Strategi för utbildning i cybersäkerhet i smarta nät (Verkställande rapport)

Författare:

Maria Valliou, Alexandros Chronis, Panos Kotsampopoulos,

Bahaa Eltahawy, Tero Vartiainen, Mike Mekkanen,

Andrejs Romanovs, Jana Bikovska, Janis Pekša,

Ruta Pirta-Dreimane, Jirapa Kamsamrong, Bjoern Siemers

Kursplansrekommendationer för cybersäkerhet i smarta nät (CC-RSG)

Strategiskt partnerskapsprojekt inom Erasmus+

Kunskapsproduktion 2

April 2022

Granskare: Foivos Palaiogiannis och Lars Fischer
Samordnare: Vasa universitet
Samarbetsparter: OFFIS, Riga Technical University, National Technical University of Athens

Detta projekt har fått finansiering från Europeiska unionens Erasmus+program inom ramen för bidragsavtal nr 2020-1-FI01-KA203-066624.

Europeiska kommissionens stöd till upprättandet av denna publikation utgör inte ett godkännande av innehållet, som endast återspeglar författarnas åsikter, och kommissionen kan inte hållas ansvarig för eventuell användning av informationen i den.

Innehåll

Definitioner, akronymer och förkortningar 2
Förteckning över tabeller 3
1. Inledning 3
1.1 Mål 3
1.2 Dokumentets struktur 3
2. Utmaningar för industrin 3
2.1 Analys av branschintervjuer och litteraturöversikt 4
2.2 Identifierade behov av förändring i policyer och utbildningar 4
3. Plan för att minska kunskapsluckor 4
3.1 Riskreducerande åtgärder 4
3.2 Svårigheter med att integrera den föreslagna färdplanen i befintliga kursplaner 6
4. Förslag till utbildningsmetodik 7
4.1 En kort redogörelse för de metoder som har beaktats 8
4.2 Exempel på användning och effekter på området energisystem - Förslag 9
5. Rekommendationer 10
6. Slutsatser 12
7. Litteraturförteckning 13

Definitioner, akronymer och förkortningar

Förkortning	Betydelse
ACM	Association for Computing Machinery
CPES	Cyberfysiska energisystem (Cyber Physical Energy System)
CSIRT	Insatsstyrka vid datorsäkerhetsincidenser (Computer Security Incident Response Team)
CTF	Capture the flag
ENISA	Europeiska byrån för nät- och informationssäkerhet
GDPR	Den allmänna dataskyddsförordningen
IT	Informationsteknik
KA	Kunskapsområde
KU	Kunskapsenhet
MQTT	MQ Telemetry Transport
NIS	Nätverks- och informationssystem
OT	Driftteknik
PBL	Problembaserat lärande
REST API	Gränssnitt för tillämpningsprogram Representational State Transfer
SAREF	Referensontologi för smarta applikationer
SIEM	Säkerhetsinformation och händelseshantering
UPRES	Stadsplanerare med kompetens inom förnybar energi

Förteckning över tabeller

Tabell 1 Kunskapsluckor i cybersäkerhet i smarta nät i CC-RSG 6

1. Inledning

Den världsomspännande integreringen av elnät med informations- och kommunikationsteknikkapacitet har skapat ett behov för yrkesverksamma som har tvärvetenskaplig kunskap från både området smarta nät och området cybersäkerhet. Vårt projekt ”Cybersecurity curricula recommendations for Smart Grids” syftar till att underlätta anpassningen av de eftergymnasiala europeiska kursplanerna, eftersom de bland annat måste omfatta inlärningsmål i förhållande till cybersäkerhet. I denna rapport används de kunskapsluckor som identifierats i IO1 för att ge anvisningar till berörda aktörer, om hur den nuvarande och framtida arbetskraften ska utbildas på ett sätt som minskar dessa kompetensbrister.

