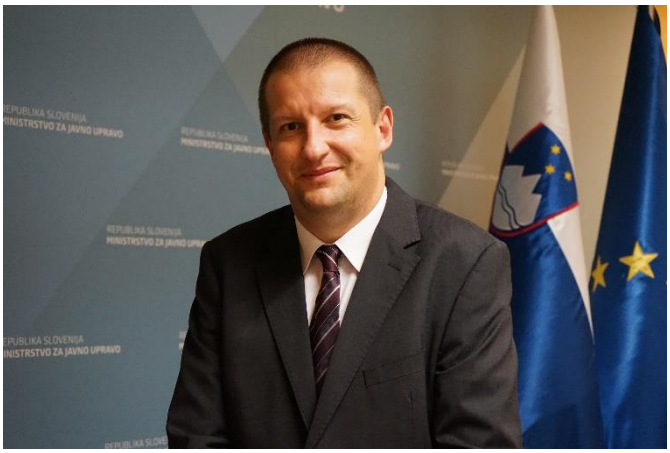
ZBORNIK

Kaj podjetjem prinaša NIS 2 direktiva in kako se na njo pripraviti?

10. 10. 2023 - Zoom spletni seminar

PRVI PREDAVATELJ: dr. Uroš Svete, direktor, Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)

Direktor Urada Vlade RS za informacijsko varnost dr. Uroš Svete je strokovnjak s področja obrambe, varnostnih študij, analize konfliktov in informacijske/kibernetske varnosti. Ima bogate izkušnje s predavateljskim in raziskovalnim delom v okviru svoje akademske kariere na Fakulteti za družbene vede Univerze v Ljubljani. Bil je eden prvih slovenskih akademikov, ki se je ukvarjal z varnostnimi in geostrateškimi razsežnostmi uporabe informacijsko-komunikacijskih tehnologij. Kot izredni profesor se je večinoma posvečal temam vojaške tehnologije in varnostnim posledicam informacijsko-komunikacijskih tehnologij. Od januarja 2011 do decembra 2015 je vodil Katedro za obramboslovje.



Konec leta 2018 je postal generalni direktor Direktorata za informacijsko družbo na Ministrstvu za javno upravo, kjer je uspešno vodil proces vzpostavitve Uprave za informacijsko varnost kot nacionalnega pristojnega organa za kibernetsko varnost, ki je delovala kot organ v sestavi Ministrstva za javno upravo. Po spremembi zakonodaje julija 2021 je bil ustanovljen Urad Vlade RS za informacijsko varnost kot nacionalni pristojni organ za kibernetsko varnost pod vodstvom kabineta predsednika vlade, za direktorja pa je bil imenovan dr. Uroš Svete.

PRVO PREDAVANJE: Kaj podjetjem prinaša NIS 2 direktiva in kako se na njo pripraviti?

Predavanje se bo nanašalo na spremembe, ki jih prinaša direktiva NIS 2. Predavatelj bo osvetlil predvsem ločevanje med zavezanci (bistveni, pomembni), razlike med njimi in predstavil kriterije za njihovo določanje. Zavezanci se bodo morali skladno z novo direktivo samo prepoznati. V ta namen bodo pripravljeni postopki za izvedbo tega. Predstavljeni bodo tudi ukrepi za izvajanje in razlike med izvedbo inšpekcijskega nadzora danes in v prihodnje.

DRUGA DVA PREDAVATELJA: Uroš Majcen, direktor kibernetske odpornosti, in Andrej Skamen, tehnični svetovalec za informacijsko varnost, Kontron d.o.o.

Uroš Majcen že več kot 25 let deluje na slovenskem in širšem prostoru na področju informacijske in kibernetske varnosti. V podjetju Kontron d.o.o.- naslednik S&T Slovenija s svojo ekipo vodi tudi oddelek Security Operations. Trenutno je njegov osnovni fokus doseganje kibernetske odpornosti, tako za Kontron kot za stranke (slika na levi).

Andrej Skamen že več kot 25 let deluje na področju informacijske varnosti, na začetku kot inženir za požarne pregrade, kasneje se je njegova vloga razširila. V zadnjih letih so njegov fokus svetovanja na področju informacijske varnosti, kibernetska varnost in z njimi povezane storitve (brez slike).

DRUGO PREDAVANJE: Kateri so nujni in potrebni koraki za učinkovito naslavljanje NIS 2 direktive s fokusom na analizo tveganj

NIS 2 direktiva je bila sprejeta v EU parlamentu in kmalu bo tudi vpeljana v slovenski pravni red. Z tem bodo mnoge organizacije v Sloveniji pred izzivom kako nasloviti NIS 2 direktivo pri sebi . Predavanje bo pokazalo praktične korake, njihov redosled in izdelke/dokumente, ki jih organizacije potrebujejo za doseganje skladnosti z direktivo. Fokus predavanja bo na praktičnih primerih

TRETJI PREDAVATELJ: Klaus Smart Com d. o. o., Vodilni inženir za kibernetsko varnost, Smart Com d.o.o.

