Foto: SeKV

Razpravljali smo o vprašanjih razvoja kadra, sodelovanja javnega in zasebnega sektorja in pravnih vidikov kibernetskih varnostnih pregledov ter podali številne predloge, kako izboljšati pogoje delovanja podjetij, ki delajo v sektorju kibernetske varnosti.

Kibernetska varnost

Teden kibernetske varnosti

Razprave v okviru Tedna kibernetske varnosti, ki je letos v hibridni obliki potekal od 4. do 8. oktobra, so potrdile nujnost ukrepanja in nadaljnjega razvoja kibernetske odpornosti za zmanjševanje kibernetskih tveganj.

Halis Tabakovič, ZIT, GZS

Odgovornost razvijalcev programske opreme zahteva, da v celotnem življenjskem ciklu produktov vgrajujejo elemente varnosti.

Sekcija za kibernetsko varnost (SeKV) pri GZS – Združenju za informatiko in telekomunikacije (ZIT) je dogodek organizirala v obdobju, ko Slovenija predseduje Svetu EU, poudarek pa je bil na ozaveščanju o nujnosti povečanja kibernetske varnosti znotraj podjetij in implementaciji ukrepov za povečanje odpornosti podjetij.

Predavatelji so predstavili stanje kibernetske varnosti v Sloveniji in številne izzive in rešitve slovenskih podjetij, namenjene krepitvi kibernetske odpornosti podjetij. Na okroglih mizah so sogovorniki razpravljali o vprašanjih razvoja kadra, sodelovanja javnega in zasebnega sektorja in pravnih vidikov kibernetskih varnostnih pregledov ter podali številne predloge, kako izboljšati pogoje delovanja podjetij, ki delajo v sektorju kibernetske varnosti. Vsi so izpostavili nujnost razvoja kadrov in intenziviranja sodelovanja vseh deležnikov na področju kibernetske varnosti.

Poleg predavanj in okroglih miz je Digitalno inovacijsko stičišče Slovenije (DIH Slovenija) organiziralo razstavo in festival rešitev, kjer so svoje zgodbe o uspehu na področju kibernetske varnosti predstavila slovenska podjetja.

Kaj vse smo slišali?

Teden kibernetske varnosti je potekal v hibridni obliki: v živo v Ljubljani v Digitalnem središču Slovenije v BTC in preko spleta. Začel se je z dogodkom »Prihodnost kibernetske varnosti v Sloveniji in Evropi«, ki ga je organizirala Fakulteta za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Predstavili so stanje kibernetske varnosti v Sloveniji, odmevne evropske razvojno-raziskovalne projekte in najbolj vplivne pilotske projekte v EU, kot so Concordia, Sparta, CyberSec4Europe in Echo. Sledila je okrogla miza »Vzpostavitev mreže kompetenčnih centrov za kibernetsko varnost v EU«, na kateri so sodelujoči izpostavili izzive upravljanja kompetenčnega centra za kibernetsko varnost v povezavi z nacionalnimi

Foto: SeKV

Foto: SeKV

Predavatelji so prikazali številne primere ogrožanja ter možnosti preventivnega ukrepanja – od dnevnega nadzora groženj do delovanja operativnega centra kibernetske varnosti in odzivanja na incidente.

koordinacijskimi centri in napredek pri vzpostavitvi omenjenih ustanov.

Na okrogli mizi »Ozaveščanje o kibernetskih tveganjih in implementacija ukrepov kibernetske varnosti v podjetjih« smo razpravljali o pogojih dela in ovirah ter potrebnih ukrepih države za nadaljnji razvoj podjetij v sektorju kibernetske varnosti, ki so pomemben del zagotavljanja kibernetske varnosti v državi. Na okrogli mizi o kadrovski problematiki pa smo slišali, da na področju kibernetske varnosti podjetja zaznavajo pomanjkanje kadrov z ustreznimi poglobljenimi specialističnimi znanji in kakšni so predlogi ter trenutni projekti za izboljšanje stanja v prihodnje.