1.1 Mål

Mer specifikt är målen för den aktuella rapporten följande:

- Analysera de utmaningar som industrin står inför när det gäller cybersäkerhet i smarta nät
- Skapa en plan för riskreducering på basis av de identifierade utmaningarna och kunskapsluckorna i WP1
- Analysera och föreslå lämpliga innovativa utbildningsmetoder för utbildningsanordnarna
- Ge rekommendationer till utbildningsanordnare, beslutsfattare och industrin

1.2 Dokumentets struktur

Dokumentet är uppbyggt på följande sätt:

I kapitel 2 identifieras de utmaningar som industrin står inför

I kapitel 3 beskrivs den föreslagna planen för riskreducering

I kapitel 4 presenteras en analys av traditionella och innovativa utbildningsmetoder med beaktande av exempel på tillämpning inom energisektorn och deras inverkan

Kapitel 5 innehåller rekommendationer på hög nivå till relevanta intressenter

Detta dokument kompletteras med en slutsats och en litteraturförteckning.

2. Utmaningar som industrin står inför

Energisystemet anses vara världens mest kritiska infrastruktur när det kommer till tillhandahållande av tjänster till andra sektorer. Ny industri 4.0 (den fjärde industriella revolutionen) som integrerar driftsteknik (OT) med informationsteknik (IT) använder och expanderar koncepten digitalisering, konnektivitet och automatisering, men intensifierar oron för cybersäkerhet för företag och systemoperatörer.

I detta avsnitt beskrivs analysen av de utmaningar som branschen står inför genom en litteraturöversikt och de kvalitativa intervjuer som genomfördes i WP1 i detta projekt, inom ramen för cybersäkerhet i smarta nät. Utmaningarna kommer att fungera som underlag för

att identifiera behovet av politiska förändringar och förändringar i utbildningar för att möjliggöra utvecklingen av en konkret strategi för cybersäkerhetsutbildning, för att möta industrins förväntningar på kompetenta cybersäkerhetsexperter.

2.1 Analys av branschintervjuer och litteraturöversikt

Utmaningarna identifierades genom en litteraturöversikt och intervjuer med branschexperter. Intervjuerna genomfördes som en del av WP1. Nedan följer de viktigaste utmaningar som identifierats med hjälp av litteraturöversikten:

1. Branschen behöver höga investeringskostnader för att skapa ett CPES med alla komponenter för att utbilda arbetskraften på ett adekvat sätt.
2. Befintliga standarder och vägledningsdokument omfattar inte de kritiska tillgångar som ska skyddas eller de rekommenderade motåtgärderna i tillräcklig utsträckning.
3. Certifieringssystem för cybersäkerhetsfärdigheter är inte allmänt antagna eller integrerade i kursplanerna.
4. Det är svårt att skapa en cybersäkerhetskultur hos arbetskraften då den inte har cybersäkerhet som ett relevant ansvarsområde i sin arbetsbeskrivning.
5. Brist på stark koppling mellan högskolor och industrin.
6. Tillsynsmyndigheterna betraktas ofta som brottsbekämpande organ snarare än som en central enhet för informationsutbyte och sammanförare av olika aktörer.

Nedan följer de viktigaste utmaningarna som identifierades under intervjuerna:

1. De intervjuade instämmer i slutsatserna i WP1, som visar att mänsklig säkerhet, organisations- och samhällssäkerhet inte behandlas i relevant litteratur.
2. Det saknas utbildningspersonal som kan lära ut både de tekniska och de icke-tekniska aspekterna av cybersäkerhet.
3. Utexaminerade saknar praktisk erfarenhet.
4. Utexaminerade saknar lednings- och kommunikationsfärdigheter.

2.2 Identifierade behov av politiska förändringar och förändringar i utbildningar

Utmaningarna används sedan för att identifiera behov i samband med politiska förändringar och utbildningsförändringar som anges nedan:

1. Tillhandahålla praktiska erfarenhets- och utbildningsprogram.
2. Förbättra det tvärfunktionella samarbetet (praktikprogram osv.).
3. Bygga en cybersäkerhetskultur.

3. Plan för reducering av kunskapsluckor

3.1 Riskreducerande åtgärder

I kapitel 3 utarbetas en plan för reducering av kunskapsluckor som beskriver riskreducerande åtgärder och som måste följas av de olika aktörerna. Ramverket Association for Computing Machinery (ACM) används som referens. Inom ACM-ramen kategoriseras de olika aspekterna av cybersäkerhet på första nivå i åtta stora grupper med namnet ”Kunskapsområden (KAs)” och på andra nivån innehåller varje KA flera ”Kunskapsenheter (KUs)”. För varje kunskapsenhet för var och ett av de viktigaste kunskapsområdena görs en bedömning av huruvida ändringen inom området främst bör inledas av utbildningsinstitutionerna eller branschen. I var och ett av fallen ges rekommendationer om en del viktiga åtgärder. I följande tabell (Tabell 1) presenteras nyckelåtgärderna

