DEVATERO ODBORU KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI

ALEŠ ŠPIDLA

KYBERNETICKÁ A INFORMAČNÍ BEZPEČNOST

Všeobecným záměrem uvedených aktivit je podpora budování důvěryhodné **informační společnosti**, jejích legislativních, technických, organizačních a dalších základů, s důrazem na ochranu informací ve všech oblastech lidské činnosti a rozvoj svobodného a bezpečného využívání a sdílení informací.

Výčet jednotlivých zamýšlených kroků

1) Strategický dokument

- ***Aktivita:*** Zpracování základního strategického dokumentu, definujícího strategické cíle a prioritní oblasti, vztahující se k zajištění kybernetické bezpečnosti České republiky (s ohledem na další strategické bezpečnostní materiály z domova i ze zahraničí).
- ***Cíl:*** Přijetí Strategie pro kybernetickou bezpečnost v České republice.

2) Legislativní rámec

- ***Aktivita:*** Analýza právního prostředí České republiky (s porovnáním právního prostředí zemí Evropské unie a dalších zemí světa). Na základě výsledků analýzy zpracování věcného záměru novelizace existujících právních norem nebo zpracování věcného záměru nového zákona o kybernetické bezpečnosti (se zvláštním zřetelem na respektování základních lidských práv svobod a účinnou ochranu osobních údajů).
- ***Cíl:*** Vytvořit právní normy reflektující nové právní skutečnosti v souvislosti s kybernetickou a informační bezpečností. Připravit právní rámec norem, směrnic a předpisů, které budou vymezovat, upravovat a standardizovat práva a povinnosti subjektů veřejného a soukromého sektoru při ochraně kybernetického prostoru – jako nezbytné podmínky funkční, proaktivní a reaktivní ochrany komunikační infrastruktury před kybernetickými hrozbami.

3) Standardy v oblasti kybernetické a informační bezpečnosti

- ***Aktivita:*** Provední analýzy v současné době používaných bezpečnostních standardů, jejich dodržování a vymahatelnosti zejména ve státní správě a subjektech zahrnutých do kritické infrastruktury. Návrh implementace standardů a návrh způsobu zajištění jejich vymahatelnosti. Stanovení minimálního souboru technických prostředků, činností a požadovaných funkcí uživatelů informační a komunikační infrastruktury pro zabezpečení včasného řešení bezpečnostních incidentů. Návrh na vytvoření systému pro kontrolu dodržování a funkčnosti bezpečnostních standardů.
- ***Cíl:*** Vytvořit standardní, z pohledu kybernetické bezpečnosti bezpečné prostředí, se srozumitelnými, jasně definovanými a důsledně „vymahatelnými“ pravidly.

4) Vnitrostátní koordinace a komunikace mezi zainteresovanými veřejnými subjekty

- ***Aktivita:*** Koordinace relevantních domácích veřejných institucí, týkající se oblasti informační bezpečnosti. Vybudování prostředků důvěryhodné komunikace na domácí úrovni (Armáda České republiky, Národní bezpečnostní úřad, zpravodajské služby České republiky) s odpovídajícím technickým, procesním a personálním zajištěním
- ***Cíl:*** Koordinovaný a efektivní postup všech zainteresovaných institucí v oblasti informační bezpečnosti přinášející efektivní opatření a využití zdrojů. Vybudování důvěryhodných komunikačních kanálů pro komunikaci s uvedenými institucemi

5) Zefektivnění mezinárodní spolupráce v oblasti zajišťování kybernetické a informační bezpečnosti; Důstojné a sebevědomé zajišťování účasti České republiky v relevantních mezinárodních institucích

- ***Aktivita:*** Vytvoření přehledu mezinárodních institucí (jichž je Česká republika členem), aktivních v oblasti kybernetické a informační bezpečnosti. Vyhodnocení dosavadního zapojení České republiky do fungování těchto platforem a činnosti zástupců České republiky v nich. Aktualizace vize zastupování České republiky v těchto institucích.
- ***Cíl:*** Zlepšení postavení České republiky v rámci uvedených platforem (se zvláštním důrazem na Evropskou unii, Severoatlantickou alianci, Radu Evropy a Organizaci pro bezpečnost a spolupráci v Evropě). Zvýšení akceschopnosti při prosazování cílů České republiky v těchto organizacích.

