

Systém na podporu vypracovania bezpečnostných projektov pre malé ISVS

Anton Kica

Školiteľ

RNDr. Daniel Olejár, PhD

FMFI Matfyz

2023

Žijeme v spoločnosti

- ▶ kde postupne nastáva informatizácia v digitálnej forme
- ▶ štátne inštitúcie, banky, firmy využívajú d-IKT(digitálne informačné a komunikačné technológie)
- ▶ je potreba ochrany týchto technológií a informácií

Právny podklad

- ▶ Vyhláška č. 179/2020 Z. z.
Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
 - ▶ vymedzuje kategorie a obsah bezpečnostných opatrení ITVS
- ▶ Zákon č. 95/2019 Z. z.
Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
 - ▶ vymedzuje organizáciu správy ITVS
 - ▶ vymedzuje základné požiadavky kladené na ITVS

Menšie okno do vyhlášky č. 179/2020

§ 3

Minimálne bezpečnostné opatrenia

- (1)** Minimálne bezpečnostné opatrenia upravuje príloha č. 2 a sú rozdelené do Kategórie I, Kategórie II a Kategórie III v rámci jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti.
- (2)** Minimálne bezpečnostné opatrenia Kategórie I jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na
- a)** obec do 6000 obyvateľov,
 - b)** obec so štatútom mesta do 6000 obyvateľov,
 - c)** právnickú osobu v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia podľa § 5 ods. 2 písm. a) až d) zákona, ktorá nie je uvedená v odsekoch 3 a 4,
 - d)** osobu podľa § 5 ods. 2 písm. g) zákona,
 - e)** komoru podľa § 5 ods. 2 písm. f) zákona.

Obr.: <https://www.zakonypreludi.sk/zz/2020-179>

Menšie okno do vyhlášky č. 179/2020

MINIMÁLNE BEZPEČNOSTNÉ OPATRENIA

- ▶ A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti
Kategória I
 - a) Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
 - b) Vypracovanie a implementácia interného riadiaceho aktu, ktorý je pre organizáciu správcu záväzný a obsahuje najmenej
 1. určenie povinnosti, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti,
 2. základné zásady a opatrenia kybernetickej bezpečnosti a informačnej bezpečnosti, ktoré organizácia správcu má zavedené a riadi sa nimi.
- ▶ B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti
- ▶ C. Personálna bezpečnosť
- ▶ ...
- ▶ P. Audit a kontrolné činnosť

Kde nastáva problém

- ▶ mnoho systémov, ktoré potrebujú komunikovať s ITVS
- ▶ nedostatok odborníkov na KIB (kybernetickú a informačnú bezpečnosť)
- ▶ vrámci organizácie osoba poverená KIB nemusí mať primeranú úroveň vedomostí

Cieľ našej práce

Predpokladáme, že vrámci organizácie manažér KIB

- ▶ nemá vedomosti z KIB
- ▶ nemá dostatok prostriedkov

my tejto osobe chceme pomôcť

- ▶ splniť si základné zákonné povinnosti
- ▶ zaviesť v organizácii systém ISMS
- ▶ udržiavať KIB na primeranej úrovni

Čo nám pomôže pri tvorbe takéhoto systému

pár nemeckých štandardov

- ▶ BSI-Standard 200-1
- ▶ BSI-Standard 200-2
- ▶ BSI-Standard 200-3
- ▶ IT-Grundschutz Compendium



or so the Germans would have us believe

Chceme teda

poskytnúť systém na zavedenie ISMS, ktorý bude obsahovať interaktívny návod a

- ▶ stručne zdôvodní zákonné povinnosti
- ▶ poskytne referencie na detailnejšie materiály
- ▶ postupne bude tvoriť databázu a zbierať informácie pre KIB

pričom získané informácie bude možno použiť na

- ▶ analýzu rizík
- ▶ evidenciu bezpečnostných incidentov
- ▶ monitorovanie aktuálneho stavu KIB v organizácií

a to by mal predstavovať náš systém na podporu vypracovania bezpečnostných projektov pre malé ISVS

Koniec

Ďakujem za vašu pozornosť

Pár pojmov

- ▶ aktívum (asset) čokoľvek, čo má pre organizáciu hodnotu, čokoľvek, čo je:
 - ▶ hmotné (zariadenia, personál..) alebo nehmotné (peniaze, informácia),
 - ▶ môže sa stať objektom útoku a
 - ▶ vyžaduje si ochranu
- ▶ informačná bezpečnosť - multiodborová disciplína, ktorá sa zaoberá
 - ▶ hrozbami voči systémom/aktívam a
 - ▶ metódami, ako aktíva pred hrozbami chrániť
- ▶ kybernetický priestor - globálny dynamický otvorený systém, ktorý tvoria:
 - ▶ telekomunikačné a počítačové siete,
 - ▶ informačné a komunikačné systémy, ich programové vybavenie
 - ▶ a údaje, ktoré sa pomocou nich spracovávajú

zdroj: Olejár D., Krátky úvod do informačnej a kybernetickej bezpečnosti a Malý výkladový slovník