Στρατηγική για την εκπαίδευση για την κυβερνοασφάλεια στα έξυπνα δίκτυα (Συνοπτική έκθεση)

Συντάκτες:

Μαρία Βάλλιου, Αλέξανδρος Χρόνης, Πάνος Κοτσαμπόπουλος, Bahaa Eltahawy, Tero Vartiainen, Mike Mekkanen, Andrejs Romānovs, Jana Bikovska, Jānis Pekša, Rūta Pirta-Dreimane, Jirapa Kamsamrong, Bjoern Siemers

Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)
Erasmus+ Strategic Partnership Project

Intellectual Output 2
Απρίλιος 2022

Αξιολογητές: Φοίβος Παλαιογιάννης και Lars Fischer
Συντονισμός: Πανεπιστήμιο της Βάασα

Συνεργάτες: OFFIS, Τεχνικό Πανεπιστήμιο Ρίγας, Εθνικό Μετσόβιο Πολυτεχνείο

Το παρόν έργο έχει χρηματοδοτηθεί από το Πρόγραμμα Erasmus+ δυνάμει της Σύμβασης επιχορήγησης με Αρ. 2020-1-FI01-KA203-066624.

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου, το οποίο αντικατοπτρίζει αποκλειστικά τις απόψεις των συντακτών και η Επιτροπή δεν θα θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται στην παρούσα.

Vaasan yliopisto
UNIVERSITY OF VAASA

National Technical University of Athens

RIGA TECHNICAL UNIVERSITY

CARL VON OSSIETZKY universität OLDENBURG

Περιεχόμενα

1. Εισαγωγή 3
1.1 Στόχοι 3
1.2 Διάρθρωση του εγγράφου 3
2. Προκλήσεις που αντιμετωπίζει η βιομηχανία 4
2.1 Ανάλυση των συνεντεύξεων και της βιβλιογραφικής ανασκόπησης 4
2.2 Ανάγκες που έχουν προσδιοριστεί ως προς τις αλλαγές στην εκπαιδευτική πολιτική 5
3. Σχέδιο αντιμετώπισης των ελλείψεων δεξιοτήτων 5
3.1 Ενέργειες αντιμετώπισης 5
3.2 Δυσκολία της ενσωμάτωσης της προτεινόμενης προσέγγισης στα υφιστάμενα προγράμματα σπουδών 8
4. Προτάσεις εκπαιδευτικών μεθοδολογιών 9
4.1 Μια σύντομη παρουσίαση των μεθόδων που εξετάστηκαν 10
4.2 Παραδείγματα χρήσης και αντικτύπου των μεθόδων στον τομέα των συστημάτων ενέργειας - Προτάσεις 11
5. Προτάσεις 12
5.1 Πανεπιστήμια 12
5.2 Πάροχοι επαγγελματικής κατάρτισης (ΕΠΑΛ/ΙΕΚ) 13
5.3 Βιομηχανία 13
5.4 Αρμόδιοι χάραξης πολιτικής 14
6. Συμπεράσματα 15
7. Βιβλιογραφία 17

Ορισμοί, ακρωνύμια και συντομογραφίες

Συντομογραφία	Σημασία
ACM	Association for Computing Machinery (Σύλλογος Μηχανημάτων Υπολογισμού)
CPES	Cyber Physical Energy System (Κυβερνο-φυσικό σύστημα ενέργειας)
CSIRT	Computer Security Incident Response Team (Ομάδα παρέμβασης σε συμβάντα που αφορούν την ασφάλεια των υπολογιστών)
CTF	Capture the flag (Προκλήσεις τύπου «Capture the flag»
ENISA	European Network and Information Security Agency (Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών)
GDPR	General Data Protection Regulation (Γενικός Κανονισμός για την Προστασία των Δεδομένων, ΓΚΠΔ)
IT	Information Technology (Τεχνολογία πληροφοριών)
KA	Knowledge Area (Γνωστική περιοχή)
KU	Knowledge Unit (Γνωστική μονάδα)
MQTT	MQ Telemetry Transport (Πρωτόκολλο ανταλλαγής μηνυμάτων MQTT)

NIS	Network and Information Systems (Συστήματα δικτύου και πληροφοριών)
OT	Operational Technology (Λειτουργική τεχνολογία)
PBL	Problem based learning (Μάθηση με βάση το πρόβλημα)
REST API	Representational State Transfer Application Programming Interface (Διασύνδεση προγραμματισμού εφαρμογών σε στυλ αρχιτεκτονικής «Κατάσταση Παραστατικής Μεταφοράς»)
SAREF	Smart Applications Reference Ontology (Οντολογία αναφοράς έξυπνων εφαρμογών)
SIEM	Security Information and Event Management (Διαχείριση ασφάλειας πληροφοριών και συμβάντων)
UPRES	Urban planners with Renewable Energy Skills (Πολεοδόμοι με δεξιότητες ως προς την ανανεώσιμη ενέργεια)

Κατάλογος πινάκων

Πίνακας 1 Σχέδιο αντιμετώπισης των ελλείψεων δεξιοτήτων στον τομέα της κυβερνοασφάλειας στα έξυπνα δίκτυα 8

1. Εισαγωγή

Η ενσωμάτωση των δικτύων επικοινωνίας και πληροφοριών στα ηλεκτρικά δίκτυα σε όλον τον κόσμο έχει δημιουργήσει την ανάγκη για επαγγελματίες που διαθέτουν διεπιστημονικές γνώσεις τόσο στο πεδίο των έξυπνων δικτύων όσο και στο πεδίο της κυβερνοασφάλειας. Το έργο μας με τίτλο «Προτάσεις για προγράμματα σπουδών κυβερνοασφάλειας για έξυπνα δίκτυα» (Cybersecurity Curricula Recommendations for Smart Grids-CC-RSG) έχει στόχο να διευκολύνει την προσαρμογή των προγραμμάτων σπουδών στη μεταδευτεροβάθμια εκπαίδευση στην Ευρώπη, καθώς πρέπει να συμπεριλαμβάνουν, μεταξύ άλλων, εκπαιδευτικούς στόχους σχετικούς με την κυβερνοασφάλεια. Σε αυτή την έκθεση οι ελλείψεις δεξιοτήτων, που προσδιορίζονται στο Πακέτο Εργασίας 1 του έργου (WP1), χρησιμοποιούνται προκειμένου να παράσχουν κατευθύνσεις στα ενδιαφερόμενα μέρη σχετικά με τον τρόπο κατάρτισης του υφιστάμενου και του μελλοντικού ανθρώπινου δυναμικού, έτσι ώστε να μετριάζονται οι εν λόγω ελλείψεις στις δεξιότητες.

1.1 Στόχοι

Πιο συγκεκριμένα, οι στόχοι της παρούσας έκθεσης είναι οι εξής:

- Ανάλυση των προκλήσεων που αντιμετωπίζει η βιομηχανία στο πεδίο της κυβερνοασφάλειας στα έξυπνα δίκτυα
- Κατάρτιση ενός σχεδίου αντιμετώπισης με βάση τις προκλήσεις και τις ελλείψεις ως προς τις δεξιότητες που προσδιορίστηκαν στο Πακέτο Εργασίας 1
- Ανάλυση και υπόδειξη κατάλληλων καινοτόμων μεθοδολογιών εκπαίδευσης στους παρόχους εκπαίδευσης
- Παροχή προτάσεων στους παρόχους εκπαίδευσης, στους αρμόδιους χάραξης πολιτικής και στην βιομηχανία

1.2 Διάρθρωση του εγγράφου

Το έγγραφο έχει διαρθρωθεί ως εξής:

Στο 2ο Κεφάλαιο προσδιορίζονται οι προκλήσεις που αντιμετωπίζει η βιομηχανία

Στο 3ο Κεφάλαιο περιγράφεται το προτεινόμενο σχέδιο αντιμετώπισης των ελλείψεων δεξιοτήτων

Στο 4ο Κεφάλαιο παρουσιάζεται μια ανάλυση των παραδοσιακών και των καινοτόμων εκπαιδευτικών μεθόδων λαμβάνοντας υπ' όψιν τα παραδείγματα εφαρμογής τους στο πεδίο του τομέα ενέργειας και του αντικτύπου τους

Στο 5ο Κεφάλαιο παρέχονται προτάσεις σε αφηρημένο επίπεδο στα σχετικά ενδιαφερόμενα μέρη

Το παρόν έγγραφο ολοκληρώνεται με τα συμπεράσματα και τη βιβλιογραφία.

