



Spisová služba a Zákon o kybernetické bezpečnosti (181/2014 Sb.)

Milan Vojáček

Praha, 22. 3. 2016

Významné informační systémy (VIS)

- Definice dle §2 písm. d) ZKB: *„informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci“*
- Identifikace konkrétních VIS závislá na **vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích**
- Je mířeno směrem k zajištění působnosti orgánů veřejné moci

Dopadová kritéria I (§4 písm. a)

a) úplná nebo částečná nefunkčnost IS způsobená narušením bezpečnosti informací by mohla mít negativní vliv na:

- 1. fungování orgánu veřejné moci**
- 2. poskytování služeb nebo informací orgánem veřejné moci veřejnosti**
- 3. hospodaření orgánu veřejné moci nebo hospodaření orgánu veřejné moci, který je správcem významného informačního systému, anebo hospodaření orgánu nebo osoby, která je správcem informačního nebo komunikačního systému kritické informační infrastruktury**
- 4. provoz jiného významného informačního systému využívajícího služeb hodnoceného informačního systému, který je nefunkční**

příčemž omezení činnosti takového systému by mohlo mít za následek omezení výkonu působnosti orgánu veřejné moci po dobu delší než 3 pracovní dny, nebo výrazné ohrožení výkonu působnosti orgánu veřejné moci, které lze odvrátit za vynaložení nepřiměřených nákladů na provoz nebo obnovu informačního systému.

Dopadová kritéria II (§4 písm. b)

b) úplná nebo částečná nefunkčnost informačního systému způsobená narušením bezpečnosti informací by mohla způsobit:

- 1. ohrožení nebo narušení prvku kritické infrastruktury**
- 2. oběti na životech s mezní hodnotou více než 10 mrtvých nebo 100 zraněných osob vyžadujících lékařské ošetření, s případnou hospitalizací s dobou delší než 24 hodin**
- 3. finanční nebo materiální ztráty s mezní hodnotou více než 5% stanoveného rozpočtu orgánu veřejné moci**
- 4. zásah do osobního života nebo do práv fyzických nebo právnických osob postihující nejméně 50 000 osob**
- 5. výrazné ohrožení nebo narušení veřejného zájmu**

přičemž následky podle bodů 1 až 4 nedosáhnou hodnot pro určení prvku kritické infrastruktury podle průřezových kritérií stanovených krizovým zákonem.

VIS – oblastní kritéria

Příloha č. 2 k vyhlášce o VIS a jejich určujících kritériích

I. U orgánu veřejné moci

1. vedení správního řízení,
2. databáze obsahující osobní údaje,
3. hospodaření orgánu veřejné moci,
4. výkon spisové služby,
5. státní dozor,
6. kontrolní a inspekční činnost,
7. příprava na krizové situace a jejich řešení,
8. tvorba právních předpisů,
9. elektronická pošta,
10. vedení internetových stránek,
11. mezirezortní spolupráce,
12. mezinárodní spolupráce,
13. zadávání veřejných zakázek,
14. státní statistická služba.

Určení VIS

1) VIS přímo stanovené v příloze č. 1 Vyhlášky č. 317/2014 Sb.

2) VIS posouzené správcem na základě určujících kritérií

(§ 3 vyhlášky č. 317/2014)

- Zákon výslovně nezmiňuje doklad o posouzení
- Ideálně interní akt schválený statutárem, jehož součástí je:
- Seznam posouzených IS
- U IS naplňujících kritéria pro VIS – odkaz na naplněná kritéria
- Identifikace odpovědné osoby za konkrétní VIS, úkoly, odpovědnost
- Datum schválení, podpis

Povinnosti dle ZKB

- Nahlášení kontaktních údajů (§16 ZKB)
- Hlášení kybernetických bezpečnostních incidentů (§8 ZKB)
- Zavést bezpečnostní opatření (standardizace) (§4 ZKB)
- Činit opatření vydané NBÚ (§11 ZKB)

Vyhláška č. 316/2014 o kybernetické bezpečnosti

Rozpracovává oblasti bezpečnostních opatření stanovené zák. 181/2014 Sb. a definuje konkrétní požadavky na organizace či osoby (§ 3-27)

• Organizační opatření

- a) systém řízení bezpečnosti informací,
- b) řízení rizik,
- c) bezpečnostní politika,
- d) organizační bezpečnost,
- e) stanovení bezpečnostních požadavků pro dodavatele,
- f) řízení aktiv,
- g) bezpečnost lidských zdrojů,
- h) řízení provozu a komunikací KII nebo VIS,
- i) řízení přístupu osob ke KII nebo k VIS,
- j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,
- k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- l) řízení kontinuity činností
- m) kontrola a audit kritické informační infrastruktury a významných informačních systémů.

• Technická opatření

- a) fyzická bezpečnost,
- b) nástroj pro ochranu integrity komunikačních sítí,
- c) nástroj pro ověřování identity uživatelů,
- d) nástroj pro řízení přístupových oprávnění,
- e) nástroj pro ochranu před škodlivým kódem,
- f) nástroj pro zaznamenávání činnosti KII a VIS, jejich uživatelů a administrátorů,
- g) nástroj pro detekci kybernetických bezpečnostních událostí,
- h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- i) aplikační bezpečnost,
- j) kryptografické prostředky,
- k) nástroj pro zajišťování úrovně dostupnosti informací
- l) bezpečnost průmyslových a řídicích systémů.

Úskalí a dopady

- 1) Další povinnosti a náklady
- 2) Možné sankce

Proč tedy usilovat o VIS?

Důvody pro určení IS jako VIS

- 1) Vyhnout se problémům spojeným s kybernetickým útokem a následnými výdaji na obnovu IS, úniku citlivých dat, omezením výkonu veřejné moci apod.
- 2) Možnost čerpat dotace na technická opatření
- výzva č. 10 IROP *Kyberbezpečnost*
- 3) Vzít v úvahu při pořizování nových systémů nebo při rozvoji stávajících systémů
- výzva č. 23 IROP

Informační a komunikační systémy a infrastruktura I.