Προηγμένο επίπεδο, τάσεις και ελλείψεις δεξιοτήτων όσον αφορά την κυβερνοασφάλεια στα έξυπνα δίκτυα (Συνοπτική έκθεση)

Συντάκτες:

Jirapa Kamsamrong, Björn Siemers, Shadi Attarha,
Sebastian Lehnhoff, Μαρία Βάλλιου, Andrejs Romanovs,
Jana Bikovska, Janis Peksa, Ruta Pirta-Dreimane,
Janis Grabis, Nadezhda Kunicina, Julija Srebko,
Tero Vartiainen, Bahaa Eltahawy, Mike Mekkanen

Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)

Erasmus+ Strategic Partnership Project

Intellectual Output 1

Απρίλιος 2022

Αξιολογητής: Φοίβος Παλαιογιάννης

Συντονισμός: Πανεπιστήμιο της Βάασα
Συνεργάτες: Πανεπιστήμιο του Όλντενμπουργκ, 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.

Περιεχόμενα

List of Tables 4
List of Figures 4
Abbreviations 5
1. Introduction 6
1.1 Objectives 6
1.2 Structure of the document 6
2. Research Methodology 7
3. Cybersecurity Policy in European Union 7
3.1 EU Policies and Strategic Directions 7
3.2 Organization related to cybersecurity 8
3.3 Industry Studies and Recommendations 8
3.4 Industry Studies and Recommendations 9
4. State of the art and trends in cybersecurity in smart grids 9
4.1 Categorization 9
4.2 Technology and Education Development 10
4.3 Gaps analysis 12
5. State of the art in education in smart grids and cyber security 14
5.1 Higher education study programs 14
5.2 Continuing education programs 14
5.3 Massive open online courses (MOOC) 14
6. Identification of skill gaps in cyber security in smart grids 15
7. Identification of useful tools for education in cyber security in smart grid 16
7.1 Basic tools for active learning about cybersecurity 16
7.2 Advanced tools for vulnerabilities experiments 16
8. Conclusion and recommendations 17
9. Bibliography 19

Κατάλογος πινάκων

Table 1 Cyberattacks classification considering CIA..... 11
Table 2 Gap analysis for existing CPES laboratory/testbed..... 12
Table 3 Cybersecurity Risks in the CPES..... 13
Table 4 Recommendation from the stakeholder workshop [70] 15
Table 5 Educational Approaches in Smart Grids and Cyber Security 16
Table 6 Cybersecurity tools for smart grids 17

Κατάλογος εικόνων

Figure 1 Research methodology of WP1 7
Figure 2 Cybersecurity education curriculum thought model 9
Figure 3 Categorization of skill gaps based on the literature review 10

Συντομογραφίες

ACM Association for Computing Machinery (Σύλλογος Μηχανημάτων Υπολογισμού)
AES Advanced Encryption Standard (Προηγμένο Πρότυπο Κρυπτογράφησης)
CIA Confidentiality, Integrity, and Availability (Εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα)
CPES Cyber Physical Energy System (Κυβερνο-φυσικό σύστημα ενέργειας)
DdoS Distributed Denial of Service (Κατανεμημένη άρνηση υπηρεσιών)
DMZ Demilitarized Zones (Αποστρατικοποιημένες ζώνες)
DoS Denial of Service (Άρνηση υπηρεσιών)
ENISA European Network and Information Security Agency (Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών)
EU Ευρωπαϊκή Ένωση
HPC Hardware performance counters (Μετρητές απόδοσης υλικού)
ICS Industrial Control Systems (Συστήματα βιομηχανικού ελέγχου)
ICT Information and Communications technology (Τεχνολογία πληροφοριών και επικοινωνίας)
IDS Intrusion detection system (Σύστημα ανίχνευσης εισβολής)
IEC International Electrotechnical Commission (Διεθνής Ηλεκτροτεχνική Επιτροπή)
IoT Internet of Things (Διαδίκτυο των πραγμάτων)
IP Internet Protocol (Πρωτόκολλο διαδικτύου)
KUs Knowledge Units (Μονάδες γνώσης)
MOOC Massive online open courses (Μαζικά ανοιχτά διαδικτυακά μαθήματα)
VET Vocational education and training (Επαγγελματική εκπαίδευση και κατάρτιση)
WP Work Package (Πακέτο εργασιών)

1. Εισαγωγή

Τα τελευταία χρόνια, ο τομέας της ενέργειας έχει αυξήσει σημαντικά τον βαθμό ψηφιακής ωριμότητάς του ενσωματώνοντας ποικίλα ψηφιακά συστήματα και τεχνολογίες πληροφορικής, επικοινωνιών και βιομηχανικού ελέγχου σε ένα εκσυγχρονισμένο και προηγμένο δίκτυο ενέργειας. Επιπλέον, η Ευρώπη στοχεύει στην πλήρη ενσωμάτωση εναρμονίζοντας τη διασυνοριακή ανταλλαγή δεδομένων αγοράς σε πραγματικό χρόνο. Λόγω των τεράστιων όγκων δεδομένων και της ευρείας χρήσης του IoT, ο τομέας της ενέργειας έχει γίνει ακόμα πιο ελκυστικός για τους εισβολείς. Απαιτεί ευρύ φάσμα διεπιστημονικών γνώσεων σε τομείς, όπως τα συστήματα ενέργειας, η δικτύωση υπολογιστών, το λογισμικό, τα ενοποιημένα συστήματα και η διαχείριση ασφάλειας.

Η Ευρωπαϊκή Επιτροπή (ΕΕ) έχει θέσει σε εφαρμογή τη στρατηγική κυβερνοασφάλειας της ΕΕ προκειμένου να ενισχύσει τη συλλογική ανθεκτικότητα της Ευρώπης έναντι των κυβερνοαπειλών και να διασφαλίσει ότι όλοι οι πολίτες και οι επιχειρήσεις θα έχουν τη δυνατότητα να ωφεληθούν πραγματικά από φερέγγυες και αξιόπιστες υπηρεσίες και ψηφιακά εργαλεία. Η στρατηγική καλύπτει την ασφάλεια των αναγκαίων υπηρεσιών, συμπεριλαμβανομένων των δικτύων ενέργειας και του ολοένα αυξανόμενου αριθμού συνδεδεμένων αντικειμένων που υπάρχουν στα σπίτια των πολιτών και στα γραφεία των εργοστασίων. Η στρατηγική υποδεικνύει ότι οι τρέχουσες δυνατότητες της ΕΕ όσον αφορά την κυβερνοασφάλεια δεν επαρκούν. Προκειμένου να βελτιωθούν οι δυνατότητες ως προς την κυβερνοασφάλεια, τόσο η στρατηγική για την κυβερνοασφάλεια όσο και το πρόγραμμα «Ψηφιακή Ευρώπη» της ΕΕ αναδεικνύουν την ανάγκη για εναρμόνιση της ευαισθητοποίησης για την κυβερνοασφάλεια και βελτίωση νέων εξειδικευμένων δεξιοτήτων για την κυβερνοασφάλεια.

1.1 Στόχοι

Οι στόχοι της έκθεσης WP1 είναι οι εξής:

- Ανάλυση των τρεχουσών τάσεων και του προηγμένου επιπέδου της πανεπιστημιακής κοινότητας.
- Ανάλυση των τρεχόντων και μελλοντικών προγραμμάτων σπουδών στην τριτοβάθμια εκπαίδευση στην ΕΕ.
- Ανάλυση των αναγκών του κλάδου ως προς τις δεξιότητες.
- Προσδιορισμός των ελλείψεων ως προς τις δεξιότητες μεταξύ της τριτοβάθμιας εκπαίδευσης και των αναγκών του κλάδου με βάση τις παραπάνω αναλύσεις.