Predavatelji so prikazali številne primere ogrožanja ter možnosti preventivnega ukrepanja – od dnevnega nadzora groženj do delovanja operativnega centra kibernetske varnosti in odzivanja na incidente –, da bi s tem vplivali na zavedanje udeležencev in širše javnosti o tveganjih v kibernetskem prostoru.

Vavčer za sistemski varnostni pregled

Posvetili smo se tudi varnostnim pregledom in penetracijskim testiranjem. Digitalno inovacijsko stičišče Slovenije (DIH Slovenija) je predstavilo vavčer za kibernetsko varnost, s katerim podjetjem sofinancirajo sistemski varnostni pregled in penetracijsko testiranje. Na okrogli mizi o pravnih vidikih izvajanja penetracijskih testov pa so udeleženci poudarili pomen jasnosti dogovora med naročnikom in izvajalcem, zagotavljanjem dopolnilnih znanj kadra, ki presegajo tehnološka znanja in upoštevanja meril v zvezi z obravnavo osebnih podatkov. Organom države so priporočili ponovno obravnavo predloga o odgovornem varnostnem razkrivanju.

Teden kibernetske varnosti je pozornost namenil tudi šifriranju, kriptografiji, anomalijam v omrežjih, standardom, avtomatizaciji kibernetske varnosti, uporabi umetne inteligence … Dogodek smo zaključili s predstavitvijo najboljših praks na Konferenci sekcije za kibernetsko varnost. Odgovornost razvijalcev programske opreme zahteva, da v celotnem življenjskem ciklu produktov vgrajujejo elemente varnosti, zagotavljajo zadostna preverjanja in certificiranja svojih produktov ter omogočajo transparenten vpogled v produkte. Pri spopadu s tveganji je ključnega pomena identifikacija groženj, kjer so bistveni vrhunsko znanje in uporaba modernih tehnologij, kot je umetna inteligenca. Proaktivni pristopi odkrivanja in preprečevanja napadov so tiste prakse, ki lahko skupaj z visoko ravnjo organiziranosti za ukrepanje v primerih incidentov bistveno zmanjšajo posledice kibernetskih napadov. Slovenska podjetja in razvojne organizacije so predstavili tudi nekaj lastnih tehnoloških rešitev, s katerimi je mogoče poglabljati znanja o ranljivostih in tehnikah napada na nove izdelke, ki se stalno pojavljajo na trgu, in so ključna za odkrivanje in spopadanje z nepoznanimi ranljivostmi, ki pa se že izkoriščajo. Brez celovitega pristopa ne bo mogoče zagotavljati ustrezne ravni odpornosti.

Vzporedno je potekal mednarodni poslovni forum »Austria – European Pioneer in Cyber Security«, kjer je Sekcija za kibernetsko varnost v sodelovanju z Advantage Austria in SPIRIT Slovenija povezala mnoga podjetja iz Avstrije in Slovenije. Sledilo je še tekmovanje »Cyber Night – Capture the flag«, na katerem so se mladi talenti soočili z reševanjem različnih varnostnih izzivov.

Teden kibernetske varnosti je bil eden najbolj obsežnih dogodkov na temo kibernetske varnosti, ki smo jih organizirali v Sloveniji – obsegal je 4 okrogle mize, 27 predavanj, mednarodni dogodek in tekmovanje v znanju in spretnostih specialistov. Širok spekter dogodkov je pokril vse aktualne izzive kibernetske varnosti. Predavanja in posnetki so na voljo na straneh SeKV in DIH Slovenija. gg

Digitalno inovacijsko stičišče Slovenije (DIH Slovenija) je predstavilo vavčer za kibernetsko varnost, s katerim podjetjem sofinancirajo sistemski varnostni pregled in penetracijsko testiranje.

Foto: SeKV

Slovenska podjetja in razvojne organizacije so predstavili tudi nekaj lastnih tehnoloških rešitev, s katerimi je mogoče poglabljati znanja o ranljivostih in tehnikah napada na nove izdelke, ki se stalno pojavljajo na trgu.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.