Project no: 2020-1-LT01-KA203-078070

O1-A2: Αποτελέσματα “ Ανάλυση των υπάρχοντων προγραμμάτων κατάρτισης Ηλεκτρινικής Ασφάλειας”

REPORT

2021

Συνεργασία

Vilnius University, Lithuania

Website: http://www.vu.lt

University of Tartu

Website: https://www.ut.ee/et

MECB - Macdac Engineering Consultancy Bureau LTD , Malta

Website: http://www.mecb.com.mt/eu

Altacom SIA, Latvia

Website: https://www.altacom.eu/

DOREA Educational Institute, Cyprus

Website: https://dorea.org/

ECDL- Information Technologies Institute, Lithuania

Website: http://www.ecdl.lt/

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project N°.: 2020-1-LT01-KA203-078070)

Περιεχόμενα

Περιχόμενα

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Λίστα Συντομογραφιών

CCS	Κοινωνία Υπολογιστών της Κύπρου
CERT.LV	Λετονική ομάδα αντιμετώπισης έκτακτης ανάγκης στον τομέα των υπολογιστών
CSSS	Cybersecurity skills shortage
ESCO	Έλλειψη δεξιοτήτων ηλεκτρονικής αφάλειας
ENISA	Ευρωπαϊκός Οργανισμός ηλεκτρονικής ασφάλειας
EU	Οργανισμός Ευρωπαϊκής Ένωσης για την ηλεκτρονική αφάλεια
HITSA	Ευρωπαϊκή Ένωση
ISACA	Εκπαιδευτικό Ίδρυμα Τεχνολογίας Πληροφοριών
ISC2	International Information System Security Certification Consortium
NCSC	Κοινοπρακτική Πιστοποίηση Διεθνούς Συστήματος Πληροφοριών
NCSS	Εθνικό Κέντρο Ηλεκτρονικής αφάλειας στο Υπουργείο Εθνικής Άμυνας (Δημοκρατία της Λιθουανίας)
OCECPR	Γραφείο Επιτροπής Ηλεκτρονικής Επικοινωνίας και Κανονισμού Ταχυδρομείων (Κυπριακή Δημοκρατία)
RIA	Αρχή συστήματος πληροφοριών
SMEs	Μικρομεσσαίες Επιχειρήσεις

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project N°.: 2020-1-LT01-KA203-078070)

1. ΕΙΣΑΓΩΓΉ

1.1. Η έλλειψη δεξιοτήτων ηλεκτρονικής ασφάλειας και οι λόγοι πίσω απο αυτό

Βασισμένη στην ετήσια παγκόσμια μελέτη απο την Ομάδα Στρατηγικής Επιχείρησης (Enterprise Strategy Group) και τον Σύλλογο Ασφάλειας Πληροφοριακών Συστημάτων (Information Systems Security Association) που διεξήχθη το 2019, η έλληψη δεξιοτήτων ηλεκτρονικής ασφάλειας έχει επηρεάσει το 74% των παγκόσμιων οργανισμών. Οι βασικές συνέπειες αυτής της έλλειψης που υποδυκνύονται στην έρευνα αυξήσαν το φόρτο εργασίασ στο ήδη υπάρχον προσωπικό, ανικανότητα εφαρμογής κάποιων τεχνολογιών ασφαλείας, πρόσληψη και εκπαίδευση κατώτερου προσωπικού αντί για πρόσληψη πιο έμπειρων επαγγελματιών. Οι κρισιμότερες ελλείψεις δεξιοτήτων είναι η ασφάλεια του υπολογιστικού νέφους (33%), η ασφάλεια των εφαρμογών (32%), και η ανάλυση της ασφάλειας και οι έρευνες πάνω σε αυτήν (30%).

Επιπροσθέτως, σύμφωνα με την έρευνα που πραγματοποιήθηκε απο τον Σύλλογο Ασφάλειας Πληροφοριακών Συστημάτων (Information Systems Security Association) το 2019, το 57% των οργανισμών έχουν κενές θέσεις στον τομέα της ηλεκτρονικής ασφάλειας. Ο χρόνος που χρειαζόταν για να συμπληρωθούν αυτές οι θέσεις ήταν συνήθως τρείς μήνες, όπως υπέδειξε περισσότερο απο το 60% των ερωτηθέντων που πήραν μέρος στην έρευνα. Οι περισσότερες απο τις κενές θέσεις εργασίας είναι μεμονωμένοι συνεργάτες (αμφότεροι τεχνικοί και όχι τεχνικοί ηλεκτρονικής ασφάλειας) και διευθυντικές θέσεις ηλεκτρονικής ασφάλειας. Η ζήτηση για θέσεις εργασίας ως μεμονωμένος συνερεγάτης (τεχνικής ηλεκτρονικής ασφάλειας) αναμένεται να αναπτυχθεί τα επόμενα χρόνια. Αντιθέτως, η ζήτηση άλλως εγασιών αναμένεται να παρεμείνει ίδια ή να αυξηθεί πάρα πολύ λίγο.

Ένας απο τους κύριους λόγους, που υποδείχθηκαν απο τους ερωτηθέντες, γιατί οι θέσεις εργασίας παραμένουν κενές είναι η έλλειψη ειδικευόμενων αιτούντων. Σχεδόν το ένα τρίτο των οργανισμών ισχυρίζονται οτι περίπου 75% των υποψηφίων δεν κατέχουν τα κατάλληλα προσόντα για αυτήν την δουλειά. Το πιο σημαντικό χάσμα δεξιοτήτων που υποδείχθηκε απο τους ερωτηθέντες είναι η έλλειψη κοινωνικών δεξιοτήτων, γνώσης πληροφορικής, ανεπαρκής διαίσθησης όσο αναφορά τις επιχειρήσεις, τεχνικής και πρακτικής εμπειρίας.

Σύφμωνα με την ENISAA[1], οι συσκέψεις με τα κράτη μέλη της αναγώρισε την επίγνωση της ηλεκτρονικής ασφάλειας και του χάσματος στον πληθυσμό ως ένα απο τα βασικά εμπόδια στη δημιουργία ενός ασφαλούς ηλεκτρονικού συστήματος. “Παρά την διαθεσιμότητα σχεδόν 600 ακαδημαϊκών ιδρυμάτων και εκπαιδευτικών κέντρων που προσέφεραν προγράμματα

[1] ENISA (2019): Cybersecurity skills development in the EU, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf (accessed

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

ηλελκτρονικής ασφάλειας σε όλη την Ευρώπη, το χάσμα της ηλεκτρονικής ασφάλειας σε όλους τους τομείς παραμένει μία σημνατική πρόκληση" (ENISA, 2019, p. 10).

Το 2020, η εκτιμώμενη παγκόσμια έλλειψη ανθρώπινου δυναμικού ηλεκτρονικής ασφάλειας ήταν περίπου 3.12 εκατομμύρια επαγγελματιών/ειδικών[2]. Αντιθέτως, μόνο στην Ευρώπη, το κενό στο ανθρώπινο δυναμικό στον τομέα της ηλεκτρονικής ασφάλειας αναμένεται να είναι 350.000 εργαζόμενοι μέχρι το 2022. Ο αριθμός αυτός διπλασιάστηκε απο αυτόν που αναμενόταν το 2018[3].

Λόγοι πίσω απο την έλλειψη δεξιοτήτων ηλεκτρονικής ασφάλειας

Η ENISA, στο άρθρο της "Η ανάπτυξη των δεξιοτήτων της ηλεκτρονικής ασφάλειας στην ΕΕ", έχει υποδείξει τέσσερις αιτίες που μπορεί να συμβαλλουν στην έλλειψη δεξιοτήτων. Οι δύο απο αυτές αναφέρονται στον χώρο εργασίας , ενώ οι υπόλοιπες δύο αναφέρονται στα προβλήματα που υπάρχουν στην εκμάθηση και στο εκπαιδευτικό σύστημα. Πιο συγκεκριμένα:

1. Η αγορά εργασίας ηλεκτρονικής ασφάλειας είναι σχετικά ανώριμη και δυναμική, με αποτέλεσμα οι προδιαγραφές εργασίας να εξαρτώνται σε μεγάλο βαθμό απο το μέγεθος και τον τομέα του οργανισμού. Για παράδειγμα, οι Μικρομεσσαίες Επιχειρήσεις (SMEs) που δεν ειδικεύονται στον τομέα της ηλεκτρονικλης ασφάλειας τείνουν να προσλαμβάνουν προσωπικό που έχει γενική γνώση Πληροφορικής (IT) και μερική γνώση πάνω στον τομέα της ηλεκτρονικής ασφάλειας.
2. Οι εργοδότες δεν προσφέρουν το κατάλληλο εκπαιδευτικό επίπεδο, το οποίο αποτρέπει αμφότερα την δημιουργία μίας συνεχούς διοχέτευσης εργατικού δυναμικού και την επαγγελματική ανάπτυξη των τωρινών εργαζομένων. Αυτό δημμιουργεί εμπόδια στους επαγγελματίες πάνω στον τομέα της ηλεκτρονικής ασφάλειας που έχουν ένα γενικότερο υπόβαθρο για περαιτέρω ανάπτυξη των απαραίτητων επαγγελματικώ δεξιοτήτων.
3. Η πανεπιστημιακή κοινότητα δεν καταφέρνει να παράγει υποψήφιους με την κατάλληλη γνώση και δεξιότητες. Οι μαθητές επίσης έχουν έλλειψη πρακτικής/χειροπιαστής εμπειρίας, με αποτέλεσμα στην ανισότητα δεξιοτήτων μεταξύ των απαιτήσεων της εταιρείας και των δεξιοτήτων που κατέχει ο μαθητής.
4. Υπάρχει αργή ταχύτητα ανταπόκρισης στο πρόγραμμα μαθημάτων/σπουδών συγκριτικά με την ανάπτυξη του τομέα αυτού. Εξαιτίας της συσχέτισης της γραφειοκρατίας, μέχρι στιγμής, το πρόγραμμα σπουδών/μαθημάτων δυσκολεύεται να συμβαδίσει με τις απειλές που αναδύονται και τις καινούργιες δεξιότητες που χρησιμοποιούνται για την αντιμετώπιση αυτών των απειλών

[2] (ISC)² (2019): (ISC)² Study Reveals the Cybersecurity Workforce Has Grown to 3.5 Million Professionals Globally, URL https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/11/11/ISC2-Study-Reveals-the-Cybersecurity-Workforce-Has-Grown-Globally (accessed 09/03/2021)
[3] (ISC)² (2019): Cybersecurity workforce study, URL https://www.isc2.org/Research/Workforce-Study (accessed 09/03/2021)

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

1.2. Πολιτική ψηφιακής εκπαίδευσης και πολτική εκπαίδευσης ηλεκτρονικής ασφάλειας στην ΕΕ

Το 2013, η Ευρωπαϊκή Επιτροπή δημοσίευσε την πρώτη της στρατηγική ηλεκτρονικής ασφάλεις, επισημαίνοντας την ευαισθητοποίηση και την ανάπτυξη των δεξιοτήτων αυτής ως βασικούς στρατηγικούς στόχους.

"Το 2017, η Ερωπαϊκή Επιτροπή και ο Ανώτατος Εκπρόσωπος της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Ασφάλειας δήλωσε ξανά οτι ύπαρχει μια έντονη εκαπιδευτική διάσταση της ηλεκτρονικής ασφάλειας και οτι η αποτελεσματική ηλεκτρονική ασφάλεια βασίζεται σε μεγάλο βαθμο στις δεξιότητες των ενδιαφερόμενων. Προτείνουν οτι μαζι με τα Κράτη Μέλη, η ΕΕ θα έπρεπε να βελτιώσουν την εκπαίδευση της ηλεκτρονικής ασάλειας και των δεξιοτήτων της με βάση το έργο των Ψηφιακών Δεξιοτήτων και του Συνασπισμού Θέσεων Εργασίας και να ιδρύσουν ενα Ευρωπαϊκό βιομηχανικό, τεχνολογικό και ερευνητικό κέντρο ικανοτήτων και δικτύων συντονισμού όλων των διεθνών κέντων ηλεκτρονικής ασφάλειας"

Το 2019, τέσσερα πρότζεκτ- CONCORDIA, ECHO, SPARTA και CyberSec4Europe[4] - ξεκίνησαν στο πλαίσιο του προγράμματος Ορίζοντας 2020 με στόχο την ανάπτυξη ενός κοινού Ευρωπαϊκού Δικτύου Ικανοτήτων της Ηλεκτρονικής Ασφάλειας και του Ευρωπαϊκού Χάρτη Πορείας Έρευνας και Καινοτομίας πάνω σε αυτήν.

Το 2020, η Ευρωπαϊκή Επιτροπή πρότεινε το Ψηφιακό Ευρωπαϊκό Πρόγραμμα[5], πρόγραμμα της ΕΕ για την επίσπευση της ψηφιακής μετμόρφωσης στην Ευρώπη. Το πρόγραμμα αναμένεται να μοιράσει 580 εκατομμύρια ευρώ για την ανάπτυξη εξειδικευμένων ψηφιακών δεξιοτήτων υποστηρίζοντας την σχεδίαση και παράδοση των ειδικών προγραμμάτων και πρακτικών ασκήσεων μελλοντικών εμπειρογνώμονων σε βασικούς τομείς όπως στον τομέα της ΤΝ (Τεχνητής Νοημοσύνης), ηλεκτρονικής ασφάλειας, κβαντική, κλπ.

Το Μάρτιο του 2021, το Ευρωπαϊκό Συμβούλιο υιοθέτησε νέα συμπεράσματα στην στρατηγική ηλεκτρονικής ασφάλειας της ΕΕ[6]. Τα συμπεράσματα αυτά αναγνώρισαν την έλλειψη ψηφιακών δεξιοτήτων και την έλλειψη δεξιοτήτων ηλεκτρονικής ασφάλειας στο εργατικό δυναμικό και εμβάθυναν στην ανάγκη της κάλυψης της ζήτησης της αγοράς μέσω της περαιτέρω ανάπτυξης προγραμμάτων εκαπίδευσης και κατάρτισης

[4] European Commission (2019): Four EU pilot projects launched to prepare the European Cybersecurity Competence Network, URL https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network (accessed 10/03/2021)
[5] European Commission (2020): Digital Europe Programme: A proposed €7.5 billion of funding for 2021-2027, URL https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027 (accessed 10/03/2021)
[6] Council of the European Union (2021): Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy (accessed 24/03/2021)

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

1.3. Διεθνής στρατηγικές ηλεκτρονικής ασφάλειας

Απο το 2017, όλα τα κράτη μέλη της ΕΕ ανέπτυξαν και δημοσίευσαν τις δικες τους στρατηγικές ηλεκτρονικής ασφάλειας.

