Stratēģija izglītībai kiberdrošības jomā viedajos energotīklos (izpildes ziņojums)

Autori:

Marija Valjū (*Maria Valliou*), Aleksandrs Hronis (*Alexandros Chronis*), Pans Kotsampopuls (*Panos Kotsampopoulos*), Bahā Eltavijs (*Bahaa Eltahawy*), Tero Vartiainens (*Tero Vartiainen*), Mike Mekanens (*Mike Mekkanen*), Andrejs Romānovs, Jana Bikovska, Jānis Pekša, Rūta Pirta-Dreimane, Džirapa Kamsamrons (*Jirapa Kamsamrong)*, Bjerns Zīmerss (*Bjoern Siemers*)

Kiberdrošības mācību programmu ieteikumi viedajiem energotīkliem (*CC-RSG*)

Erasmus+ Stratēģiskās partnerības projekts

Intelektuālais ieguldījums 2

2022. gada aprīlis

Recenzenti: Fivs Palaiojannis (*Foivos Palaiogiannis*) un Larss Fišers (*Lars Fischer*)
Koordinators: Vāsas Universitāte
Partneri: *OFFIS*, Rīgas Tehniskā universitāte, Atēnu Nacionālā tehniskā universitāte

Šis projekts ir saņēmis finansējumu no Eiropas Savienības *Erasmus+* programmas saskaņā ar dotācijas nolīgumu № 2020-1-FI01-KA203-066624.

Eiropas Komisijas sniegtais atbalsts šī izdevuma publicēšanai nenorāda uz to, ka tā atbalsta izdevuma saturu, kas atspoguļo tikai autoru viedokļus, un Komisiju nevar uzskatīt par atbildīgu attiecībā uz jebkādu izdevumā ietvertās informācijas iespējamo lietojumu.

Saturs

Definīcijas, akronīmi un saīsinājumi 2
Tabulu saraksts 3
1. Ievads 3
1.1 Mērķi 3
1.2 Dokumenta struktūra 3
2. Nozarē esošie izaicinājumi 3
2.1 Nozares pārstāvju interviju analīze un literatūras pārskats 4
2.2 Identificētas vajadzīgās politikas un izglītības izmaiņas 4
3. Prasmju trūkuma mazināšanas plāns 4
3.1 Mazināšanas pasākumi 4
3.2 Grūtības attiecībā uz piedāvātā ceļveža iekļaušanu esošajā mācību programmā 6
4. Izglītības metodoloģijas piedāvājums 7
4.1 Īss aplūkoto metožu izklāsts 8
4.2 Izmantošanas piemēri un ietekme energosistēmu jomā — piedāvājums 9
5. Ieteikumi 10
6. Secinājumi 12
7. Bibliogrāfija 13

Definīcijas, akronīmi un saīsinājumi

Saīsinājums	Nozīme
ACM	Skaitļošanas tehnikas asociācija (*Association for Computing Machinery*)
CPES	Kiberfizikālās enerģijas sistēma (*Cyber Physical Energy System*)
CSIRT	Datordrošības incidentu reaģēšanas vienība (*Computer Security Incident Response Team*)
CTF	Karoga iekarošana (*Capture the flag*)
ENISA	Eiropas Savienības Tīklu un informācijas drošības aģentūra (*European Network and Information Security Agency*)

VDAR	Vispārīgā datu aizsardzības regula
IT	Informācijas tehnoloģija
KA	Zināšanu telpa (*Knowledge area*)
KU	Zināšanu vienība (*Knowledge unit*)
MQTT	*MQ* telemetrijas transports
TIS	Tīkla un informācijas sistēmas
PT	Pielietojama tehnoloģija
PBL	Uz problēmu risināšanu balstītas mācības (*Problem based learning*)
REST API	*Representational State Transfer* lietojumprogrammu saskarne
SAREF	Viedo lietojumprogrammu atsauces ontoloģija (*Smart Applications Reference Ontology*)
SIEM	Drošības informācija un notikumu pārvaldība (*Security Information and Event Management*)
UPRES	Pilsētvides plānotāji ar prasmēm atjaunojamās enerģijas jomā (*Urban planners with Renewable Energy Skills*)

Tabulu saraksts

1. tabula. *CC-RSG* viedā energotīkla kiberdrošības prasmju trūkuma mazināšanas plāns.....6

1. Ievads

Visā pasaulē ir ieviesti elektrotīkli ar informācijas un komunikācijas tehnoloģiju iespējām, tāpēc ir radusies nepieciešamība pēc profesionāļiem, kuriem ir starpnozaru zināšanas gan viedā energotīkla, gan kiberdrošības jomā. Mūsu projekts "Kiberdrošības mācību programmu ieteikumi viedajiem energotīkliem" cenšas atvieglot Eiropas pēcvidusskolas mācību programmu pielāgošanu, jo tām jāietver mācību mērķi, kas cita starpā ir saistīti ar kiberdrošību. Šajā ziņojumā projekta *IO1* identificētais prasmju trūkums tiek izmantots, lai attiecīgajām ieinteresētajām personām sniegtu norādījumus par to, kā apmācīt esošo un turpmāko darbaspēku, lai mazinātu šo prasmju trūkumu.

1.1 Mērķi

Precīzāki šī ziņojuma mērķi ir norādīti tālāk.

