ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΖ΄ ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ
ΤΕΛΙΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ

Κυβερνοασφάλεια και αντιμετώπιση κυβερνοαπειλών για τον Δημόσιο Τομέα.

ΤΜ. ΕΞΕΙΔΙΚΕΥΣΗΣ: ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ

Επιβλέπων/ουσα:

ΠΙΠΗΣ ΑΝΔΡΕΑΣ

Σπουδαστής/στρια:

ΠΕΤΡΟΠΟΥΛΟΥ ΓΑΡΥΦΑΛΙΑ

ΑΘΗΝΑ - 2022

«Κυβερνοασφάλεια και αντιμετώπιση κυβερνοαπειλών για τον Δημόσιο τομέα»

ΑΘΗΝΑ-2022

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία πραγματεύεται το ζήτημα της κυβερνοασφάλειας και της αντιμετώπισης των κυβερνοαπειλών για τον Δημόσιο Τομέα, εστιάζοντας στο ζήτημα της κουλτούρας κυβερνοασφάλειας και στους τρόπους προαγωγής της. Αρχικά, γίνεται απόπειρα προσέγγισης των εννοιών που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, ενώ εξετάζεται το τοπίο και οι παράγοντες των απειλών. Εν συνεχεία, εξετάζονται τα τεχνικά και θεσμικά μέσα για την αντιμετώπιση των κυβερνοαπειλών σε επίπεδο υπερεθνικό αλλά και εθνικό. Περαιτέρω, αναλύεται ο ρόλος του ανθρώπινου παράγοντα στα ζητήματα ασφαλείας των οργανισμών αλλά και τα στοιχεία που συνθέτουν την έννοια της κουλτούρας κυβερνοασφάλειας και στα οποία θεμελιώνεται η δημιουργία προγραμμάτων ενίσχυσης της κουλτούρας ασφαλείας στους δημόσιους οργανισμούς. Τέλος, διερευνώνται τα βασικά συστατικά της δημιουργίας και διαχείρισης ενός ιστοτόπου που θα προσφέρει ένα πρόγραμμα επίγνωσης ασφαλείας απευθυνόμενο σε δημοσίους υπαλλήλους. Η μέθοδος που ακολουθήθηκε ήταν αυτή της βιβλιογραφικής έρευνας, η οποία συμπληρώθηκε από την δευτερογενή ανάλυση δεδομένων και την ανάπτυξη του προγράμματος εκπαίδευσης μέσω των εργαλείων για την ανάλυση, ανάπτυξη και σχεδιασμό ψηφιακού περιεχομένου. Στόχος της εργασίας είναι μια συνολική και γενική προσέγγιση του ευρύτερου πλαισίου της κυβερνοασφάλειας για τους δημόσιους οργανισμούς με απώτερο σκοπό μια συνολική πρόταση για τη δημιουργία προγραμμάτων επίγνωσης ασφαλείας.

Λέξεις κλειδιά: κυβερνοασφάλεια, κυβερνοανθεκτικότητα, κυβερνοεπίθεση, πληροφοριακό σύστημα, επίγνωση, κουλτούρα κυβερνοασφάλειας

ABSTRACT

This paper discusses the issue of cybersecurity and the ways of dealing with cyber threats by focusing on the issue of furthering cyber security culture as far as governmental organizations are concerned. Initially, an attempt is made to approach cyber security concepts while examining the threat landscape and the threat factors. Furthermore, the technical, institutional and legislative means for dealing with cyber threats at supranational and national level are examined. Moreover, the role of the human factor in the security issues of organizations, as well as the fundamental elements which compose the concept of cybersecurity culture, is analyzed. Finally, the key components of creating and managing a website that will offer a security awareness

program to civil servants are explored. The method used was that of the literature review, which was supplemented by the secondary data analysis and the development of the training program through the tools for the analysis, development and design of digital content. The purpose of this paper is a general and comprehensive approach of the overall concept of cybersecurity for governmental organizations. The ultimate aim is the general suggestion for the creation of a security awareness program.

Key words: cybersecurity, cyber- resilience, cyber-attack, information-system, awareness, cybersecurity culture

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΟΓΡΑΦΗΣΗΣ

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

CERT	Computer Emergency Response Team
CEPOL	European Union Agency for Law Enforcement Training
CKC	Cyber Kill Chain
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
ΕΕ	Ευρωπαϊκή Ένωση
ENISA	European Union Agency for Cybersecurity
EUROPOL/ΕΥΡΩΠΟΛ	European Police Office
IBM	International Business Machines Corporation)
IP	Internet Protocol Address
ITRC	Identity Theft Resource Center
LMS	Learning Management System
NIS	EU Network and Information Security directive
NIST	National Institute of Standards and technology
PWC	PricewaterhouseCoopers
VPN	Virtual Private Network
WARP	Warning, Advice and Reporting Point
WEF	World Economic Forum
XAMPP	Cross Platform Apache, Maria DB, PHP, Perl
ΑΔΑΕ	Αρχή Διασφάλισης Απορρήτου Επικοινωνιών
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΓΠΣΔΔ	Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης
ΓΕΕΘΑ	Γενικό Επιτελείο Εθνικής Άμυνας
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΕΛ.ΑΣ	Ελληνική Αστυνομία
ΕΥΠ	Εθνική Υπηρεσία Πληροφοριών
NATO	North Atlantic Treaty Organization
ΤΠΕ	Τεχνολογίες πληροφορικής και Επικοινωνιών
ΥΨΔ	Υπουργείο Ψηφιακής Διακυβέρνησης

ΔΗΛΩΣΗ

«Δηλώνω ρητά ότι, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας, δεν παραβιάζει καθ'οιονδήποτε τρόπο πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής»

Αθήνα 20/5/2022

ΠΕΤΡΟΠΟΥΛΟΥ ΓΑΡΥΦΑΛΙΑ

Ι. ΕΙΣΑΓΩΓΗ

Η κυβερνοασφάλεια αποτελεί θεμελιώδη έννοια για την ασφάλεια των πολιτών, καθώς μεγάλο μέρος της οικονομικής και κοινωνικής δραστηριότητας εξαρτάται από τη σύνδεση στο διαδίκτυο. Η ταχεία ψηφιοποίηση δημόσιου και ιδιωτικού τομέα με την ταυτόχρονη διείσδυση του διαδικτύου των πραγμάτων και της τεχνητής νοημοσύνης δημιουργούν σειρά διατομεακών αλληλεξαρτήσεων, αυξάνοντας τα τρωτά σε κυβερνοεπιθέσεις σημεία. Η εκτεταμένη χρήση νέων τεχνολογιών με χαρακτηριστικά παραδείγματα την υπολογιστική νέφους και την τεχνολογία διαχείρισης μεγάλων δεδομένων, εντείνουν την ανάγκη για τη θωράκιση των οργανισμών έναντι των κυβερνοαπειλών. Η ανάγκη για ασφαλείς ψηφιακές υποδομές θεωρείται επιτακτική, καθώς η πληροφορία και τα δεδομένα έχουν αναχθεί σε ένα από τα σημαντικότερα αγαθά.

Το πλαίσιο για την αντιμετώπιση των απειλών σε οποιοδήποτε δημόσιο οργανισμό βασίζεται στην ανάπτυξη της πολιτικής ασφαλείας, η οποία αποτυπώνει αφενός τη δέσμευση της Διοίκησης και αφετέρου τις κατευθύνσεις για την διαχείριση των απαιτήσεων ασφαλείας. Στην πολιτική ασφαλείας περιγράφονται ο σκοπός και οι στόχοι, δημιουργούνται οι ρόλοι, κατανέμονται οι ευθύνες και οι αρμοδιότητες, ορίζονται οι κανόνες και οι διαδικασίες ενώ παρέχονται συγκεκριμένες οδηγίες. Η πολιτική ασφαλείας, λαμβάνοντας υπόψη το κανονιστικό πλαίσιο, ορίζοντας το πεδίο εφαρμογής, αποτιμώντας τα αγαθά που χρήζουν προστασίας, αναλύει και διαχειρίζεται την επικινδυνότητα με την επιλογή των κατάλληλων διαδικαστικών και τεχνικών μέτρων και δημιουργεί με το σύνολο των μέτρων ασφαλείας, το Σχέδιο Ασφαλείας του οργανισμού. Προκειμένου να ευοδώσει το σχέδιο οφείλει να εφαρμόζεται η κατάλληλη οργανωτική δομή αλλά και η εκπαίδευση και ευαισθητοποίηση των χρηστών στα θέματα ασφάλειας. Η εκπαίδευση θεωρείται ένας από τους κρίσιμους παράγοντες επιτυχίας οποιουδήποτε Σχεδίου Ασφαλείας.

Ένα πρόγραμμα αύξησης της επίγνωσης για την ασφάλεια αποτελεί το μέσο για την επικοινωνία των διαδικασιών ασφαλείας στους υπαλλήλους, κατά συνέπεια γίνεται αντιληπτό ως μέσο διαμοιρασμού της γνώσης. Ο διαμοιρασμός της γνώσης αποτελεί μια πολύ σημαντική διαδικασία για κάθε οργανισμό συνιστώντας ένα από τα μέσα παραγωγής αξίας στους οργανισμούς. Πρόκειται στην πραγματικότητα για την διαδικασία μετατροπής των δεδομένων σε πληροφορία και της πληροφορίας σε γνώση, αποτελώντας στοιχείο δομικό της διαδικασίας λήψης απόφασης. Ως στοιχείο διατήρησης της οργανωσιακής μνήμης υποβοηθά την διαδικασία μεταφοράς της

γνώσης διαδικασιών, ειδικών καθηκόντων και λειτουργίας της γραφειοκρατίας από τους παλαιότερους στους νεότερους υπαλλήλους. Εντός αυτού του πλαισίου, ο μηχανισμός διαμοιρασμού της γνώσης έχει ως απώτερο αποτέλεσμα την αλλαγή οπτικής και στάσης για την ασφάλεια και την εφαρμογή της ορθής συμπεριφοράς ως δεύτερης φύσης, τη δημιουργία δηλαδή ενσυνειδησίας ασφαλείας.

Καθώς οι οργανισμοί λειτουργούν εντός ενός ευρύτερου εθνικού και υπερεθνικού πλαισίου αλλά και ενός πολυσύνθετου και συνεχώς μεταβαλλόμενου τοπίου απειλών, θα πρέπει να λαμβάνεται υπόψη το ότι η κυβερνοασφάλεια αποτελεί ένα οριζόντιο και πολυτομεακό στόχο, με τη γνώση για αυτή να προέρχεται από πολλά και διαφορετικά επιστημονικά πεδία. Η πολιτικής ασφαλείας οφείλει να συνάδει με το θεσμικό πλαίσιο αλλά και με την εθνική στρατηγική ασφαλείας. Η προστασία των πληροφοριακών συστημάτων, λόγω του εύρους και της δυναμικής των επιθέσεων, συνιστά ένα ζήτημα δημόσιας πολιτικής, που ως στόχο έχει να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα της πληροφορίας και των δεδομένων στον κυβερνοχώρο, προστατεύοντας έτσι το κράτος και την κοινωνία από τις συνέπειες των απειλών. Αναμφισβήτητα, τα κράτη αποτελούν τον κύριο δρώντα για την ανάπτυξη αυτής της πολιτικής. Κατά συνέπεια, βασική προτεραιότητα των κρατών είναι ο σχηματισμός μιας συνεκτικής στρατηγικής κυβερνοασφάλειας, η οποία συνοδευόμενη από την κατάλληλη χρηματοδότηση, αποτελεί βασικό πυλώνα του ψηφιακού μετασχηματισμού διατρέχοντας τις τομεακές δράσεις για την ψηφιοποίηση του κράτους. Παράλληλα, οποιαδήποτε στρατηγική αποτελεί μέρος μιας ευρύτερης διεθνούς και κυρίως ευρωπαϊκής συνεργασίας. Καθώς η απειλή είναι υπερεθνική, η στρατηγική υπάγεται στη διεθνή ρύθμιση και προτυποποίηση συνιστώντας μέρος της διεθνούς συνεργασίας, τόσο για την πρόληψη όσο και για την αντιμετώπιση και δίωξη του κυβερνοεγκλήματος.

ΙΙ ΚΥΡΙΟ ΜΕΡΟΣ

1 Εννοιολογικές προσεγγίσεις: το ευρύτερο πλαίσιο των οργανισμών

Στο παρόν κεφάλαιο προσεγγίζονται οι έννοιες που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, προσδιορίζοντας κατά αυτό τον τρόπο το ευρύτερο πλαίσιο εντός του οποίου οι οργανισμοί καλούνται να θωρακιστούν. Εξετάζεται το τοπίο και οι παράγοντες των απειλών αλλά και τα κίνητρά τους, στοιχεία απαραίτητα για την αξιολόγηση του κινδύνου και την δημιουργία του πλαισίου ασφαλείας. Η μέθοδος που

χρησιμοποιήθηκε ήταν αυτή της βιβλιογραφικής έρευνας με συλλογή δεδομένων από διαδικτυακές πηγές και ιστοσελίδες των επίσημων οργανισμών της Ευρωπαϊκής Ένωσης και των ΗΠΑ.

1.1 Κυβερνοασφάλεια, κυβερνοεπιθέσεις και κυβερνοανθεκτικότητα: εννοιολογικός προσδιορισμός και σημαντικότητα

Με τον όρο κυβερνοασφάλεια νοείται «το σύνολο των διασφαλίσεων και μέτρων που υιοθετούνται για την προστασία των συστημάτων πληροφοριών και των χρηστών τους έναντι μη εξουσιοδοτημένης πρόσβασης, επιθέσεων και ζημίας, ώστε να εξασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων» [1] . Η έννοια καλύπτει κάθε παράνομη δραστηριότητα, με τη χρήση ψηφιακών τεχνολογιών, στον κυβερνοχώρο συμπεριλαμβάνοντας την ασφάλεια δικτύων και συστημάτων. Τα κυβερνοπεριστατικά, άλλωστε, καλύπτουν ένα ευρύ φάσμα παράνομης δραστηριότητας: από την τυχαία κοινολόγηση πληροφοριών ως την εσκεμμένη παραπληροφόρηση και από την διαρροή δεδομένων ως την κυβερνοεπίθεση και το κυβερνοέγκλημα[2].

Ο αριθμός των κυβερνοεπιθέσεων είναι ανάλογος του αυξανόμενου ρυθμού χρήσης των νέων τεχνολογιών. Όσο η εξάρτηση από τις ψηφιακές τεχνολογίες αυξάνεται, κλιμακώνεται και η έκθεση στον κίνδυνο. Η αύξηση είναι εκθετική, κάτι που καταδεικνύεται από πληθώρα ερευνών, οι οποίες παρουσιάζουν τον πενταπλασιασμό των οικονομικών επιπτώσεων από το κυβερνοέγκλημα κατά την περίοδο 2013-2017[3], ενώ υπολογίζεται ότι το κόστος από τις κυβερνοεπιθέσεις θα βαίνει αυξανόμενο κατά 15% κάθε χρόνο ως το 2025, φτάνοντας τα 10,5$ τρις (από 3$ τρις το 2015)[4]. Η ετήσια έκθεση της PWC[5] για το 2020, βάζει την κυβερνοασφάλεια στην 3η θέση των απειλών για την προοπτική ανάπτυξης των επιχειρήσεων.

Το τοπίο των κυβερνοεπιθέσεων είναι πολυσύνθετο, με απειλές προερχόμενες από κρατικούς και μη κρατικούς παράγοντες και με κίνητρα κυρίως το οικονομικό όφελος αλλά και το πολιτικό, το στρατηγικό και το οικονομικό συμφέρον. Η έννοια του κυβερνοπολέμου κερδίζει συνεχώς έδαφος: εκστρατείες παραπληροφόρησης, ψευδείς ειδήσεις, δραστηριότητες που πλήττουν κρίσιμες υποδομές αποτελούν ένα πολλά υποσχόμενο νέο πεδίο δράσης για την επιβολή της κρατικής κυριαρχίας. Ταυτόχρονα,

[1] (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2019, σ. 40)
[2] Για τους ορισμούς βλ. ΠΑΡΑΡΤΗΜΑ 2 Ορολογία
[3] (Ευρωπαϊκή Επιτροπή, 2017, σ. 2)
[4] (The Hague Centre for Strategic Studies, 2018, σ. 36)
[5] (PwC Research , 2021)

ιδιαίτερα ζητήματα αναφορικά με την έννοια της ιδιωτικότητας και των ανθρωπίνων δικαιωμάτων αναδύονται, δημιουργώντας προκλήσεις για την δημοκρατία. Η σύνδεση στο διαδίκτυο δισεκατομμυρίων «έξυπνων» συσκευών του διαδικτύου των πραγμάτων, χωρίς η ασφάλεια να αποτελεί προτεραιότητα, δημιουργεί μεγάλο προβληματισμό σε σχέση με τις συνέπειες πιθανών επιθέσεων σε απλούς πολίτες και σε μη στρατιωτικούς στόχους. Παράλληλα, η πανδημική κρίση επιταχύνοντας την υιοθέτηση των ψηφιακών τεχνολογιών επέδρασε καταλυτικά στο τοπίο των κυβερνοεπιθέσεων, δημιουργώντας νέες προκλήσεις και προβληματισμούς.

