VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

INFORMAČNÍ BEZPEČNOST JAKO UKAZATEL VÝKONNOSTI PODNIKU
INFORMATION SECURITY AS AN INDICATOR OF BUSINESS PERFORMANCE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Rastislav Gancarčik

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Petr Sedlák

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Rastislav Gancarčik**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Informační bezpečnost jako ukazatel výkonnosti podniku

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Pro vybraný podnik na základě analýzy vypracujte metodický postup pro vytvoření výkonnostního ukazatele na základě řízení informační bezpečnosti.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha:Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

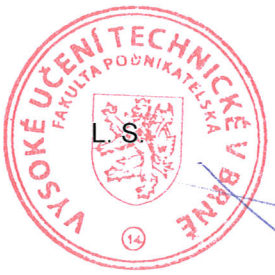
ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 28. 2. 2017



L. S.

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Obsahom tejto diplomovej práce je návrh metodického postupu pre hodnotenie výkonnosti podniku z pohľadu informačnej bezpečnosti, pričom táto výkonnosť sa posudzuje na základe splnenia noriem ISO/IEC 27001:2013, zákona č. 181/2014 Sb., nariadenia Európskeho parlamentu č. 2016/679 a smernice Európskeho parlamentu č. 2016/1148. Návrh tohto metodického postupu je spracovaný pre konkrétnu spoločnosť pôsobiacu v Českej republike.

Abstract

The content of this thesis is a proposal of methodology for evaluating company's performance in areas of information security, while their performance will be judged based on compliance with standard ISO/IEC 27001:2013, Act no. 181/2014 Coll., Regulation 2016/679 of European Parliament and Directive 2016/1148 of the European Parliament. The proposal of this methodology is designed in a particular company which operates in the Czech Republic.

Kľúčové slová

ISMS, kybernetický zákon, informačná bezpečnosť, ISO/IEC 27001, GDPR, NIS, riadenie informačnej bezpečnosti, osobné údaje

Keywords

ISMS, cyber security Law, information security, ISO/IEC 27001, GDPR, NIS, information security management, personal data

Bibliografická citácia

GANCARČIK, R. *Informační bezpečnost jako ukazatel výkonnosti podniku.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 86 s. Vedúci diplomovej práce Ing. Petr Sedlák.

Čestné prehlásenie

Prehlasujem, že predložená diplomová práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušil autorské práva (v zmysle Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brne dňa 24. mája 2017 .....

Poďakovanie

Rád by som sa poďakoval vedúcemu mojej diplomovej práce Ing. Petrovi Sedlákovi. za jeho odborné a cenné rady, ktoré mi pri spracovaní práce poskytol, aj za tie tri semestre, ktoré nás učil o informačnej bezpečnosti.

OBSAH

Úvod

Informácie v dnešnej dobe predstavujú majetok, ktorý je pre organizáciu minimálne rovnako dôležitý ako iné obchodné aktíva. Aj z tohto dôvodu musia byť vhodne chránené, či už sa jedná o informácie v papierovanej, analógovej alebo digitálnej forme, alebo sú to informácie vo forme znalostí. Vhodne chránené preto, lebo neexistuje spôsob, ako zaručiť ich absolútnu ochranu. Je ale isté, že so zvyšujúcou sa úrovňou bezpečnosti informácií budú náklady na ďalšie jej zvyšovanie rásť.

So vzrastajúcou úrovňou „komputerizácie" spoločnosti, teda zavadzaním počítačov do ďalších oblastí bežného života, je čoraz viac činností závislých na fungovaní nejakého informačného alebo komunikačného systému. To so sebou nesie aj nutnosť riešiť bezpečnosť informácií v týchto systémoch. Čo, ale ani v dnešnej dobe nie je samozrejmosť a stále sa nájde dosť firiem, ktoré informačnú bezpečnosť v rámci ich organizácie, ani v rámci produktov, ktoré ponúkajú, neriešia. Pritom je možno len otázkou času, kedy narušenie bezpečnosti v ich systémoch alebo produktoch, spôsobí im, alebo ich zákazníkom, škody obrovského významu, ktoré budú mnohonásobne vyššie ako opatrenia, ktoré by pomohli tomu predísť.

Úlohou riadenia informačnej bezpečnosti tak je, pomôcť firmám vybrať vhodné opatrenia na zaistenie primeranej úrovne bezpečnosti informácií tak, aby náklady na tieto opatrenia neboli vyššie ako možný dopad rizík s tým spojených.

1. Vymedzenie problému a ciele práce

Spoločnosť, ktorá pôsobí v energetickom odvetví v Českej republike má mnoho oblastí informačnej bezpečnosti, ktoré musí riešiť. A to nie len z dôvodu dopadov, ktoré by prípadné narušenie bezpečnosti informácií mohlo mať, ale aj z dôvodu platných zákonov týkajúcich sa kybernetickej bezpečnosti, a schváleného európskeho nariadenia na ochranu osobných údajov.

Cieľom tejto diplomovej práce je tak navrhnúť metodiku na vytváranie výkonnostných ukazovateľov na základe riadenia informačnej bezpečnosti, kybernetického zákona a európskeho nariadenia GDPR. Pričom táto metodika by mala byť aplikovateľná na uvedenú spoločnosť a mala by jej tak pomôcť so zisťovaním jej výkonnosti v daných oblastiach.

V prvej časti tejto práce predstavím teoretické východiská informačnej bezpečnosti, vrátavane noriem, ktoré sa touto problematikou zaoberajú, zákonov a nariadení. Druhá časť práce sa bude venovať analýze uvedenej energetickej spoločnosti a následne v tretej časti navrhnem riešenie. Na konci práce ešte zhodnotím výsledky a prínosy riešenia.

2. Teoretické východiská

V prvej kapitole práce sa zameriam na teoretické východiská, ktoré súvislá s informačnou bezpečnosťou a hlavne s cieľom tejto práce. Na začiatku budú predstavené základné pojmy súvisiace s touto témou a popísaný systém riadenia bezpečnosti informácií. Následne sa budem venovať normám z oblasti informačnej bezpečnosti a zakončím to informáciami o právnom prostredí.

2.1. Základné pojmy

Dáta

Podľa normy ISO predstavujú dáta opakovateľne interpretovateľné informácie vo formalizovanej podobe vhodnej pre komunikáciu, spracovanie alebo objasňovanie, ktoré môžu byť spracované ľuďmi alebo automatizovanými prostriedkami. V jednoduchosti sa dá povedať, že ide o informácie pretransformované do podoby s ktorou sa lepšie „manipuluje“, pričom ich spracovaním alebo interpretovaním opäť vznikajú informácie (6).

Informácie

Ak sa aj tu použije definícia podľa normy ISO, tak ide o vedomosti týkajúce sa objektov, ako sú fakty, udalosti, veci, procesy, alebo myšlienky vrátane koncepcií, ktoré majú v určitom kontexte osobitný význam. Zjednodušene teda ide o pojem, ktorý popisuje rôzne objekty reálneho sveta. V súvislosti s dátami môžeme o informáciách tiež hovoriť, ako o interpretovaných dátach (6).

Informačný systém

Informačný systém predstavuje akési zoskupenie častí tvoriacich zložitý celok, ktorý pozostáva z koncepčnej schémy, informačnej základne a informačného procesora, a slúži na uchovávanie a manipuláciu s informáciami (6).

Dá sa tiež definovať ako jednotný súbor informačných zdrojov zorganizovaných za účelom zhromažďovania, spracovania, uchovávania, používania, zdieľania, šírenia alebo poskytovania informácií (7).

Informačné a komunikačné technológie (ICT – Information and Communication Technology)

Pojem ICT v sebe zahrňuje všetky prostriedky (technológie), ktoré umožňujú prenos, spracovanie a interpretáciu informácií (dát).

Sieťová infraštruktúra

Je súbor všetkých sieťových prvkov a zariadení (hardware aj software), ktoré sú použité pri realizácií ICT prostredia (8).

Aktívum (Asset)

Predstavuje všetok hmotný aj nehmotný majetok, ktorý má pre organizáciu nejakú hodnotu.

Dôvernosť (Confidentiality)

Vlastnosť vyjadrujúca nedostupnosť a neprístupnosť informácie neopraveným osobám (9).

Integrita (Integrity)

Vlastnosť vyjadrujúca úplnosť a presnosť informácie (9).

Dostupnosť (Availability)

Vlastnosť vyjadrujúca prístupnosť a použiteľnosť informácie na vyžiadanie oprávnenej osoby (9).

Hrozba (Threat)

Predstavuje potenciálnu príčinu nežiaducej udalosti, ktorá môže viesť k poškodeniu systému alebo organizácie (9).

Zraniteľnosť (Vulnerability)

Je slabé miesto aktíva, ktoré môže byť zneužité jednou alebo viacerými hrozbami (9).

Opatrenia (Countermeasures)

Predstavujú všetky procesy, politiky, praktiky, zariadenia a ďalšie činnosti, ktoré môžu znížiť hrozbu, zraniteľnosť, alebo dopad hrozby.

Základné rozdelenie opatrení na typy (9), (10):

- preventívne,
- detekcia a reakcia,
- podporné.

Riziko (Risk)

V informačnej bezpečnosti predstavuje riziko možnosť, že hrozba využije zraniteľnosť informačného aktíva a spôsobí tým organizácií škodu (9), (10).

Dopad (Impact)

Predstavuje škodu, ktorá vnikne, ak hrozba využije zraniteľnosť informačného aktíva.

Bezpečnostná udalosť (Information Security Event)

Predstavuje stav systému, služby alebo siete, ktorý naznačuje možné porušenie bezpečnosti informácií, politík, alebo zlyhanie opatrení, alebo doposiaľ neznámu situáciu, ktorá môžu byť relevantná z hľadiska bezpečnosti (9).

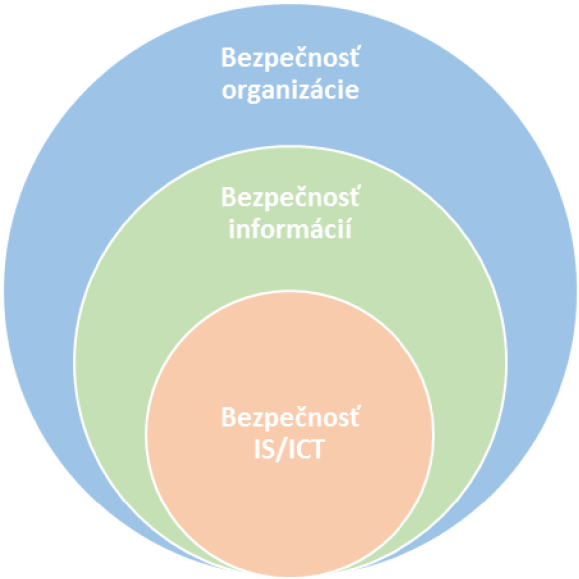
Bezpečnostná incident (Information Security Incident)

Predstavuje jednu alebo niekoľko nežiadúcich, či neočakávaných, bezpečnostný udalostí, ktoré majú značnú pravdepodobnosť ohrozenia informačnej bezpečnosti a obchodných operácií (9).

Bezpečnosť informácií (Information Security)

Informačná bezpečnosť rieši zachovanie dôvernosti, integrity a dostupnosti informácie. Jej úlohou je teda zabezpečovať, aby informácie boli v úplnej a presnej podobe dostupné kedykoľvek a poskytnúť ich len po vyžiadaní od oprávnenej osoby.

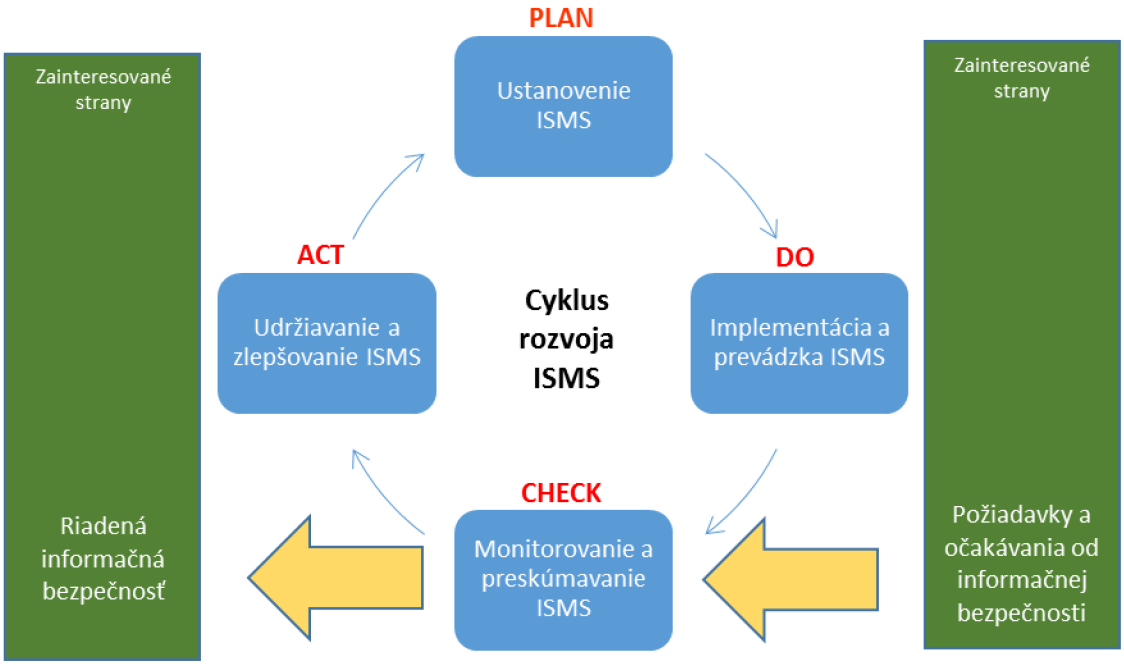
S pojmom bezpečnosť informácií sú úzko späté aj pojmy bezpečnosť organizácie a bezpečnosť IS/ICT. Pre zachovanie bezpečnosti informácií je nevyhnutné mať vyriešenú aj bezpečnosť organizácie, ktorej súčasťou je aj ochrana objektov a majetku podniku. Bezpečnosť informácií tak tvorí podmnožinu bezpečnosti organizácie. Bezpečnosť IS/ICT je zase, vzhľadom na to, že pod informačnú bezpečnosť patria aj informácie v nedigitálnej podobe a bezpečnosť IS/ICT je zameraná len na ochranu aktív IS/ICT, podmnožinou obidvoch (8).



Obrázok č. 1: Úrovne bezpečnosti (Zdroj: Vlastné spracovanie podľa (8))

2.2. ISMS

Systém riadenia bezpečnosti informácií pozostáva z rôznych smerníc, politík, postupov, súvisiacich zdrojov a činností, ktoré sú spravované organizáciou s úmyslom zaistiť ochranu jej informačných aktív. Z tohto dôvodu je súčasťou celkového systému riadenia organizácie. ISMS tak predstavuje systematický a riadený prístup k ustanoveniu, implementácii, prevádzke, monitorovaniu, preskúmavaniu, údržbe a zlepšovaniu informačnej bezpečnosti organizácie s cieľom dosahovania obchodných cieľov. Tieto procesy, ktoré tvoria ISMS, je možné aplikovať na model PDCA (Demingov model).



Obrázok č. 2: PDCA cyklus rozvoja ISMS (Zdroj: Vlastné spracovanie podľa (10))

Na tomto obrázku je názorne zobrazené, ktoré procesy patria do ktorej fázy (etapy) tohto modelu. Taktiež ilustruje, ako ISMS prijíma na vstupe požiadavky a očakávania informačnej bezpečnosti od zainteresovaných strán a prostredníctvom procesov a činností vytvára výsledky informačnej bezpečnosti, tzn. riadenú informačnú bezpečnosť, ktoré týmto požiadavkách a očakávaniam vyhovujú. A vzhľadom na to, že sa jedná o cyklus, kde sa tieto štyri činnosti (plánuj, rob, kontroluj, jednaj) neustále opakujú, dokresľuje to potrebu neustáleho rozvoja ISMS (10).

Aj keď PDCA cyklus nie je v súčasnej verzii normy ČSN ISO/IEC 27001 z roku 2014 vyslovene uvedený v úvode tejto normy, ako tomu bolo v prípade starších verzií, v štruktúre tohto štandardu je ho možné stále nájsť .

Rozdelenie kapitol ČSN ISO/IEC 27001:2014 na etapy PDCA (10):

- Plan (Plánu) – 4. Kontext organizácie, 5. Vedenie (Leadership) 6. Plánovanie, 7. Podpora,
- Do (Rob) - 8. Prevádzka,
- Check (Kontroluj) – 9. Hodnotenie výkonnosti
- Act (Jednaj) – 10. Zlepšovanie.

2.2.1. Ustanovenie ISMS

V rámci prvej etapy ISMS by tak organizácia mala (3), (10):

- určiť rozsah a hranice ISMS, ktoré budú brať do úvahy zainteresované strany a ich požiadavky relevantné k bezpečnosti informácií, a taktiež interné a externé aspekty, ktoré by mohli ovplyvniť schopnosť dosiahnutia zamýšľaného výstupu ISMS (kapitola 4.3),
- stanoviť politiku ISMS (kapitola 5.2),
- priradiť právomoci a zodpovednosti pre role relevantné bezpečnosti informácií (kapitola 5.3),
- určiť kritéria pre akceptáciu rizík a kritéria pre posudzovanie rizík, identifikovať riziká a ich vlastníkov, analyzovať zistené riziká na základe pravdepodobnosti ich výskytu a ich potenciálnych následkov, určiť úroveň rizík a ohodnotiť ich na základe definovaných kritérií pre posudzovanie (a akceptáciu) rizík (kapitola 6.1.2),
- navrhnúť a používať proces pre ošetrovanie rizík, ktorý bude brať ohľad na výsledky hodnotenia rizík; pomocou neho určiť nevyhnutné opatrenia pre ošetrovanie rizík; na jeho základe vytvoriť *Prehlásenie o aplikovateľnosti*, ktoré obsahuje nevyhnutné opatrenia a zdôvodnenia pre ich zahrnutie; a formulovať plán ošetrenia rizík a prijatia zvyškových rizík, ktorý musí byť schválený vlastníkmi rizík (kapitola 6.1.3),
- stanoviť ciele bezpečnosti informácií relevantné jednotlivým funkciám a úrovniam riadenia (kapitola 6.2),
- určiť a zaistiť potrebné zdroje na všetky etapy ISMS (kapitola 7.1),
- zaistiť osoby s potrebnou úrovňou kvalifikácie/kompetencie (kapitola 7.2),
- zaistiť, aby osoby pracúce pre organizáciu mali povedomie o politike ISMS, čo ISMS prináša a aké následky môže mať neprispôsobenie sa požiadavkám (kapitola 7.3),
- určiť kto, s kým, kedy a o čom musí komunikovať, a procesy, ktorými musí byť táto interná alebo externá komunikácia realizovaná (kapitola 7.4),

- zaistiť, že všetky informácie ISMS sú dokumentované, pravidelne aktualizované, a dostupné pre použitie kedykoľvek a kdekoľvek, pri zachovaní odpovedajúcej úrovne ich dôvernosti (kapitola 7.5).

2.2.2. Implementácia a prevádzka ISMS

V rámci druhej etapy cyklu by organizácia mala (3), (10):

- implementovať plány k dosiahnutiu stanovených cieľov bezpečnosti informácií; implementovať a riadiť procesy, ktoré sú potrebné k splneniu požiadaviek informačnej bezpečnosti; implementovať určené opatrenia, a spracovávať dokumentáciu realizácie procesov, aby mala istotu, že boli nasadené tak, ako boli naplánované (kapitola 8.1),
- pravidelne posudzovať riziká bezpečnosti informácií, a to aj v prípadoch, keď sú plánované alebo nastanú významné zmeny, a brať pri tom ohľad na definované kritéria posudzovania a akceptácie rizík (kapitola 8.2),
- implementovať navrhnutý plán ošetrovania rizík a dokumentovať výsledky tohto procesu (kapitola 8.3).

2.2.3. Monitorovanie a preskúmavanie ISMS

Audit (Audit)

Je systematický, nezávislý a zdokumentovaný proces, ktorý slúži na získanie audítorských dôkazov a ich objektívnemu hodnoteniu, s cieľom určiť, do akej miery sú splnené kritéria auditu (9).

Preskúmavanie (Review)

Predstavuje činnosť, ktorá je vykonávaná za účelom určenia vhodnosti, primeranosti a účinnosti predmetu preskúmavania na dosiahnutie stanovaných cieľov (9).

V tretej etape ISMS cyklu by organizácia mala (3), (10):

- určiť, čo sa bude monitorovať a merať, kto a kedy to bude vykonávať; určiť metodiky ktoré sa použijú na meranie, monitorovanie, analýzu a hodnotenie; určiť

kto a kedy bude výsledky z týchto meraní analyzovať a vyhodnocovať (kapitola 9.1),

- na základe stanovených metodík vyhodnocovať výkonnosť a efektívnosť ISMS, a viesť dokumentáciu o týchto meraniach a hodnoteniach (kapitola 9.1),
- mať naplánované, ustanovené a implementované auditné programy, definované kritéria auditov a ich rozsah; vybraných audítorov, ktorí uskutočňujú audity a výsledky predkladajú relevantným vedúcim pracovníkom, pričom celý proces auditu je dokumentovaný (kapitola 9.2),
- vykonávať pravidelné interné audity, ktorých úlohou je zistiť, či je ISMS efektívne implementovaný a vyhovuje požiadavkám (kapitola 9.2),
- prostredníctvom managementu organizácie preskúmavať ISMS a viesť o týchto preskúmavaniach dokumentáciu (kapitola 9.3).