1.2 Διάρθρωση του εγγράφου

Το έγγραφο έχει διαρθρωθεί ως εξής:

- Η Ενότητα 2 παρουσιάζει την ερευνητική μεθοδολογία που χρησιμοποιήθηκε στην παρούσα μελέτη για τη συλλογή των δεδομένων και την ανάλυση του αποτελέσματος, συμπεριλαμβανομένου του πεδίου εφαρμογής της μελέτης.
- Η Ενότητα 3 επεξηγεί την πολιτική της ΕΕ όσον αφορά την κυβερνοασφάλεια στο έξυπνο δίκτυο.
- Η Ενότητα 4 παρουσιάζει την άποψη της πανεπιστημιακής κοινότητας μέσα από μια βιβλιογραφική ανασκόπηση. Η βιβλιογραφική ανασκόπηση αποσκοπεί στον εντοπισμό του προηγμένου επιπέδου και των τρεχουσών τάσεων στην εκπαίδευση για τα

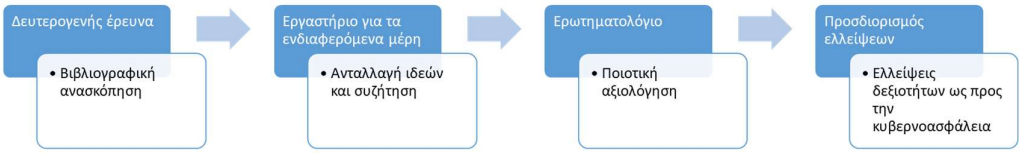
συνδυασμένα πεδία των έξυπνων δικτύων και της κυβερνοασφάλειας.

- Η Ενότητα 5 παρουσιάζει συνοπτικά τα υφιστάμενα εκπαιδευτικά προγράμματα για την κυβερνοασφάλεια, συμπεριλαμβανομένων των προγραμμάτων της τριτοβάθμιας εκπαίδευσης, της συνεχιζόμενης εκπαίδευσης και των MOOC.
- Η Ενότητα 6 προσδιορίζει τον κλάδο και τις ανάγκες του ως προς τις δεξιότητες που απαιτούνται για το προσωπικό του. Ο προσδιορισμός των αναγκών ως προς τις δεξιότητες επιτυγχάνεται μέσω ενός εργαστηρίου για τα ενδιαφερόμενα μέρη και τη διεξαγωγή μιας ειδικής έρευνας.
- Η Ενότητα 7 παρουσιάζει τα χρήσιμα εκπαιδευτικά εργαλεία για την κυβερνοασφάλεια, τα οποία αναλύονται στη βιβλιογραφική ανασκόπηση και στην έρευνα όπου συμμετείχαν ενδιαφερόμενα μέρη.
- Η Ενότητα 8 αναφέρεται αποκλειστικά στο συμπέρασμα και τις αρχικές απαιτήσεις και προτάσεις σχετικά με την κυβερνοασφάλεια για την εκπαίδευση για τα έξυπνα δίκτυα.

Το παρόν έγγραφο ολοκληρώνεται με τα συμπεράσματα και τη βιβλιογραφία.

2. Ερευνητική μεθοδολογία

Προκειμένου να αποκομιστούν βαθύτερες γνώσεις και να επιτευχθεί προηγμένο επίπεδο κυβερνοασφάλειας στα έξυπνα δίκτυα, η βιβλιογραφική ανασκόπηση είναι το πρώτο βήμα για τη συγκέντρωση των ερευνητικών τάσεων και εξελίξεων, της εκπαιδευτικής μεθόδου και των υφιστάμενων προγραμμάτων σπουδών που διατίθενται. Η ερευνητική μεθοδολογία του WP 1 εμφανίζεται στην Εικόνα 1.



Εικόνα 1 Ερευνητική μεθοδολογία του WP1

Η δευτερογενής έρευνα παρέχει μόνο πληροφορίες που βασίζονται σε συγκεκριμένα θέματα και τομείς ανάλογα με το πλαίσιο και τον στόχο της έρευνας. Προκειμένου να παρουσιαστεί μια ευρύτερη εικόνα για τις ελλείψεις στις δεξιότητες ως προς την κυβερνοασφάλεια, ειδικά από την πλευρά του κλάδου, το εργαστήριο για τα ενδιαφερόμενα μέρη είναι απαραίτητο για την ανταλλαγή ιδεών και απόψεων ανάμεσα στην πανεπιστημιακή κοινότητα και στον κλάδο.

3. Πολιτική για την κυβερνοασφάλεια στην Ευρωπαϊκή Ένωση

3.1 Πολιτικές και στρατηγικές κατευθύνσεις της ΕΕ

Η πολιτική για την κυβερνοασφάλεια μπορεί να βοηθήσει το κράτος να χειριστεί τις ουσιώδεις πτυχές που απαιτούνται για την αποτροπή των αρνητικών επιδράσεων των ευπαθειών στην κυβερνοασφάλεια. Η Ευρωπαϊκή Επιτροπή και ο ύπατος εκπρόσωπος της Ένωσης για

θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας έχουν θέσει σε εφαρμογή μια νέα 5ετή στρατηγική για την κυβερνοασφάλεια στην ΕΕ (2020-2025) με σκοπό την ενίσχυση και την προστασία του ψηφιακού μετασχηματισμού των συστημάτων από κυβερνοαπειλές. Επίσης, η στρατηγική δίνει έμφαση στη σημασία του ανθρώπινου δυναμικού εντός της ΕΕ, που διαθέτει δεξιότητες στον τομέα της κυβερνοασφάλειας. Η ετοιμότητα και η ευαισθητοποίηση όσον αφορά την κυβερνοασφάλεια τόσο στις επιχειρήσεις όσο και μεταξύ των ατόμων παραμένουν σε χαμηλά επίπεδα, ενώ υπάρχει σημαντική έλλειψη ανθρώπινου δυναμικού που ασχολείται με την κυβερνοασφάλεια.

Η στρατηγική της ΕΕ για την κυβερνοασφάλεια ευθυγραμμίζει το Αναθεωρημένο σχέδιο για την ψηφιακή εκπαίδευση της ΕΕ [1], το οποίο στοχεύει να αυξήσει την ευαισθητοποίηση των ατόμων για την κυβερνοασφάλεια, ειδικά των παιδιών και των νέων, καθώς και των οργανισμών, ειδικά των μικρομεσαίων επιχειρήσεων. Το σχέδιο έχει δύο προτεραιότητες [1]: την προώθηση ενός οικοσυστήματος ψηφιακής εκπαίδευσης υψηλών επιδόσεων και [2] την ενίσχυση των ψηφιακών δεξιοτήτων και ικανοτήτων για τον ψηφιακό μετασχηματισμό. Προκειμένου να καλυφθεί η αυξανόμενη ζήτηση για ανθρώπινο δυναμικό ICT, οι ειδικοί ασφάλειας ICT με γνώσεις για τη λειτουργία των τομέων ενέργειας έχουν γίνει πιο ανταγωνιστικοί, ενώ ενδέχεται να απαιτήσουν την ενημέρωση των προγραμμάτων σπουδών εκπαίδευσης στους κλάδους μηχανικής και ICT. Επιπλέον, το σχέδιο δράσης για την εκπαίδευση προτείνει την εκπαίδευση και κατάρτιση των ενδιαφερόμενων μερών καθ' όλη τη διάρκεια ισχύος των νέων λύσεων ασφάλειας για τα Έξυπνα δίκτυα. Διατυπώνει ότι τα προγράμματα εκπαίδευσης και κατάρτισης πρέπει να παρέχουν κίνητρα στα ενδιαφερόμενα μέρη, έτσι ώστε να σκέφτονται με διαφορετικούς, καινοτόμους τρόπους και να δοκιμάζουν νέες προσεγγίσεις. Τα προγράμματα εκπαίδευσης και μάθησης πρέπει να εστιάζουν στην ενίσχυση (και στην ανανέωση) της ευαισθητοποίησης, παρέχοντας βαθύτερες γνώσεις και προοπτικές σε ρεαλιστικά σενάρια και αναπτύσσοντας και κάνοντας πειράματα και δοκιμές σε νέες έννοιες (όπως η κυβερνοασφάλεια).