- Analizēt izaicinājumus, ar kuriem nozare sastopas kiberdrošības ziņā viedajos energotīklos.
- Izveidot mazināšanas plānu, kas balstīts uz *WP1* identificētajiem izaicinājumiem un prasmju trūkumu.
- Analizēt un ieteikt izglītotājiem novatoriskas izglītības metodoloģijas.
- Piedāvāt ieteikumus par to, kā izglītot pakalpojumu sniedzējus, politikas veidotājus un nozari.

1.2 Dokumenta struktūra

Dokuments ir strukturēts tālāk minētajā veidā.

2. nodaļā ir identificēti izaicinājumi, ar kuriem saskaras nozare.

3. nodaļā ir aprakstīts ieteiktais mazināšanas plāns.

4. nodaļā ir ietverta tradicionālo un novatorisko izglītības metožu analīze, aplūkojot to pielietošanas piemērus enerģētikas nozarē un to ietekmi.

5. nodaļa satur augsta līmeņa ieteikumus atbilstošajām ieinteresētajām personām.

Šī dokumenta nobeigumā ir secinājumi un bibliogrāfija.

2. Nozarē esošie izaicinājumi

Energosistēma tiek uzskatīta par svarīgāko infrastruktūru pasaulē, kas nodrošina pakalpojumus citām nozarēm. Jaunā nozare 4.0 (Ceturtā industriālā revolūcija), kas apvieno pielietojamu tehnoloģiju (PT) ar informācijas tehnoloģiju (IT), izmanto un paplašina digitalizācijas, savienojamības un automatizācijas jēdzienus, bet palielina uzņēmumu un sistēmu operatoru bažas par kiberdrošību.

Šī sadaļa ietver analīzi par nozarē esošajiem izaicinājumiem, kas definēti ar literatūras pārskatu un kvalitatīvām intervijām, kas tika veiktas šī projekta *WP1* kontekstā attiecībā uz kiberdrošību viedajos energotīklos. Šie izaicinājumi tiks izmantoti kā informācija, lai identificētu vajadzīgās politikas un izglītības izmaiņas, kas ļaus izstrādāt konkrētu stratēģiju izglītībai kiberdrošībā, lai tā atbilstu nozares vajadzībām pēc kompetentiem kiberdrošības profesionāļiem.

2.1 Nozares pārstāvju interviju analīze un literatūras pārskats

Izaicinājumi tika identificēti ar literatūras pārskata palīdzību un intervijās ar nozares ekspertiem. Intervijas tika veiktas kā *WP1* daļa. Tālāk minēti galvenie izaicinājumi, kas tika identificēti literatūras pārskatā.

1. Nepieciešamas lielas ieguldījumu izmaksas, lai izveidotu kiberfizikālās enerģijas sistēmu (*Cyber Physical Energy System — CPES*) ar visiem elementiem pietiekamai darbaspēka apmācībai.
2. Esošajos standartos un vadlīniju dokumentos nav pietiekamā mērā ietverti kritiski svarīgie aktīvi, kas jāaizsargā, vai arī ieteicamie pretpasākumi.
3. Kiberdrošības prasmju sertifikācijas sistēmas nav plaši pieņemtas vai ietvertas mācību programmās.
4. Ir grūti izveidot kiberdrošības kultūru darbaspēkam, kuru darba aprakstā nav tieši ietverti attiecīgie pienākumi.
5. Augstākās izglītības iestādēm (AII) un nozarei nav spēcīga starpsavienojuma.
6. Regulatori bieži tiek uzskatīti par tiesībaizsardzības iestādēm, nevis par galveno struktūrvienību attiecībā uz dalīšanos ar informāciju un savienojumu veidošanu starp dažādiem dalībniekiem.

Tālāk minēti galvenie izaicinājumi, kas tika identificēti intervijās.

1. Intervētās personas piekrīt *WP1* rezultātiem, kas norāda, ka atbilstošajā literatūrā nav aplūkota cilvēku organizatoriskā un sociālā drošība.
2. Trūkst izglītotāju, kas var iemācīt gan kiberdrošības tehniskos, gan netehniskos aspektus.
3. Absolventiem trūkst praktiskas pieredzes.
4. Absolventiem trūkst pārvaldības un komunikācijas prasmju.

2.2 Identificētas vajadzīgās politikas un izglītības izmaiņas

Pēc tam izaicinājumi tiek izmantoti, lai identificētu vajadzīgās politikas un izglītības izmaiņas, kas ir norādītas tālāk.

1. Praktiskas pieredzes un apmācības programmu nodrošināšana.
2. Starpfunkcionālas sadarbības uzlabošana (prakses programmas utt.).
3. Kiberdrošības kultūras veidošana.

3. Prasmju trūkuma mazināšanas plāns

3.1 Mazināšanas pasākumi

3. nodaļā tiek izveidots prasmju trūkuma mazināšanas plāns, kurā aprakstīti mazināšanas pasākumi, kas jāievieš vairākiem dalībniekiem. Kā atsauce tiek izmantota skaitļošanas tehnikas asociācijas (*Association for Computing Machinery — ACM*) sistēma. *ACM* sistēma kategorizē dažādus kiberdrošības aspektus pirmajā līmenī astoņās lielās grupās ar nosaukumu "Zināšanu telpas (*Knowledge areas — KA*)" un otrajā līmenī katrs *KA* ietver vairākas "Zināšanu vienības (*Knowledge Units — KU*)". Katrai zināšanu vienībai katrā no galvenajām zināšanu telpām tiek veikts novērtējums par to, vai izmaiņas jomā galvenokārt jāiesāk izglītības iestādēm vai nozarei. Katrā gadījumā ir ieteicami daži galvenie pasākumi. Tālāk redzamajā tabulā (1. tabula.) ir parādīti galvenie pasākumi.