2. Προκλήσεις που αντιμετωπίζει η βιομηχανία

Το σύστημα ενέργειας θεωρείται η πιο σημαντική υποδομή σε όλο τον κόσμο, καθώς παρέχει υπηρεσίες σε όλους τους άλλους τομείς. Η αναδυόμενη Τέταρτη βιομηχανική επανάσταση (Industry 4.0), που συνδυάζει τη επιχειρησιακή τεχνολογία (Operational Technology - OT) με την τεχνολογία πληροφοριών (Information Technology - IT), χρησιμοποιεί και διευρύνει τις έννοιες της ψηφιοποίησης, της συνδεσιμότητας και του αυτοματισμού αλλά εντείνει τον προβληματισμό των επιχειρήσεων και των διαχειριστών συστημάτων σε ό,τι αφορά την κυβερνοασφάλεια.

Η παρούσα ενότητα περιλαμβάνει την ανάλυση των προκλήσεων που αντιμετωπίζει η βιομηχανία όπως προσδιορίζονται από μια βιβλιογραφική ανασκόπηση, καθώς και μέσω συνεντεύξεων που διεξήχθησαν στο πλαίσιο του Πακέτου Εργασίας 1 του παρόντος έργου σε εκπροσώπους της βιομηχανίας του κλάδου. Οι προκλήσεις θα μας δώσουν πληροφορίες για τον προσδιορισμό των αναγκών για αλλαγές στην πολιτική και στην εκπαίδευση, προκειμένου να προωθηθεί η χάραξη μιας απτής στρατηγικής για την εκπαίδευση στην κυβερνοασφάλεια η οποία θα ανταποκρίνεται στην προσδοκία της βιομηχανίας για να εκπαιδευτούν οι μελλοντικοί επαγγελματίες.

2.1 Ανάλυση των συνεντεύξεων και της βιβλιογραφικής ανασκόπησης

Οι προκλήσεις προσδιορίστηκαν μέσα από τη βιβλιογραφική ανασκόπηση και τις συνεντεύξεις με ειδικούς της βιομηχανίας. Παρακάτω αναφέρονται οι κύριες προκλήσεις που προσδιορίστηκαν μέσω της βιβλιογραφικής ανασκόπησης:

1. Η επένδυση για τη δημιουργία κυβερνο-φυσικού συστήματος ενέργειας (Cyber Physical Energy System, CPES) με όλα τα στοιχεία για την επαρκή κατάρτιση του ανθρώπινου δυναμικού έχει ιδιαίτερα υψηλό κόστος.
2. Τα υφιστάμενα πρότυπα και τα έγγραφα καθοδήγησης δεν καλύπτουν τις κρίσιμες υποδομές ούτε προτείνουν επαρκή μέτρα προστασίας
3. Τα προγράμματα πιστοποίησης για τις δεξιότητες κυβερνοασφάλειας δεν υιοθετούνται ευρέως ούτε ενσωματώνονται στα προγράμματα σπουδών
4. Είναι δύσκολο να καλλιεργηθεί μια φιλοσοφία κυβερνοασφάλειας σε ανθρώπινο δυναμικό, το οποίο δεν διαθέτει τις σχετικές αρμοδιότητες στην περιγραφή της θέσης εργασίας του
5. Υπάρχει έλλειψη ισχυρής διασύνδεσης ανάμεσα στα Ανώτερα Εκπαιδευτικά Ιδρύματα (ΑΕΙ) και στην βιομηχανία
6. Συχνά, οι ρυθμιστικές αρχές εκλαμβάνονται ως φορείς επιβολής του νόμου αντί ως μια κεντρική οντότητα για την ανταλλαγή πληροφοριών και τη δημιουργία σχέσεων ανάμεσα στους ποικίλους συντελεστές.

Παρακάτω παρουσιάζονται οι κύριες προκλήσεις που προσδιορίστηκαν μέσω των συνεντεύξεων:

1. οι ερωτώμενοι συμφωνούν με τα πορίσματα του Πακέτου Εργασίας 1 που δείχνουν ότι η Οργανωτική Ασφάλεια και η Ασφάλεια του Ατόμου και της Κοινωνίας (Human, Societal and Organizational security) δεν καλύπτονται επαρκώς στη σχετική βιβλιογραφία,
2. υπάρχει έλλειψη εκπαιδευτικών που μπορούν να διδάξουν τόσο τις τεχνικές όσο και τις μη τεχνικές πτυχές της κυβερνοασφάλειας,
3. οι απόφοιτοι δεν διαθέτουν πρακτική εμπειρία,
4. οι απόφοιτοι δεν διαθέτουν διοικητικές και επικοινωνιακές δεξιότητες.

2.2 Ανάγκες που έχουν προσδιοριστεί ως προς τις αλλαγές στην εκπαιδευτική πολιτική

Στη συνέχεια, οι προκλήσεις χρησιμοποιούνται για τον προσδιορισμό των αναγκών για αλλαγές στην εκπαιδευτική πολιτική, που παρατίθενται παρακάτω:

1. Παροχή πρακτικής εμπειρίας και προγραμμάτων κατάρτισης
2. Ενθάρρυνση της διατμηματικής συνεργασίας (προγράμματα πρακτικής άσκησης κ.λπ.)
3. Καλλιέργεια κουλτούρας σχετικά με την κυβερνοασφάλεια

3. Σχέδιο αντιμετώπισης των ελλείψεων δεξιοτήτων

3.1 Ενέργειες αντιμετώπισης

Στο 3ο Κεφάλαιο παρουσιάζεται ένα σχέδιο αντιμετώπισης των ελλείψεων δεξιοτήτων που περιέχει τις ενέργειες αντιμετώπισης στις οποίες πρέπει να προβούν τα διάφορα ενδιαφερόμενα μέρη. Το πλαίσιο του Συλλόγου Μηχανημάτων Υπολογισμού (ACM) χρησιμοποιείται ως αναφορά. Το πλαίσιο ACM κατηγοριοποιεί σε πρώτο επίπεδο τις διάφορες πτυχές της κυβερνοασφάλειας σε οκτώ μεγάλες ομάδες (Γνωστικές περιοχές - Knowledge Areas-KA) και σε δεύτερο επίπεδο κάθε KA περιλαμβάνει πολλές «Γνωστικές μονάδες» (Knowledge Units-KU).

