo manuál pre prevenciu a kontrolu počítačového zločinu, ktorý menuje konkrétne orgány zaoberajúce sa kybernetickým právom. Ide predovšetkým o OSN, Radu Európy, Organizáciu pre hospodársku spoluprácu a rozvoj (OECD). Manuál sa zaoberá konkrétne kyberterorizmom, kybernetickou vojnou a tzv. Hi-tech hrozbami.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad relevantnej legislatívy EÚ vzťahujúcej sa na riadenie IB (2/5)

- Dôležitým je tiež dohovor Rady Európy č. 185 o kybernetickej kriminalite zo dňa 23.11.2001, ktorý sa stal účinným 1.7.2004.
- Jeho hlavnou úlohou je harmonizácia niektorých základných skutkových podstát a zavedenie efektívneho režimu spolupráce medzi jednotlivými štátmi.
- Dohovor definuje významné pojmy ako je počítačový systém, počítačové dáta, poskytovateľ služby apod.
- Neskôr bol k tomuto dohovoru pripojený Dodatkový protokol zo dňa 28.1.2003, ktorý sa zaoberá šírením xenofóbneho a rasistického obsahu. Vyplnil tým medzery Dohovoru, ktorý okrem detskej pornografie problematiku škodlivého obsahu neupravuje. Upravuje tiež skutkové podstaty 9 základných trestných činov, ktoré sú rozdelené do 4 skupín. Najzávažnejšie sú trestné činy súvisiace s detskou pornografiou.
- Spáchanie trestného činu musí byť úmyselné, teda vylučuje nedbalosť. Dodatočné náležitosti zahŕňajú jednania spôsobujúce závažnú škodu, spáchanie činu vo vzťahu k PC systému a pod.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad relevantnej legislatívy EÚ vzťahujúcej sa na riadenie IB (3/5)

- EU vydala množstvo smerníc a iných záväzných dokumentov, týkajúcich sa priamo či nepriamo problematiky internetových deliktov. Sú to napr.:
  - Smernica Rady 91/250/EHS zo dňa 14.05.1991, o právnej ochrane počítačových programov.
  - Rozhodnutí Rady 92/242/EHS zo dňa 31.03.1992, o bezpečnosti informačných systémov.
  - Smernica Európskeho parlamentu a Rady 96/9/ES zo dňa 11.03.1996 o právnej ochrane databáz.
  - Smernica Európskeho parlamentu a Rady 2002/20/ES o oprávnení pre siete a služby.
  - Smernica Európskeho parlamentu a Rady 2002/58/ES zo dňa 12.07.2002 o súkromí a elektronických komunikáciách.
  - Rámcové rozhodnutí Rady 2005/222/SVV zo dňa 24.02.2005 o útokoch proti informačným systémom.
  - Smernica Európskeho parlamentu a Rady 2006/24/ES o uchovávaní údajov vytváraných alebo spracovávaných v súvislosti s poskytovaním verejne dostupných služieb elektronických komunikácií alebo verejných komunikačných sietí a elektronických komunikácií (autorizačná smernica).

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad relevantnej legislatívy EÚ vzťahujúcej sa na riadenie IB (4/5)

- Vo februári tohto roka Európska komisia zverejnila stratégiu pre oblasť kybernetickej bezpečnosti (tzv. otvorený, bezpečný a chránený kybernetický priestor), ktorej snahou je definovať spoločnú politiku členských štátov v tejto oblasti.
- Stratégia definuje nasledovné základné oblasti, resp. priority:
  - dosahovanie odolnosti voči kybernetickým útokom,
  - prudké zníženie počítačovej kriminality,
  - rozvíjanie politiky a spôsobilostí kybernetickej obrany, ktoré súvisia so spoločnou bezpečnostnou a obrannou politikou,
  - rozvíjanie priemyselných a technologických zdrojov na účely kybernetickej bezpečnosti,
  - vytvorenie politiky súdržného medzinárodného kybernetického priestoru pre Európsku úniu a presadzovanie základných hodnôt EÚ.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad relevantnej legislatívy EÚ vzťahujúcej sa na riadenie IB (5/5)

