Kybernetická a informačná bezpečnosť

Úroveň štátu

Obsah

- Ochrana a obrana na úrovni štátu
- Legislatíva
- Štandardy
- Ďalšie čítanie

Prečo potrebujeme ochranu na úrovni štátu?

- Lokálna ochrana na úrovni organizácie alebo konkrétnych systémov nepostačuje
- Existujú hrozby presahujúce možnosti organizácie
- Čo má chrániť štát?
  - Národný digitálny ekosystém v širokom zmysle
  - V úzkom národný kybernetický priestor
- Národný digitálny ekosystém je vymedzený skôr slovenskou jurisdikciou ako fyzickou väzbou na územie Slovenska, alebo majetok slovenských subjektov

Čo by mal robiť štát?

- Kybernetická ochrana a obrana
- Ochrana štátnych informačných systémov
- Legislatíva a nástroje na jej presadzovanie
- Štandardy
- vzdelávanie

Kybernetická obrana a ochrana

- Veľa dôležitých vecí sa robí elektronicky v kybernetickom priestore
- Kto nás ohrozuje a ako:
  - Nepriateľské štáty (vojna v kybernetickom priestore)
  - Aj spriatelené štáty (politické a ekonomické záujmy)
  - Organizovaný zločin (počítačová kriminalita)
  - Teroristi
  - Politické a nátlakové skupiny (Estónsko)
  - Nadnárodné korporácie (zber osobných údajov, manipulácie s ľuďmi)
  - Hackeri
  - A iní
- Neviditeľná a asymetrická vojna

Informačná vojna

- Informačná vojna prebiehala odjakživa (šifrovanie, tajné písma, falošné správy)
- Zvlášť po objavení telegrafu, rádiového vysielania (komunikácia na veľké vzdialenosti cez nezabezpečený kanál)
- Ochrana – šifrovanie
- Útok- kryptoanalýza (Washington Naval Conference 1921-22, 2. svetová vojna – Purple a Enigma, ponorková vojna v Atlantickom oceáne, bitka o Midway)
- Ale aj po vojne UKUSA, Eschelon
- Key escrow, Skipjack, Clipper chip
- Aféra Crypto AG (1993)
- Nevysvetlené havárie podmorských telekomunikačných káblov

Kybernetické vojna

- 4 klasické bojiská: zem, voda, vzduch, kozmický priestor
- Pribudol kybernetický priestor
- Prepojenie d-IKT a reálneho sveta
  - Veľa činností prešlo z fyzického do virtuálneho priestoru (financie, administratíva, zdravotné záznamy, poisťovne, …)
  - Riadiace systémy dopravných, výrobných systémov, elektrární, vodární
  - Zabudované počítače v bežných zariadeniach
- namiesto útoku na systém stačí ovládnuť jeho riadiaci systém
- Iránsky jadrový program – Stuxnet, neskôr Duqu, Flame
- Štát: potrebuje kapacity na odhalenie a odrazenie kybernetického útoku a capacity na výrobu a použitie kybernetických zbraní

Ako organizovať obranu na úrovni štátu?

- Najprv Stratégia (čo nám hrozí, čo potrebujeme chrániť, ako)
- V SR
  - Národná stratégia informačnej bezpečnosti v SR (2008)
  - Koncepcia kybernetickej bezpečnosti SR na roky 2015-2020
  - Národná stratégia informačnej bezpečnosti 2021-2025
- Rozdelenie úloh a koordinácia
  - Príklady dobrého riadenia – USA a Nemecko
- Na Slovensku – už samotná informatika (informatizácia) bola nechceným dieťaťom
- Tradičné oblasti
  - Utajované skutočnosti MV, potom NBÚ
  - Šifrová služba – MV
  - Spravodajské služby – SIS, Vojenské spravodajstvo

Ako organizovať obranu na úrovni štátu?

- Pribudli nové oblasti (EÚ)
  - Osobné údaje
  - Kritická infraštruktúra
  - Elektronický podpis
- Banky – vlastný svet
- Informačná/kybernetická bezpečnosť
  - Problém roku 2000
  - Direktíva EÚ o elektronickom podpise a Zákon o elektronickom podpise
  - eEurope+
  - MF SR a OPIS (Stratégia, Systém vzdelávania, CSIRT, Bezpečnostné štandardy)
  - Od r. 2015 – NBÚ (zákon o kybernetickej bezpečnosti)
  - Z MF SR prešli kompetencie za ISVS na Úrad podpredsedu vlády, v súčasnosi MIRRI
  - GDPR, eIDAS – Zákon o ochrane osobných údajov a Zákon o dôveryhodných službách, Zákon e e-Governmente
  - Smernica NIS, Smernica o elektronických službách,….

Ako sa to usporiadalo?

- Obrana – vojaci, Vojenské spravodajstvo
- Koordinátor ochrany celého priestoru – NBÚ
  - Kompetenčný zákon, zákon o kybernetickej bezpečnosti
- Zvlášť banky a finančný sector
- MV – kritická infraštruktúra
- Telekomunikačný úrad
- MIRRI – verejná správa
- ÚOOÚ – GDPR
- MV – polícia počítačová kriminalita
- Vládny CSIRT, národný CSIRT?

Úlohy štátu

- Nepôjdeme do detailov
- Centrálna úroveň
  - Stratégia
  - Konkretizácia úloh
  - Rozdelenie zodpovedností
  - Akčné plány
  - Legislatíva
  - Štandardy
  - Medzinárodná spolupráca
  - Koordinácia domácich aktivít
  - pomoc pri riešení zázvažných incidentov
  - Ochrana kritických systémov
  - Vzdelávanie a budovanie knov-hov

Legislatíva

- V ďalšom sa sústredíme na dve oblasti, ktoré sa nás bezprostredne týkajú:
  - Štandardy
  - Legislatíva
- Tie vytvárajú rámec, v ktorom sa pohybujeme a riešime bezpečnostné problémy v organizácii
- prezentácia je podrobnejšia ako prednáška, ale obsahuje podrobnejší popis, ktorý nám pomôže zorientovať sa v zákonoch a nariadeniach, ktorými sa budeme riadiť
- Na prednáške sa dotkneme len najdôležitejších povinností, ktoré pre nás vyplývajú zo zákonov a vyhlášok

Normy a štandardy

- V medzinárodnom prostredí sa používa názov standard
- U nás sa hovorí o normách (technických normách) a pojem štandard sa používa (nie dôsledne) na legislatívne vymedzenie požiadaviek/postupov v nejakej oblasti (existoval napr Výnos MF SR o štandardoch pre ISVS)
- Slovenské technické normy (aspoň v oblasti informačnej a kybernetickej bezpečnosti) vznikajú preberaním medzinárodných noriem, prevažne noriem ISO občas prekladom, častejšie v angličtine
- Vyhlášky a iné podzákonné normy sa často odvolávajú na medzinárodné normy
- aj Nariadenia a vyhlášky EÚ sa často odvolávajú na existujúce normy
- Dôvody: normy sú dobré a používajú sa, vymýšľať niečo nové je problematické – ako to presadzovať

Prehľad relevantných noriem

- Skôr ako sa pozrieme na zákony, pozrime sa na normy, podľa ktorých budeme požiadavky vyplývajúce zo zákonov implementovať
- Veľa štandardizačných organizácií
  - ISO,IEC, CEN, CENELEC, ETSI, NIST, BSI, DIN,...
  - Súkromné spoločnosti RSA Labs - PKCS
  - IETF – RFC
  - Ad hoc iniciatívy (EESSI, UNCITRAL)
- Oficiálne normy a štandardy de-facto
- Dobrý štandard = koncentrované know-how, môže byť veľmi užitočný
- Najprv prehľad, neskôr sa k vybraným štandardom vrátime

ISO/IEC

- Najdôležitejšia medzinárodná štandardizačná organizácia
- Informačná bezpečnosť spadá do kompetencie podvýboru ISO/IEC JTC 1/SC 27: IT Security techniques
- Ten sa delí na 5 pracovných skupín