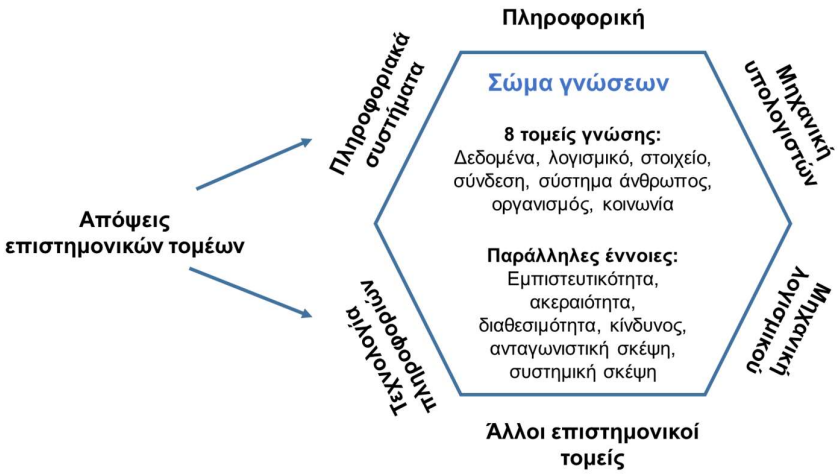
3.2 Οργανισμός σχετικός με την κυβερνοασφάλεια

Ο Οργανισμός της ΕΕ για την κυβερνοασφάλεια (ENISA) ευθύνεται για την κυβερνοασφάλεια στην ΕΕ σύμφωνα με τον Νόμο περί κυβερνοασφάλειας [2]. Ο Νόμος περί κυβερνοασφάλειας ενισχύει τον φορέα ENISA μέσω μόνιμης εξουσίας και συγκεκριμένων πόρων και καθηκόντων, προκειμένου να αυξήσει την επιχειρησιακή δραστηριότητα σε επίπεδο ΕΕ. Ο ENISA έχει την εξουσία να παρέχει υποστήριξη στα κράτη μέλη της ΕΕ για την εφαρμογή της κυβερνοασφάλειας μέσω του ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας [3]. Οι επιχειρήσεις που δραστηριοποιούνται στην ΕΕ θα πρέπει να συμμορφώνονται με τη συγκεκριμένη απαίτηση για τα προϊόντα και τις υπηρεσίες τους σύμφωνα με την οδηγία.

3.3 Μελέτες και προτάσεις για τον κλάδο

Οι ενώσεις κλάδου και οι ομάδες συμφερόντων μελέτησαν την προηγμένη εκπαίδευση για την κυβερνοασφάλεια και ετοίμασαν προτάσεις για τα προγράμματα σπουδών σχετικά με την κυβερνοασφάλεια. Εντούτοις, οι προτάσεις σχετικά με την εκπαίδευση για την κυβερνοασφάλεια στα έξυπνα δίκτυα εξακολουθούν να είναι περιορισμένες. Η Κοινή ομάδα εργασίας για την εκπαίδευση για την κυβερνοασφάλεια απαρτίζεται από πολλές ενώσεις, οι οποίες κατάρτισαν τις Κατευθυντήριες οδηγίες για το πρόγραμμα σπουδών για τα πτυχιακά προγράμματα κυβερνοασφάλειας στη μεταδευτεροβάθμια εκπαίδευση [4]. Η Κοινή ομάδα εργασίας μοιράζεται την άποψη ότι ο πλανήτης είναι αντιμέτωπος με μια τρέχουσα και αυξανόμενη έλλειψη κατάλληλα εκπαιδευμένων επαγγελματιών σε θέματα κυβερνοασφάλειας. Τα προτεινόμενα εκπαιδευτικά προγράμματα για την κυβερνοασφάλεια

εμφανίζονται στην Εικόνα 2.



Εικόνα 2 Μοντέλο σκέψης για το πρόγραμμα σπουδών εκπαίδευσης στην κυβερνοασφάλεια [4]

3.4 Μελέτες και προτάσεις για τον κλάδο

Πρόσφατα, ο τομέας της ενέργειας ξεκίνησε τη διαδικασία του ψηφιακού μετασχηματισμού εισάγοντας έξυπνα δίκτυα που εγείρουν την ανάγκη για επανεκπαίδευση του μεγαλύτερου σε ηλικία ανθρώπινου δυναμικού και την κατάρτιση των νέων εργαζομένων. Μια πλατφόρμα εκπαίδευσης για την προώθηση των θεμάτων ενεργούς μάθησης θα πρέπει να παρέχει τα εξής [5]:

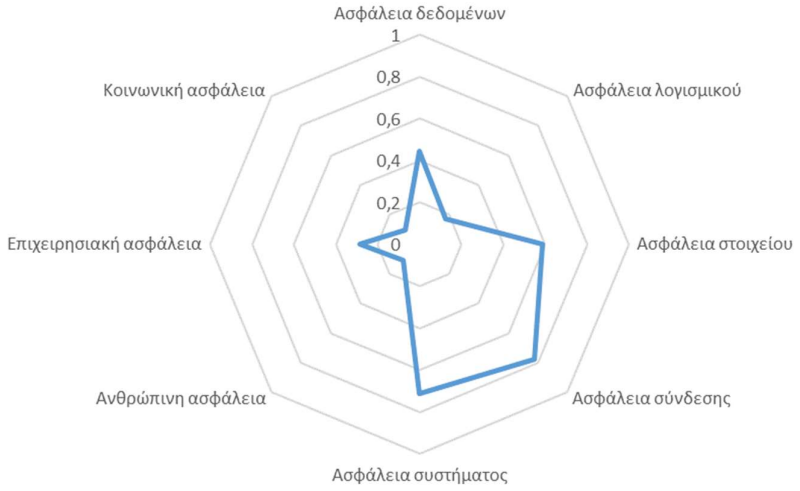
- Υποδομή για την κυβερνοασφάλεια στο δίκτυο ηλεκτρικού ρεύματος,
- Παρακολούθηση και επίγνωση της κατάστασης,
- Προηγμένη υποδομή μέτρησης,
- Έγγραφα καθοδήγησης για το έξυπνο δίκτυο,
- Μοντέλο ωριμότητας ικανοτήτων (Capability maturity model, CMM) για τον τομέα ηλεκτρισμού,
- Ιδιωτικότητα στο έξυπνο δίκτυο,
- Παραδείγματα και επίδραση στις υποδομές ζωτικής σημασίας,
- Μια προοπτική για την ασφάλεια,
- Προκλήσεις σχετικά με την ασφάλεια στον αυτοματισμό διανομής,
- Ενσωματωμένη αξιολόγηση,
- Βασικά στοιχεία συστημάτων SCADA και στιβαρού ελέγχου.