2.2.4. Udržiavanie a zlepšovanie ISMS

Nezhoda (Nonconformity)

Je nesplnenie požiadavku (9).

Nápravné opatrenie (Corrective action)

Opatrenie na odstránenie príčiny nezhody a zabránenie jej opakovaniu (9).

Organizácia by v poslednej etape cyklu ISMS mala (3):

- v prípade výskytu nezhody - zistiť jej príčinu; aký následok bude mať; implementovať vhodné opatrenie; preskúmavať efektívnosť každého prijatého nápravného opatrenia, a v prípade nutnosti uskutočniť zmenu v ISMS (kapitola 10.1),
- neustále zlepšovať efektívnosť, vhodnosť a primeranosť ISMS (kapitola 10.2).

2.2.5. Normy radu 27 000

V tejto podkapitole sa zameriam na normy riešiace informačnú bezpečnosť, čo sú dnes najmä normy radu ISO/IEC 27000. V súčasnosti do tejto rady noriem patrí celkovo už

okolo 37 noriem v rôznej fáze spracovania, ktoré riešia rôzne oblasti informačnej bezpečnosti a v rôznej úrovni špecifickosti. Vedľa všeobecných noriem riešiacich riadenie informačnej bezpečnosti, tak medzi nimi môžeme nájsť aj konkrétne návody na zabezpečenie úložísk dát (ISO/IEC 27040:2015), normu riešiacu výber, nasadenie a prevádzku IDPS (Intrusion Detection and Prevention System) (ISO/IEC 27039:2015), alebo normu, ktorá je primárne určená na zavádzanie ISMS do organizácie pôsobiacej v nejakom konkrétneho odvetví, ako napríklad, telekomunikační operátori (ISO/IEC 27011:2016) (11).

Detailnejšie predstavím len niektoré z týchto noriem, pretože na kompletný rozbor všetkých noriem tejto rodiny nie je v tejto práci priestor a ani to nie je potrebné.

ČSN ISO/IEC 27000:2017

Informačné technológie – Bezpečnostné techniky – Systémy riadenia bezpečnosti informácií – Prehľad a slovník

Táto medzinárodná norma poskytuje hlavne prehľad všetkých termínov a definícií používaných v rodine noriem ISMS, a tiež poskytuje základný prehľad o normách spadajúcich do tejto rodiny. V súčasnosti je k dispozícií už vo svojej štvrtej verzií. (11).

ČSN ISO/IEC 27001:2014

Informačné technológie – Bezpečnostné techniky – Systémy riadenia bezpečnosti informácií – Požiadavky

Táto norma, ktorá pôvodne (v roku 2005) vznikla prebratím s menšími úpravami z britskej normy BS 7799-2, tvorí v súčasnosti základ rodiny ISO 27000. Oproti pôvodnej verzií z roku 2005, prešla táto norma značnými úpravami, najmä aby sa zosúladila (harmonizovala) s inými normami systémov riadenia ISO (8).

Úlohou tejto normy je poskytovať odporúčania ako aplikovať vyprané opatrenia z ČSN ISO/IEC 27002:2014 v rámci procesov ustanovenia, prevádzky, údržby a zlepšovania systému riadenie bezpečnosti informácií. Podľa tejto normy môžu organizácie tiež definovať rozsah a hranice ISMS a nechať si svoj systém podľa nej aj certifikovať (8).

Certifikát bude platný len na oblasti špecifikované v rozsahu ISMS. V prílohe tejto normy sú uvedené aj ciele opatrení a konkrétne opatrenia z ČSN ISO/IEC 27002:2014 (8).

ČSN ISO/IEC 27002:2014

Informačné technológie – Bezpečnostné techniky – Súbor postupov pre opatrenia bezpečnosti informácií

V roku 2007 sa pôvodne britská norma ISO/IEC 17799:2005 prečíslovala na ISO/IEC 27002:2005. Táto norma dostala, rovnako ako ISO/IEC 27001, v roku 2013 svoju novú verziu a v roku 2014 bola po preložení pod označením ČSN ISO/IEC 27002:2014, prevzatá aj do súboru noriem ČSN. Norma predstavuje zbierku najlepších praktík v oblasti informačnej bezpečnosti a v aktuálne platnej verzií obsahuje celkovo 114 rôznych opatrení rozdelených do 14 oblastí. Každé z uvedených opatrení sa ešte ďalej rozpadaná na menšie (špecifickejšie) opatrenia a norma tak odporúča doslova stovky rôznych opatrení (8), (11).

ČSN ISO/IEC 27003:2012

Informačné technológie – Bezpečnostné techniky – Smernica pre implementáciu systému riadenia bezpečnosti informácií

Táto norma predstavuje návod na ustanovenie a implementáciu ISMS, a je použiteľná vo všetkých typoch organizácií, ktoré by chceli zaviesť ISMS. V roku 2017 vydala organizácia ISO najnovšiu verziu tejto normy pod označením ISO/IEC 27003:2017, ktorá ešte nebola prebraná do českého súboru noriem. Najnovšia verzia tejto normy má rovnakú štruktúru ako norma ISO/IEC 27001:2013. Namiesto tejto normy, ktorá je z dôvodu jej využitia na certifikáciu dosť formálna a strohá, ponúka norma ISO/IEC 27013:2017 pragmatické vysvetlenia, jednoduché poradenstvo a usmernenia pre tých, ktorí by chceli zaviesť ISMS (8),(11).

ČSN ISO/IEC 27004:2011

Informačné technológie – Bezpečnostné techniky – Riadenie bezpečnosti informácií - Meranie

V tejto norme sa nachádzajú odporúčania pre používanie a vývoj metrík, pre meranie účinnosti zavedeného ISMS a meranie účinnosti zavedených opatrení alebo skupín

opatrení. Tieto odporúčania sa dajú aplikovať na požiadavky, ktoré tvoria tretiu etapu ISMS cyklu. Aj táto norma má v súčasnosti už svoju druhú medzinárodnú verziu pod označením ISO/IEC 27004/2016, ktorá je rovnako ako ISO/IEC 27003:2017, viac pragmatickejšia a užitočnejšia pre organizácie praktikujúce informačnú bezpečnosť (8), (11).

ČSN ISO/IEC 27005:2013

Informačné technológie – Bezpečnostné techniky – Riadenie rizík bezpečnosti informácií

Úlohou tejto normy je poskytovať odporúčania pre riadenie rizík bezpečnosti informácií, pričom ale neposkytuje žiadnu konkrétnu metodiku, ktorá by sa na riadenie rizík dala použiť. V súlade s prístupom, ktorý je v tejto norme uvedený, je ale možné pre implementáciu požiadaviek ISMS použiť niektorú z celej rady iných metodík pre riadenie rizík (8).

2.2.6. Povinná dokumentácia ISMS

V najnovšej verzií normy ČSN ISO/IEC 27001:2014 sú stanovené povinné dokumenty, či skôr povinne dokumentované informácie, ktoré sú nevyhnutné pre dosiahnutie zhody s normou a pre certifikáciu systému. Patrí tam (12):

- Rozsah ISMS (4.3),
- Politika bezpečnosti informácií (5.2),
- Proces posudzovania rizík bezpečnosti informácií (6.1.2),
- Proces ošetrenia rizík bezpečnosti informácií (6.1.3),
- Prehlásenie o aplikovateľnosti (6.1.3 d),
- Ciele bezpečnosti informácií (6.2),
- Dôkazy o kompetencií osôb vykonávajúcich prácu, ktorá má vplyv na výkonnosť bezpečnosti informácií (7.2),
- Dokument preukazujúci realizáciu procesov, tak ako sú plánované (8.1),
- Výsledky posudzovania rizík bezpečnosti informácie (8.2),
- Výsledky ošetrenia rizík bezpečnosti informácie (8.3),
- Výsledky monitorovania a merania (9.1),
- Program auditov a výsledky auditov (9.2),

- Výsledky preskúmavania vedením (9.3),
- Výsledky nápravných opatrení (10.1 g),
- Definícia bezpečnostných rolí a ich povinností (A.7.1.2 a A.13.2.4),
- Zoznam aktív (A.8.1.1),
- Prípustné použitie aktív (A.8.1.3),
- Politika riadenia prístupu (A.9.1.1),
- Dokumentácia prevádzkových postupov (A.12.1.1),
- Princípy inžinierstva bezpečných systémov (A.14.2.5),
- Politika bezpečnosti informácií pre oblasť vzťahov s dodávateľmi (A.15.1.1),
- Postupy riadenia odozvy na incidenty bezpečnosti informácií (A.16.1.5),
- Procesy k zaisteniu kontinuity činnosti (A.17.1.2),
- Všetky zákonné, predpisové, zmluvné požiadavky príslušnej legislatívy a prístup organizácie ku splneniu týchto požiadaviek. (A.18.1.1),
- Záznamy (logy) o činnostiach a bezpečnostných udalostí od užívateľov a administrátorov (A.12.4.1 a A12.4.3).

Označenie v zátvorke udáva, ku ktorej požiadavke v rámci normy ČSN ISO/IEC 27001:2014 sa viaže daná dokumentácia, pričom dokumentované informácie s označením A (tzn. príloha A tejto normy), sú povinné len ak existuje riziko, ktoré by vyžadovalo ich implementáciu (12).

2.3. Právne prostredie

V tejto kapitole sa zameriam na zákony a nariadenia, ktoré sú relevantné k náplni tejto diplomovej práce. Budem sa v nej teda venovať smernici Európskeho parlamentu č. 216/1148, známej aj pod názvom NIS, nariadeniu Európskeho parlamentu č. 2016/679, všeobecne označovaného ako nariadenie GDPR, a českému zákonu o kybernetickej bezpečnosti č 181/2014.

Na začiatok je ale potrebné definovať niektoré pojmy, ktoré sa s týmito zákonmi spájajú.

2.3.1. Vymedzenie pojmov

Kybernetický priestor (Cyberspace)

„Digitálne prostredie umožňujúce vznik, spracovanie a výmenu informácií, tvorené informačnými systémami, a službami a sieťami elektronických komunikácií“ (13, str. 70).

Kybernetická bezpečnosť (Cyber security)

„Súhrn právnych, organizačných, technický a vzdelávacích prostriedkov smerujúcich k zaisteniu ochrany kybernetického priestoru“ (13, str. 69).

Na rozdiel od informačnej bezpečnosti, ktorá sa týka len bezpečnosti v rámci organizácie, kybernetická bezpečnosť rozširuje bezpečnostný perimeter na celý kybernetický priestor (10).

Kritická infraštruktúra (Critical infrastructure)

Označuje tú časť infraštruktúry štátu, ktorej nefunkčnosť alebo nesprávna funkčnosť by mala závažný dopad na fungovanie štátu, mohla by ohroziť jeho bezpečnosť a v konečnom dôsledku ohroziť základné životné potreby jeho obyvateľstva (13).

Kritická informačná infraštruktúra (Critical information infrastructure)

Súbor informačných a komunikačných systémov v rámci kritickej infraštruktúry, ktorých nefunkčnosť by mohla ohroziť základné životné potreby obyvateľstva, ich zdravie, bezpečnosť alebo ekonomiku štátu (13).

Kybernetická bezpečnostná udalosť (Cyber security event)

Udalosť, ktorá môže viesť k porušeniu bezpečnostnej politiky, spôsobiť narušenie bezpečnosti informácií v IS, ohroziť bezpečnosť a integritu sietí elektronických komunikácií, alebo narušiť bezpečnosť služieb (1), (13).

Kybernetický bezpečnostný incident (Cyber security incident)

Vzniká ako dôsledok kybernetickej bezpečnostnej udalosti a predstavuje už samotné porušenie alebo bezprostrednú hrozbu porušenia bezpečnostnej politiky, narušenie

bezpečnosti informácií v IS, ohrozenie bezpečnosti a integrity sietí elektronických komunikácií, alebo narušenie bezpečnosti služieb (1), (13).

Významný informačný systém

Predstavuje systém, ktorý spravuje orgán verejnej moci a narušenie jeho bezpečnosti informácií môže obmedziť činnosť tohto orgánu. Ide o systémy, ktoré nepatria do kritickej informačnej infraštruktúry a spĺňajú kritéria uvedené v príslušnej vyhláške (1).

Prevádzkovateľ základných služieb (Operator of essential services)

Subjekt, ktorý poskytuje službu, ktorá má zásadný význam pre fungovanie kľúčových spoločenských alebo ekonomických činnosti, jej poskytovanie je závislé na sieťach a informačných systémoch a prípadný bezpečnostný incident, by mohol ohroziť poskytovanie tejto služby (14).

Poskytovateľ digitálnych služieb (Digital service provider)

„Je každá právnická osoba, ktorá poskytuje digitálnu službu.“ Pričom za digitálnu službu sa v tomto prípade považuje poskytovanie služby v podobe: online trhoviska, internetového vyhľadávača alebo služby cloud computingu (14).

2.3.2. Smernica NIS

Smernica Európskeho parlamentu a rady (EÚ) č. 2016/1148, o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, ktorá bola prijatá 6. júla 2016, je prvým právnym predpisom EÚ o kybernetickej bezpečnosti a jej cieľom je posilniť celkovú úroveň kybernetickej bezpečnosti v ÉU (14).

Pre dosiahnutie týchto cieľom stanovila pre členské štáty nasledujúce povinnosti (14):

- musia prijať národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov,
- musia určiť príslušné vnútroštátne orgány, pre oblasť regulácie, určiť jednotné kontaktné miesta a tímy CSIRT (Computer Security Incident Response Team),
- musia určiť prevádzkovateľov základných služieb, pôsobiacich v stanovených odvetviach,

- musia určiť poskytovateľov digitálnych služieb,
- musia zabezpečiť, aby PZS a PDS prijímali vhodné opatrenia na riadenie rizík súvisiacich s bezpečnosťou ich sietí a IS, a na zabránenie a minimalizovanie vplyvu incidentov ovplyvňujúcich ich IS a siete,
- musia zabezpečiť aby PZS a PDS oznamovali príslušnému úradu alebo jednotke CSIRT incidenty, ktoré majú závažný vplyv na ich fungovanie.

Smernica zároveň pre podporu tohto cieľa, vytvorila skupinu pre spoluprácu a sieť jednotiek CSIRT, ktorých úlohou je uľahčiť strategickú spoluprácu a výmenu informácií medzi jednotlivými členskými krajinami (a ich CSIRT tímami).

Táto smernica vstúpila v platnosť v auguste 2016 a členské štáty majú 21 mesiacov na jej transponovanie do svojich vnútroštátnych právnych predpisov, a ďalších 6 mesiacov na identifikáciu PZS (14).

2.3.3. Kybernetický zákon a kybernetická vyhláška

Súčasťou právneho prostredia Českej republiky je už dnes Zákon o kybernetickej bezpečnosti č. 181/2014 Sb., ktorý bol prijatí 23. júla 2014 a vstúpil v platnosť 1. januára 2015.

K tomuto zákonu patria aj ďalšie zákony, vyhlášky a nariadenia, ktoré ho dopĺňajú:

- Vyhláška č. 316/2014 Sb., o kybernetickej bezpečnosti (VKB),
- Vyhláška č. 317/2014 Sb., o významných informačných systémoch a ich určujúcich kritériách (VVIS),
- Nariadenie vlády č. 432/2010 Sb, o kritériách pre určenie prvku kritickej infraštruktúry (NKI),
- Zákon č. 127/2005 Sb., o elektronických komunikáciách (ZEK) a
- Zákon č. 240/2000 Sb., o krízovom riadení a o zmene niektorých zákonov (KZ).

V súčasnosti je už takmer definitívne schválená novela tohto zákona (ZKB), do ktorej je už transponovaná smernica NIS (viď vyššie). Táto nová verzia tohto zákona si vyžiada aj novelizáciu vyhlášky o kybernetickej bezpečnosti a prijatie vyhlášky o určujúcich

kritériách PZS. Okrem definovania ďalších povinných subjektov, sa v novele zriaďuje aj nový úrad s názvom *Národní úřad pro kybernetickou a informační bezpečnost.* Tento nový úrad vznikne oddelením pôvodného *Národního centra kybernetické bezpečnosti* (NCKB – vládny CERT Českej republiky) od *Národního bezpečnostního úřadu* (15).

Novelizovaný KBZ tak definuje osem typov povinných orgánov/osôb. Najviac požiadaviek v rámci KZB a VKB je stanovených pre správcov a prevádzkovateľov informačného alebo komunikačného systému kritickej informačnej infraštruktúry. Pre zistenie, či organizácia do KII patrí sa používa KZ, ktorý definuje kritickú infraštruktúru, a NKI, ktoré určuje kritéria pre KI aj pre KII.

Novelizovaný KBZ zároveň predpisuje rovnaké povinnosti aj pre správcu a prevádzkovateľa IS základnej služby (IS ZS), a očakáva sa to aj v rámci novelizovanej VKB. K určovaniu PZS sa bude používať nová vyhláška, ktorá v súčasnosti ešte nie je pripravená.

Pre určenie VIS, ktorej správca a prevádzkovateľ má o niečo menej povinností ako predchádzajúce typy subjektov, sa používa VVIS, ktorá určuje kritéria pre ich posudzovanie.

Ďalším povinnými orgánmi/osobami v rámci KBZ sú:

- osoba alebo orgán zaisťujúca významnú sieť (VS) a
- poskytovateľ služby elektronických komunikácií a subjekt zaisťujúci sieť elektronických komunikácií (EK),

pričom definícia týchto osôb je uvedená v KBZ s odkazom na ZEK, ktorý definuje elektronické komunikácie.

Posledným povinným subjektom je PDS, ktorý je v tejto novele taktiež priamo definovaný.

Jednoduchý prehľad zákonných povinností povinných osôb/orgánov je v nasledujúcej tabuľke.

Tab. č. 1: Povinnosti KBZ

Povinnosť	EK	VS	IS/KS KII, VIS, IS ZS	PZS	PDS
Písmeno § 3 KBZ	a	b	c, d, e, f	g	h
Hlásiť kontaktné údaje národnému CERT	✓	✓	x	x	✓
Hlásiť kontaktné údaje vládnemu CERT	x	x	✓	✓	x
Detekovať kybernetické bezpečnostné udalosti	x	✓	✓	x	x
Hlásiť kybernetické bezpečnostné incidenty[1]	x	✓	✓	x	✓[2]
Zavádzať bezpečnostné opatrenia a viesť o nich dokumentáciu	x	x	✓	x	✓[3]
Zohľadňovať požiadavky vyplývajúce z bezpečnostných opatrení pri výbere dodávateľov pre ich IS alebo KS systém	x	x	✓	x	x
Zavádzať reaktívne opatrenia vydané Úradom	✓[4]	✓[4]	✓	x	x
Zavádzať ochranné opatrenia vydané Úradom	x	x	✓	x	x
Ohlasovať Úradu zavedenie reaktívneho opatrenia a jeho výsledok	✓	✓	✓	x	x

(Zdroj: Vlastné spracovanie podľa (15))

1 = subjekt hlási incident tam, kde je evidovaný (národný alebo vládny CERT) s výnimkou viď 2.

2 = pokiaľ má významný dopad na poskytovanie jeho služieb, hlási to národnému CERT, pokiaľ má významný dopad na kontinuitu poskytovania základnej služby, tak hlási vládnemu CERT.

3 = nie sú dané žiadne konkrétne opatrenia zo strany štátu, PDS prijíma opatrenia, ktoré on považuje za vhodné.

4 = len za stavu kybernetického nebezpečia alebo za núdzového stavu vyhláseného na základe žiadosti podľa § 21 odstavec 6.

Pričom, zavádzaním bezpečnostných opatrení je myslené (okrem PDS) plnenie povinnosti, ktoré má subjekt predpísané vo VKB.

2.3.4. Nariadenie GDPR

Posledným právnym predpisom, ktorému sa v teoretickej časti práci budem venovať je Nariadenie Európskeho parlamentu a rady (EÚ) č. 2016/679, o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov a o voľnom pohybe týchto údajov, ktorý sa označuje aj skratkou GDPR. Toto nariadenie, ktoré bolo prijaté 27. apríla 2016, je všeobecne záväzný právny akt, čo znamená, že je priamo uplatniteľný v celej EÚ a nie je tak nevyhnutné ho najprv transponovať do právnych predpisov jednotlivých krajín. Z tohto dôvodu sa budú musieť všetky firmy, inštitúcie, ale aj jednotlivci a online služby, ktoré spracovávajú osobné údaje občanov EÚ, od 25. mája 2018 (začiatok platnosti) týmto nariadením riadiť.

Firmy sa musia pri ochrane osobných údajov riadiť zásadou zámernej a štandardnej ochrany (Data protection by design and by default), čo znamená uvažovať o bezpečnosti už pri návrhu systému na spracovanie osobných údajov a aplikovať také opatrenia, ktoré zaručia vysokú mieru bezpečnosti týchto dát (z pohľadu dostupnosti, dôvernosti a integrity). Taktiež musí byť zaistené, že sa pri každom spracovaní osobných údajov používajú len údaje, ktoré sú pre dané spracovanie nevyhnutné. Organizácia by k zaisteniu tejto zásady mala, okrem iného, implementovať pneudoanonimizáciu a šifrovanie osobných údajov (5).

Toto nariadenie dáva občanom EÚ:

- právo na opravu – správca musí opraviť nepresné, alebo dohniť neúplné osobné údaje, ak o to subjekt údajov požiada,
- právo na výmaz (právo byť zabudnutý) – správca musí vymazať osobné údaje, ak o to subjekt údajov požiada a neexistuje právny dôvod na ich držanie,
- právo na obmedzenie spracovania – správca musí obmedziť spracovanie osobných údajov, ak o to subjekt údajov požiada a je na to legitímny dôvod,
- právo na prenositeľnosť údajov – správca musí poskytnúť všetky osobné údaje v zrozumiteľnej a použiteľnej podobe, ak o to subjekt údajov požiada,
- právo vzniesť námietku – správca nemôže spracovávať osobné údaje, ak subjekt údajov proti tomu vznesie námietku a neexistujú legitímne dôvody pre toto spracovanie,

- právo nebyť predmetom žiadneho rozhodnutia založeného výhradne na automatickom spracovaní.