Για κάθε γνωστική μονάδα και για κάθε γνωστική περιοχή διεξάγεται μια αξιολόγηση σχετικά με το εάν η αλλαγή που την αφορά θα πρέπει να ξεκινήσει κυρίως από τα εκπαιδευτικά ιδρύματα ή από την βιομηχανία. Σε κάθε περίπτωση συνιστώνται μερικές ενέργειες-κλειδιά οι οποίες παρουσιάζονται στον παρακάτω πίνακα:

Ενέργειες αντιμετώπισης												
Γνωστική περιοχή (Knowledge Area)	**Γνωστική μονάδα (Knowledge Unit)**	**Γνώση του στοιχείου του συστήματος ενέργειας**	**Διεξαγωγή έρευνας για την κυβερνοασφάλεια**	**Γνώση της ασφάλειας δικτύου**	**Επαγγελματική κατάρτιση**	**Πιστοποιητικά**	**Αυτοδιδασκαλία**	**Απόκτηση γνώσεων**	**Δεξιότητες επικοινωνίας (soft skills)**	**Εκμάθηση νέων τεχνολογιών**	**Περιπτώσεις πρακτικής εφαρμογής**	**Βασικά εργαλεία για την ανάλυση απειλών**
Ασφάλεια δεδομένων	Κρυπτογράφηση	X	X	X	X	X						
	Ψηφιακή εγκληματολογία						X	X	X	X	X	X
	Ακεραιότητα και έλεγχος ταυτότητας δεδομένων	X	X	X	X	X						
	Έλεγχος πρόσβασης	X	X	X	X	X						
	Πρωτόκολλα ασφαλούς επικοινωνίας	X	X	X	X	X						
	Κρυπτανάλυση						X	X	X	X	X	X
	Ασφάλεια αποθήκευσης πληροφοριών						X	X	X	X	X	X
Ασφάλεια λογισμικού	Θεμελιώδεις αρχές	X	X	X	X	X						
Ασφάλεια σύνδεσης	Φυσικά μέσα						X	X	X	X	X	X
	Διασυνδέσεις και συνδέσεις υλικού και φυσικών στοιχειών						X	X	X	X	X	X
	Αρχιτεκτονική κατανεμημένων συστημάτων	X	X	X	X	X						
	Αρχιτεκτονική δικτύου	X	X	X	X	X						
	Εφαρμογές δικτύου	X	X	X	X	X						
	Υπηρεσίες δικτύου						X	X	X	X	X	X
	Άμυνα δικτύου						X	X	X	X	X	X
Ασφάλεια συστήματος	Διαχείριση συστήματος						X	X	X	X	X	X
	Πρόσβαση και έλεγχος συστήματος						X	X	X	X	X	X
	Δοκιμή συστήματος	X	X	X	X	X						
	Κοινές αρχιτεκτονικές συστημάτων	X	X	X	X	X						
Ανθρώπινη ασφάλεια	Διαχείριση ταυτότητας	X	X	X	X	X						
	Κοινωνική μηχανική	X	X	X	X	X						
	Συμμόρφωση σε προσωπικό επίπεδο με τους κανόνες/την πολιτική/τους κανόνες						X	X	X	X	X	X

Ενέργειες αντιμετώπισης												
Γνωστική περιοχή (Knowledge Area)	**Γνωστική μονάδα (Knowledge Unit)**	**Γνώση του στοιχείου του συστήματος ενέργειας**	**Διεξαγωγή έρευνας για την κυβερνοασφάλεια**	**Γνώση της ασφάλειας δικτύου**	**Επαγγελματική κατάρτιση**	**Πιστοποιητικά**	**Αυτοδιδασκαλία**	**Απόκτηση γνώσεων**	**Δεξιότητες επικοινωνίας (soft skills)**	**Εκμάθηση νέων τεχνολογιών**	**Περιπτώσεις πρακτικής εφαρμογής**	**Βασικά εργαλεία για την ανάλυση απειλών**
	δεοντολογίας για την κυβερνοασφάλεια											
	Ευαισθητοποίηση και κατανόηση						X	X	X	X	X	X
	Απόρρητο και ασφάλεια δεδομένων προσωπικού χαρακτήρα	X	X	X	X	X						
Επιχειρησιακή ασφάλεια	Διαχείριση κινδύνων						X	X	X	X	X	X
	Διακυβέρνηση και πολιτική για την ασφάλεια						X	X	X	X	X	X
	Διαχείριση συστημάτων						X	X	X	X	X	X
	Δυνατότητες ασφάλειας						X	X	X	X	X	X
	Σχεδιασμός κυβερνοασφάλειας						X	X	X	X	X	X
	Δείκτες απόδοσης κυβερνοασφάλειας						X	X	X	X	X	X
	Επιχειρησιακή συνέχεια, αποκατάσταση λειτουργίας μετά από καταστροφή και διαχείριση συμβάντων						X	X	X	X	X	X
	Διαχείριση προγράμματος ασφάλειας						X	X	X	X	X	X
Κοινωνική ασφάλεια	Δίκαιο κυβερνοχώρου	X	X	X	X	X						
	Πολιτική κυβερνοχώρου	X	X	X	X	X						
	Δεοντολογία κυβερνοχώρου	X	X	X	X	X						
Εργαλεία για την κυβερνοασφάλεια	Επισκόπηση των εργαλείων για την κυβερνοασφάλεια						X	X	X	X	X	X
	SIEM						X	X	X	X	X	X
	Χρήση ψηφιακών διδύμων στην κυβερνοασφάλεια						X	X	X	X	X	X

Ενέργειες αντιμετώπισης												
Γνωστική περιοχή (Knowledge Area)	**Γνωστική μονάδα (Knowledge Unit)**	**Γνώση του στοιχείου του συστήματος ενέργειας**	**Διεξαγωγή έρευνας για την κυβερνοασφάλεια**	**Γνώση της ασφάλειας δικτύου**	**Επαγγελματική κατάρτιση**	**Πιστοποιητικά**	**Αυτοδιδασκαλία**	**Απόκτηση γνώσεων**	**Δεξιότητες επικοινωνίας (soft skills)**	**Εκμάθηση νέων τεχνολογιών**	**Περιπτώσεις πρακτικής εφαρμογής**	**Βασικά εργαλεία για την ανάλυση απειλών**
Κυβερνοασφάλεια στην εφοδιαστική αλυσίδα ενέργειας	Θεμελιώδη στοιχεία για την κυβερνοασφάλεια στην εφοδιαστική αλυσίδα ενέργειας						X	X	X	X	X	X
	Εργαλεία διαχείρισης της κυβερνοασφάλειας στην εφοδιαστική αλυσίδα ενέργειας (συμπ. των εργαλείων παρακολούθησης των ελεγκτών τομέα ενέργειας)						X	X	X	X	X	X
	Παρακολούθηση της κυβερνοασφάλειας στην εφοδιαστική αλυσίδα ενέργειας						X	X	X	X	X	X
	Διαχείριση συμβάντων κυβερνοασφάλειας στην εφοδιαστική αλυσίδα ενέργειας						X	X	X	X	X	X

Πίνακας 1 Σχέδιο αντιμετώπισης των ελλείψεων δεξιοτήτων στον τομέα της κυβερνοασφάλειας στα έξυπνα δίκτυα

3.2 Δυσκολία της ενσωμάτωσης της προτεινόμενης προσέγγισης στα υφιστάμενα προγράμματα σπουδών

Το 3ο Κεφάλαιο αναφέρει επίσης τις κύριες δυσκολίες της ενσωμάτωσης της προτεινόμενης προσέγγισης στα υφιστάμενα προγράμματα σπουδών. Οι δυσκολίες έχουν ταξινομηθεί σε τέσσερις ομάδες, δηλαδή: δυσκολίες των εκπαιδευτικών, δυσκολίες θέματος/προγράμματος σπουδών, δυσκολίες εκπαιδευόμενων και οργανωτικές δυσκολίες.