4. Προηγμένο επίπεδο και τάσεις όσον αφορά την κυβερνοασφάλεια στα έξυπνα δίκτυα

4.1 Κατηγοριοποίηση

Οι μηχανές αναζήτησης Google Scholar και Microsoft Academic χρησιμοποιούνται για τη συγκέντρωση των σχετικών μελετών από την περίοδο 2017-2020 χρησιμοποιώντας τις λέξεις-κλειδιά «κυβερνοασφάλεια» και «έξυπνο δίκτυο». Τα αποτελέσματα που εμφανίστηκαν στον

τίτλο αλλά και στο περιεχόμενο των μελετών αντιστοιχούσαν σε περίπου 164 άρθρα. Όλες αυτές οι μελέτες ελέγχονται σε υψηλό επίπεδο προκειμένου να επιλέγονται οι μελέτες που σχετίζονται με την κυβερνοασφάλεια και το έξυπνο δίκτυο. Στη συνέχεια, οι επιλεγμένες μελέτες κατηγοριοποιούνται με βάση το πλαίσιο του ACM για την κυβερνοασφάλεια, όπως εμφανίζεται στην Εικόνα 3. Κάθε επιλεγμένη μελέτη ελέγχεται διεξοδικά προκειμένου να προσδιοριστεί ο σκοπός, η μέθοδος και το αποτέλεσμα της μελέτης. Όσο υψηλότερος είναι ο αριθμός, τόσο περισσότερες μελέτες εστιάζουν στον τομέα. Θα πρέπει να ληφθεί υπ' όψιν το γεγονός ότι μία μελέτη μπορεί να καλύπτει περισσότερες από μία πτυχές.



Εικόνα 3 Κατηγοριοποίηση των ελλείψεων σε δεξιότητες με βάση τη βιβλιογραφική ανασκόπηση

Είναι σαφές ότι η εστίαση στην ασφάλεια των επιχειρήσεων, των ανθρώπων και της κοινωνίας είναι σε πολύ χαμηλό επίπεδο σε σύγκριση με την εστίαση στην ασφάλεια των συστημάτων, των συνδέσεων και των στοιχείων. Η έρευνα για την ασφάλεια της τεχνολογίας, των συστημάτων και των στοιχείων πραγματοποιείται μέσω συγκεκριμένων πλατφορμών διεξαγωγής αυστηρών δοκιμών (testbed) ή/και εργαστηρίων κυβερνο-φυσικών συστημάτων ενέργειας (CPES), προκειμένου οι φοιτητές να εκτελούν πειράματα ή/και να διδάσκονται.

4.2 Ανάπτυξη τεχνολογίας και εκπαίδευσης

4.2.1 Απειλή της κυβερνοασφάλειας στο έξυπνο δίκτυο

Το CPES περιλαμβάνει πολλαπλούς τομείς στους επιστημονικούς κλάδους της μηχανικής και της επικοινωνίας, που απαιτούν συναφή προγράμματα σπουδών και απαραίτητα εργαλεία για τον προσδιορισμό των ευπαθειών. Προκειμένου να αποτραπούν προηγούμενα και νέα περιστατικά κυβερνοεπίθεσης στο μέλλον, η λήψη παθητικών και ενεργητικών αντίμετρων είναι άκρως απαραίτητη. Οι διαχειριστές συστημάτων και οι επαγγελματίες απαιτούν μια ρεαλιστική πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed) για την εξέταση ρεαλιστικών σεναρίων και αντιμέτρων. Οι κυβερνοεπιθέσεις αφορούν συσκευές συνδεδεμένες σε δίκτυο που το λογισμικό τους μολύνεται από λογισμικό κακόβουλης λειτουργίας. Τα τελευταία χρόνια, έχουν σημειωθεί πολυάριθμες κυβερνοεπιθέσεις εναντίον συστημάτων έξυπνου δικτύου. Οι εν λόγω κυβερνοεπιθέσεις μπορεί να πραγματοποιηθούν σκόπιμα ή ασυναίσθητα και επηρεάζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα (CIA). Η διαβάθμιση της κυβερνοεπίθεσης σε συνάρτηση με την πτυχή CIA παρουσιάζεται στον Πίνακα 1.

Πίνακα 1 Διαβάθμιση των κυβερνοεπιθέσεων σε συνάρτηση με CIA

Τύπος κυβερνοεπίθεσης	Σύντομη περιγραφή	Παράδειγμα
Εμπιστευτικότητα	Προστασία των δεδομένων με την πρόληψη της μη εξουσιοδοτημένης γνωστοποίησης πληροφοριών	Επίθεση Man-in-the-Middle, Stuxnet, εκστρατεία ηλεκτρονικού «ψαρέματος», προσθήκη κακόβουλου κώδικα SQL, επίθεση πλευρικού καναλιού, κλιμάκωση προνομίων, επίθεση με AES για χρονισμό υφής μνήμης
Ακεραιότητα	Υποκλοπή και αλλαγή του μηνύματος	Έγχυση ψευδών δεδομένων, επίθεση τροποποίησης φορτίου, εκστρατεία ηλεκτρονικού «ψαρέματος», αλλοίωση
Διαθεσιμότητα	Αποκλεισμός ή καθυστέρηση μηνυμάτων/κυκλοφορίας	DoS/DDoS, ransomware, επίθεση με αποκλεισμό, κλιμάκωση προνομίων, επίθεση με AES για χρονισμό υφής μνήμης, υπερχείλιση buffer

4.2.2 Αντίμετρα

Δεν υπάρχει ένα μόνο αντίμετρο για την αντιμετώπιση όλων των επιθέσεων Κάθε επίθεση απαιτεί αντίμετρα που σχετίζονται με το γενικό πλαίσιο της επίθεσης. Ποικίλες έρευνες σχετικά με την κυβερνοασφάλεια στα έξυπνα δίκτυα υπέδειξαν την εφαρμογή κοινών αντιμέτρων, όπως το σύστημα ανίχνευσης εισβολής (IDS), οι αποστρατικοποιημένες ζώνες (DMZ), οι μετρητές απόδοσης υλικού (HPC), η μανδάλωση, η διαχείριση αρχείου καταγραφής, ο έλεγχος ταυτότητας πολλών παραγόντων, η ενεργή παρακολούθηση δικτύου, η διεύθυνση IP και η λίστα επιτρεπόμενων εφαρμογών, η τμηματοποίηση δικτύου και οι έξυπνοι διακόπτες/δρομολογητές, η εκπαίδευση ευαισθητοποίησης για την ασφάλεια.

4.2.3 Εργαστήριο κυβερνο-φυσικών συστημάτων ενέργειας (CPES)

Μέχρι σήμερα, τα πανεπιστήμια, η κυβέρνηση και ο κλάδος έχουν διαμορφώσει πλατφόρμες διεξαγωγής αυστηρών δοκιμών (testbed) για διεξαγωγή πειραμάτων έρευνας και ανάπτυξης για την κυβερνοασφάλεια. Τα θέματα κυβερνοασφάλειας είναι σύνθετα και περιλαμβάνουν γνώσεις από ποικίλους τομείς, π.χ. τεχνολογία υπολογιστών, ηλεκτρομηχανική, βιομηχανική μηχανική. Η συσχέτιση των τομέων δίνει στους επαγγελματίες τη δυνατότητα να κατανοούν και να έχουν ευρύτερη γενική εικόνα σχετικά το πώς σχετίζονται οι διαφορετικοί τομείς. Η πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed), που αφορούν πολλούς σκοπούς και τομείς, περιλαμβάνει μεγαλύτερο πλεονέκτημα σε σύγκριση με τον μεμονωμένο σκοπό ή/και τομέα. Μια απλή και χαμηλού κόστους πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed) επιτρέπει στους προπτυχιακούς φοιτητές να αναπαραγάγουν και να εξερευνούν τη θεμελιώδη αρχή της κυβερνοασφάλειας. Ένα υπερσύγχρονο εργαστήριο έχει υψηλό κόστος, ενώ η συνεργασία ανάμεσα στον κλάδο και στο πανεπιστήμιο μπορεί να επιταχύνει την προηγμένη, καινοτόμα έρευνα.