Κύπρος

Η Δημοκρατία της Κύπρου έχει επίγνωση της σημαντικότητας της ηλεκτρονικής εκπαίδευσης για την εγγύηση της Διεθνούς διαδικτυακής προστασίας. Ένας απο τους βασικούς στοόχους της υπάρχουσας στρατηγικής ηλεκτρονικής ασάλειας είναι να προωθήσει την ιδέα της ηλεκτρονικλης ασφάλειας και να αθ᾽ξησει την επίγνωση αυτής στο ευρύ κοινό (πολίτες, εργατικό δυναμικό, και νεολαία) και να χτίσει μια συλλογική ατμόσφαιρα με στόχο την εφαρμογή αυτής της στρατηγικής.

Η στρτηγικής της Δημοκρατίας της Κύπρου για την ηλεκτρονικλη ασφάλεια δημιουργήθηκε το 2012[7]. Η Κυπριακή διεθνής στρατηγική στοχεύει στην ανάπτυξη τεχνικής εκπαίδευση στον τομέα της διαδικτυακής ασφάλειας και στην εκμάθηση τρόπων με τους οποίους κάποιο μπορεί να προστατευτεί και να τπυς αντιμετωπίσει σε έκτακτες περιπτώσεις. Ένας απο τους στόχους είναι να χτίσει ένα εξειδικευμένο εργατικό δυναμικό ικανό να χειρίζεται μία αληθινή ηλεκτρονική επίθεση. Για αυτο το λόγο, έπρεπε να γίνουν κάποιες ασήσεις για να παρατηρηθεί η ανταπόκριση του εργατικού δυναμικού σε μια προσομοίωση αληθινής κρίσης. Η υλοποίηση της στρατηγικής θα έχει ως αποτέλεσμα την επιβολή περιγραφών και πιστοποιήσεων για εξειδικευμένες εργασίες στην ηλεκτρονική ασφάλεια.

Η στρατηγική αποτελείται απο 17 συγκεκριμένες ενέργειες. Αυτές οι ενέργειες περιλαμβάνουν την αναγνώριση των διαθέσιμων κατάλληλων προγραμμάτων κατάρτισης προσωπικού και πιστοποιήσεις στον τομέα της ηλεκτρονικής και ψηφιακής ασφάλειας.

Η Δημοκρατία της Κύπρου είναι επίσης αφοσιωμένη να εγκαθιδρύσει κοινή/δημόσια-ιδιωτική συνεργασία για να υποστηρίξει ανώτατα εκπαιδευτικά ιδρύματα ενσωματώνοντας θέματα ηλεκτρονικής ασφάλειας και ενισχύοντας την εκπαίδευση επαγγελματιών και ακαδημαϊκών στον τομέα της ηλεκτρονικής ασφάλειας.

Η νεότερη εκδοχή του διεθνούς εγγράφου ηλεκτρονικλης ασφάλειας αναπτύχθηκε το 2020. Η στρατηγική είναι προς το παρόν ύπο εξέταση και εκκρεμεί η τελική αποδοχή απο το Υπουργείο Επικοινωνιών και το Συμβούλιο των Υπουργών.

Η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) είναι ένας ανεξάρτητος κυβερνητικός οργανισμός υπο την επίβλεψη της Επιτροπής Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Κανονισμών. Είναι υπεύθυνο για την εφαρμογή της Ευρωπαϊκής Οδηγίας NIS (Ασφάλεια Δικτύων και Πληροφοριών),

[7] OCECPR (2012): Cybersecurity Strategy of the Republic of Cyprus , URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus (accessed 11/03/2021)

Funded by the Erasmus+ Programme of the European Union

επικεντρώνεται στην αναβάθμιση και την διατήρηση των υψηλών επιπέδων ηλεκτρονικής ασφάλειας για όλους τους χειριστές απαραίτητων υπηρεσιών και κρίσιμων υποδομών πληροφοριών στην Κύπρο. Ο οργανισμός αυτός στοχεύει επίσης να αυξήσει την επίγνωση της ηλεκτρονικής ασφάλειας ανάμεσα στην κοινωνία και γενικά να τονώσει τον διεθνή ανταγωνισμό της Κύπρου.

Άλλος σημαντικός οργανισμός στην κοινωνία πληροφορικής της Κύπρου (CCS) [8], ένας ανεξάρτητος μη-κερδοσκοπικός οργανσμός ιδρύθηκε το 1985 για να αναπτύξει, να αναβαθμίσει και να προωθήσει τον τομέα της πληροφορικής. Ο CCS επιδιώκει να θέσει υψηλά στάνταρ μεταξύ της επαγγελματικής βιομηχανίας, αναγνωρίζοντας τον αντίκτυπο που οι Πληροφοριακές και Επικοινωνικές Τεχνολογίες έχουν στην εργασία, στην επιχείρηση, στην κοινωνία και στην ποιότητα ζωής των πολιτών. Το γεγονός αυτό στοχεύει να ανακαλύψει ηλεκτρονικά ταλέντα και να παρακινήσει τους νέους να ακολουθήσουν την καριέρα τους πάνω στον τομέα της ηλεκτρονικής ασφάλειας[9].

[8] Cyprus computer society (CCS), URL https://ccs.org.cy/en/
[9] Cyprus cyber security challenge, URL https://ccsc.org.cy/#home

Funded by the Erasmus+ Programme of the European Union

(Project N⁰.: 2020-1-LT01-KA203-078070)

Εσθονία

Εσθονία ήταν μία απο τους πρωτοπόρους στην δημοσίευση στρατηγικών ηλεκτρονικής ασφάλειας και προς το παρόν έχει την τρίτη έκδοση ενός εθνικού εγγράφου ασφαλείας της ηλεκτρονικής ασφάλειας[10]. Η στρατηγική είναι χωρισμένη σε τέσσερα τμήματα: 1. Βιώσιμη Ψηφιακή Κοινωνία 2. Βιομηχανία Ηλεκτρονικής Ασφάλειας, Έρευνας και Ανάπτυξης, 3. Κορυφαίος Διαθνής Συνεργατης, 4. Ηλεκτρονικά Ελεύθερη Κοινωνία.

Η Εσθονική στρατηγική τείνει να ενισχύσει την ηλεκτρονική εκπαίδευση, η εφαρμογή αυτής περιγράφεται στο δεύτερο στόχο του σχεδίου. Απο το 2014, η χώρα έχει αρχίσει να επενδύει στην εκπαίδευση και κάνει συμφωνίες με πανεπιστήμια βστε να πρωθήσει τις ηλεκτρονικές σπουδές, να χρηματοδοτήσει πρότζεκτ και να υποστηρίξει υποτροφίες.

Το Υπουργείο Εκπαίδευσης και Έρευνας επιβλέπει αυτά τα εκπαιδευτικά πρότζεκτ και ακολουθεί τις καθιερωμένες προτεραιότητες της Στρατηγικής Ηλεκτρονικής Ασφάλειας ώστε να εκτελέσει το πλάνο της δια βίου μάθησης και να υποστηρίξει την ανάπτυξη της βασικής ηλεκτρονικής εκπαίδευσης σε όλα τα επίπεδα των πτυχιούχων.

Σύμφωνα με την στρατηγική, η εκπλήρωση των στρατηγικών στόχων υποστηρίζεται απο το Ίδρυμα Πληροφοριών και Τεχνολογίας για Εκπαίδευση (HITSA), το οποίο συνεισφέρει στην εκπαίδευση των ειδικών στο πεδίο μέσω του συντονισμού τοσο του Targalt Internetis (“Stayying Smart Online”) οσο και των προγραμμάτων πλήροφορικής της Ακαδημίας.

Άλλος ένας σημαντικός οργανισμός η Αρχή Συστήματος Πληροφοριών (RIA)[11], η οποία συντονίζει την ανάπτυξη και την διαχείριση των πληροφοριακών συστημάτων, οργαώνει δραστηριότητες σχετικές με την ασφάλεια πληροφοριών, και χειρίζεται περιστατικά ασφαλείας. Η RIA παίζει επίσης πολύ σημαντικό ρόλο στην ηλεκτρονική υγιεινή, αποτρέπει δραστηριότητες και αυξάνει την επίγνωση της κοινωνίας.

“Οι εκτρατείες για ευρεία πρόληψη και επίγνωση θα ξεκινήσουν για την διάδοση των ηλεκτρονικών απειλών σε διαφορετικές ομάδες, εμπεριέχοντας και τις επιχειρήσεις. Για να αυξηθεί το επίπεδο της ηλεκτρονικής υγιεινής σε κυβερνητικά ιδρύματα, θα γίνει υποχρεωτικό για κυβερνητικά ιδρύματα και τοπικούς κυβερνητικούς υπαλλήλους να περάσουν κάποια τέστ για την γνώση τους επάνω στον τομέα της ηλεκτρονικής ασφάλειας. Τα εκπαιδευτικά μαθήματα και οι πληροφορίες προσεγγίσης των ομάδων θα συνεχιστεί κανονικά”. (Η Δημοκρατία της Εσθονίας, Υπουργειο Οικονομικών Υποθέσεωψν και Επικοινωνιών, 2019, σελ. 64).

[10] Republic of Estonia, Ministry of Economic Affairs and Communication (2019): Cybersecurity Strategy, URL https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf (accessed 10/03/2021)
[11] Information System Authority (RIA), URL https://www.ria.ee/en.html

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Λετονία

Στην Λετονία, το θέμα της Εθνικής Ασφάλειας επίσης συνδέεται ,ε την τωρινή τεχνολογική ανάπτυξη. Η πρώτη Λετονική στρατηγική ηλεκτρονικής ασφάλειας τέθηκε σε ισχύ το 2014, με την έγκριση του σχεδίου απο το 2014 έως και το 2018. Το 2019, εγκρίθηκε μία καινούργια στρατηγική ηλεκτρονικής ασφάλειας για το διάστημα 2019-2022. Η αναβαθμισμένη αυτή στρατηγική στοχεύει να ενδυναμώσρι και να βελτιώσει τις ικανότητες της Λετονικής ηλεκτρονιθκής ασφάλειας με την βελτίωση της ευαισθητοποίησης του κοινού και την ανθεκτικότητα εναντίον τψν ηλεκτρονικών επιθέσεων. Για να πετύχει αυτούς τους στόχους, η στρατηγική προτείνει δράσεις σε έξι τομείς[12]:

1. Βελτίωση της ηλεκτρονικής ασάλειας και διαχειρίσμα ψηφιακα ρίσκα ασφαλείας,
2. Ανθεκτικότητα των συστημάτων ICT,
3. Καλύτερη καθολική πρόσβαση στα στρατηγικά συστήματα και τις υπηρεσίες της ICT,
4. Δημόσια επίγνωση, εκπαίδευση και έρευνα,
5. Διεθνή συνεργασία/συμμετοχή,
6. Επιβολή νομοθεσίας στο διαδίκτυο και πρόληψη του ηλεκτρονικου εγκληματος.

Όσο αναφορά τον τομέα της “Δημοσιας Επίγνωσης, Εκπαίδευσης και Έρευνας”, η στρατηγικη υποδικνύει πέντα βασικά καθήκοντα[13]:

- Προσφορα υποστήριξης για αναπτυξιακή έρευνα στον τομέα της ηλεκτρονικής ασφάλειας,
- Να αυξησει τις γνωσεις των μαθητών και εκπαιδευτών στην πληροφορικη, προσωπική ασφάλεια και στην χρήση αξιόπιστων ηλεκτρονικών υπηρεσιών,
- Ενδυνάμωση της δημόσιας γνώσης της χρήσεης ασφαλούς ίντερνετ (ανάπτυξη εκπαιδευτικών και πληροφοριακών εργαλείων για όλες τις ηλικίες με συστάσεις ασφαλείας, δραστηριότητες για την χρήση του ίντερνετ, οργάνωση κοινωνικών εκτρατειών). Ανάπτυξη και εφαρμογη ετήσιας διοργανικής εργασίας και σχεδίου δράσης για την ενημέρωση και την ευαισθητοποίηση των εταιρειών πάνω σε θέματα της ηλεκτρονικής ασφάλειας,
- Προώθηση γνώσης ασφαλούς χρήσης του ICT μεταξύ τοπικού και κρατικού ιδρυματικού προσωπικού,
- Προώθηση εκπαιδευτικών δραστηριοτήτων και ανταγωνισμού στον τομέα της ηελκτρονικλης ασφάλειας.

[12] Latvian Defence Ministry (2019): Latvia approves new Cyber Security Strategy 2019-2022, URL; https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022 (accessed 11/03/2021)
[13] Latvian Defence Ministry (2019): Latvia's cyber security strategy for 2019 – 2022, URL https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf (accessed 11/03/2021)

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Η στρατηγική επίσης επισημαίνει την ανάγκη για καλύτερη συμβίωση απο τους δημόσιους και ιδιωτικούς φορείς για την ενίσχυση της αντοχής των συστημάτων ηλεκτρονικής ασφάλειας και την παροχή επενδύσεων στην ασφάλεια του ICT και την εκπαίδευση των εργαζομένων.

Η Λετονική Ομάδα Ανταπόκρισης Υπολογιστων (CERT.LV) είναι υπεύθυνη για την παρακολούθηση και διαχείριση περιστατικών ηλεκτρονικής ασφάλειας. Η CERT.LV επίσης διοργανώνει εκπαιδευτικές εκδηλώσεις και εκπαιδευτικά μαθήματα για το ευρύ κοινό. Κάτω απο την νέα στρατηγική, η CERT.LV αναμένεται να αναπτύξει πόρους με τους δημόσιους και ιδιωτικούς τομείς για τη συλλογη πληροφοριών σχετικά με περιστατικά για ανάλυση και αξιολόγηση[14].

Άλλος ένας σημαντικός οργανισμός είναι το Λετονικο Κέντρο Ασφαλέστερου Διαδικτύου. Τα βασικά καθήκοντά του έιναι να εκπαιδεύσει, να ενημερώσει και να αυξήσει την δημόσια επίγνωση σχετικά με την ασφαλέστερη χρήση του ίντερνετ, να παρέχει μία πλατφόρμα για την αναφορά παράνομου περιεχομένου και παραβιάσεων ασφαλείας στο διαδίκτυο σε μια ανοιχτή γραμμη άμεσης πρόσβασης, και να προσφέρει επαγγελματική ψυχολογική υποστήτιξη μέσω αυτής της γραμμής εξυπηρέτης[15].

Λιθουανία

Το 2018, η Κυβέρνηση ενέκρινε την Λιθουανική Εθνική Στρατηγική Ηλεκτρονικλης Ασφάλειας της Δημοκρατίας της Λιθουανίας[16].

