Úvod do informačnej bezpečnosti (4)

Legislatíva a normy

Máme základ a čo ďalej?

- Čo máme?
  - Spravili sme bezpečnostný projekt pre organizáciu
  - Napísali bezpečnostnú politiku
  - Spravili analýzu rizík
  - Vyhodnotili riziká
  - Navrhli a implementovali opatrenia (tých, ktoré sa dali zvládnuť s prostriedkami, ktoré sme na to mali)
- Máme baseline a čo ďalej?
  - Príprava ľudí (všetkých aj špecialistov)
  - Zvýšenie personálnych kapacít
  - Riešenie problémov, na ktoré neboli kapacity na začiatku (treba prejsť ISO/IEC 27002)
  - Špeciálne systémy a požiadavky, ktoré na ich ochranu vyplývajú z legislatívy

Zákon o kritickej infraštruktúre
pojmy

- Zákon č. 45/2011 Z. z. Zákon o kritickej infraštruktúre
- prvok kritickej infraštruktúry je aj informačný systém
- prvkom kritickej infraštruktúry (ďalej len „prvok“) najmä inžinierska stavba,[2)] služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia,
- ochranou prvku zabezpečenie funkčnosti, integrity a kontinuity činnosti prvku s cieľom predísť, odvrátiť alebo zmierniť hrozbu jeho narušenia alebo zničenia,
- citlivou informáciou o kritickej infraštruktúre (ďalej len „citlivá informácia“) neverejná informácia, ktorej zverejnenie by sa mohlo zneužiť na činnosť smerujúcu k narušeniu alebo zničeniu prvku,

Zákon o kritickej infraštruktúre

ochrana prvku KI

Za prvok kritickej infraštruktúry zodpovedá jeho prevádzkovateľ

1) Prevádzkovateľ je povinný ochraňovať prvok pred narušením alebo zničením. Na ten účel prevádzkovateľ je povinný

a) uplatniť pri modernizácii prvku technológiu, ktorá zabezpečuje jeho ochranu,

b) zaviesť bezpečnostný plán po predchádzajúcom vyjadrení príslušného ústredného orgánu do šiestich mesiacov od doručenia oznámenia o určení prvku a o jeho zaradení do sektora, ak sa vo výnimočnom odôvodnenom prípade nedohodne s príslušným ústredným orgánom na predĺžení tejto lehoty; lehotu je možné predĺžiť iba jedenkrát, maximálne o tri mesiace,

c) prehodnocovať priebežne bezpečnostný plán, a ak je to potrebné, zaviesť po predchádzajúcom vyjadrení príslušného ústredného orgánu aktualizovaný bezpečnostný plán,

Zákon o kritickej infraštruktúre
ochrana prvku KI

d) oboznámiť svojich zamestnancov v nevyhnutnom rozsahu s bezpečnostným plánom,

e) precvičiť podľa bezpečnostného plánu aspoň raz za tri roky modelovú situáciu hrozby narušenia alebo zničenia prvku,

f) určiť oprávnenú osobu, ktorá je zároveň kontaktná osoba, ak ide o prvok európskej kritickej infraštruktúry

Bezpečnostný projekt pre prvok KI

1) Bezpečnostný plán obsahuje popis možných spôsobov hrozby narušenia alebo zničenia prvku, zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu.

(2) Bezpečnostné opatrenia na ochranu prvku sú najmä mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné opatrenia podľa osobitného predpisu (4a), fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia.

(3) Rozsah bezpečnostných opatrení na ochranu prvku sa určuje na základe posúdenia hrozby narušenia alebo zničenia prvku.

(4) Minimálny postup pri vypracúvaní bezpečnostného plánu je uvedený v prílohe č. 2.

Odkaz (4a) §20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Minimálny postup pri vypracúvaní bezpečnostného plánu (príloha 3)

A. Určujú sa dôležité zariadenia prvku.

B. Vyhodnocuje sa riziko hrozby narušenia alebo zničenia jednotlivých zariadení prvku, ich zraniteľné miesta, predpokladané dôsledky ich narušenia alebo zničenia na funkčnosť, integritu a kontinuitu činnosti prvku.

