**Zadeva: Prošnja za udeležbo na 4-dnevnem tečaju *Kibernetska varnost ICS/OT/IoT okolij***

Spoštovani vstavi ime odločevalca!

Specialistični tečaj bo potekal od DD/MM/LLLL do DD/MM/LLLL v Ljubljani. Ponuja ravno pravšnje razmerje med teoretičnim delom in praktičnimi vajami, pod vodstvom izkušenih varnostnih strokovnjakov in certificiranih etičnih hekerjev. Tečaj je novost na slovenskem trgu in je zasnovan tudi na podlagi domačih primerov iz prakse. Po vsebini je primerljiv z mednarodnimi certificiranimi izobraževanji s tega področja.

*Zato Vas vljudno prosim za odobritev udeležbe na tečaju, saj verjamem, da bom na ta način nadgradil svoja tehnična znanja* ***s poznavanjem kibernetske zaščite ICS/OT/IoT okolij****, kot tudi pridobil nova spoznanja o varnostnih rešitvah in najboljših praksah, ki jih bom lahko takoj uvedel v svoje vsakodnevno delo.*

Modernizacija ICS/OT/IoT okolij oz. operativnih procesnih okolij v industrijskih avtomatiziranih okoljih in kritični infrastrukturi je ključna komponenta digitalnega napredka podjetja, ki ga narekujejo zahteve trga in težnja v smeri večje stroškovne učinkovitosti in hitrejših dobavnih rokov.

Pospešena digitalizacija in avtomatizacija procesov zahteva varno izmenjavo informacij med poslovim (IT) in operativnim procesnim (OT) okoljem, kar vpliva na zmožnost **zaščite ICS/OT/IoT sistemov**. Tu se soočamo s celo vrsto ranljivosti, ki jih napadalec že jutri lahko izkoristi:

* uporaba naprav in sistemov starejšega izvora ('legacy'), kot je npr. operacijski sistem Windows XP, za katere varnostni popravki niso več na voljo,
* uporaba namenskih naprav in specifičnih protokolov (Profinet, S7, Modbus…), ki niso bili načrtovani z mislijo na varnost in zato ne vsebujejo varnostnih mehanizmov,
* podpora za nameščanje sodobne protivirusne zaščite ni mogoča.

**Kaj pridobim(o) s tečajem?**

Z udeležbo na tečaju bom prejel prepotrebno znanje in odgovore, kako **poskrbeti za ustrezno zaščito našega procesno operativnega okolja**, da bo odporno tako proti trenutnim kot nastajajočim kibernetskim grožnjam.

S poznavanjem pravilnega načrtovanja in varnega povezovanja poslovnega dela s procesno operativnim delom ter poznavanjem zaščite naprav, aplikacij in protokolov bomo poskrbeli za **zavarovanje kritičnih virov in nemoteno delovanje našega proizvodnega procesa** ter celotnega poslovanja podjetja.

S praktičnimi vajami v vlogi napadalca bom pridobil informacije o tem, kje so največkrat nezakrpane luknje v sistemu, ki jih hekerji radi izkoriščajo ter kako jih odpraviti.

**Predvidena investicija za okrepljeno kibernetsko varnost naše organizacije:**

* Udeležba na 4-dnevnem tečaju *Kibernetska varnost ICS/OT/IoT okolij*  
  (prenos znanja in veščin, gradivo, kosilo, osvežilni napitki): 1.500,00 EUR + DDV
* Potni stroški: dopolni EUR
* Skupni stroški za udeležbo: dopolni EUR

Menim, da je investicija v izobraževanje neprimerljiva z varnostnimi grožnjami in tveganjem nastale škode zaradi neobratovanja kritičnih sistemov in izgube ugleda oz. zaupanja strank v primeru uspešnega kibernetskega napada ali zlorab notranjih informacij v naši organizaciji.

Po tečaju bom osvojeno znanje v strnjeni predstavitvi delil z ostalimi v ekipi, saj so **ozaveščeni in usposobljeni sodelavci** najboljša obramba pred kibernetskimi napadalci.

S spoštovanjem,

vstavi ime udeleženca