Bezpečnostná politika, Bezpečnostný projekt

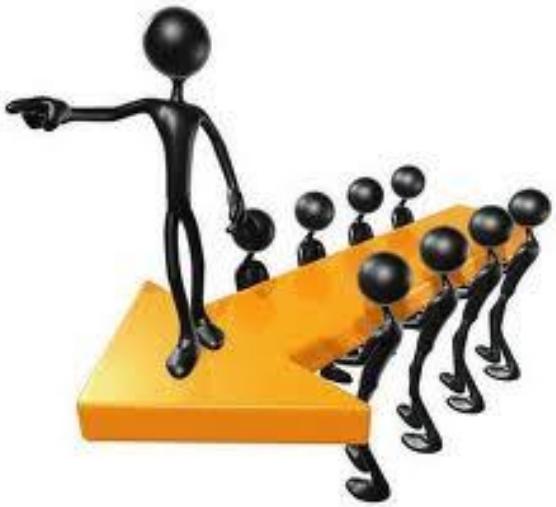
(prezentácia spoločnosti SOMI Systems a.s.)

RNDr. Daniel Schikor
Produktový manažér
Tel.: 0903 535 325
E-mail: schikor@somi.sk
Website: www.somi.sk

Obsah prezentácie

- Predstavenie spoločnosti SOMI Systems
- Bezpečnostná politika v samospráve
- Výnos Ministerstva financií 312/2002
- Definovanie pojmu „Osobný údaj“
- Zákon č. 428/2002 Z.z.
- Definovanie pojmu „Informačné systémy“
- Najčastejšie problémy z praxe
- Bezpečnostný projekt

SOMI Systems



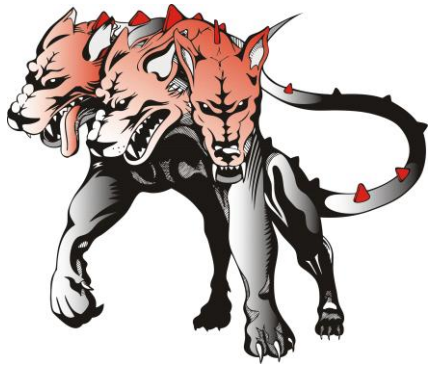
- spoločnosť založená na Slovensku
- sídlo v Banskej Bystrici
- 19 ročné pôsobenie na trhu
- tvorba vlastných produktov
- orientácia na internetovú komunikáciu
- zákaznícky segment
  - štátne a verejné inštitúcie
  - súkromné spoločnosti

SOMI Systems

- založenie a prevádzkovanie webmailového portálu

- v roku 2005 predané do spoločnosti Atlas

Produkty a služby



1. **Bezpečnosť a správa počítačových sietí**

   produkt KERBER (www.kerber.sk)

2. **Ochrana osobných údajov**

   bezpečnostné projekty/politika, audit BP

3. **Školenia a workshopy**

   bezpečnostný projekt, LINUX, laickí používatelia

4. **Projektovanie a realizácia dátových sietí**

   metalické a optické siete

5. **Predaj počítačových zariadení**
6. **Individuálne zákazkové riešenia**

   napr. šifrovaná mobilná komunikácia

BEZPEČNOSTNÁ POLITIKA V SAMOSPRÁVE

Samospráva a zákony

Zákon o ochrane osobných údajov 428/2002 Z.z.

Výnos ministerstva financií o štandardoch pre informačné systémy 312/2010

Bezpečnostná politika

Nevyhnutnou podmienkou spoľahlivej a efektívnej práce celého bezpečnostného systému je splnenie základných požiadaviek na implementáciu bezpečnostných mechanizmov, vypracovanie procedúr a zavedenie organizačnej štruktúry bezpečnosti v podmienkach organizácií. Tieto požiadavky sú definované v **Bezpečnostnej politike** a mali by byť ďalej rozpracované v interných predpisoch a metodických pokynoch.

Bezpečnostná politika musí byť ako dokument schválený vedením spoločnosti ako záväzná vnútropodniková smernica.