Ευνόητα, η ανάγκη για κυβερνοανθεκτικότητα προβάλλεται ως βασικός στόχος για ένα βιώσιμο ψηφιακό μέλλον. Κυβερνοανθεκτικότητα, θεωρείται «η ικανότητα πρόβλεψης, ανίχνευσης, ανάκαμψης και προσαρμογής σε αντίξοες συνθήκες και επιθέσεις σε συστήματα που χρησιμοποιούν πόρους του κυβερνοχώρου»[6] . Λόγω του πολυσύνθετου τοπίου των απειλών, η έννοια σχετίζεται με σειρά συνεργειών σε διεθνές, ευρωπαϊκό και εθνικό επίπεδο αλλά και με την υιοθέτηση ολιστικών προσεγγίσεων ασφάλειας από τους οργανισμούς. Ως εκ τούτου, βασικότερη συνιστώσα της έννοιας θεωρείται η διακυβέρνηση ασφαλείας, ήτοι η χάραξη πολιτικών και η δημιουργία δομών για τη διασφάλιση των απαιτήσεων ασφαλείας. Αποτελεί μάλιστα κοινή αντίληψη ότι ,παρά την αναγκαιότητα και σημασία της, η τεχνική διασφάλιση από μόνη της δεν επαρκεί για την ανθεκτικότητα σε απειλές[7]. Οι οργανισμοί, πέρα από τα τεχνικά μέτρα χρειάζεται να λάβουν υπόψη τον ανθρώπινο παράγοντα, ο οποίος θεωρείται ο «πιο αδύναμος κρίκος». Τα στοιχεία από την έρευνα καταδεικνύουν ότι το 50% των κυβερνοεπιθέσεων οφείλεται σε αυτό που ονομάζεται «εσωτερική απειλή»[8], το 25% [9] των επιθέσεων προέρχονται από «ηλεκτρονικό ψάρεμα» με αύξηση κατά 600% από την αρχή της πανδημίας, ενώ το 22% σχετίζεται με ανθρώπινο λάθος. Σύμφωνα με στοιχεία από τον ENISA[10], βάσει έρευνας που έγινε σε 30 χώρες, το κόστος για την αντιμετώπιση των επιθέσεων «λυτρισμικού» αυξήθηκε από 761,106$ το 2020 σε 1,85 εκατομμύρια το 2021, ενώ η χρονική περίοδος μη λειτουργίας του συστήματος από 15 ημέρες το 2020 αυξήθηκε στις 23 το 2021. Παράλληλα, η έρευνα από το WEF[11], για το 2021 καταδεικνύει ότι το κόστος μιας παραβίασης ανέρχεται στα 3,6$ εκ. ανά περιστατικό με

[6] (NIST, 2020)
[7] Το 2019 η IBM ανέφερε ότι για την Ευρώπη και την Ασία, η εσωτερική απειλή παραμένει ανάμεσα στις τρεις πρώτες απειλές (IBM, 2019)
[8] (Tucker Bailey, 2018)
[9] (Fintech, 2020)
[10] (ENISA, 2021)
[11] (WEF, 2022)

τους οργανισμούς να χρειάζονται κατά μέσο όρο 280 μέρες για να ανακάμψουν. Στην ίδια έρευνα οι κορυφαίοι τρεις τύποι επιθέσεων είναι το «λυτρισμικό», «οι επιθέσεις κοινωνικής μηχανικής» και η «κακόβουλη εσωτερική ενέργεια». Άρα, οι δυο στις τρεις σχετίζονται με την ανθρώπινη δραστηριότητα.

Η ανθεκτικότητα βασίζεται στην ανθρώπινη προσπάθεια, τις δεξιότητες και τις γνώσεις, στις συμπεριφορές αλλά και στο αξιακό σύστημα και τις πεποιθήσεις των υπαλλήλων. Απαιτείται, κατά συνέπεια, ένα σαφές πλαίσιο ασφαλείας, στρατηγική με αντιστοιχία στους στόχους του οργανισμού, αποτελεσματική ηγεσία σε όλα τα επίπεδα του οργανισμού, αξιόπιστες διαδικασίες και καλλιέργεια της κουλτούρας ασφαλείας.

1.2 Χαρτογραφώντας την απειλή

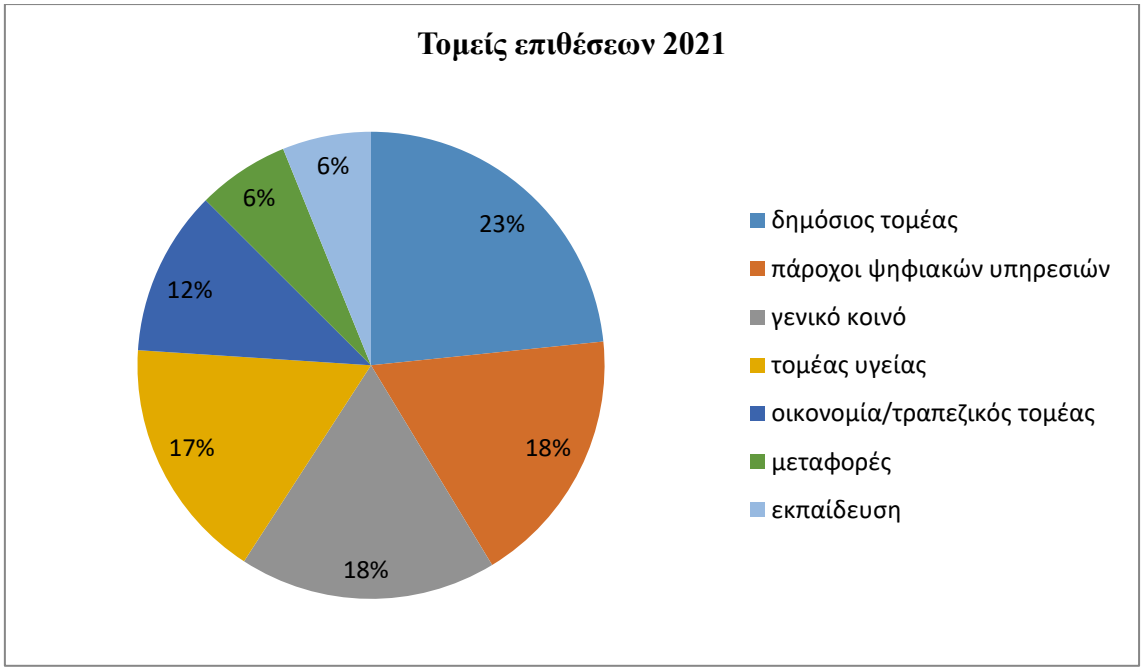
Στην προσπάθεια ανάπτυξης του πλαισίου ασφαλείας και της πολιτικής ενημερότητας και ευαισθητοποίησης του ανθρώπινου δυναμικού είναι σημαντικό να προσδιοριστούν οι πιθανές απειλές αλλά και οι πιθανές αδυναμίες του συστήματος. Απειλή σημαίνει πιθανότητα εκμετάλλευσης μιας αδυναμίας του συστήματος[12], ενώ η επίθεση σχετίζεται με την εκμετάλλευση της αδυναμίας του συστήματος. Ο NIST[13], ορίζοντας την απειλή, τονίζει ότι πρόκειται για «οποιαδήποτε περίσταση ή γεγονός που ενδέχεται να επηρεάσει αρνητικά τις οργανωτικές λειτουργίες: αποστολή, λειτουργίες, εικόνα/φήμη, οργανωτικά και περιουσιακά στοιχεία, οργανισμών ή ατόμων μέσω μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης πληροφοριών ή/και άρνησης υπηρεσίας». Ο ορισμός αναφερόμενος στους τύπους των απειλών, αποτελεί τη βάση για τη δημιουργία της τυπολογίας.

Τύποι απειλής θεωρούνται η μη εξουσιοδοτημένη πρόσβαση, η καταστροφή, η αποκάλυψη ή τροποποίηση της πληροφορίας και η άρνηση της υπηρεσίας. Από αυτές η μη εξουσιοδοτημένη πρόσβαση απειλεί την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα και ως εκ τούτου αποτελεί μια «μετά-απειλή», υπό την έννοια ότι αν μια μη εξουσιοδοτημένη οντότητα αποκτήσει πρόσβαση σε ένα σύστημα δύναται να αποκαλύψει, τροποποιήσει, καταστρέψει την πληροφορία αλλά και να δημιουργήσει άρνηση υπηρεσίας. Μια απειλή δύναται να προέρχεται από το εξωτερικό ή το εσωτερικό περιβάλλον του οργανισμού με κίνητρο την κλοπή, την κατασκοπεία, την απάτη, την δολιοφθορά ώστε να αποκομιστεί κάποιο όφελος οικονομικό ή και πολιτικό.

[12] (ISO/IEC, 2022)
[13] (NIST, 2020)

Δύνανται, όμως, να οφείλεται και σε ανθρώπινο λάθος που προέρχεται από άγνοια ή απροσεξία του χρήστη.

Οι στόχοι της απειλής μπορεί να είναι τα άτομα, οι οργανισμοί, η εφοδιαστική αλυσίδα ή οι κοινωνικές ομάδες. Σύμφωνα με την IBM[14] το 2020 ο δημόσιος τομέας κατέλαβε την 6η θέση στους στόχους των κυβερνοεπιθέσεων (7,9% των επιθέσεων στράφηκαν προς τον δημόσιο τομέα). Ο δημόσιος τομέας για το 2021 καταλαμβάνει υψηλή θέση λόγω του σημαντικού ρόλου που διαδραμάτισε κατά την περίοδο της πανδημίας. Στο παρακάτω διάγραμμα διακρίνονται οι κυριότεροι τομείς επιθέσεων για το 2021[15], βάσει των στοιχείων από τον ENISA:



Εικόνα 1 Τομείς επιθέσεων 2021, ίδια επεξεργασία με excel

Αντίστοιχα, το συμφέρον από μια κυβερνοεπίθεση διαφοροποιείται ανάλογα με το στόχο. Η επίθεση σε ένα χρήστη μπορεί να στοχεύει στην ιδιωτικότητα ή την φυσική του ασφάλεια, σε ένα οργανισμό στην φήμη και την εμπιστοσύνη του, ενώ σε μια ή πολλές κοινωνικές ομάδες δύναται να συνιστά επίθεση στην δημοκρατική έννομη τάξη. Το οικονομικό όφελος διαπερνά οριζόντια την πλειοψηφία των επιθέσεων, χωρίς να είναι το μόνο ή το πιο επικίνδυνο. Οι απειλές προέρχονται από τα κράτη και αφορούν απειλές σε άλλα κράτη για γεωπολιτικούς και στρατηγικούς λόγους, τους κυβερνοεγκληματίες, αφορούν τυπική παράνομη και εγκληματική δραστηριότητα που

[14] (IBM, 2021)
[15] (ENISA, 2021)

μεταφέρεται στο διαδίκτυο και από τους ακτιβιστές του διαδικτύου με κίνητρο ιδεολογικό και πολιτικό.

1.3 Ταξινομία των επιθέσεων

Βάσει της διεθνούς προτυποποίησης[16], οι επιθέσεις διαχωρίζονται σε παθητικές και ενεργητικές και η βασική διαφοροποίηση τους είναι ότι στην πρώτη περίπτωση ο επιτιθέμενος δεν επηρεάζει την ομαλή λειτουργία του συστήματος συλλέγοντας πληροφορίες και δεδομένα χωρίς να γίνεται αντιληπτός από τον χρήστη, ενώ στη δεύτερη περίπτωση παρεμβαίνει και τροποποιεί τον τρόπο λειτουργίας του συστήματος. Η παθητική επίθεση αφορά στην μη εξουσιοδοτημένη παρακολούθηση και υποκλοπή των δεδομένων. Είναι αρκετά δύσκολο να ανιχνευτεί, αφού δεν περιλαμβάνει κάποια αλλαγή στα δεδομένα καθώς και τα δυο μέρη δεν αντιλαμβάνονται εύκολα ότι κάποιος τρίτος διάβασε τα μηνύματα ή αντιλήφθηκε τη φύση της επικοινωνίας. Η υιοθέτηση προληπτικών μέτρων, κυρίως αυτού της κρυπτογράφησης, αποτελεί μια ενδεδειγμένη πρακτική για την αντιμετώπιση των παθητικών απειλών.

Κάποιες από τις μορφές της ενεργητικής επίθεσης είναι η «άρνηση υπηρεσίας», η «μεταμφίεση», η «εξαντλητική αναζήτηση κωδικού». Στις περιπτώσεις αυτές δημιουργείται διαταραχή και τροποποίηση στη ροή των δεδομένων, ενώ παρά το γεγονός ότι είναι πιο εύκολα ανιχνεύσιμες, είναι δύσκολη η λήψη προληπτικών μέτρων λόγω του ότι εκμεταλλεύονται ένα ευρύ φάσμα αδυναμιών. Κατά συνέπεια, η αντιμετώπιση περιλαμβάνει κυρίως ανιχνευτικά μέτρα.

Η επίτευξη του στόχου γίνεται με τη χρήση διαφόρων εργαλείων επίθεσης που συσχετίζονται με τους προαναφερθέντες τύπους των απειλών αλλά και τα είδη των επιτιθέμενων. Για παράδειγμα, η επίθεση «κατανεμημένης άρνησης υπηρεσίας» χρησιμοποιείται συχνότερα από ακτιβιστές[17], ενώ η μη εξουσιοδοτημένη πρόσβαση αποτελεί βασικό τύπο για τους κυβερνοεγκληματίες, καθώς μέσω αυτής διαπράττουν σειρά από απάτες.

1.4 Το τοπίο των επιθέσεων

Οι κυβερνοαπειλές τα τελευταία χρόνια (2018-2021)[18] αυξάνονται σταθερά, με τους επιτιθέμενους να εφευρίσκουν συνεχώς νέους και πιο σύνθετους τρόπους επιθέσεων. Το ξέσπασμα της πανδημικής κρίσης επέδρασε καταλυτικά και στο τοπίο των

[16] (William, 2017, σσ. 25-27)
[17] (European Parliament, , 2015)
[18] Βάσει των εκθέσεων του ENISA 2018-2021

επιθέσεων αυξάνοντας την επιφάνεια επίθεσης, λόγω της αυξημένης διασυνδεδεμένης παρουσίας των εργαζομένων και του υβριδικού περιβάλλοντος εργασίας. Ταυτόχρονα, η αύξηση των διασυνδεδεμένων συσκευών στρέφει προς αυτή την κατεύθυνση πληθώρα επιθέσεων, κυρίως «άρνησης υπηρεσίας» και «λυτρισμικού», ενώ παρουσιάζεται έντονα το φαινόμενο της παραπληροφόρησης. Σημαντική τάση είναι αυτή της στόχευσης των πλατφορμών κοινωνικής δικτύωσης. Ο αριθμός των θυμάτων από επιθέσεις εξαπάτησης συνεχίζει να αυξάνεται, καθώς εκμεταλλεύεται τον ανθρώπινο παράγοντα. Βάσει πρόσφατων στοιχείων της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος [19] , το πρώτο τέταρτο του 2022 υποβλήθηκαν 3.000 καταγγελίες, την ίδια στιγμή που για ολόκληρο το 2021 οι καταγγελίες ήταν 7.500.

