Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Systém na podporu vypracovania bezpečnostných projektov pre malé ISVS

Bakalárska práca

2024
Anton Kica

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Systém na podporu vypracovania bezpečnostných projektov pre malé ISVS

Bakalárska práca

Študijný program:	Informatika
Študijný odbor:	Informatika
Školiace pracovisko:	Katedra informatiky
Školiteľ:	doc. RNDr. Daniel Olejár, PhD.

Bratislava, 2024
Anton Kica

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Anton Kica
Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Systém na podporu vypracovania bezpečnostných projektov pre malé ISVS
Auxiliary system for small ISVS security projects creation.

Anotácia: Prevádzkovatelia ISVS (informačných systémov verejnej správy) sú zo zákona povinní zabezpečiť bezpečnosť svojich systémov. Základom toho je vypracovanie bezpečnostného projektu ISVS. Na Slovensku nie je dosť odborníkov, ktorí by tieto projekty boli schopní vypracovať. Bakalár naštuduje zákonné požiadavky na ochranu ISVS najnižšej kategórie, metodiku analýzy rizík a vytvorí dátové štruktúry pre relevantné informácie o ISVS a aplikáciu, ktorá správcovi ISVS umožní zozbierať, spracovať a vyhodnotiť relevantné informácie o ISVS, spraviť analýzu rizík a navrhnúť opatrenia a spravovať riziká voči ISVS.

Cieľ: vytvoriť systém, ktorý správcovi ISVS pomôže zozbierať, spracovať a vyhodnotiť relevantné informácie o ISVS, spraviť analýzu rizík, navrhnúť opatrenia a spravovať riziká voči ISVS

Literatúra:
Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zá-konov (ZoKB)
Vyhláška Národného bezpečnostného úradu, č. 362/2018 Z.z., ktorou sa ustanovuje ob-sah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
ISO/IEC 27001 — Information security management systems — Requirements.
ISO/IEC 27002 — Code of practice for information security management.
ISO/IEC 27005 — Information security risk management.
BSI Standard 200-1 Information Security Management Systems (ISMS) BSI - IT-Grundschutz - BSI-Standard 200-1: Information Security Management Systems (ISMS) (bund.de)
BSI Standard 200-2 IT Grundschutz Methodology, BSI - IT-Grundschutz - BSI-Standard 200-2: IT-Grundschutz-Methodology (bund.de)
BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz BSI - IT-Grundschutz - BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz (bund.de)

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

IT-Grundschutz Compendium, BSI 2019 BSI - IT-Grundschutz - BSI IT-Grundschutz-Compendium Edition 2019 (bund.de)
Olejár D., Krátky úvod do kybernetickej a informačnej bezpečnosti KB-K1_2_3-Uvod-do-KIB_slovnik_ver1.0.pdf (gov.sk)

Kľúčové slová: kybernetrická a informačná bezpečnosť, ISVS, bezpečnostný projekt, analýza rizík, správa rizík

Vedúci: doc. RNDr. Daniel Olejár, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 31.10.2023

Dátum schválenia: 03.11.2023

doc. RNDr. Dana Pardubská, CSc.
garant študijného programu

.....
študent

.....
vedúci práce

Poďakovanie: Ďakujem vedúcemu bakalárskej práce **doc. RNDr. Danielovi Olejárovi, PhD.** za jeho cenné vedomosti, trpezlivosť, rady, pripomienky a študijné materiály.

Abstrakt

Informatizácia spoločnosti výrazne pokročila, drvivá väčšina informácií je zaznamenávaná a spracovávaná v digitálnej forme a digitálne IKT sa stali prvkami kritickej infraštruktúry. Povinnosť chrániť informačné systémy v kybernetickom priestore je ukotvená aj v právnych normách Slovenska. Zákonné povinnosti sa týkajú mnohých vlastníkov, prevádzkovateľov a správcov informačných systémov, na Slovensku však nemáme dostatok odborníkov na kybernetickú a informačnú bezpečnosť. V tejto práci analyzujeme legislatívne požiadavky na ochranu ISVS, identifikujeme povinnosti prevádzkovateľa ISVS najnižšej kategórie, navrhneme postup, ako splniť zákonné povinnosti a navhrneme a čiastočne implementujeme pomocný systém pre manažéra kybernetickej a informačnej bezpečnosti.

Kľúčové slová: kybernetická a informačná bezpečnosť, zákon o kybernetickej bezpečnosti, zákon o informačných technológiách vo verejnej správe, ITVS, ISVS, ISMS

Abstract

The informatization of the public has significantly progressed, most of the information is digitaly recorded and processed, and digital ICT have become elements of critical infrastructure. The obligation to protect information systems in cyberspace is anchored in legal norms of Slovakia. Legal obligations concern many owners, operators, and administrators of information systems, however there is a shortage of specialist in the field of cyber and information security in Slovakia. In the bachelor's thesis we will analyze legislative requirements for ISVS protection, identify the obligations of ISVS operator in the lowest category, we will propose a procedure for fulfillment of legal obligations, and we will design and partially implement auxiliary system for the manager responsible for cyber and information security.

Keywords: cyber and information security, cybersecurity act, information security in public administration act, ITVS, ISVS, ISMS

Obsah

Úvod **1**

1 Základné pojmy **3**

2 Analýza právnych požiadaviek na bezpečnosť ISVS **5**

2.1 Zákon č. 69/2018 Z. z. 5

2.1.1 Pôsobnosť zákona vo vzťahu k mestám a obciam, prípadne ďalším organizáciám 6

2.1.2 Povinnosti prevádzkovateľa základnej služby 7

2.1.3 Tretie strany 8

2.1.4 Porušenie povinností 9

2.1.5 Lex specialis 9

2.2 Zákon č. 95/2019 Z. z. 9

2.2.1 Terminológia 10

2.2.2 Organizácia KIB 10

2.2.3 Riadenie 11

2.2.4 Bezpečnosť 11

2.2.5 Tretie strany 12

2.2.6 Prevádzka 13

2.2.7 Bezpečnostný projekt 13

2.2.8 Bezpečnostné incidenty 13

2.2.9 Ďalšie povinnosti 14

2.2.10 Prenesenie povinnosti 14

2.2.11 Porušenie povinností 15

2.3 Iné zákony 15

3 Zavádzanie ISMS **17**

3.1 Prevzatie celkovej zodpovednosti vedením organizácie za KIB 18

3.2 Určenie cieľov KIB a stratégie KIB 20

3.3 Načrtnutie politiky KIB 21

3.4 Vymenovanie manažéra KIB 22

3.5 Vytvorenie vhodnej organizačnej štruktúry KIB 23
3.6 Definícia bezpečnostných opatrení 25
3.7 Zapojenie zamestnancov do bezpečnostného procesu 25
3.8 Integrovanie KIB do procedúr a procesov celej organizácie 26

4 Systém **29**
4.1 Technická špecifikácia 29
4.2 Prezentácia výsledného systému 31
4.3 Databázový pohľad 38
4.4 Ako spustiť systém 39

5 Po bitke sú všetci... **41**
5.1 Čo nebolo a mohlo byť, čo bolo a mohlo byť lepšie 42
5.2 Zhrnutie 45

Záver **47**

Zoznam obrázkov

4.1 Úvodná stránka. 31
4.2 Stránka s návodom. 32
4.3 Odkaz na metodiku BSI. 33
4.4 Identifikovanie štruktúry organizácie, ukážka s vyplneným textom. . . . 34
4.5 Výňatok zo sekcie určenia úrovne KIB. 35
4.6 Formulár s výberom relevantných hrozieb. 36
4.7 Matica klasifikácie rizika. 36
4.8 Databázová schéma. 39

Zoznam skratiek

BSI Bundesamt für Sicherheit in der Informationstechnik.

d-IKT digitálne informačné a komunikačné technológie.

ENISA European Network and Information Security Agency.

HTML hypertext markup language.

HTTP hypertext transfer protocol.

ISMS information security management system.

ISVS informačný systém verejnej správy.

ITVS informačné technológie verejnej správy.

JVM Java virtual machine.

KIB kybernetická a informačná bezpečnosť.

MIRRI Ministerstvo investícií, regionálneho rozvoja a informatizácie.

NBÚ Národný bezpečnostný úrad.

NIS Network and information systems.

ORM object-relation mapping.

RPC remote-procedure call.

SQL structured query language.

SR Slovenská republika.

SSR server-side rendering.

URL uniform resource location.

ZoITVS Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

ZoKB Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Úvod

Posledných niekoľko desaťročí prebieha informatizácia spoločnosti, v súčasnosti je vo veľmi pokročilom stave a drvivé množstvo informácií (takmer 100%) je zaznamenávaných a spracovávaných v digitálnej forme. Potenciál digitálnych informačných a komunikačných technológií(d-IKT) si uvedomuje aj Európska únia(EÚ). Rozvoj znalostnej spoločnosti s trvalo udržateľným rozvojom sú hlavnými prioritami EÚ, ktoré sú rozpracované vo viacerých strategických dokumentoch, pre informatizáciu spoločnosti sú najdôležitejšie „Digital Single Market Strategy“[1] a „Digital Agenda for Europe“[2].

EÚ si je vedomá, že d-IKT sa stali prvkami kritickej infraštruktúry spoločnosti, je potrebné ich chrániť a preto prijala „European Cybersecurity Strategy“[3], „Network and Information Security Directive (NIS Directive)“[4] a „EU Cybersecurity Act:“[5].

Ani Slovensko nezaostalo a tiež sa snaží o informatizáciu spoločnosti cez dokumenty ako „Stratégia digitálnej transformácie Slovenska 2030“ a „Akčných plánov digitálnej transformácie Slovenska“, pre oblasť kybernetickej a informačnej bezpečnosti to sú „Národný program pre ochranu a obranu kritickej infraštruktúry“ a „Národná stratégia a akčný plán kybernetickej bezpečnosti“.

Nariadenia EÚ spolu s národnými stratégiami, koncepciami a akčnými plánmi sa premietli do viacerých zákonov Slovenskej republiky(SR). Tieto zákony podrobnejšie definujú pravidlá a upravujú povinnosti subjektov v kybernetickom priestore Slovenska a EÚ, sú to napr. 45/2011 Z. z.(zákon o kritickej infraštruktúre), 272/2016 Z. z.(zákon o elektronickom podpise) alebo 18/2018 Z. z.(zákon o ochrane osobných údajov).

Najdôležitejšie zákony a vykonávacie predpisy SR stanovujúce povinnosti subjektov v kybernetickom priestore sú:

- 69/2018 Z. z., zákon o kybernetickej bezpečnosti,
- 362/2018 Z. z., vyhláška Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,

[1] Stratégia cielená na voľný pohyb digitálneho tovaru a odstraňovania prekážok v rámci Európy.

[2] Agenda politík určených na maximalizovanie prínosu digitálnych technológií.

[3] Stratégia cielená na budovanie odolnosti voči kybernetickým hrozbám.

[4] Smernica o bezpečnostných opatreniach pre zabezpečenie vysokej úrovene informačnej bezpečnosti.

[5] Zákon na posilnenie agentúry ENISA a vytvorenie certifikačného rámca pre digitálne produkty.

- 95/2019 Z. z., zákon o informačných technológiách vo verejnej správe a
- 179/2020 Z. z., vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Vyššie uvedené právne normy určujú povinnosti v kybernetickom priestore veľkému počtu vlastníkov, prevádzkovateľov a správcov informačných systémov. Národný bezpečnostný úrad (podľa kompetenčného zákona 69/2018 Z.z. [7, §5, ods. 1]) zodpovedá za kybernetickú bezpečnosť a nedávno zaradil do registra prevádzkovateľov základných služieb mestá, obce, mestské časti a niektoré služby a organizácie spadajúce pod mestá. To znamená, že okrem informačných systémov verejnej správy(ISVS) ústredných štátnych orgánov sa prvkami kritickej infraštruktúry (podľa 69/2018 Z.z) stali aj ISVS malých miest, obcí a organizácií, ktoré spadajú do najnižšej kategórie I (podľa 69/2018 Z.z a podľa 95/2019 Z.z.).

Tu sa dostávame k veľkému problému pre SR, ktorý vyplýva z tohto zákona. Jednou z minimálnych požiadaviek 69/2018 Z.z [7, §20, ods. 4, písm a)] je ustanovenie manažéra kybernetickej bezpečnosti. To znamená, že všetky subjekty zaradené do zoznamu prevádzkovateľov základnej služby potrebujú odborne kvalifikovaného zamestnanca zodpovedného za ochranu informačných systémov a dodržiavania legislatívnych povinností. Vyjadrené číselne, ide zhruba o 20 000 ľudí, ktorých SR nemá k dispozícii a v blízkej budúcnosti ani nebude mať[6]. Tým sme sa dostali k cieľom bakalárskej práce:

- analyzovať legislatívne požiadavky na ochranu ISVS,
- identifikovať povinnosti prevádzkovateľa ISVS kategórie I,
- navrhnúť postup, ako splniť tieto povinnosti a
- vytvoriť pomocný systém pre manažéra KIB, ktorý mu pomôže si splniť legislatívne povinnosti.

V nasledujúcich kapitolách sa pokúsime tieto ciele splniť a na konci zhodnotíme, do akej miery sa nám aj naozaj podarilo ich splniť. Najprv začneme s terminológiou, aby sme začali a následne budovali na pevnom základe.

[6]Pre tak veľké množstvo odborníkov nestačia kapacity vzdelávacích inštitúcií, FMFI UK pripraví ročne menej ako 10 absolventov.

Kapitola 1

Základné pojmy

Kybernetická a informačná bezpečnosť (KIB) je multidisciplinárna oblasť ľudskej činnosti, zaoberajúca sa skúmaním hrozieb voči informáciám, informačným systémom a sieťam a návrhom riešení, ktoré by naplneniu hrozieb zamedzili, alebo aspoň zmiernili ich dopad. KIB je relatívne nová a dynamicky sa rozvíjajúca oblasť, v ktorej sa terminológia ešte neustálila[1], slovenská terminológia sa zväčša prekladá alebo preberá termíny z anglického jazyka. V tejto kapitole definujeme len základné pojmy a úlohy, ktoré rieši KIB. Budeme vychádzať zo slovníka a krátkeho úvodu do problematiky KIB[3]. Ak je čitateľ znalý v problematike KIB môže túto časť preskočiť a pokojne prejsť k ďalšej kapitole.