Mazināšanas pasākumi												
Zināšanu telpa	**Zināšanu vienība**	**Zināšanas par elementu energosistēmā**	**Starptautiskas izpētes veikšana kiberdrošībā**	**Zināšanas par tīkla drošību**	**Profesionāla apmācība**	**Sertifikāti**	**Pašmācība**	**Zināšanas**	**Funkcionālas**	**Jaunu tehnoloģiju apguve**	**Praktiskas lietošanas**	**Apdraudējuma analīzes pamatrīki**
Datu drošība	Kriptogrāfija	X	X	X	X	X						
	Digitālā kriminālistika						X	X	X	X	X	X
	Datu integritāte un autentifikācija	X	X	X	X	X						
	Piekļuves kontrole	X	X	X	X	X						
	Drošas komunikācijas protokoli	X	X	X	X	X						
	Kriptoanalīze						X	X	X	X	X	X
	Informācijas glabāšanas drošība						X	X	X	X	X	X
Programmatūras drošība	Pamatprincipi	X	X	X	X	X						
Savienojuma drošība	Datu nesēji						X	X	X	X	X	X
	Aparatūras un fizikālo elementu saskarnes un savienotāji						X	X	X	X	X	X
	Sadales sistēmu arhitektūra	X	X	X	X	X						
	Tīkla arhitektūra	X	X	X	X	X						
	Tīkla īstenošana	X	X	X	X	X						

	Tīkla pakalpojumi						X	X	X	X	X	X
	Tīkla aizsardzība						X	X	X	X	X	X
Sistēmas drošība	Sistēmu pārvaldība						X	X	X	X	X	X
	Sistēmu piekļuve un kontrole						X	X	X	X	X	X
	Sistēmas testēšana	X	X	X	X	X						
	Vispārējas sistēmu arhitektūras	X	X	X	X	X						
Cilvēku drošība	Identitātes pārvaldība	X	X	X	X	X						
	Sociālā inženierija	X	X	X	X	X						
	Individuālā atbilstība kiberdrošības noteikumiem / politikai / ētikas normām						X	X	X	X	X	X
	Informētība un izpratne						X	X	X	X	X	X
	Personas datu privātums un drošība	X	X	X	X	X						
Organizatoriskā drošība	Riska pārvaldība						X	X	X	X	X	X
	Drošības pārvaldība un politika						X	X	X	X	X	X
	Sistēmu administrēšana						X	X	X	X	X	X
	Drošības iespējas						X	X	X	X	X	X
	Kiberdrošības plānošana						X	X	X	X	X	X
	Kiberdrošības snieguma rādītāji						X	X	X	X	X	X
	Darbības nepārtrauktība, negadījuma seku novēršana un incidentu pārvaldība						X	X	X	X	X	X
	Drošības programmas pārvaldība						X	X	X	X	X	X
Sociālā drošība	Kiberlikums	X	X	X	X	X						
	Kiberpolitika	X	X	X	X	X						
	Kiberētika	X	X	X	X	X						
Kiberdrošības rīki	Kiberdrošības rīku pārskats						X	X	X	X	X	X
	SIEM						X	X	X	X	X	X
	Digitālo dvīņu izmantošana kiberdrošībā						X	X	X	X	X	X
Enerģijas piegādes ķēdes kiberdrošība	Enerģijas piegādes ķēdes kiberdrošības pamati						X	X	X	X	X	X
	Enerģijas piegādes ķēdes kiberdrošības pārvaldības rīki (tostarp enerģijas jomas pārziņu uzraudzības rīki)						X	X	X	X	X	X

	Enerģijas piegādes ķēdes kiberdrošības uzraudzība						X	X	X	X	X	X
	Enerģijas piegādes ķēdes kiberdrošības notikumu pārvaldība						X	X	X	X	X	X

1. tabula. CC-RSG viedā energotīkla kiberdrošības prasmju trūkuma mazināšanas plāns.

3.2 Grūtības attiecībā uz piedāvātā ceļveža iekļaušanu esošajā mācību programmā

3. nodaļā aplūkotas arī galvenās grūtības attiecībā uz piedāvātā ceļveža iekļaušanu esošajās mācību programmās. Tās ir izkārtotas četrās grupās — skolotāju grūtības, temata / mācību programmas grūtības, izglītojamo grūtības un organizācijas grūtības.

Galvenās grūtības, ar kurām sastopas skolotāji, ir noskaidrotas un izceltas tālāk.

1. Mācīšanas metodoloģijas pārmaiņas: izmaiņas attiecībā uz mācīšanas stilu un metodēm. Tās parasti tiek uztvertas pozitīvi izstrādes posmā, bet rezultāti pēc ieviešanas var būt ļoti atšķirīgi.
2. Nepiemērotība noteiktu tematu mācīšanai dažādās mācību programmās: lielāka uzmanība tiek pievērsta noteiktiem tematiem vai jēdzieniem, savukārt citi temati netiek pietiekami aplūkoti.
3. Izmaiņas mērķos un mācību programmā.
4. Mācību līdzekļu pielāgošana: tā ir saistīta ar 1. punktu, kā arī ar organizācijas izmaiņām nākamajā sadaļā.
5. Novērtēšana: novērtēšanas kritēriji būtu jāpielāgo, lai tie atbilstu jaunajām izmaiņām.
6. Satura strukturēšana, pieejamība un piemērojamība.