Οι κυριότερες απειλές για το 2021, σύμφωνα με τον ENISA είναι:

- Το κακόβουλο ή ιομορφικό λογισμικό, αποτελεί το κύριο εργαλείο μιας κυβερνοεπίθεσης. Στην κατηγορία εντάσσονται διαφορετικά είδη υλισμικού και κώδικα, αλλά και διάφορες παραλλαγές οι οποίες χρησιμοποιούνται ανάλογα με το στόχο. Το λογισμικό τύπου «δούρειος ίππος», στοχεύει συχνότερα τα τραπεζικά συστήματα ή τις κινητές συσκευές ενώ το «λυτρισμικό» συχνά μολύνει οργανισμούς και εταιρείες. Τα «βακτήρια» απειλούν τη διαθεσιμότητα καθώς καταναλώνουν πόρους, ενώ οι «κερκόπορτες» αποτελούν ένα από τα σημαντικότερα εργαλεία απειλής της απαίτησης για εξουσιοδοτημένη πρόσβαση. Ιδιαίτερη μνεία γίνεται στο «λυτρισμικό», το οποίο παρουσιάζει αύξηση τα τελευταία χρόνια. Πρόκειται για πρόγραμμα που κρυπτογραφεί τα δεδομένα του οργανισμού και απαιτεί πληρωμή για να αποκαταστήσει την πρόσβαση ή για να μην αποκαλύψει τα δεδομένα. Η μέθοδος πληρωμής είναι συνήθως τα κρυπτονομίσματα, λόγω ανωνυμίας. Είναι σημαντικό να τονιστεί ότι κατά τη διάρκεια του 2020[20], οι περισσότερες επιθέσεις με λυτρισμικό έγιναν μέσω «ηλεκτρονικού ψαρέματος».
- «Κρυπτοπειρατεία», ο επιτιθέμενος μυστικά χρησιμοποιεί τον υπολογιστή του θύματος για να δημιουργήσει κρυπτονομίσματα, μέσω της εγκατάστασης κακόβουλων σεναρίων. Αυτού του τύπου οι επιθέσεις αυξήθηκαν το 2021 σε σχέση με τα προηγούμενα χρόνια: 117% το α τέταρτο του 2021 λόγω του οικονομικού οφέλους από τις τιμές των κρυπτονομισμάτων. Και σε αυτή την περίπτωση, η επίθεση σχετίζεται με τον χρήστη αφού γίνεται ή με την επίσκεψη

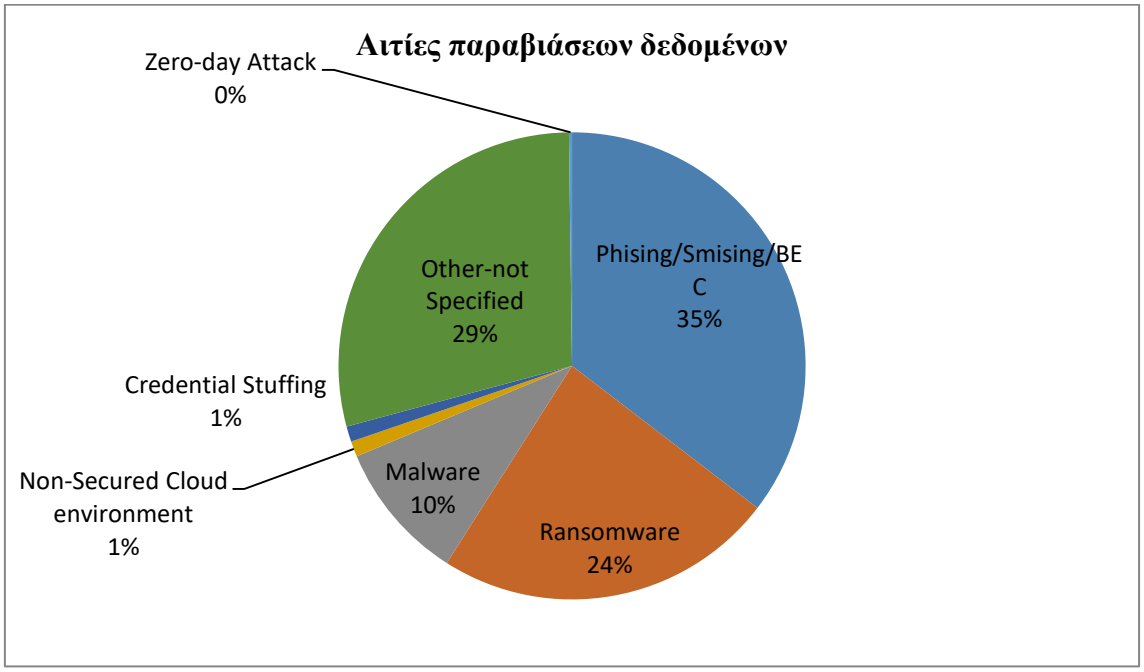
[19] (Η ΚΑΘΗΜΕΡΙΝΗ Παπαδόπουλος, 2022, Μάιος)
[20] (Coveware, 2021)

σε ιστοτόπους μολυσμένους και το κατέβασμα μολυσμένων αρχείων ή και μέσω διαφημίσεων.

- Απειλές κατά της διαθεσιμότητας και της ακεραιότητας των δεδομένων: «επιθέσεις από το διαδίκτυο» και «κατανεμημένη άρνηση υπηρεσίας». Συχνά δρουν συνδυαστικά και καλύπτουν μια τεράστια επιφάνεια επίθεσης. Η «κατανεμημένη άρνηση υπηρεσίας», δύναται να χτιστεί πάνω σε μια «διαδικτυακή επίθεση». Μέσω ενός μολυσμένου συνδέσμου, σεναρίου ή κατεβάσματος αρχείων μπορεί να δημιουργηθεί ένα «botnet», το οποίο στη συνέχεια χρησιμοποιείται για να αποστείλει αριθμό αιτημάτων ικανών ώστε το σύστημα ή ιστοσελίδα να μην ανταποκρίνεται. Φαίνεται πως η αύξηση των διασυνδεδεμένων συσκευών δημιουργεί ιδιαίτερη ανησυχία αναφορικά με αυτού του τύπου τις επιθέσεις. Η αυξητική τους τάση κατά τα τελευταία χρόνια παραμένει, ενώ από το 2020 παρουσιάστηκαν περιστατικά συνδυασμού του «λυτρισμικού» με την «άρνηση υπηρεσίας». Δηλαδή πραγματοποίηση της επίθεσης και στη συνέχεια απαίτηση λύτρων για να σταματήσει. Η πανδημία λειτούργησε και εδώ ενισχυτικά, καθώς το 2020 είχαμε πάνω από 10 εκατομμύρια τέτοιου τύπου επιθέσεις, περίπου 1,6 εκατομμύρια παραπάνω από το 2019. Οι τηλεδιασκέψεις και το υλισμικό για απομακρυσμένη συνεργασία τύπου Skype, Zoom, Teams αποτελούν μια από τις κυριότερες αιτίες για την αύξηση, λόγω αφενός των αδυναμιών στα συστήματα αυτά και αφετέρου λόγω της μεγάλης κατανάλωσης του «εύρους ζώνης», που καθώς χρησιμοποιείται για την λειτουργία αυτών των συστημάτων και της τηλεργασίας, μειώνει τη δυνατότητα του οργανισμού να αμυνθεί.
- «Απειλές σχετιζόμενες με το ηλεκτρονικό ταχυδρομείο». Διαχρονικά αποτελούν τους πιο κοινούς τρόπους επίθεσης, συσχετίζονται με αυτό που ονομάζουμε «επιθέσεις κοινωνικής μηχανικής», καθώς εκμεταλλεύονται τις αδυναμίες της ανθρώπινης φύσης. Στόχος είναι ο χρήστης του συστήματος. Ο επιτιθέμενος, εκμεταλλευόμενος τις αδυναμίες του ανθρώπινου χαρακτήρα, προσπαθεί να εξαπατήσει ή να χειραγωγήσει τον χρήστη, υποκλέπτοντας στοιχεία που δύνανται να χρησιμοποιηθούν ακόμα και για κυβερνητική κατασκοπεία. Σχετίζονται λιγότερο με τις ευπάθειες του συστήματος και περισσότερο με την γνώση και ευαισθητοποίηση του τελικού χρήστη και την εκμετάλλευση της εμπιστοσύνης. Το φάσμα αυτών των επιθέσεων είναι ιδιαίτερα ευρύ και εντάσσεται στην κατηγορία του «ηλεκτρονικού ψαρέματος». Παράλληλα,

υπάρχει η μέθοδος του «ενδιαμέσου», όπου οι δράστες αποκτούν μη εξουσιοδοτημένη πρόσβαση, κυρίως μέσω επίθεσης κοινωνικής μηχανικής και παρεμβαίνουν σε τμήματα της ηλεκτρονικής αλληλογραφίας με σκοπό να δημιουργήσουν ψεύτικη συναλλαγή. Τέλος, ιδιαίτερα συνήθης είναι κάθε τύπου «ανεπιθύμητη αλληλογραφία». Είναι ευνόητο, ότι η πανδημική κρίση οδήγησε στην αύξηση αυτού του τύπου των επιθέσεων.

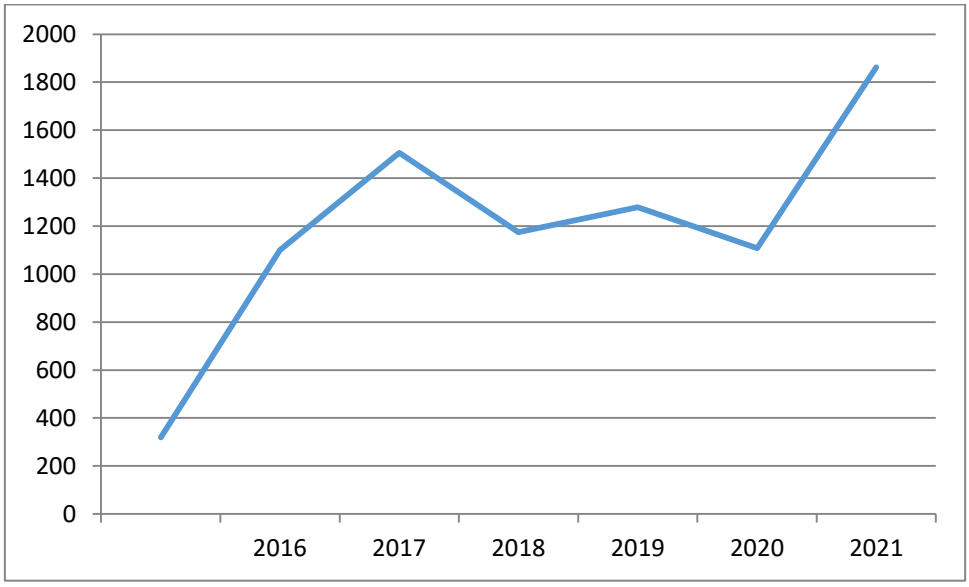
- «Απειλές κατά των δεδομένων», αποτελούν αποτέλεσμα μιας κυβερνοεπίθεσης. Σύμφωνα με τις τελευταίες έρευνες[21], το 85% σχετίζεται με τον ανθρώπινο παράγοντα καθώς οι επιθέσεις κοινωνικής μηχανικής, το ανθρώπινο λάθος αλλά και η μη ορθή δημιουργία και διαχείριση των κωδικών αποτελούν τις κυριότερες αιτίες. Η «κλοπή ταυτότητας» αποτελεί το βασικότερο κίνητρο αυτών των επιθέσεων. Η αυξανόμενη σημασία των δεδομένων για την εποχή μας οδηγεί και στην εύρεση πολλών και νέων τρόπων επίθεσης. Πάντως το μεγαλύτερο μέρος των παραβιάσεων δεδομένων οφείλεται στις επιθέσεις κοινωνικής μηχανικής[22], όπως φαίνεται και στο παρακάτω διάγραμμα:



Εικόνα 2 Παραβιάσεις δεδομένων για το 2021: οι κυριότερες αιτίες, ίδια επεξεργασία με excel

[21] (ENISA, 2021, σ. 63)
[22] Βάσει στοιχείων από (Verizon, 2020) και (ITRC, Identity Theft Resource Center, 2022)

Οι παραβιάσεις δεδομένων έχουν σχεδόν εξαπλασιαστεί από το 2015 , όπως άλλωστε φαίνεται και στην παρακάτω σύγκριση επιθέσεων από το 2015 και εξής βάσει έρευνας από την ITRC[23]:



Εικόνα 3 Παραβιάσεις δεδομένων από το 2015, ίδια επεξεργασία με excel

Ταυτόχρονα, στον δημόσιο τομέα οι επιθέσεις κοινωνικής μηχανικής αποτελούν το κυρίαρχο μοτίβο για την παραβίαση δεδομένων: το 70% των παραβιάσεων οφείλεται σε επιθέσεις κοινωνικής μηχανικής, σύμφωνα με τον ENISA[24]. Εύλογα, οι επιθέσεις αυτές κατά την περίοδο της πανδημικής κρίσης εστίασαν στα ιατρικά αρχεία αλλά και στις πληροφορίες που θα μπορούσαν να αντληθούν από την διαδικασία των εμβολίων. Μέσα σε ένα χρόνο η αύξηση των επιθέσεων στο σύστημα υγείας ήταν κατακόρυφη.

- «Παραπληροφόρηση» και «διασπορά ψευδών ειδήσεων». Ιδιαίτερη μνεία γίνεται σε αυτό το είδος της υβριδικής απειλής, η οποία εντάσσεται στο τοπίο των κυβερνοαπειλών αποτελώντας κίνητρο αλλά και επίθεση με εκμετάλλευση των αυτοματοποιημένων συστημάτων[25] αλλά και της ανθρώπινης φύσης. Οι αλγόριθμοι των προτεινόμενων θεμάτων και των «τάσεων» συνεισφέρουν στην κυκλοφορία των ψευδών ειδήσεων ενώ πληθώρα ιστοτόπων, προκειμένου να κερδίσουν χρήματα από τη διαφήμιση, διαδίδουν τις ειδήσεις αυτές. Η δυσκολία εξακρίβωσης της ακρίβειας και της πηγής της πληροφορίας δημιουργούν ένα πολύπλοκο ζήτημα που πλήττει την εμπιστοσύνη, τη βάση της

[23] (ITRC, Identity Theft Resource Center, 2022)
[24] (ENISA, 2021)
[25] Σύμφωνα με μελέτες τα social bots στο Twitter αντιπροσωπεύουν το 5% ως 15 % των χρηστών, (ENISA, 2021)

κυβερνοασφάλειας. Στόχος είναι η δημιουργία αβεβαιότητας και απάθειας απέναντι στην αλήθεια, την ίδια στιγμή που η ανακριβής πληροφορία διαταράσσει τους στόχους οποιασδήποτε δημόσιας πολιτικής. Τα μέσα κοινωνικής δικτύωσης και το «ηλεκτρονικό ψάρεμα» αποτελούν το κυριότερο μέσο για τη διάδοση της παραπληροφόρησης. Οι τεχνικές ιδιαιτερότητές τους επιτρέπουν την ταχύτατη διάδοση και εξάπλωση της ψευδούς είδησης, ενώ το αυτό ενισχύεται από το γεγονός ότι οι άνθρωποι στις κοινωνικές τους σχέσεις ανταλλάσσουν πληροφορία με ανθρώπους που έχουν τις ίδιες αντιλήψεις[26]. Ταυτόχρονα, λόγω του υβριδικού χαρακτήρα, υπάρχει δυσκολία μέτρησης της απειλής κάτι που κάνει την λήψη αντίμετρων ιδιαίτερα πολύπλοκη. Η συνθετότητα ενισχύεται από το γεγονός του συσχετισμού της με τον ανθρώπινο παράγοντα. Έρευνα του Ευρωβαρόμετρου το 2018[27] καταδεικνύει ότι το 85% των Ευρωπαίων θεωρεί το ζήτημα της παραπληροφόρησης μεγάλο πρόβλημα για τη χώρα του. Η πρόσφατη εμπειρία από την πανδημική κρίση ενισχύει τις παρατηρήσεις αυτές: ο παγκόσμιος οργανισμός Υγείας, αναφέρεται στην πανδημική κρίση ως «πανδημία πληροφορίας»[28].

2. Αντιμετώπιση των κυβερνοαπειλών

Στο παρόν κεφάλαιο εξετάζονται τα μέσα για την αντιμετώπιση των κυβερνοαπειλών σε επίπεδο υπερεθνικό αλλά και εθνικό. Αναφέρονται το θεσμικό πλαίσιο και οι επικρατέστερες προσεγγίσεις και αρχιτεκτονικές ασφαλείας. Η μέθοδος που ακολουθήθηκε είναι αυτή της βιβλιογραφικής έρευνας.

2.1 Το διεθνές και ευρωπαϊκό πλαίσιο

Από την πρώτη δεκαετία του 2000, οπότε και ξεκινά η νέα εποχή του Διαδικτύου 2.0, διαφαίνεται έντονα η ανάγκη της δημιουργίας ενός διεθνούς πλαισίου αναφοράς για την συνεργασία κατά του κυβερνοεγκλήματος. Το 2001, η σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης, αποτελεί την πρώτη διεθνή πράξη ορισμού των εγκλημάτων που διαπράττονται μέσω διαδικτύου.