“Ο πρωταρχικός σκοπός της στρατηγικής είναι να παρέχει στην Λιθουανική κοινωνία την ευκαρία να εκμεταλλευτεί την Πληροφορικη και Επικοινωνιακη Τεχνολογία (ICT) με το να αναγνωρίζει ηλεκτρονικά περιστατικά αποτελεσματικά, να αποτρέπει την ύπαρξη και την μετάδοση, και να διαχειρίζεται τις συνέπειες που συνεπάγονται απο τα ηλεκτρονικά αυτά περιστατικά. Η απόφαση για την έγκριση αυτής της εθνικής στρατηγικής ηλεκτρονικής ασφάλειας, 12 Αυγούστου 2018 No.818.

Για την επίτευξη του στόχου, η στρατηγική προτείνει πέντε στόχους:

1. Ενίσχυση της ηλεκτρονικής ασφάλειας της χώρας και ανάπτυξη των ικανοτήτων της ηλεκτρονικής άμυνας,
2. Εξασφάλιση πρόληψης και έρευνα εγκληματικλων αδικημάτων στο διαδίκτυο,
3. Προώθηση κουλτούρας ηλεκτρονικής ασφάλειας και ανάπτυξη καινοτομιών,

[14] Cyber Wiser (2021): Education and training in national cybersecurity strategy, URL https://www.cyberwiser.eu/latvia-lv (accessed 11/03/2021)
[15] ENISA, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Latvia
[16] Government of the Republic Of Lithuania (2018): Resolution on the approval of the national cyber security strategy, URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

4. Ενίσχυση κλειστής συνεργασίας μεταξύ ιδιωτικού και δημόσιου τομέα,
5. Βελτίωση διεθνούς συνεργασίας και εξασφάλιση εκπλήρωσης διεθνών υποχρεώσεων στον τομέα της ηλεκτρονικής ασφάλειας.

Η προώθηση της κουλτούρας και της καινοτομίας της ηλεκτρονικής ασφάλειας ειναι ο βασικός στόχος της εθνικής στρατηγικής. Η στρατηγική προτείνει αυτές τις ενέργειες ώστε να φτάσει σε αυτούς τους συγκεκριμένους στόχους[17]:

- Ενημερωμένα συνεχόμενα και συστηματικά εκπαιδευτικά μαθή,ατα για τους εγαζόμενους του ιδιωτικού και δημόσιου τομέα στοχεύοντας στην αύξηση της γνώσης των εργαζομένων και στο να χτίσουν μία συνολική κουλτούρα ηλεκτρονικής ασφάλειας
- Συνεχή διάδοση πληροφοριών σε καινούργια διαδικτυακά περιστατικά
- Δημιουργία του ICT ως μέρος εκπαιδευτικής διαδικασίας από μικρή ηλικία, ξεκινώντας απο το νηπιαγωγείο μεχρι και την δευτεροβάθμια εκπαίδευση
- Συνεχή αναβάθμιση και και κατάρτιση των εκπαιδευτών με σκοπό την βελτίωση των ικανοτήτων τους στον τομέα της ηλεκτρονικής ασφάλειας

Η στρατηγική εμβαθύνει στην ανάγκη για ανάπτυξη των δεξιοτήτων και ικανοτήτων της ηλεκτρονικής ασφάλειας για την συνεχή κάλυχη των αναγκών της αγοράς. Για να επιτευχθεί αυτός ο στόχος, η στρατηγική προτείνει "την δημιοργία ενός μοντέλου και προτύπων ικανοτήτων ηλεκτρονικής ασφάλειας, ανάπτυξη εκπαιδευτικών συστημάτων, διαπίστευση και πιστοποίηση προσανατολισμένη στις ανάγκες της αγοράς εργασίας, παροχή περιβάλλοντος εκπαίδευσης και δοκιμών στον τομέα της ηλεκτρονικής ασφάλειας, προσφορά εκπαίδευσης στους υπαλλήλους του ICT, κλπ." Απόφαση σχετικά με την έγκριση της εθνικής στρατηγικής ηλεκτρονικής ασφάλειας, 13 Αυγούστου 2018 No. 818.

Η στρατηγική επίσης επισημαίνει την ανάγκη ανάπτυξης καινοτομιλων στον τομέα της ηλεκτρονικής ασφάλειας. Για να πετύχει αυτόν τον στόχο, η συνεργασία μεταξύ βασικών δημόσιων και ιδιωτικών παραγόντων και ακαδημαϊκών είναι σημαντική.

Το Εθνικό Κέντρο Ηλεκτρονικής Ασφάλειας στο Υπουργείο Εθνικής Άμυνας (NCSC) [18] είναι ένα κεντρικό Λιθουανικό ίδρυμα ηλεκτρονικής ασφάλειας το οποίο είναι υπεύθυνο για την διαχείριση ηλεκτρονικών περιστατικών, παρακολουθώντας την υλοποίηση των αναγκών της ηλεκτρονικής ασφάλειας, και εγκρίνοντας τους πόρους των δεδομένων.

[17] Cyber Wiser (2021): Education and training in national cybersecurity strategy (LT), URL https://www.cyberwiser.eu/lithuania-lt (accessed 11/03/2021)
[18] National Cyber Security Centre, URL https://www.nksc.lt/en/

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Μάλτα

Η Εθνική Ψηφιακή Στρατηγική για την Μάλτα[19], γνωστή επίσης και ως Ψηφιακή Μάλτα, εφαρμόστηκε το 2016. Η στρατηγική καλύπτει την ανάγκη και τις προσδοκίες τριών βασικών εθνικών ενδιαφερόμενων - του δημοσιου τομέα, τον ιδιωτικό τομέα και την κοινωνία των πολιτών για να εξασφαλιστεί η ηλεκτρονική ασφάλεια.

Η στρατηγική προτείνει τέσσερις βασικούς στόχους:

1. Καταπολέμηση του ηλεκτρονικού εγκλήματος με την αναγνώριση των κενών και την ενίσχυση των ικανοτήτων των υπηρεσιών επιβολής του νόμου να διερευνούν το ηλεκτρονικό έγκλημα,
2. Ενίσχυση την εθνικής ηλεκτρονικής άμυνας με την καθοδήγηση και την βοήθεια δημόσιων και ιδιωτικών φορέων στην βελτίωση των ικανοτήτων τους στον τομέα της ηλεκτρονικής άμυνας
3. Εξασφάλιση υψηλότερου επιπέδου εμπιστοσύνης στο διαδίκτυο εφαρμόζοντας προγράμματα ευαισθητοποίησης και παροχής αξιόπιστων υπηρεσιών με δυνατότητα ICT.
4. Δημιουργία ικανοτήτων (επίγνωση και εκπαίδευσης ηλεκτρονικής εκπαίδευσης) με την αναγνώριση και ανάπτυξη δεξιοτήτων και απαραίτητων εκπαιδευτικών πλαισίων.

Ο τελευταίος βασικός στόχος (Γνώση και Εκπαίδευση) στοχεύει την πανεπιστημιακή κοινότητα, τον δημόσιο και τον ιδιωτικό τομέα και τους πολίτες ως μέσο για την αύξηση της ευαισθητοποίησης,της γνώσης καθώς και των ικανοτήτων και της τεχνογνωσίας στην ηλεκτρονική ασφάλεια μέσω μίας εκπαιδευτικής εκστρατείας ευαισθητοποίησης, καθώς επίσης και αυστηρων και συνεχόμενων εκπαιδευτικών και προπονητικών ασκήσεων που στοχεύουν τόσο στο τωρινό εργατικό δυναμικό όσο και στην νεότερη γενία μαθητών. Αυτό το μέτρο συνεπώς συνεπάγει κυρίως[20]:

- Περαιτέρω αναγνώριση της ανάγκης των δεξιοτήτων και των ικανοτήτων στον τομέα της ηλεκτρονικής ασφάλειας,
- Ακαδημαϊκά και εκπαιδευτικά προγράμματα σχεδιασμένα για την ενοποίηση της τεχνογνωσίας τηε ηλεκτρονικής ασφάλειας,
- Επανεξέταση των υφιστάμενων προγραμμάτων που επικεντρώνονται στην ηλεκτρονική ασφάλεια μαζι με τις ικανότητες στην ICT και στα μέσα ενημέρωσης.

[19] The Malta Information Technology Agency (2016): Malta Cyber Security strategy 2016, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Malta (accessed 12/03/2021)

[20] Cyber Wiser (2021): Education and training in national cybersecurity strategy (MT), URL https://www.cyberwiser.eu/malta-mt (accessed 12/03/2021)

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Η στρατηγική επίσης στοχεύει στην εμψύχωση των νέων μέσω του δικτύου υποστήριξης, ειδικότερα γονείς, φροντιστές, εκπαιδευτικούς και νέους εγραζομένους. Προβλέπεται οτι η "Ψηφιακή Ιθαγένεια" θα γίνει μέρος του Εθνικού Εκπαιδευτικού Προγράμματος Μαθημάτων ώστε να εφοδιάσει τα παιδιά και τους νέους με τις ικανότητες που χρειάζονται ώστε να χρησιμοποιού το ίντερνετ ενώ ταυτόχρονα παράγουν παράγουν έργο μέσω του διαδικτύου με ασφάλεια.

Η Ψηφιακή Μάλτα δηλώνει τηη δέσμευση της κυβέρνησης μέσω των εκπαιδευτικών ιδρυμάτων και της βιομηχανίας για να υποστηρίξει την δημιουργία εξειδικευμένων εκπαιδευτικών οδών, να αντιμετωπίσει τις ανάγκες της αγοράς εργασίας , και να αναπτύξει το πτόγραμμα μαθημάτων και να παρέχει τεχνικό υλικό. Τα προγράμματα εκπαίδευσης και πιστοποίησης που σχετίζονται με την ηλεκτρονική ασφάλεια θα έπρεπε να ενθαρρύνονται λιγο περισσότερο ώς ευκαιρία αποτελεσματικής αύξησης των επιπέδων ασφαλείας των οργανισμών και διατήρησης αυτού του υψηλού επιπέδου ασφάλειας μακροπρόθεσμα.

Η ηλεκτρονική ασφάλεια της Μάλτας είναι μέρος της εθνικής στρατηγικής ηλεκτρονικής ασφάλειας της Μάλτας, η οποία στοχεύει να εγκαθιδρύσει ένα κυβερνητικό πλαίσιο, καταπολέμησης του ηλεκτρονικού εγκλήματος, ενίσχυσης της εθνικής ηλεκτροινής άμυνας και παροχής εκπαίδευσης και γνώσης της ηλεκτρονικής ασφάλειας. Ένας απο τους βασικούς στόχους της Εθνικής Στρατηγικής Ηλεκτρονικής Ασφάλειας είναι η πανεθνική/παγκόσμια εκτρατεία επίγνωσης και εκπαίδευσης της ηλεκτρονικής ασφάλειας[21].

Άλλος ένας σημαντικός οργανισμός είναι η εθνική Ομάδα Ανταπόκρισης σε Περιστατικά Ασφαλείας Υπολογιστών της Μάλτας. (CSIRT). Η CSIRT της Μάλτας υποστηρίζει οτι οι σημαντικοί οργανισμοί υποδομών πρέπει να προσέχουν τους εαυτούς τους και τα δεδομένα τους απο ηλεκτρονικές απειλές και περιστατικά[22].

1.4. "Προστασία Κατα Του Ηλεκτρονικού Ψαρέματος στην Εποχή της 4ης Βιομηχανικής Επανάστασης" πρότζεκτ

Η διαδικτυακή ασάλεια αρχίζει να γίνεται μια απο τις μεγλυτερες προκλήσεις της ψηφιακής εποχής και αυτο δίοτι οι πληροφορίες εξελίσονται σε ένα ακριβό περιουσιακό στοιχείο που ασχολείται με έναν τεράστιο όγκο δεδομένων, βελτιώνοντας την επικοινωνία με το ψηδιακό περιβάλλον. Οι ψηφιακές συσκευές και τα πλροφοριακά συστήματα γίνονται όλο και περισσότερο ελκυστικά για ηλεκτρονικές επιθέσεις[23].

[21] Cyber Security Malta, URL https://cybersecurity.gov.mt/
[22] Cyber Security Intelligence, URL https://www.cybersecurityintelligence.com/csirt-malta-2727.html (accessed 12/03/2021)
[23] European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Το ηλεκτρονικό ψάρεμα είναι ένα απο τα μεγαλύτερα προβλήματα διότι οι διαδικτυακοί εγκληματίες μπορούν να χρησιμοποιούν γρηγορότερα και να περισσότερο καινοτόμα τεχνολογικά εργαλεία για να διεξάγουν εκστρατείες ηλεκτρονικού ψαρέματος. Συνεπώς το ανθρώπινο αμυντικό συστημα το οποίο μοχλεύει το ανθρώπινο ένστικτο για την ανακάλυψη και την τεχνολογία ώστε να κλιμακώσει την απόκριση αυτή θα μπορούσε να αναπτυχθεί και να είναι ελεύθερα διαθέσιμο για το ευρύ κοινό. Για τη δημιουργία ενός ανθρώπινου αμυντικού συστήματος, απαιτείται εκπαίδευση του χρήστη ώστε να είναι ικανός να αναγνωρίσει και να ανταποκριθεί στις επιθέσεις ηλεκτρονικού ψαρέματος με τον σωστό τρόπο.

Η Διεθνής μελέτη "Safeguarding against Phishing in the age of 4 Industrial Revolution" („CyberPhish") που ξεκίνησε απο το Πανεπιστήμιο του Βίλνιους της σχολής Καούνας και των συνεργατών της ξεκίνησαν στις αρχές του Νοεμβρίου του 2020 και θα διαρκέσουν για 2 χρόνια.

Ο στόχος του πρότζεκτ ειναι να εκπαιδείσει: μαθητες απο ανώτερα εκπαιδευτικά ιδρύματα, τους ίδους τους εκπαιδευτές, πανεπιστημιακό προσωπικό (μέλη της κοινότητας), άλλα εκπαιδευτικά κέντρα, επαγγελματικούς τομείς (εργοδότες και εργαζομένους), και να ενθαρρύνει την κριτική σκέψη αυτών των ομάδων στο πεδίο της διαδικτυακής ασφάλειας.

Οι συνέταιροι του προτζεκτ πρεπει να σχεδιάσουν ενα πρόγραμμα μαθημάτων, υλικό ηλεκτρονικής μάθησης, ένα συνδυαστικό μαθησιακό περιβάλλον, οπου γνώσεις και αυτοαξιολόγηση ικανοτήτων και προσομοιώσεις συστημάτων αξιολόγησης γνώσεων για μαθητές και άλλους χρήστες ώστε να αποτρέψουν επιθέσεις phising, να αυξήσουν τις ικανότητές τους, οι οποίες θα τους βοηθήσουν να επικεντρώσουν την προσοχή τους στις απειλές και να λάβουν τα κατλληλα μέτρα για να εμποδίσουν αυτες τις επιθέσεις.