Klaus Samardžić je specialist za načrtovanje optičnih (WDM-OTN) in radijskih (Wi-Fi) transportnih sistemov za telekomunikacijske operaterje in elektroenergetiko. Izkušnje in znanje nadgrajuje s certifikati Juniper Networks, Extreme Wireless, Ciena in Infinera ter CWNA, kar mu omogoča vpogled v delovanje omrežja, kot ga ima uporabnik. Svojo ekspertizo s področja omrežij nadgrajuje s poznavanjem varnosti procesnih sistemih (OT) kritične infrastrukture in industrije, kar potrjuje s prejemom certifikata GRID (GIAC Response and Industrial Defense).

TRETJE PREDAVANJE: Kako zagotoviti neprekinjeno poslovanje in krizno upravljanje skladno z NIS 2

NIS 2 direktiva podjetjem prinaša odgovornost in priložnost. Odgovornost se nanaša na delovanje podjetja ter digitalne izdelke in storitve, ki jih izmenjuje z drugimi podjetji v proizvodni verigi. Digitalizacija industrije 4.0 zahteva vse večjo uporabo omreženih, spletno omogočenih in avtomatiziranih tehnologij. V sodobni digitalni industriji 4.0 bosta obstajala dva med seboj dopolnjujoča svetova. Večina proizvodnih procesov v fizičnem svetu bo imela 'dvojnike' v digitalnem

svetu. Razvoj, nadgradnja in delovanje bodo potekali v digitalnem svetu pred realizacijo v fizičnem svetu. Podjetja, ki sodelujejo, si bodo izmenjevala digitalne modele svojih procesov z vnesenimi spremembami ali nadgradnjami. Podjetja bodo z upoštevanjem NIS 2 imela možnost zagotoviti varnost poslovnih in proizvodnih procesov danes ter v digitalni industriji 4.0. Za neprekinjeno poslovanje in krizno upravljanje bo potrebno vpeljati programske in strojne rešitve za sledenje proizvodnim procesom ter varovanje pred omrežnimi vdori. Nujno je treba preprečiti spreminjanje ali odtujevanje podatkov ali uničenje opreme. Predavatelj bo predstavil zgled vizualizacije procesov ter poudaril pomen integracije spremljanja (monitoring) in opazovanja (observability) procesov skozi čas s pomočjo umetne inteligence. Podjetjem se z vpeljavo skladnosti z NIS 2 direktivo odpira priložnost za spremljanje in varovanje procesov znotraj podjetja in procesov s povezanimi podjetji v dobrobit celotnega ekosistema. Vsi subjekti v tem ekosistemu bodo imeli priložnost seznaniti se s potencialnimi varnostnimi vdori in opozoriti vse subjekte ter izpostavljena podjetja znotraj ekosistema.

ČETRTI PREDAVATELJ: dr. Andrej Rakar, Vodja informacijske varnosti, Petrol d.d.

Andrej Rakar, dr. elektrotehniških znanosti, je na Institutu Jožef Stefan deloval na področju nadzornih sistemov tehničnih procesov in uvajanju informacijskih tehnologij v proizvodnjo. Na področju informacijske varnosti deluje že od leta 2005, praktične izkušnje pa si je pridobil na najzahtevnejših projektih za finančne ustanove, zavarovalnice, telekomunikacijske operaterje, zdravstvo in podjetja iz gospodarstva doma in v tujini. Kot vodja informacijske varnosti (CISO) v podjetju Petrol d.d. je zadolžen za upravljanje z informacijsko varnostjo, uresničevanje strategije kibernetske varnosti ter nadzor izvajanja ukrepov varovanja informacij. Poleg tega predava na različnih konferencah in drugih prireditvah s tematiko informacijske varnosti.

ČETRTO PREDAVANJE: Obvladovanje tveganj zunanjih izvajalcev in ključnih dobaviteljev – primeri iz prakse

Dobavitelji IKT opreme in zunanji izvajalci lahko predstavljajo resno varnostno grožnjo za naš informacijski sistem. Podvrženi so namreč enakim varnostnim grožnjam, ker pa jim običajno bolj zaupamo, vzpostavljene varnostne kontrole niso enako učinkovite. Zato je nujno določiti minimalne varnostne zahteve, ki jih morajo le-ti izpolnjevati in jih tudi redno preverjati.

Obvladovanje teh tveganj narekuje tudi Zakon o informacijski varnosti (ZInfV), katerega namen je ureditev področja kibernetske varnosti in zagotovitev visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države.

Na predavanju bomo predstavili, kako se problematike lotevamo na Petrolu v praksi, od tehničnih, pravnih, do organizacijskih ukrepov za zmanjšanje tveganja zunanjih izvajalcev in dobaviteljev.

Pripravil: Tomaž Čebela, SeKV, ZIT
Ljubljana, 6. 10. 2023