- Komisia zároveň zverejnila aj pripravovanú smernicu o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informácií v celej Únii, ktorá je hlavným mechanizmom, vyplývajúcim z tejto stratégie. Medzi hlavné opatrenia smernice patria nasledovné:
  - členský štát musí prijať národnú stratégiu bezpečnosti sietí a informácií a určiť vnútroštátny orgán príslušný pre bezpečnosť sietí a informácií, disponujúci dostatočnými finančnými a ľudskými zdrojmi, na účely predchádzania rizikám a incidentom v tejto oblasti, ich riešenia a reagovania na ne,
  - vytvára sa mechanizmus spolupráce medzi členskými štátmi a Komisiou na účely vzájomného včasného varovania o rizikách a incidentoch prostredníctvom chránenej infraštruktúry, a na účely spolupráce a organizácie pravidelných hodnotení,
  - prevádzkovatelia mimoriadne dôležitých infraštruktúr v niektorých špecifických odvetviach, poskytovatelia služieb informačnej spoločnosti a orgány verejnej správy musia prijať postupy riadenia rizík a podávať správy o významných bezpečnostných incidentoch.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

V. časť

VNÚTORNÁ LEGISLATÍVA ORGANIZÁCIE V OBLASTI RIADENIA IB

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vnútorná legislatíva organizácie v oblasti riadenia IB (1/2)

- Ako sme už spomenuli, norma ISO 27002 poskytla vzor pre legislatívny rámec pre metodiky a štandardy informačnej bezpečnosti vo výnose MFSR č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy.
- Norma ISO 27002 hovorí o legislatívnom súlade so zákonmi, ale aj o súlade so smernicami. Aj keď sa niektoré legislatívne normy venujú nielen všeobecným náležitostiam, ale v niektorých prípadoch uvádzajú aj značné detaily, napr. v prípade vyhlášok k zákonu o elektronickom podpise (napr. obsah bezpečnostných dokumentov, režim kľúčov, náležitosti bezpečnostného plánu a pod), či v prípade vyhlášky k zákonu o ochrane osobných údajov (o rozsahu a dokumentácii bezpečnostných opatrení), nie je táto úroveň dostatočná pre účely konkrétnej organizácie, pretože každá organizácia má svoje špecifické podmienky, či už riadenia alebo prevádzky.
- Práve týmto špecifickým podmienkam je potrebné venovať zvýšenú pozornosť a zohľadniť ich pri tvorbe internej legislatívy organizácie (tzv. smerníc v oblasti riadenia informačnej bezpečnosti).

Vnútorná legislatíva organizácie v oblasti riadenia IB (2/2)

- Medzi oblasti, ktoré by sa mali implementovať v rámci vnútorných smerníc riadenia informačnej bezpečnosti organizácie, patria najmä dobré praktiky definované v ISO 27002 a v zákone o informačných systémoch verejnej správy (ISVS).
- Organizácie teda nemajú povinnosť vymýšľať žiadne nové prevádzkové štandardy, ale môžu si naštudovať a osvojiť tieto všeobecné normy.
- Po ich prevzatí je možná úprava podľa konkrétnych požiadaviek a špecifík organizácie.
- Inak povedané interné smernice by mali jednoznačne vychádzať z aktuálnej legislatívy a noriem a mali by poskytnúť primeranú úroveň detailu prispôsobenú konkrétnym podmienkam organizácie, ktorú samozrejme nemôže poskytnúť legislatíva alebo všeobecné normy.
- Jednotlivé smernice alebo akty riadenia by mali poskytovať dostatok informácií pre osoby, ktorým sú určené, aby tieto osoby mali jasne definované svoje práva, povinnosti, činnosti a úlohy, ktoré sa od nich v rámci organizácie očakávajú, najmä v súvislosti s informačnou bezpečnosťou.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

VI. časť

ANONYMITA A SÚKROMIE VS. MONITOROVANIE ZAMESTNANCOV

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Anonymita a súkromie vs. monitorovanie zamestnancov (1/6)

- Úspešne a efektívne riadenie IB si za určitých okolností vyžaduje monitorovanie aktivít v rámci informačných systémov, ktoré sú predmetom ochrany.
- Pod pojmom „aktivity“ rozumieme v prvom rade aktivity systému ako takého z pohľadu jeho efektívneho fungovania, manažmentu kapacít prevádzky a pod., ktorých vyhodnocovanie nám pomáha zabezpečiť IS najmä z pohľadu aspektu jeho dostupnosti, prípadne integrity.
- Nakoľko je však potrebné zabezpečiť systém aj z pohľadu zachovania dôvernosti spracovávaných, uchovávaných alebo prenášaných dát je potrebné monitorovať aj aktivity jednotlivých používateľov systému, či už interných alebo externých.
- Práve pri monitorovaní týchto aktivít však prevádzkovateľ systému môže „naraziť“ na rôzne obmedzenia a práva monitorovaných osôb, vyplývajúce z legislatívneho rámca, najmä z pohľadu zachovania ich súkromia alebo prípadnej anonymity.