Riskreducerande åtgärder												
Kunskapsområde	**Kunskapsenhet**	**Kunskap om komponenter i energisystemet**	**Bedriva internationell forskning om**	**Kunskap om cybersäkerhet**	**Yrkesutbildning**	**Certifikat**	**Självlärande**	**Kunskap**	**Användbara mjuka**	**Lära sig ny teknik**	**Praktiska**	**Grundläggande verktyg för hotanalys**
Datasäkerhet	Kryptografi	X	X	X	X	X						
	Digital kriminalteknik						X	X	X	X	X	X
	Dataintegritet och autentisering	X	X	X	X	X						
	Åtkomstkontroll	X	X	X	X	X						
	Säkra kommunikationsprotokoll	X	X	X	X	X						
	Kryptoanalys						X	X	X	X	X	X
	Säkerhet för informationslagring						X	X	X	X	X	X
Programvarusäkerhet	Grundläggande principer	X	X	X	X	X						
Anslutningssäkerhet	Fysiska medier						X	X	X	X	X	X
	Gränssnitt och kopplingar för maskinvara och fysiska komponenter						X	X	X	X	X	X
	Arkitektur för distribuerade system	X	X	X	X	X						
	Nätverksarkitektur	X	X	X	X	X						
	Nätverksimplementeringar	X	X	X	X	X						
	Nätverkstjänster						X	X	X	X	X	X
	Nätverksförsvar						X	X	X	X	X	X
Systemsäkerhet	Systemhantering						X	X	X	X	X	X
	Systemåtkomst och systemkontroll						X	X	X	X	X	X
	Systemtestning	X	X	X	X	X						
	Vanlig systemarkitektur	X	X	X	X	X						
Mänsklig säkerhet	Identitetshantering	X	X	X	X	X						
	Social ingenjörskonst	X	X	X	X	X						
	Personlig efterlevnad av cybersäkerhetsregler/policy/etiska normer						X	X	X	X	X	X
	Medvetenhet och förståelse						X	X	X	X	X	X
	Sekretess och säkerhet för personuppgifter	X	X	X	X	X						
	Riskhantering						X	X	X	X	X	X

Organisations säkerhet	Säkerhetsstyrning och säkerhetsstrategi						X	X	X	X	X	X
	Systemadministration						X	X	X	X	X	X
	Säkerhetsfunktioner						X	X	X	X	X	X
	Cybersäkerhetsplanering						X	X	X	X	X	X
	Prestandaindikatorer för cybersäkerhet						X	X	X	X	X	X
	Verksamhetskontinuitet, återhämtning från katastrofer och incidenthantering						X	X	X	X	X	X
	Hantering av säkerhetsprogram						X	X	X	X	X	X
Samhällssäkerhet	Cyberlagstiftning	X	X	X	X	X						
	Cyberpolicy	X	X	X	X	X						
	Cyberetik	X	X	X	X	X						
Verktyg för cybersäkerhet	Översikt över cybersäkerhetsverktyg						X	X	X	X	X	X
	SIEM						X	X	X	X	X	X
	Användning av digitala tvillingar inom cybersäkerhet						X	X	X	X	X	X
Cybersäkerhet i energiförsörjningskedjan	Grundläggande principer för cybersäkerhet i energiförsörjningskedjan						X	X	X	X	X	X
	Verktyg för hantering av cybersäkerhet i energiförsörjningskedjan (inkl. verktyg för övervakning av energidomänkontroller)						X	X	X	X	X	X
	Övervakning av cybersäkerhet i energiförsörjningskedjan						X	X	X	X	X	X
	Hantering av cybersäkerhetshändelser i energiförsörjningskedjan						X	X	X	X	X	X

Tabell 1 Kunskapsluckor i cybersäkerhet i smarta nät i planen för riskreducering CC-RSG

3.2 Svårigheter med att integrera den föreslagna färdplanen i befintliga kursplaner

Kapitel 3 omfattar också de största svårigheterna med att integrera den föreslagna färdplanen i befintliga kursplaner. De är organiserade i fyra grupper, nämligen lärarnas svårigheter, problem med ämne/läroplan, studerandes svårigheter och organisationssvårigheter.