- **aktívum**, angl. *asset*, je čokoľvek, čo má pre organizáciu hodnotu, môžu byť cieľom útoku a má zmysel (resp. je potrebné) chrániť pred potenciálnymi hrozbami. Aktíva sú hmotné (zariadenia, infraštruktúra, personál) a nehmotné (peniaze, informácie, vedomosti).
- **primárne aktíva** sú aktivity zamerané na plnenie poslania organizácie.
- **sekundárne aktíva** sú prostriedky, ktoré umožňujú alebo podporujú činnosť primárnych aktív.
- **hrozba**, angl. *threat*, je objektívne existujúca potenciálna možnosť priamo alebo nepriamo narušiť (alebo negatívne ovplyvniť) systém, spracovávané informácie, alebo iné aktíva organizácie.
- **dopad hrozby**, angl. *threat impact*, negatívne dôsledky naplnenia hrozby na aktívach organizácie.
- **dôvernosť**, angl. *confidentiality*, je bezpečnostná požiadavka, ktorej naplnenie znamená, že informáciu obsiahnutú v správe sa nedozvedia nepovolené osoby.
- **integrita**, angl. *integrity*, je bezpečnostná požiadavka, ktorej naplnenie znamená, že údaje nie je možne zmeniť bez toho, aby to ich vlastník alebo adresát nevedel

[1] ENISA publikovala štúdiu, v ktorej porovnávala rozlične výklady pojmu kybernetická bezpečnosť naprieč šiestimi rôznymi inštitúciami.

zistiť.

- **dostupnosť**, angl. *availability*, je bezpečnostná požiadavka, ktorej naplnenie znamená, že zdroje systému sú k dispozícií oprávnenej - osobe v momente, keď o to požiada; alebo od istého okamihu; alebo v istom časovom rámci (napr. dni v týždni, časový interval počas dňa).
- **riziko**, angl. *risk*, je veličina závislá od závažnosti (možného dopadu) hrozby a pravdepodobnosti, že sa hrozba naplní.
- **hodnota rizika** je stredná hodnota dopadu rizika na aktívum,
- **analýza rizík**, angl. *risk analysis*, proces identifikácie rizík, ohodnotenia rizík a stanovenia úrovne rizík.
- **incident**, angl. *incident*, je udalosť alebo situácia, ktorá spôsobí alebo môže spôsobiť nežiadúce prerušenie činnosti, stratu, núdzový stav. zranenie, usmrtenie alebo krízu v organizácií alebo systéme.
- **kybernetická a informačná bezpečnosť** je multidisciplinárna oblasť, ktorá skúma hrozby voči aktívam a hľadá opatrenia, ktoré majú eliminovať riziká vyplývajúce z hrozieb voči aktívam. Táto disciplína skúma metódy dlhodobej, nákladovo a funkčne efektívnej ochrany aktív organizácie.
- **systém riadenia informačnej bezpečnosti**, angl. *information security management system (ISMS)*, je súbor nástrojov, metód a postupov pre zaistenie systematického riešenia informačnej bezpečnosti v organizácií. Cieľom tohto systému je zaručiť dôvernosť, integritu a dostupnosť informácie, procesov a systémov informačných technológií. Podrobnejšie sa ním budeme zaoberať v kapitole 3 o zavádzaní ISMS.

Ďalšie pojmy KIB, s ktorými sa stretneme, priebežne vysvetlíme. Čitateľovi, ktorý by mal záujem o terminológiu KIB, odporúčame preštudovať si slovník[3].

Kapitola 2

Analýza právnych požiadaviek na bezpečnosť ISVS

Je v prirodzenom záujme každého vlastníka informačného systému, aby jeho údaje systému boli chránené a jeho systém bezpečne fungoval, preto by mal vlastník informačného systému zaistiť primeranú úroveň KIB vo svojej organizácií. Vlastníkom, prevádzkovateľom a správcom ISVS túto povinnosť stanovuje legislatíva. V tejto kapitole analyzujeme najdôležitejšie zákony a vykonávacie predpisy, ktoré stanovujú bezpečnostné požiadavky na ISVS.

Obsah zákonov citujeme v plnom rozsahu, aj s odkazmi, ktoré v prípade potreby ďalej rozvinieme. Vykonávacie predpisy 62/2018 Z.z.[6] a 362/2018 Z.z.[5] rozoberáme samostatne a ich analýzu uvádzame v prílohe.

2.1 Zákon č. 69/2018 Z. z.

Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Základným zákonom (*lex generalis*), ktorý definuje riešenie kybernetickej (a informačnej) bezpečnosti v SR, je Zákon č. 69/2018 Z. z. (ZoKB). Bol prijatý v roku 2018 a prešiel niekoľkými novelizáciami *373/2018 Z. z.*, *134/2020 Z. z.*, *287/2021 Z. z.*, *55/2022 Z. z.* a *231/2022 Z. z.* Implementuje európsku smernicu NIS, a preto explicitne hovorí o bezpečnosti informačných systémov a sieti vo všeobecnosti, v porovnaní so ZoITVS, ktorý hovorí o bezpečnosti informácie v informačných technológiách verejnej správy.

2.1.1 Pôsobnosť zákona vo vzťahu k mestám a obciam, prípadne ďalším organizáciám

V ZoKB sú explicitne vymenované povinnosti Národného bezpečnostného úradu(NBÚ)[1] a ďalších štátnych inštitúcií (ďalej orgány verejnej moci). Podobne sú explicitne vymenované povinnosti poskytovateľov digitálnych služieb a prevádzkovateľov základných služieb. Základnú službu a prevádzkovateľa ZoKB rozumie [7, §3 písm. l) a m)]:

> *l) základnou službou služba, ktorá je zaradená v zozname základných služieb a*
>
> *1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1, alebo*
>
> *2. je prvkom kritickej infraštruktúry, [9)]*
>
> *m) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena l),*

V prílohe č. 1 zákon definuje sektory (a k ním príslušné podsektory) ako bankovníctvo, doprava, energetika a ďalšie. Jedným zo sektorov prílohy č.1 je aj sektor verejná správa, s podsektorom ISVS. Ústredným orgánom zodpovedným za verejnú správu je Úrad podpredsedu vlády pre investície a informatizáciu, v súčastnosti MIRRI. Správa ISVS je považovaná za prevádzku základnej služby. Prevádzkovateľmi základnej služby sú orgány verejnej moci, mesta, obce a ďalšie organizácie.

Zoznam prevádzkovateľov základných služieb je udržiavaný a spravovaný NBÚ a spôsob zaradenia do zoznamu je obsiahnutý ZoKB v §3, ods (1) písm. k):

> *k) na základe oznámenia ústredného orgánu, prevádzkovateľa základnej služby, poskytovateľa digitálnej služby alebo z vlastnej iniciatívy určuje*
>
> *1. základnú službu a zaraďuje ju do zoznamu základných služieb,*
>
> *2. digitálnu službu a zaraďuje ju do zoznamu digitálnych služieb,*
>
> *3. poskytovateľa digitálnej služby a zaraďuje ho do registra poskytovateľov digitálnych služieb,*
>
> *4. prevádzkovateľa základnej služby a zaraďuje ho do registra prevádzkovateľov základných služieb*

Pochybnosti, či je organizácia prevádzkovateľom základnej služby, vyriešilo NBÚ vlastnou iniciatívou, keď zaradilo veľkú časť miest a obcí na zoznam prevádzkovateľov základných služieb.

Pochybnosti, či sú mestá, obce, mestské časti a nimi spravované organizácie prevádzkovateľmi základných služieb vyriešilo NBÚ, tak že ich (podľa [7, §5, ods. (1) písm. k)] zaradilo do zoznamu.

[1] ZoKB nazýva NBÚ „Úrad“.

2.1.2 Povinnosti prevádzkovateľa základnej služby

Povinnosti prevádzkovateľa základnej služby sú špecifikované v [7, §19, ods. (1)]:

> *Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.*

Všeobecné bezpečnostné opatrenia určuje ZoKB a jeho vykonávacie predpisy, sektorové bezpečnostné opatrenia určuje ZoITVS a jeho vykonávacie predpisy. Úroveň bezpečnostných opatrení musí zohľadňovať klasifikáciu a kategorizáciu systémov[2]. Prijatie bezpečnostných opatrení závisí od výsledkov analýzy rizík[3].

ZoKB rámcovo stanovuje všeobecné bezpečnostné opatrenia, ktoré sú záväzné pre všetky informačné systémy a siete[4]. Tieto bezpečnostné opatrenia majú pokrývať všetky oblasti KIB. ZoKB explicitne vymenúva tieto oblasti a minimálne bezpečnostné opatrenia v [7, §20]:

> *(3) Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť*
> *a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,*
> *b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,*
> *c) personálnej bezpečnosti,*
> *d) riadenia prístupov,*
> *e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,*
> *f) bezpečnosti pri prevádzke informačných systémov a sietí,*
> *g) hodnotenia zraniteľností a bezpečnostných aktualizácií,*
> *h) ochrany proti škodlivému kódu,*
> *i) sieťovej a komunikačnej bezpečnosti,*
> *j) akvizície, vývoja a údržby informačných sietí a informačných systémov,*
> *k) zaznamenávania udalostí a monitorovania,*
> *l) fyzickej bezpečnosti a bezpečnosti prostredia,*
> *m) riešenia kybernetických bezpečnostných incidentov,*
> *n) kryptografických opatrení,*
> *o) kontinuity prevádzky,*
> *p) auditu, riadenia súladu a kontrolných činností.*
> *(4) Bezpečnostné opatrenia musia zahŕňať najmenej*

[2]Úroveň vyplýva zo závažností rizík vyplývajúcich z hrozieb voči systémom a aktívam organizácie.
[3]ZoKB implicitne predpokladá o už vykonanej analýze rizík.
[4]V pôsobnosti ZoKB.

a) určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,

b) detekciu kybernetických bezpečnostných incidentov,

c) evidenciu kybernetických bezpečnostných incidentov,

d) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,

e) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,

f) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.

Podrobná špecifikácia bezpečnostných opatrení, kategórií sieti a informačných systémov prevádzkovateľa základnej služby je uvedená vo vyhláške NBÚ č. 362/2018 Z.z.

Povinnosť riešiť bezpečnostné incidenty prevádzkovateľom základnej služby ukladá ZoKB v §24. Prevádzkovateľ základnej služby je povinný nahlasovať NBÚ závažné bezpečnostné incidenty. Ďalšie povinnosti prevádzkovateľa základnej služby sú stanovené v §27, kde sa píše, že NBÚ vydáva výstrahy a varovania pred hrozbami a ukladá prevádzkovateľom základnej služby riešiť incident alebo vykonať reaktívne (preemptívne) opatrenia. Zo ZoKB vyplýva, že prevádzkovateľ by mal mať definovaný postup riešenia bezpečnostných incidentov, vrátane nahlasovania, vyhodnocovania a prijímania adekvátnych bezpečnostných opatrení.

ZoKB síce v §24 stanovuje povinnosť prevádzkovateľovi základnej služby do dvoch rokoch po zaradení do zoznamu sa podrobiť auditu. Avšak, pre kategóriu I. vyhláška NBÚ č. 362/2018 Z.z (doplnená a novelizovaná vyhláškou NBÚ č. 264/2023 Z.z.) túto povinnosť neustanovuje[5].

2.1.3 Tretie strany

Máloktorý správca ISVS zabezpečuje prevádzku vlastnými silami. Niektoré služby ponúkajú štátne orgány, ale množstvo činností(aj tie, ktoré majú dopad na KIB) sú zabezpečované tretími stranami(outsourcing). Zodpovednosť za ISVS zostáva na strane správcu ISVS, ktorý nemá právny dosah na externých spolupracovníkov. ZoKB označuje externých spolupracovníkov a dodávateľov tretie strany a upravuje ich povinnosti voči prevádzkovateľov právnou cestou [7, §19]:

(2) Prevádzkovateľ základnej služby je povinný pri výkone činnosti, ktorá

[5]Je iba odporúčaním.

> *priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby výkonu tejto činnosti; pri uzatvorení zmluvy sa vykonáva analýza rizík.*

Podľa nasledujúceho odseku (3) nie je potreba uzavrieť takúto zmluvu, ak je tretia strana prevádzkovateľom základnej alebo digitálnej služby, alebo ak je riziko pri vykonávaní činnosti voči tretej strane nízke. Ak nie je možné uzavrieť zmluvu podľa odseku (2), tak je prevádzkovateľ základnej služby povinný informovať tretiu stranu v nevyhnutnom rozsahu o bezpečnostnom incidente.

2.1.4 Porušenie povinností

Za nesplnenie alebo porušenie povinností prevádzkovateľa základnej služby bude prevádzkovateľ finačne sankcionovaný, §29, za priestupok (od 100 eur do 5000 eur) alebo za správny delikt (od 300 eur až do výšky 30 000 eur).

2.1.5 Lex specialis

Nakoniec, podľa ZoKB môže ústredný orgán definovať špecifické bezpečnostné opatrenia a vyžadovať ich zavedenie v sektore/podsektore, za ktorý zodpovedá. Za sektor verejnej správy, podsektor informačných systémov verejnej správy zodpovedá Ministerstvo investícií, regionálneho rozvoja a informatizácie (MIRRI)[6].

2.2 Zákon č. 95/2019 Z. z.

Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

Správa informačných technológií vo verejnej správe (ITVS) je upravená Zákonom č. 95/2019 (ZoITVS). Tento zákon obsahuje aj pomerne podrobne špecifikované povinnosti správcov informačných systémov verejnej správy (ISVS) v kybernetickej a informačnej bezpečnosti[7] a je v oblasti KIB konkrétnym zákonom (*lex specialis*) pre sektor verejnej správy. ZoITVS a ZoKB sú explicitne zviazané a vzájomne sa na seba odvolávajú. KIB je explicitne koncentrovaná v §18 až §24, ale je prítomná aj v ďalších paragrafoch upravujúcich zodpovednosti a vzťahy zainteresovaných subjektov.

[6] V samotnej prílohe č. 1 ZoKB je uvedený Úrad podpredsedu vlády pre investície a informatizáciu, MIRRI je jeho nástupníckym orgánom.

[7] Oproti ZoKB je v ZoITVS explicitne použité slovo informačná.