Η συνεργασία του έργου αυτού προέρχεται απο 6 οργανισμούς οι οποίοι προέρχονται απο 5 διαφορετικές χώρες:

1. Vilnius University, Lithuania (Coordinator)
2. Information Technologies Institute, Lithuania
3. DOREA Educational Institute, Cyprus
4. University of Tartu, Estonia
5. Altacom SIA, Latvia
6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

Για περισσότερες πληροφορίες οσο αναφορά το πρότζεκτ και τις δραστηριότητες αυτου, παρακαλώ επισκεφθείτε την ιστοσελίδα του πρότζεκτ: https://cyberphish.eu/

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

2. ΑΝΆΛΥΣΗ ΜΕΛΈΤΗΣ

2.1. Η μεθοδολογία της συλλογής δεδομένων

Για την έρευνα των υφιστάμενων προγραμμάτων σπουδών και εκπαιδευτικών προγραμμάτων στον τομέα της ηλεκτρονικής ασφάλειας και του ηλεκτρονικού ψαρέματος, ο ηγετικός οργανισμός του IO1 (DOREA Educational Institute) προετοίμασε αυτό το δείγμα. Το δείγμα αυτό καλύπτει τις βασικές πληροφορίες όπως διαίστευση και ακαδημαϊκό τίτλο, δομή του προγράμματος και πληροφορίες μαθημάτων.

Table 1: Πρότυπη ανάλυση στα υφιστάμενων προγραμμάτων στην τομέα της ηλεκτρονικής ασφάλειας και στον τομέα του ηλεκτρονικού ψαρέματος

Τίτλος προγράμματος ή μαθημάτων	
Τύπος Προγράμματος	
Τομέας Σπουδών	
Πτυχίο/Βαθμός	
Οργανωτικό Ίδρυμα	
Γλώσσα Οδηγιών	
Διάρκεια (ώρες ή διδακτικές μονάδες)	
Ομάδα-Στόχος	
Βασική Ιδέα: Θέματα ή Ενότητες	
Μαθησιακά αποτελέσματα	
Μεθοδολογία (εαν εφαρμόστηκε)	
Διαδικτυακός σύνδεσμος/URL	

Όλοι οι συνέταιροι παροτρύνονται να χρησιομποιούν την Βάση Δεδομένων της Τριτοβάθμιας Εκπαίδευσης της Ηλεκτρονικής Ασφάλειας και να κάνουν την δικής τους εθνική έρευνα καθώς κάποια προγράμματα σπουδών δεν έχουν φορτωθεί ακομα στην τωρινή βάση δεδομένων[24].

Όλοι οι συνέταιροι παροτρύνονται να χρησιομποιούν την Βάση Δεδομένων της Τριτοβάθμιας Εκπαίδευσης της Ηλεκτρονικής Ασφάλειας και να κάνουν την δικής τους εθνική έρευνα καθώς κάποια προγράμματα σπουδών δεν έχουν φορτωθεί ακομα στην τωρινή βάση δεδομένων.

Ζητήθηκε επίσης απο τους συναίτερους του πρότζεκτ να προβούν σε έρευνα διθνείς/εθνικές πολιτικές/στρατηγικές για την εκπαίδευση της ηλεκτρονικλης ασφάλειας. Η έρευνα πραγματοπιήθηκε σε όλες τις χώρες εταίρους - Κύπρος, Εσθονία, Λετονία, και Μάλτα. Τα αποτελέσματα της ανάλυσης της μελέτης μεταφέρθηκαν στον Εθνικό Πίνακα Πορισμάτων/Ευρυμάτων (δομημένα ανά χώρα - Κύπρος, Εσθονία, Λετονία, και Μάλτα)

[24] The Cybersecurity Higher Education Database (CyberHEAD) is the largest validated cybersecurity higher education database in the EU and EFTA countries. URL https://www.enisa.europa.eu/topics/cybersecurity-education/education-map/education-courses

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Τα συγκεντρωμένα αυτά δεδομένα θα χρησιμοποιηθούν για την αναγνώριση των ελλείψεων των δεξιοτήτων και την προετοιμασία προτάσεων για ένα καινούργιο πρόγραμμα μαθημάτων για την ενίσχυση των δεξιοτήτων, της εκπαίδευσης και της γνώσης των χρηστών του ίντερνετ στα τελευταία προβλήματα και απειλές που αναδύονται στον τομέα της ηλεκτρονικής ασφάλειας, και ειδικότερα - στο ηλεκτρονικό ψάρεμα.

Σε γενικές γραμμές, με βάση τα αποτελέσματα που ήρθαν στην επιφάνεια της μελέτης για το υπάρχον πρόγραμμα σπουδών για την ηλεκτρονική ασφάλειακαι τα αποτελέσματα της έρευνας,

2.2.Κύπρος

Όλα τα διάσημα πανεπιστήμια της Κύπρου προσφέρουν προπτυχιακές και μεταπτυχιακές σπουδές στην επιστήμη των υπολογιστών και στον τομέα της ηλεκτρονικής ασφάλειας. Το πτυχίο στα πανεπιστήμια της Κύπρου είναι 240 διδακτικές μονάδες και το μεταπτυχιακό κυμαίνεται απο 90 έως 120 διδακτικές μονάδες. Τα προγράμματα σπουδών διδάσκονται είται στην Ελληνική είτε στην Αγγλική γλώσσα.

Table 2. Προγράμματα Σπουδών των ΑΕΙ στον τομέα της ηλεκτρονικής ασφάλειας στην Κύπρο

Τίτλος του προγράμματος	**Επιστήμη Υπολογιστών**	**Ασφάλεια υπολογιστών και δικτύων**	**Cyber Warfare Διαδικτυακός Πόλεμος**	**Communications and Network Security Ασφάλεια δικτύων και επικοινωνιών**
Τύπος προγράμματος	Πρόγραμμα σπουδών	Πρόγραμμα σπουδών	Ενότητα Μελέτης	Ενότητα Μελέτης
Πεδίο μελέτης	Μεταπτυχιακό στην επιστήμη υπολογιστών	Μεταπτυχιακό στην επιστήμη υπολογιστών	Μεταπτυχιακό στην ηλεκτρονική ασφάλεια	Μεταπτυχιακό στην ηλεκτρονική ασφάλεια
Πτυχίο	Μεταπτυχιακό	Μεταπτυχιακό	Μεταπτυχιακό	Μεταπτυχιακό
Οργανωτικό Ίδρυμα	Πανεπιστήμιο Λευκωσίας	Ανοιχτό Πανεπιστήμιο Κύπρου	Πανεπιστήμιο Κεντρικού Λάνκασιρ	Ευρωπαϊκό Πανεπιστήμιο Κύπρου
Γλώσσα	Αγγλικά	Ελληνικά	Αγγλικά	Αγγλικά
Διάρκεια	90 Διδακτικές Μονάδες	90 Διδακτικές Μονάδες	10 Διδακτικές Μονάδες	7 Διδακτικές Μονάδες
Σε ποιό κοινό απευθύνεται	Προπτυχιακούς φοιτητές ή φοιτητές με αντίστοιχο πτυχίο	Προπτυχιακούς φοιτητές ή φοιτητές με αντίστοιχο	Προπτυχιακούς φοιτητές ή φοιτητές με αντίστοιχο πτυχίο	Προπτυχιακούς φοιτητές ή φοιτητές με αντίστοιχο πτυχίο

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Θέματα ή ενότητες	• Ηλεκτρονικά φυσικά συστήματα και το • Διαδίκτυο των πραγμάτων • Κρυπτογράφηση και διαδικτυακή ασφάλεια • Κατανεμημένα συστήματα • Ηλεκτρονικός Πόλεμος • Ηθική ηλεκτρονική πειρατεία • Εργασία στην ηλεκτρονική ασφάλεια • Διαδικτυακή άμυνα και αντίποινα	• Δίκτυα Επικοινωνιών • Εγκληματολογία υπολογιστών και δικτύων • Ασφάλεια υπολογιστών και δικτύων • Κρυπτογράφηση • Διαχείριση κινσύνων συστημάτων ασφαλείας και επικοινωνιών • Μέθοδοι Έρευνας	• Βασικές αρχές ηλεκτρονικού πολέμου • Το νομικό καθεστώς του ηλεκτρονικού πολέμου και της ηθικής • Πεδίο μάψης του ηλεκτρονικού διαστήματος - Πολεμικό Κακόβουλο λογισμικό (συμπεριλαμβάνονται: Ψυχολογικά όπλα: κονωνική μηχανική, τακτικές και διαδικασίες κοινωνικής μηχανικής, κλπ.) • Προκλήσεις του ηλεκτρονικού χώρου και το μέλλον της ηλεκτρονικού αυτού πολέμου	Ανανέωση στις θεμελιώδης αρχές και συσκευές του διαδικτύου Το διαδίκτυο ως διαδρομή για ηλεκτρονικές επιθέσεις, πως το διαδίκτυο μπορεί να προστατευτεί, αδυναμές, απειλές.

Κανένα απο τα Ανώτατα Εκπαιδευτικά προγράμματα σπουδών στην Κύπρο δεν διδάσκει το ηλεκτρονικό ψάρεμα ή την κοινωνική μηχανική ως μια ξεχωριστή ενότητα. Αντιθέτως, αυτά τα θέματα συμπεριλαμβάνονται σε κάποια μαθήματα ως ενοτήτες όπως ο ηλεκτρονικός πόλεμος, Ασφάλεια Επικοινωνιών και Δικτύων, Ασφάλεια κινδύνων ασφαλείας, Ανάλυση και Διαχείριση ρίσκων ηλεκτρονικής ασφάλειας.

Ενώ σε κάποια πτυχία εμπερέχονται προγράμματα μαθηματών με ενότητες που επικεντρώνονται σε κοινωνικές δεξιότητες (π.χ., δημόσια ομιλία, ψυχολογία), τα περισσότερα μεταπτυχιακά επικεντρώνονται στην ανάπτυξη των εξειδικευμένων δεξιοτήτων των φοιτητών, παραμελώντας τις κοινωνικές δεξιότητες.

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project N°.: 2020-1-LT01-KA203-078070)

Table 3. Εκπαιδευτικά προγράμματα στον τομέα της ηλεκτρονικής ασφάλειας στην Κύπρο

Τίτλος προγράμματος	**Επίγνωση Ηλεκτρονικής ασφάλειας**	**Πιστοποιημένος και ασφαλής χρήστης υπολογιστή**	**CompTIA Security+ Πιστοποίηση**	**Εφαρμοσμένη Ηλεκτρονική ασφάλεια**
Τύπος προγράμματος	Εκπαιδευτικό πρόγραμμα	Εκπαιδευτικό πρόγραμμα	Εκπαιδευτικό πρόγραμμα	Εκπαιδευτικό πρόγραμμα
Πεδίο μελέτης	Ηλεκτρονική Ασφάλεια	Ηλεκτρονική Ασφάλεια	Ηλεκτρονική Ασφάλεια	Ηλεκτρονική Ασφάλεια
Πτυχίο	Πιστοποίηση	Πιστοποίηση	Πιστοποίηση	Πιστοποίηση
Οργανωτής	Πανεπιστήμιο Λευκωσίας και Παγκόσμιας εκπαίδευσης	ΑΚΤΙΝΑ	Εκπαιδευτικό Κέντρο Υπολογιστών Νέοι Ορίζοντες	Ινστιτούτο κοινωνικής, ηλεκτρονικής και εθνικής ασφάλειας
Γλώσσα	Αγγλικά	Αγγλικά	Αγγλικά	Αγγλικά
Διάρκεια	2 ώρες	14 ώρες	5 μέρες	12 εβδομάδες (περίπου 120 ώρες)
Σε ποιο κοινό απευθύνεται	Επιχειρηματίες, διευθυντές, προσωπικό τεχνολογίας πληροφοριών, φοιτητές/μαθητές, κλπ.	Γενικά χρήστες υπολογιστών	Επαγγελματίες και φοιτητές/μαθητές της τεχνολογίας πληροφοριών (IT)	Επαγγελματίες και σύμβουλοι ηλεκτρονικής ασφάλειας και τεχνολογίας πληρογοριών
Θέματα ή ενότητες	Ηλεκτρονική ασφάλεια, κοινωνική μηχανική/ηλεκτρονικό ψάρεμα, Επιθέσεις στα μέσα κοινωνικής δικτύωσης, ψευδείς συναγερμοί, email ηλεκτρονικού ψαρέματος, Email με κακόβουλος συνημένο αρχείο, Κακόβουλο λογισμικό, Επιθέσεις Wi-Fi, Κωδικών, Επίδειξη.	Εξασφάλιση λειτουργικών συστημάτων, Κακόβουλο λογισμικο και λογισμικό καταπολέμησης των ιών, Ιντερνετική ασφάλεια, Ασφάλεια στις ιστοσελίδες κοινωνικής δικτύωσης, Ασφάλεια επικοινωνιακών email, Κινητές συσκευές, cloud και συνδέσεις δικτύου, Δημιουργία αντιγράφων ασφαλείας και ανάκτηση κατεστραμένων δεδομένων.	Απειλές, Επιθέσεις, Αδυναμίες, Αρχιτεκτονική και σχεδιασμός, Υλοποίηση, Λειτουργίες και Αντίδραση συμβάντων.	Ηλεκτρονική ασφάλεια και ρίσκο, Τάσεις ηλεκτρονικών ρίσκων, Πρακτική εμπειρία, Πλαίσιο ηλεκτρονικής ασφάλειας απο τον Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας, Εργαλεία και τεχνικές στην αναγνώριση ηλεκτρονικών απειλών, Εκτιμήσεις κινδύνων απειλών για τις επιχειρήσεις, εκθέσεις παραπόνων και σχέδια μετριασμού.

Πολλοί δημόσιοι και ιδιωτικοί οργανισμοί προσφέρουν προγράμματα εκπαίδευσης για επαγγελματίες τεχνολογίας πληροφοριών, μαθητές, υπαλλήλους, και για το ευρύ κοινό. Η διάρκεια του προγράμματος ποικίλει απο μερικές ώρες μέχρι και μερικούς μήνες. Εξαρτάται απο το πιστοποιητικό που παρέχεται, ο συμμετέχων πρέπει να εξεταστεί για να πάρει το πιστοποιητικό σε κάποια απο τα εκπαιδετικά προγράμματα.