JTC 1/SC 27/WG 1 Information security management systems
JTC 1/SC 27/WG 2 Cryptography and security mechanisms
JTC 1/SC 27/WG 3 Security evaluation criteria
JTC 1/SC 27/WG 4 Security controls and services
JTC 1/SC 27/WG 5 Identity management and privacy technologies

Ktoré spravujú cca 200 štandardov (väčšinou si ich treba kúpiť, ale dajú sa čítať prezenčne v knižnici SÚTN)

- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

ISO/IEC štandardy

- Bezpečnostných ISO štandardov je veľa, pozri

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

- Ktoré sú základné?
- Manažment informačnej bezpečnosti 27xxx (dobrý prehľad na http://en.wikipedia.org/wiki/ISO/IEC_27000-series)
- Hodnotenie bezpečnosti systémov

Prehľad

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary [1]
- ISO/IEC 27001 — Information security management systems — Requirements
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27031 — Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27033-1 — Network security overview and concepts
- ISO/IEC 27035 — Security incident management
- ISO 27799 — Information security management in health using ISO/IEC 27002

Prehľad

- ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on the management system)
- ISO/IEC 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)
- ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ISO/IEC 27014 — Information security governance framework
- ISO/IEC 27015 — Information security management guidelines for the finance and insurance sectors
- ISO/IEC 27032 — Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
- ISO/IEC 27033 — IT network security, a multi-part standard based on ISO/IEC 18028:2006 (part 1 is published already)
- ISO/IEC 27034 — Guideline for application security
- ISO/IEC 27036 — Guidelines for security of outsourcing
- ISO/IEC 27037 — Guidelines for identification, collection and/or acquisition and preservation of digital evidence

Kľúčové ISO normy

- ISO/IEC 27001:2013 Information security management systems Requirements
- ISO/IEC 27002:2013 Code of practice for information security management
- ISO/IEC 27005 — Information security risk management
- ISO/IEC TR 27103:2018 Information technology — Security techniques — Cybersecurity and ISO and IEC Standards
- Bude určite zaujímavá pripravovaná norma
- ISO/IEC CD 27005.2 Information security, cybersecurity and privacy protection — Guidance on managing information security risks and opportunities
- Common Criteria – séria noriem ISO/IEC 15408-x ktoré tvoria základ pre budovanie a hodnotenie bezpečných informačných systémov (voľne dostupné normy)

Metodické materiály NIST

- Dobrá úroveň, dostupné, pokrytie širokého okruhu problémov, ale vychádzajúce z amerických podmienok = metodické dokumenty NIST, najmä SP 800
- https://csrc.nist.gov/publications/sp800

Spolkový úrad pre informačnú bezpečnosť
https://www.bsi.bund.de/EN/Home/home_node.html

- Metodika Grundschutz
- https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/IT-Grundschutz-Kompendium_080221.html
- 4 skvelé štandardy
  - BSI Standard 200-1 defines the general requirements for an ISMS
  - BSI Standard 200-2 explains how an ISMS can be built based on one of three different approaches
  - BSI Standard 200-3 contains all risk-related tasks
  - BSI Standard 100-4 is covering Business Continuity Management (BCM)

Iné

- IETF – vydáva RFC https://www.ietf.org/standards/rfcs/
- ITU – štandardy k PKI, identifikácii a autentizácii
- Kedysi RSA – laboratories štandardy PKCS

Vráťme sa k legislatíve

- Prečo sa podrobne zaoberáme legislatívnymi požiadavkami na kybernetickú a informačnú bezpečnosť?
- Povinnosti sa začínajú kontrolovať a nedodržiavanie sankcionovať
- V štátnej inštitúcii – explicitne stanovené povinnosti
  - Musíme dodržiavať
  - Ale môžeme sa o ne opierať vo vzťahu k vedeniu organizácie
- IT firma, alebo súkromná spoločnosť – ak chce dodávať pre štát, musí vedieť, aké požiadavky na ňu štát bude klásť

Zákony a vykonávacie predpisy stanovujúce požiadavky v kybernetickej a informačnej bezpečnosti

- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- 179 VYHLÁŠKA Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu z 22.júna 2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 373/2018 Z. z.
- Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z.,ktorou sa ustanovuje obsah bezpečnostných opatrení,obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- A ďalšie

Zákon č. 95/2019Z. z. o informačných technológiách vo verejnej správe

- Obsahuje časť Bezpečnosť informačných technológií verejnej správy (§§ 18-23)
- Prevádzka ISVS sa považuje za prevádzkovanie základnej služby (!?)
- Špeciálne o prevádzkovateľovi základnej služby
  - Povinnosť prijať a realizovať/implementovať bezpečnostné opatrenia zákon o KB
  - Obsah a rozsah bezpečnostných opatrení na ochranu ISVS – tento zákon
- Bezpečnosť rozdelená do oblastí
  - Plánovanie a organizácia
  - Obstarávanie a implementácia
  - Prevádzka, servis a podpora
  - Monitoring a hodnotenie
  - Osobitné opatrenia

Základné pojmy (§2)

(1) Informačnou technológiou je na účely tohto zákona prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby.

(2) Informačným systémom je na účely tohto zákona funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.

(3) Informačnou technológiou verejnej správy je informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Na účely tohto zákona sa povinnosti v rámci správy informačných technológií verejnej správy vzťahujú aj na údaje, procesné postupy, personálne zabezpečenie a organizačné zabezpečenie, ak tvoria funkčný celok alebo ak samy osebe slúžia na spracúvanie údajov alebo informácií v elektronickej podobe.

(4) Informačným systémom verejnej správy je informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby.

Základné pojmy (§2)

(5) Správcom na účely tohto zákona je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon alebo je ustanovený na základe tohto zákona. Ak zákon vo vzťahu k informačnej technológii verejnej správy správcu neustanovuje, je správcom na účely tohto zákona ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby; ak je takýchto orgánov riadenia viac a jedným z nich je aj ústredný orgán štátnej správy, správcom je tento ústredný orgán štátnej správy.

(6) Prevádzkovateľom je na účely tohto zákona správca, osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba. Správcom určený alebo osobitným predpisom ustanovený prevádzkovateľ vykonáva, v rozsahu povinností správcu, činnosti, ktoré mu určí správca alebo ustanoví tento osobitný predpis; ak tento osobitný predpis rozsah činností prevádzkovateľa neustanovuje, vykonáva ich v celom rozsahu činností správcu. Určením alebo ustanovením prevádzkovateľa nie je dotknutá zodpovednosť správcu za plnenie povinností podľa tohto zákona.

Základné pojmy (§3)

k) službou verejnej správy výkon právomocí, práv a povinností orgánu riadenia, ktorej rozsah a spôsob výkonu ustanovuje osobitný predpis,

l) elektronickou službou verejnej správy elektronická komunikácia s orgánom riadenia pri vybavovaní podania, oznámenia, pri prístupe k informáciám a ich poskytovaní alebo pri účasti verejnosti na správe verejných vecí,

Organizácia správy informačných technológií verejnej správy (§5)

(1) Správu informačných technológií verejnej správy vykonávajú

a) orgán vedenia, ktorým je ministerstvo investícií,

b) orgán riadenia vo vzťahu k informačným technológiám verejnej správy v jeho pôsobnosti.

Pre zaujímavosť – orgány riadenia

(2) Orgánom riadenia na účely tohto zákona je

a) ministerstvo a ostatný ústredný orgán štátnej správy,

b) Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu elektronických komunikácií a poštových služieb, Dopravný úrad, Úrad pre reguláciu sieťových odvetví a iný štátny orgán,

c) obec a vyšší územný celok,

d) Kancelária Národnej rady Slovenskej republiky, Kancelária prezidenta Slovenskej republiky, Kancelária Ústavného súdu Slovenskej republiky, Kancelária Najvyššieho súdu Slovenskej republiky, Kancelária Súdnej rady Slovenskej republiky, Kancelária verejného ochrancu práv, Úrad komisára pre deti, Úrad komisára pre osoby so zdravotným postihnutím, Ústav pamäti národa, Sociálna poisťovňa, zdravotné poisťovne, Tlačová agentúra Slovenskej republiky, Rozhlas a televízia Slovenska, Rada pre vysielanie a retransmisiu,

e) právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia uvedeného v písmenách a) až d),

Pre zaujímavosť – orgány riadenia

(2) Orgánom riadenia na účely tohto zákona je

f) komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,

g) osoba neuvedená v písmenách a) až f) okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov,

h) záujmové združenie právnických osôb DataCentrum elektronizácie územnej samosprávy Slovenska, ktorého jedinými členmi sú Ministerstvo financií Slovenskej republiky a Združenie miest a obcí Slovenska.

Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie

(1) V rámci zabezpečenia riadenia bezpečnosti podľa § 14 ods. 1 písm. i) je správca povinný vo svojej organizácii zaviesť a udržiavať systém riadenia informačnej bezpečnosti, ktorý

a) určí ciele, rozsah, podmienky, povinnosti osôb, ktoré vykonávajú činnosť pre správcu a organizačných zložiek správcu a prostriedky riadenia bezpečnosti vo forme bezpečnostnej politiky alebo inak zdokumentovaných a schválených mechanizmov riadenia bezpečnosti informačných technológií verejnej správy,

b) zriadi riadiacu, výkonnú a kontrolnú zložku systému riadenia bezpečnosti, ktoré sú navzájom personálne a kompetenčne oddelené,

c) zabezpečí identifikovanie aktív v informačných technológiách verejnej správy, zraniteľností a relevantných hrozieb a hodnotenie rizík vyplývajúcich z hrozieb, najmä vo forme bezpečnostného projektu podľa § 23 ods. 1 a 2, v nadväznosti na kritickosť aktív v informačných technológiách verejnej správy, ich vývoj a na zmeny všeobecne záväzných právnych predpisov a podmienok v organizácii správcu,

d) zadefinuje mechanizmy rozhodovania o spôsobe riadenia identifikovaných rizík,

e) identifikuje potrebné bezpečnostné opatrenia,

Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie

f) určí bezpečnostné mechanizmy na procesnej, organizačnej a na technickej úrovni v nadväznosti na identifikované bezpečnostné opatrenia a rozhodnutia o spôsobe riadenia rizika a určí opatrenia na ochranu bezpečnosti a integrity informácií vrátane opatrení včasného varovania,

g) určí prostriedky na zabezpečenie implementácie a riadneho fungovania bezpečnostných opatrení,

h) určí prostriedky kontroly uplatňovania bezpečnostných mechanizmov,

i) určí postupy riešenia bezpečnostných incidentov pri narušení definovaných bezpečnostných cieľov v nadväznosti na mechanizmy riešenia bezpečnostných incidentov.

Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie

(2) Správca prostredníctvom riadiacej zložky systému riadenia bezpečnosti zabezpečuje prerokovanie a schválenie

a) koncepčných dokumentov a strategických opatrení týkajúcich sa bezpečnosti informačných technológií verejnej správy,

b) informácií o zaznamenaných bezpečnostných incidentoch spolu s návrhom opatrení na minimalizáciu ich opätovného výskytu,

c) návrhu opatrení vyplývajúcich z analýz, riešených bezpečnostných incidentov, havarijných stavov, kontrol a auditov bezpečnosti informačných technológií verejnej správy.

Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie

(3) Správca prostredníctvom výkonnej zložky systému riadenia bezpečnosti zabezpečuje

a) vypracovanie a aktualizáciu dokumentov upravujúcich systém riadenia bezpečnosti podľa odseku 1,

b) vyhodnocovanie stavu bezpečnosti informačných technológií verejnej správy najmenej jedenkrát do roka vo forme správy a jej predloženie riadiacej zložke,

c) realizáciu bezpečnostných opatrení,

d) plánovanie, koordináciu a vyhodnocovanie činností súvisiacich s riadením bezpečnostných rizík v oblasti bezpečnosti informačných technológií verejnej správy,

e) koordináciu riešenia bezpečnostných incidentov,

f) organizáciu vzdelávacej činnosti pre oblasť bezpečnosti informačných technológií verejnej správy.

Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie

(4) Správca prostredníctvom kontrolnej zložky systému riadenia bezpečnosti zabezpečuje

a) nezávislú kontrolu dodržiavania povinností v oblasti bezpečnosti informačných technológií verejnej správy,

b) hodnotenie súladu stavu bezpečnosti s požiadavkami všeobecne záväzných právnych predpisov.

Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie

(5) Správca pri plánovaní vytvorenia alebo nadobudnutia informačného systému verejnej správy

a) určí kategóriu informačného systému verejnej správy, do ktorej bude z hľadiska klasifikácie informácií a kategorizácie sietí a informačných systémov patriť,

b) vypracuje bezpečnostnú politiku, definuje bezpečnostné problémy, ktoré ochrana informačného systému verejnej správy musí riešiť, a navrhne riešenie týchto problémov formou bezpečnostných cieľov,

c) určí osobu zodpovednú za bezpečnosť informačného systému verejnej správy, ktorá

1. rozpracuje bezpečnostné ciele podľa písmena b) do podoby bezpečnostných požiadaviek na vývoj alebo na dodanie informačného systému verejnej správy,

2. vypracuje plán postupu pre naplnenie bezpečnostných požiadaviek podľa prvého bodu a dohliada na ich dodržiavanie,

d) vypracuje analýzu rizík prostredia, v ktorom bude informačný systém verejnej správy prevádzkovaný.

Bezpečnosť informačných technológií verejnej správy v oblasti obstarávania a implementácie

(1) Správca pri vytváraní alebo nadobúdaní informačného systému verejnej správy

a) určí bezpečnostné požiadavky na informačný systém verejnej správy vrátane podmienok jeho vývoja, testovania a dodania v podmienkach vytvorenia alebo dodania informačného systému verejnej správy,

b) poskytne dodávateľovi informačného systému verejnej správy pseudonymizované kópie údajov alebo fiktívne údaje na testovanie informačného systému verejnej správy a jeho vývoj, ak poskytnutie údajov neznamená pre správcu neprimeranú záťaž s ohľadom na prínos poskytnutia pre testovanie a vývoj,

c) zabezpečí pre tento systém vypracovanie bezpečnostného projektu podľa § 23 ods. 1 a 2.

Bezpečnosť informačných technológií verejnej správy v oblasti obstarávania a implementácie

(2) Dodávateľ informačného systému verejnej správy pre vývoj tohto systému

a) zabezpečí

1. bezpečné vývojové prostredie,

2. dokumentáciu vývoja vrátane používateľskej dokumentácie a administrátorskej dokumentácie.

b) je oprávnený zabezpečiť vytvorenie časti informačného systému verejnej správy treťou osobou len po predchádzajúcom písomnom informovaní správcu,

Bezpečnosť informačných technológií verejnej správy v oblasti obstarávania a implementácie

c) je povinný

1. dodržiavať mlčanlivosť o dodávanom informačnom systéme verejnej správy aj po ukončení dodania a zaviazať rovnakou povinnosťou všetky osoby, ktoré sa na dodaní podieľali,

2. dodržiavať vhodné bezpečnostné mechanizmy a preukázať, že ich rozsah a úroveň zodpovedajú bezpečnostným požiadavkám podľa odseku 1 písm. a),

3. identifikovať bezpečnostné požiadavky na informačný systém verejnej správy podľa odseku 1 písm. a), ktoré nie sú pokryté týmto systémom, a predložiť správcovi návrh bezpečnostných opatrení na naplnenie týchto bezpečnostných požiadaviek pre prostredie, v ktorom bude informačný systém verejnej správy prevádzkovaný,

4. upozorniť správcu na kritické časti alebo na rizikové časti informačného systému verejnej správy, ktoré odhalí pri jeho dodaní, a navrhnúť opatrenia na ich riešenie,

5. preukázateľne odstrániť alebo znemožniť používanie funkcie informačného systému verejnej správy, ktoré by jemu alebo tretej strane umožňovali získať neoprávnený prístup do tohto systému a k údajom, ktoré obsahuje.

