



CyberSecPro

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training



Co-funded by
the European Union

Προστασία σταθμών φόρτισης από συγκεκριμένες απειλές - Protecting Charging Stations Against Specific Threats

CSP008_S_E

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟ:

- CRISTINA ALCARAZ , UNIVERSITY OF MALAGA, SPAIN
- ABDELKADER SHAABAN, AIT, AUSTRIAN
- STEFAN SCHAUER, AIT, AUSTRIAN
- ELIAS ATHANASOPOULOS , UNIVERSITY OF CYPRUS , CYPRUS





Co-funded by
the European Union

Αναγνώριση

Συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση. Οι απόψεις και οι γνώμες που εκφράζονται είναι, ωστόσο, μόνο του/των συγγραφέα/ων και δεν αντικατοπτρίζουν απαραίτητα εκείνες της Ευρωπαϊκής Ένωσης ή του HADEA. Ούτε η Ευρωπαϊκή Ένωση ούτε η χορηγούσα αρχή μπορούν να θεωρηθούν υπεύθυνες γι' αυτές.

Project Agreement no. 101083594



Προστασία σταθμών φόρτισης από συγκεκριμένες απειλές

01. Στόχοι: Ποιος-Τι-Γιατί χρειάζεται να παρακολουθήσετε αυτήν την

εκπαίδευση

02. Πρόοδος Εκπαίδευσης: Πότε-Που-Πως

03. Μαθησιακά Αποτελέσματα

04. Περιγράμματα Εκπαίδευσης

05. Λεπτομέρειες Ασκήσεων

06. Πρακτικές πληροφορίες και απαιτήσεις

07. Πληροφορίες εγγραφής και στοιχεία επικοινωνίας

Στόχοι: Ποιος-Τι-Γιατί πρέπει να παρακολουθήσετε αυτήν την εκπαίδευση

ΠΟΙΟΣ

Όλοι όσοι ενδιαφέρονται να μάθουν για την κυβερνοασφάλεια των υποδομών φόρτισης, όπως ο CISO, ο αρχιτέκτονας κυβερνοασφάλειας, οι ερευνητές και οι διαχειριστές κινδύνου, μεταξύ άλλων

ΤΙ

Θέτει τη βάση (αν και σε προχωρημένο επίπεδο) για την κατανόηση της σημασίας της κυβερνοασφάλειας σε έναν συγκεκριμένο τομέα του ενεργειακού τομέα

ΓΙΑΤΙ

Εξοπλισμός των συμμετεχόντων με τις απαραίτητες γνώσεις και δεξιότητες για να χαράξουν μια στρατηγική για την προστασία κρίσιμων συστημάτων, δεδομένων και βασικών πόρων, όπως ο έλεγχος και η ισχύς

CSP Πρόοδος Εκπαίδευσης:

Πότε-Που-Πως

ΠΟΤΕ

Καθώς η ενότητα διεξάγεται αρκετές φορές, συνιστάται να ελέγχετε την πλατφόρμα CyberSecPro DCM για ενημερωμένες πληροφορίες, συνολικά 4 ώρες με ένα διάλειμμα (περίπου 30 λεπτά).

ΠΟΥ

Διαδικτυακά, φυσικά ή και τα δύο. Όλες οι πληροφορίες σχετικά με τον τρόπο σύνδεσης θα δημοσιευτούν στο σύστημα DCM.

ΠΩΣ

Ένα σεμινάριο βασισμένο σε σύγχρονα μαθήματα όπου κάθε εκπαιδευτής θα εξηγήσει συγκεκριμένα θέματα και στο τέλος του σεμιναρίου θα προταθούν διάφορες δραστηριότητες και θα διεξαχθεί ένα τεστ αξιολόγησης.

