Congrès International des Réseaux Electriques de Distribution

HO CIRED, Zelinska 4, 10000 Zagreb
Telefon: (+ 385 1) 617 15 27
www.ho-cired.hr
ho@cired.hr

POZIV NA SEMINAR

HRVATSKOG OGRANKA
MEĐUNARODNE ELEKTRODISTRIBUCIJSKE KONFERENCIJE

OTPORNOST NA KIBERNETIČKE PRIJETNJE U EES-u

Zagreb, 14. ožujka 2024.

Fakultet elektrotehnike i računarstva, Siva vijećnica
Unska ulica 3, Zagreb

ožujak 2024.

Međunarodna elektrodistribucijska konferencija CIRED (akronim od Congrès International des Réseaux Electriques de Distribution; International Conference on Electricity Distribution) je udruga koja okuplja zainteresirane u području elektrodistribucijske djelatnosti: najširi krug stručnjaka iz distribucijskih poduzeća, iz instituta i fakulteta, proizvođače opreme i davatelje usluga, opskrbljivače i potrošače, regulatore. Cilj je CIRED-a, prema Statutu, povećanje stručne kompetencije i sposobnosti, umijeća i znanja, u najširem području elektroprivredne djelatnosti.

Jedan od načina širenja i produbljivanja stručne kompetencije su savjetovanja, tematski seminari, radionice i skupovi. S tim ciljem Hrvatski ogranak Međunarodne elektrodistribucijske konferencije (HO CIRED) organizira – seminar

OTPORNOST NA KIBERNETIČKE PRIJETNJE U EES-u

O SEMINARU

Do 17. listopada 2024., sve zemlje EU-a moraju prenijeti NIS 2 direktivu u nacionalni zakon. Nije lak pothvat, jer novi propisi o kibernetičkoj sigurnosti podrazumijevaju opsežne zahtjeve.

Europska unija pokrenula je Direktivu NIS-2 (Direktiva o mrežnoj i informacijskoj sigurnosti 2) kako bi ojačala kibernetičke sposobnosti unutar EU-a i promicala međunarodnu suradnju u borbi protiv kibernetičkih napada. Posebna pozornost posvećena je prevenciji incidenata kritične infrastrukture. Proširenje NIS Direktive iz 2016. već je stupilo na snagu 16. siječnja 2023. Sada vrijeme pritišće: države članice imaju vremena do 17. listopada 2024. da ga prenesu u nacionalno zakonodavstvo. Nimalo lak zadatak, jer za razliku od GDPR-a, neće postojati NIS-2 oznaka ili lista kojih se tvrtke moraju pridržavati. A u usporedbi s NIS-1, NIS-2 sa sobom donosi opsežniji skup zahtjeva i odgovornosti. U slučaju kršenja predviđene su visoke kazne do deset milijuna eura ili dva posto globalne prodaje. U najgorem slučaju, tvrtke mogu izgubiti i dozvolu za rad.

Važno je razjasniti na koje se tvrtke odnosi NIS 2 direktiva i kako se rješenja mogu pravovremeno implementirati. Prezentacija seminara će odgovoriti na ova i druga pitanja zajedno s pružateljima usluga sigurnosti i partnerima u sklopu tematskog seminara o NIS-2 direktivi.

SADRŽAJ SEMINARA

Pozdravna riječ organizatora i uvod Voditelja seminara

Tema 1:
OTPORNOST NA KIBERNETIČKE PRIJETNJE I UVOD U NIS 2 DIREKTIVU
Mario Jurčević, dipl.ing.el., Vodeći stručnjak za kibernetičku sigurnost, KONČAR-Digital

Razvojem tehnologije i povećanjem broja digitaliziranih poslovnih procesa povećavaju se i rizici koji proizlaze iz kibernetičkih prijetnji, a njihov je utjecaj sve značajniji za poslovanje. Kako bi se utjecaj rizika na poslovanje umanjio potrebno je proaktivno identificirati, procijeniti i upravljati prijetnjama i ranjivostima, te primijeniti odgovarajuće kontrole i strategiju ovladavanja rizicima. Aktivno upravljanje rizicima stvara temelj za održivu kibernetičku otpornost, a jedna je od mjera kibernetičke sigurnosti o kojoj moraju voditi računa svi subjekti u polju primjene NIS2 direktive.