Οι κύριες δυσκολίες που αντιμετωπίζουν οι εκπαιδευτικοί εντοπίζονται και αναδεικνύονται ως εξής:

1. Εναλλαγές στην διδακτική μεθοδολογία: Συνήθως, γίνονται αποδεκτές με θετικότητα ενώσω βρίσκονται στο στάδιο της ανάπτυξης, αλλά τα αποτελέσματα όταν φτάνουν στο στάδιο της εφαρμογής ενδέχεται να διαφέρουν σημαντικά.

2. Ανεπαρκής διδασκαλία ορισμένων θεμάτων: Η μετατόπιση της προσοχής προς ορισμένα θέματα ή έννοιες οδηγεί σε μη ικανοποιητική κάλυψη άλλων θεμάτων
3. Αλλαγές στους στόχους και στην ύλη
4. Προσαρμογή των μέσων διδασκαλίας: Αυτό σχετίζεται με το σημείο 1 και με τις αλλαγές στην οργάνωση που αναφέρονται στην επόμενη ενότητα
5. Αξιολόγηση: τα κριτήρια αξιολόγησης πρέπει να προσαρμόζονται προκειμένου να αντικατοπτρίζουν τις νέες αλλαγές
6. Διάρθρωση, διαθεσιμότητα και δυνατότητα εφαρμογής του περιεχομένου

Δεύτερον, ανάλογα με το θέμα, η ενσωμάτωση των νέων προγραμμάτων σπουδών ή πλαισίων, αντιμετωπίζει τις εξής προκλήσεις [1] [2]:

1. Έλλειψη πόρων μάθησης: οι πόροι δεν είναι πάντα διαθέσιμοι ώστε να καλύπτουν τις απαιτούμενες αλλαγές
2. Μη επαρκώς καταρτισμένο προσωπικό: σε σχέση με την προηγούμενη ενότητα, οι δεξιότητες του προσωπικού επηρεάζουν άμεσα την ποιότητα της παράδοσης των προγραμμάτων σπουδών. Αντίστοιχα, οι νέοι στόχοι δεν μπορούν να επιτευχθούν μέχρι το προσωπικό να αποκτήσει προσόντα υψηλού επιπέδου και να είναι έτοιμο να εφαρμόσει τα προγράμματα σπουδών που αναπτύχθηκαν
3. Υποστήριξη διοίκησης
4. Φόρτος εργασίας: η εφαρμογή των νέων στοιχείων μπορεί να είναι χρονοβόρα
5. Ετοιμότητα για αποδοχή των νέων προσεγγίσεων

Τρίτον, όσον αφορά τους φοιτητές, οι αλλαγές σε καθιερωμένα προγράμματα σπουδών ενδέχεται να εκληφθούν ως αποκλίσεις και όχι ως αλλαγή κατεύθυνσης, γεγονός που καθιστά απαραίτητη την επαρκή ενημέρωση των φοιτητών για την ανάγκη πραγματοποίησης αλλαγής στο πρόγραμμα σπουδών. Εντούτοις, οι αλλαγές θα οδηγήσουν σε αντίσταση και ενδέχεται να οδηγήσουν σε μείωση της εμπιστοσύνης προς το εκάστοτε ίδρυμα και την αξιοπιστία του. Τέλος, εφόσον η αναβάθμιση των προγραμμάτων σπουδών ενδέχεται να απαιτεί ειδικές υπηρεσίες και εργαλεία εκπαίδευσης/κατάρτισης, δεν θα έχουν όλα τα ιδρύματα την οικονομική δυνατότητα να πραγματοποιήσουν αντίστοιχες αναβαθμίσεις, πράγμα που θα μπορούσε να επηρεάσει αντίστοιχα την παράδοση και την ποιότητα των αναβαθμισμένων προγραμμάτων σπουδών.

Τα προηγούμενα ζητήματα αφορούν συνήθως τις δυσκολίες που πρέπει να λαμβάνονται υπ' όψιν για όσο τα προγράμματα σπουδών είναι στη φάση ανάπτυξης. Επίσης, όπως υποδεικνύεται στο [3], θα ήταν χρήσιμο να δοθεί ιδιαίτερη έμφαση στη δημιουργία διεθνικών προγραμμάτων σπουδών που να είναι ιδιαίτερα ευέλικτα και, ως εκ τούτου, να εξυπηρετούν περισσότερες περιοχές και τομείς.

4. Προτάσεις εκπαιδευτικών μεθοδολογιών

Σε αυτό το κεφάλαιο ο στόχος μας είναι να εντοπίσουμε τις εκπαιδευτικές μεθοδολογίες ή τεχνικές που θα είναι χρήσιμες κατά τη διδασκαλία σχετικά με την κυβερνοασφάλεια στα έξυπνα δίκτυα. Για αυτόν τον σκοπό, αρχικά αναλύουμε οκτώ καινοτόμες εκπαιδευτικές μεθόδους και, στη συνέχεια, διεξάγουμε μια ανασκόπηση της χρήσης τους στα πεδία ενδιαφέροντος είτε χωριστά είτε συνδυαστικά. Από τα αποτελέσματα της ανασκόπησης, κάνουμε προτάσεις για τα διαφορετικά διδακτικά περιβάλλοντα.

4.1 Μια σύντομη παρουσίαση των μεθόδων που εξετάστηκαν

Το παραδοσιακό μοντέλο μάθησης - Η μάθηση που βασίζεται στη διάλεξη

Η μάθηση που βασίζεται στη διάλεξη είναι η πιο ευρέως χρησιμοποιούμενη μέθοδος διδασκαλίας λόγω της δυνατότητάς της για κλιμάκωση, καθώς και επειδή ο εκπαιδευτικός ελέγχει την ύλη και τον τρόπο που διδάσκεται. Το κύριο μειονέκτημά της είναι ότι οι φοιτητές μπορεί να καταφύγουν στην απομνημόνευση και όχι στην κατανόηση, προκειμένου να περάσουν τις εξετάσεις. Συχνά, συνδυάζεται με ορισμένες μορφές βιωματικής μάθησης, όπως οι προσομοιώσεις και οι ασκήσεις σε εργαστήριο.

Βιωματική μάθηση

Ο όρος «βιωματική μάθηση» περιλαμβάνει όλες τις μορφές μάθησης όπου η γνώση αποκομίζεται μέσω της εμπειρίας. Περιγράφηκε από τον David Colb το 1984 ως ένας κύκλος που μπορεί να επαναλαμβάνεται διαρκώς όπου η εμπειρία οδηγεί στη διαμόρφωση συμπερασμάτων τα οποία μπορούν να χρησιμοποιηθούν, στη συνέχεια, για τη δημιουργία νέων πειραμάτων και την απόκτηση περισσότερης εμπειρίας.

Ενεργητική μάθηση

Η ενεργητική μάθηση είναι άλλος ένας όρος με ευρεία έννοια και βασίζεται στην αύξηση του ενδιαφέροντος των μαθητών με το να ζητείται η ενεργή συμμετοχή τους . Κατά τη διάρκεια της διάλεξης, η ενεργητική μάθηση μπορεί να λάβει τη μορφή της δημιουργίας ενός εννοιολογικού χάρτη, της υποβολής ερωτήσεων στο κοινό, της σύνταξη μιας σύντομης έκθεσης ή της διδασκαλίας μεταξύ μαθητών.

Συνεργατική μάθηση

Η συνεργατική μάθηση περιγράφει την εργασία μιας ομάδας όπου κάθε φοιτητής δεν αφιερώνει μόνο τον χρόνο του στην ομαδική εργασία αλλά, επίσης, είναι υπεύθυνος για την απόδοση της ομάδας και την αποτελεσματικότητα της κατανομής των ευθυνών στα μέλη της ομάδας.