Η δεύτερη δεκαετία του 2000 θέτει στο επίκεντρο την κυβερνοασφάλεια. Η μαζικοποίηση των επιθέσεων και το εύρος των επιπτώσεών τους, οδηγούν στην

[26] Το φαινόμενο ονομάζεται Echo chamber effect περισσότερα. (Dr Amy Ross Arguedas, 2022)
[27] (Ευρωβαρόμετρο , 2018)
[28] Infodemic (WHO, 2020)

υιοθέτηση θεσμικών, διοικητικών αλλά τεχνικών αντίμετρων καθώς και στην εντατικοποίηση της έρευνας στον τομέα αυτό. Σταδιακά αρχίζει να δημιουργείται ένα συνεκτικό θεσμικό και κανονιστικό πλαίσιο. Μεγάλη έμφαση δίνεται αφενός στην προτυποποίηση και τις κατευθυντήριες για την δημιουργία εθνικών στρατηγικών κυβερνοασφάλειας και αφετέρου στην πολυεπίπεδη συνεργασία για την αντιμετώπιση του κυβερνοεγκλήματος.

Η ΕΕ αντιλαμβανόμενη την αυξανόμενη επίδραση του διαδικτύου και την σημασία των ΤΠΕ ως άξονα οικονομικής μεγέθυνσης για την ολοκλήρωση της ψηφιακής αγοράς, από το 2001 καταρτίζει σειρά πολιτικών που σχετίζονται με την κυβερνοασφάλεια. Από το 2013 έχουν εκδοθεί στρατηγικές, οδηγίες, κανονισμοί, ανακοινώσεις και κατευθυντήριες που καταδεικνύουν ότι η κυβερνοασφάλεια αποτελεί μια από τις οριζόντιες διαστάσεις και προτεραιότητες για την προσαρμογή της Ευρώπης στην ψηφιακή εποχή. Στο παρακάτω πλαίσιο παρουσιάζονται συγκεντρωτικά και διαχωρίζονται οι στρατηγικές από τις νομοθετικές πρωτοβουλίες της ΕΕ:

Στρατηγικές Ε.Ε	Νομοθετικές πρωτοβουλίες Ε.Ε
2013: Στρατηγική για την Ασφάλεια στον Κυβερνοχώρο: για ένα ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο	2013 οδηγία 2013/40/εε του ευρωπαϊκού κοινοβουλίου και του συμβούλιου για τις επιθέσεις κατά συστημάτων πληροφοριών
2015: Ευρωπαϊκό Θεματολόγιο για την Ασφάλεια με στόχο την βελτίωση της επιβολής του νόμου	2014 Κανονισμός e-IDAS, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης
2015: Στρατηγική για την Ψηφιακή Αγορά με στόχο την καλύτερη πρόσβαση και την ενίσχυση της διαδικτυακής ασφάλειας	2016 Οδηγία NIS
2016: Συνολική Στρατηγική της ΕΕ, εισάγει την παραπληροφόρηση στα ζητήματα κυβερνοασφάλειας	2018 Τίθεται σε ισχύ ο Γενικός Κανονισμός Προστασίας Δεδομένων
2017: ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ	2019 ΠΡΑΞΗ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ
2020: ΕΠΙΚΑΙΡΟΠΟΙΗΣΗ ΤΟΥ ΘΕΜΑΤΟΛΟΓΙΟΥ ΚΑΙ ΕΓΚΡΙΣΗ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΕΕ ΓΙΑ ΤΗΝ ΕΝΩΣΗ ΑΣΦΑΛΕΙΑΣ	2019, ΑΠΟΦΑΣΗ ΚΕΠΠΑ 2019/797, ΣΧΕΤΙΚΑ ΜΕ ΤΑ ΠΕΡΙΟΡΙΣΤΙΚΑ ΜΕΤΡΑ ΚΑΤΑ ΤΩΝ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΠΟΥ ΑΠΕΙΛΟΥΝ ΤΗΝ ΕΝΩΣΗ Ή ΤΑ ΚΡΑΤΗ ΜΕΛΗ ΤΗΣ.

Εικόνα 4 Το Ευρωπαϊκό θεσμικό πλαίσιο, ίδια επεξεργασία με Canva

Η κυβερνοασφάλεια αποτελεί πρωτίστως ευθύνη των κρατών μελών, με την ΕΕ να διαδραματίζει ρόλο στην ανάπτυξη ενός κοινού ρυθμιστικού πεδίου προκειμένου για την εύρυθμη λειτουργία της εσωτερικής αγοράς. Το πλαίσιο της ΕΕ συνίσταται σε μια

σειρά αρχών. Καταρχάς, η κυβερνοασφάλεια συναρτάται με την προστασία των θεμελιωδών αρχών και αξιών της Ένωσης και νοείται ως εφαρμογή των αρχών αυτών στον ψηφιακό κόσμο. Κατά δεύτερον, αναγνωρίζεται ο ρόλος των κυβερνήσεων αναφορικά με τη διασφάλιση της πρόσβασης και την προστασία των δικαιωμάτων και κατά τρίτον η συνεργασία κράτους και ιδιωτικού τομέα κρίνεται ως εκ των ων ουκ άνευ για την ολοκλήρωση της ψηφιακής εσωτερικής αγοράς. Η ανθεκτικότητα, η αποτροπή και η άμυνα αποτελούν τους τρεις κύριους πυλώνες των μέτρων πολιτικής. Οι πυλώνες αυτοί θεμελιώνονται σε συγκεκριμένους στόχους : στην ισχυροποίηση του νομοθετικού πλαισίου για το ηλεκτρονικό έγκλημα, στην ενίσχυση της επιχειρησιακής ικανότητας των κρατών μελών, στην ανάπτυξη ικανοτήτων για την άμυνα στον κυβερνοχώρο σε σχέση με την Κοινή Πολιτική Ασφάλειας και Άμυνας, στην ενίσχυση της έρευνας και καινοτομίας, στην ανάπτυξη τεχνολογικών και βιομηχανικών πόρων για την κυβερνοασφάλεια.

Η σύγκλιση των πολιτικών θεμελιώνεται με την οδηγία NIS του 2016, αναφορικά με τα μέτρα για υψηλό κοινό επίπεδο ασφαλείας συστημάτων δικτύου και πληροφοριών. Τα κράτη μέλη καλούνται να προσδιορίσουν τους φορείς εκμετάλλευσης βασικών υπηρεσιών για κάθε τομέα και υποτομέα, να καταρτίσουν την εθνική τους στρατηγική, να δημιουργήσουν τις αρμόδιες εθνικές αρχές, το εθνικό κέντρο επαφής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών και την ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών CSIRT, ώστε να δημιουργηθεί ένα δίκτυο CSIRT. Καλούνται, επίσης, να υιοθετήσουν τις ελάχιστες απαιτήσεις για τη ασφάλεια δικτύων και πληροφοριών και να συμμετάσχουν στην ομάδα συνεργασίας σε ευρωπαϊκό επίπεδο με στόχο την ανταλλαγή πληροφοριών, εμπειριών, βέλτιστων πρακτικών και την κοινοποίηση συμβάντων. Σταδιακά, η ΕΕ επικεντρώνεται στη δημιουργία διαδικασιών πιστοποίησης και προτύπων για τα προϊόντα πληροφορικής.

Ο Κανονισμός του 2019, σχετικά με τον ENISA και την πιστοποίηση της κυβερνοασφάλειας, ενισχύει την αρμοδιότητά του για θέματα κυβερνοασφάλειας, παρέχοντας μόνιμη εντολή για τον οργανισμό αναφορικά με τη χάραξη και εφαρμογή της πολιτικής και της νομοθεσίας της ΕΕ αλλά και την επιχειρησιακή συνεργασία σε επίπεδο ΕΕ, την ίδια στιγμή που ορίζει το ευρωπαϊκό πλαίσιο πιστοποίησης για την κυβερνοασφάλεια ώστε να βελτιωθούν οι συνθήκες για την εσωτερική αγορά. Οι στόχοι ασφαλείας αφορούν: στην προστασία των δεδομένων, στην πρόσβαση από εγκεκριμένα άτομα, στον έλεγχο πρόσβασης, στην έγκαιρη αποκατάσταση της

διαθεσιμότητας, στην προστασία εξ ορισμού και από τον σχεδιασμό των προϊόντων και συστημάτων ΤΠΕ.

Ο ΓΚΠΔ το 2018, αναγνωρίζοντας τη σημασία της κυβερνοασφάλειας για την προστασία των προσωπικών δεδομένων, εισαγάγει τις αρχές της προστασίας των δεδομένων εκ του σχεδιασμού και εξ ορισμού, δίνοντας έμφαση στον συσχετισμό κυβερνοασφάλειας και προστασίας από την παραβίαση των δεδομένων. Βάσει του κανονισμού, η ασφάλεια των δεδομένων συνδέεται άμεσα με τις έννοιες της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των δεδομένων. Κατά συνέπεια η λήψη των κατάλληλων μέτρων (ψευδωνυμοποίηση, ανωνυμοποίηση, δοκιμές και αξιολογήσεις αποτελεσματικότητας των μέτρων, ορισμός σχεδίων ανάκαμψης και κώδικα δεοντολογίας), η υποχρεωτική γνωστοποίηση του συμβάντος στην ΑΠΔΠΧ αλλά και στα υποκείμενα των δικαιωμάτων, η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων, ο ορισμός υπευθύνου επεξεργασίας προστασίας δεδομένων δημιουργούν ένα ισχυρό πλαίσιο ευθύνης και αρμοδιοτήτων για τους οργανισμούς.

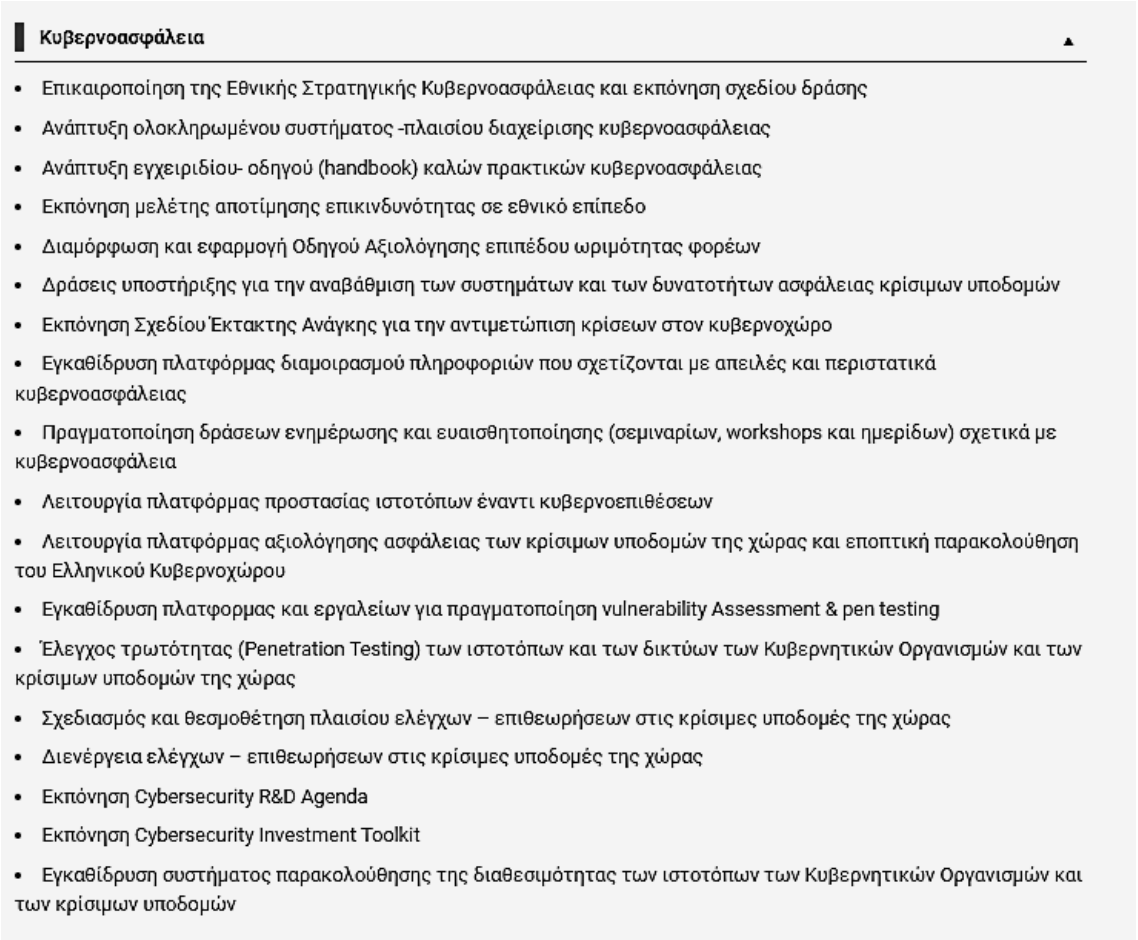
Το 2020, η στρατηγική κυβερνοασφάλειας για τη νέα δεκαετία έχοντας εμπεδώσει τα διδάγματα από την υλοποίηση και την εφαρμογή των πολιτικών κυβερνοασφάλειας την τελευταία δεκαετία, έρχεται να προσαρμοστεί στις νέες προκλήσεις των διασυνδεδεμένων συσκευών, του 5G και της τεχνητής νοημοσύνης υπό το πρίσμα του τοπίου που δημιούργησε η πανδημική κρίση. Η αναθεώρηση της οδηγίας του 2016 και η επανεξέταση της νομοθεσίας για τις κρίσιμες υποδομές προκειμένου να αυξηθεί το επίπεδο κυβερνοανθεκτικότητας των δημοσίων και ιδιωτικών υποδομών αλλά και η δημιουργία μιας κοινής μονάδας κυβερνοχώρου, αποτελούν τα κύρια σημεία της πρότασης της Επιτροπής.

2.2 Εθνικό πλαίσιο

Σύμφωνα με τη Βίβλο Ψηφιακού μετασχηματισμού[29], βασική προϋπόθεση για τον ψηφιακό μετασχηματισμό της ελληνικής κοινωνίας αποτελεί η διαφύλαξη ενός υψηλού επιπέδου ασφαλείας των ψηφιακών συστημάτων και υπηρεσιών. Η σημασία της ολιστικής προσέγγισης για την κυβερνοασφάλεια διατυπώνεται ξεκάθαρα, ενώ θεωρείται οριζόντιος άξονας παρέμβασης διαπερνώντας τα τομεακά έργα. Προβλέπεται

[29] Βίβλος ψηφιακού μετασχηματισμού: πρόκειται για την μακροπρόθεσμη αποτύπωση της εθνικής ψηφιακής στρατηγικής με ετήσια επικαιροποίηση βάσει του 4622/2019

ένα σύνολο 18 έργων ανάμεσα στα οποία και η πραγματοποίηση δράσεων ευαισθητοποίησης και εκπαίδευσης.



