ALISON
Convergence. A matter of lifestyle.

# SLASPO Fórum 2010

# Ochrana osobných údajov v informačnom systéme

**24. november 2010**

# „Privacy no longer a social norm, says Facebook founder”

Mark Elliot "Zuck“ Zuckerberg
zakladateľ Facebook

http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

## Prečo projekt na ochranu osobných údajov

- Poverenie SLASPO vykonávaním odborných skúšok
- Rozsah vstupných údajov – Opatrenie NBS č. 9 z 25.mája 2010 (rodné číslo – povinný údaj)
- Právne predpisy SR – Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov

## Základné pojmy

- Osobné údaje
- Osobitné kategórie osobných údajov
- Informačný systém
- Bezpečnostný projekt
  - Bezpečnostný zámer
  - Analýza bezpečnosti IS
  - Bezpečnostná smernica

# Použité bezpečnostné štandardy

- STN ISO/IEC 27001:2005
  - Informačné technológie - Bezpečnostné techniky – Systémy riadenia informačnej bezpečnosti – Požiadavky
- STN ISO/IEC 27002:2005
  - Informačné technológie - Bezpečnostné techniky - Súbor praktických pravidiel pre riadenie informačnej bezpečnosti
- STN ISO/IEC 27005:2005
  - Bezpečnostné metódy - Riadenie rizík informačnej bezpečnosti

# Bezpečnostný zámer

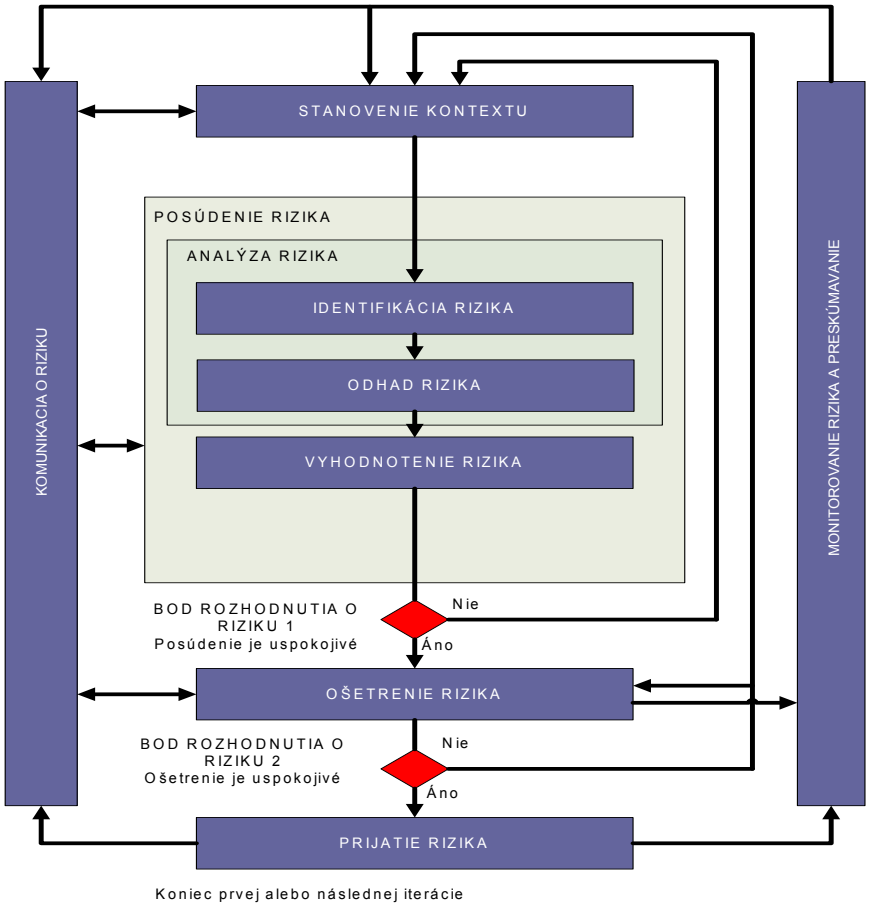
- Formulácia základných bezpečnostných cieľov
- Špecifikácia technických, organizačných a personálnych opatrení
- Vymedzenie okolia informačného systému
- Vymedzenie hraníc pre zvyškové riziká