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Στα περισσότερα απο τα προγράμματα που είναι μεγάλης διάρκειας συμπεριλαμβάνεται και το ηλεκτρονικό “ψάρεμα” και η κοινωνική μηχανική ως διαφορετικά αντικείμενα. Αντιθέτως, τα προγράμματα μικράς διάρκειας (περίπου μίας ημέρας) επικεντρώνονται αποκλειστικά στο ηλεκτρονικό “ψάρεμα” και την κοινωνική μηχανική.

Σε κάποια απο τα εκπαιδευτικά προγράμματα τα κόστη αυτών επιχορηγούνται μερικώς απο την αρχη Ανθρώπιονου Δυναμικού και Ανάπτυξης της Κύπρου ως ένα μέρος των στρατηγικών, διενεργειών και πρωτοβουλιών της ηλεκτρονικής ασφάλειας και των ψηφιακών δεξιοτήτων[25].

[25] Human Resource and Development authority in Cyprus (HRDA), UR http://www.hrdauth.org.cy/

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

2.3.Εσθονία

Τα βασικότερα ανώτατα εκπαιδευτικά ιδρύματα που προσφέρουν προγράμματα σπουδών στην επιστήμητη των υπολογιστών και στην ηλεκτρονική ασφάλεια ειναι το Πανεπιστήμιο Τεχνολογίας του Ταλίν και το Πανεπιστήμιο του Ταρτού. Το πτυχίο στα πανεπιστήμια της εσθονίας κυμαίνεται μεταξύ 180 και 240 διδακτικές μονάδες ενώ το μεταπτυχιακό κυμαίνεται μεταξύ 60 και 120 διδακτικές μονάδες. Τα εκαπιδευτικά αυτά προγράμματα γίνονται στην Εσθονική και Αγγλική γλώσσα.

Table 4. Προγράμματα Σπουδών των ΑΕΙ στον τομέα της ηλεκτρονικής ασφάλειας στην Εσθονία

Τίτλος προγράμματος	**Μηχανική Ηλεκτρονικής Ασφάλειας**	**Ηλεκτρονική Ασφάλεια**	**Κρυπτογράφηση, εξειδίκευση του SECCLO Erasmus+**
Τύπος προγράμματος	Πρόγραμμα Σπουδών	Πρόγραμμα Σπουδών	Πρόγραμμα Σπουδών
Πεδίο μελέτης	Πτυχίο στην Μηχανική Επιστήμη	Μεταπτυχιακό στην Μηχανική Επιστήμη	Μεταπτυχιακό στην Μηχανική Επιστήμη
Πτυχίο	Πτυχίο	Μεταπτυχιακό	Μεταπτυχιακό
Οργανωτικό Ίδρυμα	Πανεπιστήμιο Τεχνολογίας του Ταλίν	Πανεπιστήμιο Τεχνολογίας του Ταλίν και Πανεπιστήμιο του Ταρτού	Πανεπιστήμιο του Ταρτού
Γλώσσα	Αγγλικά	Αγγλικά	Αγγλικά
Διάρκεια	180 Διδακτικές Μονάδες	120 Διδακτικές Μονάδες	120 Διδακτικές Μονάδες
Σε ποιό κοινό απευθύνεται	Απόφοιτοι δευτεροβάθμιας εκπαίδευσης	Πτυχιούχοι ή φοιτητές με αντίστοιχο πτυχίο	Πτυχιούχοι ή φοιτητές με αντίστοιχο πτυχίο

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project N°.: 2020-1-LT01-KA203-078070)

Θέματα ή ενότητες	Κοινωνικές, επαγγελματικές και ηθικές πτυχές της πληροφορικής · Ηλεκτρονικά μαθήματα στην πληροφορική; Λογική αλληλουχία και Διακριτά Μαθηματικά; Δεξιότητες επικοινωνίας; Υπηρεσίες υποδομής πληροφορικής · Διαχείριση Linux και Windows. Βασικές αρχές της δικτύωσης; Εισαγωγή στην Πληροφορική και τους Υπολογιστές Εισαγωγή στην ηλεκτρονική ασφάλεια; Βασικές αρχές προγραμματισμού; Τεχνολογίες Ιστού; Διακυβέρνηση και διαχείριση της ηλεκτρονικής ασφάλειας · Βασικά στοιχεία βάσης δεδομένων Ασφάλεια δικτύου υπολογιστών; Κοινωνική μηχανική; Καταγραφή και παρακολούθηση; Ασφαλής προγραμματισμός.	Προγραμματισμός υπολογιστών; Διαχείριση συστήματος; Τεχνολογία Δικτύου; Εσθονική γλώσσα και πολιτισμός; Επιχειρηματικότητα και Επιχειρηματικός Σχεδιασμός, Ανθρώπινα θέματα της ηλεκτρονικής ασφάλειας; Νομικές πτυχές της ηλεκτρονικής ασφάλειας; Διαχείριση ηλεκτρονικής ασφάλειας; Τεχνολογίες ηλεκτρονικής ασφάλειας; Κρυπτογράφηση; Διαχείριση περιστατικών στην ηλεκτρονική ασφλάλεια; Ασφαλής σχεδιασμός λογισμικού; Έργο ομαδικής εργασίας Ασφάλεια δικτύου υπολογιστών; Επιθέσεις και άμυνα συστημάτων πληροφοριών · Cybersecurity I και II · Ειδικά Θέματα Κρυπτογραφίας; Εγκληματολογία κινητού τηλεφώνου; Στρατηγικές επικοινωνίες και ασφάλεια στον κυβερνοχώρο Εξόρυξη δεδομένων; Κακόβουλο λογισμικό; Λύσεις Παρακολούθησης της Cyber Defense; Τεχνολογίες διατήρησης της ιδιωτικής ζωής Ασύρματες τεχνολογίες και ασφάλεια Blockchain; Κρυπτολογία.	Κρυπτογραφικά πρωτόκολλα; Μαθηματικά θεμέλια για την Επιστήμη των Υπολογιστών; Σεμινάριο έρευνας στην κρυπτογραφία Cryptology II, κβαντική κρυπτογραφία; Θεωρία τύπου; Εισαγωγή στη Θεωρία Κωδικοποίησης. Ανάπτυξη εφαρμογών για κινητά - Έργα, Μέθοδοι στο TCS. Ειδική Εργασία στην Κρυπτογραφία Πρόγραμμα Θεωρητικής Πληροφορικής; Εσθονικά για αρχάριους I; Σεμινάριο μεταπτυχιακού επιπέδου.

Η ανάλυση των ΑΕΙ στα εκπαιδευτικά προγράμματα στην Εσθονία δεν διδάσκουν το ηλεκτρονικό “ψάρεμα” ως διαφορετικλη ενότητα. Όμως, οι πληροφορίες του ηλεκτρονικού “ψαρέματος” μπορεί να ενσωματώνονται σε άλλες ενότητες όπως στην Εισαγωγή στην ηλεκτρονική ασφάλεια, στην ασφάλεια δικτύου υπλογιστών και άλλα.

Ωστόσο, τα μαθήματα της Μηχανικής Ηλεκτρονικλης ασφάλειας που προσφέρονται απο το Τεχνολογικό Πανεπιστήμιο του Ταλίν συμπεριλαμβάνουν την Κοινωνική Μηχανική ως ξεχωριστή ενότητα. Η ενότητα στοχεύει να παρέχει στους μαθητές μία βασική γνώση της φύσης την κοινωνικής χειραγώγησης (κυρίως στο γενικό πλαίσιο του ICT) και τις βασικές μορφές, τεχνικές (συμπεριλαμβανομένων των υβριδικών επιθέσεων με με τεχνολογικό στοιχείο) και την προστασία εναντίον του. Η διάρκεια της ενότητας ειναι 3 διδακτικές μονάδες.

Το μάθημα της ηλεκτρονικής ασφάλειας προσφέρεται απο το Τεχνολογικό Πανεπιστήμιο του Ταλίν και το Πανεπιστήμιο του Ταρτού “Οι Ανθρώπινες Πτυχές της Ηλεκτρονικής ασφάλειας”. Η ενότητα στοχεύει να προσφέρει μία περίληψη των ανρώπινων πτυχών, συγκεκριμένα τα στοιχεία την κοινωνικής χειραγώγησης και των μηχανισμών προστασίας εναντίον της. Η διάρκεια της ενότητας είναι 6 διδακτικές μονάδες.

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project N°.: 2020-1-LT01-KA203-078070)

Τα εκπαιδευτικά προγράμματα περιλαμβάνουν ένα ευρύ φάσμα εξειδικευμενων εκπαιδευτικών ενοτήτων, προσφέροντας μία καλή αναλογία μεταξύ της τεχνολογικής γνώσης που απαιτείται και της πρακτικής και εκπαίδευσης, Έχουν επίσης ενότητες μαθημάτων στις κοινωνικές δεξιότητες, όπως επικοινωνιακές δεξιότητες, επιχειριματικότητα, ψυχλογογία, κλπ.

Table 5. Εκπαιδευτικά προγράμματα στον τομέα της ηλεκτρονικής ασφάλειας στην Εσθονία

Τίτλος προγράμματος	**Ασφάλεια Εφαρμογών Ιστοτόπων**	**Διαχειριστής Ασφάλειας Δικτύου**
Τύπος Προγράμματος	Εκπαιδευτικό Πρόγραμμα	Εκπαιδευτικό Πρόγραμμα
Πεδίο Μελέτης	Πειρατεία-Χακαρισμα/ pentest	Ασφάλεια δικτύου
Πτυχίο	Πιστοποιητικό	Πιστοποιητικό
Οργανωτής	Διευκρινισμλενη Ασφάλεια	NobleProg
Γλώσσα	Αγγλικά	Αγγλικα
Διάρκεια	4 μέρες	5 μέρες
Σε ποιό κοινό απευθύνεται	Προγραμματιστές WebApp, συντηρητές, διακομιστές διαδικτύου ή παρόχους / διαχειριστές φιλοξενίας, ειδικοί ασφάλειας πληροφοριών κ.λπ.	Διαχειριστές συστήματος και διαχειριστές δικτύου, όποιος ενδιαφέρεται για αμυντικές τεχνολογίες ασφάλειας δικτύου.
Θέματα ή ενότητες	Επιθέσεις πελάτη-πλευράς: (Ασφάλεια, πηγές πληροφοριών, επικοινωνία διακομιστή-πελάτη, HTTP vs HTTPS, μέθοδοι αιτήματος HTTP, ένεση JavaScript και JavaScript, χειρισμός διευθύνσεων URL και διευθύνσεων URL, χειρισμός cookie και cookie, παραβίαση συνεδρίας και περιόδου σύνδεσης, καθορισμός συνεδρίας, αιτήσεις επιθέσεων πλαστογραφίας (CSRF & OSRF), Επιθέσεις αποκατάστασης UI, Χρήση περιεχομένου τρίτων, Συνδυασμένες επιθέσεις από πλευράς πελάτη) Επιθέσεις από πλευράς διακομιστή: (Έλεγχος ταυτότητας, κωδικοί πρόσβασης και κατακερματισμοί, ευπάθειες εξουσιοδότησης, ζητήματα επιχειρησιακής λογικής, ηλεκτρονική εισβολή, διαμόρφωση διακομιστή Web και το σύστημα αρχείων, ένεση εντολών, χειρισμός αρχείων, επιθέσεις συμπερίληψης αρχείων, μεταφόρτωση αρχείων, επιθέσεις XXE (XML eXternal Entity) , Ένεση SQL)	Εισαγωγή στην Ασφάλεια Δικτύου, Πρωτόκολλα Δικτύου, Πολιτική Ασφαλείας, Φυσική Ασφάλεια, Επιθέσεις Δικτύου (Τρέχουσες Στατιστικές, Οριστικοί Όροι: Απειλές, Επίθεση και Εκμετάλλευση, Ταξινόμηση χάκερ και επιθέσεων, πλαστογράφηση; Spamming; Eaves Droping; Phishing; War Dialing; Password Cracking, Αφαίρεση ιστοσελίδας, SQL Injection; Wire Tapping; Buffer Overflow, WarDriving; War Chalking; War Flying Denial of Service (DOS) Attacks and Distributed DOS), Σύστημα ανίχνευσης εισβολής, Firewalls, Φιλτράρισμα πακέτων και διακομιστές μεσολάβησης, Bastion Host και Honeypots, Hardening Routers, Hardening Operating Systems Security, Patch Management, Application Application, Web Security, Email Security. Κρυπτογράφηση, εικονικά ιδιωτικά δίκτυα, WLAN, δημιουργία ανοχής σφαλμάτων, αντίδραση σε περιστατικά, αποκατάσταση και προγραμματισμός καταστροφών, αξιολόγηση ευπάθειας δικτύου

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Υπάρχει ένας αριθμός ιδιωτικών (Clarified Security, NoblePro, Cyberexer, Rangeforce, CTF Pärnu, κλπ.) οργανισμών που προσφέρουν εκπαιδευτικά προγράμματα σε ποικίλα θέματα όπως ηλεκτρονική μάθηση για την υγιεινή στην ηλεκτρονική ασφάλεια και την προστασία δεδομένων, οπτικοποίηση ευπάθειας, αξιολόγηση κινδύνου, ηλεκτρονική ασφάλεια, ηλεκτρονικό "ψάρεμα", κ.λπ. Αυτά τα μαθήματα στοχεύουν βασικότερα επαγγελματίες της τεχνολογία πληροφοριών, εταιρείες και ευρύ κοινό που ενδιαφέρεται να μάθει περί αυτού του θέματος. Ανάλογα με το πιστοποιητικό που παρέχεται, οι συμμετέχοντες μπορεί να πρέπει να δώσουν κάποιες εξετάσεις ώστε να παρλάβουν το πιστοποιητικό.

Για να βοηθήσει τις τοπικές επιχειρήσεις να αντιμετωπίσουν τις απειλές της ηλεκτρονικής ασφάλειας, η αρχή των πληροφοριακών συστημάτων της Εσθονίας ξεκίνησε μία πληροφοριακή εκστρατεία που στοχεύιε τις μικές και μεσσαίες επιχειτήσεις. Η εκτρατεία επικεντρώνεται στους τύπους συμβάντων ηλεκτρονικής ασφάλειας που έχουν υποστεί τις περισσότερες οικονομικές ζημιές σε εταιρείες τα τελευταία χρόνια[26].