Κυβερνοασφάλεια

- Επικαιροποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας και εκπόνηση σχεδίου δράσης
- Ανάπτυξη ολοκληρωμένου συστήματος -πλαισίου διαχείρισης κυβερνοασφάλειας
- Ανάπτυξη εγχειριδίου- οδηγού (handbook) καλών πρακτικών κυβερνοασφάλειας
- Εκπόνηση μελέτης αποτίμησης επικινδυνότητας σε εθνικό επίπεδο
- Διαμόρφωση και εφαρμογή Οδηγού Αξιολόγησης επιπέδου ωριμότητας φορέων
- Δράσεις υποστήριξης για την αναβάθμιση των συστημάτων και των δυνατοτήτων ασφάλειας κρίσιμων υποδομών
- Εκπόνηση Σχεδίου Έκτακτης Ανάγκης για την αντιμετώπιση κρίσεων στον κυβερνοχώρο
- Εγκαθίδρυση πλατφόρμας διαμοιρασμού πληροφοριών που σχετίζονται με απειλές και περιστατικά κυβερνοασφάλειας
- Πραγματοποίηση δράσεων ενημέρωσης και ευαισθητοποίησης (σεμιναρίων, workshops και ημερίδων) σχετικά με κυβερνοασφάλεια
- Λειτουργία πλατφόρμας προστασίας ιστοτόπων έναντι κυβερνοεπιθέσεων
- Λειτουργία πλατφόρμας αξιολόγησης ασφάλειας των κρίσιμων υποδομών της χώρας και εποπτική παρακολούθηση του Ελληνικού Κυβερνοχώρου
- Εγκαθίδρυση πλατφορμας και εργαλείων για πραγματοποίηση vulnerability Assessment & pen testing
- Έλεγχος τρωτότητας (Penetration Testing) των ιστοτόπων και των δικτύων των Κυβερνητικών Οργανισμών και των κρίσιμων υποδομών της χώρας
- Σχεδιασμός και θεσμοθέτηση πλαισίου ελέγχων – επιθεωρήσεων στις κρίσιμες υποδομές της χώρας
- Διενέργεια ελέγχων – επιθεωρήσεων στις κρίσιμες υποδομές της χώρας
- Εκπόνηση Cybersecurity R&D Agenda
- Εκπόνηση Cybersecurity Investment Toolkit
- Εγκαθίδρυση συστήματος παρακολούθησης της διαθεσιμότητας των ιστοτόπων των Κυβερνητικών Οργανισμών και των κρίσιμων υποδομών

Εικόνα 5 Τα έργα για την κυβερνοασφάλεια στη Βίβλο Ψηφιακού Μετασχηματισμού
https://digitalstrategy.gov.gr/projects/catalog

Με το νόμο 4727/2020, ρυθμίζεται ολοκληρωμένα η ψηφιακή διακυβέρνηση και η χρήση ΤΠΕ από τον δημόσιο τομέα. Σύμφωνα με το τρίτο άρθρου του νόμου *«οι φορείς που σχεδιάζουν και εφαρμόζουν συστήματα ψηφιακής διακυβέρνησης οφείλουν να μεριμνούν για την ασφάλεια και την πρόσβαση σε αυτά».* Ταυτόχρονα, ορίζονται αρμόδιοι φορείς και κανόνες που θεμελιώνουν τις απαιτήσεις ασφαλείας στην παροχή ηλεκτρονικών υπηρεσιών : η εγκεκριμένη διάταξη ηλεκτρονικής υπογραφής, η εγκεκριμένη ηλεκτρονική σφραγίδα, η χρονοσήμανση, η αποκλειστική αρμοδιότητα της ΓΓΠΣΔΔ για την επαλήθευση της ταυτότητας των φυσικών προσώπων, τα μοναδικά στοιχεία ταυτοποίησης του ηλεκτρονικού εγγράφου, οι διαδικασίες ταυτοποίησης και αυθεντικοποίησης φυσικών, νομικών προσώπων και οντοτήτων για τη χρήση των υπηρεσιών της Ενιαίας Ψηφιακής Πύλης αλλά και το πλαίσιο των Υπηρεσιών Εμπιστοσύνης, με τις μεθόδους ταυτοποίησης και τις αρμοδιότητες της Αρχής

Πιστοποίησης του Ελληνικού Δημοσίου, στοχεύουν στην διασφάλιση των αρχών της ασφαλείας.

Παράλληλα, με την ενσωμάτωση της οδηγίας ΕΕ 2018/1972 για τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών, ρυθμίζεται εκ νέου και το πλαίσιο ασφαλείας δικτύων και υπηρεσιών με *«τη λήψη μέτρων για την αποτροπή και ελαχιστοποίηση των επιπτώσεων από συμβάντα ασφαλείας».* Ανάμεσα στα μέτρα προτείνεται η κρυπτογράφηση ενώ οι πάροχοι ηλεκτρονικών επικοινωνιών υποχρεούνται σε εκτίμηση αντικτύπου και σε κοινοποίηση στην ΑΔΑΕ σε περίπτωση συμβάντος.

Περαιτέρω, η χώρα με το ν. 4577/2018 Α΄199 έχει εναρμονιστεί με την οδηγία NIS. Ο εν λόγω νόμος αποτελεί το καίριο νομοθέτημα για την ασφάλεια των συστημάτων καθώς θεσπίζει *«τα μέτρα για την επίτευξη υψηλού επιπέδου ασφαλείας των συστημάτων δικτύου και πληροφοριών»* αλλά και τους αρμόδιους φορείς για την εφαρμογή των μέτρων αυτών, δημιουργώντας το ελληνικό οικοσύστημα ασφαλείας ευρισκόμενο σε συνεργασία με τους αρμόδιους υπερεθνικούς φορείς. Βασική στόχευση του νόμου αποτελεί η διασφάλιση ότι η Ελλάδα είναι προετοιμασμένη για την αντιμετώπιση πιθανών συμβάντων στον κυβερνοχώρο, έχοντας ορίσει τις αρμόδιες αρχές, έχοντας δημιουργήσει τις ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια και έχοντας δημιουργήσει την εθνική στρατηγική κυβερνοασφάλειας.

Παράλληλα, με το ν. 4624/2019 βρίσκεται εν ισχύει ο ΓΚΠΔ, ο οποίος προσδιορίζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των προσωπικών δεδομένων και υποχρεώνει τους εκτελούντες την επεξεργασία να λάβουν τα μέτρα αυτά. Ταυτόχρονα με το ν. 4411/2016 η Ελλάδα, κυρώνει τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο. Η χώρα έχει προβεί σε σειρά αλλαγών στο ποινικό δίκαιο [30] αναφορικά με την ασφάλεια των συστημάτων και το κυβερνοέγκλημα, οπότε και διώκονται ποινικά τα αδικήματα: της παρακώλυσης λειτουργίας των πληροφοριακών συστημάτων, οι προπαρασκευαστικές πράξεις για τη διάπραξη τέτοιων εγκλημάτων, η παράνομη πρόσβαση σε πληροφοριακό σύστημα, η παραβίαση του απορρήτου των επικοινωνιών με χρήση τεχνικών μέσων και η φθορά ηλεκτρονικών δεδομένων .

2.3 Το ελληνικό οικοσύστημα ασφαλείας.

Από την νομοθεσία αλλά και την Εθνική Στρατηγική, εκπονηθείσα το πρώτον το 2018 και επικαιροποιημένη πρόσφατα για τα έτη 2020-20225, προκύπτει ένα οργανωμένο

[30] Ποινικός Κώδικας άρθρα 292Β, 292Γ, 370Γ, 370Δ, 370Ε, 318Α, 318Β

και πολυεπίπεδο σύστημα εμπλεκομένων φορέων, το οποίο αντανακλά την αναγκαιότητα της συνεργασίας αποτελώντας σημείο αναφοράς για οποιοδήποτε πρόγραμμα ενίσχυσης της κουλτούρας ασφαλείας, καθώς οι εμπλεκόμενοι φορείς αποτελούν κρίσιμο παράγοντα επιτυχίας για τη δημιουργία και υλοποίηση προγραμμάτων ευαισθητοποίησης Το οικοσύστημα αυτό αποτελείται από:

- Την Γενική Διεύθυνση κυβερνοασφάλειας του ΥΨΔ, που αποτελεί την Εθνική Αρχή Κυβερνοασφάλειας, με επιτελικό ρόλο στην διαχείριση της εθνικής στρατηγικής και στον συντονισμό των φορέων.
- Την Εθνική Αρχή Αντιμετώπισης Επιθέσεων, Εθνικό CERT, στην Διεύθυνση Κυβερνοχώρου της ΕΥΠ με αρμοδιότητες για τεχνικής φύσεως θέματα ασφαλείας.
- Την Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ, αποτελούσα την Ελληνική CSIRT, αναφορικά με τα περιστατικά στον στρατιωτικό χώρο.
- Την Δίωξη Ηλεκτρονικού Εγκλήματος της ΕΛ.ΑΣ. με στόχο την πρόληψη, δίωξη και καταστολή του ηλεκτρονικού εγκλήματος. Αποτελεί το «σημείο επαφής 24/7» βάσει της Οδηγίας 2013/40/ΕΕ για τη συνεχή ανταπόκριση και συνδρομή σε περιστατικά ασφαλείας.
- Την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνταγματικά κατοχυρωμένη Αρχή, με αρμοδιότητες σχετικά με την προστασία του ατόμου από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την εποπτεία για την εφαρμογή του ΓΚΠΔ.
- Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, είναι ο Εθνικός ρυθμιστής της αγοράς ηλεκτρονικών επικοινωνιών και της ταχυδρομικής αγοράς.
- Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, συνταγματικά κατοχυρωμένη ανεξάρτητη αρχή, με στόχο την διασφάλιση του δικαιώματος στην ελεύθερη επικοινωνία.
- Το Κέντρο Μελετών Ασφαλείας, φορέας ερευνητικός, επιστημονικός και συμβουλευτικός. Νομικό πρόσωπο ιδιωτικού δικαίου εποπτευόμενο από το Υπουργείο Προστασίας του Πολίτη.

2.4 Πλαίσιο Ασφαλείας

Η ασφάλεια των πληροφοριακών συστημάτων αναφέρεται σε οντότητες και αντικείμενα που αξίζει να προστατευθούν, δηλαδή στα αγαθά των οργανισμών. Το

αγαθό περιλαμβάνει την πληροφορία και τους υπολογιστικούς και ανθρώπινους πόρους. Η αξία, οι κίνδυνοι, οι ζημίες αλλά και τα μέτρα προστασίας είναι διαφορετικά για κάθε αγαθό. Τα στοιχεία του πληροφοριακού συστήματος δρουν και αλληλεπιδρούν: οι άνθρωποι και το υλικό ενεργούν, το λογισμικό και οι διαδικασίες αποτελούν σύνολα εντολών και τα δεδομένα γεφυρώνουν την αλληλεπίδραση. Οι συνιστώσες αυτές χρησιμοποιούν την παραγόμενη από τα δεδομένα πληροφορία, δημιουργώντας αξία για τους οργανισμούς. Το πληροφοριακό σύστημα αναπτύσσεται με στόχο να βοηθηθούν οι χρήστες και οι οργανισμοί, ενώ έχει μεγάλη σημασία για τον διαμοιρασμό της γνώσης εντός και εκτός του οργανισμού. Ως εκ τούτου, η ασφάλειά του αποτελεί απαραίτητη προϋπόθεση για την ορθή λειτουργία του οργανισμού. Τα αγαθά έχουν ιδιοκτήτη και χρήστη. Είναι σημαντικό εδώ να τονιστεί ότι η έννοια «χρήστης» αναφέρεται όχι μόνο σε φυσικά πρόσωπα αλλά και σε διεργασίες. Ο σκοπός χρήσης των αγαθών καθορίζει την έννοια της ιδιότητας των αγαθών, ήτοι τα χαρακτηριστικά ασφαλείας που διασφαλίζουν την χρήση του αγαθού, είτε αυτή είναι η παροχή μιας υπηρεσίας ή η προσπέλαση μιας πληροφορίας ή ενός συστήματος. Τα χαρακτηριστικά αυτά αποτελούν τον πυρήνα της ασφάλειας[31] των πληροφοριακών συστημάτων και είναι τα εξής:

- Η εμπιστευτικότητα ,διασφαλίζει ότι η πληροφορία δεν θα γίνει διαθέσιμη σε μη εξουσιοδοτημένους χρήστες. Αναφέρεται τόσο στα δεδομένα όσο και στα φυσικά πρόσωπα καθώς σχετίζεται με την ιδιωτικότητα, διασφαλίζοντας ότι τα φυσικά πρόσωπα ελέγχουν την συλλογή και αποθήκευση της πληροφορίας που τα αφορά. Απώλεια της εμπιστευτικότητας σημαίνει μη εξουσιοδοτημένη αποκάλυψη πληροφορίας.
- Η ακεραιότητα, διασφαλίζει ότι τα δεδομένα τροποποιούνται μόνο από εξουσιοδοτημένους χρήστες, με τρόπο ορισμένο και συγκεκριμένο και ότι το σύστημα επιτελεί τις λειτουργίες του, βάσει του σχεδιασμού και των εξουσιοδοτήσεων. Συνδέεται και με τις έννοιες της αυθεντικότητας και της μη αποποίησης. Απώλεια της ακεραιότητας συνεπάγεται την μη εξουσιοδοτημένη τροποποίηση, αλλοίωση και καταστροφή της πληροφορίας.
- Η διαθεσιμότητα, διασφαλίζει ότι το σύστημα λειτουργεί ανεμπόδιστα και ότι η πληροφορία βρίσκεται στη διάθεση των εξουσιοδοτημένων χρηστών. Απώλεια της διαθεσιμότητας σημαίνει διαταραχή στην παροχή της υπηρεσίας.

[31] (William, 2017, pp. 18-21)

- Η εγκυρότητα, περιλαμβάνει την ακεραιότητα και την αυθεντικότητα και σχετίζεται με την ακρίβεια και πληρότητα της πληροφορίας.
- Η αυθεντικότητα, διασφαλίζει αφενός το ότι ο χρήστης είναι αυτός που δηλώνει και αφετέρου ότι ο χρήστης μπορεί να επιβεβαιωθεί και ότι είναι έμπιστος.
- Η μη αποποίηση ευθύνης, διασφαλίζει την ευθύνη και την λογοδοσία για την εκτέλεση της συναλλαγής.
- Η ανθεκτικότητα, είναι «η ικανότητα ενός πληροφοριακού συστήματος να συνεχίσει να λειτουργεί κάτω από αντίξοες συνθήκες, διατηρώντας τις βασικές λειτουργικές του δυνατότητες και με ικανότητα ανάκαμψης μέσα σε εύλογο χρονικό διάστημα»[32].

Όταν περιοριστούν οι ιδιότητες ενός αγαθού, κάνουμε λόγο για ζημία. Η ζημία προκαλείται από κάποιο κίνδυνο, που οφείλεται σε απειλή ή σε αδυναμία. Οι κίνδυνοι είναι η μη εξουσιοδοτημένη χρήση πληροφοριών και η παραβίαση, δηλαδή ο περιορισμός κάποιας από τις ιδιότητες ασφαλείας του αγαθού. Η απειλή συνήθως, προερχόμενη εξωγενώς εκμεταλλεύεται τις ενδογενείς αδυναμίες και προκαλεί ζημία στο αγαθό. Η παραβίαση δεν προκύπτει οπωσδήποτε όταν υπάρχει συνδυασμός αδυναμίες και απειλής, για αυτό και αναφερόμαστε στην έννοια της επισφάλειας, δηλαδή στην πιθανότητα να προκύψει ένα περιστατικό παραβίασης.

Στόχος της ασφάλειας των πληροφοριακών συστημάτων είναι η μείωση των συνεπειών των κινδύνων και η μείωση των πιθανοτήτων για πρόκληση ζημίας στα αγαθά. Για αυτό και οι οργανισμοί προχωρούν στην ανάλυση επικινδυνότητας αλλά και στη χρήση προτύπων για τον σχεδιασμό της πολιτικής ασφαλείας τους. Κεντρικό σημείο αποτελεί η διάσταση του κόστους. Το κόστος για τα μέτρα προστασίας είναι αντίστοιχο των επιπτώσεων μιας παραβίασης και του συνόλου της επικινδυνότητας. Η υιοθέτηση μέτρων προστασίας πρέπει να εξασφαλίζει ότι επιτυγχάνεται ο αντικειμενικός σκοπός, δηλαδή η απομένουσα επικινδυνότητα την οποία και αποδέχεται ο ιδιοκτήτης του πληροφοριακού αγαθού, καθώς απόλυτα ασφαλές πληροφοριακό σύστημα δεν υπάρχει. Η εξασφάλιση σημαίνει ότι τα μέτρα είναι κατάλληλα, είναι αποτελεσματικά και πληρούν συγκεκριμένες προδιαγραφές. Τα μέσα προστασίας είναι:

- η στρατηγική, που αποτελεί το σύνολο των γενικών σχεδίων ασφαλείας και ορίζει το βαθμό ικανοποίησης των απαιτήσεων και αποδοχής της επισφάλειας,

[32] (NIST, 2020)

- η πολιτική ασφαλείας του οργανισμού, που αποτελεί το σύνολο των κανόνων, μέτρων και διαδικασιών και περιλαμβάνει τις γενικές συστάσεις, την ενημέρωση, τις οδηγίες, τις πολιτικές για το προσωπικό αλλά και τον έλεγχο των μεταβολών,
- οι διαδικασίες ασφαλείας που συνιστούν τα μέτρα προστασίας του οργανισμού.

