## Poročilo o izvedbi aktivnosti Akcijskega načrta izvedbe Strategije kriptografske zaščite podatkov v Republiki Sloveniji za leti 2020 in 2021

| **Zap. št.** | **Ukrep / Aktivnost** | **Nosilec** | **Sodelujoči** | **Pričakovani rezultat** | **Realizacija aktivnosti** | **Opombe** |
| --- | --- | --- | --- | --- | --- | --- |
| **CILJ 1: Vrednotenje kriptografskih rešitev** | | | | | | |
| 1.1 | Delovanje kriptološkega laboratorija za vrednotenje kriptografskih rešitev (prvo vrednotenje) | UVTP |  | Delujoč laboratorij | Aktivnost je v celoti opravljena. |  |
| **CILJ 2: Spodbujanje razvoja in uporabe kriptografskih rešitev** | | | | | | |
| 2.1 | Oblikovanje potreb in smernic razvoja kriptografskih rešitev, vključitev v Security Standards Partnership | UVTP | SOVA, MO, MNZ-Policija | Sprejete smernice | Aktivnost je delno opravljena. | Sodelujoči so se seznanili z možnostjo sodelovanja v CIS3 partnerstvu, prejeli smo podporo (MO). |
| Polnopravno članstvo v CIS3 partnerstvu | Aktivnost je delno opravljena. | Izvajanje aktivnosti se prenese v akcijski načrt za leto 2023. Pridobivanje statusa polnega članstva Republike Slovenije v CIS3 partnerstvu je v teku. |
| 2.2 | Posredovanje informacij domačim proizvajalcem kriptografskih rešitev o možnosti pridobitve potrdil za varovanje tajnih podatkov EU in NATO | UVTP | MGRT | Domači proizvajalci so informirani o možnosti pridobitve potrdil | Aktivnost je v celoti opravljena |  |
| 2.3 | Oblikovanje in sprejem politike sodelovanja z raziskovalnimi institucijami | UVTP | Raziskovalne institucije | Sprejeta politika sodelovanja UVTP z raziskovalnimi institucijami | Aktivnost je delno opravljena. | Zaznana je potreba po širšem sodelovanju strokovne javnosti in prenos znanja med državnimi organi, raziskovalnimi institucijami ter organizacijami. Aktivnost se ustrezno razširi, njeno izvajanje je predvideno tudi za leto 2023. |
| 2.4 | Sklenitev sporazuma o sodelovanju med UVTP in raziskovalnimi institucijami. | UVTP | Raziskovalne institucije | Sprejeti sporazumi sodelovanja UVTP z raziskovalnimi institucijami | Aktivnost ni opravljena. | Zaznana je potreba po širšem sodelovanju strokovne javnosti in prenos znanja med državnimi organi, raziskovalnimi institucijami ter organizacijami. Aktivnost se ustrezno razširi, njeno izvajanje je predvideno za leto 2023. |
| **CILJ 3: Upravljanje kriptografskih rešitev[[1]](#footnote-1)** | | | | | | |
| 3.1 | Izvajanje aktivnosti šifrirnega vrednotenja kriptografskih rešitev v okviru pristojnosti za kriptografsko zaščito podatkov (prvo vrednotenje) | UVTP | MO, SOVA | Izvajanje šifrirnih vrednotenj kriptografskih rešitev | Izvedeno je bilo šest postopkov ugotavljanja varnostne ustreznosti kriptografskih rešitev. | Aktivnost se je izvajala tudi v letu 2022, njeno izvajanje je predvideno tudi za leto 2023. |
| 3.2 | Koordiniranje aktivnosti pri drugem šifrirnem vrednotenju za pridobitev potrdila za varovanje tajnih podatkov EU in NATO | UVTP |  | Opravljanje drugega šifrirnega ovrednotenja | Aktivnost je v izvajanju. | Aktivnost se je izvajala tudi v letu 2022, njeno izvajanje je predvideno tudi za leto 2023. |
| 3.3 | Zasnova, produkcija, distribucija, ukinjanje/uničenje kriptografskih rešitev | UVTP, MO |  | Ustrezne kriptografske rešitve v operativni uporabi | Aktivnost je delno izvedena. | Aktivnost se je izvajala tudi v letu 2022, njeno izvajanje je predvideno tudi za leto 2023. |
