Príloha č. 1
k výzve na predkladanie ponúk

Špecifikácia predmetu zákazky

„Návrh programu kontinuálneho vzdelávania, zvyšovania povedomia, špecializovaných školení v oblasti informačnej a kybernetickej bezpečnosti v podsektore ISVS“

Predmetom poradenských služieb bude návrh komplexného programu kontinuálneho vzdelávania a zvyšovania povedomia o kybernetickej bezpečnosti v prostredí Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (ďalej aj „ÚPVII“). (vrátane delimitovanej vládnej jednotky CSIRT a Národnej agentúry pre sieťové a elektronické služby), ktorý bude obsahovať:

a) Návrh programu kontinuálneho vzdelávania v oblasti kybernetickej bezpečnosti,
b) Návrh programu zvyšovania povedomia o kybernetickej bezpečnosti,
c) Návrh obsahu špecializovaných školení kybernetickej bezpečnosti pre jednotlivé cieľové skupiny používateľov v závislosti od ich pracovného zaradenia a odborného zamerania.

Sumár aktivít:

a) Návrh programu kontinuálneho vzdelávania v oblasti kybernetickej bezpečnosti pozostávajúci z/zo:
    - rámcového zmapovania súčasného stavu kontinuálneho vzdelávania v oblasti kybernetickej bezpečnosti v prostredí ÚPVII,
    - zadefinovania vzťahu programu kontinuálneho vzdelávania v oblasti kybernetickej bezpečnosti voči celkovému vzdelávaciemu programu ÚPVII,
    - identifikácie adresovaných cieľových skupín používateľov,
    - identifikácie vzdelávacích aktivít a ich namapovanie na jednotlivé cieľové skupiny,
    - vytvorenia vzdelávacích profilov pozostávajúcich z/zo:
        - stanovenia kvalifikačných stupňov pre jednotlivé cieľové skupiny,
        - identifikácie kompetencií, ktorých dosiahnutie sa očakáva od jednotlivých cieľových skupín,
        - detailného rozpracovania jednotlivých vzdelávacích aktivít,
        - kvantifikácie časovej náročnosti vzdelávacích aktivít pre jednotlivé cieľové skupiny,
        - stanovenia merateľných ukazovateľov pre jednotlivé vzdelávacie aktivity,
        - definovania spôsobu vyhodnocovania merateľných ukazovateľov jednotlivých vzdelávacích aktivít,
    - vytvorenia akčného plánu zavedenia programu v prostredí ÚPVII,
    - zadefinovania spôsobu vyhodnocovania programu kontinuálneho vzdelávania v oblasti kybernetickej bezpečnosti.

b) Návrh programu zvyšovania povedomia o kybernetickej bezpečnosti pozostávajúci z/zo:
   - rámcového zmapovania súčasného stavu povedomia o kybernetickej bezpečnosti v prostredí ÚPVII,
   - rámcového zmapovania súčasného stavu vyspelosti procesu zvyšovania povedomia o kybernetickej bezpečnosti v prostredí ÚPVII,
   - zadefinovania vzťahu programu zvyšovania povedomia o kybernetickej bezpečnosti voči celkovému vzdelávaciemu programu ÚPVII,
   - identifikácie oblastí kybernetickej bezpečnosti, ktoré bude musieť program adresovať,
   - detailného rozpracovania jednotlivých oblastí kybernetickej bezpečnosti, ktoré bude program adresovať,
   - zadefinovanie technického spôsobu implementácie programu,
   - stanovenia merateľných ukazovateľov programu,
   - zadefinovania spôsobu vyhodnocovania merateľných ukazovateľov programu,
   - zadefinovania spôsobu celkového vyhodnocovania programu.
c) Návrh obsahu špecializovaných školení kybernetickej bezpečnosti pre jednotlivé cieľové skupiny používateľov v závislosti od ich pracovného zaradenia a odborného zamerania pozostávajúci z/zo:
   - rámcového zmapovania existujúcich špecializovaných školení pre kybernetickú bezpečnosť v prostredí ÚPVII,
   - identifikácie adresovaných cieľových skupín používateľov,
   - návrhu špecializovaných školení a ich namapovanie na jednotlivé cieľové skupiny,
   - identifikácie kompetencií, ktorých dosiahnutie sa očakáva od jednotlivých cieľových skupín po absolvovaní špecializovaných školení,
   - detailného rozpracovania jednotlivých typov špecializovaných školení,
   - kvantifikácie časovej náročnosti jednotlivých špecializovaných školení z pohľadu účastníka školenia,
   - stanovenia merateľných ukazovateľov pre jednotlivé špecializované školenia,
   - zadefinovania spôsobu vyhodnocovania merateľných ukazovateľov jednotlivých špecializovaných školení,
   - vytvorenia akčného plánu zavedenia špecializovaných školení v prostredí ÚPVII,
   - zadefinovania spôsobu vyhodnocovania efektívnosti špecializovaných školení,
   - pilotná realizácia každého z navrhnutých typov špecializovaných školení (zoznam účastníkov zabezpečí ÚPVII).

