EURÓPSKA ÚNIA
Európsky fond regionálneho rozvoja
OP Integrovaná infraštruktúra 2014 – 2020

MINISTERSTVO DOPRAVY SLOVENSKEJ REPUBLIKY

Názov prijímateľa: **Fakultná nemocnica s poliklinikou J. A. Reimana Prešov**
Názov projektu: **Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v nemocnici Prešov**
Miesto realizácie projektu: **Prešovský samosprávny kraj, FNsP J. A. Reimana Prešov**
Výška nenávratného finančného príspevku: **110 905,90 EUR**

Stručný opis projektu

Fakultná nemocnica J.A. Reimana Prešov (ďalej len „Nemocnica Prešov“) eviduje na svojej pôde zvýšenú frekvenciu útokov na údaje a dáta zbierané v rámci existujúcich informačných systémov. Nárast počtu hrozieb, zraniteľnosť a dopady jednotlivých bezpečnostných incidentov v oblasti zdravotníctva ohrozujú zdravie klientov našej nemocnice. Legislatíva SR definuje a nastavuje požiadavky, ako aj štandardy z pohľadu bezpečnostných opatrení a nemocnica Prešov musí plniť tieto požiadavky v oblasti informačnej a kybernetickej bezpečnosti (ďalej len „IB a KyB“) v stanovenom rozsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostnej dokumentácie.

Cieľom projektu prostredníctvom realizácie jednotlivých aktivít je:

1. zabezpečiť kompletnú dokumentáciu v oblasti kybernetickej bezpečnosti
2. vypracovanie dokumentov bezpečnostnej politiky
3. zriadenie riadiaceho výboru bezpečnosti organizácie a interných riadiacich aktov a ďalších dokumentov pre potreby zabezpečenia súladu jednotlivých OVM s požiadavkami IT bezpečnosti vzhľadom na požiadavky legislatívy
4. zavedenie SW nástroja pre procesné a organizačné riadenie Informačnej a kybernetickej bezpečnosti.

Realizácia:

1. Vykonať dôkladnú analýzu rizík a analýzu dopadov (AR/BIA) vrátane:
    - identifikácie aktív a ohodnotenia ich kritickosti,
    - klasifikácie aktív a kategorizácie IS a sietí,
    - identifikácie hrozieb a vektorov útokov,
    - analýzy potenciálnych dopadov,
    - identifikácie rizík na základe pravdepodobností výskytu hrozieb a možných dopadov,
    - identifikácie existujúcich opatrení a reziduálnych rizík,
    - návrhu opatrení.
2. Spracovanie stratégie informačnej a kybernetickej bezpečnosti vrátane roadmapy na implementáciu navrhnutých opatrení.
3. Zabezpečenie rozhodnutia o riadení rizík (o ich akceptácii alebo prijatí adekvátnych opatrení na ich zníženie alebo úplnú elimináciu) vedením nemocnice.
4. Vytvorenie požadovaných interných dokumentov a smerníc pre relevantné oblasti riadenia IB a KyB.
5. Zavedenie SW nástroj pre procesno-organizačné riadenie Informačnej a kybernetickej bezpečnosti.