Προτάσεις Αξίας

Οφέλη για τους συμμετέχοντες

- Διερεύνηση ενός συγκεκριμένου, αλλά πολύ κοινού, πεδίου εφαρμογής στον Ενεργειακό Τομέα
- Επίπεδο εκπαιδευτικής ενότητας: Προχωρημένο
- Επαγγελματική εκπαίδευση στον τομέα της κυβερνοασφάλειας στον τομέα των σταθμών φόρτισης
- Ανάπτυξη πρακτικών και πρακτικών δεξιοτήτων
- Βασισμένο σε ευρωπαϊκά πλαίσια δεξιοτήτων κυβερνοασφάλειας
- Πρωτοποριακές γνώσεις από ειδικούς του κλάδου και της ακαδημαϊκής κοινότητας
- Βοηθά στην ανάπτυξη δεξιοτήτων και στην επαγγελματική εξέλιξη

ΠΟΙΟΣ

Προφίλ Συμμετεχόντων στην Εκπαίδευση

- Διευθυντές και Ηγέτες
- Εργαζόμενοι στον ενεργειακό τομέα (χειριστές, μηχανικοί, διοικητικοί υπάλληλοι κ.λπ.) και ΜΜΕ
- Αρχιτέκτονες κυβερνοασφάλειας και διαχειριστές κινδύνων
- Ερευνητές και εκπαιδευτικοί στον κυβερνοχώρο
- Επαγγελματίες και λάτρεις της κυβερνοασφάλειας

ΠΟΙΟΣ

Προφίλ Εκπαιδευτή

- **Cristina Alcaraz**
Associate Professor at University of Malaga
PhD. in computer Science
- **Abdelkader Shaaban**
Scientist Security & Communication Technologies
Center for Digital Safety & Security
PhD in Computer Science
- **Stefan Schauer**
Thematic Coordinator
Center for Digital Safety & Security
PhD in Computer Science
- **Elias Athanasopoulos**
Associate Professor at University of Cyprus
PhD. in computer Science

ΤΙ

Θέματα Εκπαίδευσης

- Εισαγωγή στις Υποδομές Χρέωσης Ενέργειας
- Προκλήσεις ασφάλειας σε σταθμούς φόρτισης ενέργειας
- Εξάπλωση της Ενέργειας και Επίπτωση σε Άλλες Κρίσιμες Υποδομές
- Μέτρα ασφαλείας και βέλτιστες πρακτικές για σταθμούς φόρτισης

ΓΙΑΤΙ

Μαθησιακά Αποτελέσματα

- Κατανοήστε τον ορισμό, το πεδίο εφαρμογής και τη σημασία των σταθμών φόρτισης σε ολόκληρο τον ενεργειακό τομέα και τον αντίκτυπό τους σε άλλες κρίσιμες υποδομές
- Κατανοήστε τις μοναδικές προκλήσεις και τα τρωτά σημεία ασφαλείας που αφορούν ειδικά τους σταθμούς φόρτισης
- Ανάπτυξη γνώσεων σχετικά με τις κυβερνοαπειλές και τις φυσικές απειλές, τους φορείς επιθέσεων και τις πιθανές συνέπειες των παραβιάσεων της ασφάλειας σε σταθμούς φόρτισης
- Κατανόηση των αρχών και των μεθοδολογιών για την ανάλυση των διαδοχικών επιδράσεων και την αξιολόγηση των κινδύνων ασφαλείας
- Αποκτήστε γνώσεις σχετικά με αποτελεσματικά μέτρα ασφαλείας, ελέγχους και βέλτιστες πρακτικές για την προστασία των σταθμών φόρτισης
- Μείνετε ενημερωμένοι για τις νέες απειλές και τάσεις στον τομέα της ασφάλειας των σταθμών φόρτισης

ΓΙΑΤΙ-2

Μαθησιακά Αποτελέσματα

- Εφαρμογή βέλτιστων πρακτικών για την εφαρμογή ελέγχων φυσικής και κυβερνοασφάλειας σε υποδομές φόρτισης
- Αναγνώριση και αξιοποίηση εξειδικευμένων εργαλείων και μηχανισμών ασφαλείας
- Κριτική σκέψη και επίλυση προβλημάτων σε σενάρια ασφαλείας σταθμών φόρτισης.
- Ικανότητα ανάλυσης και ερμηνείας τεχνικών πληροφοριών και ανάπτυξης λύσεων ασφάλειας που βασίζονται σε δεδομένα.
- Ισχυρές δεξιότητες λήψης αποφάσεων βασισμένες σε ολοκληρωμένη κατανόηση των κινδύνων και των βέλτιστων πρακτικών

ΕΚΠΑΙΔΕΥΤΕΣ

- Cristina Alcaraz
- Shaaban Abdelkader

Περιγραμματα Εκπαίδευσης

Συνεδρία-1 – πρπ. 1 ώρα

Θέμα-1: Εισαγωγή στις Υποδομές Χρέωσης Ενέργειας

Σύλληψη της έννοιας των «υποδομών φόρτισης», των συστατικών τους και του περιβάλλοντός τους, καθώς και των ενδιαφερόμενων μερών και των συμφερόντων τους