Správcovia musia viesť záznamy o činnostiach spracovania a, ak je to potrebné, pred spracovaním osobných údajov vypracovať posúdenie vplyvu na ochranu osobných údajov (Data Proteciton Impact Assessment). Všetci väčší spracovatelia osobných údajov majú taktiež povinnosť vymenovať poverenca pre ochranu osobných údajov – Data Protection Officer (DPO), ktorý by mal byť nezávislý, mal by dohliadať na správne zachádzanie s osobnými údajmi, hlásiť možné porušenia nariadenia a prípadné úniky (5).

Povinnosťou správcov je tiež hlásiť prípadný únik – narušenie bezpečnosti osobných údajov (Data Breach) Úradu pre ochranu osobných údajov a to najneskôr do 72 hodín od jeho zistenia.

V prípade neplnenia povinností, hrozia subjektu, podľa typu porušenia, pokuty až do výšky 20 000 000 Eur alebo, ak sa jedná o podnik, 4 % z celkového ročného celosvetového obrazu za predchádzajúci finančný rok, podľa toho, ktorá suma bude vyššia (5).

3. Analýza súčasného stavu

Analyzovaná spoločnosť pre ktorú v tejto práci navrhujem metodický postup pre posudzovanie výkonnosti firmy z pohľadu informačnej (a kybernetickej) bezpečnosti pôsobí v Českej republike už niekoľko rokov a za ten čas si získala veľké množstvo zákazníkov. Firma tak v súčasnosti patrí v Českej republike k popredným spoločnostiam v oblasti energetiky. Medzi hlavné predmety činnosti firmy tak, vzhľadom na odvetvie v ktorom pôsobí, patrí hlavne výroba, distribúcia a predaj elektrickej energie, ale tiež distribúcia a predaj plynu.

Spoločnosť v súčasnosti svoju činnosť vykonáva v niekoľkých objektoch, ktoré sú umiestnené na rôznych miestach v republike, a zamestnáva viac ako tisíc zamestnancov, pracujúcich na rôznych pozíciách. Firmu je tak možné na základe týchto ukazovateľov a aj z hľadiska právnych definícií označiť za veľký podnik. To so sebou, mimo typických komplikácií spojených s manažovaním rozsiahlejších firiem, prináša aj ďalšie problémy spojené s riadením bezpečností informácií.

Pre spoločnosť je potrebné udržiavať úroveň bezpečnosti informácií na vysokej úrovni a to nie len z dôvodu zachovania dôvernosti interných procesov (a aktív všeobecne), ale aj z dôvodu následkov, ktoré by prípadný bezpečnostný incident mohol mať. Nehovoriac o povinnostiach vyplývajúcich zo schválených právnych predpisov (viď teoretická časť práce) týkajúcich sa informačnej (a najmä kybernetickej) bezpečnosti a ochrany osobných údajov.

Aj napriek vážnym dopadom, ktoré v prípade neriešenia informačnej bezpečnosti môžu nastať, firma do tejto oblasti neinvestuje primerané množstvo prostriedkov, čoho dôsledok je aj skutočnosť, že mnohé oblasti informačnej bezpečnosti nie sú dostatočne riešené. Mimo toho, že nemá zavedené ISMS ani v rozsahu, ktorý by pokrýval najkritickejšie prvky (aktíva) organizácie, tak nemá uspokojivo vyriešenú ani oblasť fyzickej bezpečnosti a bezpečnosti prostredia. To je vzhľadom na skutočnosť, že narušenie fyzickej bezpečnosti predstavuje pomerne veľkú hrozbu a incident v odvetví

v ktorom firma pôsobí môže mať veľký dopad, dosť nevhodný stav. Ani ďalšie oblasti nie sú pokryté v dostatočnej miere, čo ďalej zvyšuje možné riziko narušenia.

Firma sa preto (dosť veľkú úlohu v tom určite zohrali aj prijaté zákony, vyhlášky a nariadenia) rozhodla celú situáciu okolo informačnej (a kybernetickej) bezpečnosti riešiť vo väčšej miere. Pre zistenie súčasného stavu, ako na tom vlastne z pohľadu plnenia kybernetického zákona a celkovo systému riadenia bezpečnosti informácií sú, kde majú nedostatky, čo musia zaviesť a vylepšiť, by potrebovali navrhnúť metodiku, ktorá im to umožní.

Cieľom tejto novej metodiky byt teda malo byť zisťovanie úrovne výkonnosti na základe riadenia informačnej bezpečnosti. Tento ukazovateľ by im pomohol zhodnotiť súčasný stav a po implementácií nových opatrení budú môcť, podľa zmeny tohto ukazovateľa, posúdiť ako veľmi sa ich úroveň od posledného zisťovania zmenila.

4. Návrh riešenia

Praktická časť diplomovej práce sa teda zaoberá návrhom tohto metodického postupu, pričom výsledný ukazovateľ výkonnosti bude vychádzať:

- z miery plnenia požiadaviek daných v novelizovanej podobe Kybernetického zákona (v ktorom už je transponovaná Smernica Európskeho parlamentu a rady č. 2016/1148, známa aj pod skratkou NIS),
- miery zavedenia opatrení ISMS,
- a pripravenosti firmy na požiadavky dané Nariadením Európskeho parlamentu a rady č. 2016/679 (GDPR).

Táto metodika by mala byť čo najuniverzálnejšia a mala by byť aplikovateľná pre čo najširšie spektrum subjektov, najmä s prihliadnutím k rozdeleniu povinných osôb definovaných v rámci kybernetického zákona (viď teoretická časť).

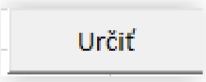
Vzhľadom na univerzálnosť riešenia a relatívnu jednoduchosť aplikovania, ktorú takáto možnosť prináša, som sa rozhodol danú metodiku spracovať v prostredí programu Microsoft Excel za použitie programovacieho jazyka VBA.

V nasledujúcich podkapitolách teda budem popisovať jednotlivé časti tohto riešenia, ako celý proces určovania výkonnosti funguje, čo je jeho výsledkom a ako ho interpretovať.

4.1. Určenie povinnej osoby a/alebo rozsahu hodnotenia

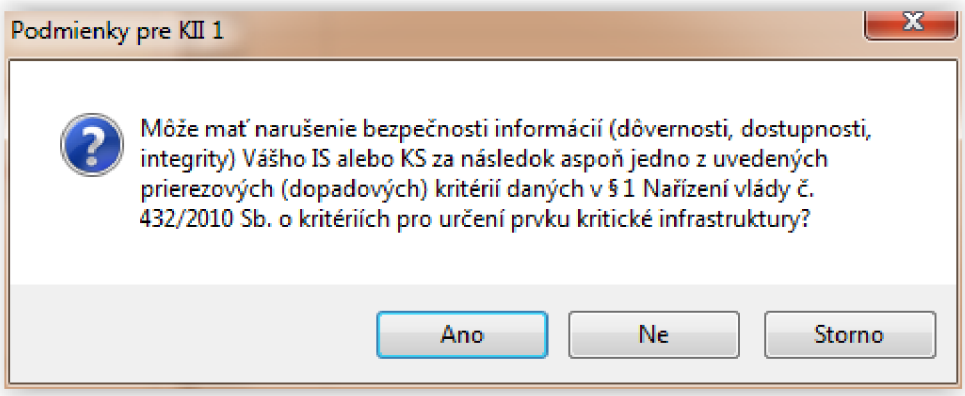
Prvou fázou v rámci metodiky je určenie, ktoré konkrétne oblasti chce organizácia ohodnotiť (KBZ, ISMS, GDPR), respektíve, či a do ktorej skupiny povinných osôb (definovaných v rámci KBZ) patrí, a tým pádom, aké požiadavky v rámci tohto zákona a vyhlášky sa na ňu vzťahujú.

Vykonávanie tejto fázy sa začne stlačením tlačidla označeného ako „Určiť“.



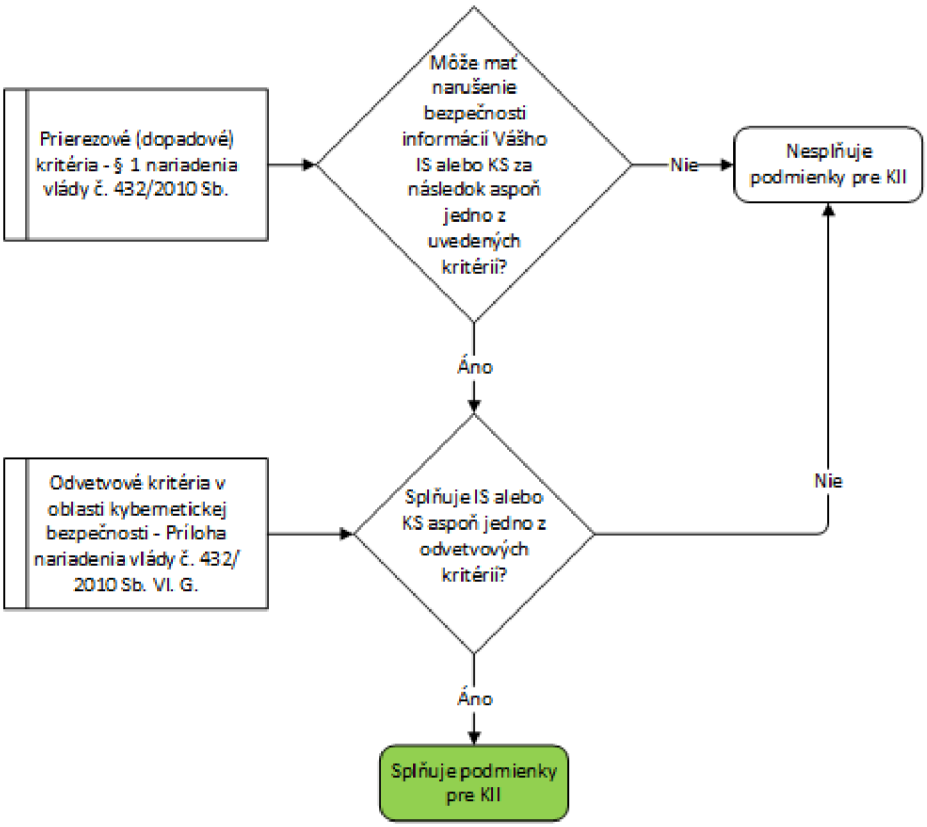
Obrázok č. 3: Určenie rozsahu hodnotenia (Zdroj: Vlastné spracovanie)

Následne sa spustí séria otázok, ktoré pomôžu firme určiť do ktorej skupiny orgánov/osôb definovaných v rámci § 3 ZKB patria.



Obrázok č. 4: Prvá otázka v rámci určovania (Zdroj: Vlastné spracovanie)

Najprv sa zisťuje, či je firma definovaná ako správca / prevádzkovateľ informačného alebo komunikačného systému kritickej informačnej infraštruktúry, pretože ten má, v rámci KBZ a VKB, určených najviac povinností. Toto zisťovanie prebieha podľa diagramu znázorneného nižšie.

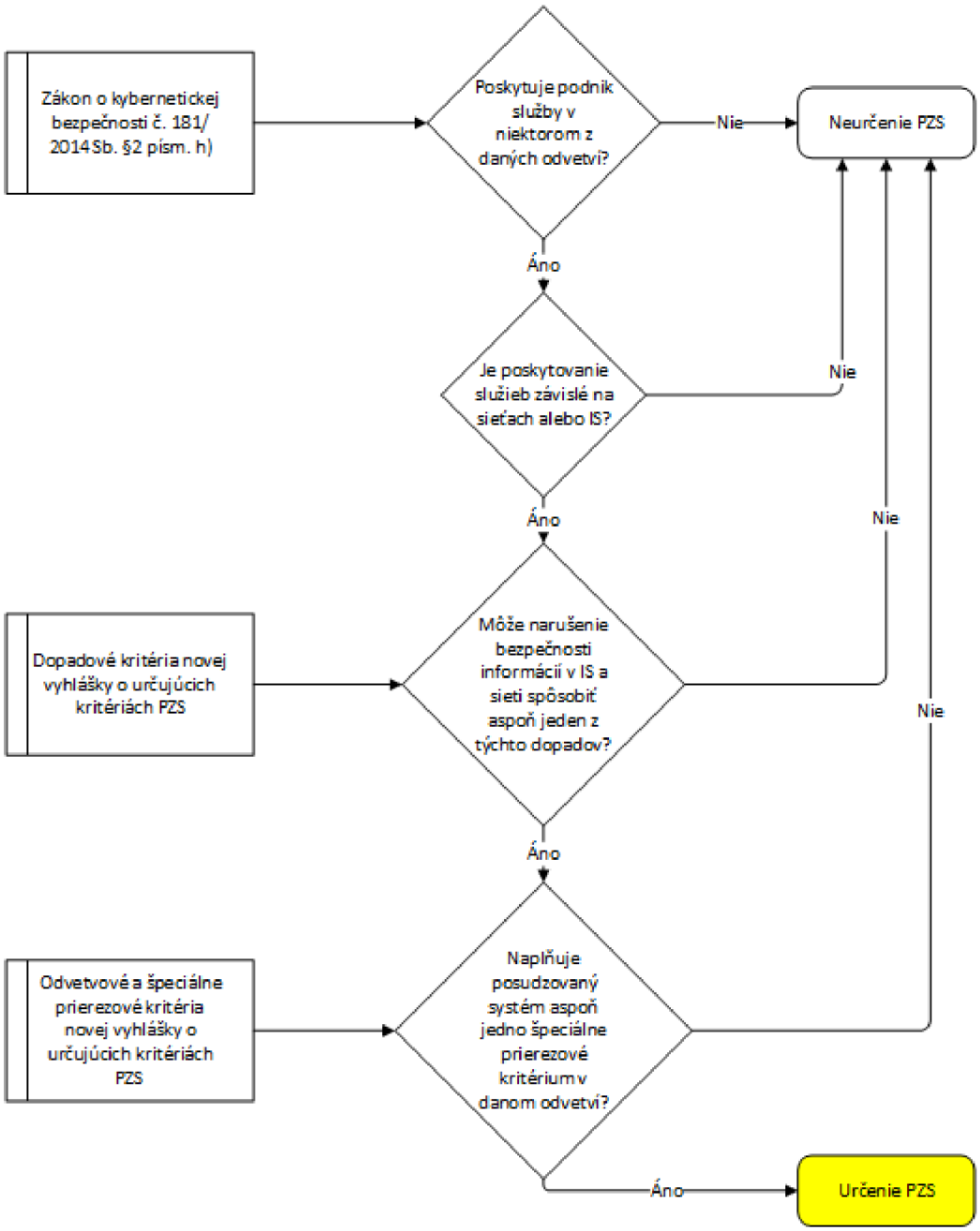


Obrázok č. 5: Proces zisťovania prvku KII (Zdroj: Vlastné spracovanie)

Ak firma spĺňa podmienky pre KII, oznámi sa táto skutočnosť pomocou MsgBoxu a ďalšie otázky týkajúce sa povinných osôb/orgánov budú preskočené, vzhľadom na to, že požiadavky pre ďalšie povinné subjekty sú menšie, nanajvýš rovnaké ako na správcu / prevádzkovateľa IS alebo KS KII.

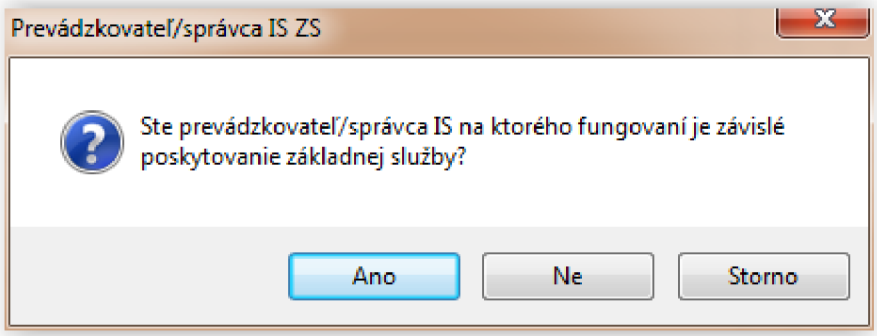
Ak firma podmienky pre KII nespĺňa (opäť MsgBox o tejto skutočnosti), tak sa prechádza na druhú sériu otázok, ktoré pomáhajú v určení prevádzkovateľa základných služieb (nový subjekt transponovaný z NIS) .

Nasledujúci diagram zobrazuje proces určovania PZS.



Obrázok č. 6: Proces určovania PZS (Zdroj: Vlastné spracovanie)

Pri splnení podmienok pre určenie ako PZS, sa (po typickom MsgBoxe informujúcom o tejto skutočnosti) zobrazí ešte jedna dodatočná otázka, ktorá (vzhľadom na skutočnosť, že v rámci novely ZKB je samotnému PZS a prevádzkovateľovi / správcovi IS PZS uložený iný rozsah povinností) určí, či sa jedná o osobu/orgán definovanú v § 3 písmena f) alebo g).

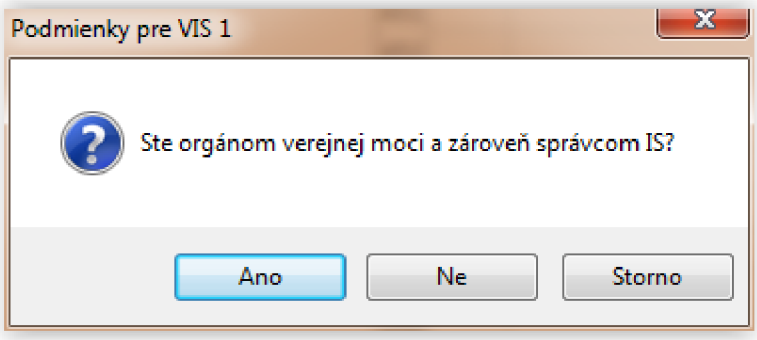


Obrázok č. 7: Otázka o IS PZS (Zdroj: Vlastné spracovanie)

Bez ohľadu na odpoveď na túto otázku sú ďalšie otázky o povinných osobách preskočené a organizácia sa tak považuje za prevádzkovateľa / správcu IS PZS (ak odpoveď bola áno) alebo iba za samotného PZS (odpoveď bola nie).

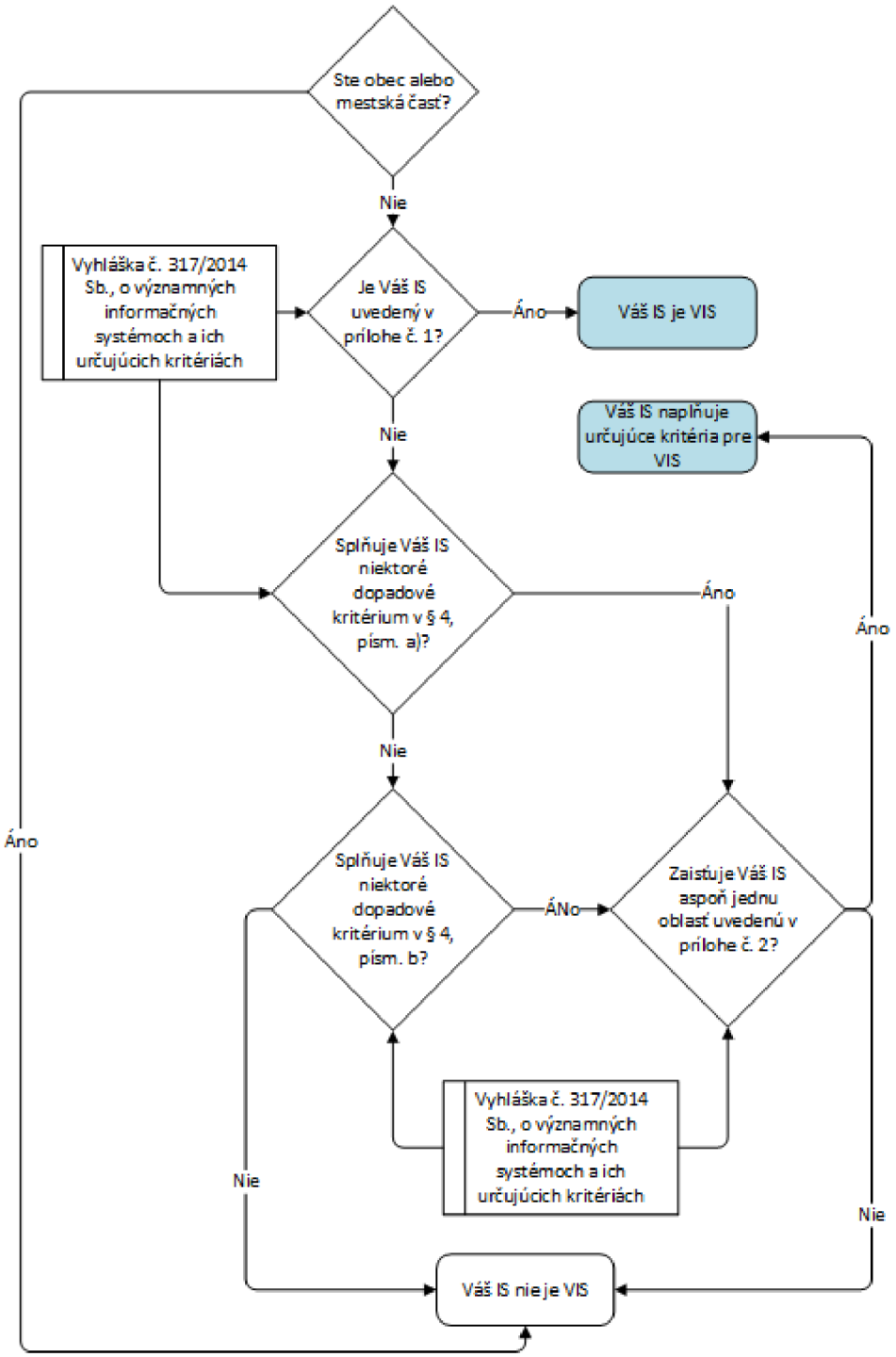
Ak neboli splnené podmienky pre určenie ako PZS (opäť MsgBox), tak sa následne zisťuje, či sa jedná o prevádzkovateľa / správcu významného informačné systému.