2.2.1 Terminológia

Na začiatok uvedieme definíciu pojmov informačná technológia a informačný systém z [8, §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.*

Správcom podľa[8, §2, ods. (5)] je orgán riadenia, ktorý používa ITVS na účely poskytovania služby verejnej správy. Prevádzkovateľom podľa[8, §2, ods. (6)] je správca, orgán riadenia alebo správcom určená osoba. Služba verejnej správy je základnou službou podľa [8, §3]:

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

2.2.2 Organizácia KIB

Subjektom zodpovedným v podsektore ISVS sú podľa ZoITVS orgán vedenia(MIRRI) a orgány riadenia. Správu ITVS tiež vykonáva orgán riadenia, ktorým je[8] podľa [8, §5, ods. (2)]:

> *c) obec a vyšší územný celok,*
>
> *e) právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia uvedeného v písmenách a) až d),*
>
> *h) záujmové združenie právnických osôb DataCentrum elektronizácie územnej samosprávy Slovenska, ktorého jedinými členmi sú Ministerstvo financií Slovenskej republiky a Združenie miest a obcí Slovenska.*

[8]Písmená a), b) a d) sú konkrétne vládne inštitúcie, úrady, kancelárie a pod., vynechali sme ich, lebo vymenúvajú desiatky subjektov spravujúcich ISVS, ktoré nie sú malými ISVS.

2.2.3 Riadenie

ZoITVS rozumie pod orgánom riadenia tú organizáciu, ktorá je vlastníkom ISVS a buď si ho sama prevádzkuje alebo čiastočne alebo úplne zabezpečuje jeho prevádzku prostredníctvom tretích strán. Úlohou orgánu rieadenia je trvalo zabezpečiť a zlepšovať elektronický výkon pôsobnosti orgánu riadenia a rozvíjať informačné technológie[9]. Orgán riadenia plní povinnosti (tohto zákona) vyplývajúce z klasifikácie informácií a kategorizácie systémov, ktorých je správcom. Klasifikácia informácií a kategorizácia informačných systémov je prebratá zo ZoKB.

Podľa ZoITVS má orgán riadenia vypracovať viacero vnútorných predpisov pre rozličné oblasti KIB. Pre malé ISVS so štandardnými systémami je vhodné postupovať podľa ustanovenia ZoITVS[8, §11, ods. (5)] – vychádzať z medzinárodne akceptovaných štandardov vychádzajúcich z uznaných technických noriem (je to nepriamy odkaz na to, že môžeme vychádzať zo série štandardov ISO/IEC 27000). Ak je vyžadované vydať viac vnútorných predpisov, je orgán riadenia povinný vydať aspoň jeden vnútorný predpis pokrývajúci všetky potrebné predpisy. Podľa [8, §12 až §16] je vlastník ISVS povinný:

- zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku ITVS,
- zabezpečiť systém proti zneužitiu v súlade s týmto zákonom a všeobecne záväznými právnymi predpismi,
- zabezpečiť riadenie bezpečnosti,
- identifikovať a udržiavať zoznam svojich aktív,
- identifikovať kritické aktíva ovplyvňujúce dostupnosť systému,
- zabezpečiť pravidlá prevádzky, servisu a riešenia bezpečnostných incidentov
- zabezpečiť riadenie kontinuity prevádzky a
- zabezpečiť riadenie bezpečnosti prevádzky.

2.2.4 Bezpečnosť

V ZoITVS §18 je explicitne opísaný vzťah ZoITVS a ZoKB. Správca je prevádzkovateľom základnej služby a prijíma bezpečnostné opatrenia v súlade so ZoKB. ZoKB je odkazovaný ako *lex generalis* a ZoITVS je k nemu vymedzený ako *lex specialis*.

V oblasti plánovania a organizácie[8, §19 ods. (1)] je správca povinný:

- zaviesť systém riadenia informačnej bezpečnosti (ISMS),
- napísať bezpečnostnú politiku,
- zriadiť riadiacu, výkonnú a kontrolnú zložku systému riadenia bezpečnosti,
- vypracovať bezpečnostný projekt[10],
- identifikovať potrebné bezpečnostné opatrenia,

[9] Ktorých správcom je orgán riadenia.

[10] Vykonať analýzu rizík a zabezpečiť správu rizík.

- určiť potrebné bezpečnostné mechanizmy a opatrenia a
- určiť postup riešenia bezpečnostných incidentov.

Riadiaca zložka iniciuje bezpečnostný proces a zavedie ISMS, prerokováva a schvaľuje navrhované bezpečnostné opatrenia, dostáva hlásenia o bezpečnostných incidentoch, výsledkoch auditu, výročnú správu o stave KIB v organizácií a plán činnosti v KIB.

Výkonná zložka plánuje, koordinuje a vyhodnocuje bezpečnostný proces, vypracováva a aktualizuje dokumenty ISMS, vyhodnocuje stav a vypracováva hlásenia o KIB, realizuje bezpečnostné opatrenia, rieši bezpečnostné incidenty a organizuje vzdelávanie o KIB v organizácií.

Kontrolná zložka nezávislé[11] kontroluje dodržiavanie povinnosti plynúcich z KIB a v súlade s legislatívnymi požiadavkami hodnotí stav KIB v organizácii.

Správca pri plánovaní vytvorenia alebo nadobudnutia ISVS kategorizuje tento systém v závislosti od spracovávanej informácie, vypracuje bezpečnostný profil[12] a určí osobu zodpovednú za jeho bezpečnosť.

V prípade malého ISVS, riadiacu zložku môže predstavovať starosta/starostka, výkonnú zložku jeden informatik a kontrolnú zložku buď ten istý informatik, alebo externý spolupracovník.

2.2.5 Tretie strany

Podobne ako ZoKB, aj ZoITVS rozoznáva externých spolupracovníkov a dodávateľov. V [8, §20] ZoITVS sú rozobraté požiadavky voči tretím stranám. Správca určuje bezpečnostné požiadavky ISVS, poskytuje dodávateľovi ISVS[8, §20 ods. (1) písm b)] „pseudonymizované kópie údajov alebo fiktívne údaje na testovanie ISVS a jeho vývoj“ a zabezpečí vypracovanie bezpečnostného projektu.

Na druhej strane dodávateľ ISVS zabezpečí dokumentáciu vývoja, používateľskú a administrátorskú príručku. Tiež je dodávateľ povinný preukázať dodržiavanie bezpečnostných požiadaviek určených správcom, doplniť chýbajúce bezpečnostné požiadavky, upozorniť správcu na kritické časti ISVS, navrhnúť opatrenia na ich riešenie a preukázateľne odstrániť „zadné vrátka“.

[11] V prípade malej organizácie, ktorá nemá finančné prostriedky pre externých auditorov, túto činnosť musí často vykonávať presne tá osoba, ktorá je zodpovedná za vypracovanie bezpečnostných opatrení.

[12] Sformuluje bezpečnostné požiadavky na systém, t.j. definuje potenciálne hrozby, riziká, náklady, vykoná analýzu rizík, sformuluje bezpečnostné ciele a pod.

2.2.6 Prevádzka

Správca zabezpečuje životný cyklus ISVS: jeho zavedenie do prevádzky, samotnú prevádzku a vyradenie z prevádzky, pričom pred zavedením do prevádzky, [8, §21 ods. (2)]:

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

Systém zavedený v prevádzke[8, §22] prijíma bezpečnostné opatrenia ZoKB v oblasti „k) zaznamenávania udalostí a monitorovania,“.

2.2.7 Bezpečnostný projekt

Správca je povinný vypracovať bezpečnostný projekt pre celú organizáciu alebo pre viacero informačných systémov v jeho správe. Bezpečnostný projekt vychádza [8, §23 ods. (1)][13]:

> *a) z bezpečnostnej politiky,*
> *b) zo všeobecne akceptovaných štandardov riadenia informačných technológií, ktoré vychádzajú z uznaných technických noriem,*
> *c) z metodických usmernení orgánu vedenia.*

Úroveň bezpečnostného projektu je vždy najvyššia spomedzi všetkých klasifikovaných systémov v pôsobnosti správcu.

2.2.8 Bezpečnostné incidenty

Začneme citáciou[14], ktorú budeme komentovať. Organ riadenia je povinný[8, §23 ods. (3)]:

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

[13] Znovu je to odkaz na to, že môžme postupovať podľa série štandardov ISO/IEC 27000.
[14] Písmená b) a d), sú vynechané, keďže podľa odseku (4) sa na malé ITVS nevzťahujú.

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).

Komentár k a)

Ak je správca zaradený do zoznamu prevádzkovateľov základnej služby, incidenty nahlasuje podľa ZoKB NBÚ, ináč hlási incidenty MIRRI. Podľa ZoKB, hlásenie incidentov sa vykonáva pomocou jednotného informačného systému[15] a hlási sa každá hrozba, ktorá negatívne vplýva na KIB, nie len závažné bezpečnostné incidenty presahujúce kritéria kategorizovaných incidentov[16].

Komentár k c)

Z odseku 5, orgán vedenia vykonáva pravidelné neinvazívne hodnotenie zraniteľností ITVS. Orgán riadenia môže požiadať MIRRI o riešenie bezpečnostného incidentu, vykonanie bezpečnostného auditu alebo vykonať hodnotenie zraniteľnosti[17]. MIRRI pri takejto žiadosti zbiera, spracúva a vyhodnocuje systémové informácie pre účely KIB.

Komentár k e) a f)

Povinnosti sú priamočiare.

2.2.9 Ďalšie povinnosti

Orgán riadenia má informačnú povinnosti voči MIRRI a to poskytovať[8, §8 odsek (2)] „údaje o informačných technológiách verejnej správy na účely štatistických analýz“ Ak dôjde k zmene podmienok (napr. novelizácia), v ktorých ITVS existujú, má orgán riadenia povinnosť šesť mesiacov, aby sa prispôsobil novým podmienkam.

2.2.10 Prenesenie povinnosti

Podľa[8, §28, odsekov (1) a (2)] za orgán riadenia môže plniť povinnosti ten orgán riadenia, ktorý voči nemu vykonáva zriaďovateľskú alebo zakladateľskú pôsobnosť. Inými slovami, mestá a obce môžu plniť povinnosti za organizácie, ktoré zriaďujú.

[15]Formulár je na stránke NBÚ: https://www.sk-cert.sk/sk/rady-a-navody/nahlasit-incident/index.html

[16]Poznámka autora, možno z tohto dôvodu sú počty bezpečnostných incidentov také početné vo výročných správach NBÚ.

[17]V zákone nie je zmienka o tom, kto bude financovať takúto žiadosť.

2.2.11 Porušenie povinností

Orgán vedenia[8, §29] uloží pokutu správcovi od 500 do 35 000 eur, ak poruší povinnosti bezpečnosti ITVS stanovené týmto zákonom.

2.3 Iné zákony

Okrem ZoKB a ZoITVS existuje v právnom poriadku SR viacero zákonov, ktoré obsahujú požiadavky na ochranu informácie a d-IKT, napríklad:

- Zákon o slobodnom prístupe k informáciám 211/2000 Z. z.,
- Zákon o ochrane utajovaných skutočností 215/2004 Z. z.,
- Zákon o kritickej infraštruktúre 45/2011 Z. z.,
- Zákon o ochrane osobných údajov 18/2018 Z. z.,
- Zákon o elektronických komunikáciách 452/2021 Z. z.

Požiadavky vyplývajúce z týchto zákonov možno zohľadniť pri plnení povinností vyplývajúcich zo zákonov ZoKB a ZoITVS, preto sa nimi nebudeme explicitne zaoberať.

Kapitola 3

Zavádzanie ISMS

Systém riadenia (angl. *management system*) je súbor politík, procedúr, zdrojov a schopností, ktoré sa zameriavajú na efektívne vykonávanie riadiacích úloh v danej doméne za účelom splniť ciele organizácie[1]. System riadenia zaoberajúci sa informačnou bezpečnosťou nazývame systém riadenia informačnej bezpečnosti (angl. *information security management system*, ISMS).

ISMS špecifikuje nástroje a metódy, pomocou ktorých manažment dokáže jasne riadiť úlohy a aktivity slúžiace na dosiahnutie informačnej bezpečnosti[9]. Cieľom ISMS je zaručiť dôvernosť, integritu a dostupnosť informácie, procesov a IT systémov. ISMS pozostáva z[1]:

- princípov riadenia informačnej bezpečnosti,
- zdrojov slúžiacich na zriadenie a udržiavanie informačnej bezpečnosti
- ľudí, ktorí priamo pracujú s informáciami, systémami a technológiami slúžiacimi na spracovanie alebo plnia špeciálne úlohy v rámci informačnej bezpečnosti a
- bezpečnostného procesu.

Zavedenie, udržiavanie a rozvoj informačnej bezpečnosti v organizácii nazývame bezpečnostný proces. Je to kontinuálny proces, ktorý prebieha počas celého životného cyklu organizácie a vďaka ktorému možno priebežne monitorovať výkon a efektivitu stratégií, konceptov a opatrení. Súčasťou bezpečnostného proces sú bezpečnostná stratégia, bezpečnostná politika, bezpečnostné ciele, bezpečnostný koncept a bezpečnostná organizácia.

Bezpečnostná stratégia slúži na orientáciu pri plánovaní ďalších krokov pre dosiahnutie stanovených bezpečnostných cieľov, ktoré sú určené vedením organizácie a sú špecifické pre každú organizáciu. Bezpečnostné ciele sú odvodené od cieľov/poslaní organizácie, povinností, podmienok, spôsobu využivania d-IKT a spôsoboch spracovávania informácia. Bezpečnostná stratégia je samostatný dokument alebo súčasť (hlavička)

[1]Štruktúra ISMS a jeho jednotlivých častí je detailne popísaná v štandardoch 27001, 27002 a BSI 200-1.

bezpečnostnej politiky.

Bezpečnostná politika vo všeobecnosti popisuje, ako má byť zavedená informačná bezpečnosť v organizácií, aký je jej účel a ktoré zdroje sú vynaložené na informačnú bezpečnosť. Obsahuje záväzok vedenia k zodpovednosti za informačnú bezpečnosť, vysvetľuje bezpečnostné ciele, čo chránia, aká je úroveň cielenej bezpečnosti a ako bezpečnostné ciele súvisia s poslaním organizácie. Ďalej popisuje vytvorenú organizáciu informačnej bezpečnosti, vytvorené roly a kto je zodpovedný za informačnú bezpečnosť.