De största svårigheterna som lärarna stöter på har tagits fram och lyfts fram på följande sätt:

1. Byte av undervisningsmetod: Ändringar görs i undervisningsstil och undervisningsmetoder. Detta upplevs vanligtvis som något positivt när man befinner sig i utvecklingsfasen, men resultaten efter genomförandet kan variera drastiskt.
2. Otillräcklig undervisning i vissa ämnen i olika kursplaner: Fokus skiftar till vissa ämnen eller koncept och andra ämnen gås inte igenom ordentligt.
3. Ändringar i mål och studieplaner.
4. Anpassning av undervisningen innebär: Detta är kopplat till punkt 1 och har även koppling till organisationsändringarna i nästa avsnitt.
5. Utvärdering: Utvärderingskriterierna skulle behöva anpassas för att motsvara de nya förändringarna.
6. Innehållets struktur, tillgänglighet och tillämplighet.

För det andra, när det gäller ämnet, står integreringen av nya läroplaner eller ramar inför följande utmaningar [1] [2]:

1. Brist på inlärningsresurser: Resurser finns inte alltid tillgängliga för att täcka utvecklingen och nödvändiga förändringar
2. Underutvecklad personal: kopplat till föregående avsnitt, personalens kompetens påverkar direkt kvaliteten på kursplanerna. Därför kan nya mål inte uppnås förrän personalen är högt kvalificerad och redo att genomföra de utvecklade läroplanerna.
3. Hanteringsstöd.
4. Arbetsmängd: Nya implementeringar kan vara tidskrävande.
5. Beredskap att acceptera nya metoder.
6. Konsekvens: I mindre situationer kan integrering av kursplaner leda till oväntade negativa effekter.

För det tredje kan förändringarna i de sedan länge etablerade kursplanerna betraktas som avvikelser och inte som en kursändring, vilket skapar ett behov av att på ett adekvat sätt informera studerandena om behovet av att ändra kursplanen. De flesta förändringar kommer dock att vara förknippade med motstånd och kan leda till lågt förtroende för organisationen och dess trovärdighet. Slutligen, eftersom en uppgradering av kursplanerna kan kräva särskilda tjänster och utbildningsverktyg har inte alla organisationer råd med sådana uppgraderingar, vilket följaktligen skulle påverka tillhandahållandet av och kvaliteten på de uppgraderade kursplanerna.

Tidigare nämnda frågor är typiska svårigheter som måste övervägas samtidigt som befintliga kursplaner utvecklas. Som angett i [3] skulle det ändå vara till hjälp att särskilt fokusera på att skapa gränsöverskridande kursplaner med stor flexibilitet, och som därmed tjänar fler regioner och sektorer.

4. Förslag till utbildningsmetoder

I detta kapitel är vårt mål att hitta de utbildningsmetoder eller tekniker som kommer att vara till hjälp vid undervisning om cybersäkerhet i smarta nät. För detta syfte analyserar vi inledningsvis åtta utbildningsmetoder och gör sedan en översikt av deras användning på intresseområdena, antingen separat eller i kombination. Utifrån resultaten av översikten lägger vi fram förslag för olika undervisningssituationer.

4.1 En kort redogörelse för de metoder som har beaktats

Den traditionella inlärningsmodellen-Föreläsningsbaserat lärande

Föreläsningsbaserat lärande är den mest använda undervisningsmetoden på grund av dess anpassningspotential och det faktum att läraren har kontroll över vad som ska undervisas och på vilket sätt. Dess huvudsakliga nackdel är att studenterna kan använda sig av memorering i stället för förståelse för att klara examina. Den kombineras ofta med vissa former av erfarenhetsbaserat lärande såsom simuleringar och labbövningar.

Erfarenhetsbaserat lärande

Erfarenhetsbaserat lärande är en term som omfattar alla former av lärande där kunskap förvärvas genom erfarenhet. År 1984 beskrevs det av David Colb som en cykel som kan upprepas kontinuerligt där erfarenheten leder till bildandet av teorier som sedan kan användas för att skapa nya experiment och få mer erfarenhet.

Aktivt lärande

Aktivt lärande är också ett ganska brett begrepp och det bygger på att öka studerandenas engagemang genom deras deltagande på olika sätt. Under föreläsningen kan det t.ex. vara att skapa en konceptkarta, ställa frågor till lyssnarna, skriva en kort essä eller kamratundervisning.