4.2.4 Πρωτόκολλα επικοινωνίας

Η έρευνα και η εκπαίδευση για την κυβερνοασφάλεια εστιάζει, επίσης, στα πρωτόκολλα επικοινωνίας ανάμεσα στις συσκευές ή/και στα συστήματα. Τα πρωτόκολλα υποβάλλονται σε δοκιμές στο εργαστήριο και σε συγκεκριμένη πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed). Όσον αφορά οποιαδήποτε μετάδοση δεδομένων μέσα σε ένα δίκτυο, η εφαρμογή τυπικών πρωτοκόλλων που θέτουν ορισμένους κανόνες για την επικοινωνία έχει ουσιώδη σημασία. Υπάρχουν πολλά πρωτόκολλα επικοινωνίας που έχουν χρησιμοποιηθεί στο έξυπνο δίκτυο με βάση τον χρόνο αναμονής, την αξιοπιστία, η ταχύτητα δεδομένων, η κλιμάκωση και

η ασφάλεια. Το IEC 61850 επιτρέπει τη διαλειτουργικότητα ανάμεσα σε διαφορετικά στοιχεία και λειτουργίες που προέρχονται από διαφορετικούς κατασκευαστές.

Καθώς το IEC 61850 γίνεται πιο δημοφιλές στα αυτόματα συστήματα ενέργειας εξαιτίας της ευκολίας σύνδεσης μέσω ethernet και δομών τυποποιημένων μηνυμάτων, εντοπίστηκαν ευπάθειες ως προς την απόκτηση πρόσβασης σε εμπιστευτικά δεδομένα και τη διακοπή υπηρεσιών λόγω της ακεραιότητας της ανταλλαγής δεδομένων. Προκειμένου να ενισχυθεί η κυβερνοασφάλεια για τις επικοινωνίες ανάμεσα στα δίκτυα ενέργειας, το πρότυπο IEC 62351 μπορεί να παρέχει ολοκληρωμένη ασφάλεια πληροφοριών για τις λειτουργίες ελέγχου των συστημάτων ενέργειας. Προσδιορίζει τις διαφορετικές απαιτήσεις για ασφαλή επικοινωνία και επεξεργασία δεδομένων στα συστήματα ενέργειας. Το πρότυπο IEC 62351 εστιάζει την ασφάλεια των πρωτοκόλλων IEC TC 57 που υποστηρίζουν τον έλεγχο ταυτότητας και την κρυπτογράφηση. Το IEC 62351 μπορεί να προσφέρει προστασία για τα μηνύματα IEC61850, όπως τα GOOSE, SV, R-GOOSE, R-SV.

4.3 Ανάλυση των ελλείψεων

Το σύστημα ενέργειας είναι σύνθετο και περιλαμβάνει διαφορετικές συσκευές και πρωτόκολλα. Η πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed) που αναπτύχθηκε από το πανεπιστήμιο είναι ανεπαρκής κυρίως ως προς την πρακτική σε πραγματικές συνθήκες του κλάδου. Προκειμένου να εκπαιδευτούν οι φοιτητές και οι επαγγελματίες, η πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed) πρέπει να δημιουργηθεί και να εξοπλιστεί με ενσωματωμένα στοιχεία και ρεαλιστικό περιβάλλον για τη διεξαγωγή ολιστικών πειραμάτων σε πολλούς τομείς. Η σύνοψη της ανάλυσης των ελλείψεων για το υφιστάμενο εργαστήριο CPES ή/και η πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed) εμφανίζονται στον Πίνακας 2.

Πίνακας 2 Ανάλυση ελλείψεων για υφιστάμενο εργαστήριο CPES/πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed)

Πτυχή	Ανάλυση έλλειψης
Σκοπός	Περιορισμένη ανάλυση μεμονωμένου τομέα είτε σε σύστημα ενέργειας είτε σε δίκτυο επικοινωνίας
Πιστότητα	Πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed) μόνο για προσομοίωση Έλλειψη εις βάθος γνώσεων για το στοιχείο ICS, τη φυσική διαδικασία και την υλοποίηση στην πράξη
Προσβασιμότητα	Μόνο φυσική πρόσβαση Έλλειψη υποστήριξης της διεπαφής πλατφόρμας
Ευελιξία	«Αδιαλλαξία» όσον αφορά την επιλογή ανάμεσα στην προσομοίωση και τη φυσική διαδικασία Αδυναμία διαμόρφωσης του πραγματικού στοιχείου λόγω του ιδιόκτητου πρωτοκόλλου Έλλειψη ικανότητας ενσωμάτωσης διαφορετικών προσομοιωτών
Κλιμάκωση	Έλλειψη της ικανότητας κλιμάκωσης του πειράματος λόγω των περιορισμένων πόρων
Φιλικότητα προς τον χρήστη	Πολλά εργαλεία προγραμματισμού Έλλειψη GUI
Οικονομική αποδοτικότητα	Υψηλό κόστος επένδυσης για πραγματικές/φυσικές συσκευές και στοιχεία
Επαναληψιμότητα	Χαμηλός βαθμός λεπτομέρειας στο αρχιτεκτονικό σχέδιο της πλατφόρμας διεξαγωγής αυστηρών δοκιμών (testbed) όσον αφορά την επαναληψιμότητα και την αξιοπιστία Αμφιβολία για τη μέτρηση Αδυναμία επανάληψης εξαιτίας της ιδιόκτητης ρεαλιστικής διαδικασίας κλάδου
Πρότυπο και πρωτόκολλο	Έλλειψη υποστήριξης των διαφόρων πρωτοκόλλων υλικού και επικοινωνίας

Πτυχή	Ανάλυση έλλειψης
	Απαιτείται καινοτόμα πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed) για ICS, που συνδυάζεται με νέα και παλαιά πρωτόκολλα Απουσία πύλης και πραγματικών συσκευών IoT
Γνώση	Έλλειψη διεπιστημονικού υποβάθρου, καθώς περιορίζεται στη μηχανική ή στην ηλεκτρομηχανική

Με βάση τα περιστατικά κυβερνοασφάλειας που έχει βιώσει ο πλανήτης μέχρι στιγμής, οι τεχνικές ικανότητες των παραγόντων απειλής έχουν εξελιχθεί σημαντικά. Ως εκ τούτου, οι κρίσιμες υποδομές στο έξυπνο δίκτυο πρέπει να έχουν τη δυνατότητα να ανιχνεύουν μια κυβερνοαπειλή και να ανακάμπτουν από αυτήν. Πίνακας 3 προσδιορίζει τις ελλείψεις ως προς την κυβερνοασφάλεια στο CPES σύμφωνα με την εφαρμογή CPES.