Ανεστραμμένη τάξη

Κατά την τεχνική της ανεστραμμένης τάξης, αναμένεται από τους φοιτητές να έχουν μελετήσει εκ των προτέρων το υλικό που τους έχει δοθεί. Το υλικό μπορεί να υπάρχει ήδη ως βιβλίο ή σειρά βίντεο αλλά μπορεί, επίσης, να δημιουργηθεί ειδικά για το μάθημα. Κατά τη διάρκεια του μαθήματος, ο εκπαιδευτικός μπορεί να χρησιμοποιήσει τεχνικές ενεργητικής μάθησης για να εμβαθύνει την κατανόηση των φοιτητών. Ένα πιθανό μειονέκτημα είναι η ανομοιογενής πρόσβαση των φοιτητών σε ηλεκτρονικά μέσα.

Διερευνητική μάθηση

Η διερευνητική μάθηση μοιάζει σε μεγάλο βαθμό με την επιστημονική μέθοδο. Τα στάδιά της περιλαμβάνουν τον Προσανατολισμό, τη Σύλληψη εννοιών, τη Διερεύνηση, το Συμπέρασμα και τη Συζήτηση. Ανάλογα με την ωριμότητα των φοιτητών, ο εκπαιδευτικός μπορεί να παρέχει περισσότερη ή λιγότερη καθοδήγηση και πληροφορίες.

Μάθηση με βάση το πρόβλημα και μάθηση με βάση το έργο

Η βάση αυτών των μεθόδων είναι η συνεργατική μάθηση. Κατά τη μάθηση με βάση το πρόβλημα (PBL), μια ομάδα φοιτητών ερευνά ένα πραγματικό πρόβλημα που δεν έχει επιλυθεί και προσπαθεί να βρει την καταλληλότερη λύση, την οποία η ομάδα θα παρουσιάσει στους υπόλοιπους φοιτητές. Η μάθηση με βάση το έργο μοιάζει με τη μάθηση

με βάση το πρόβλημα ωστόσο, συνήθως, διαρκεί περισσότερο και η λύση δεν είναι μόνο θεωρητική αλλά έχει απτό και σαφές αποτέλεσμα όπως ένα πρόγραμμα ή μοντέλο υπολογιστή.

Παιχνιδοποίηση

Κατά την παιχνιδοποίηση, τα στοιχεία και οι μηχανισμοί που ενσωματώνονται συνήθως κατά τη διάρκεια του σχεδιασμού ενός παιχνιδιού (ολοκλήρωση επιπέδων, περιορισμένος χρόνος ολοκλήρωσης μιας εργασίας και άλλα) χρησιμοποιούνται προκειμένου να αυξηθεί το ενδιαφέρον των φοιτητών.

4.2 Παραδείγματα χρήσης και αντικτύπου των μεθόδων στον τομέα των συστημάτων ενέργειας - Προτάσεις

Προκειμένου να προσδιοριστεί ο αντίκτυπος της χρήσης των διαφόρων μεθόδων κατά τη διδασκαλία για την κυβερνοασφάλεια στα έξυπνα δίκτυα, πραγματοποιήσαμε μια βιβλιογραφική ανασκόπηση σε ένα σύνολο 43 εγγράφων. 21 από αυτά έχουν γραφτεί από άτομα που χρησιμοποίησαν μερικές από τις παραπάνω μεθόδους για να διδάξουν ένα συναφές μάθημα, ενώ τα υπόλοιπα είναι πιο γενικά (π.χ. βιβλιογραφικές ανασκοπήσεις). Οι παρατηρήσεις από τη βιβλιογραφική ανασκόπηση παρατίθενται παρακάτω:

Περιορισμοί στη χρήση των τεχνικών ενεργητικής μάθησης:

Η χρήση τεχνικών ενεργητικής μάθησης απαιτεί περισσότερο προσωπικό, χρόνο και πόρους, καθώς και ομοιογενείς ομάδες φοιτητών που να κατέχουν ένα ελάχιστο επίπεδο γνώσης σχετικά με το θέμα.

Χρήση της παιχνιδοποίησης στα πανεπιστήμια:

Η παιχνιδοποίηση μπορεί να λάβει τη μορφή πραγματικών παιχνιδιών, όπως το Riskio, ένα επιτραπέζιο παιχνίδι που μπορεί να χρησιμοποιηθεί για τους εργαζομένους χωρίς τεχνικές γνώσεις.

Εκδηλώσεις τύπου «Capture the flag» και «Hacking Day»

Οι διαγωνισμοί τύπου «Capture the flag» (CTF) είναι μια μορφή παιχνιδοποίησης και περιλαμβάνουν στοιχεία από τη βιωματική και τη συνεργατική μάθηση. Κατά τους διαγωνισμούς CTF ο στόχος των παικτών είναι να ανακαλύψουν τις ευπάθειες του συστήματος (είτε στο υλικό είτε στο λογισμικό) και ένα στοιχείο (τη σημαία) που έχουν κρύψει στο σύστημα οι διοργανωτές. Μπορεί να πάρει τη μορφή δυο ομάδων που είναι αντιμέτωπες ή κάθε διαγωνιζόμενη ομάδα να προσπαθεί να εισβάλει στο σύστημα των διοργανωτών. Οι CTF διαγωνισμοί είναι κατάλληλοι για εκπαίδευση σε επιθέσεις που πραγματοποιούνται σε σύντομο χρονικό διάστημα. Θα πρέπει να δίνεται ιδιαίτερη φροντίδα στη διευκόλυνση των αρχάριων παικτών. Οι CTF διαγωνισμοί μπορούν να πάρουν τη μορφή μιας εκδήλωσης για τη σταδιοδρομία με τη συμμετοχή παραγόντων της βιομηχανίας. Ορισμένοι από τους φοιτητές μπορούν να είναι η οργανωτική ομάδα της εκδήλωσης που δυνητικά μπορεί να τους παρέχει ιδιαίτερα σημαντικές οργανωτικές δεξιότητες.

Χρήση της παιχνιδοποίησης στην βιομηχανία

Η παιχνιδοποίηση στην βιομηχανία έχει χρησιμοποιηθεί με επιτυχία σε εργαζομένους που δεν έχουν τεχνικές γνώσεις για τη βελτίωση της αποτροπής της επίθεσης ηλεκτρονικού «ψαρέματος». Είναι σημαντικό να σημειωθεί ότι, στην εταιρεία όπου συλλέχθηκαν τα δεδομένα, η ομάδα που είχε ήδη εκπαιδευτεί για την αποτροπή των επιθέσεων ηλεκτρονικού

«ψαρέματος» με απλή μέθοδο διάλεξης είχε τα ίδια αποτελέσματα με την ομάδα ελέγχου που δεν είχε εκπαιδευτεί καθόλου.

Χρήση της επίδειξης

Η επίδειξη μπορεί να χρησιμοποιηθεί τόσο για τους προπτυχιακούς φοιτητές όσο και για τους εργαζόμενους. Σε ένα παράδειγμα, χρησιμοποιήθηκε το Shodan που μπορεί να εντοπίζει διάφορες συσκευές που συνδέονται στο διαδίκτυο χωρίς διαπιστευτήρια ή με προεπιλεγμένα διαπιστευτήρια. Οι φοιτητές και οι εργαζόμενοι μπορούν να συνειδητοποιούν τον πιθανό αντίκτυπο της συμπεριφοράς τους όσον αφορά την τήρηση καλών συνηθειών κυβερνοασφάλειας.