Otrkārt, temata ziņā jauno mācību programmu vai sistēmu ieviešanai ir tālāk minētie izaicinājumi [1] [2].

1. Mācību resursu trūkums: ne vienmēr ir pieejami izstrādei un nepieciešamajām izmaiņām vajadzīgie resursi.
2. Nepietiekami attīstīts darbaspēks: tas ir saistīts ar iepriekšējo sadaļu, mācībspēka prasmes tieši ietekmē mācību programmas īstenošanas kvalitāti. Tādējādi jaunos mērķus nevar sasniegt, līdz mācībspēks nav augsti kvalificēts un gatavs ieviest izstrādāto mācību programmu.
3. Pārvaldes atbalsts.
4. Darba slodze: jaunu programmu ieviešana var būt laikietilpīga.
5. Gatavība pieņemt jaunas pieejas.
6. Ietekme: nedaudzos gadījumos mācību programmas ieviešana var radīt negaidītu negatīvu ietekmi.

Treškārt, izglītojamo ziņā izmaiņas sen izveidotā mācību programmā var tikt uzskatītas par novirzēm, nevis par virziena maiņu, tādējādi radot nepieciešamību studentus pietiekami

informēt par nepieciešamību mācību programmā veikt izmaiņas. Tomēr vairums izmaiņu sastapsies ar pretestību un var mazināt ticību organizācijai un tās uzticamībai. Visbeidzot, mācību programmu uzlabošanai var būt nepieciešami īpaši pakalpojumi un izglītības/apmācības rīki, un ne visas organizācijas var atļauties šādus uzlabojumus, kas attiecīgi ietekmētu uzlabotās mācību programmas īstenošanu un kvalitāti.

Iepriekš minētās problēmas ir raksturīgas grūtībām, kas jāņem vērā, izstrādājot esošo mācību programmu. Tomēr, kā norādīts [3], palīdzētu uzsvars uz starpvalstu mācību programmas izveidošanu, kas nodrošina lielāku elastību un tādējādi ir piemērota vairākiem reģioniem un nozarēm.

4. Izglītības metodoloģijas piedāvājums

Šajā nodaļā mūsu mērķis ir noskaidrot izglītības metodoloģijas vai metodes, kas būs noderīgas, mācot par kiberdrošību viedajos energotīklos. Šādā nolūkā mēs sākotnēji analizējam astoņas izglītības metodes un tad pārskatām to atsevišķu vai kombinētu izmantojumu interešu jomās. No pārskata rezultātiem mēs izveidojam piedāvājumus dažādām mācīšanas vidēm.

4.1 Īss aplūkoto metožu izklāsts

Tradicionālais mācību modelis – uz lekcijām balstītas mācības

Uz lekcijām balstītas mācības ir visplašāk izmantotā mācību metode, jo tai ir mērogojamības potenciāls un skolotājs kontrolē, kas tiks iemācīts un kādā veidā tas notiks. Tās lielākais trūkums ir tas, ka studenti eksāmenos var paļauties uz iegaumēšanu, nevis izpratni. To bieži kombinē ar dažādām uz pieredzi balstītām mācīšanās metodēm, piemēram, simulāciju un uzdevumiem laboratorijā.

Uz pieredzi balstītas mācības

Uz pieredzi balstītas mācības ietver visu veidu mācīšanos, kurās zināšanas tiek iegūtas caur pieredzi. Deivids Kolbs (*David Colb*) 1984. gadā to aprakstīja kā ciklu, kas var atkārtoties mūžīgi, jo pieredze izraisa teoriju veidošanos, kas pēc tam var tikt izmantotas, lai izveidotu jaunus eksperimentus un iegūtu vairāk pieredzes.

Aktīvās mācības

Arī aktīvās mācības ir diezgan plašs termins, tās ir balstītas uz studentu iesaistīšanās palielināšanu, izmantojot dažādu veidu līdzdalību. Lekcijas laikā tā var būt jēdzienu karte, jautājuma uzdošana publikai, “vienas minūtes lapiņa” vai grupas biedru mācīšana.

Kopīga mācīšanās

Kopīga mācīšanās apraksta darbu grupā, kur katrs students ne tikai atvēl laiku sava grupas darba daļas paveikšanai, bet ir arī atbildīgs par grupas sniegumu un prasmju sadalījuma efektivitāti grupā.

Apgrieztā klase

Apgrieztās klases metodē tiek sagaidīts, ka studenti pirms klases būs izpētījuši materiālus. Materiāls var būt jau pastāvošs, piemēram, grāmata vai video ierakstu sērijas, bet tas var būt arī īpaši izveidots kursam. Stundas laikā skolotājs var izmantot aktīvās mācīšanās metodes, lai pārbaudītu un padziļinātu studentu izpratni par kursa materiālu. Viens iespējams metodes trūkums ir nevienlīdzīga piekļuve elektroierīcēm studentu mājās.