Vzhľadom na to, že prevádzkovateľom / správcom VIS môže byť len orgán verejnej moci je prvá otázka zrejmá.



Obrázok č. 8: Zásadná otázka k určeniu VIS (Zdroj: Vlastné spracovanie)

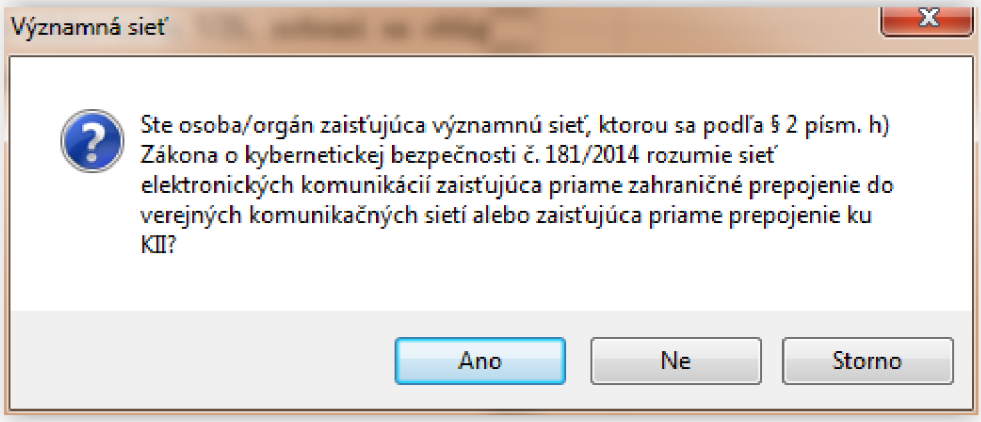
Ak je odpoveď záporná, zobrazí sa MsgBox informujúci o tom, že váš IS nie je VIS a pokračuje sa na otázky o ďalších kategóriách povinných osôb. Ak bola odpoveď kladná pokračuje sa ďalšími otázkami, ktorých odpovede určia, či sa jedná o VIS alebo nie. Samotný priebeh otázok je opäť zaznamenaný na nasledujúcom diagrame.



Obrázok č. 9: Proces určovania VIS (Zdroj: Vlastné spracovanie)

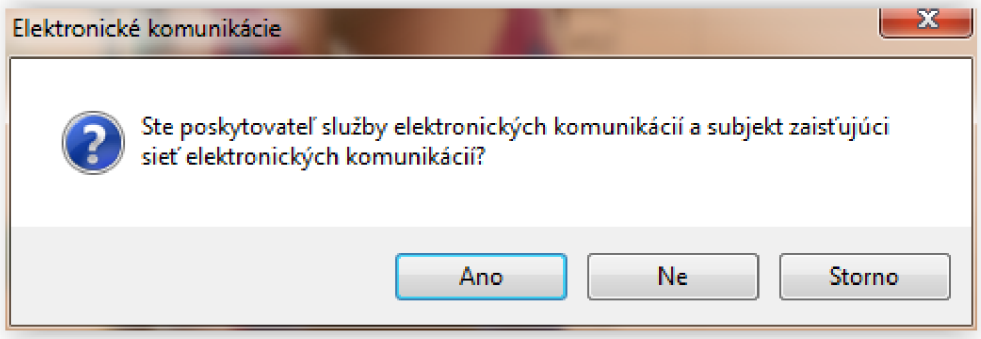
Ak výsledkom tohto procesu bude konštatovanie, že sa naozaj jedná o správcu / prevádzkovateľa VIS, zobrazí sa obligátny MsgBox informujúci o tejto skutočnosti a ďalšie otázky o povinných osobách sa opäť preskočia.

V prípade, že nejde o správcu / prevádzkovateľa VIS, pokračuje sa na otázku o tom, či sa jedná alebo nejedná o osobu definovanú ako orgán/osoba zaisťujúca významnú sieť.



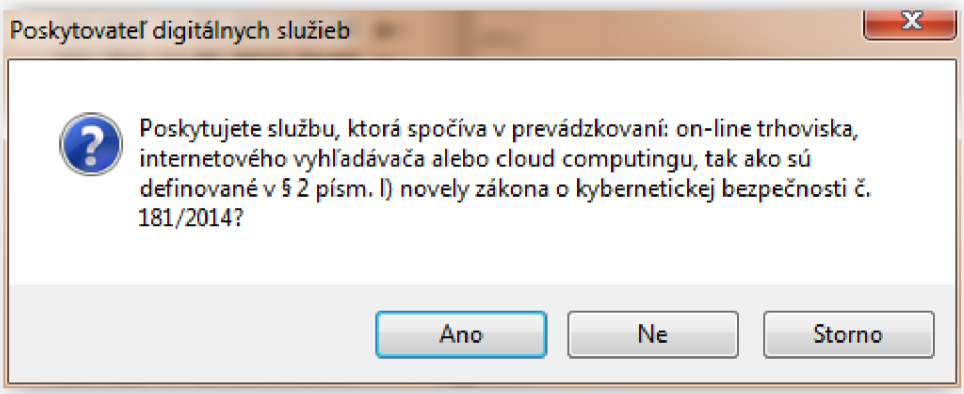
Obrázok č. 10: Osoba zaisťujúca VS (Zdroj: Vlastné spracovanie)

Odpoveďou v tomto prípade môže byť len „Áno“, v tom prípade sa ďalšie otázky (pre určovanie povinných osôb) preskočia, alebo „Nie“ a pokračuje sa na otázku, či sa nejedná o poskytovateľa služby elektronických komunikácií a subjekt zaisťujúci elektronickú komunikáciu.



Obrázok č. 11: Osoba zaisťujúca EK (Zdroj: Vlastné spracovanie)

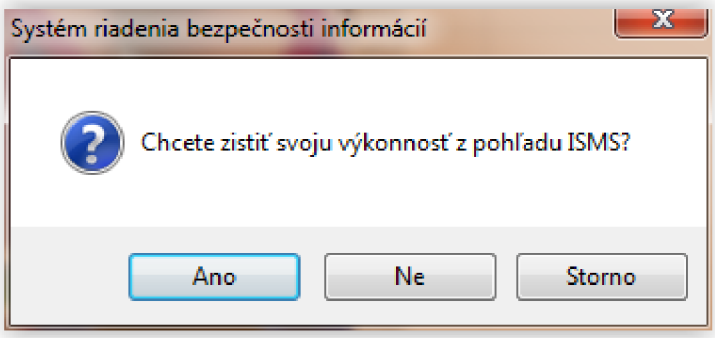
Aj v tomto prípade môže byť len jednoznačná odpoveď „Áno“, v rámci KBZ je teda definovaná ako povinná osoba podľa § 3 písm. a), alebo „Nie“ a v tom prípade sa pokračuje na otázku o tom, či sa ide o posledný typ povinnej osoby: poskytovateľa digitálnych služieb (ďalší subjekt transponovaný z NIS).



Obrázok č. 12: Poskytovateľ digitálnych služieb (Zdroj: Vlastné spracovanie)

Ak ani na túto otázku nebude odpoveď kladná tak s veľkou pravdepodobnosťou firma (organizácia) nemá žiadne povinnosti vyplývajúce z kybernetického zákona ani príslušnej vyhlášky, čo jej je prostredníctvom MsgBoxu aj oznámené.

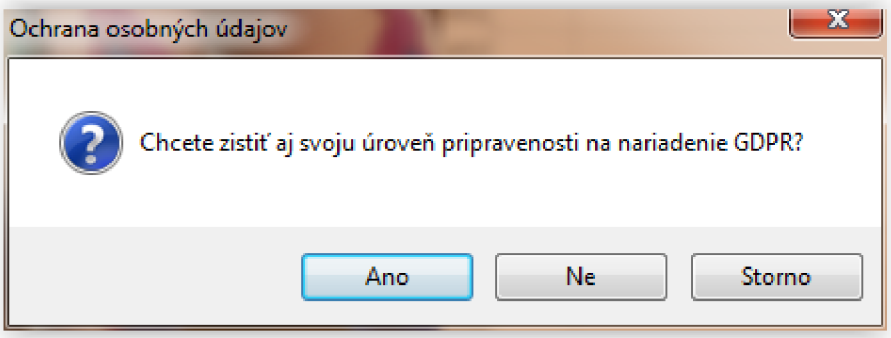
Bez ohľadu na to, aký bude výsledok procesu určovania povinnej osoby, tzn. či bude firma patriť do nejakej skupiny definovaných povinných osôb / orgánov v rámci KBZ alebo nie, tak ďalšia otázka sa bude týkať ISMS.



Obrázok č. 13: Otázka o overení výkonnosti ISMS (Zdroj: Vlastné spracovanie)

V prípade, že nechcete svoju výkonnosť z pohľadu ISMS zmerať a vyberiete teda možnosť „Nie“, tak sa po ukončení prvej fázy nezobrazia otázky týkajúce sa ISMS a budú zobrazené (podľa toho či máte nejaké povinnosti v rámci KBZ), len povinnosti dané ZKB (prípadne aj GDPR, viď nižšie). Ak bude vybraná možnosť „Áno“, tak sa zobrazia aj otázky týkajúce sa ISMS.

Po tejto otázke (ak sa nezruší) nasleduje posledná.



Obrázok č. 14: Otázka o overení výkonnosti GDPR (Zdroj: Vlastné spracovanie)

Tá je zameraná na nariadenie GDPR (viď teória), a dáva možnosť zvoliť si, či chcete v ďalšej fáze metodiky zisťovať aj svoju úroveň pripravenosti na toto nariadenia, alebo sa otázky z tohto okruhu nemajú zobraziť.

Podľa toho, ktoré možnosti v tejto fáze metodiky boli vybrané, teda či:

- ste niektorá z povinných osôb/orgánov definovaná v § 3 ZKB a ak áno tak ktorá,
- chcete zmerať svoju výkonnosť aj v rámci ISMS,
- chcete zmerať svoju úroveň pripravenosti na nariadenie GDPR,

sa zobrazia len otázky, ktoré súhlasia s vašim výberom. Všetky kombinácie týchto okruhov sú dovolené, čo znamená, že môžu byť vybrané všetky, dva, alebo len jeden z nich.

Ku každej otázke sa zároveň vygenerujú tri OptionButtony (prepínače) a v pravom hornom rohu sa zapíšu možnosti, ktoré boli vybrané, to znamená - vaše postavenie v rámci KBZ (N/A = žiadne povinnosti), či ste si vybrali ISMS a/alebo GDPR.

Taktiež sa do stĺpca J a K zapíšu tri riadky s hodnotami, ich význam bude popísaný až v jednej z ďalších podkapitol.

4.2. Požiadavky kybernetického zákona a vyhlášky

Ďalšiu fázou metodiky pre zisťovanie úrovne výkonnosti podniku je pomocou vygenerovaných prepínačov (OptionButton) vybrať pri každej požiadavke/opatrení možnosť, ktorá najviac vystihuje realitu jej splnenia.

Možnosti, ktoré sú na výber, sú:

- splnené – 1. možnosť,
- čiastočne splnené – 2. možnosť,
- a nesplnené – 3. možnosť.

Pričom, teraz sa vrátim k tým hodnotám vygenerovaným v stĺpci J a K, firma, v prípade potreby, môže zmeniť predvolenú hodnotu významu jednotlivých možností.

Tab. č. 2: Hodnotenie odpovedí

Odpoveď	Hodnota
Splnené	100%
Čiastočne splnené	50%
Nesplnené	0%

(Zdroj: Vlastné spracovanie)

Ak by chcela zmeniť hodnotu, ktorá predstavuje odpoveď „Čiastočne splnené“, z predvolenej hodnoty 50% na napríklad 40%, čo by podľa nej lepšie vystihovalo úroveň splnenia, má tu možnosť a uvedenú hodnotu stačí iba prepísať. Toto hodnotenie platí, ale celkovo pre všetky odpovede (vrátane tých z iných okruhov), takže je s tým potrebné počítať. Taktiež je tu možnosť zmeniť hodnotenie odpovedí „Splnené“ a „Nesplnené“, čo ale, vzhľadom na význam daných možností, asi nebude vhodné. Zmena hodnoty ktorejkoľvek z daných možností, samozrejme, ovplyvní aj celkové hodnotenie výkonnosti.

4.2.1. Všeobecné požiadavky podľa kybernetického zákona

V tejto časti je potrebné odpovedať na to, ktoré „všeobecné“ požiadavky dané v rámci samotného kybernetického zákona boli doteraz splnené a v akej miere (splnené, čiastočne splnené, nesplnené).

Pre ukážku funkčnosti metodiky som v prvej fáze zvolil ako typ subjektu správca / prevádzkovateľ IS/KS KII, zobrazené povinnosti preto v tejto, ako aj v ďalších častiach práce, prislúchajú k danému typu povinnej osoby.

Váha	Požiadavka / opatrenie	S	ČS	N
	Všeobecné požiadavky podľa KBZ			
2	Vládnemu CERT (NCKB) boli nahlásené kontaktné údaje.	◉	○	○
2	Detekujú sa kybernetické bezpečnostné udalostí.	◉	○	○
2	Kybernetické bezpečnostné incidenty sú hlásené CERT.	○	◉	○
2	Sú zavádzané bezpečnostné opatrenia a vedie sa o nich dokumentácia.	○	◉	○
2	Pri výbere dodávateľov pre IS alebo KS sa zohľadňujú požiadavky vyplývajúce z bezpečnostných opatrení.	○	◉	○
2	Sú zavádzané reaktívne opatrenia vydávané Úradom.	○	○	◉
2	Sú zavádzané ochranné opatrenia vydávané Úradom.	○	○	◉
2	Zavedenie reaktívneho opatrenia je ohlasované Úradu spolu s jeho výsledkom.	○	○	◉

Obrázok č. 15: Všeobecné požiadavky (Zdroj: Vlastné spracovanie podľa (1))

Všetky tieto požiadavky boli spracované na základe novely kybernetického zákona. Jednoduchý prehľad o tom, ktorý povinný orgán/osoba má v rámci kybernetického zákona aké povinnosti, je možné nájsť v teoretickej časti práce.

Vzhľadom na typ subjektu sa vo všeobecných požiadavkách nezobrazuje povinnosť *„Národnému CERT (CSIRT.CZ) boli nahlásené kontaktné údaje.“*, keďže, ako je vidieť aj v prehľade v teoretickej časti práce, správcovia / prevádzkovatelia IS/KS KII (ako aj ďalšie osoby/orgány) hlásia údaje vládnemu CERT a nie národnému CERT.

Za pozornosť stojí aj stĺpec označený ako „Váha“, hodnoty v tomto stĺpci predstavujú akúsi dôležitosť (váhu) danej požiadavky na hodnotení výkonnosti v rámci danej časti

(Všeobecné požiadavky) aj v rámci daného celku (Kybernetický zákon). Ak teda firma bude niektorú požiadavku považovať za viac dôležitú ako ostatné, môže jej priradiť väčšiu váhu a jej splnenie sa bude na ukazovateli výkonnosti podieľať väčšou mierou ako iné (tie s nižšou váhou). V prípade, ak firma nejakú požiadavku plniť nechce, alebo nemôže (je neaplikovateľná), môže tejto požiadavke priradiť hodnotenie 0 a ukazovateľ výkonnosti tak jej nesplnenie vôbec neovplyvní.

Ja som všetkým všeobecným požiadavkám priradil, ako je vidieť aj na obrázku, hodnotenie 2.

4.2.2. Organizačné opatrenia

Vyhláška č. 316/2014 Sb. o kybernetickej bezpečnosti, predpisuje bezpečnostné opatrenia, ktoré by IS KII, KS KII, IS PZS a VIS mali aplikovať a rozsah ich zavedenia. Tieto opatrenia sú rozdelené na dve časti – organizačné a technické opatrenia. Podľa jednotlivých paragrafov tejto vyhlášky som vytvoril zoznam povinností, ktoré musia dané povinné osoby plniť, pričom IS KII, KS KII a IS PZS musia plniť takmer všetky povinnosti dané touto vyhláškou a VIS len ich väčšiu časť.

	§ 3 VKB - Systém riadenia bezpečnosti informácií			
2	Je stanovený rozsah a hranice ISMS.	○	○	◉
2	Je zavedený proces riadenia rizík.	◉	○	○
2	Je vytvorená, schválená a nasadená bezpečnostná politika v oblasti ISMS, a zavedené príslušné opatrenia.	○	◉	○
2	Je zavedený proces monitorovania účinnosti bezpečnostných opatrení.	◉	○	○
2	Je zavedený proces vyhodnocovania vhodnosti a účinnosti bezpečnostnej politiky.	○	◉	○
2	Vykonáva sa audit kybernetickej bezpečnosti aspoň 1-krát ročne.	○	○	◉
2	Je zaistené vyhodnocovanie účinnosti ISMS, ktoré obsahuje hodnotenie stavu ISMS, vrátane revízie hodnotenia rizík, posúdenia výsledkov kontrol a auditov kybernetickej bezpečnosti a dopadov KBI na ISMS, a to najmenej 1-krát ročne.	○	◉	○
2	Je ISMS a príslušná dokumentácia aktualizovaná na základe zistení auditov kybernetickej bezpečnosti, výsledkov hodnotenia účinnosti ISMS, a v súvislosti s uskutočňovanými zmenami.	○	○	◉
2	Riadi sa prevádzka a zdroje ISMS, zaznamenávajú sa činnosti spojené s ISMS a riadením rizík.	○	○	◉

Obrázok č. 16: VKB - § 3 (Zdroj: Vlastné spracovanie podľa (2))

Vzhľadom na to, že, ako už bolo spomenuté, som pre testovanie metodiky zvolil v prvej fáze ako povinnú osobu správcu / prevádzkovateľa IS/KS KII, tak zobrazené požiadavky odpovedajú povinnostiam platným pre tento typ subjektu.

Tretí paragraf tejto vyhlášky obsahuje požiadavky týkajúce sa systému riadenia bezpečnosti informácií, rieši či má organizácia stanovený rozsah a hranice ISMS, schválenú politiku, zavedené opatrenia, či vyhodnocuje účinnosť a ďalšie veci týkajúce sa ISMS. Aj v prípade týchto požiadaviek som sa rozhodol oceniť ich všetky váhou 2.