C. Uskutočňuje sa výber hlavných bezpečnostných opatrení na ochranu prvku, ktoré sa členia na

a) trvalé bezpečnostné opatrenia, ktorými sú investície a postupy na zabezpečenie ochrany prvku, a to

1. mechanické zábranné prostriedky,
2. technické zabezpečovacie prostriedky,
3. bezpečnostné prvky informačných systémov,
4. organizačné opatrenia s dôrazom na postup pri vyrozumení a varovaní, ako aj na krízové riadenie,
5. odborná príprava osôb, ktoré zabezpečujú ochranu prvku,
6. kontrolné opatrenia na dodržiavanie trvalých bezpečnostných opatrení,

Minimálny postup pri vypracúvaní bezpečnostného plánu (príloha 3)

b) mimoriadne bezpečnostné opatrenia, ktoré sa uplatňujú v závislosti od intenzity hrozby narušenia alebo zničenia prvku.

D. Určujú sa hlavné bezpečnostné opatrenia na ochranu prvku.

E. Bezpečnostný plán sa počas jeho tvorby konzultuje s orgánmi, ktorých súčinnosť sa predpokladá pri ochrane prvku.

Zákon o ISVS

- 275 ZÁKON z 20. apríla 2006 o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
- Za vytváranie, správu a rozvoj informačného systému verejnej správy zodpovedá povinná osoba, ktorá je správcom, zabezpečujúca výkon verejnej správy na určenom úseku verejnej správy podľa osobitného predpisu.
- Povinná osoba musí

  b) zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, ktoré sú v ich správe, vrátane organizačného, odborného a technického zabezpečenia,

  c) zabezpečovať informačný systém verejnej správy proti zneužitiu,

  i) zabezpečovať, aby bol informačný systém verejnej správy v súlade so štandardmi informačných systémov verejnej správy (ďalej len „štandardy“),

Výnos č. 55/2014 Z. z.

- Výnos Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy
- účinnosť poslednej novely od 15.11.2018 **do 30.04.2019**
- Obsahuje Bezpečnostné štandardy
  - Riadenie informačnej bezpečnosti
  - Personálna bezpečnosť
  - Manažment rizík pre oblasť IB
  - Kontrolný mechanizmus riadenia IB
  - Ochrana proti škodlivému kódu
  - Sieťová bezpečnosť
  - Fyzická bezpečnosť a bezpečnosť prostredia
  - Aktualizácia sw
  - Monitorovanie a manažment bezpečnostných incidentov

Výnos č. 55/2014 Z. z.

- Periodické hodnotenie zraniteľností
- Zálohovanie
- Fyzické ukladanie záloh
- Riadenie prístupu
- Aktualizácia IKT
- Účasť tretej strany
- Federácia identít

Utajované skutočnosti

- Zákon č. 215/2004 Z. z.Zákon o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
- a) utajovanou skutočnosťou informácia alebo vec určená pôvodcom utajovanej skutočnosti, ktorú vzhľadom na záujem Slovenskej republiky treba chrániť pred vyzradením, zneužitím, poškodením, neoprávneným rozmnožením, zničením, stratou alebo odcudzením (ďalej len „neoprávnená manipulácia“) a ktorá môže vznikať len v oblastiach, ktoré ustanoví vláda Slovenskej republiky svojím nariadením,
- b) informáciou

    1. obsah písomnosti, nákresu, výkresu, mapy, fotografie, grafu alebo iného záznamu,

    2. obsah ústneho vyjadrenia,

    3. obsah elektrického, elektromagnetického, elektronického alebo iného fyzikálneho transportného média,

Utajované skutočnosti

- Klasifikácia utajovaných skutočností
- Personálna bezpečnosť
- Fyzická bezpečnosť
- Šifrová ochrana informácií
- V minulosti – aj informačné systémy, teraz, zákon o kybernetickej bezpečnosti, ale
- Kompetencie NBÚ pre oblasť utajovaných skutočností
  - vykonáva a zabezpečuje výskum a vývoj v oblasti bezpečnosti informačných technológií,
  - Príslušníci a zamestnanci úradu sú pri výkone kontroly oprávnení vstupovať do informačných systémov do úrovne správcu systému v rozsahu potrebnom na vykonanie kontroly,

