Žádost č. 10:

Dovoluji si Vás proto požádat o zodpovězení následujících otázek:

1. Jakým způsobem se na Váš úřad konkrétně vztahuje implementace směrnice NIS 2 do českého právního řádu, spadáte do kategorie nižších, nebo vyšších povinností?
2. Jaké nové povinnosti v oblasti kybernetické a informační bezpečnosti pro Váš úřad z implementace směrnice NIS 2 vyplývají?
3. Jaké organizační změny musel nebo musí Váš úřad v souvislosti s implementací směrnice NIS 2 učinit (např. úprava vnitřních předpisů, změna v řízení IT/bezpečnosti)?
4. Jaké personální změny byly nebo budou realizovány (např. navýšení počtu zaměstnanců odpovědných za kybernetickou bezpečnost, posílení IT oddělení)?
5. Jaká školení či vzdělávací aktivity v oblasti kybernetické bezpečnosti byla zavedena pro zaměstnance Vašeho úřadu v souvislosti s požadavky vyplývajícími z NIS 2?
6. Jaké finanční náklady (orientačně či v odhadovaném rozpětí) si implementace požadavků směrnice NIS 2 vyžádala nebo vyžádá v rozpočtu Vašeho úřadu (např. vyčlenění na personální náklady, školení, infrastrukturu, služby externích dodavatelů)?
7. Jaká materiální a technická opatření byla či budou v souvislosti s NIS 2 realizována (např. obměna hardware, zavedení nových bezpečnostních technologií, systémů pro monitorování a detekci incidentů, zálohovací a obnovovací řešení)?
8. Zda byl v souvislosti s NIS 2 vytvořen nebo aktualizován soubor vnitřních bezpečnostních politik a metodik (např. bezpečnostní politika, politika řízení přístupů, řízení rizik, kontinuita provozu, incident response plány), a pokud ano, v jakém rozsahu?
9. Jakým způsobem Váš úřad zajišťuje analýzu a řízení rizik v oblasti kybernetické bezpečnosti po účinnosti nové právní úpravy vycházející z NIS 2?
10. Zda Váš úřad podstoupil (nebo plánuje podstoupit) v souvislosti s implementací NIS 2 nějaké externí audity, penetrační testy či jiné formy nezávislého ověřování úrovně kybernetické bezpečnosti?