Επισκόπηση εξαρτήσεων και αντίκτυπο

Θέμα-2: Προκλήσεις ασφάλειας σε σταθμούς φόρτισης ενέργειας

Κύριες προκλήσεις ασφάλειας στο πλαίσιο των σταθμών φόρτισης

Επισκόπηση στις κύριες απειλές πλαισίου

Συγκεκριμένες επιθέσεις σε σταθμούς φόρτισης – μια περαιτέρω διερεύνηση του ζητήματος

Περιγραμματα Εκπαίδευσης

2η Συνεδρία (πρπ. 1 ώρα)

Θέμα-3: Εξάπλωση της Ενέργειας και Επίπτωση
σε Άλλες Κρίσιμες Υποδομές

Εισαγωγή των εξαρτήσεων και των αλληλεξαρτήσεων σε σχέση
με άλλες κρίσιμες υποδομές

Παροχή πρακτικών μελετών βασισμένων σε προσομοιώσεις και
ανάλυση αλυσιδωτών φαινομένων

ΕΚΠΑΙΔΕΥΤΕΣ

- Shaaban Abdelkader
- Elias Athanasopoulos

Περιγραφή Εκπαίδευσης

3η Συνεδρία (πρπ. 1 ώρα)

Θέμα-4: Μέτρα ασφαλείας και βέλτιστες πρακτικές για σταθμούς φόρτισης

Εισαγωγή στις εξαρτήσεις και τις αλληλεξαρτήσεις των σταθμών φόρτισης σε σχέση με άλλες κρίσιμες υποδομές

Παροχή πρακτικών μελετών βασισμένων σε προσομοιώσεις και ανάλυση αλυσιδωτών φαινομένων

Θέμα 1: Εισαγωγή στις Υποδομές Χρέωσης Ενέργειας

Θα καλύψουμε αυτές τις ικανότητες

- Εισαγωγή στην έννοια των «σταθμών φόρτισης»: Σε αυτήν την ενότητα θα γίνουν γνωστά τα κύρια συστήματα που συμμορφώνονται με μια υποδομή φόρτισης, καθώς και τα κύρια στοιχεία, τα πρωτόκολλα και τις τεχνολογίες τους.
- Ενδιαφερόμενοι και συμφέροντα: Αυτή η ενότητα θα παρουσιάσει τους κύριους ενδιαφερόμενους φορείς που ενδιαφέρονται για τη χρήση ή τη διαχείριση των σταθμών φόρτισης, είτε για σκοπούς κατανάλωσης, διαχείρισης είτε συντήρησης.
- Σχέσεις με άλλες κρίσιμες υποδομές: Αυτή η ενότητα θα παρουσιάσει μια απλή επισκόπηση της άμεσης σχέσης μεταξύ των σταθμών φόρτισης και του κύριου δικτύου, με αντίκτυπο σε άλλες κρίσιμες υποδομές.

Θέμα-2: Προκλήσεις ασφάλειας σε σταθμούς φόρτισης ενέργειας

Θα καλύψουμε αυτές τις ικανότητες

- Κύριες προκλήσεις ασφαλείας: Αυτή η ενότητα θα περιγράψει λεπτομερώς τις κύριες προκλήσεις ασφαλείας σε πολλές πτυχές που σχετίζονται με τον τύπο ανάπτυξης, τα κυβερνοφυσικά στοιχεία και τις επικοινωνίες.
- Προκλήσεις ασφάλειας και απορρήτου σε συστήματα φόρτισης (CS): Αυτή η ενότητα θα ασχοληθεί τόσο με τις τυπικές όσο και με τις συγκεκριμένες επιθέσεις σε σταθμούς φόρτισης, δείχνοντας την ευαισθησία του πλαισίου σε πολλαπλές επιθέσεις κατά του ελέγχου και της ισχύος.