Bezpečnosť informačných technológií verejnej správy v oblasti prevádzky, servisu a podpory

(1) V rámci zabezpečenia riadenia služieb bezpečnosti prevádzky podľa § 16 ods. 1 písm. d) správca zabezpečuje

a) zavedenie informačného systému verejnej správy do prevádzky,

b) prevádzku informačného systému verejnej správy,

c) vyradenie informačného systému verejnej správy z prevádzky.

(2) V rámci zabezpečenia zavedenia informačného systému verejnej správy do prevádzky správca

a) overí splnenie funkčných, výkonnostných a bezpečnostných požiadaviek pred zavedením do prevádzky a nezavedie do prevádzky informačný systém verejnej správy, ktorý tieto požiadavky nespĺňa,

b) dbá na to, aby pri zavádzaní informačného systému verejnej správy do prevádzky nebol dodávateľovi umožnený prístup k ostatným informačným systémom a údajom, ktoré sa v nich spracúvajú, a ak to nie je možné, zabezpečí potrebnú kontrolu dodávateľa po celý čas, po ktorý je potrebný prístup k ostatným informačným systémom alebo k údajom, ktoré sa v nich spracúvajú, a zaviaže dodávateľa záväzkom mlčanlivosti vo vzťahu k údajom v informačných systémoch a povinnosťou použiť ich len na účel zavádzania informačného systému do prevádzky.

Bezpečnosť informačných technológií verejnej správy v oblasti prevádzky, servisu a podpory

(3) V rámci zabezpečenia prevádzky informačného systému verejnej správy správca

a) zabezpečí pre informačný systém verejnej správy

1. určenie a pravidelné aktualizovanie bezpečnostných cieľov,

2. naplnenie bezpečnostných cieľov a eliminovanie negatívnych vplyvov a udalostí na informačný systém verejnej správy pri jeho prevádzkovaní,

Bezpečnosť informačných technológií verejnej správy v oblasti prevádzky, servisu a podpory

b) v závislosti od zaradenia informačného systému verejnej správy z pohľadu klasifikácie informácií a kategorizácie sietí a informačných systémov

1. aktualizuje bezpečnostný projekt pre tento systém vypracovaný podľa § 20 ods. 1 písm. c),

2. zavedie jednotný systém riadenia informačnej bezpečnosti pre všetky informačné systémy, ktoré sú v jeho správe,

3. zabezpečí riadenie konfigurácie informačného systému verejnej správy a jeho častí,

4. určí bezpečnostne závažné operácie, ktorými sa rozumejú najmä správa prístupov a prístupových údajov, ukladanie záznamov o systémových udalostiach, realizácia bezpečného oddelenia vnútornej časti systému a siete od vonkajšej časti, a zavedie dokumentovanie postupov pre tieto operácie,

5. zabezpečí nepretržitý monitoring informačného systému verejnej správy,

6. zabezpečí vykonanie bezpečnostného auditu informačného systému verejnej správy v pravidelných intervaloch určených najmä s ohľadom na dôležitosť informačného systému verejnej správy a na minulé zistenia bezpečnostných auditov a pri zistení závažných bezpečnostných nedostatkov prepracuje bezpečnostný projekt a naň nadväzujúce dokumenty.

Bezpečnosť informačných technológií verejnej správy v oblasti prevádzky, servisu a podpory

(4) V rámci vyradenia informačného systému verejnej správy z prevádzky správca

a) vypracuje plán vyradenia informačného systému verejnej správy z prevádzky, ktorý obsahuje najmä

1. uchovanie kritických informácií vyraďovaného informačného systému verejnej správy, ktoré sú už nepotrebné pre funkčnosť iného informačného systému,

2. spoľahlivé odstránenie informácií z pamäťových médií vyraďovaného informačného systému verejnej správy,

3. postup vyraďovania programových prostriedkov a technických prostriedkov informačného systému verejnej správy,

b) zabezpečí, aby nedošlo ku strate alebo k úniku informácií a k narušeniu práv priemyselného vlastníctva a duševného vlastníctva.

Bezpečnosť informačných technológií verejnej správy v oblasti monitoringu a hodnotenia

V oblasti monitoringu a hodnotenia správca vo vzťahu k informačným technológiám v jeho správe prijíma a vykonáva bezpečnostné opatrenia pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov podľa osobitného predpisu.[23])

§ 20 ods. 3 písm. k) zákona č. 69/2018 Z. z.

Osobitné opatrenia na úseku bezpečnosti informačných technológií verejnej správy

(1) Bezpečnostný projekt informačného systému verejnej správy je dokument obsahujúci komplexné posúdenie bezpečnostných potrieb, určenie bezpečnostných požiadaviek a návrh spôsobu ich efektívneho naplnenia. Bezpečnostný projekt môže byť vypracovaný aj pre viacero informačných systémov verejnej správy, ktoré sú v správe jedného správcu. Vypracovanie bezpečnostného projektu informačného systému verejnej správy zabezpečí správca, vychádzajúc

a) z bezpečnostnej politiky,

b) zo všeobecne akceptovaných štandardov riadenia informačných technológií, ktoré vychádzajú z uznaných technických noriem,

c) z metodických usmernení orgánu vedenia.

(2) Správca vypracuje bezpečnostný projekt vždy pre informačný systém verejnej správy, ktorý je z pohľadu klasifikácie informácií a kategorizácie sietí a informačných systémov v najvyššej kategórii z hľadiska jeho významnosti, funkcie a účelu použitia s ohľadom na potrebu zabezpečenia ochrany dôvernosti a integrity a zabezpečenia dostupnosti a úrovne činností vykonávaných s jeho použitím.

Osobitné opatrenia na úseku bezpečnosti informačných technológií verejnej správy

(3) Orgán riadenia podľa § 5 ods. 2 písm. a) a b) a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti sú povinní vo vzťahu k informačným technológiám verejnej správy

a) ak sú zaradení do registra prevádzkovateľov základných služieb podľa osobitného predpisu,[24]) nahlasovať spôsobom podľa osobitného predpisu[25]) aj kybernetický bezpečnostný incident,[26]) na ktorý sa nevzťahuje povinnosť nahlasovania podľa osobitného predpisu;[27]) ak nie sú do tohto registra zaradení, nahlasujú takýto kybernetický bezpečnostný incident orgánu vedenia ním určeným spôsobom,

b) zasielať automatizovaným spôsobom a najviac v rozsahu ustanovenom v štandardoch orgánu vedenia ním určené systémové informácie z informačných technológií verejnej správy,

c) poskytnúť orgánu vedenia súčinnosť a spoluprácu pri plnení jeho úloh podľa odseku 5,

d) prijať alebo upraviť bezpečnostné opatrenia vrátane vypracovania bezpečnostného projektu, ak bezpečnostný audit alebo hodnotenie zraniteľnosti vykonané orgánom vedenia zistí riziko[28]) alebo hrozbu[29]) pre informačnú technológiu verejnej správy a oznámiť mu prijaté alebo upravené bezpečnostné opatrenia,

e) zasielať najmenej jedenkrát do roka orgánu vedenia zoznam aktív podľa § 19 ods. 1 písm. c),

f) určiť jeden kontaktný bod na nahlasovanie kybernetických bezpečnostných incidentov podľa písmena a).

Osobitné opatrenia na úseku bezpečnosti informačných technológií verejnej správy

(4) Orgán riadenia neuvedený v odseku 3 je povinný plniť povinnosti podľa odseku 3 písm. a), c), e) a f).

(5) Orgán vedenia vo vzťahu k informačným technológiám verejnej správy

a) môže na žiadosť orgánu riadenia vykonávať činnosti na účely riešenia kybernetického bezpečnostného incidentu podľa odseku 3 písm. a), jeho predchádzania alebo odstraňovania zistení bezpečnostného auditu alebo hodnotenia zraniteľnosti,

b) zbiera, spracúva a vyhodnocuje systémové informácie na účely predchádzania kybernetickým bezpečnostným incidentom, ich riešenia a obnovenia kybernetickej bezpečnosti,[30])

c) vykonáva pravidelné neinvazívne hodnotenie zraniteľnosti služby verejnej správy, služby vo verejnom záujme, verejnej služby a ďalších služieb informačných technológií poskytovaných prostredníctvom siete internet alebo prostredníctvom Govnetu,

d) môže na žiadosť orgánu riadenia podľa odseku 3 za tento orgán riadenia vykonať bezpečnostný audit alebo preň vykonať hodnotenie zraniteľnosti.