Sumár výstupov:

a) Návrh programu kontinuálneho vzdelávania v oblasti kybernetickej bezpečnosti:
   - program kontinuálneho vzdelávania, ktorý bude obsahovať:
     - zoznam cieľových skupín používateľov,

- vzdelávacie profily pre jednotlivé cieľové skupiny používateľov pokrývajúce:
  - vzdelávacie aktivity a ich namapovanie na jednotlivé cieľové skupiny,
  - kvalifikačné stupne pre jednotlivé cieľové skupiny,
  - kompetencie, ktorých dosiahnutie sa očakáva od jednotlivých cieľových skupín,
  - detailné rozpracovanie jednotlivých vzdelávacích aktivít,
  - časovú náročnosť vzdelávacích aktivít pre jednotlivé cieľové skupiny,
  - merateľné ukazovatele pre jednotlivé vzdelávacie aktivity,
  - spôsob vyhodnocovania merateľných ukazovateľov jednotlivých vzdelávacích aktivít,
- spôsob celkového vyhodnocovania programu,

- akčný plán zavedenia programu kontinuálneho vzdelávania v prostredí ÚPVII.

b) Návrh programu zvyšovania povedomia o kybernetickej bezpečnosti:

- program zvyšovania povedomia, ktorého obsahom bude:
  - definovanie oblastí kybernetickej bezpečnosti, ktoré bude program adresovať,
  - detailné rozpracovanie jednotlivých oblastí kybernetickej bezpečnosti, ktoré bude program adresovať,
  - technický spôsob realizácie programu,
  - merateľné ukazovatele programu,
  - spôsob vyhodnocovania merateľných ukazovateľov programu,
  - spôsob celkového vyhodnocovania programu.
- akčný plán zavedenia programu zvyšovania povedomia v prostredí ÚPVII.

c) Návrh obsahu špecializovaných školení kybernetickej bezpečnosti pre jednotlivé cieľové skupiny používateľov v závislosti od ich pracovného zaradenia a odborného zamerania:

- súbor školiacich materiálov pripravených špeciálne pre jednotlivé cieľové skupiny používateľov, ktoré budú pokrývať najmenej:
  - terminológiu,
  - základné povedomie pre oblasť kybernetickej bezpečnosti,
  - schopnosť používania stanovených bezpečnostných mechanizmov,
  - znalosť a uplatnenie interných procesov (smerníc) týkajúcich sa kybernetickej bezpečnosti v rôznych situáciách,
  - schopnosť správne analyzovať a zhodnotiť situáciu ohrozujúcu kybernetickú bezpečnosť,
  - znalosť právnych predpisov a medzinárodných noriem a štandardov súvisiacich s informačnou a kybernetickou bezpečnosťou,
  - znalosť bezpečnostných zásad, postupov a techník kybernetickej bezpečnosti,
  - znalosť zásad fyzickej a objektovej bezpečnosti,

    - znalosť zásad personálnej bezpečnosti,
    - znalosť princípov testovania s dôrazom na kybernetickú bezpečnosť,
    - znalosť zásad auditu informačnej a kybernetickej bezpečnosti,
    - znalosť metodík a procesov riadenia rizika a postupov analýzy rizík informačnej bezpečnosti,
    - znalosť typických kybernetických hrozieb, postupov pre identifikáciu hrozieb a identifikácia zraniteľností,
    - schopnosť analýzy a hodnotenia bezpečnostných opatrení,
    - znalosť metodík podnikovej architektúry,
    - znalosť procesov incident handlingu,
    - znalosť princípov Disaster Recovery (DR) a Business Continuity (BC),
    - znalosť princípov logovania a bezpečnostného monitorovania,
    - znalosť konceptov počítačových sietí, zásad architektúry sietí a základných bezpečnostných princípov,
    - znalosť riadenia IT služieb,
- akčný plán zavedenia špecializovaných školení v prostredí ÚPVII,
- pilotná realizácia každého z navrhnutých typov špecializovaných školení.