NIS2 direktiva jedan je od ključnih okvira za podizanje razine sigurnosti, a pruža jasne smjernice i zahtjeve koji se odnose na kritičnu infrastrukturu i digitalne usluge. Razumijevanje i implementacija ovih smjernica ne samo da osiguravaju usklađenost s regulatornim okvirom, već i pridonose stvaranju otpornosti organizacije na kibernetičke prijetnje. Otpornost organizacije ne zahtijeva samo primjenu tehničkih sigurnosnih mjera već i prilagodbe procesa i ulaganja u zaposlenike.

Cilj izlaganja je naglasiti važnost proaktivnog pristupa za unaprjeđenje kibernetičke sigurnosti te pružiti korisne informacije o implementaciji NIS2 direktive kao ključnog koraka prema jačanju otpornosti u digitalnom dobu.

Tema 2:

NEK KIBERNETIČKA SIGURNOST- EPRI Technical Assessment Metthodology

Roman Kočnar, dipl.ing., Nuklearna elektrana Krško

Opisat će se način na koji NEK regulira područje kibernetičke sigurnosti kritičnih digitalnih sustava. Navedena je razlika između važećih slovenskih zakona " Zakon o informacijski varnosti" (napisan na temelju EU NIS direktive) i " Pravilnik o dejavnikih sevalne in jedrske varnosti" (napisan na temelju US 10CFR73.54). Opisani su kriteriji kako NEK procjenjuje kritičnost digitalnog sustava u smislu kibernetičke sigurnosti.

Opisana je metoda EPRI Technical Assessment Methodology (TAM) kojom izrađujemo analizu odnosno utvrđujemo rizike za svaki kritični digitalni sustav i kako utvrđujemo potrebne sigurnosne mjere za zaštitu, detekciju, odgovor i oporavak u slučaju cyber incidenta.

Tema 3:

PREDUVIJETI OTPORNOSTI EES-a NA KIBERNETIČKE PRIJETNJE

mr.sc. Krešimir Kristić, dipl.ing.el, CISM, HEP d.d.

Sprječavanje kibernetičkog napada, a ako se on ipak dogodi, smanjenje ili u najboljem slučaju potpuno otklanjanje mogućih posljedičnih šteta, primarni je cilj aktivnosti usmjerenih na zaštitu kritičnih elektroenergetskih infrastruktura. Drugim riječima, cilj je postići otpornost kritične infrastrukture na kibernetičke (cyber), ili u širem kontekstu, kombinirane hibridne fizičke i kibernetičke (cyber) prijetnje i napade. Prikazani su preduvjeti za pravocrtno, ekonomski opravdano, učinkovito i djelotvorno postizanje primarnog cilja zaštite kritičnih elektroenergetskih infrastruktura, uz poštivanje specifičnosti i načela supsidijarnosti u svakom pojedinačnom slučaju.

Tema 4:

STRATEGIJE ZA RAZVOJ ČVRSTIH OKVIRA ZAŠTITE OD PRIJETNJI

Ana Balaško, dipl.ing.el, HEP-ODS
Ivan Periša, dipl.ing.el, HEP-ODS

Kibernetička sigurnost i otpornost su od vitalnog značaja u elektroenergetskom sektoru, kritičnoj infrastrukturi koja podržava druge važne sektore poput zdravstva, komunikacija, transporta, financija i sl. Napadi na elektroenergetsku infrastrukturu mogu imati ozbiljne posljedice na društvo i gospodarstvo, uključujući gubitak proizvodnje, ekonomske štete te ugrožavanje života i sigurnosti ljudi. Razvoj čvrstih okvira zaštite od kibernetičkih prijetnji u elektroenergetskom sustavu ključan je za osiguravanje sigurnosti, stabilnosti i otpornosti na kibernetičke prijetnje. Energetska tranzicija i transformacija distribucijske elektroenergetske mreže u naprednu distribucijsku mrežu dodatno su usložnili poslovne procese, povećali povezanost s informacijskim tehnologijama te povećali rizik od kibernetičkih napada. Seminarom će se obuhvatiti područja kibernetičke sigurnosti, otpornosti i informacijske sigurnosti u elektroenergetskom sustavu te strategije za izgradnju otpornosti na kibernetičke prijetnje. Redovita revizija i ažuriranje strategija su ključni u dinamičnom kibernetičkom okruženju, dok je integracija kibernetičke sigurnosti ključna za uspješnu energetsku tranziciju i očuvanje stabilnosti društva i gospodarstva.

Tema 5:

PRIMJERI NAJBOLJIH PRAKSI I INDUSTRIJSKE NORME

Dr.sc. Tamara Hadjina, Voditelj istraživačkih projekata kibernetičke sigurnosti, KONČAR-Digital

EES je kompleksan, ali dobro osmišljen sustav, koji je od samih početaka dizajniran kako bi bio pouzdan i siguran. Međutim, ubrzana integracija sustava informacijske i operativne tehnologije dovodi do stvaranja novih potencijalnih vektora za kibernetičke napade na EES.

Povećanje otpornosti na novonastale kibernetičke prijetnje postiže se kombinacijom proaktivnih mjera, uključujući robusne preventivne okvire, mehanizme otkrivanja prijetnji, strategije odgovora na incidente i kontinuirano praćenje. Cilj prezentacije je pružiti razumijevanje izazova koje kibernetičke prijetnje postavljaju operativnoj tehnologiju u EES-u te ponuditi praktična rješenja za jačanje otpornosti sektora.

Tema 6:

GOVERNANCE FUNKCIJA U KIBERNETSKOJ SIGURNOSTI IZMEĐU EKOSUSTAVA DIGITALNIH PLATFORMI I DIGITALNIH BLIZANACA

Prof. dr. Hrvoje Pandžić, FER
Prof. dr. Slavko Vidović, ILBA Institut
Mr.sc. Domen Verdnik, INFODOM Grupa
Dr.sc. Stjepan Sučić, Končar Digital

Upravljački sustavi kritičnih infrastruktura su temeljeni na digitalnim tehnologijama i primjeni alata Industrije 5.0. Uz njihovu kompleksnost i funkcionalni značaj kao digitalnih platformi, oni predstavljaju najosjetljiviji dio kritičnih infrastruktura (KI).
Kibersigurnost je pozicionirana među najvažnija područja rizika, tako da je upravljanje rizicima interes ne samo poduzeća iz KI, nego i interes njemu povezanih subjekata, kao dijela poslovnog ekosustava poduzeća.
EU je kroz direktive NIS2, DORA i CER pokrenula sinkronizirano rješavanje ovih potreba u svim zemljama EU, a do 17. listopada 2024. godine članice EU moraju usvojiti i objaviti mjere za usklađivanje s NIS2 Direktivom. Kao nova funkcija i ključno proširenje u NIS2 postavljana je ishodišno GOVERNANCE funkcija pored pet dosadašnjih funkcija.
U partnerstvu FER-a, Končara d.d. i Beyondi d.o.o. (Osijek), InfoDom d.o.o., Zagreb organizirao je provedbu EU financiranog projekta „Razvoj digitalne platforme za izgradnju sustava zaštite kritičnih infrastruktura u pametnim industrijama — CIP 4 SI“. Kroz rad i prezentaciju prikazat će se integracijska arhitektura kompleksne platforme (koja se tehnički temelji na tri povezane platforme: napredna Smart SCADA od Končara te platforme za upravljanje rizicima i za provedbu DX transformacije, s primjenom DLT tehnologije - Blockchaina za rad digitalnih blizanaca).
U suradnji sa "Institutom za hibridne prijetnje" provedena su i pripadna istraživanja.
Na rezultatima ovog projekta omogućava se poduzećima iz KI ubrzati primjenu EU Direktive NIS2 i kontrolirati usklađenost sa nacionalnim i EU propisima, te podržati unapređenja sustava zaštite kritičnih infrastruktura.