Správne delikty (§29)

(1) Orgán vedenia uloží pokutu

a) od 500 eur do 35 000 eur správcovi, ktorý poruší povinnosť podľa § 6 ods. 1, § 12 ods. 1 písm. a), § 14 ods. 6, § 15 ods. 2 alebo § 16 ods. 3 písm. e) alebo povinnosti na úseku bezpečnosti informačných technológií verejnej správy podľa § 19 až 21 alebo § 23,

Zmocňovacie ustanovenia (§31)

Všeobecne záväzný právny predpis, ktorý sa v Zbierke zákonov Slovenskej republiky vyhlasuje uverejnením úplného znenia a ktorý vydá ministerstvo investícií, ustanoví

a) jednotlivé kategórie informačných technológií verejnej správy a podrobnosti o spôsobe zaraďovania do týchto kategórií s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov podľa osobitného predpisu na účely podľa § 11 ods. 4,

i) podrobnosti o bezpečnosti informačných technológií verejnej správy podľa § 18 až 23, obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostného projektu a rozsah bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov,

Vyhláška 179/2020 z.z.

Vyhláška 179/2020 z.z.

- Vydaná na základe §31 zákona o IT vo VS
- Klasifikácia/kategorizácia ITVS
  - Zaraďovanie do kategórií
  - Zohľadňuje klasifikáciu informácií , sietí a informačných systémov podľa vyhlášky NBÚ 362/2018 Z. z.
- Rozpracováva ustanovenia zákona 95/2019 o ITVS
  - Obsah bezpečnostných opatrení
  - Obsah a štruktúra bezpečnostného projektu
- Minimálne bezpečnostné opatrenia pre jednotlivé kategórie
- Sľubujú, že správcom ITVS dajú návody, školiace materiály, ukážky šablóny a vzory dokumentácie
- Prílohy
  - Zoznam aktív
  - Minimálne bezpečnostné opatrenia
  - Obsah a štruktúra bezpečnostného projektu ISVS

Bezpečnostné opatrenia

- 3 sady bezpečnostných opatrení pre jednotlivé kategórie
- Vyššia úroveň má prednosť
- Zobrali si orgány riadenia podľa §5 zákona a rozdelili ich na 3 skupiny
- 1. skupina (opatrenia kategórie I)
  - Obec alebo mesto do 6000 obyvateľov
  - právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia podľa § 5 ods. 2 písm. a) až d) zákona, ktorá nie je uvedená v odsekoch 3 a 4,
  - osoba neuvedená v písmenách a) až f) okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov,
  - komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,

Bezpečnostné opatrenia

2. Skupina (opatrenia I. a II. Kategórie)

a) obec nad 6000 obyvateľov,

b) obec so štatútom mesta nad 6000 obyvateľov okrem krajských miest,[3)]

c) mestskú časť s právnou subjektivitou,[4)]

d) Kanceláriu verejného ochrancu práv,

e) Úrad komisára pre deti,

f) Úrad komisára pre osoby so zdravotným postihnutím,

g) Radu pre vysielanie a retransmisiu,

h) prevádzkovateľa základných služieb podľa osobitného predpisu,[2)] ktorého siete a informačné systémy sú zaradené do Kategórie I alebo Kategórie II podľa osobitného predpisu[1)] neuvedeného v odseku 4.

Bezpečnostné opatrenia

3. Skupina (opatrenia I. ,II. a III. Kategórie)

a)obec, ktorá je aj krajským mestom,[3)]

b)samosprávny kraj,

c) ministerstvo a ostatný ústredný orgán štátnej správy,[5)]

d) Úrad pre reguláciu sieťových odvetví,

e) Úrad pre reguláciu elektronických komunikácií a poštových služieb,

f)Najvyšší kontrolný úrad Slovenskej republiky,

g) Úrad pre dohľad nad zdravotnou starostlivosťou,

h) Úrad na ochranu osobných údajov Slovenskej republiky,

i) Generálnu prokuratúru Slovenskej republiky,

j) Dopravný úrad,

Bezpečnostné opatrenia

3. Skupina (opatrenia I. ,II. a III. Kategórie)

k)Ústav pamäti národa,

l) Tlačovú agentúru Slovenskej republiky,

m) Rozhlas a televíziu Slovenska,

n) Kanceláriu Súdnej rady Slovenskej republiky,

o) Kanceláriu Najvyššieho súdu Slovenskej republiky,

p) Kanceláriu Ústavného súdu Slovenskej republiky,

q) Kanceláriu prezidenta Slovenskej republiky,

r) Kanceláriu Národnej rady Slovenskej republiky,

s) Finančné riaditeľstvo Slovenskej republiky,

t) Národnú agentúru pre sieťové a elektronické služby,

u) Zbor väzenskej a justičnej stráže,

v)DataCentrum Ministerstva financií Slovenskej republiky,

Bezpečnostné opatrenia

3. Skupina (opatrenia I. ,II. a III. Kategórie)

w) DataCentrum elektronizácie územnej samosprávy Slovenska,

x) Sociálnu poisťovňu,

y) zdravotnú poisťovňu,

z) Národné centrum zdravotníckych informácií,

aa) prevádzkovateľa základných služieb podľa osobitného predpisu,[2)] ktorého siete a informačné systémy sú zaradené do Kategórie III podľa osobitného predpisu.[1)]

Zodpovednosť a vlastné riešenia bezpečnosti (§4)

(1) Za bezpečnosť informačných technológií verejnej správy je zodpovedný jeho správca. Ak je na bezpečnosť informačných technológií verejnej správy vhodné prijať iný súbor opatrení, ako sú opatrenia uvedené v tejto vyhláške, zmeny v rozsahu opatrení správca zadokumentuje, odôvodní a tieto zmeny schválené štatutárnym orgánom zašle orgánu vedenia.

(2) Ak sa v tejto vyhláške ustanovuje použitie postupu podľa technickej normy, slovenskej technickej normy, európskeho normalizačného produktu alebo európskej normy, je možné postupovať aj podľa ich ekvivalentu, ak sa takýmto postupom dosiahne rovnaký výsledok a dodržia sa požiadavky podľa tejto vyhlášky. Pri pochybnostiach o vhodnosti použitia ekvivalentnej normy alebo špecifikácie podľa prvej vety je rozhodujúce vyjadrenie orgánu vedenia k možnosti ich použitia.

Termíny

- 30. jún 2022 pre existujúce organizácie správcu VS
- 1. skupina – vnútorné riadiace akty do 30. júna 2021 (ďalšie povinnosti do 30. júna 2022)

Prílohy Vyhlášky 179/2020 z.z.

Prílohy
Zoznam aktív

- Väčšinu vyhlášky tvoria prílohy
- Príloha 1: zoznam aktív
  - Príliš podrobný
  - Nezodpovedá štandardom
  - Sústreďuje sa na technické zariadenia a programové vybavenie
  - Chýbajú nehmotné aktíva, údaje

Aktíva

a) pracovná stanica – stolová,

b) pracovná stanica – prenosná,

c) aplikačný softvér,

1. kancelársky softvér,
2. **i**nternetový prehliadač,
3. antivírusový softvér,
4. komunikačný softvér,
5. ďalší využívaný komerčný softvér,

d) všetky druhy serverov,

e) virtualizačné prostredie,

f) databázové prostredie,

g) komerčný podnikový softvér,

h) sieťový firewall,

i) sieťový router,

j) sieťový prepínač,

k) komunikačné prostredie,

l) zálohovacie prostredie,

m) mobilné zariadenia,

n) dátové úložiská,

o) ostatné zariadenia alebo sieťové prvky schopné komunikovať so zvyškom ekosystému informačných technológií verejnej správy,

p) prenosné zariadenia.