Χρήση της μάθησης με βάση το έργο:

Η μάθηση με βάση το έργο είναι η μέθοδος που χρησιμοποιείται πιο συχνά μαζί με την παιχνιδοποίηση. Σε μια έρευνα προτείνεται ότι όταν οι φοιτητές διδάσκονται ένα μάθημα χρησιμοποιώντας πρακτικές εφαρμογές, σημειώνεται σημαντική βελτίωση στο ποσοστό συγκράτησής της γνώσης από τους φοιτητές, μερικές εβδομάδες μετά την ολοκλήρωση του σεμιναρίου. [4]

Εικονικά εργαστήρια και απομακρυσμένη πρόσβαση:

Η τάση για χρήση των εικονικών εργαστηρίων, η οποία εμφανίστηκε το 2010, ενισχύθηκε εξαιτίας της πανδημίας COVID-19. Τα στατιστικά στοιχεία που περιλαμβάνονται στο [5] δείχνουν ότι οι φοιτητές τείνουν να χρησιμοποιούν τα εργαστήρια κατά τις ώρες που είναι συνήθως κλειστά για το κοινό. Ωστόσο η απομακρυσμένη πρόσβαση απαιτεί πρόσθετες ώρες εργασίας από το προσωπικό του εργαστηρίου για λόγους τεχνικής υποστήριξης.

Χρήση πλατφορμών διεξαγωγής δοκιμών (testbed) για τη διδασκαλία της κυβερνοασφάλειας:

Ο πιο ολοκληρωμένος και ρεαλιστικός τρόπος για τη μελέτη των επιδράσεων μιας κυβερνοεπίθεσης και της αποκατάστασης της λειτουργίας μετά από καταστροφή εξαιτίας της είναι να χρησιμοποιηθεί μια πλατφόρμα διεξαγωγής δοκιμών (testbed). Σε μια πλατφόρμα διεξαγωγής δοκιμών (testbed) πραγματοποιείται εξαιρετικά λεπτομερής προσομοίωση του συστήματος. Το επίπεδο της λεπτομέρειας αυξάνεται καθώς περισσότερα από τα στοιχεία του συστήματος περιλαμβάνονται στην φυσική τους μορφή αντί να προσομοιώνονται και καθώς προστίθενται περισσότερα στοιχεία του ίδιου συστήματος. Παραδείγματα χρήσης προσομοιωτών σε πραγματικό χρόνο για τη μελέτη των κυβερνοεπιθέσεων υπάρχουν στα [6], [7].

5. Προτάσεις

Το τελευταίο μέρος της έκθεσης αποτελείται από προτάσεις σε αφηρημένο επίπεδο που απευθύνονται ξεχωριστά στα διάφορα ενδιαφερόμενα μέρη, όπως τα πανεπιστήμια, οι πάροχοι επαγγελματικής κατάρτισης (ΕΠΑΛ/ΙΕΚ), η βιομηχανία και οι αρμόδιοι χάραξης πολιτικής. Οι προτάσεις ήταν αποτέλεσμα της μελέτης πολλών εγγράφων (κυρίως ευρωπαϊκών), όπως οι εκθέσεις Ομάδων Εργασίας, τα παραδοτέα ευρωπαϊκών έργων και άλλα. Στις επόμενες παραγράφους παρουσιάζουμε συνοπτικά τις προτάσεις προς τα διάφορα ενδιαφερόμενα μέρη.

5.1 Πανεπιστήμια:

- Δημιουργία παρατηρητηρίου για συνεχή παρακολούθηση των αποτελεσμάτων από νέες έρευνες αλλά και από έρευνες σε εξέλιξη στο συνδυασμένο πεδίο της κυβερνοασφάλειας και των Έξυπνων Δικτύων
- Δημιουργία βάσης δεδομένων από ειδικούς και ερευνητές σε συνδυασμό με τους τομείς εργασίας τους για τη δημιουργία κοινών μεταπτυχιακών προγραμμάτων που, επί του παρόντος, δεν υπάρχουν στο Erasmus Mundus για το συγκεκριμένο πεδίο.
- Συνέχιση και διεύρυνση της χρήσης του Ευρωπαϊκού συστήματος μεταφοράς ακαδημαϊκών μονάδων σύμφωνα με τη Συμφωνίας της Μπολόνια. Η εναρμόνιση των ευρωπαϊκών συστημάτων πιστοποίησης είναι προαπαιτούμενο για την ύπαρξη των κοινών προγραμμάτων σπουδών.
- Αντιμετώπιση του εμποδίου της έλλειψης εξοπλισμού δημιουργώντας μία πλατφόρμα για πρόσβαση σε υποδομές σύμφωνα με το παράδειγμα του έργου ERIGRID 2.0.
- Δημιουργία αποθετηρίου για πανεπιστημιακά μαθήματα και κοινοποίηση του σχεδιασμού των μαθημάτων και των βέλτιστων πρακτικών για την επιτάχυνση της υιοθέτησης τους.
- Τα πανεπιστήμια θα πρέπει να προσανατολιστούν περισσότερο στην εκπαίδευση μηχανικών με δεξιότητες σε σχήμα Τ, οι οποίοι διαθέτουν ευρύ φάσμα γενικών γνώσεων (οριζόντιο τμήμα του Τ) και υψηλό επίπεδο εξειδικευμένων γνώσεων (κάθετο τμήμα του Τ)
- Οι γενικές γνώσεις θα πρέπει να συμπεριλαμβάνουν τις δεοντολογικές, κοινωνικές και νομικές πτυχές

5.2 Πάροχοι επαγγελματικής κατάρτισης (ΕΠΑΛ/ΙΕΚ):

- Δημιουργία έργων όπως το UP-RES [8], το οποίο ήταν επίσης παράδειγμα ενός έργου όπου συνδυάζονται δυο επιστημονικοί τομείς, δηλαδή οι ανανεώσιμοι πόροι ενέργειας και η πολεοδομία. Το αποτέλεσμα θα είναι η αποφοίτηση καταρτισμένων επαγγελματιών, οι δημιουργία βέλτιστων πρακτικών για την εκπαίδευση, το εκπαιδευτικό υλικό και η πιθανή συνεργασία μεταξύ πανεπιστημίων.
- Οι πάροχοι δια βίου επαγγελματικής εκπαίδευσης και κατάρτισης (C-VET) θα πρέπει να διαμορφώσουν σεμινάρια και ενότητες ηλεκτρονικής εκπαίδευσης με πολύ συγκεκριμένο σημείο εστίασης, όπως ο τρόπος εφαρμογής ενός πρωτοκόλλου επικοινωνίας σε μια συσκευή παλαιού τύπου (legacy device). Οι συγκεκριμένοι πάροχοι μπορούν να διαμορφώσουν ένα μικρό μεταπτυχιακό πρόγραμμα (micro-master), το οποίο ισοδυναμεί με ένα εξάμηνο ενός μεταπτυχιακού προγράμματος κανονικής διάρκειας.
- Ορισμένα σεμινάρια μπορούν να έχουν τον ρόλο της προετοιμασίας για την απόκτηση ενός πιστοποιητικού που γενικά μπορεί να συμβάλλει στην αύξηση της δυνατότητας εύρεσης εργασίας του αποφοίτου, δίνοντας ιδιαίτερη προσοχή στην επιλογή των πιστοποιήσεων.