Zavádzanie ISMS je dlhý a komplexný proces, podnet na jeho zavedenie musí byť iniciovaný vedením organizácie. V ďalšej časti popíšeme kroky potrebné na zavedenie ISMS, postupovať budeme podľa Kompendia[2] IT-Grundschutz[15] Spolkového úradu pre informačnú bezpečnosť(BSI). Pred začatím ďalšej sekcie si vyjasníme ešte dve veci.

Prvá vec, modálne slovesá používané na označenie požiadaviek, majú byť interpretované nasledovne:

- **MUSÍ**, vyjadruje povinnú požiadavku a
- **MAL BY**, vyjadruje odporúčanie.

V metodikách sa v súvislosti s bezpečnostnými opatreniami používa aj budúci čas „**SHALL**“, ktorý vyjadruje povinnosť. Kvôli zjednodušeniu[3] navrhovaného riešenia sme povinnosti a bezpodmienečné povinnosti nerozlišovali.

Druhá vec, doposiaľ sme v tejto kapitole používali pojem informačná bezpečnosť, v ďalšej časti tejto kapitoly budeme používať už známy pojem KIB. Pre účely tejto kapitoly budeme pojmy informačná bezpečnosť a KIB vnímať ako jeden a ten istý.

Formát ďalšej časti, v ktorej popíšeme postupnosť krokov, je nasledovný:

- na začiatku sekcie uvedieme opatrenie,
- pod opatrením budú vymenované úlohu na jeho splnenie a
- pod zoznamom úloh budú komentáre pre objasnenie jednotlivých úloh.

3.1 Prevzatie celkovej zodpovednosti vedením organizácie za KIB

1. Vedenie organizácie MUSÍ prevziať celkovú zodpovednosť za KIB, tak aby to bolo jasné každému.
2. Vedenie organizácie MUSÍ spustiť, riadiť a monitorovať bezpečnostný proces.
3. Vedenie organizácie MUSÍ byť dobrým príkladom pri dodržiavaní zásad KIB.
4. Vedenie organizácie MUSÍ vymenovať zamestnancov zodpovedných za KIB, poskytnúť im potrebné právomoci a zdroje.

[2]Slovník cudzích slov: kompendium – vedecká príručka so základnými poznatkami daného odboru.
[3]Tiež, aby sme zbytočne nemiatli čitateľa.

5. Vedenie organizácie MUSÍ byť v pravidelných intervaloch informované o stave KIB v organizácii, možných rizikách a dôsledkoch nedostatočných bezpečnostných opatrení.

Komentár k 1

Vedenie je zodpovedné za plnenie poslania organizácie, dosiahnutie svojich cieľov a je zodpovedné za spoľahlivý beh svojich systémov. Vyhlásenie vedenia sa nachádza v politike KIB, jeho účelom je vyslať jasný signál všetkým zainteresovaným stranám[4], že vedenie organizácie bude uplatňovať svoju autoritu a zdroje na zabezpečenie potrebnej úrovne KIB.

Za predpoklad, že v organizácii už došlo k rozhodnutiu zaviesť ISMS, je táto úloha je iba formalitou.

Komentár k 2

Jedine vedenie má potrebnú autoritu na spustenie bezpečnostného procesu. Vedenie má mnoho ďalších povinností, nemôže sa plne venovať vykonávaniu a ani nemá dostatočné zručnosti na riešenie KIB. Preto musí delegovať zodpovednosť za KIB kvalifikovaným zamestnancom, zadávať im úlohy a kontrolovať, ako splnili svoje úlohy. Vedenie bude musieť vytvoriť vhodnú organizačnú štruktúru, definovať roly KIB do ktorých zaradí zamestnancov.

Komentár k 3

Zavedené opatrenia KIB musí dodržiavať aj vedenie, čim dokáže efektívne motivovať zamestnancov, aby ich rovnako dodržiavali. Ak bude vedenie obchádzať zavedené opatrenia, nemôže očakávať, že zamestnanci sami budú dodržiavať opatrenia[5].

Komentár k 4

Na zavedenie systematického riešenia KIB v organizácií bude potrebných mnoho zdrojov, či už ľudských alebo finančných, zamestnancom sa rozšíria pracovné povinnosti, možno bude potrebné prijať nových ľudí alebo dokúpiť zariadenia. Zodpovednosť za KIB je zvyčajne priradená roli manažéra KIB[6], jeho povinnosti rozoberieme neskôr.

Zamestnanci zaradení do rolí KIB potrebujú mať dostatočnú kvalifikáciu a zručnosti. Ak by bol, povedzme z nutnosti, do roly zaradený niekto neznalý, nemôže sa od

[4]Niekto tento pojem pozná z angl. *shareholder*.

[5]Ľudovo povedané, aby nepili víno a nekázali vodu.

[6]V medzinárodných štandardoch a metodikách je rola manažéra KIB pomenovaná angl. *Information security officer(ISO)* alebo *Chief information security officer(CISO)*.

neho očakávať, že ošetrí a vyrieši všetky bezpečnostné problémy, naopak bude potrebovať čas na to, aby sa zaučil.

Komentár k 5

Povinnosťou manažéra KIB je vyhotovovať ročné správy o KIB, ktoré bude predkladať vedeniu, aby malo dostatok informácií pri riadení bezpečnostného procesu. Dôležité je vyzdvihnúť kritické procesy, riziká, ktorým čelia a potenciálne škody v prípade, že by došlo k bezpečnostnému incidentu[7].

3.2 Určenie cieľov KIB a stratégie KIB

1. Vedenie organizácie MUSÍ spustiť bezpečnostný proces.
2. Vedenie organizácie MUSÍ zadefinovať a zdokumentovať ciele KIB a stanoviť stratégiu KIB.
3. Vedenie organizácie MUSÍ prevziať zodpovednosť a podporovať ciele KIB a stratégiu KIB.
4. Vedenie organizácie MUSÍ v pravidelných intervaloch revidovať ciele KIB a stratégiu KIB.

Komentár k 1 a 2

Vstupom pre bezpečnostný proces sú ciele KIB a stratégia KIB. Ciele sú špecifické pre každú organizáciu, na tejto úrovni sú všeobecné a odvíjajú sa od jej poslania, príkladom sú:

- vysoká spoľahlivosť spracovania informácie vzhľadom k dôvernosti, integrite a dostupnosti,
- dobre meno organizácie,
- ochrana zamestnancov, osobných údajov a vysoko cenných informácií,
- plnenie si zákonných povinností.

Na určenie stratégie KIB je potrebná vysokoúrovňová analýza rizík, pomocou ktorej bude možné identifikovať hlavné aktíva, ktorým hrozbám čelia a pod akým rizikom sú. Výsledok vysokoúrovňovej analýzy rizík sa premietne do bezpečnostnej stratégie[8], kde

[7] Pohroziť alebo vystrašiť môže byť vhodnou motiváciou pre vedenie, aby poskytlo dostatočné zdroje.

[8] V skutočnosti je to začarovaný kruh, na jednej strane na určenie stratégie KIB potrebujeme vedieť, ktoré aktíva potrebujeme chrániť, na druhej strane analýza rizík vychádza zo stratégie, kde sa popisuje, čo treba chrániť. Jedným z riešením je useknúť to a začať vysokoúrovňovou analýzou rizík, ktorá ale nezachádza do detailov, iba poskytuje dostatočný nadhľad.

sa popíše, čo chránime, pred čím, spôsob ochrany, ako to súvisí s cieľmi KIB a ako naplniť ciele.

Komentár k 3

Stratégia KIB je schvaľovaná vedením a zvykne byť súčasťou politiky KIB, v ktorej (mimo iné) je zdôraznený záväzok vedenia k určeným cieľom KIB a stratégii KIB.

Komentár k 4

Prostredie, strategicky kontext, ciele organizácie a potenciálne hrozby sa časom menia, preto je potrebné v pravidelných intervaloch[9] vhodne prispôsobovať ciele KIB a stratégiu KIB meniacim sa podmienkam.

3.3 Načrtnutie politiky KIB

1. Vedenie organizácie MUSÍ prijať zastrešujúcu politiku KIB.
2. Politika KIB MUSÍ popísať význam KIB.
3. Rozsah pôsobnosti politiky KIB MUSÍ byť jasne určený.
4. Politika KIB MUSÍ byť sprístupnená všetkým zamestnancom a externým spolupracovníkom.
5. Politika KIB BY MALA byť revidovaná v pravidelných intervaloch.

Komentár k 1

Politika KIB praktickejšie popisuje to, ako sa realizuje KIB v organizácií, predstavuje ústavu KIB, ktorú podrobnejšie rozpracúvajú politiky druhej úrovne pre jednotlivé oblasti. V jej hlavičke sa zvykne nachádzať aj stratégia KIB.

Komentár k 2 a 3

Politika vysvetľuje význam KIB pre organizáciu, ako súvisia ciele KIB s poslaním organizácie, najdôležitejšie aspekty stratégie KIB a vytvorenú organizačnú štruktúru KIB. Musí byť jasné, na ktoré časti organizácie sa vzťahuje a kde sa má uplatňovať.

[9]Pol roka a menej môže byť príliš často, každý rok je primerane dlhá doba, no dlhší časový interval sa môže prejaviť ako rizikový. Samozrejme, v prípade výnimočných situácií bude potrebné konať hneď a nečakať na ďalšiu plánovanú revíziu.

Komentár k 4

Politika KIB je určená každému subjektu, ktorý pristupuje k informáciám, informačným systémom a sieťam organizácie. Vysvetľuje im ciele KIB, ako ich plánuje dosiahnuť a ktorými pravidlami sa majú riadiť, nepôjde však do veľkých detailov, aby jej porozumel aj človek, ktorý nie je znalý v oblasti KIB.

Komentár k 5

Politiku KIB vypracováva a je za ňu zodpovedný manažér KIB. Aktualizácia obsahu politiky KIB prebieha v ročných intervaloch, po zisteniach nedostatkov auditov alebo v mimoriadnych prípadoch. Zmeny bude potrebné predložiť vedeniu na schválenie a následne vhodne oboznámiť zamestnancov a externých spolupracovníkov o týchto zmenách.

3.4 Vymenovanie manažéra KIB

1. Vedenie organizácie MUSÍ vymenovať manažéra KIB.
2. Manažér KIB MUSÍ podporovať KIB a pomáhať riadiť bezpečnostný proces.
3. Vedenie organizácie MUSÍ poskytnúť manažérovi KIB dostatočné zdroje.
4. Manažér KIB MUSÍ mať možnosť komunikovať priamo s vedením organizácie.
5. Manažér KIB MUSÍ byť prítomný v rannom štádiu zavádzaní nových aplikácií a IT systémov.

Komentár k 1 a 2

Manažér KIB pomáha s koordináciou a usmerňovaním bezpečnostného procesu, ideálne by mal poznať organizáciu, jej procesy (a ako spolu súvisia), štruktúru organizácie, externých spolupracovníkov a dodávateľov. Manažér KIB by mal byť schopný samostatnej činnosti, vedieť obhájiť a presadiť bezpečnostné opatrenia[10].

Prirodzene, manažér KIB musí mať dostatočné vedomosti a zručnosti, aby vedel imlpementovať efektívne a účinné opatrenia. Ešte podotkneme, že vykonávací predpis 492/2022 Z. z. ZoKB ustanovuje znalostné štandardy aj pre rolu manažéra KIB[11], v tejto práci sa jej ale nebudeme venovať.

Podobne, ako pri prevzatí celkovej zodpovednosti za KIB, aj tu predpokladáme, že už bol manažér KIB menovaný vedením organizácie.

[10]Mnohé opatrenia zasahujú do pohodlia používateľov, čo môže vyvolať odpor a ústupčivý manažér KIB v dôsledku nemusí presadiť potrebné bezpečnostné opatrenia.

[11]Sú to rôznorodé a rozsiahle požiadavky na vedomosti, zručnosti, vzdelanie, prax a špecifické kompetencie, ktorými má manažér KIB disponovať.

Komentár k 3

Vedenie organizácie musí manažérovi KIB vytvoriť vhodné podmienky a poskytnúť mu dostatočne kompetencie a zdroje na riadenie bezpečnostného procesu. Manažér KIB bude musieť zaviesť nové roly pre KIB(do ktorých menuje zamestnancov), organizovať školenia alebo zakúpiť nové prostriedky.

Komentár k 4

Manažér KIB musí mať možnosť podávať hlásenia priamo vedeniu[12] pre účely podávania výročných správ, informovaní o závažných bezpečnostných incidentoch, o nedostatkoch/slabinách KIB, o výsledkoch auditov, o analýze rizík a iných dôležitých veciach týkajúcich sa KIB.

Komentár k 5

Je jednoduchšie navrhovať bezpečnostné opatrenia v počiatočných štádiách nových projektov. Brať do úvahy potenciálne hrozby a bezpečnostné problémy ešte v ranných fázach plánovania a analýzy môže ušetriť čas aj problémy v neskorších fázach, kde bude treba už existujúce riešenia opätovne prerábať.

3.5 Vytvorenie vhodnej organizačnej štruktúry KIB

1. Organizácia MUSÍ mať vhodnú vysokoúrovňovú organizačnú štruktúru KIB.
2. MUSIA byť vytvorené nové role KIB.
3. Do rolí MUSIA byť zaradení kvalifikovaní zamestnanci s dostatočnými zdrojmi.
4. Roly, úlohy, zodpovednosti a kompetencie MUSIA byť transparentne priradené.
5. MUSÍ byť stanovené efektívne pravidlá zastupovania pre všetky dôležité časti organizácie.
6. Komunikačné kanály MUSIA byť naplánované, opísané, zavedené a zverejnené.
7. Organizačná štruktúra KIB MUSÍ byť revidovaná v pravidelných intervaloch.

Komentár k 1 a 2

Pre potreby KIB je potrebné jasne vymedziť, kto za čo zodpovedá, ktoré úlohy má plniť a komu sa má hlásiť. Roly KIB majú pomôcť sprehľadniť celý bezpečnostný proces, oproti individuálnemu prístupu, kde úlohy zadávame jednotlivým zamestnancom. Bezpečnostné roly môžu predstavovať:

- manažér KIB, ktorý je centrálnou kontaktnou osobu pre zamestnancov,

[12] Priamo v zmysle cez garanta KIB.