Aktíva podľa ISO/IEC 27005

- Systematické členenie
- Hierarchia + prepojenie s poslaním organizácie a významom pre plnenie poslania
- Dá sa logicky odvodiť a zdôvodniť, čo sú aktíva a do akej úrovne podrobností ísť
- Primárne
  - Procesy (Business processes & activities)
  - Informácia
- Sekundárne
  - Hw
  - Sw
  - Sieť
  - Ľudia
  - Sídlo
  - Štuktúra organizácie

Identifikácia aktív podľa ISO

- Najdôležitejšie procesy vieme odvodiť aj my (manažéri K/IB)
- Potrebujeme ísť hlbšie, identifikovať aktíva, na ktorých proces závisí
- Toto koordinuje manažér, ale spolupracuje s vecne zodpovednými riadiacimi pracovníkmi, informatikmi a používateľmi
- Záleží aj od hĺbky a účelu analýzy rizík
- Podľa ISO:

1 - Business processes (or sub-processes) and activities, for example:

- Processes whose loss or degradation make it impossible to carry out the mission of the organization
- Processes that contain secret processes or processes involving proprietary technology
- Processes that, if modified, can greatly affect the accomplishment of the organization's mission
- Processes that are necessary for the organization to comply with contractual, legal or regulatory requirements

Identifikácia aktív podľa ISO

- Podľa ISO:

2 – Information: More generally, primary information mainly comprises:

  - Vital information for the exercise of the organization's mission or business
  - Personal information, as can be defined specifically in the sense of the national laws regarding privacy
  - Strategic information required for achieving objectives determined by the strategic orientations
  - High-cost information whose gathering, storage, processing and transmission require a long time and/or involve a high acquisition cost

- Identifikácia primárnych aktív stanoví rozsah analýzy rizík
- Poďme sa pozrieť na sekundárne aktíva

Identifikácia aktív podľa ISO

- Poďme sa pozrieť na sekundárne aktíva
- Hardvér
  - Zariadenia na spracovanie informácie
  - Prenosné zariadenia
  - Stacionárne počítače
  - Periférie
  - Pasívne pamäťové media (zabudované v počítačoch a zariadeniach)
  - Prenosné pamäťové media (elektronické)
  - Iné pamäťové media (papierové)
- Softvér
  - Programové vybavenie, ktoré sa podieľa na spracovaní údajov
  - Aplikácie (business application)
    - Štandardné
    - špecifické

Identifikácia aktív podľa ISO

- Sieť
  - Technická časť (komunikačné kanály, aktívne prvky)
  - Protokoly
  - Komunikačné rozhrania
- Ľudia
  - Riadiaci pracovníci (vlastníci primárnych aktív, manažéri veľkých projektov,…)
  - Používatelia (obyčajní a privilegovaní)
  - Správcovia, operátori, technici, bezpečnostní operátori/technici zabezpečujúci prevádzku systémov
  - Vývojári

Identifikácia aktív podľa ISO

- Sídlo – jedna alebo viac lokalít kde sú umiestnené budovy, priestory
  - lokalita
    - Externé prostredie
    - Budovy (perimeter)
    - Zóny
    - Podstatatné služby (čo potrebujeme, aby zariadenia/systémy mohli fungovať)
    - Komunikácia
    - Podporné prostriedky a služby (napájanie, voda, klimatizácia, odvoz odpadu, klimatizácia a filtrovanie vzduchu,…)

Identifikácia aktív podľa ISO

- Organizácia
  - riadiaca štruktúra organizácie (štatút, organizačný poriadok, prakticky – obsadenie pozícií)
  - Organizačná štruktúra (sekcie, oddelenia, odbory,…)
  - Organizácia projektov a systémov (existujúce systémy, zmeny)
  - Subkontraktori, dodávatelia, výrobcovia

- Vyplatí sa pozrieť aj BSI štandardy

Vyhláška vs. ISO norma

- Vyhláška – značne zjednodušený pohľad,
- Ale povoľuje aplikovať normy
- Poďme podľa noriem

Opatrenia

Príloha 2

Prechádzajú cez jednotlivé oblasti kybernetickej a informačnej bezpečnosti a definujú súbory opatrení pre jednotlivé kategórie (I.II a III)

A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti
B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti
C. Personálna bezpečnosť
D. Riadenie prístupov
E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami
F. Bezpečnosť pri prevádzke informačných systémov a sietí
G. Hodnotenie zraniteľností a bezpečnostné aktualizácie
H. Ochrana proti škodlivému kódu
I. Sieťová a komunikačná bezpečnosť
J. Akvizícia, vývoj a údržba informačných technológií verejnej správy
K. Zaznamenávanie udalostí a monitorovanie
L. Fyzická bezpečnosť a bezpečnosť prostredia
M. Riešenie kybernetických bezpečnostných incidentov
N. Kryptografické opatrenia
O. Kontinuita prevádzky informačných technológií verejnej správy
P. Audit a kontrolné činnosti

Čo by bolo treba?

- Porovnať opatrenia vyhlášky s opatreniami normy ISO/IEC 27002, lebo
  - predchádzujúci Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy vychádzal v časti bezpečnosť z ISO/IEC 27002
  - ISO/IEC 27002 je medzinárodná norma, vyhláška má lokálnu platnosť
  - Samotná vyhláška pripúšťa použitie noriem
- Obávam sa, že navrhované opatrenia nie sú realizovateľné (ľudia, peniaze)

Organizácia KIB (Kategória I)

- Pozrieme sa na opatrenia navrhované pre jednotlivé kategórie, lebo toto sa nás bude bezprostredne týkať

Kategória I

a) Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.

b) Vypracovanie a implementácia interného riadiaceho aktu, ktorý je pre organizáciu správcu záväzný a obsahuje najmenej

1. určenie povinnosti, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti,

2. základné zásady a opatrenia kybernetickej bezpečnosti a informačnej bezpečnosti, ktoré organizácia správcu má zavedené a riadi sa nimi.

Organizácia KIB (Kategória II)

Kategória II

a) Vypracovanie a implementácia interného riadiaceho aktu Politika kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý je pre organizáciu správcu záväzný a obsahuje najmenej

1. určenie povinnosti, zodpovednosti a právomoci manažéra kybernetickej bezpečnosti a informačnej bezpečnosti a všetkých zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,

2. základné zásady a opatrenia kybernetickej a informačnej bezpečnosti v štruktúre oblastí definovaných touto vyhláškou.

Komentár

- Štandardná bezpečnostná politika, dať si pozor, aby explicitne obsahovala všetky oblasti KIB, ktoré uvádza vyhláška

Organizácia KIB (Kategória II)

Určenie a personálne zabezpečenie roly manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu zodpovedného za koordináciu a plnenie týchto úloh:

1. vypracovať, udržiavať a aktualizovať Politiku kybernetickej bezpečnosti a informačnej bezpečnosti a ďalšie interné riadiace akty podľa písmena c),

2. riadiť a zaisťovať kybernetickú a informačnú bezpečnosť podľa všeobecne záväzných právnych predpisov a interných riadiacich aktov,

3. metodicky viesť správcov informačných technológií verejnej správy, gestorov informačných technológií verejnej správy, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov,

4. v súčinnosti s ostatnými organizačnými útvarmi analyzovať, definovať a monitorovať bezpečnostné hrozby a riziká organizácie,

Organizácia KIB (Kategória II)

Určenie a personálne zabezpečenie roly manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu zodpovedného za koordináciu a plnenie týchto úloh:

5. navrhovať opatrenia na zamedzenie alebo minimalizáciu rizík a dopadov hrozieb, bezpečnostných udalostí, incidentov, mimoriadnych situácií, monitorovať plnenie a efektivitu týchto opatrení a viesť evidenciu bezpečnostných incidentov,

6. koordinovať vypracovanie plánov kontinuity a obnovy činností organizácie správcu,

7. predkladať odborné stanoviská, analýzy k procesom, projektom, zmenám a ostatným aktivitám organizácie majúcich vplyv na kybernetickú bezpečnosť a informačnú bezpečnosť organizácie správcu,

8. zabezpečiť pravidelné – najmenej raz za dva roky – preskúmanie stavu informačnej bezpečnosti a spolupracovať pri realizácii auditov vykonávaných internými a externými subjektmi,

9. zabezpečovať školenia zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,

10. spolupracovať s inými orgánmi verejnej moci.