| 3.4 | Strokovni nadzor upravljanja in izvajanje evidentiranja kriptografskega materiala v celotnem življenjskem ciklu | UVTP | Uporabniki kriptografskega materiala | Izveden strokovni nadzor kriptografskega materiala | Aktivnost ni bila izvedena. | Aktivnost ni predvidena v akcijskem načrtu za leto 2023. |
| 3.5 | Generiranje kriptografskih ključev za potrjene kriptografske rešitve | UVTP | Uporabniki kriptografskega materiala | Delujoči sistemi | Aktivnost je bila v celoti opravljena. | Aktivnost se je izvajala tudi v letu 2022, njeno izvajanje je predvideno tudi za leto 2023. |
| **CILJ 4: Raziskovanje na področju kriptologije** | | | | | | |
| 4.1 | Financiranje raziskovalnega projekta za področje kriptografije | UVTP in ARRS | Državni organi, raziskovalne organizacije | Aplikativna uporabnost rezultatov raziskav pri razvoju končnih produktov | Aktivnost je bila v celoti izvedena. | Aktivnost se je izvajala tudi v letu 2022, njeno izvajanje je predvideno tudi za leto 2023. |
| **CILJ 5: Usposabljanje uporabnikov kriptografskih rešitev, ozaveščanje in razvoj znanja** | | | | | | |
| 5.1 | Umestitev vsebin ozaveščanja o varnem komuniciranju in obravnavi podatkov za novo zaposlene v javni upravi v obstoječe programe usposabljanj | UVTP in MJU |  | Ozaveščeni uporabniki, višja stopnja varnostne kulture | Aktivnost ni bila izvedena. | Aktivnost ni predvidena v akcijskem načrtu za leto 2023. |
| 5.2 | Priprava predloga posodobitve izobraževalnih programov | UVTP | ZRSŠ, UVTP, MNZ, MO, MJU, SOVA, MIZŠ, univerze | Novi, prenovljeni ali posodobljeni izobraževalni program | Aktivnost ni bila izvedena. | Aktivnost ni predvidena v akcijskem načrtu za leto 2023. |
| 5.3 | Usposabljanje skrbnikov kriptografskega materiala in strokovnih sodelavcev | UVTP |  | Visoka usposobljenost skrbnikov in drugih strokovnih sodelavcev pri ravnanju s kriptografskim materialom | Aktivnost ni bila izvedena. | Izvajanje aktivnosti so onemogočali ukrepi zoper COVID. Aktivnost se je izvedla v letu 2022, njeno izvajanje se prenese tudi v akcijski načrt za leto 2023. |
| 5.4 | Promocija kriptografije v RS, ozaveščanje uporabnikov kriptografskih rešitev in predstavitev uporabe | UVTP |  | Večja prepoznavnost pomena kriptografske zaščite podatkov | Aktivnost je bila deloma izvedena. | Izvajanje aktivnosti so onemogočali ukrepi zoper COVID. Aktivnost se je izvedla v letu 2022, njeno izvajanje se prenese tudi v akcijski načrt za leto 2023. |
| 5.5 | Izobraževanje strokovnih delavcev, udeležba na strokovnih konferencah, izobraževanje za namene drugega vrednotenja v skupini AQUA | UVTP |  | Učinkovita zaščita sistemov, ki obravnavajo tajne podatke. | Aktivnost je bila deloma izvedena. | Izvajanje aktivnosti so onemogočali ukrepi zoper COVID. Aktivnost se je izvedla v letu 2022, njeno izvajanje se prenese tudi v akcijski načrt za leto 2023. |
| 5.6 | Organizacija tekmovanj na področju kriptografije | MIZŠ | ZRSŠ, UVTP, MO, MNZ, SOVA, MJU | Organizirano tekmovanje na državni ali mednarodni ravni | Aktivnost je bila v celoti izvedena. | Aktivnost se je nadaljevala tudi v letu 2022, prav tako je izvajanje predvideno v letu 2023. |

1. Pri ukrepih/aktivnostih 3.3, 3.4 in 3.5 se upošteva Navodilo o obravnavanju kriptografskega materiala (dok. št. 0220-2/2016/44 z dne 1. 8. 2016, INTERNO). [↑](#footnote-ref-1)