Tema 7:

PRAKTIČNI SAVJETI ZA OBNOVU NAKON NAPADA

mr.sc. Berislav Crkvenac, tehnički direktor, DIVERTO

Učinkovitost odgovora na kibernetičke napade u industrijskim okruženjima neraskidivo je povezana sa zrelošću temeljnih poslovnih procesa u sustavu. Funkcionalan proces upravljanja rizicima najbolja je zaštita te preduvjet uspješnom i kontroliranom oporavku u slučaju neželjenih događaja. Složeni i isprepleteni lanci opskrbe te sve izraženija ovisnost o uslugama vanjskih partnera povećavaju izloženost kompanije kibernetičkim prijetnjama, a odgovor na moguće incidente čine složenijim. Domena kibernetičke sigurnosti se tradicionalno smatra domenom napredne tehnologije, no nužno je sagledati cjelokupan poslovni ekosustav kojeg čine ljudi, procesi i tehnologija. Naglasak valja staviti na izradu cjelokupnog plana oporavka, a osobito planiranje i osiguravanje učinkovite komunikacije prije i tijekom incidenata, kako interno unutar kompanije, tako i s vanjskim dionicima.

Podijeliti ćemo pojedine dobre prakse iz industrije i svoja iskustva stečena u radu, s ciljem izbjegavanja i što brže obnove poslovanja u slučaju kibernetičkih napada.

Tema 8:

NIS2 IMPERATIV OT SIGURNOSTI EES-a- Koja je Vaša strategija?

Ivan Turčin, Senior Data & AI Applications Specialty Leader, IBM

Kako se industrijska okruženja digitalno transformiraju, postaju povezanija i ranjivija. Industrijski sustavi razvijaju se od parnih strojeva potaknuli su prvu industrijsku revoluciju 1800-ih. Na svakom koraku te transformacije, inovacije industrijskih uređaja su poboljšale sposobnost industrije da brže,
učinkovitije, sigurnije i po nižoj cijeni obave svoj posao. Kako je automatizacija postajala sve prisutnija, tako je nastala i operativna tehnologija (OT) i započela sa upotrebom hardvera i softvera za nadzor i kontrolu uređaja. Sustavi industrijske kontrole (ICS) postali su nužnost za OT okruženja. Oni
prate i reguliraju procesne vrijednosti poput temperature, tlaka, protoka, napona, jakost, frekvencija, … te nadziru uređaje kako bi otkrili i spriječili opasna stanja i kvarove.

Ova godina i nekoliko koje slijede će donijeti veliki fokus na uvođenje NIS2 EU direktive. Ta direktiva će dodatno pooštriti uvjete i nadzor kibernetičke sigurnosti ključnih subjekata bitnih za funkcioniranje društva, države i infrastrukture. Elektroenergetski sustav (EES), kao jedan od fokalnih, osim klasične sigurnosti informacijsko tehnoloških (IT) sustava morati će uvesti i poseban nadzor okolina operacijske tehnologije (OT) i provjeru/nadzor subjekata u njihovom kritičnom lancu dobave. Obveznici regulative morat će voditi računa da odabrana tehnološka rješenja zadovoljavaju sve zahtjeve regulatora i odabrati rješenja koja implementiraju aspekte i IT i OT sigurnosti.

Donosimo prikaz IT/OT sigurnosnih tehnologija, rješenja za EES, pristupa uslugama za zaštitu OT-a i strategija koje pomažu organizacijama na različitim razinama sigurnosne zrelosti da poboljšaju sigurnosti OT-a i ubrzaju vrijeme u kojem će implementirati sljedeću razinu sigurnosti OT-a.