Organizácia KIB (Kategória II)

c) Vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej bezpečnosti a informačnej bezpečnosti v rozsahu a detaile zodpovedajúcom veľkosti a štruktúre organizácie správcu, významu informačných technológií verejnej správy v jeho správe a štruktúre existujúcich interných riadiacich aktov s detailným opisom jednotlivých opatrení a postupov pre tieto oblasti:

1. organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
2. riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
3. personálna bezpečnosť,
4. riadenie prístupov,
5. riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami,
6. bezpečnosť pri prevádzke informačných systémov a sietí,
7. hodnotenie zraniteľnosti a bezpečnostné aktualizácie,
8. ochrana proti škodlivému kódu,

Organizácia KIB (Kategória II)

9. sieťová a komunikačná bezpečnosť,
10. akvizícia, vývoj a údržba informačných technológií verejnej správy,
11. zaznamenávanie udalostí a monitorovanie,
12.riadenie kontinuity procesov. fyzická bezpečnosť a bezpečnosť prostredia,
13. riešenie kybernetických bezpečnostných incidentov,
14. kryptografické opatrenia,
15. kontinuita prevádzky informačných technológií verejnej správy,
16. audit a kontrolné činnosti.

Organizácia KIB (Kategória II)

d) Zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti podľa osobitného predpisu.[6)]

e) Monitorovanie a vyhodnocovanie dodržiavania Politiky kybernetickej bezpečnosti a informačnej bezpečnosti a efektivity jednotlivých opatrení a postupov.

f) Aktualizácia Politiky kybernetickej bezpečnosti a informačnej bezpečnosti najmenej raz za rok.

Organizácia KIB (Kategória III)

a) Vytvorenie bezpečnostného výboru s rozsahom povinností a právomocí určených štatútom.

b) Bezpečnostný výbor pri výkone svojej činnosti najmä

1. riadi stratégie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,

2. riadi bezpečnostné riziká v rozsahu celej organizácie, akceptuje bezpečnostné riziká, ktoré sa týkajú viac ako jednej organizačnej jednotky organizácie správcu,

3. schvaľuje a rozhoduje o implementácii významných bezpečnostných opatrení a postupov,

4. schvaľuje odporúčania, návrhy strategických a koncepčných materiálov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, predkladaných manažérom kybernetickej bezpečnosti a informačnej bezpečnosti,

5. predkladá štatutárnemu orgánu na schválenie návrh zodpovednosti za implementáciu a uplatňovanie jednotlivých opatrení a postupov kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii.

Organizácia KIB (Kategória III)

c) Bezpečnostný výbor sa skladá najmenej z

1. štatutára správcu, jeho zástupcu alebo ním poverenej osoby,

2. manažéra kybernetickej bezpečnosti a informačnej bezpečnosti,

3. vedúceho zamestnanca organizačného útvaru zodpovedného za správu informačno-komunikačnej infraštruktúry,

4. vedúceho zamestnanca organizačného útvaru zodpovedného za právne a legislatívne služby,

5. zodpovednej osoby za ochranu osobných údajov.

Minimálne zloženie bezpečnostného výboru možno doplniť o ďalšie osoby.

Organizácia KIB (Kategória III)

d) Vytvorenie pozície manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu mimo organizačného útvaru zodpovedného za správu a prevádzku informačných technológií verejnej správy.

e) Manažér kybernetickej bezpečnosti a informačnej bezpečnosti pri výkone svojej činnosti najmä

1. navrhuje stratégie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,
2. informuje bezpečnostný výbor alebo štatutárny orgán správcu o stave informačnej bezpečnosti v organizácii správcu najmenej raz za rok,
3. bezodkladne informuje bezpečnostný výbor alebo štatutárny orgánu správcu o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach,
4. zabezpečuje nezávislé preskúmanie stavu informačnej bezpečnosti a spoluprácu pri realizácii auditov vykonávaných internými a externými subjektmi.

Organizácia KIB (Kategória III)

f) Zabezpečenie kontinuálneho vzdelávania manažéra kybernetickej bezpečnosti a informačnej bezpečnosti.

g) Uplatňovanie princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie správcu tak, že rovnaká osoba nie je zodpovedná za vykonávanie a zároveň aj schvaľovanie alebo kontrolu bezpečnostne relevantných aktivít a činností.

h) Zabezpečenie preskúmania a identifikácie bezpečnostných rizík v počiatočných fázach procesu riadenia projektov v organizácii správcu a určenie adekvátnych opatrení na zníženie každého identifikovaného rizika na prijateľnú úroveň. Definovanie osoby zodpovednej za kybernetickú a informačnú bezpečnosť v projektovom tíme.

i) Zabezpečenie vypracovania bezpečnostného projektu informačného systému verejnej správy.

Čo s tým?

- Som manažér KIB v organizácii
  - I. Kategória –
    - je to celé na mne,
    - Jednoduchý bezpečnostný projekt (identifikácia hlavných aktív, hrozieb, povinností, analýza rizík, návrh a implementácia opatrení, dokumentácia, system kontroly opatrení, správa vedeniu organizácie spolu s rozpočtom na ďalší rok)
  - II. Kategória – žarty končia, ideme na ISMS
    - Bezpečnostná politika a množstvo ďalšej bezpečnostnej dokumentácie
    - Treba definovať povinnosti všetkých, ktorí mi môžu pomôcť
    - Zatiaľ neexistuje kolektívny organ (až od III. Kategórie)
    - Intenzívna komunikácia s vedením organizácie, ale aj externými orgánmi, externý audit
    - Bezpečnosť v činnosti organizácie
    - Prejsť si cez zákon o IT vo VS, vyhlášku a ostatné relevantné zákony, vypísať si povinnosti, usporiadať ich a namapovať na ISO normy (tu sú povinnosti, ale nie súvislosti ani návody, ako ich plniť)

Čo s tým?

- III. Kategória
  - Ostávajú v platnosti opatrenia II a I. úrovne, ktoré nie sú prekryté II. úrovňou
  - Značná časť zodpovednosti prechádza na bezpečnostný výbor
  - Ale pracovných povinností mi neubudlo
  - Iniciatívna rola bezpečnostného manažéra – má prichádzať s návrhmi
    - Riadenie KIB podľa ISO alebo BSI
    - Potrebujem výkonných ľudí
      - Na plný úväzok (akých, čo budú robiť?)
      - Čiastočné úväzky
      - Rozšírenie povinností
      - Externí špecialisti (audit, CSIRT)
  - Asi tiež zavedenie ISMS

Bezpečnostný projekt

Príloha 3 Bezpečnostný projekt

OBSAH A ŠTRUKTÚRA BEZPEČNOSTNÉHO PROJEKTU INFORMAČNÉHO SYSTÉMU VEREJNEJ SPRÁVY

(1) Pri spracovaní bezpečnostného projektu informačného systému verejnej správy sa prihliada najmä na zložitosť informačného systému verejnej správy, komplexnosť agendy pokrytej informačným systémom verejnej správy a stanovenie bezpečnostných požiadaviek na informačný systém verejnej správy. Zohľadniť sa musí taktiež kategória, do ktorej je informačný systém verejnej správy zaradený.

(2) (2) Bezpečnostný projekt informačného systému verejnej správy pozostáva z dvoch hlavných výstupov: bezpečnostného zámeru a analýzy bezpečnosti. Jednotlivé výstupy vznikajú v určenom poradí a sú priebežne aktualizované počas celého projektu informačného systému verejnej správy realizovaného v súlade so zákonom.