Samarbetsinriktat lärande

Samarbetsinriktat lärande beskriver arbetet i en grupp där varje studerande inte bara avsätter tid för att utföra en del av gruppens arbete, utan också att varje studerande är ansvarig för gruppens prestationer och för hur effektivt kompetensfördelningen mellan gruppmedlemmarna fungerar.

Omvänt klassrum

I omvända klassrum förväntas studerandena ha studerat föreläsningsmaterialet på förhand. Materialet kan redan finnas som bok eller en serie videoklipp, men det kan också göras speciellt för kursen. Under föreläsningen kan läraren använda aktiva inlärningstekniker för att testa och fördjupa elevernas förståelse av kursmaterialet. En möjlig nackdel är att tillgången till elektroniska hjälpmedel skiljer sig mellan studerandena.

Forskningsbaserat lärande

Forskningsbaserat lärande liknar den vetenskapliga metoden mest. Dess faser inkluderar inriktning, konceptualisering, undersökning, slutsats och diskussion. Läraren kan ge mer eller mindre handledning och input beroende på studerandenas mognadsgrad.

Problembaserat lärande och projektbaserat lärande

Grunden för dessa två metoder är samarbetsinriktat lärande. I problembaserat lärande undersöker en grupp studerande ett olöst, verkligt problem och försöker hitta den lämpligaste lösningen som gruppen sedan presenterar för sina andra medstuderande. Projektbaserat

lärande har många likheter med problembaserat lärande, men det varar vanligtvis längre och lösningen är inte bara teoretisk utan har ett konkret och uttryckligt resultat som ett datorprogram eller en modell.

”Spelifiering” (eng. gamification)

I gamification används element och mekanismer som vanligtvis ingår i utformningen av ett spel (att klara nivåer, begränsad tid för att slutföra en uppgift och andra) för att öka studerandenas engagemang.

4.2 Exempel på användning och effekter inom området energisystem - Förslag

För att identifiera effekterna av användningen av de olika undervisningsmetoderna i cybersäkerhet för smarta nät genomförde vi en litteraturöversikt med 43 dokument. 21 av dem är skrivna av författare som använt några av de ovanstående metoderna för undervisning i en relativ kurs och resten är mer allmänna. Kommentarerna från litteraturöversikten presenteras nedan:

Begränsningar i användningen av aktiva inlärningstekniker:

Användningen av aktiva inlärningstekniker kräver inte bara mer personal, tid och resurser utan också att studerandegrupperna är homogena och redan har en miniminivå av kunskap i ämnet.

Användning av gamification vid universitet:

Gamification vid universitet kan ske i form av verkliga spel som Riskio, som är ett brädspel och kan användas för studerande eller anställda inom industrin, som inte har teknisk bakgrund.

Capture the flag och Hacker dagar-evenemang:

Capture The Flag-tävlingar är en form av spel och de har inslag från erfarenhetslärande och samarbetslärande. I CTF-tävlingar tävlar spelarna om att upptäcka systemets sårbarhet (antingen i maskinvara eller programvara) och upptäcka en nyckel som ligger dold i systemet av organisatörerna (flaggan). Det kan ske i form av två team som spelar mot varandra eller där varje tävlingsteam försöker hacka organisatörernas system. CTF-tävlingar är lämpliga för utbildning i attacker som sker inom en kort tidsperiod. Särskild omsorg bör ägnas åt att underlätta för nybörjare. CTF-tävlingar kan vara en del av en karriärdag där representanter från industrin deltar. Några av studenterna kan vara det organiserande teamet under evenemanget, vilket ger dem mycket värdefulla färdigheter för branschen.

Användning av gamification i industrin

Gamification i industrin har framgångsrikt använts av personal som inte har teknisk bakgrund, för att förbättra förebyggandet av en nätfiskeattack. Det är viktigt att notera att i det företag där uppgifterna samlades in så hade gruppen som tidigare utbildats för att förhindra nätfiskeattacker via e-post samma resultat som kontrollgruppen utan någon som helst utbildning.