[26] Cyber security campaign, URL https://itvaatlik.ee/

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

2.4. Λετονία

Τα βασικότερα ανώτατα εκπαιδευτικά ιδρύματα που προσφέρουν προγράμματα σπουδών στην επιστήμητη των υπολογιστών και στην ηλεκτρονική ασφάλεια ειναι το πανεπιστήμιο της Τουρίμπα, το Τεχνολογικό Πανεπιστήμιο της Ρήγας, το πανεπιστήμιο Εφαρμοσμένων επιστημών της Βίτζεμ και η σχολη ΒΑ επιχειρήσεων και χρηματοοικονομικών. Το πτυχίο στα Λετονικά πανεπιστήμια κυμαινέται μεταξυ 160 και 240 διδακτικών μονάδων και το μεταπτυχιακο είναι 120 διδακτικές μονάδες. Τα μαθήματα γίνονται στην Λετονική και στην Αγγλική γλώσσα.

Table 6. Προγράμματα Σπουδών των ΑΕΙ στον τομέα της ηλεκτρονικής ασφάλειας στην Λετονία

Τίτλος προγράμματος	**Συστήματα Υπολογιστώμ**	**Μηχανική Ηλεκτρονικής ασφάλειας**	**Τεχνολογία Πληροφοριών**
Τύπος πορογράμματος	Πρόγραμμα Σπουδών	Πρόγραμμα Σπουδών	Πρόγραμμα Σπουδών
Πεδίο μελέτης	Πτυχίο στα συστήματα υπολογιστών	MSc in Cybersecurity Engineering Μεταπτυχιακό στην μηχανιλη ηλεκτρονικής ασφάλειας	Μεταπτυχιακό στην τεχνολογία πληροφορίων
Πτυχίο	Πτυχίο	Μεταπτυχιακό	Μεταπτυχιακό
Οργανωτικό Ίδρυμα	Πανεπιστήμιο της Τουρίμπα	Τεχνολογικό Πανεπιστήμιο της Ρηγάς	Πανεπιστήμιο εφαρμοσμένων επιστημών της Βίτζεμ
Γλώσσα	Λετονικά και Αγγλικά	Αγγλικά	Αγγλικά
Διάρκεια	240 διδακτικές μονάδες	120 διδακτικές μονάδες	120 διδακτικές μονάδες
Σε τι κοινό αναφέρεται	Απόφοιτοι δευτεροβάθμιας εκπαίδευσης	Πτυχιούχοι ή φοιτητές με αντίστοιχο πτυχίο	Πτυχιούχοι ή φοιτητές με αντίστοιχο πτυχίο

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Θέματα ή ενότητες	Αγγλικές και Λετονικές γλώσσες · Πολιτική και περιβαλλοντική άμυνα; Αρχιτεκτονική Υπολογιστών, Μηχανική Υπολογιστών και Συστήματα. Μαθηματικά; Βασικές αρχές ανάπτυξης λογισμικού; Σχεδιαστική λογική; Οικονομικά και Επιχειρηματικότητα; Δοκιμή και ποιότητα λογισμικού. Κωδικοποίηση και Κρυπτογραφία Ασφάλεια πληροφορικής και διαχείριση κινδύνων · Μηχανική εκμάθηση και ευφυείς αναλύσεις. Διαχείριση έργου λογισμικού; Ανάλυση δεδομένων και συγκριτική αξιολόγηση Συστήματα και μέθοδοι Green / IT · Εισαγωγή στην Έρευνα Επιχειρήσεων; Οικονομικά και Λογιστική; Νόμος και πνευματικά δικαιώματα IT Ρομποτική.	Ηλεκτρονική Ασφάλεια; Αξιοπιστία των Πληροφοριακών Συστημάτων; Αρχιτεκτονική Επιχειρήσεων Πληροφορικής; Βασικές αρχές ελέγχου των κρίσιμων υποδομών · Βιομηχανική ασφάλεια Ασφάλεια δικτύου; Ασφάλεια λογισμικού; Τεχνολογίες Κρυπτογραφίας και Ασφάλειας Δεδομένων. Σχεδιασμός προσαρμοστικών συστημάτων. Μηχανική Ασφάλεια Συστημάτων; Κοινωνικοτεχνική Μοντελοποίηση Συστημάτων; Εξόρυξη Δεδομένων και Ανακάλυψη Γνώσης Διαχείριση έργου; Ασφαλείς τεχνολογίες ηλεκτρονικού εμπορίου · Τεχνολογίες ολοκλήρωσης δεδομένων; Κοινωνική ευθύνη και επιχειρήσεις.	Ηθική εισβολή; Αντίστροφη μηχανική; Ασφάλεια δικτύου, κινητών και cloud Ψηφιακή εγκληματολογία; Ασφαλής σχεδιασμός λογισμικού. Αντιμετώπιση περιστατικών και αντίδραση. Μηχανική ασφάλειας συστήματος; Διαχείριση έργου; Στρατηγική διαχείριση ΤΠΕ; Εξόρυξη δεδομένων; Επικοινωνία; Κριτική σκέψη; Εργαστήριο ανάλυσης κοινωνικών μέσων; Ψυχολογία Διαδικτύου; Δικαιώματα, υποχρεώσεις και ευθύνη των φορέων στο Διαδίκτυο · Νόμος για την ασφάλεια και την έρευνα δεδομένων · Πολιτική ηλεκτρονικής ασφάλειας; Έλεγχοι και διασφάλιση συστημάτων πληροφοριών · Διαχείριση κινδύνου ασφάλειας πληροφοριών · Πολιτισμός ασφάλειας; Κρυπτογράφηση; Καινοτομία και δημιουργική επίλυση προβλημάτων.

Η ανάλυση των ΑΕΙ στα εκπαιδευτικά προγράμματα στην Λετονία δεν διδάσκουν το ηλεκτρονικό “ψάρεμα” ή την κοινωνική μηχανική ως διαφορετικές ενότητες. Όμως, οι πληροφορίες σε αυτά τα θέματα είναι ενσωματωμένες σε άλλες ενότητες όπως η τεχνολογία πληροφοριών και την διαχείριση κινδύνου, την ασφάλεια διαδικτύου, την ηλεκτρονικη ασφάλεια και την ασφάλεια πληροφοριών, την ψυχολογία του διαδικτύου και άλλα.

Όπως στην Εσθονία, τα προγράμματα σπουδών που προσφέρονται φαίνεται να είναι ευρείας βάσης και πρακτικά προσανατολισμένα, περιλαμβάνουν μαθήματα κοινωνικών δεξιοτήτων, όπως οι επικοινωνιακές δεξιότητες, η επιχειρηματικότητα, η δημιουργικότητα στην επίλυση προβλημάτων, κλπ.

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project N°.: 2020-1-LT01-KA203-078070)

Table 7. Εκπαιδευτικά προγράμματα στον τομέα της ηλεκτρονικής ασφάλειας στην Λετονία

Τίτλος προγράμματος	**ESET Remote Cyber Security Knowledge**	**IT security training for users**	**"Kiberdrošība"**
Τύπος προγράμματος	Εκπαιδευτικό πρόγραμμα	Εκπαιδευτικό πρόγραμμα	Εκπαιδευτικό πρόγραμμα
Πεδίο μελέτης	Ασφάλεια δικτύου	Ακαδημία Ηλεκτρονικής ασφάλειας	Ηλεκτρονική ασφάλεια
Πτυχίο	Πιστοποιητικό	Πιστοποιητικό	Πιστοποιητικό
Οργανωτής	ESET Λετονία	Ακαδημία Ηλεκτρονικής ασφάλειας	"Dialogs AB" Εκπαιδευτικό κέντρο
Γλώσσα	Λετονικά και Αγγλικά	Λετονικά, Αγγλικά, Ρωσσικά	Λετονικά
Διάρκεια	2 ώρες	4 ώρες	1 εβδομάδα (42 ώρες)
Σε τι κοινό αναφέρεται	Εταιρείες και υπάλληλοί τους	Διευθυντές επιχειρήσεων, διαχειριστές ασφάλειας πληροφορικής, εταιρείες και το ευρύ κοινό	Διευθυντές επιχειρήσεων, προγραμματιστές τεχνολογίας πληροφοριών, το ευρύ κοινό.
Θέματα ή ενότητες	Επισκόπηση απειλής (Τύποι κακόβουλου λογισμικού, αρχές απάτης και κοινωνική μηχανική) Θεωρίες κωδικών πρόσβασης; Εργασία εξ αποστάσεως, Ασφάλεια παντού. Anti-phishing; Ασφάλεια email (spam, phishing και απλοί απατεώνες). Διαχείριση εφαρμογών.	Γιατί είναι σημαντικό να γνωρίζετε τις απειλές για την ασφάλεια πληροφορικής; Αναγώριση του εχθρού, Φυσική ασφάλεια Ασφαλής κωδικός πρόσβασης, Κοινωνική μηχανική; Ηλεκτρονικό ψάρεμα, Λείανση; Vishing; Ασφάλεια προσωπικών δεδομένων	Λειτουργία και ρόλος της πληροφορικής · Πόροι πληροφόρησης και ο ρόλος τους ,· απειλές για την ασφάλεια των πληροφοριών, τους τύπους και τον αντίκτυπό τους,· Εργαλεία και μέθοδοι διαχείρισης ασφάλειας πληροφοριών · Σημασία τεκμηρίωσης της ηλεκτρονικής ασφάλειας.

Σύμφωνα με την έρευνα που έγινε, αρκετοί οργανισμοί προσφέρουν εκπαίδευση ηλεκτρονικής ασάλειας σε εταιρείες, επαγγελματίες τεχνολιγίας πληροφοριών, και στο ευρύ κοινό. Ενώ η μιρότερης διάρκεια εκπαίδευσης τείνει να επικεντρώνεται αποκλειστικά στους τύπους απειλών, συμπεριλαμβάνοντας το ηλεκτρονικό ψάρεμα, την κοινωνική μηχανική, και τρόπους με τους οποίους κάποιος μπορεί να προστατευτεί, η μεγαλύτερης διάκρειας εκπαίδευση προσφέρει μια ευρύτερη οπτική για την ηλεκτρονική ασφάλεια. Οι πάροχοι της εκπαίδευσης στοχεύουν κυρίως διευθυντές επιχειρήσεων, γενικούς υπαλλήλους, επαγγελματίες πληροφορικής και το κοινό που ενδιαφέρεται.

Από το 2018, το Ινστιτούτο Αντίδρασης σε Ασφάλεια Τεχνολογίας Πληροφοριών της Δημοκρατίας της Λετονίας (CERT.LV) εφαρμόζει μια ενέργεια που ονομάζεται "Βελτίωση των ικανοτήτων της ηλεκτρονικής ασφάλειας στη Λετονία" Κατά τη διάρκεια της εκστρατείας, το CERT.LV

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project N°.: 2020-1-LT01-KA203-078070)

ανέπτυξε έναν ενημερωτικό οδηγό και βίντεο, διοργάνωσε ένα συνέδριο Cybersecurity και ξεκίνησε έναν ιστότοπο που περιέχει πόρους ηλεκτρονικής ασφάλειας στο χώρο εργασίας.

Το κέντρο ασφάλειας του ίντερνετ επίσης προσφέρει επίσης δωρεάν διαδικτυακά σεμινάρια για μαθητές σχετικά με την ασφάλεια στο Διαδίκτυο. Αντιθέτως, το Κέντρο Εκπαίδευσης Τοπικής Αυτοδιοίκησης της Λετονίας προσφέρει μαθήματα για ενήλικες σχετικά με την ασφαλή χρήση του Διαδικτύου και των κοινωνικών μέσων[27].

[27] Latvian Safer Internet Centre, URL https://drossinternets.lv/lv/nodarbibas

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

2.5. Λιθουανία

Τα περισσότερα πανεπιστήμια και κολέγια στη Λιθουανία προσφέρουν πτυχία και μεταπτυχιακά στην επιστήμη των υπολογιστών ή στον τομέα της ηλεκτρονικής ασφάλειας. Το πτυχίο στα Λιθουανικά ΑΕΙ κυμαινέται μεταξύ 180 και 240 διδακτικών μονάδων και το μεταπτυχιακό κυμαίνεται μεταξύ 90 και 120 διδακτικών μονάδων. Τα μαθήματα γίνονται στην Λιθουανική και στην Αγγλική γλώσσα.

Table 8. Προγράμματα Σπουδών των ΑΕΙ στον τομέα της ηλεκτρονικής ασφάλειας στην Λιθουανία

Τίτλος προγράμματος	**Σύστημα πληρογοριών και ηλεκτρονικής ασφάλειας**	**Ασφάλεια και τεχνολογία πληροφοριών**	**Διαχείριση ηλεκτρονικής ασφάλειας**
Τύπος προγράμματος	Πρόγραμμα σπουδών	Πρόγραμμα σπουδών	Πρόγραμμα σπουδών
Πεδίο μελέτης	Πτυχίο στην πληροφορική	Μεταπτυχιακό στην μηχανική ηλεκτρονικής ασφάλειας	Μεταπτυχιακό στην διοίκιση επιχειρήσεων
Πτυχίο	Bachelor's degree Προπτυχιακό	Master's degree Μεταπτυχιακό	Master's degree Μεταπτυχιακό
Οργανωτικό Ίδρυμα	Πανεπιστήμιο του Βίλνιους	Τεχνικό Πανεπιστήμιο Γκετιμίνας του Βίλνιους	Πανεπιστήμιο Mykolas Romeris
Γλώσσα	Λιθουανικά και Αγγλικα	Αγγλικά	Λιθουανικά και Αγγλικά
Διάρκεια	210 διδακτικές μονάδες	120 διδακτικές μονάδες	90 διδακτικές μονάδες
Σε τι κοινό αναφέρεται	Απόφοιτοι δευτεροβάθμιας εκπαίδευσης	Πτυχιούχοι ή φοιτητές με αντίστοιχο πτυχίο	Πτυχιούχοι ή φοιτητές με αντίστοιχο πτυχίο

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Θέματα ή ενότητες	Θεωρία Αλγορίθμου και Δομές Δεδομένων; Μαθηματικά; Νομικοί κανονισμοί για την ηλεκτρονική ασφάλεια, Εισαγωγή στον προγραμματισμό; Πληροφοριακά συστήματα και βάσεις δεδομένων. Ψηφιακή εγκληματολογία; Λειτουργικά συστήματα και η ασφάλειά τους. Γλώσσες προγραμματισμού; WWW Τεχνολογική Ανάπτυξη; Δημιουργία Πληροφοριακών Συστημάτων; Ηλεκτρονικές συναλλαγές και η ασφάλειά τους; Χακάρισμα, Ασφάλεια πληροφοριών και διαχείριση κινδύνων · Δίκτυα υπολογιστών και η ασφάλειά τους. Ασφάλεια δεδομένων και κρυπτογραφία Σχεδιασμός Υπολογιστικών Υποδομών; Εικονικά συστήματα; Εξόρυξη δεδομένων; Δοκιμή συστημάτων πληροφοριών και διασφάλιση ποιότητας · Δικανική ανάλυση ψηφιακού περιεχομένου και ανάλυση κακόβουλου λογισμικού	Μέθοδοι ασφάλειας τεχνολογίας πληροφοριών; Βάσεις δεδομένων και ασφάλεια ηλεκτρονικών εγγράφων · Κρυπτογραφικά συστήματα; Βασικές αρχές επιστημονικής έρευνας και καινοτομίας · Δίκτυα υπολογιστών και ασφάλεια λειτουργικού συστήματος. Εικονική υποδομή και ασφάλεια υπολογιστικού νέφους · Τεχνικές χακαρίσματος; Εγκληματολογία ηλεκτρονικής ασφάλειας; Διαχείριση ασφάλειας πληροφοριών, Ασφαλής προγραμματισμός.	Οι μελέτες καλύπτουν μεθόδους ασφάλειας συστήματος και δικτύου, κρυπτογραφία, τεχνολογίες ηθικής εισβολής, διερεύνηση εγκλήματος ηλεκτρονικής ασφάλειας, διαχείριση ασφάλειας πληροφοριών και άλλες ειδικές ενότητες μαθημάτων. Υποχρεωτικά μαθήματα: Αποφάσεις ηλεκτρονικής διακυβέρνησης και ηλεκτρονικής δημοκρατίας · Νομικό περιβάλλον της ηλεκτρονικής ασφάλειας; Διαχείριση της ηλεκτρονικής ασφάλειας, Στρατηγική δημοσίων σχέσεων; Προστασία προσωπικών δεδομένων και δεδομένων Οικονομικά Ασφαλείας; Πνευματική ιδιοκτησία; Διαχείριση Έργου Πληροφορικής, Μοντελοποίηση ασφάλειας ηλεκτρονικών πληροφοριών.