5.3 Βιομηχανία:

Οι ικανότητες των εργαζομένων όσον αφορά την κυβερνοασφάλεια μπορούν να αναλυθούν σε δύο ευρείες κατηγορίες που περιλαμβάνουν: πρώτον, τις τεχνικές δεξιότητες και γνώσεις που είναι συναφείς με το προϊόν ή την υπηρεσία που προσφέρει η εταιρεία και, δεύτερον, την ευαισθητοποίηση σχετικά με το πώς ο ανθρώπινος παράγοντας (τόσο οι εργαζόμενοι όσο και οι πελάτες) μπορεί να επηρεάσει την ασφάλεια του συστήματος.

- Τα θέματα και οι αρχές που θα πρέπει να διδαχτούν στους εργαζομένους περιλαμβάνουν τα εξής:
    - Το ότι ανάμεσα στο μοντέλο Κοινόχρηστης Βάσης Δεδομένων (shared-database model) και στο μοντέλο που βασίζεται στο μήνυμα (message-based model), το δεύτερο είναι αυτό που ωφελεί [9]
    - Το Μοντέλο Οντολογίας Αναφοράς Έξυπνων Εφαρμογών (SAREF), το οποίο αναλύει σε βάθος τις οικιακές συσκευές IoT και τις σχέσεις μεταξύ τους.
    - Τον προσανατολισμό σχετικά με το πώς μπορούν τα διάφορα εξαρτήματα να ενημερώνονται και να αναβαθμίζονται διαρκώς.
    - Την εφαρμογή των αρχών **προστασία ήδη από τον σχεδιασμό** και **προστασία εξ ορισμού**.
    - Τη σχετική νομοθεσία. Μια ικανοποιητική επισκόπηση, που καλύπτει διάστημα έως τα μέσα του 2017, υπάρχει στο [10], ενώ, πιο πρόσφατα, προστέθηκαν ο ΓΚΠΔ (Γενικός Κανονισμός Προστασίας Δεδομένων ΓΚΠΔ) και η οδηγία NIS 2.0.

Τα τρία σημεία που διαφοροποιούν το πεδίο της κυβερνοασφάλειας στον τομέα της ενέργειας σε σχέση με τον γενικό τομέα της κυβερνοασφάλειας είναι [11] η χρήση εξοπλισμού παλαιού τύπου (legacy devices), οι «αλυσιδωτές» επιπτώσεις εξαιτίας του υψηλού βαθμού διασύνδεσης ανάμεσα στα ευρωπαϊκά ηλεκτρικά συστήματα και οι απαιτήσεις σε πραγματικό χρόνο, πράγμα που σημαίνει ότι κάποιες ενέργειες στο πλαίσιο του δικτύου ενέργειας θα πρέπει να εκτελούνται πολύ γρήγορα, ενώ θα πρέπει να επιλέγονται αντιστοίχως τα πρωτόκολλα ασφάλειας. Για καθέναν από αυτούς τους τρεις τομείς συνιστάται να διδάσκονται οι παρακάτω αρχές και βέλτιστες πρακτικές:

Εξοπλισμός παλαιού τύπου: Συστηματική διαχείριση ενημερώσεων κώδικα και τακτική ανάλυση κινδύνων σχετικά με τις συσκευές παλαιού τύπου

«Αλυσιδωτές» επιπτώσεις: Ταξινόμηση των τμημάτων του ηλεκτρικού δικτύου και προσδιορισμός των σημαντικών κόμβων για αποφυγή μοναδικού σημείου αποτυχίας (single point of failure)

Απαιτήσεις σε πραγματικό χρόνο: Διαχωρισμός δικτύων

- Προτάσεις σχετικές με τις επιπτώσεις του ανθρώπινου παράγοντα στην κυβερνοασφάλεια
    - Οι εταιρείες θα πρέπει να οργανώνουν σεμινάρια για να εκτιμάται η ικανότητα των εργαζομένων και η ποιότητα των αποφάσεων που λαμβάνουν, οι οποίες σχετίζονται με την κυβερνοασφάλεια
    - Οι διευθυντές θα πρέπει να λαμβάνουν πρόσθετη κατάρτιση για το πώς η συμπεριφορά τους επηρεάζει τους υφισταμένους τους [12], για παράδειγμα, να καθιστούν σαφές ότι η ασφάλεια δεν θα πρέπει να παραμελείται προς όφελος της παραγωγικότητας.
    - Θα πρέπει να χρησιμοποιείται το εργαλείο του ENISA «Good practices for IoT and Smart Infrastructures Tool» (Ορθές πρακτικές για το IoT και τις έξυπνες υποδομές), το οποίο μπορεί να είναι χρήσιμο, ειδικά, στις μικρές επιχειρήσεις.

5.4 Αρμόδιοι χάραξης πολιτικής:

- Τα κράτη μέλη θα πρέπει να ελέγχονται για το πώς εφαρμόζουν την οδηγία NIS 2.0, που μπορεί να χρησιμοποιηθεί ως μοντέλο αναφοράς. Η ύπαρξη της αρχής NIS που θεσμοθετεί την ύπαρξη Ομάδων Παρέμβασης σε Συμβάντα που αφορούν την Ασφάλεια των Υπολογιστών (CSIRT) είναι σημαντική. Οι σχετικές εταιρείες θα πρέπει να διατηρούν

καταγραφή με τον εξοπλισμό που διαχειρίζονται, τις εργασίες και τα στοιχεία των κρίσιμων υποδομών τους, καθώς και να προσδιορίζουν τους διαχειριστές των υπηρεσιών ουσιώδους σημασίας (essential services) σύμφωνα με την οδηγία NIS.

- Δημιουργία αποθετηρίου όπου οι διαχειριστές να μπορούν να κοινοποιούν αναλυτικές πληροφορίες σχετικά με περιστατικά και έγκαιρες προειδοποιήσεις σχετικά με τις επιθέσεις και τις παραβιάσεις.
- Θα πρέπει να καταρτιστεί και να τηρείται αυστηρά ένα πρόγραμμα ελάχιστης ασφάλειας.
- Οι πλατφόρμες που χρησιμοποιούνται θα πρέπει είναι γνωστές όπως και τα κριτήρια για την διαλειτουργικότητα τους, όπως υποδεικνύουν οι συνιστώμενες πρακτικές αρχιτεκτονικής των επιχειρήσεων [13].
- Δημιουργία ενός αποθετηρίου όπου η βιομηχανία θα μπορεί να παρακολουθεί διαρκώς τις δεξιότητες που χρειάζονται.
- Δημιουργία μιας κοινής γλώσσας που θα συμβάλλει στην απομάκρυνση των εμποδίων στην επικοινωνία ανάμεσα σε διευθυντές και εργαζομένους με τεχνικές γνώσεις.
- Συνιστάται ιδιαίτερα να χρησιμοποιούνται τα υπάρχοντα μέσα επικοινωνίας, όπως τα MQQT και REST API, αντί να δημιουργούνται εκ του μηδενός καινούριες λύσεις.
- Λεπτομερέστερη ανάλυση των καινούριων ρόλων/επαγγελμάτων σχετικών με τα δεδομένα, ίσως με χρήση του Εναρμονισμένου προτύπου για την αγορά ηλεκτρικού ρεύματος (Harmonized Electricity Market Role Model, HEMRM)
- Εφαρμογή των προτύπων του κοινού μοντέλου δεδομένων (Common Information Model, CIM) στον Διαχειριστή συστήματος μεταφοράς (Transmission System Operator, TSO) και στον Διαχειριστή συστήματος διανομής (Distribution System Operator, DSO)

5.4.1 Προτάσεις σχετικά με τον τρόπο προώθησης της συνεργασίας μεταξύ των ενδιαφερόμενων μερών:

Όπως προαναφέρθηκε, η εκπαίδευση για την κυβερνοασφάλεια στα συστήματα ενέργειας πρέπει να αποτελεί συντονισμένη ενέργεια πολλών ενδιαφερόμενων μερών, καθώς είναι ένα ταχέως μεταβαλλόμενο πεδίο. Προτείνουμε τη σύσταση ενός φόρουμ διαλόγου γενικού επιπέδου, το οποίο θα διεξάγεται κάθε έτος ή κάθε δύο έτη και θα συμμετέχουν οι σχετικοί αρμόδιοι χάραξης πολιτικής, οι DSO, οι TSO, τα πανεπιστήμια και οι πάροχοι επαγγελματικής κατάρτισης, προκειμένου να ανταλλάσσουν πληροφορίες σχετικά με τις δραστηριότητες σε εξέλιξη και τις προγραμματισμένες δραστηριότητες στον τομέα.