	§ 4 VKB - Riadenie rizík			
1	Sú stanovené metodiky pre identifikáciu a hodnotenie aktív, a pre identifikáciu a hodnotenie rizík, vrátane stanovených kritérií pre prijateľnosť rizík.	◉	○	○
1	Vykonáva sa identifikácia a hodnotenie dôležitosti aktív, ktoré patria do rozsahu ISMS, podľa § 8 VKB minimálne v rozsahu prílohy č. 1 VKB a výstupy sú zapracované do správy o hodnotení aktív a rizík.	○	◉	○
1	Vykonáva sa identifikácia rizík, pri ktorej sa zohľadnia hrozby a zraniteľnosti, posúdia možné dopady na aktíva, ohodnotia sa tieto riziká minimálne v rozsahu prílohy č. 2 VKB, sú určené a schválené prijateľné riziká a spracovaná správa o hodnotení aktív a rizík.	○	◉	○
1	Na základe bezpečnostných potrieb a výsledkov hodnotenia rizík je spracované prehlásenie o aplikovateľnosti, ktoré obsahuje prehľad vybraných a zavedených bezpečnostných opatrení	◉	○	○
1	Je spracovaný plán zvládania rizík, ktorý obsahuje ciele a prínosy bezpečnostných opatrení pre zvládanie rizík, určené osoby zodpovedné za presadzovanie bezpečnostných opatrení pre zvládanie rizík, potrebné finančné, technické, ľudské a informačné zdroje, termín ich zavedenia a popis väzieb medzi rizikami a príslušnými bezpečnostnými opatreniami.	○	◉	○
1	Bez zbytočného odkladu sú zohľadňované reaktívne a ochranné opatrenia vydané Úradom v hodnotení rizík a v prípade, že hodnotenie rizík aktualizované o nové zraniteľnosti spojené s realizáciou aktívneho alebo ochranného opatrenia prekročí stanované kritéria pre prijateľnosť rizík, doplní sa plán zvládania rizík.	○	○	◉
1	Riadenie rizík je zaistené iným spôsobom (než ako je stanovené v odstavci 1 § 4 VKB) a je doložené, že použité opatrenia zaisťujú rovnakú alebo vyššiu úroveň riadenia rizík.	○	○	◉

Obrázok č. 17: VKB - § 4.1 (Zdroj: Vlastné spracovanie podľa (2))

	Sú zvažované hrozby, ktoré súvisia s/so:			
1	porušením bezpečnostnej politiky, vykonaním neoprávnených činností, zneužitia oprávnení zo strany užívateľov a administrátorov.	◉	○	○
1	poškodením alebo zlyhaním technického alebo programového vybavenia.	◉	○	○
1	zneužitím identity fyzickej osoby.	○	◉	○
1	užívaním programového vybavenia v rozpore s licenčnými podmienkami.	○	○	◉
1	kybernetickým útokom z komunikačnej siete.	○	◉	○
1	škodlivým kódom (napríklad, vírusy, spyware, trojské kone).	○	○	◉
1	nedostatkami pri poskytovaní služieb IS KII, KS KII, IS PZS alebo VIS.	○	◉	○
1	narušením fyzickej bezpečnosti.	○	○	◉
1	prerušením poskytovaní služieb elektronických komunikácií alebo dodávok elektrickej energie.	◉	○	○
1	zneužitím alebo neoprávnenou modifikáciou údajov.	◉	○	○
1	trvale pôsobiacimi hrozbami.	◉	○	○
1	odcudzením alebo poškodením aktíva.	○	○	○
1	porušením bezpečnostnej politiky, vykonaním neoprávnených činností, zneužitia oprávnení zo strany administrátorov KII alebo IS PZS.	◉	○	○
1	pochybením zo strany zamestnancov.	○	◉	○
1	zneužitím vnútorných prostriedkov, sabotážou.	○	◉	○
1	dlhodobým prerušením poskytovania služieb elektronických komunikácii, dodávky elektrickej energie alebo iných dôležitých služieb.	○	○	○
1	nedostatkom zamestnancov s potrebnou odbornou úrovňou.	◉	○	○
1	cieleným kybernetickým útokom pomocou sociálneho inžinierstva, použitím špionážnych technik.	◉	○	○
1	zneužitím vymeniteľných technických nosičov dát.	○	◉	○
	Sú zvažované zraniteľnosti, ktoré súvisia s/so:			
1	nedostatočnou ochranou vonkajšieho perimetra.	◉	○	○
1	nedostatočným bezpečnostným povedomím užívateľov a administrátorov.	○	◉	○
1	nedostatočnou údržbou IS KII, KS KII, IS PZS alebo VIS.	○	◉	○
1	nevhodne nastavenými prístupovými oprávneniami.	○	○	○
1	nedostatočnými postupmi pri identifikovaní a odhaľovaní negatívnych bezpečnostných javov, kybernetických bezpečnostných udalostí a KBI.	○	◉	○
1	nedostatočným monitorovaním činností užívateľov a administrátorov a neschopnosťou odhaliť ich nevhodné alebo závadné spôsoby chovania.	○	◉	○
1	nedostatočným určovaním bezpečnostných pravidiel, nepresným alebo nejednoznačným vymedzením práv a povinností užívateľov, administrátorov a bezpečnostných rolí.	○	○	◉
1	nedostatočnou ochranou prostriedkov KII alebo PZS.	○	○	◉
1	nevhodnou bezpečnostnou architektúrou.	◉	○	○
1	nedostatočnou mierou nezávislej kontroly.	○	◉	○
1	neschopnosťou včasného odhalenia pochybenia zo strany zamestnancov.	○	○	◉

Obrázok č. 18: VKB - § 4.2 (Zdroj: Vlastné spracovanie podľa (2))

Ďalšou oblasťou, v ktorej vyhláška predpisuje povinnosti, je riadenie rizík. Zisťuje sa, či osoba/orgán má stanovené metodiky na identifikáciu a hodnotenie aktív, rizík a či tieto činnosti podľa týchto metodík aj vykonáva. Taktiež predpisuje aké hrozby a zraniteľnosti by sa mali pri analýze brať do úvahy a aj ďalšie povinnosti súvisiace s managementom rizík. Tieto požiadavky sú ohodnotené už štandardnou váhou 1.

	§ 5 VKB - Bezpečnostná politika			
	Je stanovená bezpečnostná politika v oblastiach:			
2	ISMS.	◉	○	○
2	organizačnej bezpečnosti.	◉	○	○
2	riadenia vzťahov s dodávateľmi.	○	◉	○
2	klasifikácie aktív.	◉	○	○
2	bezpečnosti ľudských zdrojov.	○	◉	○
2	riadenia prevádzky a komunikácií.	◉	○	○
2	riadenia prístupu.	○	◉	○
2	bezpečného chovania užívateľov.	○	○	◉
2	zálohovania a obnovy.	○	◉	○
2	bezpečného predávania a výmeny informácií.	○	○	◉
2	riadenia technických zraniteľností.	◉	○	○
2	bezpečného používania mobilných zariadení.	○	◉	○
2	poskytovania a nadobúdania licencií programového vybavenia a informácií.	○	○	◉
2	dlhodobého ukladania a archivácie informácií.	○	◉	○
2	ochrany osobných údajov.	○	◉	○
2	fyzickej bezpečnosti.	○	◉	○
2	bezpečnosti komunikačnej siete.	○	○	◉
2	ochrany pred škodlivým kódom.	◉	○	○
2	nasadenia a používania nástroja pre detekciu kybernetických bezpečnostných udalostí.	◉	○	○
2	využitia a údržby nástroja pre zber a vyhodnocovanie kybernetických bezpečnostných udalostí.	○	◉	○
2	používania kryptografickej ochrany.	◉	○	○
2	Účinnosť bezpečnostnej politiky je pravidelne hodnotená a aktualizovaná.	○	◉	○

Obrázok č. 19: VKB - § 5 (Zdroj: Vlastné spracovanie podľa (2))

V § 5 vyhláška určuje v akých oblastiach by firma mala mať stanovenú svoju bezpečnostnú politiku. Politiky som, aj vzhľadom na ich dôležitosť pri presadzovaní systému riadenia bezpečnosti informácií, ohodnotil všetky váhou 2.

	§ 6 VKB - Organizačná bezpečnosť			
1	Zavedená organizácia riadenia bezpečnosti informácií, v rámci ktorej je určený výbor pre riadenie kybernetickej bezpečnosti a bezpečnostné role a ich práva a povinnosti súvisiace s IS KII, KS KII, IS PZS alebo VIS.	◉	○	○
1	Je určená bezpečnostná rola: manažér kybernetickej bezpečnosti.	◉	○	○
1	Je určená bezpečnostná rola: architekt kybernetickej bezpečnosti.	○	○	◉
1	Je určená bezpečnostná rola: audítor kybernetickej bezpečnosti.	○	◉	○
1	Je určená bezpečnostná rola: garant aktíva (podľa §2 písm. m).	◉	○	○
1	Je určený výbor pre riadenie kybernetickej bezpečnosti.	○	○	◉
1	Je zaistené odborné školenie osôb, ktoré zastávajú bezpečnostné role v súlade s plánom rozvoja bezpečnostného povedomia (podľa §9 odst. 1b).	◉	○	○

Obrázok č. 20: VKB - § 6 (Zdroj: Vlastné spracovanie podľa (2))

Paragraf šesť predpisuje povinným orgánom/osobám povinnosti v rámci organizačnej bezpečnosti, tzn. určuje, aké bezpečnostné role by mali by stanovené. Tieto požiadavky majú váhu nastavenú na 1.

	§ 7 VKB - Stanovenie bezpečnostných požiadavkou pre dodávateľov			
1	Sú stanovené pravidlá pre dodávateľov, ktoré zohľadňujú potreby riadenia bezpečnosti informácií, a podľa nich sa riadi výber dodávateľov alebo iných subjektov, ktorí sa podieľajú na rozvoji, prevádzke alebo zaistení bezpečnosti IS KII, KS KII alebo VIS. Rozsah zapojenia dodávateľov na rozvoji, prevádzke alebo zaistení bezpečnosti IS KII, KS KII, IS PZS alebo VIS je zadokumentovaný v písomnej zmluve, ktorej súčasťou je ustanovenie o bezpečnosti informácií.	○	◉	○
1	U dodávateľov uvedených v odstavci 1 sa pred uzavretím zmluvy vykonáva hodnotenie rizík (podľa prílohy č. 2 k VKB), ktoré sú spojené s podstatnými dodávkami.	◉	○	○
1	U dodávateľov uvedených v odstavci 1 sa uzatvára zmluva o úrovni služieb, ktorá stanovuje spôsoby a úrovne realizácie bezpečnostných opatrení a určuje vzťah vzájomnej zmluvnej zodpovednosti za zavedenie a kontrolu bezpečnostných opatrení.	○	◉	○
1	U dodávateľov uvedených v odstavci 1 sa pravidelne vykonáva hodnotenie rizík a pravidelná kontrola zavedených bezpečnostných opatrení u poskytovaných služieb a zistené nedostatky odstraňuje, alebo po dohode s dodávateľom zaistí ich odstránenie.	○	○	◉

Obrázok č. 21: VKB - § 7 (Zdroj: Vlastné spracovanie podľa (2))

V tomto paragrafe sa určujú opatrenia vzhľadom na bezpečnosť spojenú s dodávateľmi, o pravidlách pri ich výbere, požiadavkách na nich a ich kontrole. Aj tieto opatrenia dostali váhu 1.

	§ 8 VKB - Riadenie aktív			
1	Sú identifikované a evidované primárne aktíva.	◉	○	○
1	Sú určení garanti aktív, ktorí sú zodpovední za primárne aktíva.	◉	○	○
1	Je hodnotená dôležitosť primárnych aktív z hľadiska dôvernosti, integrity a dostupnosti, a tieto aktíva sú zaradené do jednotlivých úrovní minimálne v rozsahu podľa prílohy č. 1 k VKB.	○	◉	○
	Pri hodnotení dôležitosti primárnych aktív sa posudzuje predovšetkým:			
1	rozsah a dôležitosť osobných údajov alebo obchodného tajomstva.	○	◉	○
1	rozsah dotknutých právnych povinností alebo iných záväzkov.	○	○	◉
1	rozsah narušenia vnútorných riadiacich a kontrolných činností.	○	◉	○
1	poškodenie verejných, obchodných alebo ekonomických záujmov.	○	○	○
1	možná finančná strata.	◉	○	○
1	rozsah narušenia bežných činností orgánu a osoby.	○	◉	○
1	dopad spojený s narušením dôvernosti, integrity a dostupnosti.	◉	○	○
1	dopad na zachovanie dobrého mena alebo ochranu dobrej povesti.	○	◉	○
1	Sú identifikované a evidované podporné aktíva.	◉	○	○
1	Sú určení garanti aktív, ktorí sú zodpovední za podporné aktíva.	○	◉	○
1	Sú určené väzby medzi primárnymi a podpornými aktívami, a hodnotené dôsledky závislostí medzi primárnymi a podpornými aktívami.	○	◉	○
	Sú stanovené pravidlá ochrany, nutné pre zabezpečenie jednotlivých úrovní aktív tým, že:			
1	sú určené spôsoby rozlišovania jednotlivých úrovní aktív.	○	◉	○
1	sú stanovené pravidlá pre manipuláciu a evidenciu s aktívami podľa úrovne aktív, vrátane pravidiel pre bezpečné elektronické zdieľanie a fyzické prenášanie.	◉	○	○
1	sú stanovené prípustné spôsoby používania aktív.	◉	○	○
1	Sú zavedené pravidlá ochrany zodpovedajúce úrovni aktív.	○	◉	○
1	Sú určené spôsoby pre spoľahlivé zmazanie alebo zničenie technických nosičov dát s ohľadom na úroveň aktív.	◉	○	○

Obrázok č. 22: VKB - § 8 (Zdroj: Vlastné spracovanie podľa (2))

Ôsmy paragraf stanovuje pre povinné osoby požiadavky v rámci riadenia aktív, hlavne sa vyžaduje rozdelenie aktív podľa ich dôležitosti, minimálne na úroveň primárne a podporné aktíva, a taktiež mať určených garantov aktív. Opatrenia v tomto prípade majú tiež váhu 1.

	§ 9 VKB - Bezpečnosť ľudských zdrojov			
1	Je stanovaný plán rozvoja bezpečnostného povedomia, ktorý obsahuje formu, obsah a rozsah potrených školení, a sú určené osoby uskutočňujúce realizáciu jednotlivých činnosti, ktoré sú v pláne uvedené.	○	○	◉
1	V súlade s plánom rozvoja bezpečnostného povedomia je zaistené poučenie užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role o ich povinnostiach a o bezpečnostnej politike formou vstupných a pravidelných školení.	◉	○	○
1	Je zaistená kontrola dodržania bezpečnostnej politiky zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role.	○	○	◉
1	Je zaistené vrátenie zverených aktív a odobranie prístupových oprávnení pri ukončení zmluvného vzťahu s užívateľmi, administrátormi alebo osobami zastávajúcimi bezpečnostné role.	◉	○	○
1	O školeniach podľa odstavca 1 sú vedené prehľady, ktoré obsahujú predmet školenia a zoznam osôb, ktoré školenie absolvovali.	○	◉	○
1	Sú stanovené pravidlá pre určenie osôb, ktoré budú zastávať bezpečnostné role, role administrátorov alebo užívateľov.	○	◉	○
1	Je hodnotená účinnosť plánu rozvoja bezpečnostného povedomia, vykonaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia.	◉	○	○
1	Sú určené pravidla a postupy pre riešenie prípadov porušenia stanovaných bezpečnostných pravidiel zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role.	○	◉	○
1	Je zaistená zmena prístupových oprávnení pri zmene postavenia užívateľov, administrátorov alebo osôb zastávajúcich bezpečnostné role.	○	○	◉

Obrázok č. 23: VKB - § 9 (Zdroj: Vlastné spracovanie podľa (2))

Bezpečnosti ľudských zdrojov sa venuje deviati paragraf VKB, jeho obsahom sú hlavne požiadavky na zvyšovanie bezpečnostného povedomia zamestnancov, kontrolu dodržiavania bezpečnostnej politiky zo strany zamestnancov, pravidlá pre určovanie osôb, ktoré budú zastávať bezpečnostné role, a ďalšie opatrenia s tým súvisiace. Váha týchto opatrení je stanovená na 1.

	§ 10 VKB - Riadenie prevádzky a komunikácií			
1	Pomocou technických nástrojov uvedených v § 21 až 23 VKB sú detekované KBU, pravidelne vyhodnocované získané informácie a na zistené nedostatky reagované v súlade s § 13 VKB.	◉	○	○
1	Je zaistená bezpečná prevádzka IS KII, KS KII, IS PZS a VIS. Za týmto účelom sú stanovené prevádzkové pravidlá a postupy.	○	◉	○
	Prevádzkové pravidlá a postupy obsahujú:			
1	práva a povinnosti osôb zastávajúcich bezpečnostné role, administrátorov a užívateľov.	○	◉	○
1	postupy pre spustenie a ukončenie chodu systému, pre reštart alebo obnovenie chodu systému po zlyhaní a pre ošetrenie chybových stavov alebo mimoriadnych javov.	○	○	◉
1	postupy pre sledovanie KBU a pre ochranu prístupu k záznamom o týchto činnostiach.	○	◉	○
1	spojenie na kontaktné osoby, ktoré sú určené ako podpora pri riešení neočakávaných systémových alebo technických problémov.	◉	○	○
1	postupy riadenia a schvaľovania prevádzkových zmien.	○	○	◉
1	postupy pre sledovanie, plánovanie a riadenie kapacity ľudských a technických zdrojov.	◉	○	○
1	Vykonáva sa pravidelné zálohovanie a overovanie použiteľnosti vytvorených záloh.	○	○	◉
1	Je zaistené oddelenie vývojového, testovacieho a produkčného prostredia	○	◉	○
	Sú riešené reaktívne opatrenia vydané Úradom tým, že orgán alebo osoba:			
1	posudzuje očakávané dopady reaktívneho opatrenia na IS KII, KS KII alebo IS PZS a na zavedené bezpečnostné opatrenia, vyhodnocuje možné negatívne účinky a bez zbytočného odkladu ich oznámi Úradu.	○	○	◉
1	stanovuje spôsob rýchleho vykonania reaktívneho opatrenia, ktorý minimalizuje možné negatívne účinky, a určuje časový plán jeho vykonania.	○	○	◉
1	Je zaistená bezpečnosť a integrita komunikačných sietí a bezpečnosť komunikačných služieb podľa § 17 VKB.	○	○	◉
1	Sú určené pravidlá a postupy pre ochranu informácií, ktoré sú prenášané komunikačnými sieťami.	◉	○	○
1	Výmena a odovzdávanie informácií sa vykonáva na základe pravidiel stanovaných právnymi predpismi za súčasného zaistenia bezpečnosti informácií a tieto pravidlá sú zdokumentované.	○	◉	○
1	S ohľadom na klasifikáciu aktív je vykonávaná výmena a odovzdávanie informácií na základe písomných zmlúv, ktorých súčasťou je ustanovenie o bezpečnosti informácií.	○	○	◉

Obrázok č. 24: VKB - § 10 (Zdroj: Vlastné spracovanie podľa (2))

Riadenie prevádzky a komunikácií tak je nazvaný § 10 VKB, v ktorom sú určené požiadavky na detekciou KBU a ich pravidelnú analýzu, čo majú obsahovať prevádzkové

postupy a ako majú byť riešené reaktívne opatrenia vydávané Úradom. Váhu týchto opatrení som taktiež nastavil na 1.

	§ 11 VKB - Riadenie prístupu a bezpečné chovanie užívateľov			
1	Na základe prevádzkových a bezpečnostných potrieb je prístup k IS KII, KS KII, IS PZS a VIS riadený a každému užívateľovi je pridelený jednoznačný identifikátor.	◉	○	○
1	Sú prijaté opatrenia, ktoré slúžia k zaisteniu ochrany údajov, ktoré sú používané pre prihlásenie užívateľov a administrátorov IS KII, KS KII, IS PZS a VIS podľa § 18 a 19 VKB, a ktoré bránia v zneužití týchto údajov neoprávnenou osobou.	○	◉	○
1	Pristupujúcim aplikáciám je pridelený samostatný identifikátor.	○	◉	○
1	Je obmedzené prideľovanie administrátorských oprávnení.	◉	○	○
1	Prideľovanie a odoberanie prístupových opravení je v súlade s politikou riadenia prístupu.	○	◉	○
1	Pravidelne sa vykonáva preskúmavanie nastavení prístupových oprávnení, vrátane rozdelení jednotlivých užívateľov v prístupových skupinách alebo roliach.	◉	○	○
1	Je využívaný nástroj na overovanie identity užívateľov podľa § 18 VKB a nástroj pre riadenie prístupových oprávnení podľa §19.	○	◉	○
1	Sú zavedené bezpečnostné opatrenia potrebné pre bezpečné používanie mobilných zariadení, prípadne i bezpečnostné opatrenia spojené s využitím technických zariadení, ktorými povinná osoba nedisponuje.	○	◉	○

Obrázok č. 25: VKB - § 11 (Zdroj: Vlastné spracovanie podľa (2))

V § 11 sú riešené požiadavky na opatrenia, ktoré majú chrániť autentizačné údaje užívateľov a administrátorov IS KII, KS KII, IS PZS a VIS, vyžaduje sa, aby bolo pravidelné kontrolované nastavenie prístupových oprávnení a aby bol zavedený nástroj na overovanie identity užívateľov. Tieto opatrenia majú váhu nastavenú na 1.

	§ 12 VKB - Akvizícia, vývoj a údržba			
1	Sú stanovené bezpečnostné požiadavky na zmeny IS KII, KS KII, IS PZS alebo VIS spojené s ich akvizíciou, vývojom a údržbou, a sú zahrnuté do projektu akvizície, vývoja a údržby systému.	○	○	◉
1	Sú identifikované, hodnotené a riadené rizika súvisiace s akvizíciou, vývojom a údržbou IS KII, KS KII alebo IS PZS; pre postupy hodnotenia a riadenia rizík sa metodiky podľa § 4 odst. 1 a) obdobne použijú.	○	○	◉
1	Je zaistená bezpečnosť vývojového prostredia a zaistená ochrana používaných testovacích dát.	○	◉	○
1	Je vykonávané bezpečnostné testovanie zmien IS KII, KS KII alebo IS PZS pred ich zavedením do prevádzky.	○	◉	○

Obrázok č. 26: VKB - § 12 (Zdroj: Vlastné spracovanie podľa (2))

Aj povinnosti v rámci § 12 majú určenú váhu 1 a týkajú sa hlavne požiadaviek na bezpečnosť v súvislosti so zmenou systému.

	§ 13 VKB - Zvládanie kybernetických bezpečnostných udalostí a incidentov			
1	Sú prijaté nevyhnutné opatrenia, ktoré zaistia oznamovanie KBU u IS KII, KS KII, IS PZS a VIS zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role, a o oznámeniach sú vedené záznamy.	◉	○	○
1	Je pripravené prostredie pre vyhodnocovanie oznámených KBU detekovaných technickými nástrojmi podľa § 21 až 23 VKB, je vykonávané ich vyhodnotenie a sú identifikované KBI.	○	◉	○
1	Je vykonávaná klasifikácia KBI, prijímané opatrenia pre odvrátenie a zmiernenie dopadu KBI, vykonávané hlásenia KBI podľa § 32 VKB a zaistený zber vierohodných podkladov potrebných pre analýzu KBI.	○	○	◉
1	Sú prešetrené a určené príčiny KBI, vyhodnotená účinnosť riešenia KBI a na základe vyhodnotenia sú stanovené nutné bezpečnostné opatrenia k zamedzeniu opakovania KBI.	◉	○	○
1	Zvládanie KBI je dokumentované.	○	◉	○

Obrázok č. 27: VKB - § 13 (Zdroj: Vlastné spracovanie podľa (2))

Paragraf 13 predpisuje povinným osobám, aby si pripravili prostredie pre vyhodnocovanie KBU, klasifikovali KBI, primali opatrenia na odvrátenie a zmiernenia dopadu a dokumentovali zvládanie KBI. Aj váha týchto predpisov je 1.