6) Pracoviště typu CSIRT/CERT

- ***Aktivita:*** Analýza současného stavu (potřeb, prostorových, technických a systémových možností) co se týče zajišťování střechových funkcí v oblasti kybernetické bezpečnosti v České republice. Vytvoření zadávací dokumentace pro vybudování centra pro boj s kybernetickými hrozbami – vládní CERT. Vývoj procesů a standardů pro komunikaci centra s ostatními obdobnými pracovišti v České republice i ve světě. Zajištění jeho monitorovacích, analytických funkcí a forenzních a schopnosti efektivního vyrozumění státních orgánů, institucí, subjektů kritické infrastruktury a participujících pracovišť.
- ***Cíl:*** Vybudování Centra pro boj s kybernetickými hrozbami, určeného pro monitoring vládních sítí a kritické infrastruktury, pro koordinaci a metodické vedení dalších dílčích center tohoto typu, které fungují či budou fungovat v rámci konkrétních veřejných institucí. Toto Centrum se bude mimo jiné zabývat analýzou hrozeb a zranitelností a jejich řešením, sběrem a distribucí informací o hrozbách z/do participujících center. Vytvoření registru incidentů, hrozeb a zranitelností, přístupného odpovídajícím subjektům. Vytvoření pracoviště pro aktivní ochranu kyberprostoru České republiky. Vytvoření systému včasného varování o kybernetických hrozbách.

7) Public relations, vzdělávání profesionálů, uživatelů, vzdělávání v oblasti kybernetické a informační bezpečnosti v rámci školského systému České republiky

Aktivita: Návrh bezpečnostně právního, procesního a technicko-organizačního modelu pro odborné vzdělávání managementu, dalších expertů i širokého spektra koncových uživatelů informačních technologií. Perspektiva doplnění vzdělávacích osnov všech stupňů škol o problematiku kybernetické a informační bezpečnosti. Příprava public-relations kampaně k tématu rizik, souvisejících s užíváním informačních technologií se zaměřením na širokou veřejnost.

- ***Cíl:*** Zvýšení povědomí odborné i laické veřejnosti o hrozbách, souvisejících s užíváním informačních technologií s cílem omezit jejich možný negativní dopad na společnost.

8) Problematika cvičení v oblasti kybernetické a informační bezpečnosti

- ***Aktivita:*** Vypracovat systém a návrhy postupu pro pořádání (respektive účast na) národních i mezinárodních cvičeních tohoto typu (vzdělávací aktivity pro relevantní experty, moderní metody simulace incidentů). Vypracovat návrh pro integraci „kybernetických“ cvičení do rámce „ostatních“ cvičení orgánů krizového řízení.
- ***Cíl:*** Zvýšení připravenosti relevantních managerů a dalších expertů (především v rámci Ministerstva vnitra a veřejné správy České republiky jako celku) na možná ohrožení v informační oblasti. S tím souvisí i snížení zranitelnosti či dokonce úplná eliminace některých bezpečnostních hrozeb. Prohloubení spolupráce a výměny informací orgánů krizového řízení

na národní i mezinárodní úrovni, zaměřené na společné řešení situací spojených s kybernetickými incidenty.

9) Komplexní sdílení know-how v oblasti kybernetické a informační bezpečnosti

- ***Aktivita:*** Vypracovat systém pro zapojení komerční a akademické sféry do spolupráce při řešení akutních i dlouhodobých úkolů v oblasti informační bezpečnosti.
- ***Cíl:*** Vytvoření stabilního know-how zázemí pro efektivní zajišťování úkolů statní správy v oblasti informační bezpečnosti.