Πίνακας 3 Κίνδυνοι κυβερνοασφάλειας στο CPES

Τομέας/Εφαρμογή	Κίνδυνος κυβερνοασφάλειας
Προστασία ορίων	- Μη εξουσιοδοτημένη δραστηριότητα σε που δεν εντοπίστηκε σε συστήματα κρίσιμης σημασίας - Λιγότερο ισχυρά όρια ανάμεσα σε ICS και δίκτυα επιχειρήσεων.
Κατανομή πόρων	- Δεν υπάρχει εναλλακτικό ή εφεδρικό προσωπικό για την επάνδρωση της θέσης σε περίπτωση αδυναμίας εργασίας του κύριου προσωπικού - Απώλεια σημαντικών γνώσεων για τα συστήματα ελέγχου
Διαχείριση λογαριασμού	- Επικοινωνίες με μη ασφαλείς κωδικούς πρόσβασης που έχουν παραβιαστεί - Η παραβίαση του κωδικού πρόσβασης θα μπορούσε να επιτρέψει αξιόπιστη μη εξουσιοδοτημένη πρόσβαση στα συστήματα
Ταυτοποίηση και έλεγχος ταυτότητας	- Έλλειψη ανάληψης ευθύνης και δυνατότητας εντοπισμού των ενεργειών του χρήστη σε περίπτωση παραβίασης ενός λογαριασμού - Αυξημένη δυσκολία σε λογαριασμούς ασφαλείας όταν το προσωπικό φεύγει από τον οργανισμό, κάτι ιδιαίτερα ευαίσθητο όσον αφορά τους χρήστες που έχουν πρόσβαση με δικαιώματα διαχειριστή.
Έλεγχος φυσικής πρόσβασης	- Η μη εξουσιοδοτημένη φυσική πρόσβαση σε εξοπλισμό και τοποθεσίες για το πεδίο παρέχει αυξημένες ευκαιρίες για: o Κακόβουλη τροποποίηση, διαγραφή ή αντιγραφή προγραμμάτων και υλικολογισμικού συσκευών o Πρόσβαση στο δίκτυο ICS o Κλοπή ή βανδαλισμός των περιουσιακών στοιχείων κυβερνοχώρου - Προσθήκη παραπλανητικών συσκευών για την καταγραφή και αναμετάδοση της κίνησης δικτύου
Ελάχιστη λειτουργικότητα	- Αυξημένα διανύσματα επίθεσης για κακόβουλη πρόσβαση σε συστήματα ζωτικής σημασίας. - Πραγματοποίηση παραπλανητικής εσωτερικής πρόσβασης

5. Προηγμένη εκπαίδευση για τα έξυπνα δίκτυα και την κυβερνοασφάλεια

5.1 Προγράμματα σπουδών τριτοβάθμιας εκπαίδευσης

Εξετάστηκαν συνολικά 84 πανεπιστήμια που προσφέρουν προγράμματα σπουδών τεχνολογίας πληροφοριών, τα οποία σχετίζονται με την ασφάλεια. Από 14 από τα 84 πανεπιστήμια, που περιλαμβάνονται στον κατάλογο, δεν εμπίπτουν στα γενικά κριτήρια. Εντούτοις, συγκεκριμένα κριτήρια προγραμμάτων σπουδών για την κυβερνοασφάλεια, όπως τα προγράμματα τεχνολογίας πληροφοριών, πληροφορικής ή συστημάτων υπολογιστών, δεν παρέχουν εμπεριστατωμένες γνώσεις για την κυβερνοασφάλεια. Η τεχνική εξέλιξη στην εκπαίδευση για την κυβερνοασφάλεια επιταχύνεται αλλά, σε γενικές γραμμές, η προσαρμογή των προγραμμάτων σπουδών ενός πανεπιστήμιο διεξάγεται με αργό ρυθμό. Η γεφύρωση του χάσματος ανάμεσα στις ανάγκες του κλάδου και τα εκπαιδευτικά αποτελέσματα, σε συνάρτηση με τους μελλοντικούς ερευνητές και μηχανικούς, είναι πάντα μια πρόκληση. Μια από τις κύριες ενέργειες είναι να εξετάζεται τακτικά το πρόγραμμα σπουδών για να βελτιωθεί η ενημέρωση του ηλεκτρονικού περιεχομένου και των μεθόδων διδασκαλίας.

5.2 Συνεχιζόμενα εκπαιδευτικά προγράμματα

Τα υφιστάμενα προγράμματα επαγγελματικής κατάρτισης [6] έχουν σκοπό να προετοιμάσουν τους φοιτητές και τους επαγγελματίες για σταδιοδρομία στον αναδυόμενο τομέα της κυβερνοασφάλειας στα έξυπνα δίκτυα. Τα ποικίλα εξειδικευμένα μαθήματα πιστοποίησης παρέχουν τη δυνατότητα αύξησης των ικανοτήτων και των δεξιοτήτων των ειδικών και προσφέρουν συγκεκριμένο εύρος γνώσεων. Μια μελέτη [7] έδειξε ότι, πολλές χώρες, προσφέρουν υψηλότερη κάλυψη των μονάδων γνώσης. Για παράδειγμα, κατά την εξέταση των ποσοστών κάλυψης, η Ισπανία, η Γαλλία, η Γερμανία και η Ιταλία καλύπτουν το 75% των μονάδων γνώσης (KU) με υποχρεωτικά μαθήματα. Εντούτοις, το μέγεθος της χώρας δεν αποτελεί καθοριστικό παράγοντα [7]. Η διαθεσιμότητα και η προώθηση των διαφόρων επαγγελματικών πρακτικών είναι δυνατόν να παρατηρηθούν, πράγμα που επιτρέπει τη διεύρυνση των γνώσεων και την ενίσχυση της συγκεκριμένης εμπειρίας σε τεχνικά θέματα που απαιτούνται από τον κλάδο σε γενικές γραμμές.

5.3 Μαζικά ανοιχτά διαδικτυακά μαθήματα (MOOC)

Τα διαδικτυακά μαθήματα γίνονται ολοένα πιο δημοφιλή επειδή είναι προσιτά σε περισσότερα άτομα. Υπάρχουν διαθέσιμα διαδικτυακά μαθήματα που αφορούν στην κυβερνοασφάλεια και πραγματοποιούνται μέσω edX. Εντούτοις, τα διαθέσιμα εκπαιδευτικά μαθήματα για την κυβερνοασφάλεια οργανώνονται με βάση το θέμα και όχι με βάση τα εργαλεία που χρησιμοποιούνται, πράγμα που δυσκολεύει τους εκπαιδευόμενους να εφαρμόσουν στην πράξη συγκεκριμένες γνώσεις για την κυβερνοασφάλεια. Το μαζικό ανοιχτό διαδικτυακό μάθημα (MOOC) εξακολουθεί να έχει περιθώρια ανάπτυξης των δυνατοτήτων του όσον αφορά την κατάρτιση στην κυβερνοασφάλεια και στα έξυπνα δίκτυα. Αυτό είναι δυνατόν να επιτευχθεί με την παροχή πρακτικών παραδειγμάτων που προσφέρουν στους εκπαιδευόμενους την ευκαιρία να αποκομίσουν εμπειρίες σε πραγματικά εργαστήρια, δηλαδή σε ρεαλιστικές προσομοιώσεις.

6. Προσδιορισμός των ελλείψεων δεξιοτήτων στην κυβερνοασφάλεια στα έξυπνα δίκτυα

Προκειμένου να επιτευχθεί η βελτίωση της κατανόησης μιας ρεαλιστικής κατάστασης στον κλάδο και στην ακαδημαϊκή κοινότητα, πραγματοποιήσαμε ένα εικονικό εργαστήριο για να παρουσιάσουμε τα αποτελέσματα της βιβλιογραφικής ανασκόπησης και ένα γενικό πλαίσιο για συζήτηση σχετικά με τα απαραίτητα εργαλεία και δεξιότητες όσον αφορά το θέμα της κυβερνοασφάλειας στον τομέα της ενέργειας. Πίνακας 4 παρουσιάζει το αποτέλεσμα του εργαστηρίου για τα ενδιαφερόμενα μέρη. Οι προτάσεις που συγκεντρώθηκαν από το εργαστήριο υποδεικνύουν ότι η βασική γνώση σχετικά με την κυβερνοασφάλεια σε διαφορετικούς τομείς (π.χ. επικοινωνία δικτύων, υποδομή ζωτικής σημασίας), η αυξημένη πρακτική εμπειρία και η εργασία με διαφορετικά εργαλεία για την κυβερνοασφάλεια είναι απαραίτητα εφόδια για την πανεπιστημιακή κοινότητα. Είναι σημαντικό να αναφερθεί ότι η διδασκαλία και η παρουσίαση της θεωρίας στα προγράμματα σπουδών για την κυβερνοασφάλεια δεν αρκούν για τους φοιτητές που επιδιώκουν να εργαστούν μελλοντικά στον κλάδο.