	§ 14 VKB - Riadenie kontinuity činností			
1	Sú stanovené práva a povinnosti garantov aktív, administrátorov a osôb zastávajúcich bezpečnostné role.	◉	○	○
	Sú stanovené ciele riadenia kontinuity činností formou určenia:			
1	minimálnej úrovne poskytovaných služieb, ktorá je prijateľná pre používanie, prevádzku a správu IS KII, KS KII, IS PZS alebo VIS.	○	◉	○
1	doby obnovenia chodu, behom ktorej bude po KBI obnovená minimálna úroveň poskytovaných služieb IS KII, KS KII, IS PZS alebo VIS.	○	○	◉
1	doby obnovenia dát ako termínu, ku ktorému budú obnovené dáta po KBI.	○	◉	○
1	Je stanovená stratégia riadenia kontinuity činností, ktorá obsahuje naplnenie cieľov podľa písmena b).	○	○	○
1	Sú vyhodnocované a dokumentované možné dopady KBI a posudzované možné riziká súvisiace s ohrozením kontinuity činnosti.	○	◉	○
1	Sú stanovené, aktualizované a pravidelne testované plány kontinuity činnosti IS KII, KS KII a IS PZS.	◉	○	○
1	Sú realizované opatrenia pre zvýšenie odolnosti IS KII, KS KII a IS PZS voči KBI a je využívaný nástroj pre zaisťovanie úrovne dostupnosť podľa § 26 VKB.	○	◉	○
	Sú stanovené a aktualizované postupy pre vykonávanie opatrení vydaných Úradom podľa § 13 a 14 ZKB, v ktorých je zohľadnené:			
1	výsledky hodnotenia rizík vykonaných opatrení.	○	○	◉
1	stav dotknutých bezpečnostných opatrení.	○	○	◉
1	vyhodnotenie prípadných negatívnych dopadov na prevádzku a bezpečnosť IS KII, KS KII alebo IS PZS.	○	○	◉

Obrázok č. 28: VKB - § 14 (Zdroj: Vlastné spracovanie podľa (2))

Paragraf 14 VKB vyžaduje od povinných subjektov, aby mali stanovené minimálne úrovne poskytovaných služieb, dobu obnovenia chodu, dobu obnovenia dát a ďalšie veci súvisiace s riadením kontinuity činností. Aj pri tých požiadavkách zostala zachovaná váha 1.

	§ 15 VKB - Kontrola a audit kybernetickej bezpečnosti			
1	Je posúdený súlad bezpečnostných opatrení s právnymi predpismi, vnútornými predpismi, inými predpismi a zmluvnými záväzkami vzťahujúcimi sa k IS KII, KS KII, IS PZS a VIS, a sú určené opatria k ich presadzovaniu.	○	○	◉
1	Sú vykonávané a dokumentované pravidelné kontroly dodržovania bezpečnostnej politiky a výsledky týchto kontrol sú zohľadnené v pláne rozvoja bezpečnostného povedomia a plánu zvládania rizík.	○	◉	○
1	Je zaistené vykonávanie auditu kybernetickej bezpečnosti osobou s odbornou kvalifikáciou podľa § 6 odst. 6 VKB, ktorá hodnotí správnosť a účinnosť zavedených bezpečnostných opatrení.	○	◉	○
1	Pre IS KII, KS KII a IS PZS je vykonávaná kontrola zraniteľností technických prostriedkov pomocou automatizovaných nástrojov a ich odborného vyhodnotenia, a je reagované na zistené zraniteľnosti.	○	○	◉

Obrázok č. 29: VKB - § 15 (Zdroj: Vlastné spracovanie podľa (2))

Posledným paragrafom v rámci organizačných opatrení je § 15, ktorý vyžaduje od organizácií pravidelnú kontrolu, audit ich kybernetickej bezpečnosti a ďalšie opatrenia. Váhu majú aj tieto požiadavky nastavené na štandardnú 1.

4.2.3. Technické opatrenia

Ďalším druhom opatrení, ktorých splnenie (či neplnenie) je potrebné v tejto fáze metodiky označiť sú technické opatrenia. Všetky tieto požiadavky boli rovnako ako aj organizačné opatrenia spracované na základe vyhlášky o kybernetickej bezpečnosti (§ 16 až § 27). Väčšina týchto opatrení sú hlavne požiadavky dané na konkrétne nástroje, ktoré by mali riešiť organizačné opatrenia stanovené v § 3 až § 15. Aj preto všetky majú váhu nastavenú na základnú 1, a majú tak na výslednom hodnotení výkonnosti identický podiel.

	§ 16 VKB - Fyzická bezpečnosť			
1	Sú prijaté nevyhnutné opatrenia k zabráneniu neoprávneného vstupu do vymedzených priestorov, kde sú spracovávané informácie a umiestnené technické aktíva IS KII, KS KII, IS PZS alebo VIS.	○	◉	○
1	Sú prijaté nevyhnutné opatrenia k zabráneniu poškodenia a zásahom do vymedzených priestorov, kde sú uchovávané informácie a umiestené technické aktíva IS KII, KS KII, IS PZS alebo VIS.	○	○	◉
1	Je predchádzané poškodeniu, krádeži alebo zneužitiu aktív, alebo prerušeniu poskytovania služieb IS KII, KS KII, IS PZS alebo VIS.	○	◉	○
1	Sú uplatňované prostriedky fyzickej bezpečnosti pre zaistenie ochrany úrovni objektov.	○	○	◉
1	Sú uplatňované prostriedky fyzickej bezpečnosti pre zaistenie ochrany v rámci objektov, v ktorých sú umiestené technické aktíva IS KII, KS KII alebo IS PZS.	◉	○	○

Obrázok č. 30: VKB - § 16 (Zdroj: Vlastné spracovanie podľa (2))

Jedným z paragrafov, ktorý nie je primárne zameraný na konkrétne nástroje je § 16. V tejto časti je potrebné odpovedať na to, ako sa plnia požiadavky týkajúce sa fyzickej bezpečnosti organizácie.

	§ 17 VKB - Nástroj pre ochranu integrity komunikačnej siete			
	Pre ochranu integrity rozhrania vonkajšej komunikačnej siete, ktorá nie je pod správou orgánu alebo osoby, a vnútornej komunikačnej siete, ktorá je pod správou orgánu alebo osoby, je zavedené(á):			
1	riadenie bezpečného prístupu medzi vonkajšou a vnútornou sieťou.	◉	○	○
1	segmentácia, najmä za použitia DMZ ako špeciálneho typu siete používaného ku zvýšeniu bezpečnosti aplikácií dostupných z vonkajšej siete a k obmedzeniu priamej komunikácie vnútornej siete s vonkajšou sieťou.	◉	○	○
1	použitie kryptografických prostriedkov (§ 25 VKB) pre vzdialený prístup, vzdialenú správu alebo pre prístup pomocou bezdrôtových technológií.	◉	○	○
1	opatrenie pre odstránenie alebo blokovanie prenášaných dát, ktoré neodpovedajú požiadavkám na ochranu integrity komunikačnej siete.	○	◉	○
1	Sú využívané nástroje pre ochranu integrity vnútornej komunikačnej siete, ktoré zaistia jej segmentáciu.	◉	○	○

Obrázok č. 31: VKB - § 17 (Zdroj: Vlastné spracovanie podľa (2))

	§ 18 VKB - Nástroj pre overovanie identity užívateľov			
1	Sú používané nástroje pre overenie identity užívateľov a administrátorov IS KII, KS KII, IS PZS a VIS.	◉	○	○
	Nástroj pre overovanie identity užívateľov, ktorý používa len autentizáciu heslom, zaisťuje:			
1	minimálnu dĺžku hesla osem znakov.	◉	○	○
1	minimálnu zložitosť hesla tak, že heslo bude obsahovať aspoň 3 z nasledujúcich 4 požiadavkou: 1. najmenej jedno veľké písmeno, 2. najmenej jedno malé písmeno, 3. najmenej jednu číslicu, alebo 4. najmenej jeden špeciálny znak, ktorý nie je uvedený v bodoch 1 až 3.	◉	○	○
1	maximálnu dobu pre povinnú výmenu hesla nepresahujúcu 100 dní; táto požiadavka sa nevyžaduje pre samostatné identifikátory aplikácií.	○	◉	○
	Je používaný nástroj pre overovanie identity, ktorý:			
1	znemožňuje opätovné používanie v minulosti používaných hesiel a neumožňuje viac zmien hesla jedného užívateľa počas stanoveného obdobia, ktoré je najmenej 24 hodín.	○	◉	○
1	vykonáva opätovné overenie identity po určitej dobe nečinnosti.	◉	○	○
1	Je využívaný nástroj pre overovanie identity administrátorov. V prípade, že tento nástroj využíva autentizáciu heslom, zaisťuje presadenie minimálnej dĺžky hesla 15 znakov pri dodržaní požiadavkou podľa 3 b) a 3 c).	◉	○	○
1	Nástroj pre overovanie identity užívateľov je zaistený inými spôsobmi, než aké sú stanovené v odstavcoch 3 až 5, a orgán a osoba má doložené, že použité opatrenia zaisťujú rovnakú alebo vyššiu úroveň odolnosti hesla.	○	○	◉

Obrázok č. 32: VKB - § 18 (Zdroj: Vlastné spracovanie podľa (2))

	§ 19 VKB - Nástroj pre riadenie prístupových oprávnení			
	Je používaný nástroj pre riadenie prístupových oprávnení, ktorým sa zaisťuje riadenie oprávnení:			
1	pre prístup k jednotlivým aplikáciám a dátam.	◉	○	○
1	pre čítanie dát, pre zápis dát a pre zmenu oprávnení.	◉	○	○
1	Je používaný nástroj pre riadenie prístupových oprávnení, ktorý zaznamenáva použitie prístupových opravení v súlade s bezpečnostnými potrebami a výsledkami hodnotenia rizík.	○	◉	○

Obrázok č. 33: VKB - § 19 (Zdroj: Vlastné spracovanie podľa (2))

	§ 20 VKB - Nástroj pre ochranu pred škodlivým kódom			
	Pre riadenie rizík spojených s pôsobením škodlivého kódu je používaný nástroj pre ochranu IS KII, KS KII, IS PZS a VIS pred škodlivým kódom, ktorý zaisťuje overenie a stálu kontrolu:			
1	komunikácie medzi vnútornou a vonkajšou sieťou.	◉	○	○
1	serverov a zdieľaných dátových úložísk.	◉	○	○
1	pracovných staníc.	◉	○	○
1	Pravidelne je vykonávaná aktualizácia nástroja pre ochranu pred škodlivým kódom, jeho definícií a signatúr.	◉	○	○

Obrázok č. 34: VKB - § 20 (Zdroj: Vlastné spracovanie podľa (2))

	§ 21 VKB - Nástroj pre zaznamenávanie činností KII, VIS, IS PZS, ich užívateľov a administrátorov			
	Je používaný nástroj pre zaznamenávanie činností IS KII, KS KII, IS PZS a VIS, ktorý zaisťuje:			
1	zber informácií o prevádzkových a bezpečnostných činnostiach, najmä typ činnosti, dátum a čas, identifikáciu technického aktíva, ktoré činnosť zaznamenalo, identifikáciu pôvodcu a miesta činnosti, a úspešnosť alebo neúspešnosť činnosti.	◉	○	○
1	ochranu získaných informácií pred neoprávneným čítaním alebo zmenou.	○	◉	○
	Za pomoci nástroja pre zaznamenávanie činností IS KII, KS KII, IS PZS a VIS sú zaznamenávané:			
1	prihlásenia a odhlásenia užívateľov a administrátorov.	◉	○	○
1	činnosti vykonané administrátormi.	◉	○	○
1	činnosti vedúce ku zmene prístupových oprávnení.	◉	○	○
1	nevykonané činnosti v dôsledku nedostatku prístupových oprávnení a ďalšie neúspešné činnosti užívateľov.	◉	○	○
1	zahájenia a ukončenia činnosti technických aktív IS KII, KS KII, IS PZS a VIS.	◉	○	○
1	automatické varovné alebo chybové hlásenia technických aktív.	◉	○	○
1	prístupy k záznamom o činnostiach, pokusy o manipuláciu so záznamami o činnostiach a zmeny nastavení nástroja pre zaznamenávanie činností.	◉	○	○
1	použitia mechanizmov identifikácie a autentizácie, vrátane zmeny údajov, ktoré slúžia k prihláseniu.	◉	○	○
1	Záznamy činností zaznamenávané podľa odst. 2 sú uchovávané po dobu najmenej 3 mesiacov.	○	◉	○
1	Najmenej raz za 24 hodín je vykonávaná synchronizácia jednotného systémového času technických aktív patriacich do IS KII, KS KII, IS PZS alebo VIS.	○	◉	○

Obrázok č. 35: VKB - § 21 (Zdroj: Vlastné spracovanie podľa (2))

	§ 22 VKB - Nástroj pre detekciu kybernetických bezpečnostných udalostí			
1	Je používaný nástroj pre detekciu KBU, ktorý vychádza zo stanovených bezpečnostných potrieb a výsledkov hodnotení rizík a ktorý zaistí overenie, kontrolu a prípadné zablokovanie komunikácie medzi vnútornou a vonkajšou komunikačnou sieťou.	◉	○	○
	Je používaný nástroj pre detekciu KBU, ktorý zaistí overenie, kontrolu a prípadné zablokovanie komunikácie:			
1	v rámci vnútornej komunikačnej siete.	○	◉	○
1	serverov patriacich do IS KII, KS KII alebo IS PZS.	◉	○	○

Obrázok č. 36: VKB - § 22 (Zdroj: Vlastné spracovanie podľa (2))

	§ 23 VKB - Nástroj pre zber a vyhodnotenie kybernetických bezpečnostných udalostí			
	Je používaný nástroj pre zber a priebežné vyhodnocovanie KBU, ktorý v súlade s bezpečnostnými potrebami a výsledkami hodnotenia rizík zaisťuje:			
1	integrovaný zber a vyhodnotenie KBU z IS KII, KS KII a IS PZS.	○	◉	○
1	poskytovanie informácií pre určené bezpečnostné role o detekovaných KBU v IS KII, KS KII alebo IS PZS.	○	◉	○
1	nepretržité vyhodnocovanie KBU s cieľom identifikácie KBI, vrátane včasného varovania určených bezpečnostných rolí.	○	○	◉
1	Je zaistená pravidelná aktualizácia nastavení pravidiel pre vyhodnocovanie KBU a včasné varovanie, aby boli obmedzované prípady nesprávneho vyhodnotenia udalostí alebo prípady falošných varovaní.	○	◉	○
1	Je zaistené využívanie informácií, ktoré sú pripravované nástrojom pre zber a vyhodnocovanie KBU, pre optimálne nastavenie bezpečnostných opatrení IS KII, KS KII a IS PZS.	○	○	◉

Obrázok č. 37: VKB - § 23 (Zdroj: Vlastné spracovanie podľa (2))

	§ 24 VKB - Aplikačná bezpečnosť			
1	Sú vykonávané bezpečnostné testy zraniteľností aplikácií, ktoré sú prístupné z vonkajšej siete, a to pred ich uvedením do prevádzky a po každej zmene bezpečnostných mechanizmov.	○	○	◉
1	Je zaistená trvalá ochrana aplikácií a informácií dostupných z vonkajšej siete pred neoprávnenou činnosťou, popretím vykonaných činností, kompromitáciou alebo neautorizovanou zmenou.	◉	○	○
1	Je zaistená trvalá ochrana transakcií pred ich nedokončením, nesprávnym smerovaním, neautorizovanou zmenou odovzdávaného dátového obsahu, neautorizovaným duplikovaním alebo opakovaním.	○	◉	○

Obrázok č. 38: VKB - § 24 (Zdroj: Vlastné spracovanie podľa (2))

	§ 25 VKB - Kryptografické prostriedky			
	Pre používanie kryptografickej ochrany je (sú) stanovená(é):			
1	úroveň ochrany s ohľadom na typ a silu kryptografického algoritmu.	○	◉	○
1	pravidlá kryptografickej ochrany informácií pri prenose po komunikačných sieťach, pri uložení na mobilné zariadenie alebo vymeniteľné technické nosiče dát.	○	◉	○
1	V súlade s bezpečnostnými potrebami a výsledkami hodnotení rizík sú používané kryptografické prostriedky, ktoré zaistia ochranu dôvernosti a integrity odovzdávaných alebo ukladaných dát, a preukázanie zodpovednosti za vykonané činnosti.	◉	○	○
1	Pre používanie kryptografických prostriedkov je stanovený systém správy kľúčov, ktorý zaistí generovanie, distribúciu, ukladanie, archiváciu, zmeny, ničenie, kontrolu a audit kľúčov.	◉	○	○
1	Sú používané odolné kryptografické algoritmy a kryptografické kľúče; v prípade nesúladu s minimálnymi požiadavkami na kryptografické algoritmy uvedenými v prílohe č. 3 VKB, riadi riziká spojené s týmto nesúladom.	○	○	◉

Obrázok č. 39: VKB - § 25 (Zdroj: Vlastné spracovanie podľa (2))

	§ 26 VKB - Nástroj pre zisťovanie úrovne bezpečnosti			
1	V súlade s bezpečnostnými potrebami a výsledkami hodnotenia rizík je používaný nástroj pre zaisťovanie úrovne dostupnosti informácií.	○	◉	○
	Je používaný nástroj pre zaisťovanie úrovne dostupnosti informácií, ktorý zaistí:			
1	dostupnosť IS KII, KS KII a IS PZS pre splnenie cieľov riadenia kontinuity činností.	◉	○	○
1	odolnosť IS KII, KS KII a IS PZS voči KBI, ktoré by mohli znížiť ich dostupnosť.	◉	○	○
1	zálohovanie dôležitých technických aktív IS KII, KS KII a IS PZS	◉	○	○
1	1. využitím redundancie v návrhu riešenia a	◉	○	○
1	2. zaistením náhradných technických aktív v určenom čase.	◉	○	○

Obrázok č. 40: VKB - § 26 (Zdroj: Vlastné spracovanie podľa (2))

	§ 27 VKB - Bezpečnosť priemyselných a riadiacich systémov			
	Pre bezpečnosť priemyselných a riadiacich systémov, ktoré sú IS KII, KS KII, IS PZS alebo ich súčasťou, sú používané nástroje, ktoré zaistia:			
1	obmedzenie fyzického prístupu k sieti a zariadeniam priemyselných a riadiacich systémov.	◉	○	○
1	obmedzenie prepojení a vzdialeného prístupu k sieti priemyselných a riadiacich systémov.	○	◉	○
1	ochranu jednotlivých technických aktív priemyselných a riadiacich systémov pred využitím známych zraniteľností.	◉	○	○
1	obnovenie chodu priemyselných a riadiacich systémov po KBI.	◉	○	○

Obrázok č. 41: VKB - § 27 (Zdroj: Vlastné spracovanie podľa (2))

4.3. Systém riadenia bezpečnosti informácií

Ďalším okruhom opatrení, ktorých splnenie (zavedenie/aplikovanie) je v tejto fáze metodiky potrebné označiť, sú opatrenia vychádzajúce z ISMS, konkrétne z normy ČSN ISO/IEC 27002:2014. Rozdelenie týchto opatrení do jednotlivých skupín vychádza rovnako z tejto normy, okrem prvých dvoch skupín, ktoré sú viacmennej výberom, ktorý som vytvoril na základe požiadaviek v rámci ČSN ISO/IEC 27001:2013. Taktiež je potrebné spomenúť, že niektoré opatrenia majú svoj ekvivalent už v opatreniach VKB, preto som niektoré z týchto opatrení zahrnul aj do výberu v rámci hodnotenia výkonnosti ISMS.

Samozrejme je nutné pripomenúť nutnosť odpovedať na otázku o ISMS v prvej fáze metodiky kladne, v opačnom prípade sa tieto opatrenia v excelovskom zošite nezobrazia.

4.3.1. Všeobecné požiadavky ISMS

Všeobecné požiadavky predstavujú môj výber z opatrení uvedených v § 3 VKB, ktoré, podľa môjho názoru, reflektujú základnú podstatu ISMS a teda PDCA cyklus. Nehovoriac o základnej požiadavke pri zavádzaní ISMS - stanoviť rozsah ISMS. Z tohto dôvodu je aplikovanie týchto opatrení nevyhnutný krok pre správne fungovanie ISMS a má teda podiel aj na hodnotení podniku z pohľadu informačnej bezpečnosti.

Ak bola v prvej fáze metodiky vybraná len možnosť ISMS (prípadne aj v kombinácií s GDPR), tak sa tento výber požiadaviek zobrazí samostatne, v opačnom prípade (pri vybraní povinnej osoby KBZ, ktorá má tieto povinnosti), budú zobrazené normálne medzi povinnosťami danými VKB. Ich plnenie/neplnenie sa ale okrem hodnotenia v rámci KBZ, premietne aj do hodnotenia v rámci ISMS.

4.3.2. Analýza rizík

Túto skupinu som spracoval na základe požiadaviek ČSN ISO/IEC 27001:2014, vzhľadom na fakt, že analýza rizík je podstatnou časťou ISMS a mať stanovené metodiky pre ich analýzu a hodnotenie je jedným z predpokladov potrebným pre výber správneho

opatrenia. Vzhľadom na prílišnú konkrétnosť analýzy rizík vo VKB som odpovede v danej časti k hodnoteniu tejto časti nepoužil.