Bezpečnostná politika

Bezpečnostná politika ponúka odpoveď na niekoľko základných otázok:

- čo chceme chrániť
- prečo to chceme chrániť
- ako to chceme chrániť
- čo budeme robiť, keď dôjde k zlyhaniu systému

Bezpečnostná politika

Bezpečnostná politika sú dokumenty a postupy, ktorý schvaľuje vedenie organizácie a určujú:

- hlavné ciele, ktoré sa majú dosiahnuť implementáciou bezpečnostnej politiky
- postup implementácie jednotlivých súčastí bezpečnostného systému a zodpovednosť zamestnancov za túto implementáciu
- zodpovednosť za prevádzku a kontrolu bezpečnostného systému a popis vzťahu medzi organizačnými zložkami vo veciach bezpečnosti

Bezpečnostná politika

Bezpečnostná politika sú dokumenty a postupy, ktorý schvaľuje vedenie organizácie a určujú:

- dobu a spôsob aktualizácie kľúčových dokumentov dotýkajúcich sa bezpečnosti (najmä Bezpečnostného projektu)
- spôsob a periodicitu vyhodnocovania stavu bezpečnosti v organizácii
- postup pri povoľovaní použitia nových komponentov informačného systému, zariadení majúcich vplyv na bezpečnosť a ochranu organizácii

Bezpečnostná politika

Aktíva – sú všetky hmotné i nehmotné hodnoty, ktoré úrad vlastní, alebo využíva a slúžia najmä na plnenie jeho služieb obyvateľstvu. Medzi hmotné aktíva patria najmä administratívne priestory, počítače, počítačové siete, komunikačné zariadenia a ďalšie hmotné premety vo vlastníctve úradu. Medzi nehmotné aktíva patria pracovné postupy, know-how, údaje o zamestnancoch, ekonomické, finančné a obchodné údaje, majetkové a obdobné práva a ďalší nehmotný majetok. Medzi aktíva patria tiež osoby, ktoré sú v zamestnaneckom, obchodnom, majetkovom alebo inom obdobnom vzťahu k úradu.

Hrozby – sú vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne, alebo neúmyselne vplývajú na aktíva úradu tak, že ich úrad nemôže využívať, alebo inak ohrozujú oprávnené záujmy úradu.

Bezpečnostná politika

Zavedenie bezpečnostnej politiky do života organizácie

- Spracovanie detailnej analýzy rizík pre vybrané aktíva z oblasti informačných systémov, oblasti technológií, fyzickej a režimovej ochrany, ochrany osôb
- Vypracovanie bezpečnostných dokumentov
- Okamžité kroky ochrany - realizácia krátkodobých opatrení na odstránenie najväčších rizík
- Integrácia bezpečnostných mechanizmov do aplikácií a informačného systému

Bezpečnostná politika

Zavedenie bezpečnostnej politiky do života organizácie

- Realizácia opatrení technickej a režimovej ochrany pre ochranu zamestnancov a im zverených prostriedkov
- Implementácia bezpečnostných mechanizmov do bežnej prevádzky a chodu organizácie (automatizovaných aj neautomatizovaných)
- Sledovanie a vyhodnocovanie stavu bezpečnosti informačného systému
- Realizácia systémových a organizačných opatrení, realizácia výchovno-vzdelávacieho programu
- Zavedenie auditu

Bezpečnostná politika

Bezpečnostná politika a jej zavedenie by sa malo týkať hlavne :

- **fyzická bezpečnosť** – zahŕňa pôsobenie hrozieb na hmotné aktíva potrebné pre prevádzkovanie IS ale aj spôsoby zničenia už nepotrebných informácií alebo už nepotrených médií s informáciami

- **komunikačná bezpečnosť** – zahŕňa pôsobenie hrozieb na nehmotné aktíva počas ich prenosu, ukladania a spracovávania, proti vírusom, trojským koňom, červom, ochranou pred neoprávneným prienikom zo siete Internet

Bezpečnostná politika

Bezpečnostná politika a jej zavedenie by sa malo týkať hlavne :

- **počítačová bezpečnosť** – zahŕňa pôsobenie hrozieb na hmotné aktíva (hardvér) potrebné pre spracovanie, zahŕňa aj výber a spoľahlivosť technických prostriedkov IS, zabezpečenie ich okamžitého servisu, kontrolu prístupu k týmto prostriedkom

- **logická bezpečnosť** – zahŕňa pôsobenie hrozieb na nehmotné aktíva nevyhnutné pre fungovanie IS z hľadiska organizačného spracovania informácie – t.j. aby bola zabezpečená kontrola prístupu, identifikácia a autentizácia užívateľov, rozdelenie právomocí užívateľom, sledovanie a záznam činnosti systému aj užívateľov

- **personálna bezpečnosť** – zaoberá sa predovšetkým elimináciou hrozieb spôsobených ľudským faktorom

Bezpečnostná politika

Kritické faktory úspechu:

- bezpečnostná politika, ciele a aktivity odrážajúce podnikateľské ciele organizácie
- prístup a rámec na implementovanie, udržiavanie, monitoring a zlepšovanie informačnej bezpečnosti, ktorý je konzistentný s podnikovou kultúrou organizácie
- viditeľná podpora a angažovanosť na všetkých úrovniach riadenia
- dobré porozumenie bezpečnostným požiadavkám, ohodnoteniu rizík a riadeniu rizík

Bezpečnostná politika

Kritické faktory úspechu:

- efektívny marketing informačnej bezpečnosti pre všetkých manažérov, zamestnancov a tretie strany s cieľom dosiahnuť primerané bezpečnostné povedomie
- distribúcia návodu na používanie politiky informačnej bezpečnosti a noriem ku všetkým manažérom, zamestnancom a tretím stranám
- poskytovanie finančných prostriedkov pre aktivity informačnej bezpečnosti
- poskytovanie vhodného bezpečnostného povedomia, školení a vzdelávania

Bezpečnostná politika

Kritické faktory úspechu:

- zavedenie efektívneho procesu riadenia incidentov informačnej bezpečnosti
- spätná väzba na inšpirovanie zlepšenia

Bezpečnostná politika

Ukončením zavedenia bezpečnostnej politiky do praxe nedochádza k trvalému vyriešeniu bezpečnosti informačného systému, k trvalému vyriešeniu technickej a režimovej ochrany majetku, ochrany osôb. Nevyhnutnou podmienkou spoľahlivej a efektívnej práce celého bezpečnostného systému je neustále vyhodnocovanie jeho používania, vyhodnocovanie incidentov, aktualizácia dokumentov a kritické prehodnocovanie schopností bezpečnostného systému plniť svoje funkcie.

Výnos MF 312/2010

Dňom 1.októbra 2008 nadobudol platnosť výnos Ministerstva financií o štandardoch pre informačné systémy verejnej správy, ktorý bol upravený a doplnený výnosom Ministerstva financií 312/2010 s účinnosťou od 15.7.2010 .

Štandardom je súbor pravidiel spojených s vytváraním, rozvojom a využívaním informačných systémov verejnej správy, ktorý obsahuje charakteristiky, metódy, postupy a podmienky, najmä pokiaľ ide o bezpečnosť a integrovateľnosť s inými informačnými systémami. Štandardy musia byť otvorené a technologicky neutrálne.

Výnos MF 312/2010

Štandardy pre architektúru riadenia

Riadenie informačnej bezpečnosti (§28)

Informačná bezpečnosť ako taká musí byť niekým riadená a fungovať na základe určených pravidiel, aby bolo možné predísť bezpečnostným incidentom (napr. únikom informácií, zneužitím právomocí používateľov, útokom na iné systémy atď.) alebo ho čo možno najrýchlejším zásahom potlačiť, prípadne vyvodiť dôsledky. Dobre vytvorené riadenie informačnej bezpečnosti je základom istoty pri používaní info-komunikačných technológii. Základ bezpečnostnej politiky je ekvivalentný s bezpečnostným zámerom podľa §16 ods. 4 zákona č. 428 / 2002 Z. z. o ochrane osobných údajov, s rozšíreniami o niektoré presnejšie špecifikácie. Bezpečnostná politika ako taká vychádza z STN ISO/IEC 27001 a ďalších súvisiacich noriem.

Výnos MF 312/2010

Štandardy pre architektúru riadenia

Personálna bezpečnosť (§29)

Organizácia má zabezpečiť, aby si zamestnanci boli vedomí svojej zodpovednosti a boli pravidelne informovaní alebo školení o aktuálnych trendoch v oblastiach informačnej bezpečnosti, vedeli ako sa majú správať v prípade narušenia niektorého aspektu informačnej bezpečnosti, t. j. musia byť jasne definované pravidlá bezpečnej prevádzky systému/ systémov. Dôležitou súčasťou je aj vyvodzovanie dôsledkov narušenia bezpečnosti a zodpovednosť relevantných osôb a užívateľov.

Výnos MF 312/2010

Štandardy pre architektúru riadenia

Manažment rizík pre oblasť informačnej bezpečnosti (§30)

implementácia systému riadenia a monitorovania rizík v súvislosti s informačnými systémami verejnej správy, a to najmä podľa relevantných technických noriem (STN ISO 27001 alebo 17799), a pravidelné zbieranie relevantných údajov súvisiacich s rizikami.