Uz izpēti balstītas mācības

Uz izpēti balstītas mācības visvairāk atgādina zinātnisko metodi. To posmi ietver orientāciju, konceptualizēšanu, izpēti, secinājumu un diskusiju. Atkarībā no studentu vecuma skolotājs var iesaistīties un sniegt padomus lielākā vai mazākā mērā.

Uz problēmu risināšanu balstītas mācības un uz projektiem balstītas mācības

Šo divu metožu pamatā ir kopīga mācīšanās. Uz problēmu risināšanu balstītās mācībās (*Problem-based learning — PBL*) studentu grupa izpēta atvērta tipa īstās pasaules problēmu un mēģina izveidot vispiemērotāko risinājumu, kuru grupa pēc tam izklāsta citiem studentiem. Uz projektiem balstītas mācības būtībā ir ļoti līdzīgas uz problēmu risināšanu balstītām mācībām, bet tās parasti notiek ilgāk un risinājums ir ne tikai teorētisks, bet arī ar konkrētu un skaidru iznākumu, piemēram, datorprogramma vai modelis.

Spēliskošana

Spēliskošanā studentu iesaistīšanās palielināšanas nolūkā tiek izmantoti elementi un mehānismi, kas bieži ir ietverti spēles uzbūvē (līmeņa pārvarēšana, ierobežots laiks kādam uzdevumam utt.).

4.2 Izmantošanas piemēri un ietekme energosistēmu jomā — piedāvājums

Lai noteiktu dažādu metožu izmantošanas ietekmi attiecībā uz kiberdrošības viedajos energotīklos mācīšanu, mēs veicām literatūras pārskatu, kas ietvēra 43 dokumentus. 21 dokumentu bija sarakstījuši autori, kas izmantoja kādu no iepriekš minētajām metodēm, lai mācītu līdzīgu kursu, bet pārējie dokumenti bija vispārīgāki. Piezīmes no literatūras pārskata ir sniegtas tālāk.

Ierobežojumi, kurus nosaka aktīvo mācību metožu izmantošana.

Aktīvo mācību metodēm nepieciešams ne tikai lielāks mācībspēks, laiks un resursi, bet arī studentu grupas, kuras ir vienlīdzīgas un jau ir ar minimālām zināšanās par tematu.

Spēliskošanas izmantošana universitātēs.

Spēliskošana universitātēs var izpausties kā īstas spēles, piemēram, galda spēle *Riskio*, un to var izmantot bakalaura līmeņa studentiem vai netehniskiem darbiniekiem nozarē.

Karoga iekarošana un Hacking Day pasākumi

Karoga iekarošanas konkursi ir spēliskošanas veids, tajā ir uz pieredzi balstītu mācību un kopīgas mācīšanās elementi. *CTF* konkursos spēlētāju mērķis ir atklāt sistēmas ievainojamību (aparatūrā vai programmatūrā) un atrast atslēgu, kuru sistēmā paslēpa organizētāji (karogu). Tās var būt divas komandas, kas cīnās savā starpā, vai dalībnieku komandas, kas cenšas uzlauzt organizētāja sistēmu. *CTF* ir piemērots apmācībām par uzbrukumiem, kas notiek īsā laika posmā. Īpaši jārūpējas, lai palīdzētu iejusties spēlētājiem, kas ir iesācēji. *CTF* var izpausties kā karjeras diena, kurā piedalās nozares pārstāvji. Daži studenti var būt pasākuma organizētāju komanda, kas ļauj viņiem iegūt nozarē ļoti svarīgas prasmes.

Spēliskošanas izmantošana nozarē

Spēliskošana nozarē ir tikusi sekmīgi izmantota netehniskajiem darbiniekiem, lai sekmīgāk novērstu pikšķerēšanas uzbrukumus. Ir svarīgi norādīt, ka uzņēmumā, kura dati tika apkopoti, grupai ar iepriekšēju apmācību e-pasta pikšķerēšanas uzbrukumu novēršanā bija tādi paši rezultāti kā kontrolgrupai bez jebkādas apmācības.

Demonstrējuma lietošana

Demonstrējumu var izmantot gan bakalaura līmeņa studentiem, gan darbiniekiem. Vienā piemērā tiek izmantota programma *Shodan*, kas var atrast vairākas ierīces, kas ir savienotas ar internetu bez akreditācijas datiem vai ar noklusējuma akreditācijas datiem. Studenti un darbinieki var saprast, kāda ir potenciālā ietekme viņu uzvedībai attiecībā uz labiem kiberdrošības paradumiem.

Uz projektiem balstītu mācību lietošana

Uz projektiem balstītas mācības ir visbiežāk izmantotā metode, tāpat kā spēliskošana. Vairāki aptauju rezultāti norāda uz to, ka ievērojami uzlabojas dažas nedēļas pēc kursa beigām saglabāto zināšanu daudzums, ja studentu mācībās tika izmantotas praktiskas pieredzes metodes. [4]

Virtuālās laboratorijas un attālināta piekļuve

Virtuālo laboratoriju lietošanas tendence, kas aizsākās 2010. gadā, kļuva populārāka Covid-19 pandēmijas dēļ. Statistikas rezultāti no [5] norāda, ka studentiem ir vajadzība izmantot laboratorijas stundās, kurās tās parasti ir slēgtas apmeklētājiem, bet laboratorijas uzstādīšana ietver papildu darba stundas tehniskā atbalsta darbiniekiem.

