**Technické specifikace**

**1. Současný stav**

Česká obchodní inspekce (dále jen „ČOI“) provozuje dle vyhlášky č. 317/2014 Sb., o významných IS, od roku 2018 významný informační systém (dále jen „VIS“) Mercurius. Tento systém podporuje plnění kompetencí ČOI v oblasti kontroly vnitřního trhu ČR a souvisejících činností. V návaznosti na tyto skutečnosti, povinnosti vyplývající ze zákona a vyhlášky o kybernetické bezpečnosti, byly v ČOI v období 2018-19 zpracovány a cestou ústředního ředitele ČOI vydány tyto dokumenty:

1. Rozdílová analýza informačních a komunikačních systémů ČOI
2. Systémová bezpečnostní politika
3. Směrnice pro ochranu osobních údajů
4. Určení bezpečnostních rolí
5. Řízení rizik a analýza rizik
6. Politika bezpečného chování uživatelů
7. Informační koncepce

Je definován Systém řízení bezpečnosti informací pokrývající rámec organizačního uspořádání ČOI. Na základě resortní smlouvy (MPO) byla ČOI v letech 2018-2020 zahrnuta do externího auditu kybernetické bezpečnosti, který prováděla 2 x ročně firma AlefNula, a. s. Z těchto externích auditů jsou k dispozici kontrolní zprávy. Na základě opatření ústředního ředitele „Určení bezpečnostních rolí“ byl ustanoven Výbor KB ČOI, který se schází 2x ročně a vyhodnocuje stav a přijatá opatření v KB. Manažer KB ČOI je členem rozšířeného výboru KB MPO. V rámci analýzy rizik jsou definována primární, podpůrní aktiva, hrozby, zranitelnosti a míra rizik. Je zpracováno prohlášení o aplikovatelnosti a je definován plán zvládání rizik. Jsou evidovány bezpečnostní incidenty a události.

ČOI provozuje v souladu s požadavky platné legislativy bezpečnostní technologie, jejichž cílem je chránit vnitřní perimetr organizace. Je realizována segmentace sítě a nasazen protokol 802.1X.

**2. Požadovaný stav**

V návaznosti na současný stav se požaduje dodání bezpečnostních politik dle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, příloha č. 5, odst. 1.1. – 1.23. Pokud již tato politika existuje, potom se požaduje její aktualizace tak, aby tato „zapadla“ do celého kontextu dodaných dokumentů. V tomto smyslu se i předpokládá doporučení (nikoliv vypracování) aktualizace dokumentu řízení rizik (§ 5 vyhlášky o KB), obdobně doporučení v oblasti Politiky řízení kontinuity činností, pokud tato předpokládá existenci jiných dokumentů (Analýza dopadů). Pokud existující stav brání vypracování požadované politiky se standardní mírou detailu, bude dodán v obecnější podobě s doporučeními přijetí konkrétních opatření.

Dále se požaduje návrh vhodného seskupení (optimalizace) dodaných politik tak, aby nebylo navrhováno k vydání 23 opatření ústředního ředitele ČOI (23 politik).