Användning av demonstrationer

Demonstrationer kan användas både för studerande och anställda. I ett exempel används Shodan, som kan hitta olika enheter som är anslutna till internet utan autentiseringsuppgifter

eller med standardinloggningsuppgifter. Studerande och anställda kan inse den potentiella effekten av sitt beteende när det gäller att upprätthålla goda cybersäkerhetsvanor.

Användning av projektbaserat lärande:
Projektbaserat lärande är den metod som oftast används i spel. Genom resultat från enkäter har det hävdats att när studerande undervisas i en kurs med hjälp av praktisk teknik, sker en betydande förbättring av andelen som hålls kvar några veckor efter kursens slut. [4]

Virtuella laboratorier och fjärråtkomst:
Trenden att använda virtuella laboratorier som inleddes 2010 har stärkts på grund av covid-19-pandemin. Statistiska resultat i [5] visar att studenterna behöver använda laboratorierna under de timmar som de vanligtvis är stängda för allmänheten, men för att ställa i ordning labbet krävs det ytterligare arbetstimmar för labbets tekniska stöd.

Användning av testbeds för att undervisa om cybersäkerhet:
Det mest fullständiga och realistiska sättet att studera effekterna och återhämtningsprocessen av en cyberattack är att använda en testbed. I en testbed simuleras systemet mycket detaljerat. Detaljnivån ökar när fler komponenter i det simulerade systemet representeras av maskinvara snarare än av programvara och när fler komponenter läggs till i samma system. Exempel på användning av realtidssimulatorer för att studera cyberattacker finns i [6], [7].

5. Rekommendationer

Den sista delen av rapporten består av rekommendationer på hög nivå, organiserade enligt de intressenter som de riktar sig till, nämligen universitet, yrkesutbildningar, industri och beslutsfattare. Rekommendationerna är resultatet av en sammanfattning av många (huvudsakligen europeiska) dokument, en rapport från en arbetsgrupp, resultat från ett projekt och övrigt. I nästa punkt presenterar vi kort rekommendationerna för de olika intressenterna.

5.1.1 Universitet:

- Skapa ett observatorium för att kontinuerligt övervaka de nya och pågående forskningsresultaten på det kombinerade området.
- Skapa en databas över experter och forskare tillsammans med deras verksamhetsområden, för att bidra till skapandet av gemensamma magisterprogram som för närvarande saknas i Erasmus Mundus inom området i fråga.
- Fortsatt och utökad användning av europeisk meritöverföring i enlighet med Bolognaprocessen. Harmoniseringen av de europeiska ackrediteringssystemen är en förutsättning för gemensamma kursplaner.
- Övervinna hindret brist på utrustning, genom att skapa en inventering av infrastrukturen enligt exemplet i ERIGRID 2.0-projektet.
- Skapa en kursmodulsdatabas för att kunna dela med sig av utformning av kurser och bästa praxis för att påskynda antagandet av relevanta läranderesultat.
- Universiteten bör rikta in sig mer på att skapa T-formade ingenjörer som har både ett brett spektrum av allmänna kunskaper (horisontella stapeln i T:t) och ett högspecialiserat område (vertikala stapeln i T:t).
- De allmänna kunskaperna bör omfatta de etiska, sociala och rättsliga aspekter som kan förbises i STEM-program (Naturvetenskap Teknik Ingenjörsvetenskap Matematik).

5.1.2 Yrkesutbildningar

- Skapa ett projekt som UP-RES [8] som också är ett exempel på ett projekt med två områden som skulle kombineras, nämligen förnybara energikällor och stadsplanering. Resultaten kommer att bli utbildade yrkesverksamma, bästa praxis för utbildning, utbildningsmaterial och eventuellt samarbete mellan universitet.
- Anordnare av C-yrkesutbildning bör formulera kurser och onlineutbildningsmoduler med mycket specifikt fokus på hur man genomför ett kommunikationsprotokoll i en äldre enhet. Detta kan utgöra ett MicroMaster-program som motsvarar en magisterstermin.
- Vissa kurser kan fungera som förberedelser för erhållande av ett certifikat som i allmänhet bidrar till att öka chansen att bli anställd för den examinerade studerande, där certifikat har en särskild inverkan vid urvalet.

5.1.3 Industri:

De anställdas kompetens i cybersäkerhet kan analyseras i två breda kategorier. För det första, färdigheter och kunskaper som är tekniska och relevanta för företagets produkt eller tjänst, och för det andra, medvetenheten om hur den mänskliga faktorn (både arbetstagaren och kunden) kan påverka systemets säkerhet.