- garant KIB, člen vedenia, ktorému sa bude manažér KIB priamo hlásiť,
- správca IT systému, ktorý zodpovedá za vývoj a bezpečnosť daného systému,
- informatik, ktorý vyvíja a udržiava systémy,
- koncový používateľ, ktorý zaobchádza so systémom,
- vlastník systému/aktíva, ktorý je zodpovedný za systém/aktívum,
- a iné.

Komentár k 3 a 4

Špecifické roly (ako manažér KIB) si vyžadujú istú kvalifikáciu a zručnosti na zaručenie správneho fungovania celého bezpečnostného procesu a vymedzené prostriedky, aby svoje povinnosti mohli vykonávať v plnom rozsahu. Zaradenie do roly nie je statické a musí súvisieť s tým, čo vykonáva daný človek a v prípade preradenia na inú pracovnú pozíciu sa môže meniť.

Organizácia si musí stanoviť pravidlá pre správu roly: Kto rozhoduje o zaradení zamestnanca do role? Kto priraďuje príslušné oprávnenia? Čo sa má udiať v prípade zmeny pracovnej pozície/náplne?

Komentár k 5

Počas neprítomnosti preberá zástupca všetky povinnosti svojho kolegu, aby boli prípadné problémy riešené čo najskôr. Problémy nečakajú na príchod zodpovedného zamestnanca a je dôležite ich udržiavať pod kontrolou, aby neprerástli do rádovo väčších problémov.

Komentár k 6

Pre všetky roly musí byť určené, kto koho informuje, čo všetko má vedieť a ktoré akcie má podniknúť. Treba sa dohodnúť na spôsobe komunikácie, ako má komunikácia prebehnúť a či/ako komunikovať s tretími stranami.

Pripomenieme, že ZoKB v §24 a z ZoITVS §23 ukladajú povinnosť nahlasovania KIB incidentov.

Komentár k 7

Podobne, ako politiku a stratégiu KIB, tak aj organizáciu KIB je potrebné v pravidelných intervaloch aktualizovať a prispôsobovať zmenám v organizácii a zmenám v okolí.

3.6 Definícia bezpečnostných opatrení

1. Pre všetky aspekty spracovania informácie MUSIA byť definované detailné a primerané bezpečnostné opatrenia.
2. Všetky bezpečnostné opatrenia BY MALI byť systematický dokumentované v bezpečnostných konceptoch.
3. Bezpečnostné opatrenia BY MALI byť pravidelne revidované.

Komentár k 1

V organizácii bude potrebné zhromaždiť existujúce opatrenia, identifikovať aktíva, relevantné hrozby a vyhodnotiť úroveň rizika. Pre zníženie rizika na akceptovateľnú úroveň bude potrebné prijať a dodržiavať nové opatrenia.

Bude potrebné vypracovať bezpečnostný projekt a vykonať analýzu rizík. Bezpečnostný projekt sa môže vykonať pre celú organizáciu (všeobecné opatrenia) alebo pre nejakú časť organizácie(špecifické opatrenia).

Komentár k 2 a 3

Ľudia ľahko zabudnú, prečo boli niektoré opatrenia zavedené a prečo práve v takej forme. Zavedené opatrenia môžu byť časom redundantné, málo efektívne alebo nedostatočné, keďže sa môžu objaviť nové hrozby a zraniteľnosti. Eventuálne bude potreba opatrenia upraviť alebo doplniť.

3.7 Zapojenie zamestnancov do bezpečnostného procesu

1. Všetci zamestnanci MUSIA byť integrovaní do bezpečnostného procesu.
2. Zamestnanci MUSIA byť informovaní o nebezpečenstvách, ktoré sú pre nich relevantné.
3. Zamestnanci MUSIA vedieť o nebezpečenstvách a vedieť, ako implementovať bezpečnostné opatrenia súvisiace s ich pracoviskom.
4. Zamestnancom MUSÍ byť umožnené aktívne prispievať k bezpečnosti.
5. Zamestnanci BY MALI byť prítomní v rannom štádiu plánovania bezpečnostných opatrení.
6. Pri zavádzaní bezpečnostných politík a nástrojov zamestnanci MUSIA vhodne informovaní, ako s nimi majú zaobchádzať.
7. Zamestnanci MUSIA byť oboznámení s následkami porušenia bezpečnostných pravidiel.

Komentár k 1, 2 a 3

Zamestnanci musia mať povedomie o KIB, relevantných hrozbách a povinnostiach, ktoré majú voči KIB. Zamestnanci musia vedieť o bezpečnostných opatreniach súvisiacich s vykonávaním ich práce, musia vedieť, kde nájsť základne dokumenty KIB, kde sa nachádzajú upozornenia/varovania pred nebezpečenstvami a kde sú zverejnené návody alebo iné vzdelávacie materiály KIB.

Noví zamestnanci, ešte pred výkonom svojej práce a prístupom k systémom a informačným technológiám organizácie, musia byť zaškolení[13] v oblasti KIB, existujúcich zamestnancov treba preškoliť a informovať o relevantných bezpečnostných problémoch.

Komentár k 4 a 5

Zamestnanci majú povinnosť upozorniť na nedostatky KIB, hlásiť bezpečnostné incidenty, s ktorými sa stretnú a musia vedieť, komu hlásiť tieto problémy. Tiež by mali byť súčasťou prípravy bezpečnostných opatrení, ktoré sa ich týkajú, aby mohli byť prijaté bezpečnostné opatrenia, ktoré sú realistické a vyhovujú obom[14] stranám.

Komentár k 6

Podľa obsahu a rozsahu opatrení treba zvoliť vhodnú formu oboznámenia[15], vysvetliť, čo sa od zamestnancov očakáva, prečo a aké povinnosti pre nich vyplývajú.

Komentár k 7

Zamestnanci musia vedieť, že svoje povinnosti musí plniť a v prípade ich neplnenia, aké sankcie im budú uložené.

3.8 Integrovanie KIB do procedúr a procesov celej organizácie

1. KIB MUSÍ byť integrovaná do všetkých procesov organizácie.
2. Manažér KIB MUSÍ byť adekvátne zapojený pri všetkých rozhodnutiach súvisiacich s bezpečnosťou.
3. KIB BY mala byť koordinovaná s ďalšími oblasťami organizácie zaoberajúce sa riadením rizík a bezpečnosti.

[13] Napríklad súčasťou povinného BOZP môže byť aj školenie o KIB.

[14] Manažérovi KIB, ktorý vytvára a predkladá bezpečnostné opatrenia a zamestnancom, ktorý majú dodržiavať navrhované bezpečnostné opatrenia.

[15] Napríklad pripraviť školenie, spomenúť na rannom/obednajšom meetingu, zverejniť na webovej stránke organizácie, zaslať mail s návodom.

Komentár k 1

Pre všetky činnosti vykonávané organizáciou treba určiť zodpovedných vlastníkov. Pomocou vlastníkov určí manažér KIB, ktoré informácie sa v systémoch spracovávajú, aké bezpečnostné opatrenia si vyžadujú, kto k nim má prístup, ktorým hrozbám čelia a akému riziku sú vystavené. Pri nových procesoch bude môcť manažér KIB zabudovať bezpečnostné opatrenia už pri návrhu.

Komentár k 2

Manažér KIB by mal posúdiť bezpečnostnú stránku navrhovaných riešení/opatrení a upozorniť na prípadné problémy.

Komentár k 3

Manažér KIB bude napríklad potrebovať pomôcť právneho oddelenia pri vytváraní/uzatváraní zmlúv a dodatkov, pomoc personálneho oddelenia pri výbere zamestnancov a zmenách pracovnej náplne alebo pomoc správcu budovy pri závadzaní opatrení chrániacimi pred prírodnými alebo fyzickými hrozbami.

Kapitola 4

Systém

V kapitole 2 sme zanalyzovali právne požiadavky ZoKB a ZoITVS, ktoré nám uložili povinnosť zaviesť ISMS. V nasledujúcej kapitole 3 sme pomocou kompendia IT-Grundschutz[15] popísali a vysvetlili štruktúru ISMS na základnej úrovni. Teraz máme všetko potrebné na to, aby sme navrhli a čiastočne implementovali systém pre manažéra KIB, ktorý:

- mu poskytne minimálne znalosti v oblasti KIB,
- prevedie ho úvodnými krokmi zavádzania ISMS a
- pomôže mu zozbierať informácie potrebné na vypracovanie bezpečnostnej dokumentácie[1].

Pri vypracovaní systému a písaní obsahu sme vychádzali z materiálov a metodík BSI 200-1[9], BSI 200-2[10], BSI 200-3[11], kompendia IT-Grundschutz[15] a IT-Grundschutz Online Course[12]. Rozhranie systému sme realizovali vo forme webovej aplikácie, systém beží lokálne na počítači a je prístupný cez ľubovoľný prehliadač. Zdrojový kód je v prílohe a súčasne je zverejnený na GitHub-e `https://github.com/AntonKica/spvbp-isvs-portal-backend/tree/bachelor-thesis`, vetva „bachelor-thesis“.

V tejto kapitole sa budeme venovať technickej špecifikácií, prezentácií výsledného systému, databázovému pohľadu a ako nakoniec tomu, ako spustiť systém. Teraz prejdeme k ďalšej časti, kde popíšeme technickú špecifikáciu, nástroje a technológie použité na vypracovanie systému.

4.1 Technická špecifikácia

Systém je logicky rozdelený na dve vrstvy – backend a frontend[2]. Backend tvorí logiku systému, spracováva dáta a ukladá ich do databázy. Frontend poskytuje užívateľské ro-

[1] Konkrétne politiky KIB.

[2] Pre slovenských čítateľov sú známejšie v poradí pojmy serverová časť a klientská časť. My sme sa rozhodli používať anglické výrazy, ktoré nám prišli prirodzenejšie.

zhranie, užívateľ tu zadáva vstupné údaje, ktoré sa posielajú backendu na spracovanie. Komunikácia medzi týmito dvoma vrstvami je realizovaná prostredníctvom protokolu HTTP a RPC[3].

Backend

Na vývoj backendu sme použili programovací jazyk Java verzie 21 a ekosystém vybudovaný okolo nej. Voľba programovacieho jazyka bola motivovaná najmä tým, že:

- dobré poznáme jazyk Java a máme skúsenosti jej ekosystémom,
- frameworky, knižnice a nástroje Javy sme využívali pri vývoji podstatných častí systému a
- sme nemuseli zbytočne strácať čas nad riešením technických úloh/problémov nesúvisiacimi s našou bakalárskou prácou.

Správu knižníc a balíčkov, kompiláciu a spustenie sme vyriešili pomocou nástroja Gradle verzie 8.

Na spracovanie RPC sme použili framework Spring Boot verzie 3, ktorý sme tiež využili aj na:

- celkovou konfiguráciou backendu,
- prehľadným definovaním rozhrania a endpointov[4] pre komunikáciu s frontendom
- serializáciou/deserializáciou vystupných/vstupných dát a
- manažmentom tried a repozitárov.

Na ukladanie dát systému sme použili SQL databázu PostgreSQL verzie 16. S databázou sme nekomunikovali priamo, ale pomocou ORM[5] frameworku Hibernate verzie 6. Pomocou Hibernate sme vyriešili problém s opakovaným kódom[6] a nemuseli sme opakovane písať SQL dotazy pri zmenách štruktúry tried.

Na testovanie sme využili knižnicu JUnit verzie 5. Avšak, v priebehu vývoja sme zistili, že nie je potrebné písať testy, ktoré by nás nanajvýš zdržiavali. Dôvodom bolo to, že pri zmenách kódu sme nepotrebovali kontrolovať funkcionalitu a konzistenciu dát[7].

[3] Z angl. *remote procedure call*, volanie vzdialenej procedúry, vďaka ktorému možno vykonať kód zo vzdialeného miesta, na inom zariadení.

[4] Koncové body, URL linka v prehliadači.

[5] Z angl. *object-relation mapping*, objektovo relačné mapovanie, vďaka ktorému sú triedy zmapované na štruktúry databázy.

[6] Dizajnový problém programovacích jazykov, kde programátor musí písať opakovane veľké množstvo kódu, aby dosiahol drobnú funkcionalitu.

[7] Pracovali sme sami a chyby sme si ešte vedeli ustrážiť.

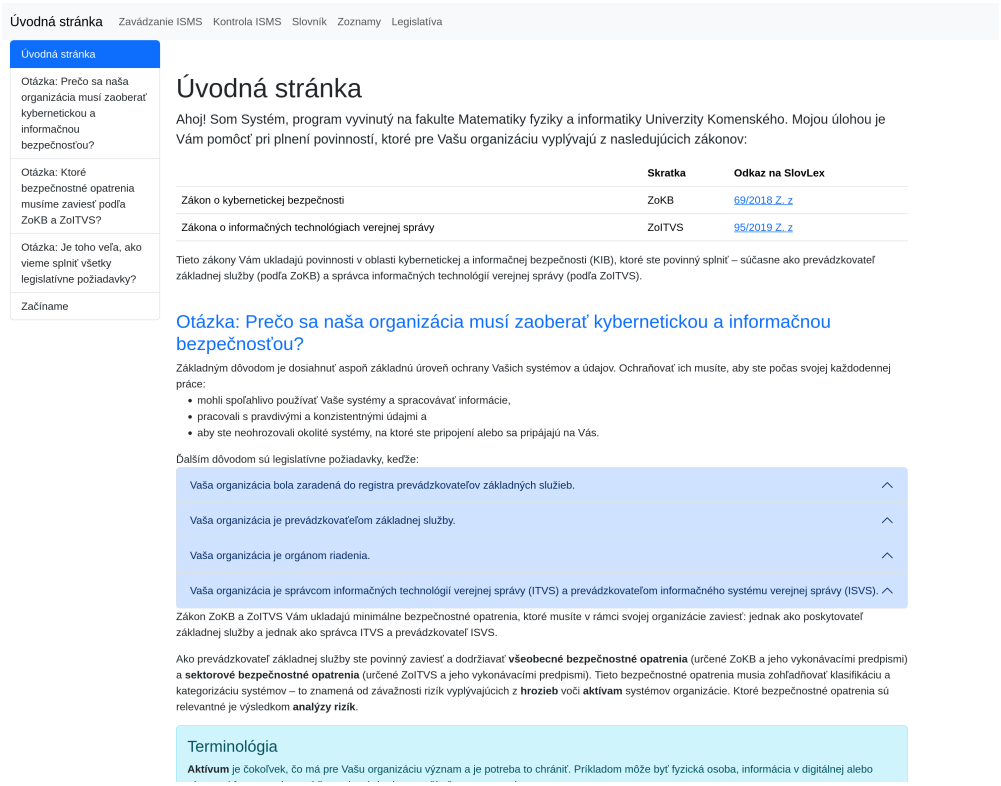
Frontend

Na vývoj frontendu sme použili HTML5 a v menšom rozsahu JavaScript[8]. Pre dosiahnite estetickejšieho vzhľadu[9] sme použili kaskádové štýly sady nástrojov Bootstrap verzie 5.