Η ανάλυση των ΑΕΙ στα εκπαιδευτικά προγράμματα στην Λετονία δεν διδάσκουν το ηλεκτρονικό “ψάρεμα” ως διαφορετικές ενότητες. Όμως, οι πληροφορίες σε αυτά τα θέματα είναι ενσωματωμένες σε άλλες ενότητες όπως η ηλεκτρονική ασφάλεια, η ασφάλεια πληροφοριών και η διαχείριση κινδύνου, τα δίκτυα υπολογιστιών και η ασφάλεια αυτών η ιδιωτικότητα και η προστασία δεδομένων.

Σε αντίθεση με τα προγράμματα σπουδών που προσφέρονται στη Λετονία και την Εσθονία, τόσο οι προπτυχιακές όσο και οι μεταπτυχιακές σπουδές στη Λιθουανία φαίνεται να επικεντρώνονται κυρίως στην ανάπτυξη των τεχνικών δεξιοτήτων των μαθητών, δίνοντας λιγότερη έμφαση στη σημασία των κοινωνικών δεξιοτήτων.

Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project N°.: 2020-1-LT01-KA203-078070)

Table 9. Εκπαιδευτικά προγράμματα στον τομέα της ηλεκτρονικής ασφάλειας στην Λιθουανία

Τίτλος προγράμματος	**Εκπαίδευση γνώσεων απομακρυσμένης ηλεκτρονικής ασφάλεια ESET**	**IT security awareness training Εκπαίδευση γνώσεων σχετικά με την ασφάλεια στον τομέα της τεχνολογίας πληροφοριών**	**The Basics of Cybersecurity for Consumers Τα βασικά της ηλεκτρονικής ασφάλειας για τους καταναλωτές**
Τύπος προγράμματος	Εκπαιδευτικό πρόγραμμα	Εκπαιδευτικό πρόγραμμα	Εκπαιδευτικό πρόγραμμα
Πεδίο μελέτης	Ηλεκτρονική ασφάλεια	Ηλεκτρονική ασφάλεια	Ηλεκτρονική ασφάλεια
Πτυχίο	Πιστοποιητικό	Πιστοποιητικό	Πιστοποιητικό
Οργανωτής	ESET	UAB "Hermitage Solutions"	Vilnius University
Γλώσσα	Λιθουανικά	Λιθουανικά	Λιθουανικά
Διάρκεια	2 ώρες	6 ώρες	8 ώρες
Σε τι κοινό αναφέρεται	Εταιρείες και υπαλλήλους	Διευθυντές επιχειρήσεων, διαχειριστές ασφάλειας πληροφορικής, εταιρείες, εργαζόμενοι και το ευρύ κοινό	Ευρύ κοινό
Θέματα ή ενότητες	Ηλεκτρονικό ψάρεμα, απομακρυσμένη εργασία; Σύνδεση σε εταιρικό δίκτυο. Προληπτικά μέτρα; Επισκόπηση απειλής, Πολιτική κωδικού πρόσβασης; Διαδικτυακή ασφάλεια; Το διαδίκτυο των πραγμάτων; Ελ. προστασία μέσω email; Πρακτικές συμβουλές	Γιατί ο αλφαβητισμός ασφάλειας πληροφορικής είναι σημαντικός για όλους; Αναγνώριση της απειλής · Προστασία φυσικών δεδομένων; Κωδικοί πρόσβασης Κοινωνική μηχανική; Ηλεκτρονικό ψάρεμα Προστασία δεδομένων κινητής τηλεφωνίας; Προστασία προσωπικών δεδομένων.	Αρχές ασφάλειας προσωπικών δεδομένων · ισχυροί κωδικοί πρόσβασης δραστηριότητες κοινωνικής δικτύωσης · Αρχές χρήσης Wi-Fi; Κοινωνική μηχανική (οι πιο δημοφιλείς επιθέσεις κατά της κοινωνικής μηχανικής · πώς να αναγνωρίσετε επιθέσεις κοινωνικής μηχανικής · μέτρα ασφαλείας).

Αρκετοί δημόσιοι και ιδιωτικοί οργανισμοί προσφέρουν μαθήματα κατάρτισης ηλεκτρονικής ασφάλειας για επαγγελματίες πληροφορικής, εταιρείες, υπαλλήλους και το ευρύ κοινό. Υπάρχουν επίσης αρκετοί οργανισμοί που διοργανώνουν εξατομικευμένα μαθήματα στον τομέα της ηλεκτρονικής ασφάλειας που στοχεύουν εταιρείες και τους υπαλλήλους τους. Τα μαθήματα περιλαμβάνουν θέματα ηλεκτρονικού ψαρέματος και κοινωνικής μηχανικής και η διάρκειά τους κυμαίνεται από μερικές ώρες έως αρκετές ημέρες.

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Το 2020, η ομάδα «Δημιουργία Λιθουανίας» σε συνεργασία με το Υπουργείο Εθνικής Άμυνας και το Εθνικό Κέντρο Ηλεκτρονικής Ασφάλειας , πραγματοποίησε έρευνα και κυκλοφόρησε έναν οδηγό «Cyber Security and Business. Τι πρέπει να γνωρίζει κάθε διαχειριστής εταιρείας[28]». Ο οδηγός συζητά τη σημασία της ηλεκτρονικής ασφάλειας και παρέχει πρακτικές συμβουλές για την αξιολόγηση των κινδύνων απειλών και συστάσεων για τη διαχείριση πιθανών συμβάντων στο διαδίκτυο κ.λπ.

[28] Create Lithuania (2020): "Cyber Security and Business. What every company manager should know", UR https://www.enterpriselithuania.com/naujienos/isleistas-leidinys-kibernetinis-saugumas-ir-verslas-ka-turetu-zinoti-kiekvienas-imones-vadovas/ (accessed 17/03/2021)

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

2.6. Μάλτα

Απο τα βασικά ιδρύματα τριτοβάθμιας εκπαίδευσης που προσφέρουν προγράμματα σπουδών στην επιστήμη των υπολογιστών ή στην ηλεκτρονική ασφάλεια είναι το Πανεπιστήμιο της Μάλτας, το Αμερικανικό Πανεπιστήμιο της Μάλτας και το Κολλέγιο Τεχνών, Επιστήμης και Τεχνολογίας της Μάλτας. Το πτυχίο στα πανεπιστήμια της Μάλτας κυμαίνεται μεταξύ 180 έως 240 διδακτικές μονάδες για προπτυχιακό και μεταξύ 60 έως 120 διδακτικές μονάδες για μεταπτυχιακό. Τα προγράμματα σπουδών διδάσκονται στην αγγλική γλώσσα.

Table 10. Προγράμματα Σπουδών των ΑΕΙ στον τομέα της ηλεκτρονικής ασφάλειας στην Μάλτα

Τίτλος προγράμματος	**Επιστήμη στην Τεχνολογία Πληροφοριών**	**Ασφάλεια και Τεχνολογία πληροφοριών**	**Τεχνολιγία πληροφοριών και Πληροφοριακά Συστήματα**
Τύπος προγράμματος	Πρόγραμμα σπουδών	Πρόγραμμα σπουδών	Πρόγραμμα σπουδών
Πεδίο μελέτης	Προπτυχιακό στην ηλεκτρονική ασφάλεια	Μεταπτυχιακό στην Μηχανική ηλεκτρονικής ασφάλειας	Μεταπτυχιακό στην Τεχνολιγία πληροφοριών και Πληροφοριακά Συστήματα
Πτυχίο	Προπτυχιακό	Μεταπτυχιακό	Μεταπτυχιακό
Οργανωτικό Ίδρυμα	Ανώτατη Εκπαίδευση STC	Αμερικάνικο Πανεπιστήμιο της Μάλτας	Κολλέγιο Τεχνών, Επιστήμης και Τεχνολογίας της Μάλτας
Γλώσσα	Αγγλικά	Αγγλικά	Αγγλικά
Διάρκεια	180 ECTS 180 διδακτικές μονάδες	96 ECTS 96 διδακτικές μονάδες	90 ECTS 90 διδακτικές μονάδες
Σε τι κοινό αναφέρεται	Απόφοιτοι δευτεροβάθμιας εκπαίδευσης	Πτυχιούχοι ή φοιτητές με αντίστοιχο πτυχίο	Πτυχιούχοι ή φοιτητές με αντίστοιχο πτυχίο

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Θέματα ή ενότητες	Δεξιότητες για υπολογιστές; Συστήματα Υπολογιστών; Δίκτυα υπολογιστών; Βάσεις δεδομένων; Σχεδιασμός και ανάπτυξη ιστότοπου. Τεχνικές ανάπτυξης λογισμικού; Σχεδιασμός & ανάπτυξη αντικειμενοστρεφών προγραμμάτων, · Ανάπτυξη λύσεων γραφείου; Αρχιτεκτονική και Λειτουργίες Ηλεκτρονικής Ασφάλειας, Δικτύωση υπολογιστών; Ασφάλεια δικτύου; Χάκινγκ; Αντικειμενοστρεφής σχεδιασμός και προγραμματισμός. Εξόρυξη δεδομένων; Προηγμένα δίκτυα; Ψηφιακή ιατροδικαστική διαχείριση κινδύνων και κυβερνοασφάλειας. Αρχιτεκτονική συστημάτων και Διαδίκτυο πραγμάτων; Έργο και επαγγελματισμός με τεχνούργημα ηλεκτρονικής ασφάλειας, Ηλεκτρονική Ευφυΐα.	Μέθοδοι ασφάλειας τεχνολογίας πληροφοριών; Βάσεις δεδομένων και ασφάλεια ηλεκτρονικών εγγράφων · Κρυπτογραφικά συστήματα; Βασικές αρχές επιστημονικής έρευνας και καινοτομίας · Δίκτυα υπολογιστών και ασφάλεια λειτουργικού συστήματος. Εικονική υποδομή και ασφάλεια υπολογιστικού νέφους · Τεχνικές ηθικής εισβολής; Εγκληματολογία ηλεκτρονικής ασφάλειας; Διαχείριση ασφάλειας πληροφοριών Ασφαλής προγραμματισμός.	Πληροφοριακά Συστήματα και Διαχείριση; Λειτουργικά συστήματα και Cloud Computing. Πρωτόκολλα δικτύου και αυτοματοποίηση δικτύου, Επιστήμη δεδομένων και ανάλυση πρόβλεψης. Τα θεμέλια της ηλεκτρονικής αφάλειας; Τεχνολογίες Ιστού και Ασφαλές Ηλεκτρονικό Εμπόριο, Κινητά τηλέφωνα και δικτύωση 5G. Διαδίκτυο των πραγμάτων (IoT); Χρηματοοικονομικός υπολογισμός και κρυπτονομίσματα Διαχείριση επιχειρηματικότητας και καινοτομίας.

Όπως και σε άλλες χώρες που αναλύθηκαν (εκτός της Εσθονίας), τα προγράμματα σπουδών των ΑΕΙ της Μάλτας δεν προσφέρουν ηλεκτρονικό "ψάρεμα" ή κοινωνική μηχανική ως ξεχωριστή ενότητα. Ωστόσο, οι πληροφορίες σχετικά με αυτά τα θέματα μπορεί να ενσωματωθούν σε άλλες ενότητες μαθημάτων όπως η διαχείριση της ηλεκτρονικής ασφάλειας, η αρχιτεκτονική και οι λειτουργίες της ηλεκτρονικής ασφάλειας, η διαχείριση ασφάλειας πληροφοριών, τα θεμέλια της ηλεκτρονικής ασφάλειας, η ασφάλεια και η διασφάλιση πληροφοριών κ.λπ.

Η πλειονότητα των προγραμμάτων σπουδών επικεντρώνεται στην ανάπτυξη τεχνικών δεξιοτήτων. Από όλες τις μελέτες, τα προγράμματα που αναλύθηκαν, μόνο το Κολλέγιο Τεχνών, Επιστήμης και Τεχνολογίας της Μάλτας και το Πανεπιστήμιο της Μάλτας προσφέρουν ενότητες σπουδών που εστιάζουν σε κοινωνικές δεξιότητες, όπως Διαχείριση Επιχειρηματικότητας και Καινοτομίας, Επιχειρηματικότητα: Εκκίνηση της καινοτόμου επιχείρησής σας, διαχείριση έργων κ.λπ.

