Okvirna strategija razvoja horizontale SRIP IKT-KV (Kibernetska varnost)

Napovedati prihodnje varnostno okolje je zelo tvegano, saj so spremembe stalne in zahtevajo stalno prilagajanje. Vse več vrednosti je povezanih s Z rastjo stopnje digitalizacije rastejo tudi tveganja s katerim se soočamo posamezniki, podjetja in skupnosti, ki zahtevajo vedno nove in bolj kompleksne ukrepe za zagotavljanje varnosti kritičnih storitev. Le s celovitimi ukrepi je mogoče zaščititi vrednosti, ki jih podjetja imajo v podatkih, znanju in infrastrukturi, ki podatke zagotavlja in omogoča njihovo učinkovito uporabo. Okvirna strategija razvoja SRIP IKT-KV združuje inovativne projekte na specifičnih segmentih, ki bodo spodbudili razvoj varnostnih zmogljivosti in prispevali k razvoju digitalizacije skupnosti.

Trenutno stanje varnosti na področju pametnih mest, e-in m-zdravja, prometa, interneta stvari je zaskrbljujoče. Z razvojem interneta stvari (IoT), ki je gonilo razvoja pametnih rešitev (mesta, omrežja, tovarne), se povečujejo tudi varnostna tveganja. Težava je v tem, da se je v fazi razvoja strojne in programske opreme premalo pozornosti namenilo varnosti. To pa ne velja le na področju IoT: bolj kot bo družba digitalizirana, večja bo prostor za napade, večja bodo tveganja in obseg posledic napadov.

Standardi in dobre prakse naslavljajo pomen ustreznega pristopa pri zagotavljanju kibernetske varnosti v vseh fazah življenjskega cikla informacijskih rešitev in pomagajo pri zniževanju varnostnih tveganj. Na področju novih tehnologij, kot je IoT, pa teh okvirov in dobrih praks še ni.

Horizontala bo strateško usmerjena v pridobivanje, ustvarjanje, izmenjavo in uporabo znanja in informacij na področju kibernetske varnosti. Zato bo usmerjena v aktivnosti:

1) Za uspešno zagotavljanje varnosti moramo zmanjšati število uspešnih napadov in njihove posledice. Zato je potrebno izdelati in uporabljati ustrezen okvir pri razvoju in implementaciji IoT rešitev, kakor tudi z uvedbo skupnega Varnostno operativnega centra (VOC).

2) Zagotavljanje ustreznega nivoja kompetenc je kritičnega pomena za uspešno bojevanje proti kibernetskim napadom. Znanje in informacije o zaznanih napadih in poskusih napadov je nujno deliti med seboj, v omenjeno okolje pa je nujno vključiti organizacije, ki zagotavljajo tehnična znanja in ustrezno infrastrukturo.

Omenjeno strategijo bodo upoštevali vsi ponudniki vertikalnih storitev, tako Pametnih mest in skupnosti, pametnih zgradb in domov z lesno verigo, Mrež za prehod v krožno gospodarstvo, trajnostne pridelave hrane, trajnostnega turizma, kakor tudi Tovarn prihodnosti, ter izvajalci storitev na področjih zdravja, mobilnosti in razvoja materialov.

S pojavom IoT kot novega in enega glavnih elementov dodane vrednosti pri razvoju pametnih rešitev je področje varovanja informacij dobilo nove razsežnosti in kritičnost zagotavljanja ustreznega nivoja tveganja je nuja! Potrebno je holistično upravljanje varovanja informacij, kajti v sodobni družbi so informacije nosilci dodane vrednosti.

To so večinoma razlogi, da se bodo morale organizacije na področju zagotavljanja kibernetske varnosti povezovati in skupno delovati.

Skupina organizacij s področij gospodarstva, izobraževanja in javne uprave, zbranih v SeKV pri ZIT na GZS lahko razvija poslovni model Varnost kot storitev. S svojimi strokovnjaki z ustreznimi izkušnjami, kompetencami in povezavami lahko uspešno upravlja različne varnostne funkcije, kakor tudi aktivno posreduje pri zagotavljanju razvoja znanja kibernetske varnosti.

