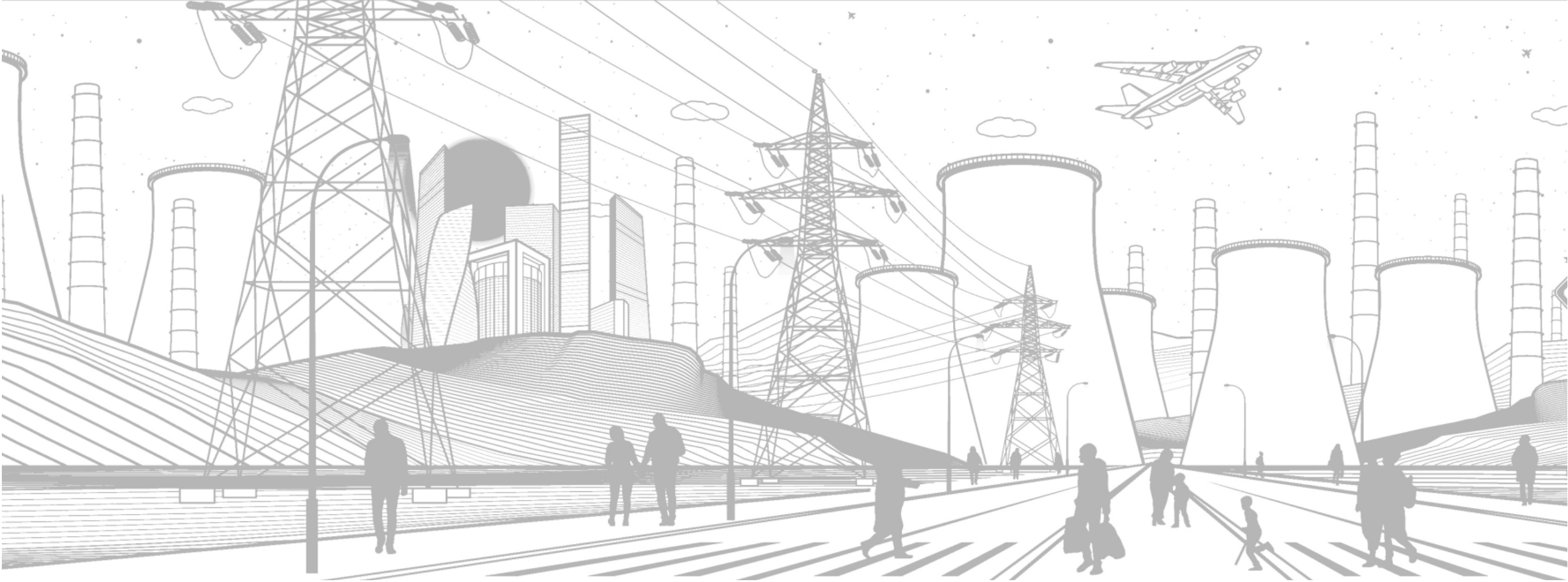

Novela zákona o kybernetické bezpečnosti – připomínky AKI

28. března 2022 | Jakub Ludvík, Asociace kritické infrastruktury ČR

Asociace kritické infrastruktury
České republiky

„Asociace kritické infrastruktury ČR rozvíjí odolnost kritické (informační) infrastruktury státu a jeho připravenost na krizové stavy“

Asociace kritické infrastruktury
České republiky

Připomínky

1. Zavedení nástrojů centralizace v rámci podnikatelských skupin spočívajících v možnostech:

   1) skupinového řízení kybernetické bezpečnosti,

   2) ustanovení jedné pověřené osoby pro celou skupinu,

   3) dobrovolného sjednocení režimů povinností v rámci skupiny,

   4) zajištění zákonných povinností třetími stranami.

2. Zmírnění požadavků kladených na

   poskytovatele regulované služby v režimu nižších povinností a přehodnocení významu institutu inspektorů

3. Nepřehledné zveřejňování informací více kanály

Asociace kritické infrastruktury České republiky

Připomínky

4. Lepší ukotvení bezpečnostních rolí a jasnější vymezení jejich odpovědností přímo do zákona, nikoli formou vyhlášky nebo pouhých doporučení

5. Možnost určit významné dodavatele subjektu KI jako poskytovatele regulované služby v režimu vyšších povinností na základě podnětu určeného poskytovatele regulované služby v režimu vyšších povinností

6. Omezení povinnosti hlášení kybernetických incidentů pouze na významné incidenty

7. Zveřejňování informací o kybernetickém bezpečnostním incidentu jen po konzultaci s poskytovatelem regulované služby

8. Právo odmítnout zveřejnění informací o kybernetickém bezpečnostním incidentu, pokud mají negativní dopad na provoz nebo na bezpečnost regulované služby a povinné osoby

9. Stanovení limitů pro součinnost povinných osob a zrušení bezplatnosti

Přípomínky

10 Změnit definici lhůt pro lepší dosažení záměru zákona

11 Narovnání definici Prohlášení o aplikovatelnosti v souladu s ISO/IEC 27001, zavedenou praxí a ustáleným významem ve znění:

„…prohlášení o aplikovatelnosti, které obsahuje přehled všech bezpečnostních opatření požadovaných touto vyhláškou, která, i) jsou aplikovatelná včetně odůvodnění jejich aplikovatelnosti a zda jsou nebo nejsou zavedena ii) jsou neaplikovatelná včetně zdůvodnění jejich neaplikovatelnosti“

Asociace kritické infrastruktury České republiky