Zákon o kybernetickej bezpečnosti

- Existuje podrobný Komentár
- Zákon mal implementovať
  - Smernica NIS
  - Zákon o informačnej bezpečnosti
- Implementoval smernicu NIS
  - NBÚ ako orgán zodpovedný za kybernetickú bezpečnosť a kontaktný bod pre EU orgány
  - Povinnosti prevádzkovateľa digitálnej služby a poskytovateľa podstatnej služby
  - Nahlasovanie bezpečnostných incidentov
  - Rozšírenie sektorov KRITIS a stanovenie zodpovedných štátnych orgánov
  - Povinnosť zriadiť CSIRT
  - Riešenie a nahlasovanie bezpečnostných incidentov
  - Medzinárodná spolupráca

Osobné údaje (1)

- GDPR
- Dva protichodné záujmy:
  - Ochrana osobnosti
  - voľný pohyb osôb, tovaru a služieb

Článok 1

Predmet úpravy a ciele

1. Týmto nariadením sa stanovujú pravidlá ochrany fyzických osôb pri spracúvaní osobných údajov a pravidlá týkajúce sa voľného pohybu osobných údajov.

2. Týmto nariadením sa chránia základné práva a slobody fyzických osôb, najmä ich právo na ochranu osobných údajov.

3. Voľný pohyb osobných údajov v rámci Únie sa nesmie obmedziť ani zakázať z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov.

Osobné údaje (2)

- „osobné údaje“ sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;
- Toto nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.
- „informačný systém“ je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe;

Osobné údaje (3)

- Dotknutá osoba (osoba, ku ktorej sa vzťahujú osobné údaje)
- Prevádzkovateľ (controller)- určí účely a prostriedky spracúvania osobných údajov;
- Sprostredkovateľ (processor) je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa;
- Príjemca – dostáva osobné údaje
- Tretia strana – je poverená spracovaním osobných údajov prevádzkovateľom alebo sprostredkovateľom
- Príklad:
  - Dotknutá osoba – študent
  - Prevádzkovateľ – UK
  - UPJŠ (AIS2) sprostredkovateľ alebo tretia strana

Osobné údaje (4)

- Zásady spracúvania osobných údajov
  - Zákonnosť
  - Spravodlivosť
  - Transparentnosť
  - Obmedzenie účelu
  - Minimalizácia údajov
  - Správnosť
  - Minimalizácia uchovávania
  - Integrita a dôvernosť
- Zodpovednosť prevádzkovateľa za dodržiavanie zásad

Osobné údaje (5)

- Zákonnosť:
  - Súhlas dotknutej osoby
  - Spracovanie je nevyhnutné na plnenie zmluvy
  - Spracovanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa;
  - spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby;
  - spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;
  - spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa.

Osobné údaje (6)

- Práva dotknutej osoby
  - Aké osobné údaje spracovávate a prečo (web)
  - Oprava, vymazanie, obmedzenie spracovania, preposlanie
  - Zdroj osobných údajov (ak ich neposkytla sama)
  - Kópia osobných údajov
- Bezpečnosť (prevádzkovateľ a sprostredkovateľ – primeraná úroveň ochrany, aj tretie strany)
  - V podstate ide o bezpečnostný projekt
  - Explicitne sa požaduje CIAA a robustnosť systémov a služieb
  - Riešenie bezpečnostných incidentov
  - Správa rizík
- Kritériá sú CIA
- Kódex a certifikácia

Bezpečnostné incidenty narušujúce osobné údaje

- Nahlasovacia povinnosť
  - Prevádzkovateľ: Do 72 hodín nahlásiť Úradu
  - Sprostredkovateľ – prevádzkovateľovi
  - Dotknutým osobám (výnimky)

Organizačné opatrenia a zaujímavosti

- Ustanovenie oprávnenej osoby
- Kódexy správania
- monitorovanie dodržiavania kódexov správania
- Akreditácia auditorov
- Certifikácia
- Cezhraničné prenosy

* * *

Služby dôvery (eIDAS)

- **Zákon č. 272/2016 Z. z. Zákon o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) (Národný bezpečnostný úrad SR)** upravuje podmienky poskytovania dôveryhodných služieb, povinnosti poskytovateľov dôveryhodných služieb, pôsobnosť Národného bezpečnostného úradu v oblasti dôveryhodných služieb a sankcie za porušenie povinností podľa osobitného predpisu a tohto zákona.
- Implementácia nariadenie eIDAS
- Nepodarený preklad kľúčových pojmov
- Nahradzuje zákon o elektronickom podpise

Ďalšie zákony (1)