Kontrolný mechanizmus riadenia informačnej bezpečnosti (§31)

V rámci kontinuity činnosti sa odporúča uskutočňovať aj testovanie a audit samotných bezpečnostných procedúr.

Výnos MF 312/2010

Štandardy minimálneho technického zabezpečenia

Ochrana proti škodlivému kódu (§32)

Škodlivý kód zahŕňa najmä škodlivý softvér, ale taktiež napr. aj skripty (na webových sídlach a podobne), ktoré sa vo všeobecnosti nepovažujú za softvér a takisto môžu byť zdrojom bezpečnostných incidentov.

Sieťová bezpečnosť (§33)

Zavádzanie firewallu a ďalších relevantných ochranných prostriedkov sa odporúča nielen na hraničných miestach siete do vonkajšieho prostredia, ale aj na vstupe jednotlivých používateľských staníc (PC) do siete, nakoľko veľké percento bezpečnostných incidentov je spôsobené infikovaním „zvnútra“ siete.

Výnos MF 312/2010

Štandardy minimálneho technického zabezpečenia

Fyzická bezpečnosť a bezpečnosť prostredia (§34)

Obyčajný výpadok prúdu môže mať omnoho citeľnejšie následky na kontinuitu činnosti a produktivitu organizácie ako bezpečnostný prienik. Vytvorenie zabezpečeného priestoru najmä pre servery obsahujúce zdrojové údaje a podobne je nevyhnutnou súčasťou ochrany informačného systému verejnej správy.

Aktualizácia softvéru (§35)

Zneužívanie bezpečnostných chýb softvérov je v súčasnosti záležitosťou veľmi krátkeho obdobia (od vzniku povedomia o chybe do jej zneužitia sú to iba dni). Je preto potrebné mať všetky ochranné prostriedky neustále aktuálne a „zaplátané.

Výnos MF 312/2010

Štandardy minimálneho technického zabezpečenia

Monitorovanie a manažment bezpečnostných incidentov (§36)

Dôležitou súčasťou ochrany informačných systémov verejnej správy na národnej úrovni je výmena informácií o bezpečnostných incidentoch, čo má za následok prevenciu pred opakovanými útokmi rovnakého typu na rôzne systémy verejnej správy. Upozorňujeme, že takáto výmena informácií by mala prebiehať dôveryhodným spôsobom a dôveryhodným osobám.

Periodické hodnotenie zraniteľnosti (§37)

Vzhľadom na neustále dopĺňanie a aktualizáciu funkcií a súčastí informačných systémov, ako aj stále vznikajúce nové hrozby a možnosti nových technológií, je aktualizácia zraniteľnosti nevyhnutnou súčasťou bezpečnostnej údržby informačných systémov.

Výnos MF 312/2010

Štandardy minimálneho technického zabezpečenia

Zálohovanie (§38)

Za vytvorenie zálohy na dátovom nosiči sa považuje vytvorenie kópie definovaných údajov na DVD, CD, prenosnom hard disku (HD), sieťovom zálohovacom mieste alebo inom podobnom médiu. V zmysle výnosu MF SR je nutné, aby súčasne existovali tri zálohy – jedna prevádzková a dve archivačné.

Fyzické ukladanie záloh (§39)

Fyzické ukladanie prevádzkových záloh, jednej kópie archivačnej zálohy a dátových nosičov s licencovaným softvérom do uzamykateľného priestoru. Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte.

Výnos MF 312/2010

Štandardy minimálneho technického zabezpečenia

Riadenie prístupu (§40)

Prístup do informačných systémov a k rôznym údajom je vnímaný ako jedno z najkritickejších miest ochrany bezpečnosti, nakoľko jeho zneužitie môže mať rozsiahle finančné, morálne, ale aj iné následky.

Nutnosť vypracovať interný akt riadenia prístupu k údajom a funkciám informačného systému verejnej správy založeného na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh.

Určenie bezpečnostných zásad na mobilné pripojenie do informačného systému verejnej správy a pre prácu na diaľku.

Automatické zaznamenávanie každého prístupu každého používateľa vrátane administrátora do informačného systému verejnej správy

Výnos MF 312/2010

Štandardy minimálneho technického zabezpečenia

Aktualizácia informačno-komunikačných technológií (§41)

Všetky zmeny existujúcich informačných systémov, ako aj zavádzanie nových informačných systémov alebo ich častí, musia už od začiatku zahŕňať informačnú bezpečnosť ako svoju neoddeliteľnú súčasť. Jedným z najväčších problémov nedostatočnej ochrany IKT, ktorej dôsledkom je napr. existencia množstva neidentifikovaných zraniteľností, býva práve dodatočné dopĺňanie bezpečnosti ako nadstavby systému a nie jej priamej integrácie počas budovania systému.