Stránky sme síce písali v jazyku HTML, no na ich zobrazenie sme použili šablónovací jazyk a techniku SSR[10], kde sme opäť využili ekosystém Javy. Šablónovací nástroj Thymeleaf verzie 3 nám pomohol so svojim dialektom HTML prehľadne zobraziť dáta, zoznamy, triedy a definovať tzv. fragmenty – vizuálne prvky, ktoré sme mohli opakovane použiť pri tvorbe jednotlivých stránok.

4.2 Prezentácia výsledného systému

Pomocou nástrojov využitých v backende a frontende sme vytvorili ukážkový systém, s ktorým interaguje používateľ, manažér KIB. Systém sa skladá z dvoch hlavných častí, jednej menšej – úvod (obr. 4.1), a druhej nosnej – návod (obr. 4.2).

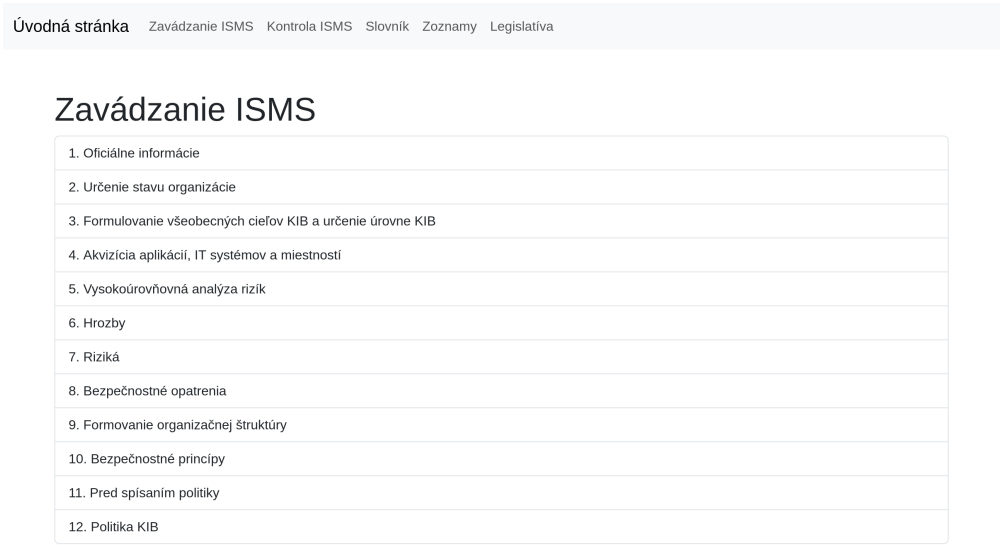


Obr. 4.1: Úvodná stránka.

[8]Na verziách veľmi nezáleží, používali sme funkcionalitu podporovanú väčšinou, ak nie všetkými modernými prehliadačmi.

[9]Pre čitateľa zdôraznime, aby od nás nečakal veľmi úhľadné vizuály, že sme informatici, nie grafici.

[10]Z angl. *server-side rendering*, spôsob, kde sa celá stránka plne zostaví/vykreslí na strane servera, pričom server zašle klientovi čistý HTML súbor.



Obr. 4.2: Stránka s návodom.

Ďalej si prejdeme obsah každej časti s krátkym komentárom.

Systém: Úvodná stránka

Na úvodnej stránke (obr. 4.1) predstavíme náš systém, uvedieme používateľa do problematiky a predstavíme mu zákony, ktoré sa ho týkajú – ZoKB a ZoITVS. Pokračujeme metódou kladenia otázok a odpovedí na ne, pričom odhadujeme, čo by sa manažér KIB mohol opýtať. Najprv manažérovi KIB vysvetlíme, prečo sa v organizácii musia zaoberať KIB (morálne a legislatívne dôvody) a vhodne to odôvodníme.

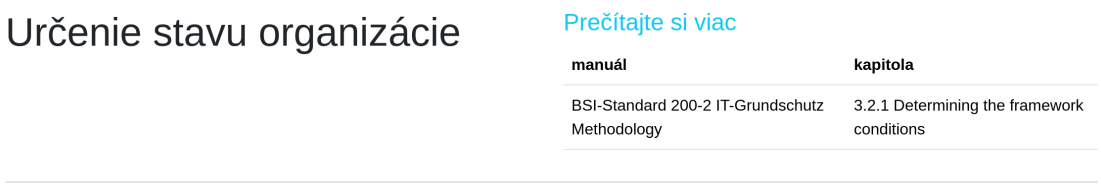
Po tom, ako vysvetlíme potrebu venovať sa KIB, očakávame prirodzenú otázku – Čo všetko musia (z hľadiska zákona) urobiť, aby v dostatočnej miere splnili zákonné požiadavky? Manažéra KIB stručne oboznámime s požiadavkami ZoKB a ZoITVS, pričom ho odkážeme na relevantné paragrafy (odkazujeme na portál Slov-lex). Tiež spomenieme súvisiace vykonávacie predpisy, a predpoklad, že systémy patria do kategórie I z hľadiska kategorizácie sieti a informačných systémov a súčasne do kategórie I ako prevádzkovatelia ISVS.

Nakoniec očakávame otázku – Čo to znamená splniť požiadavky, ktoré boli uložené organizácii? V krátkosti opíšeme celkový postup zavádzania ISMS a ktoré kroky budú musieť podniknúť. Po všetkých otázkach odkážeme používateľa na časť „Zavádzanie ISMS“.

Systém: Zavádzanie ISMS

V tejto časti systému (obr. 4.2) vidíme prehľad častí, ktorými prevedieme používateľa, aby mohol v organizácii zaviesť ISMS. V jednotlivých častiach, ak vychádzam z metodík

BSI, tak na začiatku uvedieme metodiku a kapitolu/sekciu, z ktorej sme čerpali (obr. 4.3), ak by si čitateľ chcel naštudovať problematiku podrobnejšie.



Obr. 4.3: Odkaz na metodiku BSI.

Postup pri zavádzaní ISMS je zložený z 12-tich krokov a je zavŕšený vypracovaním základného dokumentu ISMS – politiky KIB. Ďalej stručne popíšeme a vysvetlíme jednotlivé kroky.

Systém: Oficiálne informácie

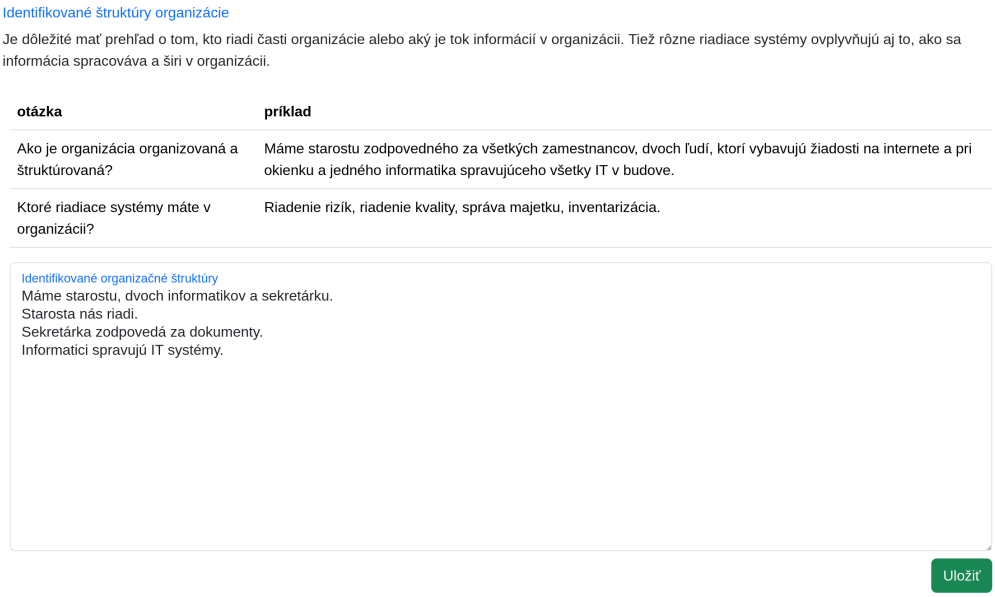
V tejto časti užívateľ vyplní krátky dotazník o svojej organizácii – názov, charakter organizácie, na základe čoho, resp. ktorého zákona bola zriadená ich organizácia. Tieto informácie využijeme aj neskôr pri písaní politiky KIB na identifikovanie poslania a hlavných aktív organizácie.

Systém: Určenie stavu organizácie

V tejto časti sme postupovali podľa BSI 200-2[10], kapitola „3.2.1 Determining the framework conditions“. Zisťujeme odpovede na základné otázky ohľadom organizácie – Aké sú ciele organizácie? Aké organizačné štruktúry existujú v organizácií? Spolupracujete s tretími stranami? Aký je strategický kontext organizácie? Uvádzame aj príklady, aby sme manažérovi KIB pomohli sa zorientovať a správne odpovedať (obr. 4.4). Na konci čaká manažéra KIB dotazník, kde má identifikovať dôležité biznisové procesy.

Biznisové procesy sa dajú odvodiť od poslania organizácie a sú zaujímavé tým, že zároveň predstavujú informačné toky. Spracovávajú sa v nich informácie a preto sú pre manažéra KIB dôležité, aby mohol neskôr identifikovať kritické biznisové procesy[11], ktoré budú tvoriť východisko pre vysokoúrovňovú analýzu rizík.

[11] V slovenčine neexistuje ekvivalentný termín, biznosové procesy sú procesy súvisiace s výkonom činností zameraných na plnenie poslania organizácie.



Obr. 4.4: Identifikovanie štruktúry organizácie, ukážka s vyplneným textom.

Systém: Formulovanie všeobecných cieľov KIB a určenie úrovne KIB

V tejto časti sme postupovali podľa BSI 200-2[10], kapitol „3.2.2 Formulate general information security objectives“ a „3.2.3 Determining the appropriate security level of the business processes“, stránka je rozdelená na dve sekcie.

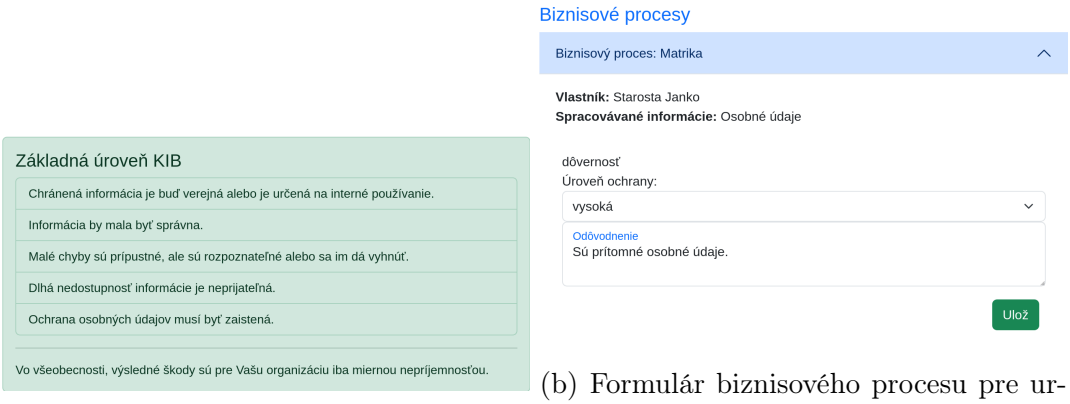
Prvá sekcia sa venuje formulovaniu všeobecných cieľov KIB. Manažéra KIB sa snažíme podnietiť, aby sformuloval všeobecné ciele KIB, ktoré vychádzajú z poslania organizácie a sústreďujú sa na základné aspekty KIB (dôvernosť, integritu a dostupnosť). Takáto skorá formulácia cieľov KIB má pomôcť zosúladiť politiku KIB so skutočnými požiadavkami KIB organizácie[12]. Manažér KIB za pomoci príkladov sformuluje všeobecné ciele KIB a uloží ich do systému.

Druhá sekcia sa venuje určeniu úrovne KIB, používateľovi predstavíme a vysvetlíme tri úrovne ochrany – základná, stredná a vysoká (obr. 4.5a). Nakoniec pre biznisové procesy identifikované v predchádzajúcej časti určí, akú úroveň ochrany si vyžadujú vzhľadom k základným aspektom KIB a prípadne odôvodní, prečo tak urobil (obr. 4.5b).

Systém: Akvizícia aplikácií, IT systémov a miestností

V tejto časti sme postupovali podľa BSI 200-2[10], kapitol „3.2.2 Formulate general information security objectives“ a inšpirovali sme sa príkladmi z IT-Grundschutz On-

[12]Manažér KIB by si tu mal uvedomiť, čo chce a má dosiahnuť pomocou KIB a celkovo zriadením ISMS.



(a) Vysvetlenie základnej úrovne ochrany KIB.

(b) Formulár biznisového procesu pre určenie úrovne ochrany KIB z hľadiska dôvernosti.

Obr. 4.5: Výňatok zo sekcie určenia úrovne KIB.

line Course[12], kapitoly „Lesson 3: Determining protection requirements“. Snažíme sa pomôcť manažérovi KIB urobiť si prehľad o aplikáciach, IT systémoch a miestnostiach, ktoré majú v organizácii. Ukážeme mu rôzne príklady a za pomoci formulárov mu umožníme uložiť si do systému získane informácie o organizácii.