- **Zákon č. 351/2011 Z. z. Zákon o elektronických komunikáciách** okrem iného upravuje práva a povinnosti podnikov a užívateľov elektronických komunikačných sietí a elektronických komunikačných služieb, ochranu elektronických komunikačných sietí a elektronických komunikačných služieb, ochranu súkromia a ochranu spracúvania osobných údajov v oblasti elektronických komunikácií a pôsobnosť orgánov štátnej správy v oblasti elektronických komunikácií.
- **Zákon č. 300/2005 Z. z. Trestný zákon** okrem iného upravuje trestné činy z oblasti počítačovej kriminality.
- **Zákon č. 211/2000 Z. z. Zákon o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) ()** upravuje podmienky, postup a rozsah slobodného prístupu k informáciám.

Ďalšie zákony (2)

- **Zákon č. 305/2013 Z. z. Zákon o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente),** ktorý upravuje o.i. identifikáciu osôb a autentifikáciu osôb vo virtuálnom priestore.
- **Zákon č. 395/2002 Z. z. Zákon o archívoch a registratúrach a o doplnení niektorých zákonov (MV SR),** ktorý o.i. upravuje elektronický záznam (informácií).
- **Zákon č. 575/2001 Z. z.** o organizácii činnosti vlády a organizácii ústrednej štátnej správy.
- **Zákon č. 110/2004 Z. z.** o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru.
- **Výnos MVSR č. 525/2011 Z. z.** o štandardoch pre elektronické informačné systémy na správu registratúry.

Štandardy

- Rôzne (oficiálne, aj de-facto štandardy)
- Z právneho hľadiska – odporúčania (ak nie sú podporené zákonom)
- V informačnej bezpečnosti
  - ISO
  - RFC
  - PKCS
  - Národné štandardy (NIST, BSI)

ISO

- Informatika je veľká oblasť aj na normalizáciu
- Spoločný technický výbor s IEC (ISO/IEC JTC 1) International Electrotechnical Commission
- Podrobne na adrese https://en.wikipedia.org/wiki/ISO/IEC_JTC_1
- SC 27 – informačná bezpečnosť
- cca 100 štandardov

Working Group	Working Area
ISO/IEC JTC 1/SC 27/SWG-M	Management
ISO/IEC JTC 1/SC 27/SWG-T	Transversal items
ISO/IEC JTC 1/SC 27/WG 1	Information security management systems
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies

Manažment IB v ISO normách

- WG 1
- Robí sa veľké upratovanie (séria 270xx)
- Približne 40 noriem https://en.wikipedia.org/wiki/ISO/IEC_27000-series
- podstatné normy
- ISO/IEC 27000 — Information security management systems — Overview and vocabulary[6]
- ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems — Requirements. · ISO/IEC 27002 — Code of practice for information security management -
- ISO/IEC 27005 — Information security risk management[8]

Manažment IB v ISO normách

- Potenciálne zaujímavé normy
  - · ISO/IEC 27032 — Guideline for cybersecurity
  - · ISO/IEC 27033-1 — Network security - Part 1: Overview and concepts
  - · ISO/IEC 27033-2 — Network security - Part 2: Guidelines for the design and implementation of network security
  - · ISO/IEC 27033-3 — Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
  - · ISO/IEC 27033-5 — Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
  - · ISO/IEC 27033-6 — Network security - Part 6: Securing wireless IP network access
  - · ISO/IEC 27034-1 — Application security - Part 1: Guideline for application security

Manažment IB v ISO normách

- Potenciálne zaujímavé normy
  - · ISO/IEC 27034-2 — Application security - Part 2: Organization normative framework
  - · ISO/IEC 27034-6 — Application security - Part 6: Case studies
  - · ISO/IEC 27035-1 — Information security incident management - Part 1: Principles of incident management
  - · ISO/IEC 27035-2 — Information security incident management - Part 2: Guidelines to plan and prepare for incident response

Common Criteria

- Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) (ISO/IEC 15408)
- Posudzovanie bezpečnosti a certifikácia systémov
- Voľne dostupné na http://www.commoncriteriaportal.org/cc/

Iné štandardy

- IETF a RFC
- NIST – SP 800 a FIPS
- BSI (nemecké) 4 BSI štandardy + množstvo metodických materiálov
- EESSI resp. ETSI
- ITU
- RSA Laboratories
- Vzdelávanie CBK, EBK,...
- Je toho viac, ako sa dá zvládnuť