Uchovávanie a aktualizácia dokumentácie o informačných systémoch verejnej správy. Neexistencia dokumentácie býva zásadným problémom najmä pri výmene ľudských kapacít.

Výnos MF 312/2010

Štandardy minimálneho technického zabezpečenia

Účasť tretej strany (§42)

Vzhľadom na to, že dodávanie informačných systémov je väčšinou riešené outsourcovaním, upozorňujeme, že outsourcovať sa dá vyhotovenie diela resp. vykonanie práce, nie však zodpovednosť za informačný systém. Tá naďalej zostáva jeho správcovi prípadne prevádzkovateľovi.

Okrem základných požiadaviek na bezpečnosť sa odporúča zabezpečiť dodávacie zmluvy tak, aby prípadné „skryté“ funkcie, ktoré môžu umožniť tvorcovi systému jeho zneužívanie, boli zásadným spôsobom sankcionované a právne postihnuteľné.

Osobné údaje

Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu – napríklad Meno, priezvisko, akademický titul, dátum narodenia, rodné číslo, adresa, meno, priezvisko, dátum narodenia, rodné číslo, akademický titul, manžela (manželky) a detí počet detí, náboženské vyznanie, majetkové pomery, údaje o dosiahnutom vzdelaní, údaje o príjmoch, poberaní dôchodku, členstvo v politických organizáciách, členstvo v odborovej organizácii... Pritom za jeden z najdôležitejších osobných údajov s atribútom všeobecne použiteľný identifikátor, je považované rodné číslo, ktoré jednoznačne identifikuje dotknutú osobu.

Osobné údaje

Osobné údaje znamenajú akúkoľvek informáciu, ktorá sa týka identifikovanej alebo identifikovateľnej fyzickej osoby .

- **„akékoľvek informácie“** - Z hľadiska charakteru informácií zahŕňa pojem osobné údaje akýkoľvek druh údajov o osobe. Vzťahuje sa na „objektívne“ informácie a zahŕňa aj „subjektívne“ informácie, názory alebo hodnotenia.

  Príklad : Telefónbanking: V prípade telefónbankingu, pri ktorom sa hlas zákazníka, ktorý dáva banke pokyny, nahráva na pásku, by sa takéto nahrané pokyny mali považovať za osobné údaje.

  Príklad : Videomonitorovanie : Obrazy osôb zachytených systémom videomonitorovania môžu byť osobnými údajmi, pokiaľ sú jednotlivci rozpoznateľní.

Osobné údaje

- **„týkajúce sa“** - Informácie sa vo všeobecnosti môžu pokladať za informácie, ktoré sa „týkajú“ jednotlivca, ak sú *o uvedenom jednotlivcovi.*

  Tento vzťah sa dá v mnohých situáciách ľahko určiť. Napríklad údaje nachádzajúce sa v individuálnom súbore osoby na personálnom oddelení sa jasne „týkajú“ zamestnaneckého postavenia osoby. Rovnako aj údaje o výsledkoch lekárskych vyšetrení pacienta uvedené v jeho zdravotných záznamoch alebo obraz osoby na videozázname z pohovoru s uvedenou osobou.

  Príklad : Hodnota konkrétneho domu je informáciou o veci. Je zrejmé, že pravidlá o ochrane údajov sa nebudú uplatňovať v prípadoch, keď sa takáto informácia bude používať iba na uvedenie príkladu úrovne cien nehnuteľností v určitom okrese. Za určitých okolností by sa však takéto informácie mali považovať aj za osobné údaje. Dom je v skutočnosti majetkom vlastníka, ktorý sa takto použije na stanovenie rozsahu povinnosti tejto osoby, napríklad v súvislosti s platením daní. Z tohto hľadiska bude nepopierateľné, že takéto informácie by sa mali pokladať za osobné údaje.

Osobné údaje

- **„identifikovaná a identifikovateľná“** - Fyzická osoba sa vo všeobecnosti môže považovať za „identifikovanú“ vtedy, keď je v rámci skupiny osôb „odlíšená“ od všetkých ostatných príslušníkov skupiny. Fyzická osoba je preto „identifikovateľná“ vtedy, keď napriek tomu, že osoba ešte nebola identifikovaná, je možné ju identifikovať.