2	Sú stanovené metodiky pre identifikáciu a hodnotenie rizík bezpečnosti informácií, vrátane stanovených kritérií pre prijateľnosť rizík.	◉	○	○
	V stanovených metodikách sú určené:			
1	spôsoby ako identifikovať riziká, ktoré môžu ohroziť dôvernosť, integritu alebo dostupnosť informácií.	◉	○	○
1	spôsoby ako identifikovať vlastníka rizika.	◉	○	○
1	kritéria hodnotenia dopadov (následkov) a pravdepodobnosti výskytu.	○	◉	○
1	spôsoby, ako sa bude riziko počítať.	◉	○	○
1	kritéria akceptácie rizika.	◉	○	○
2	Podľa týchto metodík sa vykonáva analýza rizík, kde sú identifikované riziká ohodnotené podľa kritérií dopadu a pravdepodobnosti, určený vlastníci rizík, určené a schválené prijateľné riziká, a spracovaná správa o hodnotení rizík.	◉	○	○
2	Na základe bezpečnostných potrieb a výsledkov hodnotenia rizík je spracované prehlásenie o aplikovateľnosti, ktoré obsahuje prehľad vybraných a zavedených bezpečnostných opatrení	○	◉	○
1	Je spracovaný plán zvládania rizík, ktorý obsahuje ciele a prínosy bezpečnostných opatrení pre zvládanie rizík, určené osoby zodpovedné za presadzovanie bezpečnostných opatrení pre zvládanie rizík, potrebné finančné, technické, ľudské a informačné zdroje, termín ich zavedenia a popis väzieb medzi rizikami a príslušnými bezpečnostnými opatreniami.	○	◉	○

Obrázok č. 42: ISMS - Analýza rizík (Zdroj: Vlastné spracovanie podľa (4))

4.3.3. Politiky bezpečnosti informácií

Aj táto časť viacmennej kopíruje požiadavky na to mať stanovené politiky bezpečnosti informácií v rôznych oblastiach, uvedených vo VKB. Preto sa k hodnoteniu ISMS v oblasti bezpečnostných politík aj ISMS celkovo požijú odpovede z uvedenej časti VKB. Pričom aj tu treba spomenúť, že v prípade nevybratia žiadnej povinnej osoby KBZ sa tieto otázky zobrazia samostatne.

4.3.4. Organizácia bezpečnosti informácií

Tieto opatrenia sú už výberom z ČSN ISO/IEC 27002:2014 tykajúce sa organizačnej bezpečnosti uvedenými v kapitole 6. K hodnoteniu výkonnosti z tejto oblasti sú použité aj dva ďalšie opatrenia uvedené v rámci opatrení VKB.

1	*Role a zodpovednosti bezpečnosti informácií* - Sú definované a pridelené všetky role a zodpovednosti za bezpečnosť informácií.	◉	○	○
1	*Princíp oddelenia povinností* - Všetky konfliktné povinnosti a oblasti pôsobnosti sú oddelené.	○	◉	○
1	*Kontakt s príslušnými orgánmi a autoritami* - Sú udržiavané primerané kontakty s príslušnými autoritami.	◉	○	○
1	*Kontakt so záujmovými skupinami* - Sú udržiavané primerané kontakty so zvláštnymi záujmovými skupinami alebo špecialistami na bezpečnosť.	◉	○	○
1	*Bezpečnosť informácií v riadení projektu* - Bez ohľadu na typ projektu je v každom riešená bezpečnosť informácií.	○	○	◉
1	*Práca na diaľku* - Je zavedená politika a podporné bezpečnostné opatrenia, ktoré riešia ochranu informácií ku ktorým sa pristupuje v rámci práce na diaľku, spracovaných alebo ukladaných v miestach práce na diaľku.	○	◉	○

Obrázok č. 43: ISMS - 6 (Zdroj: Vlastné spracovanie podľa (4))

4.3.5. Bezpečnosť ľudských zdrojov

Opäť výber opatrení z ČSN ISO/IEC 27002:2014 tentokrát z kapitoly 7. K hodnoteniu sú tiež použité opatrenia uvedené v § 9 VKB a tiež ďalšie dva uvedené v iných častiach vyhlášky, ktoré spadajú do tejto oblasti.

1	*Preverovanie* - Podľa klasifikácií informácií, ku ktorým má byť umožnení prístup, požiadavkám súvisiacich s činnosťou organizácie, v súlade s príslušnými zákonmi, nariadeniami a v súlade s etikou je primerane preverovaná minulosť všetkých uchádzačov o zamestnanie.	○	○	◉
1	*Podmienky pracovného pomeru* - V zmluvách so zamestnancami a zmluvnými stranami sú uvádzané zodpovednosti zamestnancov/zmluvných strán a organizácie za bezpečnosť informácií.	◉	○	○
1	*Zodpovednosť pri ukončení alebo zmene pracovného pomeru* - Zodpovednosti a povinnosti v oblasti bezpečnosti informácií, ktoré zostávajú v platnosti aj po ukončení alebo zmene zamestnania sú definované, oznamované zamestnancom alebo zmluvnej strane a sú presadzované.	○	◉	○

Obrázok č. 44: ISMS – 7 (Zdroj: Vlastné spracovanie podľa (4))

4.3.6. Riadenie aktív

Okrem vybraných opatrení z 8. kapitoly ČSN ISO/IEC 27002:2014 sa k hodnoteniu tejto časti používa tiež 10 ďalších opatrení z VKB, najmä tých uvedených v § 8.

1	*Klasifikácia informácií* - Informácie sú klasifikované z hľadiska právnych požiadaviek, hodnoty, kritickosti a citlivosti vo vzťahu k neoprávnenému prezradeniu alebo modifikácií.	◉	○	○
1	*Označovanie informácií* - Sú vypracované a implementované vhodné súbory postupov pre označovanie informácií, v súlade so schémou klasifikácie informácií prijatých organizáciou.	◉	○	○
1	*Manipulácia s aktívami* - Sú vyvinuté a zavedené postupy pre zaobchádzanie s aktívami, v súlade s ich klasifikáciou.	○	◉	○
1	*Správa výmenných médií* - Sú zavedené postupy pre správu výmenných médií, v súlade so schémou klasifikácie prijatých organizáciou.	○	◉	○
1	*Preprava fyzických médií* - Behom prepravy sú všetky média obsahujúce informácie chránené pre neoprávneným prístupom, zneužitím alebo poškodením.	○	○	◉

Obrázok č. 45: ISMS – 8 (Zdroj: Vlastné spracovanie podľa (4))

4.3.7. Riadenie prístupu

Opatrenia riešiace riadenie prístupu sú taktiež vybrané z normy ČSN ISO/IEC 27002:2014, konkrétne z 9. kapitoly. Aj tu sa k hodnoteniu berú do úvahy aj dve ďalšie opatrenia VKB.

1	*Prístup k sieťam a sieťovým službám* - Užívatelia majú prístup len k tým sieťam a sieťovým službám, pre použitie ktorých boli zvlášť oprávnení.	○	◉	○
1	*Registrácia a zrušenie registrácie užívateľa* - Je zavedený formálny proces registrácie a deregistrácie užívateľa.	○	◉	○
1	*Správa užívateľských prístupov* - Je zavedený formálny proces prideľovania a odoberania prístupových práv ku všetkým systémom a službám.	◉	○	○
1	*Správa tajných autentizačných informácií užívateľov* - Prideľovanie tajných autentizačných informácií je riadené prostredníctvom formálneho procesu riadenia.	○	○	◉
1	*Odoberanie alebo úprava prístupových práv* - Prístupové práva všetkých zamestnancov a užívateľov z externých strán k informáciám a vybaveniu pre spracovanie informácií sú odstránené ihneď po ukončení zmluvy, ich zamestnania alebo vypršaní dohody, alebo sú ihneď po zmene upravené.	○	◉	○
1	*Používanie tajných autentizačných informácií* - Je vyžadované, aby užívatelia dodržovali pri používaní tajných autentizačných informácií postupy stanovené organizáciou.	○	○	◉
1	*Obmedzenie prístupu k informáciám* - Je obmedzený prístup k informáciám a funkciám aplikácií v súlade s politikou riadenia.	○	◉	○
1	*Bezpečné postupy prihlásenia* - Prístup k systémov a aplikáciám sa riadi postupmi bezpečného prihlásenia.	○	◉	○
1	*Systém správy hesiel* - Využíva sa systém správy hesiel, ktorý je interaktívny a zaisťuje používanie kvalitných hesiel.	◉	○	○

Obrázok č. 46: ISMS - 9 (Zdroj: Vlastné spracovanie podľa (4))

4.3.8. Kryptografia

V tomto prípade sa k hodnoteniu informačnej bezpečnosti z pohľadu kryptografie používa v plnej miere paragraf § 25 VKB, spolu s požiadavkou mať stanovenú politiku v oblasti používania kryptografickej ochrany.

4.3.9. Fyzická bezpečnosť a bezpečnosť prostredia

K hodnotenie fyzickej bezpečnosti a bezpečnosti prostredia sa využíva 13 vybraných opatrení z 11. kapitoly ČSN ISO/IEC 27002:2014 a taktiež požiadavka na stanovanie politiky v oblasti fyzickej bezpečnosti vo VKB.

1	*Fyzický bezpečnostný perimeter* - Sú definované a používané bezpečnostné perimetre, ktoré sa používajú k ochrane oblastí s citlivými alebo kritickými informáciami a vybavením pre spracovanie informácií.	○	◉	○
1	*Fyzické kontroly vstupu* - Prístup do bezpečných oblastí je povolený len oprávneným osobám a tieto oblasti sú chránené vhodným systémom vstupných kontrol.	○	◉	○
1	*Zabezpečenie kancelárií, miestností a vybavenia* - Sú navrhnuté a uplatňované opatrenia pre fyzickú bezpečnosť kancelárií, miestností a vybavení.	○	○	◉
1	*Ochrana pred vonkajšími hrozbami a hrozbami prostredia* - Je navrhnutá a uplatňovaná fyzická ochrana pred prírodnými katastrofami, zlomyseľnými útokmi alebo nehodami.	○	○	◉
1	*Práca v zabezpečených oblastiach* - Sú navrhnuté a uplatnené postupy pre prácu v zabezpečených oblastiach.	○	◉	○
1	*Oblasti pre nakládku a vykládku* - Miesta prístupu, kde by mohli neoprávnené osoby vstupovať do objektov sú kontrolované a pokiaľ je to možné sú izolované od vybavenia pre spracovanie informácií.	○	◉	○
1	*Umiestnenie zariadení a ich ochrana* - Zariadenia sú umiestňované a chránené tak, aby sa znížilo riziko nebezpečia a hrozieb daných prostredím a aby sa obmedzili príležitosti pre neoprávnený prístup.	○	◉	○
1	*Podporné služby* - Zariadenia sú chránené pred výpadkom napájania a ďalšími poruchami spôsobenými zlyhaním podporných služieb.	◉	○	○
1	*Bezpečnosť káblových rozvodov* - Káblové rozvody, ktoré sú určené na prenos dát alebo podporu informačných služieb, sú chránené pred poškodením, rušením alebo odpočúvaním.	○	◉	○
1	*Údržba zariadenia* - Zariadenia sú správne udržiavané, aby sa zaistila ich stála dostupnosť a integrita.	◉	○	○
1	*Presunutie aktív* - Bez predchádzajúceho schválenia nesmú byť zariadenia, informácie alebo software premiestňované mimo priestorov organizácie.	○	○	◉
1	*Bezpečná likvidácia alebo opakované použitie zariadenia* - Všetky časti zariadení, ktoré obsahujú pamäťové média, sú pred likvidáciou alebo opakovaným použitím skontrolované, s cieľom zaistiť odstránenie alebo bezpečné prepísanie všetkých citlivých dát a licencovaného softwaru.	○	○	◉
1	*Zásada prázdneho stola a prázdnej obrazovky* - Je prijatá zásada prázdneho stola vo vzťahu k dokumentom a prenosným pamäťovým médiám a zásada prázdnej obrazovky monitoru u vybavenia pre spracovanie informácií.	○	◉	○

Obrázok č. 47: ISMS - 11 (Zdroj: Vlastné spracovanie podľa (4))

4.3.10. Bezpečnosť prevádzky

Mimo 9 opatrení z ČSN ISO/IEC 27002:2014 sa k hodnoteniu výkonnosti v tejto oblasti používa aj miera plnenia 4 ďalších opatrení v rámci VKB.

1	*Dokumentované prevádzkové postupy* - Prevádzkové postupy sú dokomentované a sú prístupné všetkým užívateľom podľa potreby.	◉	○	○
1	*Riadenie zmien* - Všetky zmeny v organizácií, podnikových procesoch, vybavení pre spracovávanie informácií a systémoch, ktoré majú vplyv na bezpečnosť informácií sú riadené a kontrolované.	○	○	◉
1	*Opatrenia proti malwaru* - Sú implementované opatrenia na detekciu, prevenciu a obnovu, ktoré slúžia na ochranu pred malwarom, v kombinácií s vhodným zvyšovaním povedomia užívateľov.	◉	○	○
1	*Zálohovanie informácií* - Pravidelne sa vykonávajú a testujú záložné kópie informácií, softwaru a bitových kópií systémov v súlade so schválenou politikou zálohovania.	◉	○	○
1	*Zaznamenávanie udalostí formou logov* - Pravidelne sa vytvárajú, uchovávajú a preskúmavajú logy udalostí zaznamenávajúce aktivity užívateľov, zlyhania, výnimky a udalostí bezpečnosti informácií.	◉	○	○
1	*Ochrana logov* - Prostriedky pre zaznamenávanie logov a aj samotné logy sú chránené proti sfalšovaniu a neoprávnenému prístupu.	○	◉	○
1	*Logy administrátorov a operátorov* - Všetky aktivity systémového administrátora a operátora sú logované a logy chránené a pravidelne preskúmavané.	◉	○	○
1	*Synchronizácia hodín* - Podľa referenčného zdroja času sa synchronizujú všetky dôležité systémy pre spracovanie informácií v rámci organizácie alebo bezpečnostných domén.	○	◉	○
1	*Riadenie technických zraniteľností* - Sú prijaté opatrenia k včasnému získavaniu informácii o technických zraniteľnostiach použitých IS, vyhodnocuje sa ohrozenie organizácie týmito zraniteľnosťami a prijímajú sa primerané opatrenia k riešeniu súvisiacich rizík.	○	◉	○

Obrázok č. 48: ISMS - 12 (Zdroj: Vlastné spracovanie podľa (4))

4.3.11. Bezpečnosť komunikácie

Bezpečnosť komunikácie sa hodnotí podľa miery splnenia týchto 5 opatrení z ISO a tiež 3 ďalších z VKB. Ide najmä o požiadavku na stanovenie politiky v oblasti riadenia prevádzky a komunikácií.

1	*Opatrenia v sieťach* - Pre ochranu informácií v systémoch a aplikáciách sú siete riadené a kontrolované.	◉	○	○
1	*Bezpečnosť sieťových služieb* - Do zmlúv o sieťových službách sa identifikujú a zahrňujú bezpečnostné mechanizmy, úrovne služieb a požiadavky na správu a riadenie sieťových služieb, či už sú tieto služby zaisťované interne alebo pomocou vonkajších zdrojov.	○	◉	○
1	*Princíp oddelenia v sieťach* - V rámci sietí sú oddelené skupiny informačných služieb, užívateľov a IS.	○	◉	○
1	*Politiky a postupy pri prenose informácií* - Sú zavedené formálne politiky, postupy a opatrenia k ochrane prenosu informácií prostredníctvom všetkých druhov komunikačných zariadení.	◉	○	○
1	*Elektronické predávanie správ* - Informácie, ktoré sa presúvajú elektronicky sú primerané chránené.	○	◉	○

Obrázok č. 49: ISMS – 13 (Zdroj: Vlastné spracovanie podľa (4))

4.3.12. Akvizícia, vývoj a údržba systémov

Vzhľadom na konkrétne zameranie opatrení VKB na prvky IS/KS KII a IS PZS, sa v tejto časti k určovaniu výkonnosti používa hlavne 8 opatrení vybraných z 14. kapitoly ČSN ISO/IEC 27002:2014, ale tiež jedno opatrenie vybrané z VKB.

1	*Analýza a špecifikácie požiadaviek na bezpečnosť informácií* - Do požiadaviek na nové IS alebo na vylepšenie súčasných IS sa zahrňujú požiadavky súvisiace s bezpečnosťou informácií.	○	◉	○
1	*Zabezpečenie aplikačných služieb vo verejných sieťach* - Informácie, ktoré sú zahrnuté v aplikačných službách prebiehajúcich cez verejné siete sú chránené pred podvodnou činnosťou, zmluvnými spormi, neoprávnením sprístupnením a zmenou.	◉	○	○
1	*Ochrana transakcií aplikačných služieb* – Informácie, ktoré sú zahrnuté v transakciách aplikačných služieb sú chránené, aby sa zabránilo ich nedokončenému prenosu, neoprávnenej zmene správy, chybnému smerovaniu, neoprávnenému zverejneniu, neoprávnenému duplikovaniu alebo opakovanému zaslaniu správy.	◉	○	○
1	*Postupy riadenia zmien systémov* - Zmeny systémov v rámci životného cyklu vývoja sú riadené a kontrolované pomocou formálnych postupov riadenia zmien.	◉	○	○
1	*Technické preskúmavanie aplikácií po zmenách prevádzkovej platformy* - Aby sa zaistilo, že zmena prevádzkovej platformy nebude mať nepriaznivý dopad na prevádzku alebo bezpečnosť organizácie, pred každou zmenou sú preskúmavané a testované aplikácie kritické pre činnosť organizácie.	○	◉	○
1	*Obmedzenie zmien softwarových balíkov* – Modifikácie softwarových balíkov sú striktne riadené a akékoľvek zmeny, ktoré nie sú nevyhnutné sú nežiadúce.	○	○	◉
1	*Testovanie bezpečnosti systému* - Testovanie funkčnosti bezpečnosti sa uskutočňuje už behom vývoja.	○	○	◉
1	*Testovanie akceptácie systému* - Sú zostavené programy pre akceptačné testy a súvisiace kritéria pre nové IS, aktualizácie a nové verzie systémov.	◉	○	○

Obrázok č. 50: ISMS – 14 (Zdroj: Vlastné spracovanie podľa (4))

4.3.13. Dodávateľské vzťahy

Z rovnakého dôvodu tak aj v prípade dodávateľských vzťahov, hodnotenie vychádza najmä z miery plnenia vybraných opatrení ČSN ISO/IEC 27002:2014 a tiež požiadavky na stanovenie politiky v oblasti riadenia vzťahov s dodávateľmi uvedenou v § 5 VKB.

1	*Politika bezpečnosti informácií pre oblasť vzťahov s dodávateľmi* - S dodávateľmi sú vyjednávané a dokumentované všetky požiadavky v oblasti bezpečnosti informácií na zmiernenie rizík spojených s prístupom dodávateľa k aktívam organizácie.	○	◉	○
1	*Riešenie bezpečnosti v rámci zmlúv s dodávateľmi* - S každým dodávateľom, ktorý môže pristupovať k informáciám organizácie, spracovávať ich, ukladať, prenášať alebo pre nich poskytovať komponenty ICT infraštruktúry, sú dohodnuté a odsúhlasené všetky podstatné požiadavky na bezpečnosť informácií.	◉	○	○
1	*Reťazec dodávateľov ICT technológií* - Požiadavky na riešenie rizík v oblasti bezpečnosti informácií súvisiacich so službami ICT technológií a produktami reťazca dodávateľov sú zahrňované do zmlúv s dodávateľmi.	○	○	◉
1	*Monitorovanie a preskúmavanie služieb dodávateľov* - Dodávky služieb dodávateľov sú pravidelne monitorované, preskúmavané a auditované.	○	○	◉

Obrázok č. 51: ISMS – 15 (Zdroj: Vlastné spracovanie podľa (4))

4.3.14. Riadenie incidentov bezpečnosti informácií

Ďalšia hodnotená časť ISMS sa týka riadenia incidentov bezpečnosti informácií a k posudzovaniu tejto časti sa okrem 5 vybraných opatrení z ISO, používajú aj 2 ďalšie opatrenia z VKB.

1	*Zodpovednosť a postupy* - Sú ustanovené zodpovednosti a postupy managementu s cieľom zaistiť rýchlu, efektívnu a riadnu odozvu na incidenty bezpečnosti informácií.	◉	○	○
1	*Podávanie správ o udalostiach bezpečnosti informácií* - Všetky udalosti bezpečnosti informácií sú čo najrýchlejšie oznamované prostredníctvom príslušných riadiacich kanálov.	◉	○	○
1	*Posudzovanie a rozhodovanie o udalostiach bezpečnosti informácií* - O udalostiach bezpečnosti informácií sa rozhoduje a posudzuje sa, či nemajú byť klasifikované ako incidenty bezpečnosti informácií.	○	◉	○
1	*Odozva na incidenty bezpečnosti informácií* - V súlade s dokumentovanými postupmi sa reaguje na incidenty bezpečnosti informácií.	◉	○	○
1	*Ponaučenie z incidentov bezpečnosti informácií* - Znalosti, ktoré sa získajú z riešenia incidentov sa používajú ku zníženiu pravdepodobnosti alebo dopadu budúcich incidentov.	○	○	◉

Obrázok č. 52: ISMS – 16 (Zdroj: Vlastné spracovanie podľa (4))

4.3.15. Aspekty riadenia kontinuity činnosti organizácie

Posledná časť ISMS, v ktorej bude zisťovaný výkonnostný ukazovateľ, je spojená s riadením kontinuity činnosti organizácie. Na posudzovanie bezpečnosti informácií z tejto oblasti budú využité štyri vybrané opatrenia z ISO.