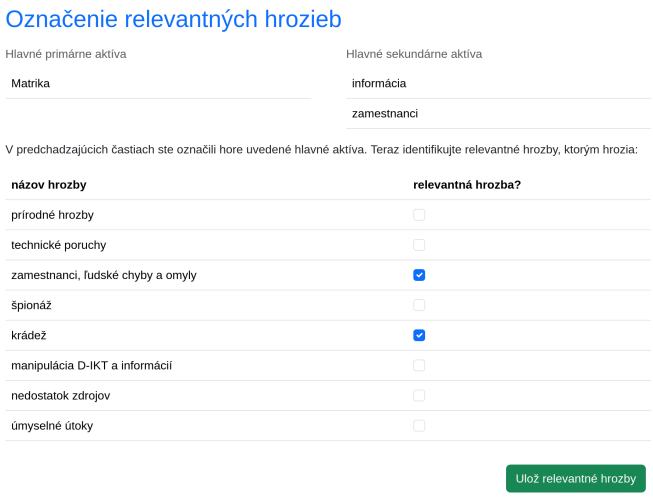
Systém: Vysokoúrovňová analýza rizík

Po zbere všeobecných informácií a získaní prehľadu o organizácii prejdeme k prvým krokom vysokoúrovňovej analýzy rizík. Vysvetlíme pojmy prímárne a sekundárne aktívum a pre každú z dvojice sa spýtame manažéra KIB, ktoré z aktív sú hlavné, bez ktorých organizácia nedokáže fungovať.

Primárne aktíva už boli identifikované – biznisové procesy, sekundárne aktíva ešte nie. Pri sekundárnych aktívach sme sa rozhodli urobiť krok späť, nerozoberali sme ich detailne, ani sme presne neidentifikovali, ktoré to sú. Miesto toho sme predstavili a vysvetlili charakteristické skupiny (napr. know-how alebo zamestnanci) a manažérovi KIB sme dali možnosť si vybrať, ktoré považuje za hlavné.

Systém: Hrozby

Po tom, ako manažér KIB identifikoval hlavné primárne a sekundárne aktíva, sa môžeme venovať všeobecným hrozbám, ktorým môžu čeliť. Manažérovi KIB predstavíme a vysvetlíme niekoľko všeobecných hrozieb a opätovne, v kontexte hlavných aktív, ho necháme si vybrať relevantné hrozby (obr. 4.6).

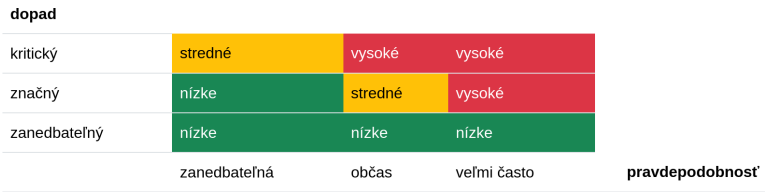


Obr. 4.6: Formulár s výberom relevantných hrozieb.

Systém: Riziká

Máme identifikované hlavné aktíva a relevantné hrozby, ktorým tieto aktíva čelia. Teraz môžeme vyhodnotiť/klasifikovať riziká, ktoré z nich vyplývajú. Manažéra KIB oboznámime s dvoma metódami, ako klasifikovať riziko – kvalitatívna metóda a kvantitatívna metóda, my sme sa rozhodli postupovať kvantitatívnou metódou, ktorá používa aj metodika BSI 200-3[11].

Výsledkom kvantitatívnej metódy je dvojrozmerná matica, kde na horizontálnej osi je vyjadrená pravdepodobnosť naplnenia hrozby, na vertikálnej osi je vyjadrená úroveň dopadu hrozby[13] a políčko reprezentuje výslednú klasifikáciu rizika. Pre jednoduchosť sme sa zvolili trojúrovňovú škálu pravdepodobnosti výskytu, úrovne dopadu a klasifikácie (obr. 4.7). Škály sme vysvetlili, aby pre hrozby vedel manažér KIB čo najpresnejšie



Obr. 4.7: Matica klasifikácie rizika.

vyhodnotiť pravdepodobnosť výskytu a úroveň dopadu. Nakoniec sme sa opýtali, aká je akceptovateľná úroveň rizika v organizácii. Výsledok klasifikácie rizík využijeme v ďalšej časti o bezpečnostných opatreniach.

[13] Obsah horizontálnej osi môžme vymeniť za obsah vertikálnej osi, na poradí nezáleží.

Systém: Bezpečnostné opatrenia

Vysoké úrovne rizík musí manažér KIB ošetriť, no na to, aby mohol znížiť riziká na akceptovateľnú úroveň, musí prijať bezpečnostné opatrenia. Časť s bezpečnostnými opatreniami sme podľa hrozieb rozdelili do príslušných oblasti. Na ukážku sme v systéme vypracovali oblasť „Zamestnanci, ľudské chyby a omyly“, ktorú ďalej rozoberieme.

Pri vypracovaní bezpečnostných opatrení pre oblasť „Zamestnanci, ľudské chyby a omyly“ sme vychádzali z kompendia IT-Grundshutz[15], kapitoly „ORP.2 Personnel“. Na začiatku pripomeniemie manažérovi KIB úroveň rizika, ktorú určil v časti systému „Riziká“, kde ho aj odkážeme v prípade, že by chcel prehodnotiť svoje rozhodnutie. Vo zvyšnej časti stránky rozoberieme zodpovednosť, čiu spoluprácu bude musieť manažér KIB vyhľadať, slabé miesta tejto oblasti a zakončíme to rozsiahlym zoznamom navrhovaných bezpečnostných opatrení na zníženie identifikovaného rizika.

Systém: Formovanie organizačnej štruktúry

V tejto časti sme čiastočne vychádzali z BSI 200-2[10], kapitoly „4 Organisation of the security process“ a držali sme sa ZoITVS §19 ods(1), ktorý popisuje organizáciu bezpečnostného procesu. Vysvetlili sme, čo to znamená sformovať organizačnú štruktúru, jej členenie na zložky (riadiacu, výkonnú a kontrolnú) a popísali sme základne roly KIB. Na konci nás (aj v mene manažéra KIB) špeciálne zaujímalo, kto je garantom KIB v organizácií[14].

Systém: Bezpečnostné princípy

Bezpečnostné princípy určujú filozofiu ISMS a sú povinnou súčasťou politiky KIB. Metodiky BSI neponúkajú žiaden zoznam bezpečnostných princípov, preto sme vychádzali z magisterský prednášok o manažmente KIB[4]. Účelom bezpečnostných princípov je explicitne stanoviť základné zásady, ktoré sa premietajú tak do riešení KIB ako aj celej činnosti organizácie. Manažéra KIB oboznámime s niekoľkými základnými bezpečnostnými princípmi a na záver mu dáme možnosť si vybrať tie princípy, ktoré by si želal aplikovať v celej organizácii.

Systém: Pred spísaním politiky

V tejto časti systému sa manažéra KIB pýtame na rôzne veci súvisiace so spísaním a vydaním politiky KIB. Opýtame sa na to, s kým bude musieť prerokovať navrhnutú politiku KIB, akým spôsobom bude vydaná, či majú v organizácii vypracované nejaké

[14]Pre manažéra KIB je to dôležitá osoba, je to jeho kontakt na vedenie organizácie.

dokumenty súvisiace s KIB a na zamestnancov zodpovedných za rozličné oddelenia organizácie[15].

Systém: Politika KIB

Dostali sme sa do poslednej časti nášho systému o zavádzaní ISMS. Obsah, resp. šablónu politiky KIB sme vypracovali na základe internej štúdie MIRRI (osobnej komunikácie)[2]. Formulácie časti textov sme spísali za manažéra KIB a do textu sme doplnili informácie, ktoré sme získali v nadväzujúcich častiach systému[16]. Do politiky KIB sme zakomponovali aj sekciu o riešení kybernetických incidentov, ktorej sme sa síce nevenovali, ale vzhľadom na jej dôležitosť sme ju zakomponovali.

Táto politika KIB však nie je ešte kompletná, chýbajú jej niektoré časti ktorým sme sa nevenovali, to sú najmä – riadenie informačných aktív, klasifikácia sieti a informačných systémov, kontinuita prevádzky, riadenie prístupov a niekoľko ďalších.

Zvyšné časti systému

Pozornému čitateľovi iste neuniklo, že vo vrchnej časti v navigácií sa nachádzajú ešte karty ako kontrola ISMS, slovník, zoznamy a legislatíva. V aktuálnej verzii systému je funkčná iba karta zoznamov, kde si používateľ môže pozrieť údaje, ktoré zadal do systému Zvyšným kartám sa budeme venovať v poslednej kapitole.

4.3 Databázový pohľad

Mimo obsahu a vizuálnej stránky nášho systému je menšou súčasťou aj databázová štruktúra údajov, ktoré evidujeme v systéme. Na generovanie nasledovnej databázovej schémy sme použili nástroj DBeaver.

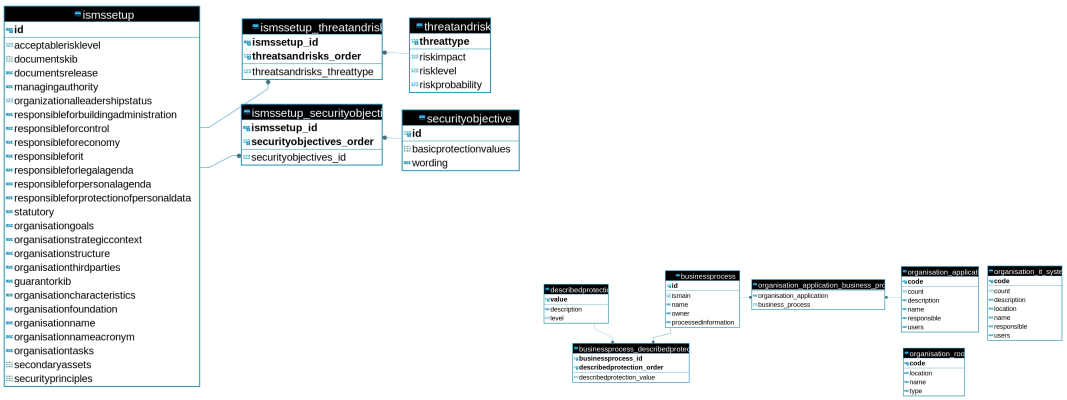
Na obrázku 4.8a vidíme agregátnu triedu, resp. tabuľku[17], ktorú sme nazvali „ISMS setup“. Je to jedinečná trieda, v systéme predstavuje singleton a obsahuje takmer väčšinu zozbieraných dát – reťazce znakov, zoznamy prvkov číselníkov a mapovania „one to many“. Trieda „ISMS setup“ slúži na zber dát, ktoré sme použili ako vstup pri generovaní politiky KIB.

Na druhom obrázku 4.8b vidíme schémy biznisových procesov, aplikácií, IT systémov a miestností. Tu sme jasnejšie videli výhodu separátnych tried a perspektívu

[15]Na ilustráciu, za pomoci zamestnanca zodpovedného za personálnu agendu, manažér KIB vhodne upraví/doplní pracovné povinnosti vyplývajúce z povinností KIB.

[16]Rôzne informácie o organizácii, ciele KIB, hlavné aktíva, hrozby, riziká alebo princípy.

[17]Pojmy trieda, schéma a tabuľka ľubovoľne zamieňame, myslíme tým jednu a tú istú vec, v tomto prípade zoskupenie premenných/stĺpcov.



(a) Hlavná schéma „ISMS setup“. (b) Zvyšné schémy.

Obr. 4.8: Databázová schéma.

pri budúcom vývoji softvéru, preto sme ich vyčlenili do samostatných tried a nie sú v zhluku dát „ISMS setup“.

Trieda „ISMS setup“ môže pôsobiť mohutne a určite sú v nej informácie, ktoré by sa dali vyčleniť, ináč zoskupiť alebo logicky rozdeliť do samostatných tried. Zatiaľ sme sa ale rozhodli uchovať aj nesúvisiace dáta v jednej tabuľke, zjednodušovalo to celkový model aj kód systému. Pri ďalšom vývoji systému, keď by sme mali lepšiu perspektívu a lepšie chápali súvislostí medzi dátami v systéme, túto triedu určite rozbijeme a upraceme.

4.4 Ako spustiť systém

Na spustenie systému je potrebné mať nainštalovanú Javu verzie 21 a dostupnú[18] databázu PostgreSQL verzie aspoň 16, predpokladáme prácu s príkazovým riadkom na operačnom systéme GNU/Linux. Zdrojový kód skompilujeme nasledujúcim príkazom:

```
./gradlew build -x test
```

Keď sa úspešne skončí kompilácia zdrojového kódu, spustíme systém nasledujúcim príkazom, pričom nakonfigurujeme databázové pripojenie parametrami JVM[19] – v hranatých zátvorkách sú Vami zvolené/známe parametre:

```
java \
  -Ddatasource.application.jdbcUrl=jdbc:postgresql://[server +
      port]/[databaza] \
  -Ddatasource.application.username=[pouzivatel] \
  -Ddatasource.application.password=[heslo] \
```

[18] Lokálne alebo vzdialene nakonfigurovanú.

[19] Angl. *Java virtual machine*, virtuálny stroj Javy.

```
-jar build/libs/spvbp-isvs-portal-backend-0.0.1-SNAPSHOT.jar
```

Systém je teraz prístupný na adrese a porte http://localhost:8000.

Kapitola 5

Po bitke sú všetci...

Pôvodná predstava a zámer bakalárskej práce v počiatočnom štádiu výskumu a analýzy bol jednoduchý. Náš plán predstavoval niekoľko krokov, ktoré tvorili základ problematiky:

1. Identifikovať požiadavky na bezpečnosť ISVS vyplývajúce z legislatívy.
2. Konkretizovať legislatívne požiadavky na základe noriem.
3. Navrhnúť postup, ktorým by sme efektívne naplnili tieto legislatívne požiadavky.
4. Vytvoriť systém na podporu zavedenia ISMS[1] v organizácii pre osobu poverenú touto úlohou – manažéra KIB.
5. Usporiadať a logicky zoskupiť informácie získane pri zavádzaní ISMS.
6. Získané informácie využiť pri správe rizík.

Počiatočný predpoklad bol taký, že na „malé“ ISVS budú kladené iba základne (malé) bezpečnostné požiadavky a potrebný systém na podporu by bol pomerne malý a jednoduchý. Ukázalo sa však, že opak bol pravdou a problematika sa v skutočnosti ešte väčšmi rozšírila a vyšlo najavo, čo všetko sa v skutočnosti skrýva v požiadavkách zákonov. Nami navrhnutý systém je síce nekompletný, nepokrýva všetky požiadavky stanovené zákonmi, no aj napriek tomu je veľmi rozsiahly.