- Följande ämnen och principer bör läras ut till de anställda:
  - Om man jämför en delad databasmodell och en meddelandebaserad modell är den meddelandebaserade modellen fördelaktig. [9]
  - Referensontologi för smarta applikationer-modellen (SAREF) som analyserar enheter i sakernas internet i hemmen i sina byggstenar och relationerna mellan dem.
  - Handledning om hur du aktiverar kontinuerlig uppdatering och uppgradering av komponenterna.
  - Tillämpning av principerna om **security-by-design** och **security-by-default**.
  - Relevant lagstiftning. En bra översikt fram till mitten av 2017 finns i [10] och på senare tid har dataskyddsförordningen och NIS 2.0-direktivet har lagts till.

De tre punkter som skiljer energisektorns cybersäkerhetsområde från cybersäkerhetsområdet i allmänhet är [11] användningen av äldre utrustning, förekomsten av följdefterverkningar på grund av den höga sammankopplingen mellan de europeiska näten och kraven på realtidsinformation, vilket innebär att vissa åtgärder i ett energinät måste ske mycket snabbt och att säkerhetsprotokollen måste väljas i enlighet med detta. För var och en av dessa tre sektorer rekommenderas undervisning i följande principer och bästa praxis:

Äldre utrustning: Systematisk hantering av uppdateringar och regelbunden riskanalys med inriktning på äldre enheter.

Följdefterverkningar: Klassificering av tillgångar och identifiering av kritiska knutpunkter för att undvika att ha en enda felkritisk systemdel.

Realtidskrav: Uppdelning av nätverk

- Rekommendationer som är relevanta för den mänskliga faktorn i cybersäkerhet
  - Företagen bör anordna möten där de anställdas kompetens mäts, och kvaliteten på de beslut de fattar som är relevanta för cybersäkerheten.
  - Cheferna bör få ytterligare utbildning om hur deras beteende påverkar de personer de leder [12], till exempel för att klargöra att säkerhet inte bör försummas till förmån för produktiviteten.

- Användning av ENISA-verktyget ”Good practices for IoT and Smart Infrastructures Tool”, som kan vara till hjälp särskilt för små företag.

5.1.4 Beslutsfattare:

- Man bör undersöka hur medlemsstaterna genomför NIS 2.0-direktivet, som kan fungera som referensmodell. Det är viktigt att det finns en NIS-myndighet och en insatsstyrka vid datorsäkerhetsincidenser (Computer Security Incident Response Team). Utöver att identifiera leverantörer av samhällsviktiga tjänster i enlighet med NIS-direktivet bör industrier göra en förteckning av sina tillgångar, verksamheter och kritiska infrastrukturkomponenter.
- Skapa en databas där operatörer och andra parter kan utbyta detaljerad information om incidenter och tidiga varningar om attacker och överträdelser.
- Ett system för minimisäkerhet bör fastställas och strikt följas.
- De plattformar som används bör antecknas och kriterierna för plattformarnas driftskompatibilitet bör definieras i enlighet med metoderna för företagsarkitekturs rekommendationer [13].
- Skapa en databas där industrin kontinuerligt kan övervaka de kompetenser som behövs.
- Skapa ett gemensamt språk som hjälper till att avlägsna kommunikationshinder, särskilt mellan chefer och teknisk personal.
- Användning av befintliga tillgängliga sätt att kommunicera t.ex. MQQT och REST API, rekommenderas starkt, istället för att använda egna lösningar.
- Utveckla de nya uppgiftsrollerna, kanske genom att använda den harmoniserade modellen för elmarknaden.
- Tillämpa standarderna i Common Information Model för systemansvariga för överföringssystem (TSO) och systemansvariga för distributionssystem

5.1.5 Rekommendationer om hur samarbete mellan berörda parter kan främjas:

Som det har sagts tidigare behöver utbildningar i cybersäkerhet i energisystem samordnade åtgärder från många berörda parter, och det är ett område som förändras i snabb takt. Vi rekommenderar att man inrättar ett högnivåforum för dialog som sammanträder årligen eller vartannat år, med representanter i form av berörda beslutsfattare, systemansvariga för distributionssystem, systemansvariga för överföringssystem, universitet och yrkesutbildningsinstitutioner, för att utbyta information om pågående och planerad verksamhet på området.