***Komentár**: nie je reálne, aby sa na každý systém verejnej správy vypracoval samostatný bezpečnostný projekt; iba ak by sa za informačný system považovali všetky IKT organizácie. Reálne – treba rozlišovať 2 úrovne – bezpečnosť organizácie a bezpečnosť jednotlivých systémov*

Príloha 3 Bezpečnostný projekt

(3) Ako prvý výstup bezpečnostného projektu informačného systému verejnej správy sa vypracuje dokument bezpečnostný zámer. Bezpečnostný zámer určuje najmä kontext a zameranie bezpečnostného projektu, preto obsahuje najmenej

a) formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov orgánu riadenia, technických noriem a štandardov dobrej praxe,

b) zoznam právnych predpisov aplikovaných v bezpečnostnom projekte, ako aj interných riadiacich aktov,

c) metodický prístup ku kvalitatívnej analýze rizík, ktorá je v bezpečnostnom projekte vykonaná,

d) rámcovú špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany informačného systému verejnej správy, jeho služieb a údajov v ňom spracúvaných s ohľadom na kategóriu, do ktorej je informačný systém verejnej správy zaradený,

e) vymedzenie okolia informačného systému verejnej správy a jeho vzťah k možnému narušeniu bezpečnosti informačného systému verejnej správy vrátane zoznamu integrácií na informačný systém verejnej správy,

f) vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,

g) ohraničenia bezpečnostného projektu (explicitné vysvetlenie oblastí, ktoré bezpečnostný projekt nezahŕňa alebo kladie požiadavky na ich riešenie mimo projektu informačného systému verejnej správy),

h) postupy revízie/aktualizácie bezpečnostného zámeru.

Príloha 3 Bezpečnostný projekt

Komentár: Ak by v organizácii existovala bezpečnostná politika, prípadne ISMS, potom by sa dalo na tieto dokumenty v bezpečnostnom zámere len odvolávať a len upresniť alebo konkretizovať veci, ktoré sú v bezpečnostnej politike napísané len všeobecne

Príloha 3 Bezpečnostný projekt

(4) Ako hlavný výstup bezpečnostného projektu informačného systému verejnej správy sa vypracuje dokument analýza bezpečnosti, ktorého súčasťou je kvalitatívna analýza rizík. Rizikom sa v bezpečnostnom projekte chápe miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami. Analýza rizík je zameraná na získanie aktuálnych a vierohodných poznatkov o pravdepodobných rizikách týkajúcich sa aktív informačného systému verejnej správy a jeho okolia. Analýza rizík sa vykonáva pre informačný systém verejnej správy priebežne počas celého projektu v súlade so zákonom a priamo nadväzuje na dokument bezpečnostný zámer. Analýza rizík pozostáva z výkonu týchto činností:

a) vytvorenie podkladových katalógov na analyzované riziká určených na identifikáciu aktív, identifikáciu hrozieb a zraniteľností a identifikáciu vplyvov,

b) identifikácia a opis analyzovaných rizík v štruktúre podľa oblastí ustanovených osobitným predpisom[2)] alebo podľa technickej normy,[11)]

c) priradenie aktív, hrozieb, zraniteľností a vplyvov ku každému z identifikovaných rizík,

d) identifikácia realizovaných bezpečnostných opatrení,

e) vyhodnotenie rizík spôsobom kombinácie pravdepodobnosti realizácie scenáru rizika a závažnosti vplyvu,

f) opis navrhovaných bezpečnostných opatrení.

Príloha 3 Bezpečnostný projekt

(5) Pri každom riziku sa zohľadňuje pravdepodobnosť situácie, pri ktorej hrozby využijú existujúce zraniteľnosti a spôsobia negatívny vplyv na aktíva orgánu riadenia. Pri hodnotení závažnosti výsledného vplyvu sa zohľadňuje celková závažnosť vplyvov, ktoré môžu byť spôsobené pri realizácii rizika. Úroveň vplyvov sa určuje osobitne pre každé analyzované riziko a zahŕňa všetky aktíva dotknuté príslušným rizikom. Analyzované riziko môže mať na aktíva orgánu riadenia viaceré vplyvy, ktoré je potrebné sumárne vyhodnotiť a zdokumentovať. Výsledná miera rizika musí zohľadňovať aj všetky realizované bezpečnostné opatrenia.

(6) Metodický postup výkonu analýzy rizík musí byť v súlade s technickou normou.[12)] Výsledné vyhodnotenie rizík podľa použitej metodiky musí byť premietnuté do trojstupňovej stupnice nízke riziko, stredné riziko, vysoké riziko.

ISO/IEC 27005

Príloha 3 Bezpečnostný projekt

(7) Pri tvorbe navrhovaných bezpečnostných opatrení je potrebné určiť prostriedky a procesy odstraňovania nedostatkov zistených v rámci jednotlivých rizík. Cieľom návrhu bezpečnostných opatrení je vytvorenie takého okruhu bezpečnostných opatrení, že po ich implementácii a následnom prehodnotení rizík sú všetky zvyškové riziká akceptovateľné. Pri niektorých typoch opatrení je prípustné sa odkazovať aj na dokumentáciu k informačnému systému verejnej správy v súlade so zákonom. Opis navrhovaných bezpečnostných opatrení zohľadňuje

a) opatrenia ustanovené touto vyhláškou alebo osobitným predpisom,[1])

b) požiadavky vyplývajúce z aplikovateľnej legislatívy,

c) náležitosti implementácie a prevádzky analyzovaného informačného systému verejnej správy a spôsob uplatňovania bezpečnostných opatrení v konkrétnych podmienkach orgánu riadenia,

d) opatrenia realizovateľné v pôsobnosti analyzovaného informačného systému verejnej správy, ale aj opatrenia vo vzťahu k jeho okoliu,

e) dostupné možnosti prístupu k riadeniu rizika,

f) spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení.

Príloha 3 Bezpečnostný projekt

(8) Výstupný dokument analýzy bezpečnosti s výsledkami analýzy rizík obsahuje najmä

a) ciele a priority analýzy rizík,

b) opis použitej metodiky analýzy rizík,

c) opis rizík založený na identifikácii aktív, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností a na identifikácii vplyvov na aktíva najmä v dôsledku straty dôvernosti, integrity a dostupnosti,

d) vyhodnotenie rizík podľa použitej metodiky,

e) opis navrhovaných bezpečnostných opatrení pre identifikované riziká v závislosti od ich závažnosti,

f) celkové zhrnutie výsledkov analýzy rizík, vrátane zoznamu vysokých a stredných rizík usporiadaných podľa dôležitosti, s opisom navrhovaného postupu ich riadenia a kľúčových navrhovaných bezpečnostných opatrení,

g) postupy revízie/aktualizácie analýzy bezpečnosti.

(9) Štruktúra výstupu analýzy bezpečnosti musí zodpovedať oblastiam ustanoveným osobitným predpisom[2)] alebo technickou normou.[11)] Finalizácia dokumentácie bezpečnostného projektu informačného systému verejnej správy je realizovaná v etape IMPLEMENTÁCIA A TESTOVANIE v súlade so zákonom.

Zhrnutie

- Je problém robiť bezpečnostný projekt pre každý systém, ak ich má organizácia veľa
- Riešaním je zavedenie ISMS podľa ISO noriem ISO/IEC 27001 a 2, alebo BSI štandardov
  - Bezpečnostná politika organizácie, obsahujúca bezpečnostný zámer
  - V BP stanovený rámec, identifikované hlavné aktíva, ...
  - Analýza právnych požiadaviek
  - Base line opatrenia pre všetky systémy a celú organizáciu
  - Pre kritické/dôležité systémy – analýza rizík; ale nielen lokálne opatrenia, ale aj globálne (pre celú organizáciu) – aj úprava base line
  - Správa rizík a postupné budovanie ISMS
  - Bezpečnostné projekty pre nové systémy, pre exitujúce keď na to bude dôvod a čas
- Ďalšie zákony a z nich vyplývajúce bezpečnostné požiadavky – sledovať, lebo sa menia

Ďalšie čítanie

- Prečítať: Zákon o KB, zákon o ITVS, vyhlášky k nim, GDPR
- Prelistovať
  - Štandardy BSI
  - Common criteria, aspoň 1. časť
  - NIST SP 800
- Zľahka prejsť cez obsah RFC