Na druhej strane, bakalárska práca ukázala, že takýto systém na podporu vývoja bezpečnostného projektu sa dá vytvoriť:

1. Podrobne sme analyzovali legislatívne požiadavky zákonov ZoKB a ZoITVS a vykonávacích predpisov 362/2018 a 179/2020 v kapitole 2.
2. Zosúladili sme legislatívne požiadavky uvedených právnych noriem.
3. Vyjadrili sme všeobecné požiadavky právnych noriem pomocou technických noriem ISO/IEC 27001[13] a ISO/IEC 27002[14][2], s ktorými sú kompatibilné BSI 200-1, BSI 200-2, BSI 200-3 a kompendium IT-Grundschutz.
4. Upravili, resp. zjednodušili sme postup pri zavádzaní ISMS uvedený v metodikách

[1] Zaviesť systém riadenia informačnej bezpečnosti od nás explicitne vyžadovala legislatíva.
[2] Z týchto dvoch technických noriem vychádzajú ZoKB a ZoITVS.

BSI, aby bol zrozumiteľný aj pre neznalého a začínajúceho manažér KIB malého ISVS a najnižšej bezpečnostnej kategórie[3]. KIB

5. Vytvorili sme jednoduchý systém, ktorý prevedie manažéra KIB postupom zavádzania ISMS, poskytne mu základné informácie o KIB, legislatívnych požiadavkách a navrhovaných riešeniach.

Nami vytvorený systém je dôkazom toho, že sa to dá, je to hľadaný „proof of concept" toho, že taký pomocný systém je možné vypracovať.

Nič však nie je dokonale a aj nášmu systému chýba mnoho ďalších vecí, na ktoré sme nemali dostatok času a boli mimo rámec bakalárskej práce. Preto by sme sa teraz radi venovali veciam, ktoré sme v písomnej práci alebo systéme nespomenuli, no mali by byť súčasťou v nasledujúcich fáz[4], rozoberieme aj veci, ktoré by sme mohli lepšie rozvrhnúť, lebo teraz už aj my sme generáli.

5.1 Čo nebolo a mohlo byť, čo bolo a mohlo byť lepšie

Ochrana osobných údajov

Jednu z najväčších vecí, ktoré sme nespomenuli a sme sa jej vôbec nevenovali, je ochrana osobných údajov. Určite sme už všetci počuli o nariadení 2016/679 Európskej únie, tiež známe ako GDPR[5] a vysokých sankciách udelených v prípade jeho porušenia. V organizácii by mala byť určená zodpovedná osoba, ktorá sa venuje ochrane osobných údajov. Určite by bolo potrebné vysvetliť túto problematiku v systéme, no toto samo o sebe je rozsiahla oblasť hodná i svojej vlastnej záverečnej práce.

Príbuzná legislatíva

V slovenskej legislatíve existujú ďalšie zákony, ktoré sú relevantné z hľadiska KIB. Systém by mohol obsahovať prehľad a stručnú charakteristiku požiadaviek vyplývajúcich z týchto zákonov, aby mal manažér KIB prehľad aj o požiadavkách na ochranu špecifických systémov, ktoré existujú v organizácii. Ako príklad uvedieme 241/2001 Z. z. (zákon o ochrane utajovaných skutočnostiach), 493/2022 Z. z. (vyhláška o audite KIB) a 78/2020 Z. z. (vyhláška o štandardoch pre ITVS).

[3]Kategórie I z hľadiska kategorizácie sieti a informačných systémov (ZoKB) a správcu ISVS kategórie I (ZoITVS).

[4]Poznamenáme, že zoznam určite nie je kompletný

[5]Po angl. *General data protection regulation*, všeobecné nariadenie o ochrane údajov.

Bezpečnostné politiky druhej úrovne

Politika KIB je všeobecný dokument, ktorý je síce rozsiahly, no nič špecifické nehovorí. Politiky druhej úrovne podrobnejšie rozoberajú oblasti KIB obsiahnuté v politike KIB, ktoré sú rámcovo stanovené ZoKB a ZoITVS. Podrobne rozpracovať oblasti je však veľmi rozsiahle.

Čo po spísaní politiky

Spísať politiku KIB a zaviesť ISMS v organizácii je iba prvotný krok bezpečnostného procesu, v skutočnosti bude potrebné udržiavať zavedený ISMS na dostatočnej úrovni, čím sa začne sa životný cyklus ISMS. Organizáciu ešte čaká vypracovanie bezpečnostných projektov, inventarizácia a riadenie aktív, analýza a riadenie rizík.

Kategórie II a III

Doposiaľ sme sa venovali iba najmenšej a z princípu najľahšej kategórii I[6]. Podrobnú analýzu sme síce vykonali pre kategóriu I, no nahliadli sme aj do vyšších kategórií, kde sú požiadavky na prevádzkovateľov základných služieb a správcov ISVS rádovo väčšie. V krátkosti to znamená viac povinností, komplexnejšiu organizačnú štruktúru, väčší počet opatrení, zložitejšia politika KIB a mnoho ďalšieho skrytého v legislatívnych požiadavkách.

Modulárnosť

Vieme si zhruba predstaviť, aký veľký by vedel byť tento systém. V súvislosti s predchádzajúcim bodom, niektoré jeho časti nemusia byť relevantné pre každý typ organizácie[7] a možnosť zvoliť si potrebné časti by sprehľadnila systém.

Používatelia systému

Systém bol pôvodné navrhovaný iba pre manažéra KIB, no obsahuje veľa zaujímavých a užitočných informácií, ktoré by sa dali doplniť o moduly pre vzdelávanie a získavanie dát (dotazníky pre zamestnancov). Potom by však bolo potrebné vyriešiť správu systému, definovať roly a vyriešiť riadenie prístupu.

Je to aj otázka dostupnosti, čo ak by náš systém (alebo jeho derivácia) bola v budúcnosti úspešná? Malé ISVS by si nemuseli robiť starosti s inštaláciou systému, ba priam systém by bežal vo vládnom cloude. Na to ale treba vyriešiť autentifikáciu a autorizáciu používateľov systému.

[6] Podľa ZoKB a ZoITVS.

[7] Ak si čitateľ spomenie, na toto sme pýtali na začiatku zavádzania ISMS.

Upozornenia, správy a hlásenia

Systém by mohol mať pomocnú funkcionalitu, ako hlásenie bezpečnostných incidentov pre zamestnancov[8], evidencia bezpečnostných incidentov a generovanie reportov za nejaké obdobie. Keby sa niekto pozabudol, systém by ho mohol v pravidelných intervaloch upozorniť, napr. pripomenúť manažérovi KIB, že má neošetrené rizika.

Zmeny zákonov

Zákon sa zvyknú meniť, ale ako by náš systém riešil zmeny zákonov je ešte otvorená otázka. Nemôžme len tak zmeniť obsah systému bez toho, aby sme o tom nejak informovali používateľa. Zatiaľ nemáme predstavu o vhodnom spôsobe, ako tento problém vyriešiť.

Zamestnanci a roly

Problém s tým, ako spracovávame zamestnancov a roly sme už spomenuli pri pohľade na databázu a tabuľku „ISMS setup“. Bolo by potrebné vytvoriť vhodné triedy na reprezentáciu vzťahov zamestnancov, rolí, vlastníkov, aktív, procesov a pod. Manažér KIB by lepšie vedel „cestovať“ v systéme cez rôzne prepojenia, čo by sprehľadnilo navigáciu v systéme. Tiež by to umožnilo ďalšiu funkcionalitu, napr. pre roly KIB by bola možná kontrola konfliktu záujmov, na čo by mohol systém upozorniť manažéra KIB.

Kontrola ISMS, slovník a legislatíva

V prvotných návrhov systému sme sa zamýšľali nad mnohými funkcionalitami systému, karty „kontrola ISMS“, „slovník“ a „legislatíva“ boli jednými z nich.

Zavádzanie ISMS predstavuje mnoho krokov a manažér KIB by sa mohol ľahko stratiť v procese. S tým by mu pomohla časť „kontrola ISMS“, kde by bol prehľad splnených, rozpracovaných a zostávajúcich krokov.

Karta „slovník“ by bola prirodzená, keďže v KIB je mnoho termínov, v ktorých sa začínajúci manažér KIB môže stratiť. Mať jedno miesto so všetkými pojmami a vysvetleniami by bolo veľmi nápomocné.

Nakoniec, keď referujeme na rôzne sekcie zákonov, tak sa odkazujeme na portál Slov-lex, no z nášho pohľadu to má jeden nedostatok. Keď odkazujeme na špecifický odsek alebo písmeno, nedokážeme používateľovi zvýrazniť podstatné časti, čo môže viesť k tomu, že sa v tom stratí a pri ďalšej príležitosti bude odradený si pozrieť obsah

[8]Koniec koncov aj zákony vyžadujú zaviesť v organizácií jednotný systém hlásenia.

zákona. Toto sme chceli adresovať v karte „legislatíva“, kde by sme mali prítomné zákony a mali kontrolu nad nasmerovaním pozornosti čitateľa pri odkazoch na zákony.

Používateľská príručka

Bakalárska práca ani systém neobsahujú žiadnu používateľskú príručku. Vypracovanie používateľskej príručky, návodov a dokumentácie systému by bolo podstatné pre používateľov, ktorý by chceli prakticky používať náš systém.

5.2 Zhrnutie

Praktických návrhov a zlepšení vie byť nespočetne veľa, preto zhrnieme čo z tejto bakalárskej práce je použiteľné a čo by bolo ešte potrebné urobiť, aby náš systém bol plnohodnotný. Použiteľné časti našej bakalárskej prace by sme zhrnuli na:

- analýza právnych predpisov,
- analýza právnych požiadaviek,
- základné pojmy a informácie o KIB,
- opis postupu zavádzania ISMS,
- zber údajov o organizácii a
- zobrazenie zozbieraných informácii.

Dôležité časti bakalárskeho systému, ktoré by bolo potrebné rozšíriť/prepracovať pre plnohodnotný systém by sme zhrnuli na:

- vysvetlenie príbuznej legislatívy a problematiky,
- vypracovanie politik druhej úrovne,
- životný cyklus ISMS,
- vypracovanie bezpečnostných projektov, riadenia aktív a rizík,
- rozšírenie o kategórie II a III úrovne,
- modulárnosť systému,
- upozornenia, správy, hlásenia a kontrola stavu ISMS,
- správa používateľov a
- používateľská príručka.

Pri vypracovaní bakalárskej práce a jej systému sme sa dotkli iba špičky ľadovca, ďalej zostáva preskúmať to, čo sa skrýva pod hladinou vody.

Záver

Pôvodný zámer bakalárskej práce bol vytvoriť podporný systém pre manažérov KIB, ktorý nemajú mnoho znalostí v oblasti KIB. Tento systém im mal pomôcť naplniť legislatívne požiadavky na ochranu informačných systémov ISVS pod ich správou[9].

Počas prípravy bakalárskej práce sa ukázalo, že povinnosti vyplývajúce z legislatívnych noriem([7], [6], [8] a [5]) bolo podstatne viac, než sme na začiatku predpokladali a vnútorne tvorili zložitý a nekonzistentný systém. Ťažisko práce pozostávalo v analytickej činnosti, kde sme potrebovali identifikovať legislatívne požiadavky a následne ich konkretizovať pomocou technických noriem ([13] a [14]) a metodik ([9], [10], [11], [15]).

Právne normy obsahovali veľké množstvo všeobecných a technických požiadaviek. Zo všetkých požiadaviek pre správcu malého ISVS je najdôležitejšie mať manažéra KIB a zaviesť ISMS pokrývajúci všetky informačné systémy organizácie. Tým dostalo riešenie KIB pevný rámec. Ale aj postup podľa jednoduchého návodu pri zavádzaní ISMS si vyžaduje aspoň základné znalosti KIB od vedenia organizácie, manažéra KIB a zamestnancov. Bez základných znalostí by nebolo možné ani vytvoriť odborné dokumenty KIB, ani by sa nedalo očakávať, že tým dokumentom niekto porozumie a bude sa nimi vedieť riadiť.

Vytvorili sme jednoduchý systém, ktorý manažéra KIB oboznámi a vysvetlí mu problematiku KIB, získa od neho informácie o aktuálnom stave KIB v organizácií a povedie ho pri zavádzaní ISMS[10]. Tento „bakalársky“ systém je použiteľný ako základ profesionálneho systému pre podporu manažérov KIB. Po jeho čiastočnej implementácii sme tiež získali predstavu o tom, ako by bolo potrebné systém upraviť a rozšíriť, aby vyhovoval potrebám manažéra KIB.

Vytvorenie profesionálneho podporného systému si vyžaduje nie len prax a podrobnejšiu znalosť prostredia, v ktorom sa má systém používať, ale aj podstatne viac času, vedomostí a práce, ktorej rozsah a odborná úroveň presahuje rámec bakalárskej práce a úsilie jedného človeka.

[9] Ciele práce sme rozoberali v Úvode a aj v kapitole 5.

[10] Dokonca počas tohoto procesu od neho získame dôležité informácie pre spísanie rôznych dokumentov KIB.

Literatúra

[1] FitSM-0 overview and vocabulary. https://www.fitsm.eu/download/748/?tmstv=1716036382.

[2] Interná štúdia MIRRI, súkromná komunikácia.

[3] Krátky úvod do informačnej a kybernetickej bezpečnosti a malý výkladový slovník. https://mirri.gov.sk/wp-content/uploads/2022/02/KB-K1_2_3-uvod-do-KIB_slovnik_ver1.1.pdf.

[4] Manažment kybernetickej a informačnej bezpečnosti, magisterská prednáška, FMFI UK.

[5] Vyhláška č. 179/2020 z. z. vyhláška Úradu podpredsedu vlády slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2020/179/.

[6] Vyhláška č. 362/2018 z. z., vyhláška národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/362/.

[7] Zákon č. 69/2018 z. z., zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/.

[8] Zákon č. 95/2019 z. z., zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/95/.

[9] *BSI Standard 200-1*, 2017.

[10] *BSI Standard 200-2*, 2017.

[11] *BSI Standard 200-3*, 2017.

[12] *IT-Grundschutz Online Course*, 2018.

[13] *ISO/IEC 27001*, 2022.

[14] *ISO/IEC 27002*, 2022.

[15] *IT-Grundschutz-Compendium*, 2022.