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Table 11. Εκπαιδευτικά προγράμματα στον τομέα της ηλεκτρονικής ασφάλειας στην Μάλτα

Τύπς προγράμματος	**Μαθήματα Χακινγκ**	**(CISSP)Πιστοποιημένη επαγγελματική ασφάλεια συστημάτων πληροφοριών**	**Πληροφόρηση και επαγγελματική ηλεκτρονική ασφάλεια**
Τύπος προγράμματος	Εκπαιδευτικό πρόγραμμα	Εκπαιδευτικό πρόγραμμα	Εκπαιδευτικό πρόγραμμα
Πεδίο μελέτης	Ηλεκτρονική Ασφάλεια	Συστήματα Πληροφόρησης	Ηλεκτρονική Ασφάλεια
Πτυχίο	Πιστοποιητικό	Πιστοποιητικό	Πιστοποιητικό
Οργανωτής	ICE Μάλτας	Ηλεκτρονική ασφάλεια Μάλτας	Εκπαίδευση
Γλώσσα	Αγγλικά	Αγγλικά	Αγγλικά
Διάρκεια	24 ώρες	5 μέρες	12 μέρες / 6 διδακτικές μονάδες
Σε τι κοινό αναφέρεται	Μαθητές και ευρύ κοινό	Επαγγελματίες, ελεγκτές, σύμβουλοι, ερευνητές ή εκπαιδευτές που σχετίζονται με την ασφάλεια της πληροφορικής.	Διευθυντές, Επαγγελματίες Ασφάλειας Πληροφοριών και Πληροφορικής, Λειτουργοί Συμμόρφωσης, Λογιστές κ.λπ.
Θέματα ή ενότητες	Εισαγωγή στο Χακάρισμα; Ιδρύματα δικτύωσης; Αποτύπωμα και αναγνώριση; Ερευνα; Κωδικοί πρόσβασης Sniffing; Κοινωνική μηχανική; Κρυπτογράφηση; Ασύρματα συστήματα εισβολής	Ασφάλεια και διαχείριση κινδύνων; Ασφάλεια περιουσιακών στοιχείων; Μηχανική ασφαλείας, Επικοινωνία και ασφάλεια δικτύου,· Διαχείριση ταυτότητας και πρόσβασης, · Συμβάντα ασφαλείας - Προετοιμασία, απόκριση και ανάκτηση. Αξιολόγηση και δοκιμή ασφάλειας, Επιχειρήσεις ασφαλείας, Ασφάλεια ανάπτυξης λογισμικού.	Τα θεμέλια της ασφάλειας πληροφοριών, Αξιολογήσεις ηλεκτρονικής ασφάλειας και της απόκρισης περιστατικών, Έλεγχος και διαχείριση συστημάτων πληροφοριών

Αρκετοί δημόσιοι και ιδιωτικοί οργανισμοί προσφέρουν μαθήματα κατάρτισης ηλεκτρονικής ασφάλειας για επαγγελματίες πληροφορικής, επαγγελματίες που σχετίζονται με την ασφάλεια, εταιρείες, εργαζόμενους, φοιτητές και το ευρύ κοινό. Υπάρχει επίσης ένας αριθμός ιδιωτικών οργανισμών που προσφέρουν εξατομικευμένα μαθήματα στον τομέα της ηλεκτρονικής ασφάλειας και της διείσδυσης και των δοκιμών κοινωνικής μηχανικής. Τα περισσότερα από τα μαθήματα κατάρτισης που εξετάστηκαν παρέχουν μια ευρύτερη προοπτική για την ασφάλεια στον κυβερνοχώρο αντί να επικεντρώνονται μόνο σε θέματα ηλεκτρονικού ψαρέματος ή κοινωνικής μηχανικής.

Το 2018, ξεκίνησε η Εθνική Εκστρατεία για την Ευαισθητοποίηση και την Εκπαίδευση ηλεκτρονικής ασφάλειας στη Μάλτα. Η εκστρατεία αποσκοπούσε στην ευαισθητοποίηση σχετικά με τον τρόπο βελτίωσης της ψηφιακής ασφάλειας, δίνοντας έμφαση, χαρακτηριστικά, στην ανάγκη

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

για μεγαλύτερους κωδικούς πρόσβασης και να τους αλλάζετε τακτικά, αυξάνοντας την επιφυλακτικότητα όσον αφορά την παροχή προσωπικών δεδομένων και την αγορά. Η εκστρατεία είχε επίσης ως στόχο να εκπαιδεύσει τους ανθρώπους σχετικά με τον εντοπισμό ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, την υπεύθυνη χρήση των κοινωνικών μέσων και το φαινόμενο του ηλεκτρονικού ψαρέματος (phishing).

Επιπλέον, σε συνεργασία με τον Κοινοβουλευτικό Γραμματέα Χρηματοοικονομικών Υπηρεσιών και Ψηφιακής Οικονομίας και Καινοτομίας, την ίδια χρονιά η Υπηρεσία Πληροφορικής της Μάλτας ξεκίνησε ένα νέο πρόγραμμα για την προώθηση και την ενίσχυση της ετοιμότητας ηλεκτρονικής ασφάλειας στον ιδιωτικό τομέα. Το πρόγραμμα βοηθά τον ιδιωτικό τομέα να αξιολογήσει τη στάση των ψηφιακών περιουσιακών στοιχείων τους έναντι των ηλεκτρονικών απειλών και παρέχει εκπαίδευση στους εργαζομένους[29].

Το πρότζεκτ BeSmartOnline[30] της Μάλτας! στοχεύει στην ευαισθητοποίηση και την εκπαίδευση των παιδιών, των νέων και του πεδίου υποστήριξής τους, όπως οι φροντιστές, οι γονείς και οι εκπαιδευτικοί, για την ασφαλή χρήση του Διαδικτύου με τη δημιουργία, τη λειτουργία και την προώθηση εγκαταστάσεων αναφοράς για κατάχρηση Διαδικτύου.

[29] B-SECURE Scheme, URL https://cybersecurity.gov.mt/bsecure/#1569427288152-9f8f5200-6588
[30] BeSmartOnline! project, URL https://www.besmartonline.org.mt/

Co-funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

3. ΠΕΡΊΛΗΨΗ ΚΑΙ ΚΎΡΙΑ ΠΟΡΊΣΜΑΤΑ

- Η έλλειψη δεξιοτήτων ηλεκτρονικής ασφάλειας έχει επηρεάσει το 74% των οργανισμών παγκοσμίως. Το 57% των οργανισμών είχε κενές θέσεις σε αυτόν τον τομέα το 2019. Ο χρόνος που απαιτείται για τη συμπλήρωση αυτών των θέσεων ήταν συνήθως τρεις μήνες.

- Οι πιο κρίσιμες ελλείψεις δεξιοτήτων περιλαμβάνουν την ασφάλεια υπολογιστικού νέφους (33%), την ασφάλεια εφαρμογών (32%) και την ανάλυση ασφάλειας και έρευνας (30%).

- Ένας από τους κύριους λόγους που υποδεικνύουν οι ερωτηθέντες στις θέσεις παραμένουν κενές είναι η έλλειψη ειδικευμένων αιτούντων. Σχεδόν το ένα τρίτο των οργανισμών ισχυρίστηκε ότι σχεδόν το 75% των υποψηφίων δεν είχαν τα κατάλληλα προσόντα για την εργασία. Τα πιο σημαντικά κενά δεξιοτήτων που επισημάνθηκαν από τους ερωτηθέντες ήταν η έλλειψη κοινωνικών δεξιοτήτων, η γνώση πληροφορικής, η ανεπαρκής επιχειρηματική διορατικότητα, η τεχνική εμπειρία ηλεκτρονικής ασφάλειας και η πρακτική εμπειρία.

- Το 2020, η εκτιμώμενη παγκόσμια έλλειψη εργατικού δυναμικού ηλεκτρονικής ασφάλειας ήταν περίπου 3,12 εκατομμύρια επαγγελματίες. Αντίθετα, μόνο στην Ευρώπη, το κενό εργατικού δυναμικού στον κυβερνοχώρο εκτιμάται ότι θα ανέλθει σε 350 000 εργαζόμενους έως το 2022. Ο αριθμός αυτός έχει διπλασιαστεί από ό, τι εκτιμήθηκε το 2018.

- Ο ENISA, στην έκθεση «Ανάπτυξη δεξιοτήτων στον τομέα της ηλεκτρονικής ασφάλειας στην ΕΕ», εντόπισε τέσσερις κύριες αιτίες που θα μπορούσαν να αποδοθούν στην έλλειψη δεξιοτήτων ηλεκτρονικής ασφάλειας. Δύο από αυτές επικεντρώνονται σε ζητήματα στο χώρο εργασίας, ενώ οι υπόλοιπες δύο σχετίζονται με ζητήματα στο σύστημα εκπαίδευσης και κατάρτισης.

- Το 2013, η Ευρωπαϊκή Επιτροπή δημοσίευσε την πρώτη της στρατηγική για την ηλεκτρονική ασφάλεια, επισημαίνοντας την ευαισθητοποίηση και την ανάπτυξη δεξιοτήτων ως βασικούς στρατηγικούς στόχους. Από το 2017, όλα τα κράτη μέλη της ΕΕ έχουν αναπτύξει και δημοσιεύσει τις εθνικές στρατηγικές τους για την ηλεκτρονική ασφάλεια (NCSS).

- Ένας από τους βασικούς στόχους στις εθνικές στρατηγικές ασφάλειας όλων των χωρών εταίρων του έργου είναι η ενίσχυση της διαδικτυακής εκπαίδευσης και της ευαισθητοποίησης στοχεύοντας στην ακαδημαϊκή κοινότητα, τον δημόσιο και τον ιδιωτικό τομέα και το ευρύ κοινό.

- Οι εθνικές στρατηγικές ασφάλειας σε όλες τις χώρες εταίρους του έργου δίνουν επίσης έμφαση σε δημόσιες, ιδιωτικές και ακαδημαϊκές συνεργασίες για την ενίσχυση της ανθεκτικότητας των συστημάτων ηλεκτρονικής ασφάλειας, των

Co-funded by the Erasmus+ Programme of the European Union

επενδύσεων στην ασφάλεια των ΤΠΕ, της εκπαίδευσης προσωπικού και της ανάπτυξης δεξιοτήτων ασφάλειας των μαθητών για την κάλυψη των αναγκών της αγοράς.

- Η ανάλυση των προγραμμάτων σπουδών των ΑΕΙ σε όλες τις χώρες εταίρους του έργου, εκτός από την Εσθονία, δεν περιλαμβάνει θέματα ηλεκτρονικού ψαρέματος και κοινωνικής μηχανικής ως ξεχωριστές ενότητες. Ωστόσο, οι πληροφορίες σχετικά με αυτά τα θέματα μπορεί να ενσωματωθούν σε άλλες ενότητες μαθημάτων. 2 προγράμματα σπουδών σε ΑΕΙ στην Εσθονία περιλαμβάνουν ενότητες σπουδών που εστιάζονται στην κοινωνική μηχανική. Η μέση διάρκεια τέτοιων ενοτήτων είναι 4,5 ECTS.

- Τα αναλυθέντα προγράμματα σπουδών στα ΑΕΙ στην Εσθονία, τη Λετονία και τη Μάλτα, περιλαμβάνουν ενότητες μαθημάτων σε κονωνικές δεξιότητες, όπως δεξιότητες επικοινωνίας, επιχειρηματικότητα, ψυχολογία κ.λπ. Αντίθετα, τα προγράμματα σπουδών σε ΑΕΙ στην Κύπρο και τη Λιθουανία επικεντρώνονται κυρίως στις τεχνικές δεξιότητες, δίνοντας λιγότερη έμφαση τη σημασία των κοινωνικών δεξιοτήτων.

- Σε όλες τις χώρες εταίρους, υπάρχει ένας αριθμός δημόσιων και ιδιωτικών οργανισμών που προσφέρουν μαθήματα κατάρτισης στον τομέα της ηλεκτρονικής ασφάλειας με στόχο τους επαγγελματίες της πληροφορικής, τις εταιρείες, τους υπαλλήλους και το ευρύ κοινό. Ενώ τα μαθήματα κατάρτισης μικρότερης διάρκειας τείνουν να επικεντρώνονται αποκλειστικά σε διαφορετικούς τύπους απειλών, συμπεριλαμβανομένου του ηλεκτρονικού ψαρέματος, της κοινωνικής μηχανικής και των τρόπων προστασίας του εαυτού τους, τα μαθήματα κατάρτισης μεγαλύτερης διάρκειας παρέχουν μια ευρύτερη προοπτική για την ηλεκτρονική ασφάλεια. Υπάρχουν επίσης αρκετοί οργανισμοί που προσφέρουν διείσδυση και δοκιμή κοινωνικής μηχανικής που στοχεύουν τις εταιρείες και τους υπαλλήλους τους.

Co-funded by the Erasmus+ Programme of the European Union

4. ΒΙΒΛΙΟΓΡΑΦΊΑ

5. (ISC)2 (2019): (ISC)² Study Reveals the Cybersecurity Workforce Has Grown to 3.5 Million Professionals Globally, URL https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/11/11/ISC2-Study-Reveals-the-Cybersecurity-Workforce-Has-Grown-Globally
6. (ISC)2 (2019): Cybersecurity workforce study, URL https://www.isc2.org/Research/Workforce-Study
7. Cyber Wiser (2021): Education and training in national cybersecurity strategy (LT), URL https://www.cyberwiser.eu/lithuania-lt
8. Cyber Wiser (2021): Education and training in national cybersecurity strategy (MT), URL https://www.cyberwiser.eu/malta-mt
9. Cyber Wiser (2021): Education and training in national cybersecurity strategy (LV), URL https://www.cyberwiser.eu/latvia-lv
10. Council of the European Union (2021): Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy
11. ENISA, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Latvia
12. European Commission (2013): Cybersecurity Strategy of the European Union, URL https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
13. European Commission (2019): Four EU pilot projects launched to prepare the European Cybersecurity Competence Network, URL https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network
14. European Commission (2020): Digital Europe Programme: A proposed €7.5 billion of funding for 2021-2027, URL https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027
15. European Union Agency for Cybersecurity (2019): Cybersecurity skills development in the EU
16. European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020
17. Government of the Republic Of Lithuania (2018): Resolution on the approval of the national cybersecurity strategy, URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf

Co-funded by the Erasmus+ Programme of the European Union

18. ISACA (2020): State of Cybersecurity 2020 Part 1: Global Update on Workforce Efforts and Resources, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf
19. Jon Oltsik (2019): The Life and Times of Cybersecurity Professionals 2018, URL https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/surveys/esg-issa-2018-survey-results.pdf
20. Latvian Defence Ministry (2019): Latvia approves new Cyber Security Strategy 2019-2022, URL; https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022
21. Latvian Defence Ministry (2019): Latvia's cybersecurity strategy for 2019 – 2022, URL https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
22. OCECPR (2012): Cybersecurity Strategy of the Republic of Cyprus, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus
23. The Republic of Estonia, Ministry of Economic Affairs and Communication (2019): Cybersecurity Strategy, URL https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
24. The Malta Information Technology Agency (2016): Malta Cyber Security strategy 2016, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Malta

Co-funded by the Erasmus+ Programme of the European Union