Testēšanas vides izmantošana, lai mācītu par kiberdrošību

Vispilnīgākais un reālistiskākais veids, kā pētīt kiberuzbrukuma ietekmi un atlabšanas procesus, ir izmantot testēšanas vides. Testēšanas vidē sistēma tiek ļoti detalizēti simulēta. Detalizācijas pakāpe palielinās, aizvien vairāk simulētās sistēmas elementiem tiekot attēlotiem ar aparatūru, nevis programmatūru un pievienojot aizvien vairāk tās pašas sistēmas elementu. Piemēri reāllaika simulatoru izmantošanai kiberuzbrukumu izpētei ir sniegti [6], [7].

5. Ieteikumi

Ziņojuma pēdējā daļa ietver augsta līmeņa ieteikumus, kas izkārtoti saskaņā ar ieinteresēto personu, kurai tie paredzēti, proti, universitātēm, PIA, nozari un politikas veidotājiem. Ieteikumi tika veidoti no daudzu (galvenokārt Eiropas) dokumentu, piemēram, darba grupu ziņojumu, projekta nodevumu un citu dokumentu, kopsavilkuma. Nākamajās rindkopās mēs īsi izklāstīsim ieteikumus dažādām ieinteresētajām personām.

5.1.1 Universitātes

- Izveidot novērošanas centru, lai nepārtraukti uzraudzītu jaunās un esošās izpētes rezultātus kombinētajā jomā.
- Izveidot datubāzi ar ekspertiem un pētniekiem, norādot viņu darba jomas, lai izveidotu kopīgas maģistra programmas, kas pašlaik programmā "*Erasmus Mundus*" nepastāv attiecīgajā jomā.
- Turpināt un paplašināt Eiropas kredītpunktu pārnesi saskaņā ar Boloņas procesu. Kopīgu mācību programmu pastāvēšanas priekšnoteikums ir Eiropas akreditācijas sistēmu saskaņošana.
- Pārvarēt aprīkojuma trūkuma radītos šķēršļus, izveidojot infrastruktūras pārskatu saskaņā ar *ERIGRID* 2.0 projekta sniegto piemēru.
- Izveidot kursa moduļu repozitoriju, lai kopīgotu kursu dizainu un paraugpraksi ar mērķi paātrināt attiecīgu mācīšanās rezultātu ieviešanu.

- Universitātēm vairāk jāpievēršas “T formas” inženieru, kuriem ir plašas vispārējās zināšanas (T burta horizontālā līnija) un augstas specialitātes jomas zināšanas (T burta vertikālā līnija), veidošanai.
- Vispārējām zināšanām būtu jāietver ētiskie, sociālie un juridiskie aspekti, ko var ievērot STEM (*Science Technology Engineering and Mathematics* — zinātnes, tehnoloģiju, inženierzinātņu un matemātikas) programmās.

5.1.2 PIA

- Izveidot *UP-RES* [8] līdzīgu projektu, kas bija arī piemērs projektam ar divām jomām, kas jākombinē, proti, atjaunojamās enerģijas resursiem un pilsētplānošanu. Rezultāts būs apmācīti profesionāļi, izglītības paraugprakses, izglītības materiāls un iespējama universitāšu sadarbība.
- Tālākās profesionālās izglītības un apmācības nodrošinātājiem jāizveido kursi un tiešsaistes apmācības moduļi par ļoti konkrētu tematu, piemēram, kā senākā ierīcē ieviest komunikācijas protokolu. Tie var veidot maģistra “mikrokursu”, kas ir ekvivalents maģistra programmas semestrim.
- Daži kursi var tikt izmantoti kā sagatavošanās sertifikāta iegūšanai, kas kopumā var palīdzēt uzlabot absolventa nodarbinātības iespējas, ja sertifikāti ir īpaši rūpīgi izvēlēti.

5.1.3 Nozare

Darbinieku kiberdrošības kompetenci var analizēt divās plašās kategorijās, kas, pirmkārt, ir tehniskas un ar uzņēmuma produktu vai pakalpojumu saistītas prasmes un zināšanas un, otrkārt, ir informētība par to, kā sistēmas drošību var ietekmēt cilvēka faktors (gan darbinieka, gan klienta).

- Darbiniekiem mācāmie temati un principi ietver tālāk minētos.
  - Salīdzinot kopīgotās datubāzes modeli ar modeli, kas balstīts uz ziņojumiem, uz ziņojumiem balstīts modelis ir izdevīgāks. [9]
  - Viedo lietojumprogrammu atsauces ontoloģijas (*Smart Applications REFerence — SAREF*) modelis, kas analizē mājokļa lietu interneta ierīces attiecībā uz to būvblokiem un savstarpējām attiecībām.
  - Orientācija par to, kā iespējot elementu nepārtrauktu atjaunošanu un uzlabošanu.
  - **Integrētas drošības** un **drošības pēc noklusējuma** principu pielietošana.
  - Attiecīgie tiesību akti. Labs pārskats līdz 2017. gada vidum atrodas [10], un nesen tika pievienota VDAR un TIS 2.0 direktīva.

Trīs punkti, kas atšķir kiberdrošības jomu enerģētikā no vispārējas kiberdrošības jomas, ir [11] senāka aprīkojuma lietošana, lavīnveida seku pastāvēšana Eiropas tīklu lielo starpsavienojumu skaita dēļ un reāllaika prasības, kas nozīmē, ka dažas darbības energotīklā jāveic ļoti ātri un attiecīgi jāatlasa drošības protokoli. Katrā no šiem aspektiem ieteicams mācīt tālāk minētos principus un paraugprakses.