Πίνακας 4 Πρόταση από το εργαστήριο για τα ενδιαφερόμενα μέρη [8]

Τομέας	Έναρξη	Συνέχεια	Περισσότερες ενέργειες	Λιγότερες ενέργειες
Ακαδημαϊκή κοινότητα	• Συνδυασμός των γνώσεων για την υποδομή των συστημάτων ενέργειας και επικοινωνίας. • Σχεδιασμός, ανάπτυξη και προδραστική παρακολούθηση των μέτρων και των πολιτικών για την κυβερνοασφάλεια. • Κατανομή μεγαλύτερου προϋπολογισμού για έρευνα.	• Πλατφόρμα διεξαγωγής αυστηρών δοκιμών (testbed). • Απαραίτητα εργαλεία ανάπτυξης και ελέγχου • Γνώσεις για την κυβερνοασφάλεια σε πολλούς τομείς (π.χ. σημαντικές υποδομές, συστήματα επικοινωνίας, συστήματα ενέργειας). • Πρακτική εμπειρία.	• Γνώση του στοιχείου στο σύστημα ενέργειας (RTU, IED, PMU). • Διεξαγωγή έρευνας διεθνούς επιπέδου για την κυβερνοασφάλεια. • Επαγγελματική κατάρτιση • Πιστοποιητικά (π.χ CISM/CISSP/CISA/CEH)	• Μόνο θεωρία
Βιομηχανία	• Βαθιά κατανόηση των διαφόρων τύπων απειλών για την ασφάλεια	• Αυτοδιδασκαλία. • Κατανόηση πολλών τομέων (π.χ. συστήματα ενέργειας, δίκτυο επικοινωνίας). • Μηδενικό επίπεδο εμπιστοσύνης	• Αυτοδιδασκαλία. • Γνώση των ευπαθειών του συστήματος ενέργειας και του δικτύου επικοινωνίας. • Διαχειρίσιμες οριζόντιες δεξιότητες. • Εκμάθηση νέων τεχνολογιών • Γνώση των πιο δημοφιλών πλατφορμών SCADA. • Περιπτώσεις χρήσης στην πράξη • Βασικά εργαλεία για την ανάλυση απειλής.	-

7. Προσδιορισμός των χρήσιμων εργαλείων για την εκπαίδευση στην κυβερνοασφάλεια στα έξυπνα δίκτυα

7.1 Βασικά εργαλεία για ενεργή μάθηση σχετικά με την κυβερνοασφάλεια

Υπάρχουν πολλές προσεγγίσεις για τη διάδοση της γνώσης που μπορούν να χρησιμοποιηθούν στα πεδία της κυβερνοασφάλειας γενικά αλλά, ειδικά, στα έξυπνα δίκτυα. Πίνακας 5 παρουσιάζει τις εκπαιδευτικές προσεγγίσεις για τα έξυπνα δίκτυα και την κυβερνοασφάλεια με σκοπό την οικοδόμηση εμπεριστατωμένης γνώσης και κατανόησης των κύριων εννοιών που σχετίζονται με το πεδίο, καθώς τις αναλυτικές δεξιότητες που απαιτούνται για περαιτέρω εξέλιξη.

Πίνακας 5 Εκπαιδευτικές προσεγγίσεις ως προς τα έξυπνα δίκτυα και την κυβερνοασφάλεια

Προσέγγιση	Σκοπός	Παραδείγματα εργαλείων
Εργαστήρια εξ αποστάσεως και εικονικά εργαστήρια	αυτοδιδασκαλία και για δημιουργία αλληλεπίδρασης που πλησιάζει την εμπειρία της αληθινής τάξης	Labview, OMWeb, NI ELVIS, Labster, LabAlive
Επαυξημένη πραγματικότητα	αλληλεπιδραστική μάθηση	Worklink, CoSpaces, Merge Cube
Απεικόνιση δεδομένων	απεικόνιση και ανάλυση	Tableau, Microsoft Power Bi, IBM Congos Analytics
Cloud computing	προηγμένοι αλγόριθμοι και λειτουργίες, όπως η εξόρυξη δεδομένων και η μάθηση σε βάθος	Google Classroom, Microsoft Education Center, Amazon Web Services
Αντίστροφη μάθηση	ενεργή μάθηση για τη μηχανική	Massive Open Online Courses (MOOC)
Παιχνιδοποίηση και θεωρία παιγνίων	ανάλυση πιθανοτήτων και σεναρίων κυβερνοασφάλειας	Kahoot, Gimkit
Προσομοίωση	εξάσκηση και δοκιμή διαφορετικών περιπτώσεων	MATLAB, Simulink

7.2 Προηγμένα εργαλεία για πειράματα με ευπάθειες

Το σύστημα έξυπνου δικτύου είναι σύνθετο καθώς ενσωματώνει το δίκτυο ενέργειας και τα δίκτυα επικοινωνίας. Τα τελευταία χρόνια τα συστήματα έξυπνων δικτύων έχουν δεχτεί πολλές κυβερνοεπιθέσεις, οι οποίες έχουν προκαλέσει σοβαρές συνέπειες. Οι οχλήσεις είναι εγγενώς σύνθετες και μπορούν να αποδοθούν σε ευρύ φάσμα αιτιών, συμπεριλαμβανομένων των φυσικών συμβάντων και των συμβάντων που προκλήθηκαν από ανθρώπους. Πίνακας 6 δείχνει τα προηγμένα εργαλεία ταξινομημένα βάσει των λειτουργιών τους για την αντιμετώπιση των ευπαθειών και τον πειραματισμό με αυτές.

Πίνακας 6 Εργαλεία κυβερνοασφάλειας για έξυπνα δίκτυα

Εργαλείο	Λειτουργία
Πλατφόρμα ασφάλειας	Ενοποιημένη διαχείριση της ασφάλειας για παροχή κεντρικού ελέγχου και εκτέλεση ενεργειών για την αντιμετώπιση απειλών που επηρεάζουν την υποδομή μιας επιχείρησης
Παρακολούθηση δικτύου	Για την παρακολούθηση της ποιότητας του δικτύου για την αντιμετώπιση οποιασδήποτε αστοχίας ή διακοπής και, ως εκ τούτου, για τη διασφάλιση της συνέχειας και του επιπέδου απόδοσης
Ανίχνευση ευπαθειών	Για σάρωση διαφορετικών συστημάτων και στοιχείων λογισμικού που υποβάλλονται σε δοκιμή για τον εντοπισμό ελαττωμάτων και αδυναμιών που μπορεί να γίνουν αντικείμενο εκμετάλλευσης
Δοκιμή παρείσδυσης	Για αξιολόγηση της ασφάλειας των συστημάτων μέσω της εκμετάλλευσης ευπαθειών που εντοπίστηκαν
Packet sniffer και port scanner	Για παρακολούθηση της κίνησης δικτύου, προσδιορισμό εκτέλεσης υπηρεσιών και αξιολόγηση των πολιτικών για την ασφάλεια
Κρυπτογράφηση	Για διατήρηση της εμπιστευτικότητας και της συνοχής των πληροφοριών, προστατεύοντας, ως εκ τούτου, τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση
Προστασία από ιούς	Για ανίχνευση και λήψη μέτρων κατά κακόβουλου λογισμικού και άλλου παράνομου λογισμικού, όπως το ransomware, το works, οι δούρειοι ίπποι κ.λπ.
Τείχη προστασίας	Για παροχή προστασίας από επιθέσεις εμποδίζοντας το κακόβουλο λογισμικό να εισέλθει σε ορισμένα δίκτυα ή έξυπνες συσκευές
Ασύρματη ασφάλεια	Για αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε ένα ασύρματο δίκτυο, καθώς και για προστασία της κίνησης που μεταδίδεται διασφαλίζοντας υψηλό επίπεδο κρυπτογράφησης δεδομένων
Διαχείριση κωδικού πρόσβασης	Για ασφαλή έλεγχο των λογαριασμών

Τα υφιστάμενα προηγμένα εργαλεία καλύπτουν κυρίως τα τεχνικά ζητήματα που σχετίζονται με φυσικά κυβερνοσυστήματα. Τα προηγμένα εργαλεία θα πρέπει να μπορούν να αντιμετωπίζουν τις αντίστοιχες λανθασμένες απειλές που δεν έχουν αναγνωριστεί σωστά, καθώς και τον πιο αργό εντοπισμό και χρόνο απόκρισης. Αυτό θα συμβάλλει στην εκπαίδευση των φοιτητών προκειμένου να έχουν πρακτική εμπειρία μέσα από την ενεργή μάθηση.