Μια άλλη επιλογή ώστε να διατηρείται η επικοινωνία σε εξέλιξη, είναι η οργάνωση σημαντικών εκδηλώσεων στα εκπαιδευτικά ιδρύματα με την υποστήριξη της βιομηχανίας που θα μπορούσε να παρέχει τον εξοπλισμό. Παράλληλα, οι εν λόγω εκδηλώσεις θα μπορούσαν να αποτελούν εκδηλώσεις για τη σταδιοδρομία και να αυξάνουν τις πιθανότητες να επιλέξουν οι φοιτητές την κυβερνοασφάλεια ως επαγγελματικό τομέα.

6. Συμπεράσματα

Στην παραπάνω έκθεση στόχος μας ήταν να γίνει κατανοητό σε ποιους τομείς υπάρχουν ελλείψεις στην εκπαίδευση για την κυβερνοασφάλεια στα έξυπνα δίκτυα, να προτείνουμε αποτελεσματικές εκπαιδευτικές μεθόδους και να πραγματοποιήσουμε προτάσεις γενικού επιπέδου, προκειμένου να βελτιωθεί η εκπαίδευση σε αυτόν τον τομέα. Η ανάλυση πραγματοποιήθηκε μέσω εκτεταμένης βιβλιογραφικής ανασκόπησης, συνεντεύξεων με εκπροσώπους της βιομηχανίας και ειδικά εργαστήρια που διεξήχθησαν στο πλαίσιο του CC-RSG τον Μάιο του 2021.

Οι προκλήσεις που αντιμετωπίζει η βιομηχανία σχετίζονται κυρίως με το ότι οι νέοι πτυχιούχοι δεν έχουν επαρκή κατάρτιση σε πρακτικές καταστάσεις όμοιες με αντίστοιχες που θα αντιμετωπίσουν κατά τη διάρκεια της εργασίας τους ούτε σε ζητήματα διαχείρισης και επικοινωνίας.

Όσον αφορά τις εκπαιδευτικές μεθόδους, η παιχνιδοποίηση φαίνεται να είναι η πιο πολλά υποσχόμενη για το πεδίο της κυβερνοασφάλειας. Μπορεί να χρησιμοποιηθεί για την κατάρτιση των εργαζομένων στον κλάδο των συστημάτων ενέργειας, τόσο για εκείνους που δεν έχουν τεχνικές γνώσεις, αλλά και για την κατάρτιση του τεχνικού προσωπικού βοηθώντας το να αποκτήσει πρακτική εμπειρία. Διαπιστώθηκε ότι η μάθηση με βάση το έργο βελτιώνει το ποσοστό συγκράτησης της γνώσης από τους μαθητές μετά από μερικές εβδομάδες αλλά, όπως όλες οι μέθοδοι ενεργητικής μάθησης έχει ορισμένους περιορισμούς, με πιο σημαντικούς το ότι μπορεί να εφαρμοστεί σε φοιτητές που διαθέτουν ήδη ένα επίπεδο αυτονομίας στο σχετικό θέμα και ότι οι ομάδες φοιτητών πρέπει να είναι ομοιογενείς ως προς την γνώση.

Το θέμα που μελετάμε σχετίζεται πολύ στενά με πρακτικά συστήματα, οπότε είναι πολύ σημαντικό να αναπτυχθούν τρόποι που θα βοηθήσουν όσο το δυνατόν περισσότερα ενδιαφερόμενα μέρη να αποκτήσουν πρόσβαση στον σχετικό εξοπλισμό. Αυτό μπορεί να γίνει με πολλούς τρόπους, όπως η επέκταση της χρήσης της απομακρυσμένης προσβασιμότητας των πλατφορμών διεξαγωγής δοκιμών (testbed) που υπάρχουν στα ερευνητικά κέντρα ή στα εκπαιδευτικά ιδρύματα, η οργάνωση της κοινής χρήσης της υποδομής (για παράδειγμα, το έργο ERIGRID 2.0 της ΕΕ) ή η παρότρυνση της βιομηχανίας να συμμετέχει στην οργάνωση των μαθημάτων που διεξάγουν τα πανεπιστήμια. Οι εξοπλισμός μπορεί να περιλαμβάνει γενικό εξοπλισμό υλικού, όπως υπολογιστές, και εξειδικευμένο εξοπλισμό, όπως PMU, RTU, προσομοιωτές πραγματικού χρόνου κ.λπ.

Οι προτάσεις προς τα ενδιαφερόμενα μέρη σχετίζονται σε μεγάλο βαθμό με τους τρόπους επικοινωνίας και την αντιστοίχιση των διαθέσιμων πόρων (επαγγελματίες, βέλτιστες πρακτικές, υποδομή). Η αντιστοίχιση είναι η βάση για την ανάπτυξη αποτελεσματικών τρόπων για τη συγκέντρωση των διαθέσιμων πόρων, όπως η δημιουργία κοινών πτυχίων, ένα σύστημα έγκαιρης προειδοποίησης για τα περιστατικά σχετικά με την κυβερνοασφάλεια και άλλοι. Εκτός από τις προηγούμενες προτάσεις, συμπεριλάβαμε μια σύντομη ανάλυση των γνώσεων που θα μπορούσαν να διδαχθούν στο τεχνικό προσωπικό και το πώς η κυβερνοασφάλεια των συστημάτων ενέργειας διαφέρει γενικά από το πεδίο της κυβερνοασφάλειας.

Όσον αφορά τους αρμόδιους χάραξης πολιτικής, η πιο σημαντική αποστολή είναι να δημιουργήσουν οδούς επικοινωνίας, όπως μια κοινή γλώσσα, για διευθυντές και τεχνικούς, το Ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας (European Cybersecurity Skills Framework, ECSF), που προβλέπεται από τον ENISA (αν και δεν αφορά συγκεκριμένα τα συστήματα ενέργειας), καθώς και οδηγίες και κανονισμούς για την ελαχιστοποίηση της χρήσης ιδιόκτητων λύσεων (proprietary solutions).

Η παραπάνω ανάλυση παρουσιάζει τα πλεονεκτήματα της ανάπτυξης πλατφορμών διεξαγωγής δοκιμών (testbed) σε πραγματικό χρόνο, οι οποίες μοντελοποιούν τόσο το σύστημα ενέργειας όσο και το δίκτυο επικοινωνιών. Στη συνέχεια, αυτό το μοντέλο μπορεί να χρησιμοποιηθεί για την ανάλυση πιθανών επιθέσεων (ίσως, σε συνδυασμό με ανθρώπινα λάθη) στο πλαίσιο των μοναδικών συνθηκών και των απαιτήσεων υπό τις οποίες λειτουργούν τα έξυπνα δίκτυα (και τα συστήματα ενέργειας, γενικά).

7. Βιβλιογραφία

[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. [Online]. Διατίθεται στο: 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,* 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]. Διατίθεται στο: 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.