V skupnosti, kot je Slovenija, lahko z medsebojnim sodelovanjem dosežemo ustrezne sinergijske učinke, saj so po pravilu posamezne organizacije, ki nastopajo na trgu, premajhne za samostojno upravljanje kibernetske varnosti, ravno to pa je tudi lahko konkurenčna prednost, saj se lahko z združevanjem ustrezno optimizirajo stroški razvoja varnostnih rešitev na področju pametnih storitev, kakor tudi ustrezen odziv na zaznane varnostne incidente.

Z vzpostavitvijo ustreznih ciljev in kazalnikov uspešnosti, kot so na primer število zaznanih poskusov vdorov, uspešnost delitve informacij za preprečevanje nadaljnjih vdorov, stroškovna uspešnost odprave posledice uspešnih vdorov ipd. lahko ustrezno dokažemo, da je omenjeno sodelovanje in združevanja konkurenčna prednost pred oblikami, ki medsebojno manj sodelujejo in so zaradi tega manj izkoriščene.

Z dokazano uspešnim modelom lahko nastopimo tudi na tujih tržiščih, kjer zaradi manjše fleksibilnosti ustrezno primerljivi projekti ne morejo tako hitro zaživeti. Hkrati dokažemo, da zaradi ustrezne izkoriščenosti kompetentnih kadrov dosežemo dvig dodane vrednosti na zaposlenega, visoko ekspertno znanje in tehnologije pa lahko tako plasiramo tudi na zunanji trg.

Okvirni načrt aktivnosti razvoja SRIP horizontale IKT-KV (Kibernetska varnost)

Operativni in kompetenčni center kibernetske varnosti

Namen horizontale je zagotoviti preventivno delovanje, nadzor nad notranjimi in zunanjimi varnostnimi informacijami ter dogodki, učinkovito izmenjavo znanja in informacij z okoljem za celovito obvladovanje kibernetskih tveganj MSO doma in v regiji:

Razvoj in operiranje platforme, ki bo z razvojem svojih storitev omogočala:

- Izboljšanje preventive in nadzora kibernetske varnosti,
- Uveljavljanje standardov in metod analize kibernetskih tveganj ter načrtovanja varnostnih ukrepov,
- Obvladovanje informacij o varnostnih grožnjah,
- Obvladovanje incidentov in odprava posledic,
- Zagotavljanje dostopa do informacij in storitev za MSP in javne organizacije v regiji,
- Izboljševanje zavedanja o kibernetski varnosti in možnost izmenjave informacij,
- Izvajanje specializiranih storitev (forenzika, vdorna testiranja, analize ranljivosti,…)
- Upravljanje varnosti v pametnih omrežjih
- Aktivno povečevanje kompetenc na področju kibernetske varnosti v sodelovanju z izobraževalno sfero

Izgradnja modela za izračun stroškov in koristi v kibernetski varnosti

Rezultat bo okvir (model) za izračun kibernetskih tveganj v realnem času. Okvir upošteva prihajajoče grožnje in incidente (v realnem času) z namenom izračuna trenutnega ostanka tveganj v organizaciji in podporo izračunom premij pri zavarovanjih kibernetskih tveganj. Projekt aktivno podpira cilje omrežne in informacijske varnosti z:

- Raziskovanjem sposobnosti in razširljivosti obstoječih okvirjev za analiziranje tveganj,
- Izvedbo socialno ekonomskih aktivnosti obvladovanje tveganj (analize stroškov in koristi implementacije rešitev za obvladovanje tveganj, izmenjavo znanja o informacijski varnosti in razvoja metod za določanje vpliva na poslovanje),
- Razvojem metod za izračun zavarovalniških premij,
- Vzpostavitvijo platforme za podporo premijskih izračunov,
- Vrednotenjem sposobnosti in razširljivosti razvitega okvirja obvladovanja tveganj ter njegove sposobnosti izračunavanja premij za zavarovanje kibernetskih tveganj.