KPMG
cutting through complexity™

Anonymita a súkromie vs. monitorovanie zamestnancov (2/6)

- Právo na súkromný život a jeho ochranu je zakotvené už v Dohovore Rady Európy o ochrane ľudských práv a základných slobôd z roku 1950, v článku 7 Charty základných práv EÚ a rovnako aj v druhom oddiely Ústavy SR. Okrem týchto predpisov je možné určité formulácie ohľadom súkromia nájsť aj v Občianskom zákonníku.
- Okrem práva na súkromie, by však malo byť, v súlade s článkom 22 Ústavy SR, zaručené aj listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov. Podľa tohto článku nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo iným spôsobom. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením.
- Samozrejme výnimkou môžu byť prípady, ktoré ale musia byť ustanovené na úrovni zákona. Ide napr. o bezpečnosť štátu, vyšetrovanie kriminálnych činov a pod.

Anonymita a súkromie vs. monitorovanie zamestnancov (3/6)

- Toto právo sa však v súvislosti so zabezpečením informačnej bezpečnosti, resp. ochrany údajov v IS, dostáva do konfrontácie s ochranou práv zamestnávateľa a jeho podnikateľských činností, resp. v prípade verejnej správy, zákonom daných činností. Problémom, resp. bodom konfrontácie, môže byť aj fakt, že v záujme zamestnávateľa monitorovať zamestnancov často nebýva len ochrana informácií, ale napr. aj sledovanie efektivity ich pracovnej činnosti, využívanie pracovného času, využívanie zdrojov zamestnávateľa na prípadné súkromné aktivity a pod.
- Môžeme povedať, že v rámci legislatívy SR, je tejto problematike najväčšia pozornosť venovaná v Zákonníku práce (zákon č. 311/2001 Z. z. Zákonník práce).
- Podľa článku 11 základných zásad Zákonníka práce môže zamestnávateľ o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Anonymita a súkromie vs. monitorovanie zamestnancov (4/6)

- Konkrétnejšie sa problematike súkromia na pracovisku v súvislosti s monitorovaním zamestnancov venuje §13 Zákonníka práce, ktorý okrem iného hovorí:
  - „Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje, vykonáva záznam telefonických hovorov uskutočňovaných technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronickú poštu odoslanú z pracovnej elektronickej adresy a doručenú na túto adresu bez toho, aby ho na to vopred upozornil. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.“
- Pokiaľ by sme sa pozreli na uvedenú definíciu podrobnejšie určite by sme si všimli minimálne dve zásadné skutočnosti.
- Tou prvou je, že zamestnávateľ musí mať vážny dôvod narúšať súkromie zamestnanca.
- Druhou je fakt, že zamestnávateľ by mal zamestnancov informovať o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.

KPMG
cutting through complexity™

Anonymita a súkromie vs. monitorovanie zamestnancov (5/6)

- Nanešťastie zákon nešpecifikuje čo sú to vážne dôvody a ani neuvádza žiadne príklady, čo presne by sa mohlo považovať za vážny dôvod, ktorý by oprávňoval zamestnávateľa k uvedeným činnostiam monitorovania a narúšania súkromia.
- Môžeme však predpokladať, že monitorovanie z pohľadu bezpečnosti, t.j. zachovania dôvernosti, integrity a dostupnosti informačných aktív zamestnávateľa sa dá za takýto dôvod považovať.
- Nemalo by sa však zabúdať na informovanie zamestnancov o tom, že takéto kontroly sú na pracovisku realizované. Zároveň by mal byť rozsah a spôsob týchto kontrol primeraný účelu a nemal by narúšať súkromie zamestnanca viac ako je pre daný účel nevyhnutné.
- Všetky použité kontrolné a monitorovacie opatrenia by nemali zasahovať do súkromia zamestnanca, t.j. mali by sa používať nástroje a postupy, ktoré napr. sledujú prítomnosť vírusov alebo iného škodlivého softvéru, alebo zaznamenávajú aktivity v systéme, ale ktoré nevykonávajú, z pohľadu ochrany súkromia, nežiaducu analýzu obsahu e-mailovej komunikácie, obsahu prezeraných stránok na internete, neodpočúvajú telefonickú alebo IP komunikáciu a pod.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Anonymita a súkromie vs. monitorovanie zamestnancov (6/6)