Τα προληπτικά μέτρα αποσκοπούν στον περιορισμό πρόσβασης σε εξουσιοδοτημένους χρήστες, πρόκειται στην ουσία για ελέγχους προσπέλασης στο σύστημα και στην πληροφορία μέσω ελέγχων ανάγνωσης και εγγραφής, αλλά και στην φυσική προστασία των συστημάτων. Σχετίζονται και με την ενίσχυση μηχανισμών λογοδοσίας και απόδοσης ευθυνών. Θεωρείται ότι τα μέτρα αυτά διαφυλάσσουν την απαίτηση της εμπιστευτικότητας. Τα μέτρα ανίχνευσης αποτελούν στην ουσία την επίβλεψη του συστήματος, ώστε να εντοπίζονται έγκαιρα τυχόν παραβιάσεις. Στοχεύουν στην μεγιστοποίηση της δυνατότητας ενός συστήματος να διατηρεί το επίπεδο της ασφαλείας του, παρά τις αστοχίες των συστατικών του. Διαφυλάσσουν την απαίτηση για διαθεσιμότητα και ακεραιότητα της πληροφορίας. Περαιτέρω, τα μέτρα που λαμβάνονται για τον περιορισμό των συνεπειών σχετίζονται με την μεταβίβαση της επικινδυνότητας, την ανάκαμψη, το σχέδιο συνέχειας και τη δημιουργία αντιγράφων ασφαλείας.

Η υλοποίηση των ανωτέρω μέτρων δημιουργεί ένα σύνθετο μηχανισμό ασφαλείας καθορισμένο από διεθνή πρότυπα[33]. Ο μηχανισμός αυτός υλοποιεί τις απαιτήσεις ασφαλείας, όπως φαίνεται στον παρακάτω πίνακα:

[33] Ενδεικτικά τα πρότυπα X800 (ITU, 2022)

Απαίτηση	Μηχανισμός						
	Κρυπτογράφηση	Πιστοποίηση	Διαβάθμιση διάκριση καθηκόντων	Έλεγχος πρόσβασης	Ψηφιακή Υπογραφή-χρονοσήμανση	Καταγραφή δραστηριοτήτων	Αντίγραφα και εφεδρικές γραμμές ασφαλείας
Εμπιστευτικότητα	Ναι		Ναι			Ναι	
Ακεραιότητα	Ναι		Ναι		Ναι		
Διαθεσιμότητα				Ναι			Ναι
Εγκυρότητα			Ναι				
Αυθεντικότητα	Ναι		Ναι	Ναι	Ναι		
Μη αποποίηση ευθύνης		Ναι	Ναι		Ναι		
Ανθεκτικότητα							Ναι

Εικόνα 6 Μηχανισμοί υλοποίησης των απαιτήσεων ασφαλείας

Ταυτόχρονα, βάσει των διεθνών προτύπων[34] και συστάσεων δημιουργείται ένα πλαίσιο αρχών που καθοδηγούν τη δημιουργία των μηχανισμών. Οι αρχές αυτές είναι[35]:

- Η οικονομικότητα: η ενσωμάτωση των χαρακτηριστικών ασφαλείας τόσο στο υλικό όσο και στο υλισμικό, πρέπει να είναι απλή και σχετικά μικρή καθώς όσο πιο σύνθετος είναι ο μηχανισμός τόσο πιο πιθανό είναι να προκύψουν ελαττώματα.
- Η ασφάλεια εξ ορισμού: η υλοποίηση του συστήματος θα πρέπει να ενσωματώνει από την σχεδίαση τις απαιτήσεις ασφαλείας, ενώ οι ρυθμίσεις προστασίας είναι εξ ορισμού ενεργοποιημένες.

[34] (NIST, 2021)
[35] (William, 2017, σσ. 33-35)

- Η αρχή της αναλογικότητας: οι πόροι και τα μέτρα ασφαλείας να είναι αντίστοιχα των κινδύνων και της αξίας των αγαθών. Η επίτευξη απόλυτης ασφάλειας δεν είναι εφικτός στόχος, οπότε στοχεύεται το ποσοστό ασφάλειας και η μείωση της επιφάνειας επίθεσης.
- Η αρχή του ελάχιστου προνομίου: ο χρήστης να έχει τα λιγότερα δικαιώματα πρόσβασης στην πληροφορία και το σύστημα, δικαιώματα αναγκαία για την εκπλήρωση των καθηκόντων του.

Περαιτέρω έμφαση δίνεται και στην αποδοχή από τον χρήστη, με την έννοια ότι οι μηχανισμοί και τα μέτρα ασφαλείας είναι κατανοητά από τον χρήστη και δεν παρεμβαίνουν ή διακόπτουν την εργασία του, αφού τότε είναι πιο πιθανό να τα απενεργοποιήσει.

2.5 Προσεγγίσεις και αρχιτεκτονικές ασφαλείας

Για την επίτευξη της ασφάλειας και την επαρκή αντιμετώπιση των κυβερνοαπειλών έχουν προταθεί αρκετές προσεγγίσεις για την καθοδήγηση των Υπευθύνων Ασφαλείας των Οργανισμών, κατά την οργάνωση και εφαρμογή πολιτικών αλλά και διαδικασιών ασφαλείας.

Το Πλαίσιο Κυβερνοασφάλειας του NIST, αποτελεί ένα πλαίσιο διαχείρισης κινδύνου για κάθε οργανισμό. Στον πυρήνα του Πλαισίου δημιουργείται ένα μοντέλο αναφοράς για την ασφάλεια. Προτείνονται πέντε ταυτόχρονες και αλληλοεξαρτώμενες λειτουργίες: η αναγνώριση, η προστασία, ο εντοπισμός, η απόκριση και η ανάκτηση. Με την αναγνώριση κατανοείται το περιβάλλον λειτουργίας του οργανισμού αποτιμώντας το σύνολο των πληροφοριακών αγαθών και διασυνδέσεων του οργανισμού. Η λειτουργία αυτή καθορίζει ρόλους, αρμοδιότητες και εκτιμά τους κινδύνους. Η προστασία στοχεύει στην ανάπτυξη και υλοποίηση των κατάλληλων μέτρων για την διασφάλιση της παροχής των υπηρεσιών. Στην λειτουργία αυτή αναπτύσσονται διαδικασίες ελέγχου πρόσβασης και διασφάλισης των δεδομένων, η εκπαίδευση και κατάρτιση των υπαλλήλων και η ανάπτυξη τεχνολογιών προστασίας των συστημάτων. Ο εντοπισμός σχετίζεται με τον έγκαιρο εντοπισμό των συμβάντων μέσω διαδικασιών συνεχούς παρακολούθησης των υποδομών αλλά και των δικτυακών ροών. Η απόκριση είναι η λειτουργία ανάπτυξης και εφαρμογής των κατάλληλων δράσεων για την αντιμετώπιση των συμβάντων και η ανάκτηση σχετίζεται με το σχέδιο έγκαιρης αποκατάστασης των δομών και των υπηρεσιών.

Μια ακόμα προσέγγιση είναι η καθοδήγηση των υπευθύνων ασφαλείας για την κατανόηση του τρόπου δράσης των εισβολέων. Το μοντέλο αυτό «της γνώσης καθοδηγούμενης από την άμυνα του οργανισμού», βασίζεται στη συλλογή πληροφοριών από τη δράση των επιτιθέμενων, δημιουργώντας δείκτες επίθεσης με σκοπό να αναγνωριστούν και να εντοπιστούν οι στόχοι, οι ικανότητες και οι περιορισμοί των αντιπάλων. Η τοποθέτηση μηχανισμών πρόληψης και αντιμετώπισης των εισβολών και η άντληση και ανάλυση στοιχείων από αυτούς οδηγούν στην γνώση για τον αντίπαλο. Για παράδειγμα, η παρακολούθηση της διεύθυνσης IP ή τα αναγνωριστικά ευπάθειας αποτελούν σημαντικούς δείκτες. Ένα άλλο σημαντικό σημείο σε αυτή την προσέγγιση είναι η κατανόηση της «αλυσίδας ενεργειών» των εισβολέων, ώστε να παγιδευτεί ο μη εξουσιοδοτημένος χρήστης. Ο επιτιθέμενος πρώτα αναγνωρίζει τον στόχο, στη συνέχεια εξοπλίζεται με το κατάλληλο λογισμικό το οποίο ενσωματώνει σε κάποιο άλλο πρόγραμμα, παραδίδει το κακόβουλο αρχείο, τις περισσότερες φορές μέσω μηνύματος ηλεκτρονικού ταχυδρομείου, ιστοσελίδας ή αφαιρούμενης συσκευής αποθήκευσης , εκμεταλλεύεται τις ευπάθειες προκειμένου να εγκαταστήσει το κακόβουλο πρόγραμμα και τελικά μέσω εντολής και ελέγχου (command και control) δημιουργεί το κανάλι επικοινωνίας προκειμένου να επιτευχθούν οι στόχοι, για παράδειγμα, η υποκλοπή ευαίσθητων πληροφοριών ή η χρήση της δικτυακής συσκευής ως κομβικού σημείου. Σε κάθε στάδιο αντιστοιχούν αμυντικοί μηχανισμοί και σειρά ενεργειών δράσης.

Πιο συγκεκριμένα, ο εντοπισμός ενός κακόβουλου λογισμικού δύναται να γίνει με την εγκατάσταση ενός «αντιϊκού» προγράμματος, που ελέγχει τις μετακινήσεις αρχείων αλλά και τα εκτελέσιμα αρχεία προκειμένου να βρει τις ακολουθίες που αντιστοιχούν σε ιούς. Ο εντοπισμός των επιθέσεων απαιτεί ένα «σύστημα ανίχνευσης επιθέσεων», δηλαδή ένα σύστημα ασφαλείας που ελέγχει και παρακολουθεί το σύστημα, συλλέγει πληροφορίες για το δίκτυο, ελέγχει τις ευπάθειες, αναλύει τις πληροφορίες ενώ παρακολουθεί και αναλύει την δραστηριότητα του χρήστη. Τα συστήματα αυτά διατηρούν αρχεία καταγραφής με τις εισβολές και ενημερώνουν τον διαχειριστή για την κατάσταση του δικτύου. Τα IDS μπορεί να βασίζονται στον κεντρικό υπολογιστή ή στο δίκτυο και να παρακολουθούν τις κινήσεις που εξελίσσονται στον κυβερνοχώρο. Τα συστήματα ανίχνευσης απειλών θεωρούνται ιδιαίτερα χρήσιμα σχεδόν σε όλα τα στάδια της αλυσίδας CKC. Η προστασία του τοπικού δικτύου από κακόβουλη ενέργεια δύναται να πραγματοποιηθεί και με ένα «τείχος προστασίας», λογισμικό πρόγραμμα ή συσκευή που λειτουργεί ως φίλτρο στο επίπεδο των πρωτοκόλλων επικοινωνίας, μέσω

της εγκατάστασής του στα τελικά σημεία ανάμεσα στο εξωτερικό και εσωτερικό δίκτυο, ρυθμίζοντας την κυκλοφορία των δεδομένων. Το τείχος προστασίας αποτελεί αμυντικό μηχανισμό τόσο της εκμετάλλευσης των ευπαθειών όσο και του σταδίου της εντολής και ελέγχου. Άλλη τακτική είναι η χρήση «των συστημάτων και δικτύων παγίδευσης», αποτελούν λειτουργικά συστήματα που περιλαμβάνουν εφαρμογές προσομοίωσης αλλά και πραγματικά δίκτυα με επιμέρους συστήματα και εφαρμογές. Χρησιμοποιούνται για την παραπλάνηση του εισβολέα και δύνανται να ανακαλύψουν νέες μορφές επίθεσης. Χρησιμοποιούνται για την απώθηση του τελευταίου σταδίου της αλυσίδας CKC, αυτό της επίτευξης των στόχων.

Μια ακόμα προσέγγιση ασφαλείας είναι αυτή της «Άμυνας σε βάθος»[36], που αποτελεί και μια ολιστική προσέγγιση χρησιμοποιώντας διάφορα εμπόδια για να ανατρέψει την διείσδυση των μη εξουσιοδοτημένων χρηστών. Συνδυάζει τη συνεργασία ανθρώπινων και υπολογιστικών πόρων. Πρόκειται για δημιουργία πολλαπλών και ετερογενών μεθόδων ασφαλείας και κατά συνέπεια το μοντέλο χρησιμοποιείται σε σχέση με την αξία και τη σημασία των αγαθών του Οργανισμού. Βασικά στοιχεία της στρατηγικής άμυνας σε βάθος είναι[37]:

1. Η διαχείριση του κινδύνου μέσω του προσδιορισμού και του χαρακτηρισμού τους.
2. Η αρχιτεκτονική κυβερνοασφάλειας βάσει προτύπων, συστάσεων και διαδικασιών.
3. Η διαχείριση των συνεργατών και προμηθευτών, για παράδειγμα αναφορικά με τις υπηρεσίες νέφους.
4. Οι πολιτικές, οι διαδικασίες και η κατάρτιση και ευαισθητοποίηση των ανθρώπινων πόρων.

Στο επίπεδο των υπολογιστικών συστημάτων άμυνα σε βάθος σημαίνει:

- Φυσική προστασία και ασφάλεια.
- Αυθεντικοποίηση και χρήση διαπιστευτηρίων.
- Η ασφάλεια στην είσοδο μέσω ενημερωμένων εκδόσεων.
- Περιμετρική ασφάλεια, μέσω «τειχών προστασίας» και ελέγχου απομακρυσμένης πρόσβασης μέσω «εικονικών ιδιωτικών δικτύων».
- Χρήση «αντιϊκών».
- Παρακολούθηση ασφαλείας με συστήματα IDS.

[36] (NIST, 2020) και
[37] (Ιωάννης, 2015)

- Βιομετρικά στοιχεία.
- Χρονοκαθυστερήσεις στην είσοδο.
- Λογισμικά με άδειες.
- Έλεγχος των «αρχείων καταγραφής».
- Αρχιτεκτονική του δικτύου μέσω εικονικών δικτύων.

Ιδιαίτερη μνεία πρέπει να γίνει στα συστήματα διαμοιρασμού πληροφοριών «CTI», τα οποία επικεντρώνονται στις δυνατότητες, τα κίνητρα και τους στόχους των επιτιθέμενων, μέσω πληροφορίας και γνώσης που συλλέγεται από τις επιθέσεις. Τα συστήματα αυτά λειτουργούν στον πυρήνα της ανίχνευσης και αποτροπής των εισβολών, ενώ τα ευρήματα μιας κυβερνοεπίθεσης χρησιμοποιούνται από άλλους οργανισμούς. Πρόκειται για μια σύγχρονη και αρκετά εξελιγμένη μέθοδο, η οποία εν τούτοις πρέπει να εξετάζεται βάσει της συμμόρφωσης με το κανονιστικό πλαίσιο αναφορικά με τα προσωπικά δεδομένα.

Ολοκληρώνοντας τις προσεγγίσεις ασφαλείας είναι σημαντικό να επισημανθεί ότι οι σύγχρονοι οργανισμοί υιοθετούν συνδυαστικά μια ή και περισσότερες προσεγγίσεις. Ο τεχνικός σχεδιασμός γίνεται βάσει της πολλαπλής προσέγγισης ασφάλειας, αφορώντας όλους τους πόρους του συστήματος (ανθρώπους, τεχνολογία, λειτουργικό). Η διαστρωμάτωση αυτή στην ασφάλεια, επιτρέπει την αντιμετώπιση μιας επίθεσης παρέχοντας πολλαπλά και κλιμακούμενα εμπόδια.

Η πιο σύγχρονη στρατηγική πάντως, θεωρείται αυτή της «μηδενικής εμπιστοσύνης». Βάσει πρόσφατης έρευνας [38], η αρχιτεκτονική αυτή πρόκειται να αυξήσει την αποτελεσματικότητα της κυβερνοασφάλειας κατά 144%. Πρόκειται για μια αρχιτεκτονική που επικεντρώνεται στο ότι η εμπιστοσύνη αποτελεί ευπάθεια. Κατά συνέπεια, τα μοντέλα ασφαλείας δεν πρέπει να στηρίζονται στο γεγονός ότι οι οντότητες εντός του οργανισμού είναι άξιες εμπιστοσύνης. Η αρχιτεκτονική μηδενικής εμπιστοσύνης βασίζεται στη λογική "never trust, always verify"[39] και μετατοπίζει το βάρος από την προστασία του εξοπλισμού στην επαλήθευση των αιτημάτων ως προς την αυθεντικότητα και την εξουσιοδότηση. Με την αρχιτεκτονική συνάδει η αρχή του ελάχιστου προνομίου, ενώ ενδείκνυται για τα σύγχρονα περιβάλλοντα απομακρυσμένης σύνδεσης και υπολογιστικής νέφους. Η συνεχής επαλήθευση αποτελεί τη απάντηση στις διασυνδεδεμένες συσκευές, που αυξάνουν την επιφάνεια επίθεσης. Το μοντέλο αφορά στον έλεγχο του δικτύου, των υποδομών, των δεδομένων μέσω της γνώσης , της

[38] (Symmetry Systems και η Osterman Research, 2021)
[39] «Ποτέ μην εμπιστεύεσαι, πάντα να επαληθεύεις»

ταξινόμησης και της «κλιμακωσιμότητας», ενώ δεσπόζουσα αντίληψη είναι η «κατ' εξαίρεση» εμπιστοσύνη. Χρησιμοποιείται στην ουσία η ταυτότητα και η αρμοδιότητα των εμπλεκομένων προκειμένου να αποκτήσουν κάποιο επίπεδο πρόσβασης. Ο έλεγχος αποτελεί μια δυναμική διαδικασία. Ενδεικτικά μέσα του μοντέλου είναι: η «αυθεντικοποίηση πολλών παραγόντων», η χρήση «αλγόριθμων κρυπτογράφησης» και η σε πραγματικό χρόνο παρακολούθηση και δυναμική άντληση δεδομένων, ενώ απαιτείται συνεχής ενημερότητα των χρηστών και ανανέωση της γνώσης τους.