  Osobu možno identifikovať priamo menom alebo nepriamo telefónnym číslom, evidenčným číslom auta, číslom sociálneho poistenia, číslom cestovného pasu alebo spojením dôležitých kritérií, ktoré umožňujú, aby bola spoznaná zúžením skupiny, do ktorej patrí (vek, povolanie, bydlisko, atď.)“.

  Príklad : Zverejnenie röntgenových snímok spolu s pacientovým krstným menom Veľmi nezvyčajná röntgenová snímka jednej ženy bola uverejnená vo vedeckom časopise spolu s jej krstným menom. Krstné meno osoby spolu s vedomosťou jej príbuzných a známych, že trpí určitou chorobou, činia túto osobu identifikovateľnou mnohým osobám a röntgenová snímka by sa potom mala pokladať za osobný údaj.

Zákon č. 428/2002

- Pojednáva o ochrane osobných údajov.
- Doplnený zákonmi č.602/2003, č. 576/2004, č. 90/2005.
- Zákonom je upravená pôsobnosť, oprávnenia a povinnosti orgánov štátnej správy, územnej samosprávy, verejnej moci ako aj ostatných právnických a fyzických osôb, ktoré spracúvajú a ďalej využívajú osobné údaje.
- Zákon stanovuje, že každý subjekt, ktorý plánuje prevádzkovať informačný systém obsahujúci osobné údaje dotknutých osôb je povinný ešte pred začatím ich spracúvania prihlásiť informačný systém na registráciu, respektíve vykonať nevyhnutné administratívne a procedurálne úkony súvisiace s jeho evidenciou a zosúladením so zákonom.

Zákon č. 428/2002

Vymedzenie základných pojmov :

- **prevádzkovateľom** je orgán štátnej správy, orgán územnej samosprávy, iný orgán verejnej moci alebo iná právnická osoba alebo fyzická osoba, ktorá sama alebo spoločne s inými určuje účel a prostriedky spracúvania osobných údajov. Ak účel, prípadne aj prostriedky spracúvania osobných údajov ustanovuje osobitný zákon, prevádzkovateľom je ten, koho na plnenie účelu spracúvania ustanoví zákon alebo kto splní zákonom ustanovené podmienky. To platí aj vtedy, ak tak ustanovuje právny akt Európskych spoločenstiev a Európskej únie.

- **sprostredkovateľom** je orgán štátnej správy, orgán územnej samosprávy, iný orgán verejnej moci alebo iná právnická osoba alebo fyzická osoba, ktorá spracúva osobné údaje v mene prevádzkovateľa alebo zástupcu prevádzkovateľa

Zákon č. 428/2002

Vymedzenie základných pojmov :

- **oprávnenou osobou** je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania alebo v rámci výkonu verejnej funkcie, ktorá môže osobné údaje spracúvať len na základe pokynu prevádzkovateľa, zástupcu prevádzkovateľa alebo sprostredkovateľa, ak tento zákon alebo osobitný zákon neustanovuje inak

- **dotknutou osobou** je každá fyzická osoba, o ktorej sa spracúvajú osobné údaje

Zákon č. 428/2002

- **§ 6 – pojednáva o povinnostiach prevádzkovateľa – účel a prostriedky spracovania osobných údajov**
  - Povinnosť vymedziť účel spracovania osobných údajov pred samotným začatím spracovávania
  - Vylučuje možnosť takých osobných údajov, ktoré sú nezlučiteľné z daným účelom
- **§ 8 – Osobné kategórie osobných údajov**
  - Zakazuje spracovávanie osobných údajov ktoré odhaľujú rasový alebo etnický pôvod, politické názory, vieru, ...
  - Odsek 2 upravuje podmienky spracovávania rodného čísla. rodné číslo možno spracúvať len vtedy, ak bez jeho použitia by mohlo prísť k porušeniu práv a slobôd dotknutých osôb alebo k vážnym chybám pri spracúvaní alebo by bolo znemožnené samotné spracúvanie. Zakazuje sa zverejňovať rodné číslo.