- Inak povedané mali by sa zaznamenávať len údaje typu dĺžka hovoru alebo prístupu, číslo volaného alebo ID osoby v prípade chatu, dátum a hodina začiatku a konca udalosti a pod.
- Zamestnávateľ by sa mal vyvarovať neprimeraným zásahom do súkromia, ktorým môže byť napr. sledovanie obrazovky zamestnanca, monitorovanie stlačených kláves (tzv. „keylogger“) sledovanie obsahu súkromných e-mailov, odpočúvanie komunikácie a pod.
- Samozrejmosťou Zákonníka práce je okrem iného aj právo zamestnanca, ktorý sa domnieva, že jeho súkromie na pracovisku alebo v spoločných priestoroch bolo narušené, domáhať sa právnej ochrany na súde.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

VII. časť

ETIKA A MORÁLNY KÓDEX

KPMG
cutting through complexity™

Etika a morálny kódex (1/6)

- Kde končí zákon, nastupuje etika a morálny kódex. Aj týmito slovami by sa dal charakterizovať význam slov etika a morálny kódex, najmä vzhľadom na skutočnosť, že zákony a právne predpisy nedokážu, a ani nemôžu definovať všetky potrebné detaily a konkrétne kroky alebo postupy.
- V určitých špecifických prípadoch je preto potrebné definovať určité zásady „rozumného“ správania sa, tzv. morálne kódexy.
- Definovanie týchto zásad môže, v niektorých prípadoch, slúžiť aj na zvýšenie profesionálneho renomé a dôveryhodnosti v konkrétnu organizáciu alebo spoločnosť, resp. ľudí, ktorí sú jej súčasťou.
- Definovanie a samozrejme aj riadenie sa príslušnými etickými a profesionálnymi kódexmi môžeme vidieť najmä pri organizáciách zaoberajúcimi sa oblasťou riadenia, bezpečnosti a kontroly informačných systémov a technológií (napr. medzinárodná organizácia ISACA - Information Systems Audit and Control Association).

Etika a morálny kódex (2/6)

- Dodržiavanie etických princípov pri používaní Internetu a IKT vôbec je základným predpokladom udržania bezpečnosti štátu a súkromia občanov. V súvislosti so súčasným trendom v oblasti rozvoja technológií a ich priaznivých dopadov na náš každodenný život je tiež nutné poukázať na etickú a morálnu stránku používateľov a rovnako aj správcov týchto technológií.
- Predstava toho, čo jedinec považuje za správne vychádza z postojov, hodnôt a pravidiel, ktoré sa menia vzhľadom na okolie a kultúru.
- Obe strany (subjekt prijímateľa aj morálne vzory, ktoré nás obklopujú) sú menné v čase a kontexte, ktorý môže byť politický, spoločenský a technologický.
- Jedinec si vytvára určitú hodnotovú preferenciu na základe určitých stretov hľadísk a hodnôt vštepovaných odpozorovaním správania podľa všeobecne akceptovaných noriem.
- Tieto všeobecne prijímané normy správania môžu byť formalizované a prevedené do právnych noriem a príkazov, tým dochádza k vytvoreniu legislatívneho rámca, alebo do noriem platných v rámci organizácie. Od legislatívy sa neformalizovaná etika líši tým, že nie je právne zakotvená a jej porušenie nemôže byť súdne vymáhané, za určitých podmienok však môže byť stále sankcionované.

Etika a morálny kódex (3/6)

- Naša sloboda je závislá na mnohých činiteľoch, ktoré nám zároveň poskytujú základnú oporu pre osobný rozvoj.
- Každý jedinec by mal preto poskytovať ostatným priestor na takú osobnú slobodu, akú si sám želá mať a tým vytvoriť základ pre rozvoj vzájomnej úcty.
- Tvorba, sprístupňovanie a šírenie informácií masovým médiom, ako je Internet ponúka platformu pre formovanie charakteru jedincov koexistujúcich v spoločnosti.
- Vzrastá preto potreba definovania morálnych pravidiel pre narábanie s informáciami.