Θέμα-3: Εξάπλωση της Ενέργειας και Επίπτωση σε Άλλες Κρίσιμες Υποδομές

Θα καλύψουμε αυτές τις ικανότητες

- Εξαρτήσεις και αλληλεξαρτήσεις: Αυτή η ενότητα θα καλύψει τη μελέτη που απαιτείται για την κατανόηση της διαδοχικής επίδρασης μεταξύ κρίσιμων υποδομών, όπως οι τομείς της υγειονομικής περίθαλψης και της ναυτιλίας.
- Αλυσιδωτή επίδραση από πρακτική άποψη: Αυτή η ενότητα θα επισημάνει τη σημασία της πρόληψης και, τελικά, του μετριασμού των επιπτώσεων που ενδέχεται να επηρεάσουν σοβαρά άλλες κρίσιμες υποδομές.

Θέμα – 4: Μέτρα ασφαλείας και βέλτιστες πρακτικές για σταθμούς φόρτισης

Θα καλύψουμε αυτές τις ικανότητες

- Βέλτιστες πρακτικές και συστάσεις: Αυτή η ενότητα θα καλύψει ένα σύνολο βέλτιστων πρακτικών και συστάσεων που παρέχονται από διεθνείς οργανισμούς όπως ο ENISA.
- Πιο προσαρμοσμένα αντίμετρα ασφαλείας: Αυτή η ενότητα θα ασχοληθεί με συγκεκριμένα μέτρα τόσο όσον αφορά την ανάπτυξη, την επικοινωνία όσο και τα στοιχεία

Πρακτικές Ασκήσεις Εκπαίδευσης

Θα προσφέρονται διάφορες δραστηριότητες καθ' όλη τη διάρκεια της ενότητας rious:

- **Ανάλυση μελετών περίπτωσης που επικεντρώνονται στον ενεργειακό τομέα – προαιρετική εργασία**
- **Ένα τεστ αξιολόγησης – υποχρεωτική εργασία**

Μέθοδος Εκτίμησης

Περιγράψτε τα στοιχεία εκτίμησης και διαδικασία αξιολόγησης

Στοιχείο Εκτίμησης	Πως	Σημειώσεις
Τελική αναφορά σχετικά με μια περίπτωση χρήσης	Η ατομική αναφορά υποβλήθηκε εγκαίρως	Απαιτείται ανάλυση και συζήτηση για ένα συγκεκριμένο θέμα
Δοκιμές	Τεστ αξιολόγησης, το οποίο μπορεί να ενσωματώνει μελέτες περίπτωσης όπου οι μαθητές πρέπει να επιδείξουν πρακτικές γνώσεις	Παρουσία των εκπαιδευτών (περίπου 10-15 λεπτά)
ΑΠΑΙΤΟΥΜΕΝΑ		

Προηγούμενες Γνώσεις & Προαπαιτούμενα

Προηγούμενες Γνώσεις:

- Βασικές γνώσεις βασικών αρχών κυβερνοασφάλειας (σχετικές με την ενότητα 1 του CSP)
- Βασική κατανόηση υπολογιστών και δικτύων
- Εμπειρία με λειτουργικά συστήματα

Προαπαιτούμενα:

- Βασικές γνώσεις πληροφορικής και κυβερνοασφάλειας
- Εμπειρία με λειτουργικά συστήματα, διαμορφώσεις δικτύου και πρωτόκολλα επικοινωνίας

Τεχνικά Εργαλεία και άλλες απαιτήσεις

Τεχνικά εργαλεία

- Υπολογιστής με πρόσβαση στο Διαδίκτυο για σύνδεση
- Πρόσβαση στην πλατφόρμα DCM
- Office εργαλεία για τις αναφορές
- Τεχνικά εργαλεία: Κανένα αυτή την στιγμή

Άλλες Απαιτήσεις

- Προθυμία για μάθηση και πειραματισμό
- Επίγνωση των πρακτικών ασφάλειας στο Διαδίκτυο και η προσοχή σας στις σχετικές πρακτικές
- Ενεργή Συμμετοχή

Πηγές: Βιβλία και Αναφορές

1. IEA, Electric Vehicles, <https://www.iea.org>
2. Global Market Insights (GMI), "Europe Electric Vehicle Charging Station Market Size", 2022, <https://www.gminsights.com/industry-analysis/europe-electric-vehicle-charging-station-market>
3. C. Alcaraz, J. Lopez, and S. Wolthunsen, "OCPP Protocol: Security Threats and Challenges", IEEE Transactions on Smart Grid, vol. 8, pp. 2452 - 2459, 2017
4. Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." Computers & Security 112 (2022): 102511
5. Open Charge Point Protocol (OCPP) Security Explained (wevo.energy), accessed in March 2024
6. [EV Charging Station Applications – a Growing Cyber Security Risk – Radware Blog](#), accessed in March 2024
7. C. Alcaraz, J. Cumplido, A. Triviño, "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0", International Journal of Information Security, 2023, ISSN: 16155262.
8. MITRE, MITRE ATT&CK, <https://attack.mitre.org>
9. Figures attributed to Vecteezy, <https://www.vecteezy.com>, 2024 – Thanks!