3 Δημιουργώντας κουλτούρα κυβερνοασφάλειας στους οργανισμούς

Στο παρόν κεφάλαιο εξετάζονται τα στοιχεία που συνθέτουν την έννοια της κουλτούρας κυβερνοασφάλειας και αποτελούν τη βάση για τη δημιουργία προγραμμάτων ενίσχυσης της κουλτούρας ασφαλείας στους δημόσιους οργανισμούς. Η μέθοδος που χρησιμοποιήθηκε ήταν αυτή της βιβλιογραφικής έρευνας και της σύγκρισης στοιχείων από ευρωπαϊκές και εθνικές πηγές.

3.1 Οργανωσιακή κουλτούρα και δημόσια διοίκηση

Η οργανωσιακή κουλτούρα[40] συνδέεται με τις αξίες, τις πεποιθήσεις, τα πρότυπα ερμηνείας και δράσης και το όραμα ενός οργανισμού, αποτελεί μέρος της οργανωτικής νοοτροπίας και δημιουργεί τις συνθήκες για την χρήση μιας κοινής γλώσσας και συμπεριφοράς από τους εργαζομένους. Πρόκειται για μια αφηρημένη και όχι εύκολα προσδιορίσιμη έννοια καθώς εμπεριέχει στοιχεία υλικά αλλά και άυλα. Αποτελεί κεντρικό σημείο στη λειτουργία ενός οργανισμού. Ποικίλοι κοινωνικοοικονομικοί, πολιτικοί, πολιτισμικοί, και εθνικοί παράγοντες συνδιαμορφώνουν την έννοια της κουλτούρας, ενώ σημαντικό ρόλο φαίνεται να παίζει και η ανθρώπινη φύση. Οι οργανισμοί λειτουργώντας εντός του ευρύτερου κοινωνικοοικονομικού και πολιτικού περιβάλλοντος, επηρεάζονται σαφώς από τις αλλαγές στο περιβάλλον αυτό. Η συχνότητα και η ταχύτητα των αλλαγών επηρεάζει αντίστοιχα τις αξίες και τις συμπεριφορές. Ανάλογα με την σχέση με το περιβάλλον, ο οργανισμός δύναται να υιοθετεί μια κουλτούρα προσαρμοστικότητας με βασικά χαρακτηριστικά την ευελιξία και την γρήγορη προσαρμογή στις αλλαγές, μια κουλτούρα προσανατολισμένη στα αποτελέσματα, με ιδιαίτερα στοιχεία τον επαγγελματισμό και την ανταγωνιστικότητα, μια κουλτούρα συμπερίληψης, με χαρακτηριστικά την συμμετοχή και την εμπλοκή των υπαλλήλων και μια κουλτούρα συνοχής με βασικά στοιχεία τον ορθολογικό και

[40] (Βαγδατζόγλου, 2018)

ιεραρχικό τρόπο οργάνωσης. Η επιλογή στάσης απέναντι στο περιβάλλον εξαρτάται από την ηγεσία του οργανισμού και επαφίεται στην διοίκηση να διαμορφώσει την κατάλληλη για τους στόχους του οργανισμού κουλτούρα, εισάγοντας νέα αξιακά δεδομένα.

Σήμερα, οι ραγδαίες τεχνολογικές εξελίξεις φαίνεται ότι διαμορφώνουν νέες οπτικές για την πραγματικότητα, επηρεάζοντας αναπόφευκτα την συνολική κουλτούρα της κοινωνίας. Μπροστά σε αυτές τις εξελίξεις η συζήτηση για την οργανωσιακή κουλτούρα εισαγάγει τη θεματική της καινοτομίας, με ζητούμενα την αποτελεσματική ανταπόκριση των δημοσίων οργανισμών στις απαιτήσεις της κοινωνίας της πληροφορίας και την παροχή ψηφιακών υπηρεσιών. Σημαντικά ζητήματα που εγείρονται είναι η δημιουργία του περιβάλλοντος για τη δημιουργία πολιτοκεντρικών συστημάτων παροχής υπηρεσιών αλλά και η συνεργασία των ενδιαφερομένων μερών.

Είναι σαφές ότι μιλώντας για τον δημόσιο τομέα , η οργανωσιακή κουλτούρα συνδέεται με συγκεκριμένες και προκαθορισμένες αρχές και αξίες που ενσωματώνονται στην συνολική διοικητική κουλτούρα και λειτουργούν ως βάση για την ανάπτυξη της οργανωσιακής κουλτούρας, έκαστου οργανισμού. Οι αρχές [41] αυτές διέπουν και νομιμοποιούν τη δράση της διοίκησης, ενώ ερείδονται στο Σύνταγμα αποτελώντας τη βάση του διοικητικού δικαίου. Η ίδια η έννοια της δημόσιας διοίκησης, εξάλλου, συνδέεται με την διαχείριση των δημοσίων υποθέσεων και ως εκ τούτου είναι προσανατολισμένη στην εξυπηρέτηση του δημοσίου συμφέροντος. Παράλληλα, τη λειτουργία της διέπει η αρχή της νομιμότητας, η οποία και εγγυάται την υποχρέωση των οργάνων της διοίκησης να δρουν εντός του ορισμένου νομοθετικού και κανονιστικού πλαισίου του ευνομούμενου και δημοκρατικού κράτους δικαίου. Η σημασία των αρχών είναι καθοριστική για την ερμηνεία των κανόνων του διοικητικού δικαίου ενώ αποτελούν και τη βάση για τον σχεδιασμό και την υλοποίηση οποιασδήποτε δημόσιας πολιτικής.

Τούτων λεχθέντων, γίνεται αντιληπτό ότι οι δημόσιοι οργανισμοί στοχεύουν στην προώθηση της γενικής κοινωνικής ευημερίας, κάτι που επηρεάζει την δομή και λειτουργία τους. Η εμβέλεια της δράσης τους, καθορίζει και την ιδιαιτερότητα της φύσης τους, με αποτέλεσμα η οργανωσιακή κουλτούρα των δημοσίων οργανισμών να διαφέρει από αυτή των ιδιωτικών. Αδρομερώς, βασικά χαρακτηριστικά της είναι η εσωτερική τυπικότητα, η ιεραρχία, οι κανόνες και οι διαδικασίες ελέγχου ενώ δίνεται

[41] Αρχή της νομιμότητας, της αναλογικότητας, της υπεροχής του δημοσίου συμφέροντος, της ισότητας, της αξιοκρατίας, της διαφάνειας, της αποτελεσματικότητας και της χρηστής διοίκησης.

ιδιαίτερη έμφαση στο εσωτερικό περιβάλλον του οργανισμού και στη συμμετοχή των υπαλλήλων[42]. Σε αυτή τη βάση δύναται να οικοδομηθεί η προσαρμογή στις προκλήσεις της ψηφιακής εποχής καθώς η εμπλοκή των εργαζομένων, η συμπερίληψη και η κατανόησή τους θα καθορίσει και το τελικό αποτέλεσμα της οργανωσιακής αλλαγής.

3.2 Κουλτούρα κυβερνοασφάλειας

Η κουλτούρα κυβερνοασφάλειας συνδέεται με την δημιουργία ανθεκτικότητας στις επιθέσεις. Η σημασία που της αποδίδεται είναι μεγάλη καθώς απαντάται τόσο ως στόχος της ευρωπαϊκής όσο και ως στόχος των εθνικών στρατηγικών για την κυβερνοσφάλεια, ενώ αποτελεί μια από τις βασικές συνιστώσες των προσεγγίσεων ασφαλείας. Παρά την αναγνωρισμένη σημασία της, φαίνεται ότι πολλάκις οι οργανισμοί επενδύουν περισσότερο στην τεχνική διασφάλιση του συστήματος, παρά στην δημιουργία της κουλτούρας ασφαλείας. Ταυτόχρονα, ενώ οι πολιτικές που σχετίζονται με τον τελικό χρήστη αποτελούν κοινό τόπο στους οργανισμούς, οι χρήστες συνεχίζουν να τις αντιλαμβάνονται περισσότερο ως κατευθυντήριες παρά ως κανόνες. Οι περιορισμένοι πόροι, η δυσκολία για τους μη ειδικούς να κατανοήσουν την πολυπλοκότητα της κυβερνοασφάλειας, η έλλειψη στοιχείων για τον βέλτιστο τρόπο αύξησης της ενημέρωσης, η διασφάλιση της ενεργού συμμετοχής όλων των εμπλεκομένων μερών, η έλλειψη στόχευσης δημιουργούν ένα σχετικά περίπλοκο τοπίο για την επιτυχία των προγραμμάτων που σχετίζονται με την δημιουργία επίγνωσης ασφαλείας εντός των οργανισμών

Η κουλτούρα κυβερνοασφάλειας θεωρεί οτιδήποτε και οποιονδήποτε που συνδέεται με τον κυβερνοχώρο ως αγαθό που πρέπει να προστατευτεί ενώ προσδιορίζεται και από στοιχεία και παράγοντες πέρα του οργανισμού, έχει κρατική και υπερκρατική οπτική. Σύμφωνα με τον ENISA[43] «η κουλτούρα κυβερνοασφάλειας αναφέρεται στις γνώσεις, τα πιστεύω, τις αντιλήψεις, τις στάσεις, τις αξίες και τις συμπεριφορές των ανθρώπων αναφορικά με την κυβερνοασφάλεια και πώς αυτά εκφράζονται στην συμπεριφορά των ανθρώπων στο διαδίκτυο και γενικότερα απέναντι στις τεχνολογίες πληροφορικής».

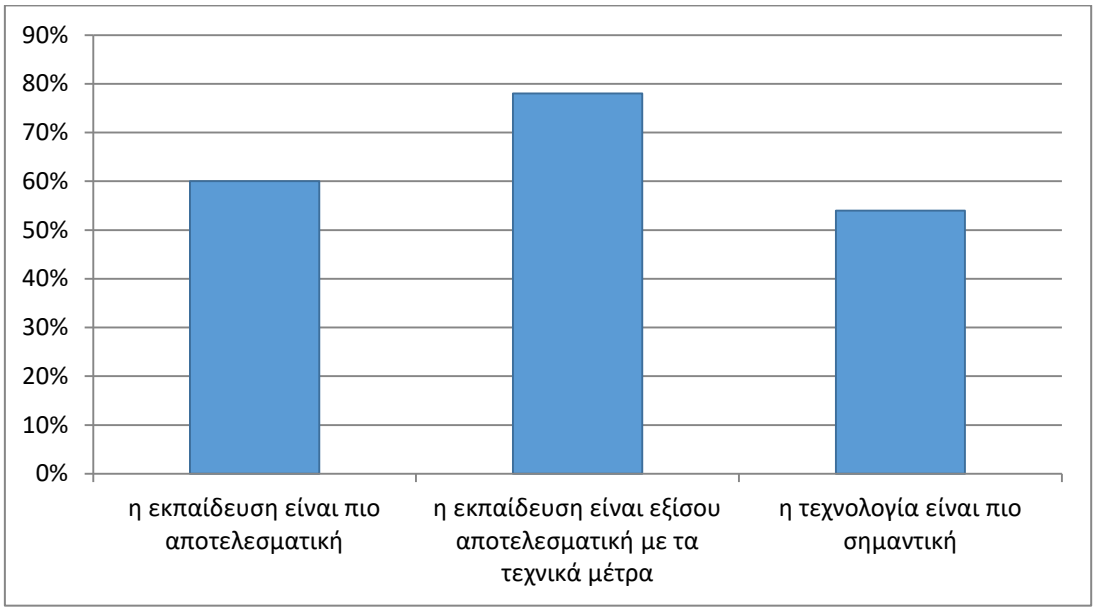
Η καλλιέργεια της κουλτούρας αυτής στοχεύει στο να γίνει το πλαίσιο ασφαλείας αναπόσπαστο στοιχείο της καθημερινής συμπεριφοράς του υπαλλήλου. Θεμελιώνεται στις τυποποιημένες πρακτικές και τους κανόνες ασφαλείας, προχωρά στη δημιουργία των αξιών που αντανακλώνται στη στρατηγική, εμβαθύνει περαιτέρω στη δημιουργία

[42] (Μπουραντάς Δημήτρης, 2016)
[43] (ENISA, 2017)

αντιλήψεων και απόψεων για την ασφάλεια για να οδηγηθεί στο τελικό σημείο, την πραγματική και εμπεδωμένη γνώση για την ασφάλεια.

3.3 Ο ρόλος του ανθρώπινου παράγοντα

Όπως διαπιστώθηκε και από τη μελέτη του τοπίου των απειλών, ο ανθρώπινος παράγοντας σχετίζεται με το μεγαλύτερο ποσοστό παραβιάσεων. Ένας, εξάλλου, από τους κρίσιμους παράγοντες επιτυχίας των πολιτικών ασφαλείας αποτελεί η αποδοχή τους από τους υπαλλήλους του οργανισμού αλλά και από τους συνεργάτες του. Βάσει ερευνών[44] προκύπτει ότι τέσσερις στους πέντε Υπευθύνους Ασφαλείας των οργανισμών θεωρούν ότι η εκπαίδευση είναι τόσο σημαντική όσο και τα τεχνολογικά αντίμετρα, ενώ το 96% των ανώτατων στελεχών κατανοούν ότι η εκπαίδευση ευαισθητοποίησης στα θέματα ασφαλείας διαδραματίζει καίριο ρόλο. Στον πίνακα αστικοποιούνται τα δεδομένα από την παραπάνω έρευνα:



Εικόνα 7 Εκπαίδευση και τεχνολογία, ίδια επεξεργασία με excel

Παράλληλα σε πανελλήνια έρευνα του 2021, που διενεργήθηκε από πάροχο ψηφιακών τεχνολογιών και λύσεων ασφαλείας[45] ανάμεσα σε υψηλόβαθμα στελέχη πληροφορικής εταιρειών, το 70,4% των ερωτηθέντων απάντησε πως η μεγαλύτερη πρόκληση ασφαλείας είναι η εκπαίδευση των χρηστών. Προς αυτή την κατεύθυνση, αρκετές μελέτες[46] προσπαθούν να διερευνήσουν το ρόλο του ανθρώπινου παράγοντα στην ασφάλεια των οργανισμών, καθώς πολλάκις η χρήση τεχνικών μέτρων προστασίας δεν

[44] (Osterman Research, 2020)
[45] (INFOCOM, 2021)
[46] (Hadlington, 2017)

κατέστη δυνατό να προστατέψει τον οργανισμό από τυχόν κυβερνοεπιθέσεις. Καταρχάς, είναι σημαντικό να τονιστεί ότι συχνά η κακόβουλη ενέργεια σχετίζεται με την αποκόμιση ίδιου οφέλους ή συνδέεται με χαρακτηριστικά της προσωπικότητας του υπαλλήλου. Μπορεί να οφείλεται σε λάθος, σε έλλειψη δεξιότητας, σε γνωσιακή προκατάληψη, σε παρορμητικότητα, στον εθισμό ή και στην εκδίκηση. Ο προσδιορισμός του κινήτρου αναδεικνύεται ιδιαίτερα σημαντικός στην προσπάθεια σχεδιασμού ενός προγράμματος επίγνωσης ασφαλείας, ενώ ενέχει και τη δυσκολία ποσοτικοποίησης των ανθρωποκεντρικών απειλών.