Etika a morálny kódex (4/6)

Morálne kódexy:

- Profesijné kódexy nie sú právne zakotvené, tvoria len určité pomocné rámce pri rozhodovaní v hraničných situáciách, vychádzajú z obecnej etiky a spoločenských princípov.
- Etický kódex profesionála v oblasti IT by mal vychádzať z niekoľkých základných princípov:
  - chrániť právo na súkromie používateľov informačného systému, ktorý spravuje,
  - rešpektovať právo na duševné vlastníctvo, zásady intelektuálnej slobody,
  - dodržiavať zásady ochrany osobných údajov, zakotvené v legislatíve,
  - nepresadzovať vlastné záujmy na úkor používateľov,
  - zodpovedne zabrániť cenzúre,
  - dodržiavať hranice medzi vlastným presvedčením a profesijnými povinnosťami.

Etika a morálny kódex (5/6)

Počítačová kriminalita a etický hacking:

- Môžeme konštatovať, že etický hacking je v podstate auditom, t.j. hodnotením bezpečnosti systému, vrátane pokusu o narušenie daného systému pomocou rovnakých techník, aké by v praxi použil nebezpečný útočník.
- Samotné narušenie systému sa nazýva penetračným testom.
- Cieľom takejto činnosti je poskytnúť objednávateľovi auditu správu o zraniteľnostiach, ktorá mu pomôže zbaviť sa všetkých zraniteľností testovaného systému, ideálne ešte predtým, než by mohol byť vystavený reálnemu riziku.

Etika a morálny kódex (6/6)

Počítačová kriminalita a etický hacking:

- V rámci etického hackingu organizácie dochádza spravidla k manuálnemu posudzovaniu bezpečnosti sieťovej infraštruktúry, vo väčšine prípadoch aj s využitím automatizovaných nástrojov.
- Samotný výstup automatizovaných nástrojov nie je ani zďaleka postačujúci, pretože hrozby súvisiace so zraniteľnosťami sa navzájom zosilňujú a spolu predstavujú omnoho vyššie riziko, ktoré musí byť posúdené skúseným profesionálom v oblasti informačnej bezpečnosti.
- Pred vykonaním auditu sa zvyčajne podpisuje zmluva, ktorá definuje v akom rozsahu a do akej hĺbky bude testovanie bezpečnosti prevedené.
- Dohaduje sa tiež úroveň agresivity, ktorú môžu etickí hackeri pri tejto činnosti použiť, aby sa neohrozila produkčná, alebo inak dôležitá infraštruktúra, definujú sa prípadné miery sankcií, ktoré vyplývajú z nedodržania podmienok zmluvy a pod.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

VIII. časť

VEREJNÉ OBSTARÁVANIE IKT

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Verejné obstarávanie IKT (1/4)

- Ministerstvo financií Slovenskej republiky rôznymi návrhmi opatrení prispelo k účelnému, transparentnému a efektívnemu obstarávaniu IKT.
- Na základe podnetov od odbornej aj laickej verejnosti vydalo "Návrh opatrení na zvýšenie transparentnosti v súvislosti s nákupom a využívaním informačno-komunikačných technológií vo verejnom sektore". Následne boli vypracované rôzne metodické usmernenia.
- Ďalším dôležitým činiteľom, ktorý prispel k vyššej transparentnosti verejného obstarávania je zákon č. 25/2006 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov. Je dôležité korigovať pokrytie biznis procesov informačnými systémami a podporovať konkurenčné prostredie, nediskriminovať rôzne spôsoby poskytovania služieb pri nákupe prostriedkov IKT.
- Práve tento zákon o verejnom obstarávaní má za úlohu zaistiť nezávislosť projektov na konkrétnych proprietárnych riešeniach a zabrániť nevyhnutnej závislosti objednávateľa na konkrétnych dodávateľoch.
- Úrad pre verejné obstarávanie zároveň vydal aj metodické usmernenie.

Verejné obstarávanie IKT (2/4)

- Hlavné body metodického usmernenia ÚVO z pohľadu IB:
  - ???

- Na základe aktuálnych skúsenosti a praxe môžeme konštatovať, že neoddeliteľnou súčasťou súťažných podkladov by mali byť aj požiadavky:
  - z pohľadu bezpečnosti riešenia a požadovanej bezpečnostnej funkcionality obstarávaných systémov a aplikácií,
  - na vykonanie, od dodávateľa nezávislého, posudzovania kvality implementácie,
  - na vykonanie nezávislého auditu súladu s požiadavkami legislatívy, najmä výnosu MFSR o štandardoch pre ISVS, ešte pred ukončením a odovzdaním diela,
  - na vykonanie nezávislého bezpečnostného auditu systémov a aplikácií a auditu súladu naplnenia definovaných bezpečnostných požiadaviek, rovnako pred odovzdaním a akceptovaním samotného diela.