Zákon č. 428/2002

- **§ 10 – získavanie osobných údajov**
  - Špecifikuje pravidlá získavania osobných údajov do IS
  - Povinnosť informovať dotknutú osobu o účele spracovania osobných údajov a názve a sídle prevádzkovateľa
  - Informovanie o poskytnutí údajov tretej strane
  - Získavanie osobných údajov pri jednorazovom vstupe do priestorov
  - Podmienky monitorovania priestoru videokamerami
- **§ 13 – likvidácia osobných údajov**
  - Po splnení účelu spracovania je potrebné osobné údaje zlikvidovať
  - Upravuje prípady keď sa nevyžaduje bezodkladne likvidácia osobných údajov

Zákon č. 428/2002

- **§ 15 – zodpovednosť za bezpečnosť osobných údajov**
  - Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ tým, že ich cháni pred náhodným, ako aj nezákonným poškodením a zničením, náhodnou stratou, nedovoleným prístupom a aj akýmikoľvek inými neprípustnými formami spracúvania.
  - Na tento účel prijme primerané technické, organizačné a personálne opatrenia
- **§ 16 – bezpečnostný projekt**
  - Bezpečnostný projekt vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

Zákon č. 428/2002

- **§ 17 – Poučenie**
  - Prevádzkovateľ alebo sprostredkovateľ je povinný poučiť oprávnené osoby o právach a povinnostiach ustanovených týmto zákonom a o zodpovednosti za ich porušenie. Poučenie sa vykoná pred prvým pokynom na vykonanie operácie s osobnými údajmi.
- **§ 18 – Povinnosť mlčanlivosti**
  - Prevádzkovateľ a sprostredkovateľ sú povinní zachovávať mlčanlivosť o osobných údajoch, ktoré spracovávajú. Mlčanlivosť treba zachovať aj po ukončení spracovávania. Takisto musí zachovať mlčanlivosť aj poverená osoba.

Zákon č. 428/2002

- **§ 19 – dohľad nad ochranou osobných údajov**
  - Za dohľad nad ochranou osobných údajov zodpovedá prevádzkovateľ
  - Ak prevádzkovateľ zamestnáva viac ako päť osôb, výkonom dohľadu poverí zodpovednú osobu. Poverenie musí byť písomné.
  - Povinnosťou prevádzkovateľa je zabezpečiť odborné vyškolenie zodpovedných osôb. Úrad má pravo preveriť vedomosti školeného.
  - Zodpovedná osoba je povinná pred začatím spracúvania osobných údajov vykonať kontrolu, čí ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb.
  - Zodpovedná osoba v priebehu spracúvania osobných údajov upozorňuje na porušenie ustanovení zákona o ochrane osobných údajov

Zodpovedná osoba

- Ak má organizácia viac ako 5 osôb.
- Musí byť písomne poverený zamestnávateľom
- Posudzuje nebezpečenstvo narušenia osobných údajov
- Zabezpečuje súčinnosť s ÚOOÚ, dohľad nad plnením zákona
- Realizáciu technických, organizačných a personálnych opatrení
- Môže byť len bezúhonná fyzická osoba, nemôže byť štatutár
- Povinnosť informovať ÚOOÚ do 30 dní

Zákon č. 428/2002

- **§25, § 26 a § 29 – registrácia a evidencia informačného systému**
  - Za prihlásenie informačného systému na registráciu zodpovedá prevádzkovateľ. Je povinný ho prihlásiť ešte pred začatím spracúvania osobných údajov.
  - Ak informačný systém podlieha dohľadu zodpovednej osoby, ktorú písomne poveril prevádzkovateľ podľa §19 ods. 2 alebo 8 a ktorá vykonáva dohľad nad ochranou osobných údajov nie je povinný IS registrovať
  - O informačnom systéme, ktorý nepodlieha registrácii, prevádzkovateľ vedie len evidenciu, a to najneskôr odo dňa začatia spracúvania údajov
  - Evidenciu netreba viesť o informačných systémoch ktoré obsahujú osobné údaje slúžiace na identifikáciu osôb pri jednorazovom vstupe do priestorov prevádzkovateľa

Informačné systémy

- Je to akýkoľvek usporiadaný súbor, sústava, kartotéka alebo databáza obsahujúca osobné údaje o jednej alebo viacerých osobách, ktoré sú systematicky spracúvané s použitím automatizovaných, čiastočne automatizovaných (s použitím programového vybavenia na počítači) alebo iných ako automatizovaných prostriedkov spracúvania (manuálne), napríklad kartotéka, zoznam, register, operát, záznam alebo sústava obsahujúca spisy, doklady, zmluvy, potvrdenia, posudky, hodnotenia, testy, mzdová agenda, personálna agenda...