1	*Plánovanie kontinuity bezpečnosti informácií* - Sú stanovené požiadavky na bezpečnosť informácií a kontinuitu riadenia bezpečnosti informácií v nepriaznivých situáciách, ako sú napríklad krízy alebo katastrofy.	◉	○	○
1	*Implementácia kontinuity bezpečnosti informácií* - Sú stanovené, zdokumentované, zavedené a udržiavané procesy, postupy a opatrenia k zaisteniu požadovanej úrovne kontinuity bezpečnosti informácií behom nepriaznivých situácií.	◉	○	○
1	*Verifikácia, preskúmavanie a vyhodnocovanie kontinuity bezpečnosti informácií* - V pravidelných intervaloch sa overujú zriadené a implementované opatrenia kontinuity bezpečnosti informácií, aby sa zaistilo, že v prípade nepriaznivých situácií budú platné a efektívne.	○	◉	○
1	*Dostupnosť vybavenia pre spracovanie informácií* - Vybavenie pre spracovanie informácií je zavádzané s dostatočnou redundanciou, aby boli naplňované požiadavky na dostupnosť.	◉	○	○

Obrázok č. 53: ISMS – 17 (Zdroj: Vlastné spracovanie podľa (4))

4.4. Povinnosti z GDPR

Poslednou oblasťou druhej fázy metodiky pre vyhodnocovanie výkonnosti je, respektíve môže byť (podľa výberu v 1. fáze), vybranie možností, ktoré najviac zodpovedajú stupňu splnenia (splnené, čiastočne splnené, nesplnené) jednotlivých povinností určených v nariadení GDPR.

Zoznam týchto povinností som spracoval na základe samotného nariadenia GDPR a predstavuje tak akýsi súhrn tých najdôležitejších bodov daného nariadenia. Podľa vlastného presvedčenia som niektorým požiadavkám dal váhu 2, ostatné som nechal na štandardnej 1.

	GDPR			
2	Je vymenovaný poverenec pre ochranu osobných údajov - Data Protection Officer (DPO)	○	○	◉
1	Pred zahájením spracovania je, ak je to potrebné, vypracované posúdenie vplyvu na ochranu osobných údajov (Data Protection Impact Assessment).	○	○	◉
1	Každé spracovanie osobných údajov je podmienené zákonným dôvodom, alebo explicitným súhlasom subjektu údajov (FO) a ten ma právo súhlas kedykoľvek odvolať.	◉	○	○
1	Je zavedený systém (a stanovené postupy), ktorý umožňuje prenositeľnosť osobných údajov klienta, a teda umožňuje im vyžiadať si všetky ich osobné údaje a dostať ich v zrozumiteľnej a použiteľnej podobe. *(Právo na prenositeľnosť údajov)*	◉	○	○
1	Je zavedený systém (a stanovené postupy), ktorý umožňuje na žiadosť vymazať všetky osobné údaje, ktoré sa vedú o žiadateľovi, pokiaľ nebude existovať právny dôvod na ich držanie. *(Právo na výmaz)*	◉	○	○
1	Sú stanovené postupy (mechanizmy), ktoré umožňujú subjektu údajov opravu osobných údajov, alebo doplnenie neúplných osobných údajov. *(Právo na opravu)*	◉	○	○
1	Sú stanovené postupy (mechanizmy), ktoré umožňujú subjektu údajov vzniesť námietku proti spracovaniu osobných údajov. *(Právo vzniesť námietku)*	◉	○	○
1	Sú stanovené postupy (mechanizmy), ktoré umožňujú obmedziť spracovanie osobných údajov v prípade, že subjekt údajov o to legitímne požiada. *(Právo na obmedzenie spracovania)*	○	◉	○
1	Priebežne sa vymazávajú údaje, ktoré už nie sú nevyhnutné a pre ktoré už neplatí súhlas.	○	○	◉

Obrázok č. 54: GDPR - povinnosti 1 (Zdroj: Vlastné spracovanie podľa (5))

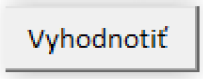
	Pre zaistenie zámernej a štandardnej ochrany osobných údajov sú zavedené:			
2	nástroje ako pseudoanonimizácia a šifrovanie osobných údajov.	○	◉	○
2	opatrenia súvisiace so schopnosťou zaistiť neustálu dôvernosť, integritu, dostupnosť a odolnosť systémov a služieb spracovania.	◉	○	○
2	opatrenia súvisiace so schopnosťou obnoviť dostupnosť osobných údajov a prístup k nim včas v prípade fyzických či technických incidentov.	◉	○	○
2	procesy pravidelného testovania, posudzovania a hodnotenia účinnosti zavedených technických a organizačných opatrení pre zaistenie bezpečnosti spracovania.	○	◉	○
2	vhodné technické a organizačné opatrenia k zaisteniu toho, aby sa štandardne spracovávali len osobné údaje, ktoré sú pre každý konkrétny účel daného spracovania nevyhnutné.	○	○	◉
	Vedú sa záznamy o činnostiach spracovania, ktoré obsahujú tieto informácie:			
1	meno a kontaktné údaje správcu, spracovateľa a DPO,	○	◉	○
1	účely spracovania,	◉	○	○
1	popis kategórií subjektov údajov a kategórií osobných údajov,	◉	○	○
1	kategórie príjemcov, ktorým boli alebo budú osobné údaje sprístupnene,	◉	○	○
1	informácie o medzinárodnom odovzdávaní dát,	○	○	◉
1	termíny pre výmaz jednotlivých kategórií údajov,	○	○	◉
1	popis technických a organizačných bezpečnostných opatrení.	○	○	◉
1	Povinnosť informovať orgán kontroly (Úřad pro ochranu osobních údajů) o úniku osobných údajov do 72 hodín od doby jeho zistenia, je súčasťou vnútorných smerníc/politík.	○	○	◉

Obrázok č. 55: GDPR - povinnosti 2 (Zdroj: Vlastné spracovanie podľa (5))

4.5. Vytvorenie výkonnostných ukazovateľov

Poslednou fázou metodického postupu pre vytvorenie výkonnostného ukazovateľa je vyhodnotenie zadaných údajov.

K tomu slúžiť tlačidlo označené ako „Vyhodnotiť“.



Obrázok č. 56: Vytvorenie ukazovateľov (Zdroj: Vlastné spracovanie)

Po jeho aktivácií sa spustí makro, ktoré najprv preverí, či bol určení rozsah hodnotenia (1. fáza), ak nebol, upozorní na túto skutočnosť MsgBoxom a ukončí sa. Ak bol riadne určený (v pravom hornom rohu sú vypísané vybrané možnosti), zistí ktoré možnosti boli vybrané a podľa toho vyhodnotí výkonnosť vo vybraných oblastiach.

Pri vytváraní ukazovateľov sa berie do úvahy váha nastavená jednotlivým opatreniam/požiadavkám a číselné hodnotenie každej odpovede - stĺpce J a K (vysvetlenie viď vyššie). V prípade, že je niektoré opatrenia neaplikovateľné, je možné, ako už bolo napísané vyššie, priradiť mu váhu 0, čo zapríčiní, že žiadnym spôsobom neovplyvní výsledné hodnotenie.

Ak bola v prvej fáze zvolená len povinná osoba/orgán v rámci KBZ a na otázky o ISMS a GDPR boli dané záporné odpovede, do listu „Vyhodnotenie“ sa vytvoria iba ukazovatele k tomu prislúchajúce. V prípade, že ide o subjekt, ktorý má povinnosti dané len v rámci KBZ, zobrazí sa len hodnotenie „Všeobecných požiadaviek“, ak ale patrí k povinným osobám s povinnosťou zavádzať aj opatrení z VKB, budú vypočítané aj ukazovatele predstavujúce percento plnenia technických a organizačných opatrení, spolu s ukazovateľom výkonnosti z pohľadu KBZ.

Ak bola v prvej fáze zvolená aj (len) možnosť ISMS, vypočítajú sa výsledky pre každú skupinu opatrení a tiež ukazovateľ výkonnosti z pohľadu ISMS. V prípade, že bol zvolený aj povinný subjekt KBZ vypočíta sa tiež ukazovateľ celkového hodnotenia výkonnosti z pohľadu informačnej bezpečnosti. Tento ukazovateľ predstavuje vážený priemer ukazovateľov výkonnosti z pohľadu KBZ a z pohľadu ISMS, pričom ukazovateľ z pohľadu ISMS má dvojnásobnú váhu.

Pri určovaní ukazovateľa výkonnosti v rámci GDPR sa vychádza podobne, čo znamená, že ak bola v prvej fáze odpoveď na otázku o GPDR kladná, vypočíta sa ukazovateľ predstavujúci percento plnenia aj pre toto nariadenie.

S úspešným dokončením výpočtu ukazovateľov sa ukáže MsgBox informujúci o tejto skutočnosti.

Prezentácií výsledných ukazovateľov pre údaje zadané v predchádzajúcej fáze, spolu s interpretáciou a možným využitím týchto výsledkov sa budem zaoberať v nasledujúcej kapitole.

4.6. Manažérske rozhodovanie

Náplňou tejto kapitoly je teda ukážka výsledkov navrhnutej metodiky tvorby výkonnostných ukazovateľov informačnej bezpečnosti a ich možné využitie v procese manažérskeho rozhodovania.

Tab. č. 3: Výsledky hodnotení jednotlivých kategórií

Kategória	Ukazovateľ
Všeobecné požiadavky KBZ:	43,75 %
Organizačné opatrenia VKB:	51,88 %
Technické opatrenia VKB:	74,60 %
Všeobecné požiadavky ISMS:	38,89 %
Analýza rizík:	83,33 %
Politiky bezpečnosti informácií:	59,09 %
Organizácia bezpečnosti informácií:	61,11 %
Bezpečnosť ľudských zdrojov:	43,75 %
Riadenie aktív:	75,00 %
Riadenie prístupu:	50,00 %
Kryptografia:	83,33 %
Fyzická bezpečnosť a bezpečnosť prostredia:	43,33 %
Bezpečnosť prevádzky:	71,88 %
Bezpečnosť komunikácie:	77,78 %
Akvizícia, vývoj a údržba systémov:	61,11 %
Vzťahy s dodávateľmi:	41,67 %
Riadenie incidentov bezpečnosti informácií:	72,22 %
Aspekty riadenia kontinuity činnosti organizácie z hľadiska bezpečnosti informácií:	87,50 %
Povinnosti GDPR:	53,57 %

(Zdroj: Vlastné spracovanie)

Prvá tabuľka ukazuje výsledky hodnotenia v jednotlivých kategóriách. Prvé tri sa vzťahujú k požiadavkám daným v kybernetickom zákone a kybernetickej vyhláške. Ďalších 15 patrí k systému riadenia bezpečnosti informácií a posledný ku GDPR. Hodnoty ukazovateľov pri jednotlivých oblastiach určujú mieru (percento) plnenia povinností, respektíve mieru zavedenia opatrení určených v jednotlivých oblastiach.

Tab. č. 4: Ukazovatele výkonnosti

	Číselné hodnotenie	Slovné hodnotenie
Ukazovateľ výkonnosti z pohľadu KBZ:	**56,79 %**	Stredná
Ukazovateľ výkonnosti z pohľadu ISMS:	**60,45 %**	Stredná
Ukazovateľ celkovej výkonnosti z pohľadu informačnej bezpečnosti:	**59 %**	Stredná

(Zdroj: Vlastné spracovanie)

Táto tabuľka už ukazuje jednotlivé vypočítané ukazovatele výkonnosti podniku. Prvý ukazovateľ predstavuje výkonnosť podniku len z pohľadu KBZ a jeho plnenia, druhý ukazovateľ ukazuje výkonnosť z pohľadu ISMS, tretí ukazovateľ predstavuje kombináciu predchádzajúcich dvoch a ukazuje celkovú výkonnosť organizácie z pohľadu informačnej (a kybernetickej) bezpečnosti. Detail jeho výpočtu je uvedený v predchádzajúcej kapitole.

Pre slovné hodnotenie výkonnosti sa používa hodnotiaca stupnica uvedená v nasledujúcej tabuľke.

Tab. č. 5: Hodnotiaca stupnica výkonnosti

Hodnotiaca stupnica výkonnosti		
Od	*Do*	*Výkonnosť*
0,00	0,10	Veľmi nízka
0,10	0,40	Nízka
0,40	0,70	Stredná
0,70	0,90	Vysoká
0,90	1,00	Veľmi vysoká

(Zdroj: Vlastné spracovanie)

Pre hodnotenie výkonnosti „Veľmi vysoká“ je potrebné mať ukazovateľ výkonu vyšší ako 90 %. Čo znamená mať pokryté všetky oblasti ISMS a zavedenú väčšinu opatrení z VKB.

Vzhľadom na explicitný význam získaných ukazovateľov, môže manažér takýmto spôsobom zistiť, ako si v rámci informačnej bezpečnosti a plnenia zákonných požiadaviek stojí a reagovať na prípadné nedostatky. Pretože sú jednotlivé skupiny opatrení ISMS ohodnotené aj samostatne, vie tak určiť, ktoré oblasti sú nedostatočne pokryté a je ich potrebné riešiť. Taktiež si môže jednotlivé ukazovatele zaznamenávať a sledovať, ako sa podniková informačná bezpečnosť vyvíja v čase, či sa niekam posúva alebo nie. Takto získané údaje je možné prezentovať aj vedeniu firmy a požadovať od nich viac zdrojov na pokrytie „nezabezpečených“ oblastí, ak sa im vysvetlí nutnosť a správnosť tohto kroku. V prípade nízkych hodnotení výkonnosti totiž hrozí riziko, že prípadný bezpečnostný incident môže mať veľké dopady a ohroziť nie len firmu samotnú, ale aj jej okolie, čo môže mať vplyv na jej finančné výsledky, ale aj na jej existenciu.

5. Zhodnotenie a prínosy práce

V rámci mojej diplomovej práce som vytvoril metodiku na vytváranie výkonnostných ukazovateľov na základe riadenia informačnej bezpečnosti, zákona o kybernetickej bezpečnosti a všeobecného nariadenia pre ochranu osobných údajov. Vzhľadom na množstvo nevyriešených oblastí v rámci bezpečnosti informácií v analyzovanej firme, im táto metodika pomôže identifikovať oblasti, ktoré musí začať riešiť a ktoré opatrenia musí zaviesť, aby sa ich výkonnosť zlepšila.

Toto zlepšenie je nutné nie len z dôvodu zachovania bezpečnosti informácií v rámci organizácie, ale aj z dôvodu platných zákonov. Tie predpisujú povinným osobám veľké množstvo povinností a opatrení, ktoré musia zaviesť. Neimplementovanie povinných opatrení a neplnenie si ďalších povinností vyplývajúcich zo zákona, môže pre firmu znamenať pokutu až 5 000 000 Kč. V prípade neplnenia povinností uvedených v európskom nariadení GDPR môže byť dokonca uložená pokuta až do výšky 20 000 000 EUR (alebo 4 % celkového ročného obratu, podľa toho ktorá suma bude vyššia), čo je už dosť veľká suma na to, aby bola ignorovaná.

Aj keď do začiatku platnosti GDPR ostáva ešte viac ako rok, je potrebné ho začať riešiť už skôr a vyhnúť sa prípadným problémom, ktoré by mohli vzniknúť. Mnou navrhnutá metodika, kde sú uvedené aj najhlavnejšie povinnosti tohto nariadenia, s tým môže podniku pomôcť a ušetriť im tak financie, ktoré by museli minúť na platenie pokút v prípade problémov. Nehovoriac o tom, že zákon o kybernetickej bezpečnosti je v platnosti už viac ako rok, preto s implementáciou opatrení netreba vyčkávať.

Kybernetický zákon tu nie je len na to, aby chránil samotné organizácie, ale hlavne preto, aby prípadný bezpečnostný incident nemal vážnejšie následky celospoločenského významu, preto by sa subjekty, ktorým sa v rámci zákona ukladajú povinnosti, nemali ich plneniu vyhýbať, ale začať rýchlo konať. K tomu môže pomôcť aj mnou navrhnutá metodika, ktorá im uľahčí sa zorientovať v tom, ktoré opatrenia majú zaviesť a ako na tom momentálne sú.

Spísanie všetkých požiadaviek a opatrení z noriem a zákonov mi zabralo desiatky hodín práce. Rovnako ako naprogramovanie makra vo VBA, ktoré mi taktiež zabralo okolo 20 hodín času a to najmä z dôvodu množných variácií výberu. Finálne makro má tak viac ako 900 riadkov a viac ako 28 tisíc znakov. V rámci metodiky sú tak, ale riešené všetky prípady, ktoré môžu nastať a vytvoril som tak univerzálny nástroj, ktorý môže byť použitý aj iným subjektom než firmou, ktorá je objektom analýzy súčasnej situácie.

Táto univerzálna metodika tak môže byť použitá na zisťovanie výkonnostných ukazovateľov v každej spoločnosti, ktorá chce riešiť svoju informačnú (a kybernetickú) bezpečnosť, a každej firme ktorá musí riešiť spracovávanie osobných údajov.

Záver

Cieľom mojej diplomovej práce bolo pre vybraný podnik navrhnúť metodický postup na vytváranie výkonnostných ukazovateľov na základe informačnej bezpečnosti, kybernetického zákona a európskeho nariadenia GDPR. Po analýze spoločnosti som určil, akým spôsobom budem výkonnosť v daných oblastiach posudzovať a vybral vhodný nástroj na tvorbu tejto metodiky.

Keďže som sa rozhodol spracovať danú metodiku v programe Microsoft Excel za použitia programovacieho jazyka VBA, ďalším krokom bolo spracovať do dokumentu všetky požiadavky a opatrenia súvisiace so systémom riadenia bezpečnosti informácií, zákonom o kybernetickej bezpečnosti, a s ochranou osobných údajov. Vychádzal som pri tom z opatrení uvedených vo vyhláške kybernetického zákona, opatrení z normy ČSN ISO/IEC 27002 a povinností z nariadenia GDPR.

Následne som za pomoci programovacieho jazyka VBA naprogramoval makrá, ktoré organizácií pomôžu určiť, aký typ povinnej osoby je. V rámci tejto naprogramovanej procedúry sa teda zobrazí séria otázok a na základe odpovedí na tieto otázky, sa zobrazia len tie povinnosti / opatrenia, ktoré sa daného výberu týkajú. Táto procedúra taktiež vygeneruje prepínacie tlačidlá (OptionButton-y) ku každej povinnosti / opatreniu, ktoré umožňujú vybrať stupeň splnenia danej požiadavky (splnené, čiastočne splnené, nesplnené). V ďalšom kroku som naprogramoval makro, ktoré rieši už samotný výpočet ukazovateľov výkonnosti. Pričom makro je naprogramované tak, že ukazovatele výkonnosti vypočíta len pre oblasti vybrané v prvej fáze metodiky.

Následne som vytvorenú metodiku overil za pomoci testovacích údajov, popísal interpretáciu výsledkov a uviedol možné využitie týchto výsledkov v praxi. Na záver som zhodnotil prínos tejto metodiky pre podnik, v čom im môže pomôcť a taktiež som do zhodnotenia napísal, koľko času mi spracovanie tejto metodiky zabralo.

Navrhnutá metodika nie len, že spĺňa zadaný cieľ tejto práce, ale ho dokonca aj presahuje. Je totiž univerzálna a je ju tak možné použiť v akomkoľvek type organizácie.

Zoznam použitej literatúry

(1) ČESKÁ REPUBLIKA. Zákon o kybernetické bezpečnosti. In: *Sbírka zákonů*. Praha, ročník 2014, číslo 181.

(2) ČESKÁ REPUBLIKA. Vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů*. Praha, ročník 2014, číslo 316.

(3) ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(4) ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(5) EURÓPSKA ÚNIA. Nariadenie Európskeho parlamentu a rady (EÚ). In: *Úradný vestník Európskej únie*. Brusel, ročník 2016, číslo 679.

(6) ISO/IEC 2382:2015. *Information technology - Vocabulary.* Ženeva: International Organization for Standardization, 2015.

(7) NIST.IR.7298r2. *Glossary of Key Information Security Terms.* Gaithersburg: National Institute of Standards and Technology, 2013.

(8) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(9) ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* Ženeva: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

(10) SEDLÁK, Petr. *Management informační bezpečnosti.* Prednáška. Brno: Vysoké učení technické, Fakulta podnikatelská, akademický rok 2015/2016 a 2016/2017.

(11) IsecT. ISO27k infosec management standards. *Iso27001security.com* [online]. © 2017 [cit. 2017-05-14]. Dostupné z: http://iso27001security.com/

(12) Advisera Expert Solutions. ISO 27001:2013 list of mandatory documents and records. *Advisera.com* [online]. © 2017 [cit. 2017-05-15]. Dostupné z: https://advisera.com/27001academy/knowledgebase/list-of-mandatory-documents-required-by-iso-27001-2013-revision/

(13) JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
(14) EURÓPSKA ÚNIA. Smernica Európskeho parlamentu a rady (EÚ). In: *Úradný vestník Európskej únie*. Brusel, ročník 2016, číslo 1148.
(15) Vláda ČR. Materiál - Portál Aplikace ODok. *Odok.cz* [online]. © 2017 [cit. 2017-05-14]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=ALBSABVH86O2

Zoznam obrázkov

Zoznam tabuliek

Zoznam použitých skratiek

ZKB -	Zákon o kybernetickej bezpečnosti
VKB -	Vyhláška o kybernetickej bezpečnosti
KBU -	Kybernetická bezpečnostná udalosť
KBI -	Kybernetický bezpečnostný incident
KII -	Kritická informačná infraštruktúra
KS -	Komunikačný systém
IS -	Informačný systém
VIS -	Významný informačný systém
PZS -	Prevádzkovateľ základnej služby
PDS -	Poskytovateľ digitálnej služby
ISMS -	Systém riadenia bezpečnosti informácie
NIS -	Network and Information Security
GDPR -	General Data Protection Regulation
VBA -	Visual Basic for Applications