Verejné obstarávanie IKT (3/4)

- Uvedený prístup umožňuje efektívne vynakladanie prostriedkov, nakoľko prípadné nedostatky musia byť odstránené v rámci dodávky a nie až na základe dodatočných „change requestov“ za dodatočné finančné náklady. Zároveň sa eliminuje riziko, že bude do prevádzky spustený systém, ktorý predstavuje bezpečnostné riziko pre dáta a informácie, ktoré tento systém spracováva.
- Je dôležité zabezpečiť aby bezpečnosť bola integrálnou súčasťou projektu, t.j. už jeho úvodných analytických fáz a samozrejme aj fázy návrhu riešenia a samotnej implementácie a záverečných testov. Vo veľa prípadoch je bezpečnosť len „okrasný prívesok“, ktorý sa na riešenie zavesí niekedy na konci projektu, alebo vôbec.

Verejné obstarávanie IKT (4/4)

- Rovnako je potrebné myslieť na požiadavky týkajúce sa testovanie systému, najmä ak bude potrebné niektoré testy vykonať na produkčných, tzv. „ostrých“ dátach, napr. v testovacom prostredí dodávateľa. V tomto prípade sa odporúča zvoliť vhodný typ „anonymizácie“ týchto dát, tak aby „anonymizované“ dáta nemali žiadnu vypovedaciu hodnotu ale zároveň aby spĺňali požiadavky potrebné na samotné testovanie funkčnosti systému.
- V prípade obstarávania zložitejších systémov, resp. systémov, kedy súčasťou dodania nie je len produkčné prostredie ale napr. aj vývojové alebo minimálne testovacie prostredie je potrebné v požiadavkách zadefinovať aj príslušné bezpečnostné požiadavky vyplývajúce z uvedenej skutočnosti, napr. požiadavky na infraštruktúru, sieťové prostredie, prípadne aj fyzické oddelenie jednotlivých prostredí a pod.
- Rovnako je potrebné pri uzatváraní zmluvného vzťahu s vybraným dodávateľom pamätať aj na tzv. „NDA (Non Disclosure Agreement)“ dohody, čiže ustanovenia o zachovávaní mlčanlivosti a samozrejme aj na tzv. „SLA (Service Level Agreement) dohody, ktoré špecifikujú úrovne poskytovaných služieb, najmä pre účely údržby a servisu ale aj v prípade, že dodávateľ priamo poskytuje („outsourcuje“) službu, ktorú by mal za štandardných okolností poskytovať objednávateľ.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

IX. časť

FORENZNÁ ANALÝZA

KPMG
cutting through complexity™

Forenzná analýza (1/8)

- Cieľom forenznej analýzy je spravidla potvrdiť, alebo vyvrátiť podozrenie z nelegálnej činnosti, t.j. usvedčiť páchateľa, alebo dokázať nevinu obvineného. Na tento účel sa podľa prísnych pravidiel získavajú dôkazy z tzv. „dôkazových médií“ tak, aby tieto dôkazy neboli napadnuteľné na súde.
- Ďalším krokom v postupe je analyzovať získané dôkazy a bezpečne ich uchovať. Medzi etické pravidlá, ktoré je forenzný analytik povinný pri spracovaní dodržať patrí prezentácia výsledkov analýzy iba oprávneným adresátom.
- Legislatíva v oblasti súdneho vyšetrovania viazaná na aspekty forenznej analýzy je pokrytá súdnym poriadkom, zákonom o znalcoch a zákonom o policajnom zbore.
- Uvedené zákony čiastočne stanovujú aj to, aké postupy je vhodné pri forenznej analýze zvoliť.
- Postupy pri forenznej analýze však spravidla nasledujú rámec:
  - príprava,
  - otvorenie prípadu,
  - získavanie dôkazov,
  - bezpečné uchovanie dôkazov,
  - analýza dôkazov,
  - vytvorenie hlásenia,
  - uzatvorenie prípadu,
  - svedectvo.