Senāks aprīkojums: sistemātiska ielāpu pārvaldība un regulāra risku analīze attiecībā uz senākām ierīcēm.

Lavīnveida sekas: aktīvu klasificēšana un kritiski svarīgu punktu identificēšana, lai izvairītos no vienota atteices punkta.

Reāllaika prasības: tīklu nošķiršana.

- Ieteikumi attiecībā uz cilvēkfaktora ietekmi uz kiberdrošību.

- Uzņēmumiem jāorganizē semināri, kuros tiek noteikta darbinieku kompetence to lēmumu kvalitāte, ko viņi pieņem saistībā ar kiberdrošību.
- Vadītājiem jāapgūst papildu apmācības par to, kā viņu uzvedība ietekmē viņiem pakļautās personas [12], piemēram, lai skaidri norādītu, ka drošību nedrīkst mazināt ražīguma nolūkos.
- *ENISA* rīka "*Good practices for IoT and Smart Infrastructures Tool*" (Lietu interneta un viedo infrastruktūru paraugprakses rīks) izmantošana, kas var būt noderīgs tieši maziem uzņēmumiem.

5.1.4 Politikas veidotāji

- Jāpārbauda, kā dalībvalstis ir ieviesušas TIS 2.0 direktīvu, kas var tikt izmantots kā atsauces modelis. Ir svarīgi pastāvēt TIS iestādei un Datordrošības incidentu reaģēšanas vienībai. Saskaņā ar TIS direktīvu nozarēm jānorāda savi aktīvi, darbības un svarīgie infrastruktūras komponenti, kā arī jāidentificē būtisko pakalpojumu operatori.
- Izveidot repozitoriju, kur operatori un citas puses var kopīgot detalizētu informāciju par incidentiem un veikt agrīnu brīdināšanu par uzbrukumiem un pārkāpumiem.
- Jādefinē un stingri jāievēro minimālās drošības sistēma.
- Jānorāda izmantotās platformas un platformu sadarbspējas kritēriji jādefinē tā, kā tas ieteikts uzņēmuma arhitektūras praksē [13]
- Izveidot repozitoriju, kur nozares pārstāvji var nepārtraukti uzzināt nepieciešamās prasmes.
- Izveidot kopīgu valodu, kas palīdzēs atbrīvoties no komunikācijas šķēršļiem, it īpaši vadītāju un tehnisko darbinieku starpā.
- Ļoti ieteicams ar pieejamajiem komunikācijas līdzekļiem, piemēram, *MQQT* un *REST API*, nomainīt pašizstrādātus risinājumus.
- Izstrādāt jaunas datu lomas, iespējams, izmantojot *Harmonized Electricity Market Role Model* (Saskaņotas elektroenerģijas tirgus paraugu).
- Piemērot vienotas informācijas modeļa standartus pārvades sistēmas operatoram un sadales sistēmas operatoram.

5.1.5 Ieteikumi par sadarbības veicināšanu ieinteresēto personu starpā

Kā minēts iepriekš, izglītībai kiberdrošības jomā energosistēmās jābūt vairāku ieinteresēto personu koordinētai darbībai, un tā ir joma, kurā notiek straujas izmaiņas. Mēs iesakām izveidot augsta līmeņa forumu dialogam, kas tiks sasaukts katru gadu vai divreiz gadā un kurā piedalīsies attiecīgie politikas veidotāji, sadales sistēmu operatori, pārvades sistēmu operatori, universitātes, PIA, lai dalītos ar informāciju par esošajām un plānotajām darbībām nozarē.

Vēl viena iespēja, kā saglabāt komunikāciju, ir lielu pasākumu rīkošana izglītības iestādēs ar nozares pārstāvju atbalstu, kas varētu nodrošināt aprīkojumu, Šādi pasākumi var arī darboties kā karjeras dienas un palielināt iespēju, ka studenti karjeras veidošanai izvēlēsies kiberdrošības nozari.

6. Secinājumi

Šajā ziņojumā mēs centāmies izprast, kādos aspektos izglītībai kiberdrošības jomā viedajos energotīklos ir trūkumi, un piedāvāt efektīvas izglītības metodes un citus augsta līmeņa ieteikumus, lai palīdzētu uzlabot izglītību šajā jomā. Analīze tika veikta, izmantojot plašu

literatūras pārskatu, intervijas ar nozares pārstāvjiem un īpašu semināru, kas notika *CC-RSG* kontekstā 2021. gada maijā.

Nozarē sastopamie izaicinājumi galvenokārt ir saistīti ar to, ka jaunajiem absolventiem nav pietiekamu apmācību attiecībā uz praktiskām situācijām, kas līdzinās tām, kas radīsies darba laikā, kā arī pārvaldības un komunikācijas problēmām.

Attiecībā uz izglītības metodēm kiberdrošības jomā visdaudzsološākā šķiet spēliskošana. To var izmantot, lai apmācītu netehniskos darbiniekus, kas strādā energosistēmu nozarē, lai viņi gūtu kiberdrošības pratību, un to var izmantot arī tehnisko darbinieku apmācībā, it īpaši palīdzot viņiem iegūt praktisku pieredzi.