# Analýza bezpečnosti IS

- Analýza rizík = proces
- Odpovedá na otázky
  - **ČO** je potrebné chrániť
  - proti **ČOMU** je treba chrániť
  - a akou **SILOU** je treba chrániť

# Procesy riadenia rizík informačnej bezpečnosti

- STN ISO/IEC 27005
  - Stanovenie kontextu
  - Posúdenie rizika
  - Ošetrenie rizika
  - Prijatie rizík
  - Komunikácia o riziku
  - Monitorovanie a prehodnotenie rizík



# Analýza bezpečnosti IS

- Možnosti analýzy rizík
  - Neautomatizovaný spôsob – tzv. funkcionálna AR
  - Automatizovaný spôsob – softvérové nástroje
- Základné pojmy
  - Aktívum
  - Hrozba
  - Zraniteľnosť
  - Riziko

# Analýza bezpečnosti IS

| Aktívum<br>- popis jednotlivých aktív identifikovaných počas analýzy | | Hrozba | | Zraniteľnosť | | Riziko | Správa rizika | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Hod<br>- ohodnotené v škále od 4 (najvyššia hodnota) po 1<br>4 - narušením, poškodením alebo zničením (dopad na dôvernosť, dostupnosť, integrita) môže byť SLAPSO spôsobená veľmi vysoká škoda až ohorozenie existencie IS<br>3 - narušením, poškodením alebo zničením (dopad na dôvernosť, dostupnosť, integrita) môže prísť k narušeniu viacerých významných procesov, škoda je vysoká ale nie je ohorzená existenica IS<br>2 - narušením, poškodením alebo zničením (dopad na dôvernosť, dostupnosť, integrita) môže prísť k narušeniu viacerých významných procesov, finančný dopad sa odrazí len na aktuálnom rozpočte SLASPO<br>1 - narušením, poškodením alebo zničením (dopad na dôvernosť, dostupnosť, integrita) môže prísť k narušeniu menej vyznamných procesov, škodu je možné okamžite kompenzovať (dopad na rozpočet je nevýznamný) | Hrozba<br>- priradená relevantná hrozba zo zoznamu | Hod<br>- výška hrozby, ktorá pôsobí na aktívum je hodnotená stupňami: (V) –vysoká, (S) – stredná a (N) – nízka. | Popis<br>- zraniteľnosť popísaná slovne v zmysle dôvernosti, dostupnosti a integrity | Hod<br>- pravdepodobnosť využitia zraniteľnosti vzhľadom na danú hrozbu. Zraniteľnosť je hodnotená stupňami (V) – vysoká, (S) – stredná, (N) – nízka. | Hod<br>- úroveň rizík pre jednotlivé aktíva SLASPO. Riziká sa hodnotili v škále od 0 po 8. | R<br>- riadenie rizika | V<br>- vyhnutie sa riziku | P<br>- prenos rizika | A<br>- akceptovanie rizika |
| Popis<br>- stručný popis | | | | | | | | | | |

# Bezpečnostné opatrenia

- Cieľ
  - Eliminácia identifikovaných rizík a zraniteľností
- Navrhnuté v súlade s požiadavkami
  - Zákona č. 428/2002 o ochrane osobných údajov
  - STN ISO/IEC 27002:2005
- Typ
  - Technické – bezpečnostný softvér a hardvér
  - Organizačné – procesy, interná legislatíva
  - Personálne

## Bezpečnostná smernica

- Záväzná interná legislatíva
- „Návod“ pre všetkých zamestnancov a používateľov informačných systémov
- Preukázateľné oboznámenie sa
- Osobná zodpovednosť

## Audit a kontrola

- Pri významnej zmene IS, alebo raz za 2 roky
- Úrad na ochranu osobných údajov

# Ďakujeme za pozornosť


- Annamária Balážová - annamaria.balazova@alison-group.sk
- Ivan Masný - ivan.masny@alison-group.sk


- **ALISON Slovakia** - systémový integrátor, ktorý poskytuje:
  - Hlasové a dátové služby pre pevné a mobilné siete
  - Informačnú bezpečnosť, bezpečnostné projekty, ochranu US
  - Unifikovanú komunikáciu (hlas, video, dáta v jednom)
  - Šifrovú ochranu informácií
  - Dodávky špeciálnej výpočtovej techniky (ochrana proti NEV)
  - Manažované služby