Forenzná analýza (2/8)

Požiadavky na zaistenie dôkazov použiteľných v právnych úkonoch:

- Dôkazovými médiami sú v prípade vyšetrovania bezpečnostných incidentov spravidla pevné disky, flash disky, CD a DVD, pamäťové karty.
- Základnou dobrou praktikou v súvislosti s vyšetrovaním je vytvoriť bitový obraz analyzovaného média.
- Tento by mal byť vytvorený na tento účel certifikovanými nástrojmi, ktoré dokážu urobiť obraz pamäťového média jedna k jednej, vrátane „prázdneho“ pamäťového miesta, resp. miesta aktuálne neobsadeného žiadnym súborom.
- Nie všetky nástroje, ktoré dokážu urobiť napr. obraz HDD sú na takúto činnosť vhodné, pretože väčšina komerčných alebo aj „free“ produktov vykonáva len obraz obsadeného pamäťového miesta a navyše pre zníženie nárokov na kapacitu uloženia takto vytvoreného obrazu realizujú aj komprimáciu týchto dát.

Forenzná analýza (3/8)

- Operačnú pamäť je možné vyšetrovať pri zapnutom zariadení, ktorého funkčný stav nie je dobré vychyľovať, dochádza tým k nežiaducemu pozmeneniu informácií o tom, ako bol počítač používaný v čase incidentu.
- Problémom je, že stav pamäte sa pri bežiacom systéme mení bez ohľadu na aktivity súvisiace s forenznou analýzou.
- Forenzná analýza pamäťových modulov využíva fakt, že bežné mazanie je nedokonalé – za normálnych okolností vymazané dáta s vysokou pravdepodobnosť nie sú vymazané bezpečne.
- Pokiaľ páchateľ nepoužil sofistikované spôsoby niekoľkonásobného vymazania a prepísania disku vygenerovanými náhodnými dátami, je možná ich obnova a tiež zistenie času vymazania.

Forenzná analýza (4/8)

- Ďalším dôkazovým materiálom sú logy sieťových zariadení a serverov poskytujúcich služby, pokiaľ sa uchovávajú relatívne, resp. vzhľadom na konkrétny prípad dostatočne dlho.
- Okrem prípadného vyhodnocovania incidentov je možné ich použiť aj na optimalizáciu prevádzky systému alebo siete.
- Logovacie záznamy sieťových zariadení sa tiež často exportujú do geograficky vzdialených lokalít a preto je už aj v málo zložitých infraštruktúrach takmer nemožné sa ich zbaviť.
- Dôkazy je možné zbierať pri aktívnom zariadení („in vivo“), alebo pri neaktívnom zariadení („post mortem“).

Forenzná analýza (5/8)

- Pri prvom spôsobe sa najefektívnejšie analyzuje operačná pamäť a je možné z nej „vydolovať“ veľké množstvo informácií.
- Pri realizácii tohto druhu analýzy na systéme je neprípustné dôverovať výstupu aplikácií systémových binárnych súborov nainštalovaných na inkriminovanom systéme.
- Je preto užitočné mať k dispozícii dôveryhodné binárne súbory. Súbory získavané z tohto druhu analýzy majú rôzne stupne „volatility“ („dočasnosti“). Preto sa dostupnými prostriedkami získava v prvom rade cache procesora, neskôr môže nasledovať obraz pamäte RAM, swap pamäť, pevné disky a pamäťové médiá USB, CD a DVD médiá.
- Tento spôsob získavania dôkazov umožňuje obísť plné šifrovanie dát uložených na disku, pretože sú odšifrované použitím kľúčov uložených v operačnej pamäti. Tieto kľúče je možné z bežiaceho systému extrahovať. Túto techniku využívajú napríklad aj útočníci pri pokusoch o kompromitáciu bežiacich systémov metódou „cold boot attack“.

Forenzná analýza (6/8)

- Druhý spôsob analýzy je menej komplikovaný, vyžaduje nižšiu úroveň expertízy. Nevýhodou môže byť, pri určitých typoch incidentov, nižšia efektivita získavania relevantných dôkazov a tiež ich nižšie konečné množstvo. V takomto prístupe sa pomocou špecifických nástrojov analyzuje získaný obraz média.
- Pri vyšetrovaní bezpečnostných incidentov sa postupuje v súlade s niekoľkými hlavnými atribútmi, ktorými sú:
  - korektnosť – môžeme zaručiť, že získané dáta sú totožné s dátami na originálnom médiu,
  - autentickosť – získané dáta sme skutočne získali z analyzovaného zariadenia v danom čase,
  - integrita – dáta, ktoré sme získali, nesmú byť pozmenené voči originálu,
  - minoritne tiež dôvernosť a dostupnosť, ktoré ale nie sú priamym predmetom vyšetrovania,
  - opakovateľnosť – každý krok vyšetrovania je možné zopakovať na základe dokumentácie s použitím bezpečne uložených originálnych dôkazových materiálov,
  - akceptovateľnosť – metóda musí byť súdom akceptovaná ako legitímna,
  - spoľahlivosť – metóda musí byť dokázateľne správna,
  - logická nadväznosť na predmet prípadu.