Ir atklāts, ka uz projektiem balstītas mācības uzlabo pēc pāris nedēļām saglabāto zināšanu daudzumu, bet, tāpat kā visām citām aktīvo mācību metodēm, tām ir zināmi ierobežojumi, no kuriem svarīgākie ir tas, ka to var izmantot studentiem, kuriem noteiktajā tematā jau ir zināma līmeņa autonomija, un ka studentu komandām jābūt vienlīdzīgām.

Attiecīgais temats ir ļoti cieši saistīts ar aparatūru, tāpēc ir ļoti svarīgi izstrādāt viedus, kā pēc iespējas vairāk ieinteresētajām personām iegūt piekļuvi attiecīgajam aprīkojumam. To var paveikt dažādos veidos, piemēram, paplašinot testēšanas vižu attālinātās piekļuves lietošanu pētniecības centros vai izglītības iestādēs, organizējot infrastruktūras kopīgošanas veidus (piemēram, ES projekts *ERIGRID* 2.0) vai aicinot nozares pārstāvjus piedalīties attiecīgos universitātes kursos. Aprīkojums var būt gan vispārējs aparatūras aprīkojums, piemēram, datori, un arī specializēts aprīkojums, piemēram, *PMU*, RTU, reāllaika simulators utt.

Ieinteresētajām personām izteiktie ieteikumi lielā mērā attiecas uz komunikācijas veidiem un pieejamo resursu (profesionāļu, paraugprakses, infrastruktūras) kartēšanu. Kartēšana ir pamatā tam, kā izveidot efektīvus pieejamo resursu apkopšanas veidus, piemēram, izveidojot kopīgus grādus, agrīnās brīdināšanas sistēmu kiberdrošības incidentiem utt.

Kopā ar iepriekš minētajiem ieteikumiem esam ietvēruši arī īsu analīzi par zināšanām, kuras nozares pārstāvjiem būtu jācenšas iemācīt tehniskajiem darbiniekiem, un analīzi par to, kā energosistēmu kiberdrošība atšķiras no vispārējas kiberdrošības jomas.

Politikas veidotājiem svarīgākais uzdevums ir izveidot komunikācijas ceļus, piemēram, kopīgu valodu vadītājiem un tehniķiem, *European Cybersecurity Skills Framework* (Eiropas kiberdrošības prasmju pamatnostādnes), kuras sagaida *ENISA* (lai gan tās neattiecas tikai uz energosistēmām) un direktīvas un regulas, lai mazinātu pašizstrādātu risinājumu izmantošanu.

Iepriekš minētā analīze parāda priekšrocības, ko sniedz reāllaika testēšanas vides izveidošana, kas atveido gan energosistēmu, gan komunikācijas tīklu. Šo modeli pēc tam var izmantot, lai analizētu iespējamos uzbrukumus (iespējams, kopā ar cilvēka kļūdu) unikālos apstākļos un prasībās, kādas ir viedajiem energotīkliem (un energosistēmām kopumā).

7. Bibliogrāfija

[1] R. R. &. S. S. Hipkins, “Curriculum changes, priorities and issues: Findings from the NZCER secondary 2006 and primary 2007 national surveys.,” NZCER, 2008.

[2] B. (. B. Rachel Lowe, “Pre-Service Teachers’ Experiences With Curriculum Integration: A Qualitative Study,” 2017.

[3] J. M. T. Nyamkhuu, “Challenges in integrating 21st century skills into education systems,” 2019. [Tiešsaistē]. Pieejams: https://www.brookings.edu/blog/education-plus- development/2019/02/05/challenges-in-integrating-21st-century-skills-into-education- system/.

[4] K. O. K. K. Yoshitatsu Ban, “Effectiveness of Experiential Learning for Keeping Knowledge Retention in IoT Security Education,” in *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 2017.

[5] B. H. R. D. A. S. a. S. B. Kara Nancea, “Virtual Laboratory Environments: Methodologies for Educating Cybersecurity Researchers,” *Methodological Innovations Online,* 4. sēj., Nr.. 3, 3-14 lpp., 2009.

[6] S. L. L. W. M. K. S. Q. A. J.-N. P. S. L. Lixi Zhang, “Cybersecurity Study of Power System Utilizing Advanced CPS Simulation Tools,” in *PAC World Americas Conference*, Raleigh, North Carolina, USA, 2019.

[7] A. S. R. Liu, “Integrated Simulation to Analyze the Impact ofCyber-Attacks on the Power Grid,” in *2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Seattle, WA, USA, 2015.

[8] Euroheat & Power, “UP-RES: Urban Planners with Renewable Energy Skills,” [Tiešsaistē]. Pieejams: https://www.euroheat.org/our-projects/res-urban-planners-renewable- energy-skills/.

[9] BRIDGE project: Data management working group, “Main findings and recommendations,” 2019.

[10] R. Leszczyna, “Cybersecurity and Privacy in Standards for Smart Grids – a Comprehensive Survey,” *Computer Standards & Interfaces 56,* 09 2017.

[11] BRIDGE project: Data management working group, “Cybersecurity and Resilience,” 2019.

[12] ENISA, “Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity,” 2018.

[13] BRIDGE project: Data management and Regulation working groups, “TSO-DSO Coordination,” 2019.

[14] BRIDGE project, “Minutes BRIDGE Topics meeting,” 2019.