Tema 9:

INTEGRACIJA ZAHTJEVA NIS 2 i DORA-e U SIGURNOSNE STRATEGIJE KRITIČNE INFRASTRUKTURE
dr.sc. Natalija Parlov Una, **ACCREDI APICURA**

Sigurnosne strategije u kritičnoj infrastrukturi predstavljaju sveobuhvatne planove dizajnirane da zaštite vitalne sisteme i mreže od različitih vrsta prijetnji vezanih uz potencijal narušavanja njene sigurnosti i otpornosti. Potencijalne prijetnje, uz ostalo, uključuju i kibernetičke napade, prirodne katastrofe te slučajne ili namjerne ljudske pogreške. Glavni izazovi u definiranju ovih strategija obuhvaćaju upravljanje složenim rizicima vezanim uz održavanje visoke razine informacijske sigurnosti i otpornosti odnosno smanjenja mogućeg nepovoljnog utjecaja na kontinuitet poslovanja kritične infrastrukture i ključnih servisa, osiguravanje usklađenosti s novim regulativama te prilagodbu brzim promjenama ne samo u tehnološkom, već i u regulatornom okruženju.

Izlaganje je usmjereno na integraciju NIS2 i DORA-e u sigurnosne strategije, naglašavajući ulogu standarda ISO 27001, ISO 22301 i IEC 62443 kao kvalitativnih alata za usklađivanje s novim zahtjevima, osobito u aspektima upravljanja rizicima vezanih uz ljudski faktor te rizicima vezanim uz usluge trećih strana odnosno IT/OT opskrbni lanac, kao jednima od ključnih faktora u održavanju otpornosti kritične infrastrukture i potreba za njenom kontinuiranom digitalnom transformacijom te skalabilnosti i prilagodljivosti sigurnosnih, ističući važnost uspostave fleksibilnih strategija koje mogu odgovoriti na stalne promjene.

Zaključno, izlaganje pruža praktične smjernice za organizacije u izradi sigurnosnih strategija koje su usklađene s NIS2 i DORA-om, naglašavajući značaj holističkog pristupa i kontinuirane evaluacije u dinamičnom tehnološkom i regulatornom okruženju.

RASPRAVA SUDIONIKA I ZAVRŠNA RIJEČ VODITELJA SEMINARA

Sažetak ključnih spoznaja i zahvala sudionicima na sudjelovanju
TBD, CIRED

Congrès International des Réseaux Electriques de Distribution

HO CIRED, Zelinska 4, 10000 Zagreb
Telefon: (+ 385 1) 617 15 27
www.ho-cired.hr
ho@cired.hr

Seminar „Otpornost na kibernetičke prijetnje u EES-u“ HO CIRED-a održat će se **u četvrtak, 14. ožujka 2024.** u

Sivoj vijećnici, Fakultet elektrotehnike i računarstva
Unska ulica 3, Zagreb

u vremenu od 9 do 14 sati
sa sljedećim okvirnim rasporedom:

8:30 – 9:00	Prijava sudionika i jutarnje osvježenje
9:00 – 11:45	Prvi dio seminara
11:45 – 12:30	Ručak
12:30 – 14:00	Drugi dio seminara

Kotizacija za sudjelovanje na ovom seminaru iznosi

160,00 EUR + 40 EUR PDV = 200,00 EUR bruto

i uključuje jutarnje osvježenje i ručak.

Sadržaj predavanja i prezentacije bit će dostupni za preuzimanje na službenoj web stranici www.ho-cired.hr

Kotizacija se uplaćuje na IBAN HR93 2340 0091 1102 5968 2, Privredna banka Zagreb.
Prijavnicu poslati e–poštom na adrese: ho@cired.hr i tomko.zg.hr@gmail.com.
Broj sudionika je ograničen pa će se njihov konačni broj zaključiti redoslijedom prijave.

Prijavnica za Seminar dostupna je i na web–portalu www.ho-cired.hr, i šalju se ispunjeni e–poštom na adrese: ho@cired.hr i tomko.zg.hr@gmail.com.