Forenzná analýza (7/8)

- Šifrovanie dát obvinenému pomôže zachovať ich dôvernosť, ale prítomnosť šifrovacieho softvéru, alebo priamo zašifrovanie celého disku môže nepriamo naznačovať snahu páchateľa o skrývanie dôkazov.
- Rovnako je to s prítomnosťou steganografických nástrojov určených na skrývanie dát do zdanlivo bežných multimediálnych súborov, akými sú obrázok, alebo audio/video sekvencia.
- Pre obvineného je často rozumnejšie si v prípade steganografie vytvoriť a aplikovať vlastný algoritmus.
- Pri steganografii sa totiž dá uplatniť podobné pravidlo ako pre používanie šifrovania, že ak obvinený dokázateľne použil steganografický nástroj, môže to byť pre súd nepriamym náznakom jeho viny.

Forenzná analýza (8/8)

- Tieto prípady je však nutné posudzovať v súvislosti s inými faktami, ktoré sú o obvinenom známe – nebolo by legitímne obvineného odsúdiť kvôli používaniu anonymizačných techník, šifrovania, alebo steganografie, ktorých využívanie je inak na území SR celkom legálne.
- Nástroje, ktorých výrobcovia proklamujú, že majú tzv. „anti-forenznú“ funkcionalitu sú často neúčinné. Zničenie dát, ktoré slúžia ako materiál pre forenznú analýzu, je v praxi veľmi náročné.
- Ani fyzická likvidácia často nie je postačujúca, určité časti dát je možné zrekonštruovať aj zo zničeného média.
- Pre vyššiu presnosť zistení je užitočné dôkazy získané pri forenznej analýze IKT doplniť metadátami a nedigitálnymi dôkazmi a tým získať komplexný obraz o incidente.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Záver

ČO POVEDAŤ ÚPLNE NA ZÁVER?

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Záver (1/2)

- V súvislosti s informatizáciou sa verejný sektor stáva závislým na robustných informačných systémoch a ich uplatnení, najmä v oblasti zdravotníctva, energetiky, verejnej správy a elektronického obchodu.
- Je prakticky nerealizovateľné riešiť zabezpečenie IKT systémov pomocou individuálnych projektov a je nutné stanoviť systematické bezpečnostné požiadavky.
- Činnosti koordinácie ochrany digitálneho priestoru sú zo zákona zabezpečované viacerými štátnymi aj neštátnymi inštitúciami. Legislatíva v oblasti informačnej bezpečnosti významne prispela k zlepšeniu stavu informačnej bezpečnosti v SR.
- Zároveň môžeme konštatovať, že má pozitívny trend, nakoľko boli identifikované aktivity ohľadom prípravy a prijímania ďalších nových predpisov, ako je napr. „zákon o informačnej bezpečnosti“.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Záver (2/2)

- Je však potrebné si uvedomiť, že prijatím samotných zákonov sa problém s informačnou bezpečnosťou nevyrieši.
- Vývoj v oblasti IKT a aj v oblasti zraniteľnosti a ich zabezpečovania je fenomén, ktorý sa nedá zastaviť, takže túto „imaginárnu“ a virtuálnu vojnu“ o bezpečnosť systémov a nimi spracovávaných, prenášaných alebo uchovávaných informácií bude potrebné viesť neustále.
- Z uvedeného dôvodu je potrebné, aktuálnym podmienkam a okolnostiam, neustále prispôsobovať nie len samotné systémy, ale aj príslušné legislatívne rámce.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky?

Priestor na otázky:

- Aké sú vaše skúsenosti s aplikovaním bezpečnostných opatrení v podmienkach MF?
- Čo by ste vyzdvihli ako pozitívum a čo naopak zmenili?

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

ĎAKUJEME ZA POZORNOSŤ!

KPMG
cutting through complexity™