Uvedené poskytnutie poradenských služieb na zistenie stavu kapacít (zdrojov, schopností a spôsobilostí) v oblasti informačnej a kybernetickej bezpečnosti v podsektore ISVS vo forme štúdie realizovateľnosti, vychádza z nasledujúcich faktorov:

Kybernetická bezpečnosť je dynamicky sa vyvíjajúcim odvetvím, ktoré musí neustále reagovať na nové výzvy. Z tohto dôvodu je nutné zaviesť procesy pre zvládnutie situácie prelomenia bezpečnosti tak, aby bola do čo možno najvyššej možnej miery zabezpečená biznis kontinuita informačných systémov a aby bol minimalizovaný dopad kybernetických bezpečnostných incidentov.

Základným strategickým cieľom „Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020“ (ďalej aj „Koncepcia kybernetickej bezpečnosti“) schválenej vládou SR, je „otvorený, bezpečný a chránený národný kybernetický priestor, t. j. vybudovanie dôvery v spoľahlivosť a bezpečnosť najmä kritickej informačnej a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku“.

Pre zaistenie včasnej a efektívnej reakcie na kybernetické útoky vo verejnej správe je potrebné, aby ÚPVII- vrátane delimitovanej vládnej jednotky CSIRT a Národnej agentúry pre sieťové a elektronické služby - disponoval adekvátne odborne pripravenými špecialistami, riadiacimi kádrami a výkonnými zamestnancami, ktorí budú schopní správne, rýchlo a odborne reagovať v momente kybernetického ohrozenia a útoku.

Na účely zabezpečenia kybernetickej bezpečnosti a účinného reagovania na kybernetické bezpečnostné incidenty je nevyhnutné zabezpečiť neustále vzdelávanie a zvyšovanie

povedomia nielen bežných používateľov, ale rovnako tak i rôznych skupín odborníkov medzi ktorých patria bezpečnostní manažéri, bezpečnostní architekti, administrátori bezpečnostných systémov, špecialisti manažmentu IT rizík, audítori bezpečnosti informačných systémov, bezpečnostní analytici, kryptológovia či vyšetrovatelia bezpečnostných incidentov. To všetko sú špecialisti, ktorí sa v každodennej praxi zaoberajú otázkami ochrany informačných aktív, manažmentu IT rizík, forenznou informatikou, testovaním bezpečnostných systémov, auditom bezpečnosti, architektonickým návrhom informačných systémov z pohľadu informačnej a kybernetickej bezpečnosti a implementáciou bezpečnostnej infraštruktúry.

Potreba riešenia programov odbornej prípravy v oblasti bezpečnosti sietí a informačných systémov je aj predmetom zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, ktorým sa implementuje smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

Koncepcia kybernetickej bezpečnosti v kapitole 3 predstavuje základné prostriedky realizácie cieľov stanovených koncepciou, medzi ktoré patrí aj systematická osveta a komplexný systém vzdelávania v oblasti kybernetickej bezpečnosti. Koncepcia kybernetickej bezpečnosti taktiež navrhuje sedem kľúčových opatrení, z ktorých obzvlášť významným je opatrenie 4: „Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti“. Uvedené opatrenie detailne rozpracúva „Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020“ (ďalej aj „Akčný plán“).

Obsahom tejto zákazky je poskytnutie poradenských služieb, prostredníctvom ktorých ÚPVII v rámci svojej pôsobnosti prispeje k plneniu úloh zadefinovaných Koncepciou kybernetickej bezpečnosti a Akčným plánom.

Poskytnuté poradenské služby budú jednou z hlavných aktivít národného projektu „Vybudovanie centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti“ a vedľajšou aktivitou národného projektu „Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe“.