Εγγραφή: Πως να εγγραφείτε και να δείτε περισσότερες πρακτικές πληροφορίες

Η συγκεκριμένη διαδικασία εγγραφής για την εκπαίδευση στα Βασικά Στοιχεία Κυβερνοασφάλειας και Διαχείρισης ενδέχεται να διαφέρει ανάλογα με τον πάροχο ή το ίδρυμα εκπαίδευσης.

Ωστόσο, τα γενικά βήματα περιγράφονται λεπτομερώς στην πλατφόρμα DCM.

Συνδεθείτε με CyberSecPro: Πως να εγγραφείτε και να δείτε περισσότερες πρακτικές πληροφορίες

1. Ιστοσελίδα:
www.cybersecpro-project.eu
2. X (Twitter):
https://twitter.com/CyberSecPro_eu
3. LinkedIn:
<https://www.linkedin.com/company/cybersecpro-euproject/>



**Co-funded by
the European Union**

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

 ACEEU ACCREDITATION COUNCIL FOR ENTREPRENEURIAL & ENGAGED UNIVERSITIES	 AIT AUSTRIAN INSTITUTE OF TECHNOLOGY	 APIROPLUS SOLUTIONS	 SINTEF	 SOCIAL ENGINEERING ACADEMY	 TAL TECH
ACEEU GmbH Germany Visit Website	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH Austria Visit Website	APIROPLUS SOLUTIONS LTD Cyprus Visit Website	SINTEF AS Norway Visit Website	Social Engineering Academy GmbH Germany Visit Website	Tallin University of Technology Estonia Visit Website
Logo missing	 COFAC COOPERATIVA DE FORMAÇÃO E ANIMACAO CULTURAL C.R.L.	 Consiglio Nazionale delle Ricerche	 Technische Universität Braunschweig	 TECHNICAL UNIVERSITY OF CRETE	 trustilio Enhance your Trustworthiness
C2B CONSULTING Portugal Visit Website	COFAC Portugal Visit Website	Consiglio Nazionale delle Ricerche Italy Visit Website	Technical University of Braunschweig Germany Visit Website	Technical University of Crete Greece Visit Website	trustilio B.V. The Netherlands Visit Website
 focal point Cyber Defence Exercises as a Service	 GOETHE UNIVERSITÄT FRANKFURT AM MAIN	 ITML	 UNINOVA	 UNIVERSIDAD DE MÁLAGA	 NOVA UNIVERSIDADE NOVA DE LISBOA
FOCAL POINT Belgium Visit Website	Goethe University Frankfurt Germany Visit Website	Information Technology for Market Leadership Greece Visit Website	Uninova Portugal Visit Website	Universidad de Malaga Spain Visit Website	Universidade Nova De Lisboa Portugal Visit Website
 Institut Mines-Télécom	 LAUREA	 GRUPPO Maggioli	 University of Cyprus	 FACULTY OF SCIENCES NOVI SAD 1969 SERBIA	 UNIVERSITY OF PIRAEUS RESEARCH CENTER
Institut Mines-Télecom France Visit Website	Laurea University of Applied Sciences Finland Visit Website	Maggioli S.p.A. Italy Visit Website	University of Cyprus Cyprus Visit Website	University of Novi Sad Faculty of Sciences Serbia Visit Website	University of Piraeus Research Center Greece Visit Website
 PDMFC	 Security Labs Consulting Ltd	 SGI	 Zelus		
PDMFC Portugal Visit Website	Security Labs Consulting Ltd Ireland (Republic) Visit Website	Serious Games Interactive Denmark Visit Website	ZELUS P.C. Greece Visit Website		

Σας ευχαριστώ

Για απορίες στείλτε μας ένα e-mail

- Cristina Alcaraz
alcaraz@uma.es
- Abdelkader Shaaban
abdelkader.shaaban@ait.ac.at
- Stefan Schauer
stefan.schauer@ait.ac.at
- Elias Athanasopoulos
athanasopoulos.elias@ucy.ac.cy