8. Συμπέρασμα και προτάσεις

Η εκπαίδευση για την κυβερνοασφάλεια έχει αναγνωριστεί ως μία από τις στρατηγικές ψηφιακές δεξιότητες στο πλαίσιο της ΕΕ, οι οποίες πρέπει να εναρμονιστούν με την παροχή επίσημης και ανεπίσημης εκπαίδευσης (όπως η VET, συνεχιζόμενη εκπαίδευση) και της πρακτικής εφαρμογής θεμάτων (πρακτική) σε προγράμματα έρευνας και ανάπτυξης σε επιχειρήσεις. Η κυβερνοασφάλεια αντιπροσωπεύεται σε διαφορετικές μορφές εκπαίδευσης, όπως στην τριτοβάθμια εκπαίδευση, στη συνεχιζόμενη εκπαίδευση και στα MOOC. Οι κύριες απαιτήσεις για τη βελτίωση των προγραμμάτων σπουδών για την κυβερνοασφάλεια για την ανάπτυξη των έξυπνων δικτύων έχουν ως εξής:

- Η εκπαίδευση πρέπει να είναι προσβάσιμη για όλες τις διαφορετικές ομάδες πολιτών της ΕΕ (συμπεριλαμβανομένων των επιχειρήσεων, των ηγετικών στελεχών, των

ενηλίκων που θέλουν να βελτιώσουν τις δεξιότητές τους και να αποκτήσουν νέες, καθώς και των νέων ειδικών).

- Συνιστάται να παρέχονται ευκαιρίες μάθησης για την κυβερνοασφάλεια, τόσο εξ αποστάσεως και διαδικτυακά, όσο και μικτές ευκαιρίες μάθησης, προκειμένου η βελτίωση των δεξιοτήτων και η απόκτηση νέων δεξιοτήτων να είναι πιο προσιτή στους ενηλίκους.
- Η εκπαίδευση πρέπει να καλύπτει τα γενικά πεδία κυβερνοασφάλειας και τα θέματα που αφορούν ειδικά στον κλάδο (όπως η κυβερνοασφάλεια της εφοδιαστικής αλυσίδας ενέργειας και τα εργαλεία/οι μέθοδοι και τα μέτρα για την παρακολούθηση και τον έλεγχό της).
- Πρέπει να παρέχει θεωρητικές διαλέξεις και πρακτική κατάρτιση, όπως η χρήση των εργαλείων διαχείρισης της κυβερνοασφάλειας και τα εικονικά εργαστήρια, καθώς και η εκτέλεση προσομοιώσεων και πειραμάτων χρησιμοποιώντας ψηφιακά δίδυμα και παρόμοια περιβάλλοντα. Στην εκπαίδευση για την κυβερνοασφάλεια στα έξυπνα δίκτυα, τα ειδικά εργαλεία που σχετίζονται με την κυβερνοασφάλεια στα έξυπνα δίκτυα, όπως τα εργαλεία παρακολούθησης των χειριστηρίων ενεργητικών τομέων, είναι απαραίτητα.
- Τα προγράμματα εκπαίδευσης και κατάρτισης πρέπει να αναπτύσσονται σε συνεργασία με σχετικούς συνεργάτες (όπως τα πανεπιστήμια και οι εκπρόσωποι του κλάδου).
- Όσον αφορά τα προγράμματα για την κυβερνοασφάλεια στα έξυπνα δίκτυα, θα πρέπει να δίνεται προσοχή σε όλους αυτούς τους παρακάτω τομείς, όπως [9]: Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα (συμπεριλαμβανομένης της απόδοσης και της έγκαιρης εκτέλεσης ενεργειών), καθώς και η προστασία των προσωπικών δεδομένων (ο συνδυασμός της οργάνωσης, της ακεραιότητας και της εμπιστευτικότητας) και η μη αποκήρυξη της ταυτότητας (π.χ. συμβάσεις σε ηλεκτρονική μορφή). Επομένως, το πεδίο εφαρμογής περιλαμβάνει πολύ περισσότερα από την ασφάλεια των δεδομένων, εφόσον η ασφάλεια των δεδομένων είναι μία από τις πτυχές της ασφάλειας (αλλά σημαντική), ενώ εφαρμόζονται τα έξυπνα δίκτυα στην Ευρώπη.
- Τα θέματα της κυβερνοασφάλειας θα πρέπει να ενσωματώνονται ως υποχρεωτικό μέρος των προγραμμάτων σπουδών για την ενέργεια.
- Προκειμένου η εκπαίδευση για την κυβερνοασφάλεια να γίνει πιο αλληλεπιδραστική και ελκυστική για τους φοιτητές, συνιστάται η ενσωμάτωση στοιχείων παιχνιδοποίησης, όπως τα παιχνίδια απειλής, τα εικονικά περιβάλλοντα κυβερνοτεχνολογίας και τα δωμάτια απόδρασης κυβερνοασφάλειας.
- Οι δομές προσομοίωσης σε πραγματικό χρόνο και τα σενάρια πρακτικής εφαρμογής θα πρέπει να παρέχονται στους φοιτητές, καθώς και να είναι διαθέσιμα τα βασικά και προηγμένα εργαλεία για ενεργή μάθηση.
- Στο πλαίσιο της σχετικά ανώτερης εκπαίδευσης για την κυβερνοασφάλεια, η κινητικότητα των φοιτητών θα πρέπει να θεωρείται μέρος των προγραμμάτων.

9. Βιβλιογραφία

[1] The European Commission, The Revised Digital Education Action Plan. The European Commission, 2020.

[2] The European Parliament, “Cybersecurity act,” 2019.

[3] The European Commission, The EU cybersecurity certification framework.

[4] J. T. F. on Cybersecurity Education, Curriculum Guidelines for Post- Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, 2017.

[5] Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) https://tcipg.org/.

[6] T. Yardley, S. Uludag, K. Nahrstedt, and P. Sauer, “Developing a smart grid cybersecurity education platform and a preliminary assessment of its first application,” in 2014 IEEE Frontiers in Education Conference (FIE) Proceedings, 2014.

[7] N. Dragoni, A. Lluch Lafuente, F. Massacci and A. Schlichtkrull, "Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]," in IEEE Security & Privacy, vol. 19, no. 1, pp. 81-88, Jan.-Feb. 2021, doi: 10.1109/MSEC.2020.3037446

[8] B. Siemers et al., "Modern Trends and Skill Gaps of Cyber Security in Smart Grid: Invited Paper," IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, 2021, pp. 565-570, doi: 10.1109/EUROCON52738.2021.9535632.

[9] The European Commission, European Commission Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids. European Commission, 2019.