En annan möjlighet att upprätthålla kommunikationen är att anordna stora evenemang vid utbildningsinstitutionerna med bidrag från industrin, som skulle kunna tillhandahålla utrustningen. Samtidigt kunde dessa evenemang fungera som karriärdagar och öka chansen att studerande väljer cybersäkerhet som en framtida karriär.

6. Slutsatser

I rapporten ovan syftade vi till att förstå på vilka områden utbildning i cybersäkerhet i smarta nät saknas och föreslå effektiva utbildningsmetoder och andra rekommendationer på hög nivå för att bidra till att förbättra utbildningen på detta område. Analysen gjordes genom omfattande litteraturöversikt, intervjuer med företrädare för industrin och en särskild workshop som genomfördes inom ramen för CC-RSG i maj 2021.

De utmaningar som branschen står inför är främst relevanta för unga akademiker som inte fått tillräcklig utbildning i praktiska situationer som liknar dem som kommer att uppstå under arbetslivet, eller tillräcklig utbildning i lednings- och kommunikationsfrågor.

När det gäller utbildningsmetoderna verkar gamification vara den mest lovande inom området cybersäkerhet. Den kan användas både för utbildning av personal som arbetar inom energisystemindustrin, men som saknar teknisk bakgrund, för att skaffa sig kunskap om cybersäkerhet, och den kan också användas för utbildning av teknisk personal, särskilt för att hjälpa dem att få praktisk erfarenhet.

Projektbaserat lärande har visat sig förbättra andelen som hålls kvar efter några veckor, men eftersom alla metoder för aktivt lärande är föremål för vissa begränsningar, varav den viktigaste är att de kan tillämpas på studenter som redan har en viss grad av självständighet i ämnet i fråga och att studerandeteamen måste vara homogena.

Det aktuella ämnet är mycket nära kopplat till hårdvara, så det är mycket viktigt att utveckla sätt för att så många intressenter som möjligt kan få tillgång till relevant utrustning. Detta kan göras på många sätt, som att utöka användningen av fjärråtkomst till testbeds i forskningscentrum eller utbildningsinstitut, organisera ett sätt att dela infrastrukturen (EU ERIGRID 2.0-projektet som exempel) eller bjuda in branschen att delta i relevanta universitetskurser. Utrustning kan innebära både allmän maskinvaruutrustning som datorer och specialutrustning som PMU, RTU:er, Realtidssimulatorer osv.

Rekommendationerna till intressenterna berör i stor utsträckning sätt att kommunicera och kartlägga tillgängliga resurser (yrkesverksamma, bästa praxis, infrastruktur). Kartläggning är grunden för att utveckla effektiva sätt att slå samman tillgängliga resurser, som att skapa gemensamma examina, ett system för tidig varning för cybersäkerhetsincidenter och andra.

Bortsett från de tidigare rekommendationerna har vi även inkluderat en kortfattad analys av den kunskap som industrin bör försöka undervisa rörande sina tekniska saker och hur cybersäkerheten i energisystem skiljer sig från cybersäkerhetsområdet i allmänhet.

För beslutsfattare är den viktigaste uppgiften att skapa kommunikationsvägar, som ett gemensamt språk för chefer och tekniker, den europeiska kompetensramen för cybersäkerhet som förutses av ENISA (även om det inte är specifikt för energisystem) och direktiven och förordningarna för att minimera användningen av äganderättsligt skyddade lösningar.

Analysen ovan visar fördelarna med att utveckla testbeds i realtid som gör modeller av både energisystemet och kommunikationsnätet. Den här modellen kan sedan användas för att analysera möjliga attacker (kanske i kombination med mänskliga fel) under de unika förhållanden och krav som smarta nät (och energisystem i allmänhet) använder.

7. Litteraturförteckning

[1] R. R. &. S. S. Hipkins, ”Curriculum changes, priority 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. T. T. Nyamkhuu, ”Challenges in integrating 21st century skills into education systems,” 2019. [Online]. Tillgänglig: 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. A. a. S. B. Kara Nancea, ”Virtual Laboratory Environments: Methodologies for Educating Cybersecurity Researchers,” *Methodological Innovations Online,* vol. 4, no. 3, pp. 3-14, 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 of Cyber-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,” [Online]. Tillgänglig: 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.