- Ak je pripojený do internetu priamo alebo prostredníctvom počítačovej siete je potrebný bezpečnostný projekt

- Ak je určená zodpovedná osoba tak informačný systém stačí len evidovať. Obsahuje údaje podľa § 26 ods. 3

Najčastejšie nedostatky

- neaktuálny bezpečnostný projekt, bezpečnostné smernice
- bezpečnostné smernice spravidla neobsahovali spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačných systémov
- neobsahovali postupy pri haváriách, poruchách a iných mimoriadnych situáciách, neobsahovali opatrenia, ktoré určujú zodpovednosť oprávnených osôb počas mimoriadnych situáciách,
- bezpečnostné smernice neobsahovali rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému (nie všetky oprávnené osoby vykonávajú tie isté spracovateľské operácie osobnými údajmi),

Najčastejšie nedostatky

- Nie je písomne poverená zodpovedná osoba
- výpis z registra trestov bol s neskorším dátumom ako písomné poverenie
- poučenia oprávnených osôb boli veľmi stručné, nebolo z nich zrejmé aké práva a povinnosti majú jednotlivé oprávnené osoby – chýbala špecifikácia podľa popisu pracovnej činnosti
- prevádzkovatelia nedisponovali poučeniami podľa § 17
- chýbalo poučenie o povinnosti mlčanlivosti s možnými následkami pre oprávnenú osobu pri porušení § 18

Najčastejšie nedostatky

- nevedenie evidencie informačných systémov
- vedenie evidencie, avšak pre viac informačných systémov na jednom evidenčnom liste
- nesprávne vyplnenie evidenčného listu

Bezpečnostný projekt

- Za bezpečnosť údajov zodpovedá prevádzkovateľ a sprostredkovateľ. A ako hovorí zákon o ochrane osobných údajov chránia ich pred náhodným, ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením, ako aj pred akýmikoľvek neprípustnými formami spracúvania.

- Na tento účel prijme primerané technické, organizačné a personálne opatrenia. Podľa §15 zákona.

- Ak sa pracuvávajú údaje podľa §8 a ak je pripojený do internetu priamo alebo prostredníctvom počítačovej siete je potrebném vypracovať bezpečnostný projekt

Bezpečnostný projekt

- Súbor pravidiel, smerníc, opatrení a praktík potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém prevádzkovateľa (spracúvajúceho osobné údaje) z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

- Bezpečnostný projekt tvorí :

  - **Bezpečnostný zámer** – vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému
  - **Analýza bezpečnosti** informačného systému – podrobný rozbor stavu bezpečnosti informačného systému
  - **Bezpečnostné smernice** – upresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovateľa informačného systému

Bezpečnostný projekt

Bezpečnostný zámer

Vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti, a obsahuje najmä :

- formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení
- špecifikáciu technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov
- vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti
- vymedzenie hraníc určujúcich množinu zvyškových rizík

Bezpečnostný projekt

Riziková analýza bezpečnosti

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému, ktorá obsahuje najmä :

- kvalitatívnu analýzu rizík, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva

- použitie bezpečnostných štandardov a určenie iných metód a prostriedkov ochrany osobných údajov

Výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov, s uvedením rozsahu možného rizika, návrhov opatrení, ktoré eliminujú alebo minimalizujú vplyv rizík, a s vymedzením súpisu nepokrytých rizík.

Bezpečnostný projekt

Bezpečnostné smernice upresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovaného informačného systému a obsahujú najmä :

- popis technických, organizačných a personálnych opatrení vymedzených v bezpečnostnom projekte a ich využitie v konkrétnych podmienkach,
- rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému,
- rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov (§ 19),
- spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,
- postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií amožností efektívnej obnovy stavu pred haváriou.

Osobné údaje – elektronická forma

Čo treba mať na zreteli :

- Notebooky a prenosné média – šifrovanie dát
- Mailová a internetová komunikácia – šifrovanie príloh, vírusy, malware
- Prenos dát v lokálnej počítačovej sieti, WiFi
- Zdieľanie dát v počítačovej sieti
- Zabezpečenie dát na počítači
- Archivácia a likvidácia dát

Osobné údaje – papierová forma

Čo je potrebné zabezpečiť :

- Pravidlo čistého stola, dočasné odkladacie boxy na dokumenty
- Diskrétna vzdialenosť a stolové boxy
- Archivácia dokumentov a skartácia dokumentov
- Tlač dokumentov
- Kľúčový režim
- Nepovolané osoby

Čo môžeme pre vás urobiť

- Vypracovanie bezpečnostného projektu a bezpečnostných smerníc
- Zavedenie výsledkov bezpečnostného projektu do praxe
- Zosúladenie bezpečnostnej politiky s legislatívou
- Bezpečnostný audit a audit používaného softvéru
- Audit a vypracovanie plánu kabeláže
- Penetračné testy

Ďakujem za pozornosť