Φαίνεται πως όχι μόνο οργανωσιακοί αλλά και συμπεριφορικοί παράγοντες επηρεάζουν την στάση και τη συμμόρφωση των εργαζομένων απέναντι στις πρακτικές ασφαλείας. Πολλοί μελετητές προσπάθησαν να συσχετίσουν βασικά χαρακτηριστικά της ανθρώπινης προσωπικότητας, εξωστρέφεια, αυθορμητισμό, αλλά και ευσυνειδησία, με τις επιθέσεις κοινωνικής μηχανικής. Ταυτόχρονα, απόπειρες συσχετισμού του βαθμού εθισμού στο διαδίκτυο με την πιθανότητα παράκαμψης των μέτρων ασφαλείας καταδεικνύουν ότι υπάρχει αρκετά ισχυρή συσχέτιση ανάμεσα σε αυτές τις παραμέτρους[47].Το ίδιο φαίνεται να ισχύει και για την παρορμητικότητα ως παράγοντα επικινδυνότητας. Ένα ιδιαίτερα ενδιαφέρον σημείο σε σχέση με την συμπεριφορά του εργαζόμενου είναι «η λογική του αντισταθμίσματος». Καθώς λειτουργεί εντός προστατευμένου περιβάλλοντος, υπό την έννοια ότι στον οργανισμό ισχύουν μέτρα ασφαλείας, είναι πιο πιθανό να προβεί σε πιο επικίνδυνες για την ασφάλεια συμπεριφορές.

Η προσπάθεια για την οργάνωση του πλαισίου της κουλτούρας για την ασφάλεια είναι αναγκαίο να λάβει υπόψη και τις ψυχοκοινωνικές αναλύσεις καθώς αναλύοντας τα κίνητρα αντιλαμβανόμαστε ότι βρισκόμαστε αντιμέτωποι με ένα ευρύ φάσμα συμπεριφορών και εύλογα με την ανάγκη διαφορετικής αντιμετώπισης. Η εκπαίδευση για την ασφάλεια χρειάζεται να προσπεράσει την απλή παροχή πληροφορίας στον χρήστη, συνίσταται να είναι στοχευμένη, σχετική με τα καθήκοντα και τις αρμοδιότητες του χρήστη, αλληλεπιδραστική και να οδηγεί στην ανατροφοδότηση. Μέσα, εξάλλου, από τέτοιες πρακτικές εκπαίδευσης είναι ευκολότερο να εντοπιστούν τα κενά αλλά και οι συμπεριφορές με υψηλότερη επικινδυνότητα και να εκπαιδευτούν περαιτέρω οι χρήστες.

[47] Έρευνα στο Ηνωμένο Βασίλειο το 2017 ανάμεσα σε 538 εργαζόμενους, (Hadlington, 2017)

3.4 Η κουλτούρα ασφαλείας στην Ευρωπαϊκή Ένωση

Στον στρατηγικό στόχο της ανθεκτικότητας ως βασικό σημείο δράσης αναδεικνύεται η ευαισθητοποίηση του τελικού χρήστη, κάτι που απαντάται σε σειρά ευρωπαϊκών κειμένων. Ταυτόχρονα, ο ENISA με τον κανονισμό του 2019 καλείται να παίξει σημαντικό ρόλο στην ευαισθητοποίηση. Η πρόταση για την νέα στρατηγική, εστιάζει στα ζητήματα εκπαίδευσης, κατάρτισης και συνειδητότητας για την ασφάλεια. Έμφαση δίνεται και στην ανάπτυξη δεξιοτήτων. Η ΕΕ αντιλαμβανόμενη την αυξανόμενη έλλειψη δεξιοτήτων στον τομέα της κυβερνοασφάλειας, την μη ισορροπημένη κατανομή των δυο φύλων στον τομέα αυτό και την μη επαρκή ακαδημαϊκή εκπαίδευση αναφορικά με τον κυβερνοχώρο, κατευθύνει τα κράτη μέλη σε αναθεώρηση των προγραμμάτων για την ψηφιακή εκπαίδευση αλλά και την ενίσχυση των προγραμμάτων ειδίκευσης και κατάρτισης των επαγγελματιών ΤΠΕ καθώς και των δημοσίων υπαλλήλων και των δικαστικών λειτουργών. Προκρίνεται η δημιουργία ενός μείγματος δεξιοτήτων αλλά και η δημιουργία πανευρωπαϊκών προτύπων για την επιμόρφωση και την πιστοποίηση, λόγω του διασυνοριακού χαρακτήρα του κυβερνοεγκλήματος. Ένας από τους βασικούς άξονες της «Διακήρυξης του Βερολίνου για την Ψηφιακή Κοινωνία και την προστιθέμενη Αξία της Ψηφιακή Διακυβέρνησης» αποτελεί η ενδυνάμωση της ψηφιακού εγγραμματισμού για όλους τους πολίτες και ειδικότερα για τους δημοσίους υπαλλήλους, ενώ η πρώτη και πρόσφατη έκθεση[48] σε σχέση με την εφαρμογή των στόχων της διακήρυξης καταδεικνύει ότι ο συνολικός μέσος όρος των κρατών-μελών βρίσκεται στο 69%, κάτι που σημαίνει ότι υπάρχουν περιθώρια βελτίωσης των πολιτικών ευαισθητοποίησης των κρατών-μελών.

Σε γενικές γραμμές, η ΕΕ έχει θεσπίσει μια σειρά σημαντικών πρωτοβουλιών κατάρτισης για τον κυβερνοχώρο. Εμβληματικές πρωτοβουλίες αποτελούν: τα προγράμματα κατάρτισης της Ευρωπόλ και του CEPOL , τα προγράμματα κατάρτισης του ENISA, το Δίκτυο Ευρωπαϊκής Ακαδημίας Ασφάλειας και Άμυνας, το οποίο παρέχει πολιτικο-στρατιωτική κατάρτιση αλλά και το Ευρωπαϊκό Δίκτυο Κατάρτισης Δικαστικών. Παράλληλα, η οργάνωση ασκήσεων αποτελεί μια βασική συνιστώσα της εκπαίδευσης και κατάρτισης σχετικά με τον κυβερνοχώρο. Η πραγματοποίηση της επιχειρησιακής άσκησης *Cyber Europe* ανά διετία, της τεχνικής άσκησης με το NATO, *Locked Shields* και της ετήσιας *Cyber Challenge* από τον ENISA έχουν ως στόχο την ενίσχυση της ετοιμότητας των κρατών, ενώ η συνεχής διεύρυνση με στοιχεία πολιτικής

[48] (European Comission,Directorate General for Informatics, 2022,Μάιος)

από τους τομείς οικονομικών, νομικών και επικοινωνιακών ζητημάτων καταδεικνύει την ανάγκη πολυτομεακής ενίσχυσης της επίγνωσης για την κυβερνοασφάλεια. Παράλληλα, με στόχο την ενημέρωση και την ευαισθητοποίηση, ετησίως διοργανώνεται ο Ευρωπαϊκός μήνας για την ασφάλεια στον Κυβερνοχώρο καθώς και η ημέρα Ασφαλέστερου Διαδικτύου. Εδώ και επτά χρόνια εξάλλου διοργανώνεται και ο πανευρωπαϊκός διαγωνισμός Κυβερνοασφάλειας *European Cyber Security Challenge* από τον ENISA με συμμετοχή και της Ελλάδας.

Ο ENISA [49] προτείνει ένα πλαίσιο σχεδιασμού, εφαρμογής και υλοποίησης προγραμμάτων ενίσχυσης της κουλτούρας κυβερνοασφάλειας. Απαρχή του προγράμματος θα πρέπει να αποτελεί η συγκέντρωση των στοιχείων για την κυβερνοασφάλεια αναφορικά με τον τομέα δράσης του οργανισμού. Τα στοιχεία δύνανται να αντληθούν από τους εθνικούς CERTS αλλά και από το τμήμα Πληροφορικής του Οργανισμού. Η καταγραφή των διαδικασιών και η διαθεσιμότητα των πόρων χρειάζεται να ληφθούν σοβαρά υπόψη, ενώ σημαντικό στοιχείο αποτελεί η συνεργασία όλων και ιδιαίτερα η συνεργασία μεταξύ διοίκησης και του τμήματος Πληροφορικής, ώστε να υπάρξει αποτελεσματική κατανομή των ρόλων και των αρμοδιοτήτων. Η συμπερίληψη και η συνεργασία αποτελούν λέξεις κλειδιά για την επιτυχία του προγράμματος. Στον παρακάτω πίνακα παρουσιάζεται ο οδηγός οχτώ βημάτων του ENISA για τη δημιουργία ενός προγράμματος ευαισθητοποίησης:

[49] (ENISA, 2017)

Δράση	Τρόπος επίτευξης	Στόχος
Δημιουργία ομάδας εργασίας	Συνεργασία μεταξύ: Υπεύθυνων Ασφαλείας, Ανθρωπίνου Δυναμικού, Επικοινωνίας, Πληροφορικής, Νομικών Στρατηγικού Σχεδιασμού	Διασφάλιση της επίβλεψης και μεγιστοποίηση της επιτυχίας. Λογοδοσία
Επιχειρησιακή κατανόηση και ανάλυση ρίσκου	Επικοινωνία με υπαλλήλους και συγκέντρωση, σύγκριση στοιχείων	Κατανόηση κουλτούρας, τεχνικών και μέτρων που πρέπει να εφαρμοστούν
Προσδιορισμός στόχων, κρίσιμων παραγόντων επιτυχίας και ακροατηρίων	Συλλογή δεδομένων, προτεραιοποίηση ζητημάτων και ελλείψεων.	Μετρήσιμα αποτελέσματα για την επιτυχία του προγράμματος. Συλλογή συγκρίσιμων στοιχείων
Εκτίμηση της υφιστάμενης κατάστασης διενέργεια ανάλυσης ελλείψεων μεταξύ υφιστάμενης και στόχων	Παρακολούθηση και καταγραφή διαδικασιών ασφαλείας.	Δημιουργία χάρτη πορείας
Αναλυτική καταγραφή των δραστηριοτήτων και των στόχων	Δημιουργία χρονοδιαγράμματος Επιλογή περιεχομένου και μέσων.	Δημιουργία δεικτών Αποδοτικότητα και οικονομικότητα προγράμματος
Εκτέλεση	Κάθε μία δραστηριότητα ξεχωριστά ή και σε συνδυασμό.	Επίβλεψη
Μέτρηση αποτελεσμάτων	Σύγκριση με στόχους	Αξιολόγηση και ανατροφοδότηση
Προσδιορισμός αποτελεσμάτων	Μελέτη των μετρήσεων	Τροποποίηση και επαναπροσδιορισμός στρατηγικής και στόχων

Εικόνα 8 Τα 8 βήματα δημιουργίας του προγράμματος ευαισθητοποίησης

3.5 Η κουλτούρα ασφαλείας στην εθνική Στρατηγική

Η εθνική στρατηγική για την Κυβερνοασφάλεια ορίζει τις βασικές αρχές για την προστασία των φορέων. Βασιζόμενη στις κατευθυντήριες του ENISA υιοθετεί τον κύκλο ζωής των τεσσάρων φάσεων. Ειδικότερα, ο σχεδιασμός, η υλοποίηση, η αξιολόγηση και η παρακολούθηση αποτελούν μια ανατροφοδοτούμενη διαδικασία με στόχο την επικαιροποίηση των στρατηγικών, λόγω της δυναμικής του τοπίου των επιθέσεων.

Εικόνα 9 Κύκλος στρατηγικής Κυβερνοασφάλειας, κατά ENISA

Γενικότερα, η δημιουργία μιας στρατηγικής για την κυβερνοασφάλεια περιλαμβάνει την ανάλυση αξιολόγησης κινδύνου ενώ λαμβάνει υπόψη το κανονιστικό πλαίσιο, τις υπάρχουσες πολιτικές, τις κατευθυντήριες αλλά και τις βέλτιστες πρακτικές. Απαιτείται η δημιουργία μιας ξεκάθαρης δομής διακυβέρνησης με ρόλους, αρμοδιότητες και λογοδοσία για όλους τους εμπλεκομένους αλλά και η εγκαθίδρυση ένα μηχανισμού ανταλλαγής πληροφοριών μεταξύ των εμπλεκομένων. Βασικά στοιχεία της στρατηγικής είναι η ανάπτυξη των εθνικών σχεδίων έκτακτης ανάγκης, η προστασία κρίσιμων υποδομών, η διοργάνωση ασκήσεων κυβερνοασφάλειας, ο καθορισμός των βασικών κοινών μέτρων προστασίας της πληροφορίας και η καθιέρωση μηχανισμών αναφοράς περιστατικών, η ευαισθητοποίηση του χρήστη και η δημιουργία εκπαιδευτικών προγραμμάτων, κυρίως για την εξειδίκευση επαγγελματιών

πληροφορικής. Η στρατηγική θέτει και εξειδικεύει ένα σύνολο στόχων και δράσεων. Οι στόχοι εξυπηρετούν το στρατηγικό όραμα: την οικοδόμηση ενός σύγχρονου ψηφιακού περιβάλλοντος με τη δημιουργία υψηλού επιπέδου κυβερνοασφάλειας, την ενίσχυση της εμπιστοσύνης στην ψηφιακή διακυβέρνηση και την προστασία των δικαιωμάτων. Οι στόχοι φαίνονται στον παρακάτω πίνακα:

ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ	ΚΑΛΥΠΤΟΜΕΝΟΙ ΣΤΟΧΟΙ ENISA
Λειτουργικό σύστημα Διακυβέρνησης	Ανάπτυξη σχεδίων έκτατης ανάγκης, συμμετοχή σε διεθνείς συνεργασίες, θεσμοθέτηση συνεργασίας μεταξύ δημοσίων οργανώσεων
Θωράκιση κρίσιμων υποδομών ασφαλείας και νέες τεχνολογίες	Προστασία της υποδομής κρίσιμων πληροφοριών, θέσπιση βασικών μέτρων ασφαλείας, εξισορρόπηση ασφάλειας με προστασία ιδιωτικής ζωής
Βελτιστοποίηση διαχείρισης περιστατικών κυβερνοεγκλήματος, καταπολέμηση κυβερνοεγκλήματος και προστασία της ιδωτικότητας	Καθιέρωση μηχανισμών αναφοράς συμβάντων, καθιέρωση ικανότητας αντιμετώπισης συμβάντων, αντιμετώπιση του εγκλήματος στον κυβερνοχώρο
Ένα σύγχρονο επενδυτικό περιβάλλον με έμφαση στην προαγωγή της Έρευνας και Ανάπτυξης	Προώθηση της Έρευνας και Ανάπτυξης, παροχή κινήτρων στον ιδιωτικό τομέα για επενδύσεις σε μέτρα ασφαλείας, αξιοποίηση ΣΔΙΤ
Ανάπτυξη ικανοτήτων (capacity building), προαγωγή της ενημέρωσης και ευαισθητοποίησης	Αύξηση της ευαισθητοποίησης των χρηστών, οργάνωση ασκήσεων ασφαλείας στον κυβερνοχώρο, ενίσχυση των προγραμμάτων κατάρτισης και εκπαίδευσης.

Εικόνα 10 Οι 5 στόχοι της Εθνικής στρατηγικής για την κυβερνοασφάλεια

Ο πέμπτος στόχος αφορά στην ανάπτυξη ικανοτήτων με την αύξηση της ευαισθητοποίησης των χρηστών, την οργάνωση ασκήσεων ασφαλείας και την ενίσχυση προγραμμάτων κατάρτισης και εκπαίδευσης. Ειδικότερα, η οργάνωση ασκήσεων κυβερνοασφάλειας στοχεύει στην εκπαίδευση, αξιολόγηση και ενίσχυση της

ετοιμότητας των φορέων αλλά και στην ανταλλαγή πληροφοριών και γνώσεων. Προτείνονται η ανάπτυξη και η χρήση ειδικών πλατφορμών για την προσομοίωση των ασκήσεων, η τεχνική εκπαίδευση των στελεχών των φορέων αλλά και η συμμετοχή της χώρας στις προαναφερθείσες ασκήσεις. Παράλληλα, στοχεύει στην αξιοποίηση σύγχρονων μεθόδων και εργαλείων κατάρτισης, στην εκπόνηση Σχεδίου Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση και στην δημιουργία του πλαισίου αναβάθμισης Τεχνογνωσίας και Ικανοτήτων Επαγγελματιών. Ταυτόχρονα, προβλέπει την διαρκή ενημέρωση φορέων και πολιτών σε θέματα Κυβερνοασφάλειας με την δημιουργία του εθνικού Προγράμματος Ευαισθητοποίησης και τη διαμόρφωση του πλαισίου επικοινωνιακής διαχείρισης περιστατικών.

Η στρατηγική αναφορικά με το στόχο της εκπαίδευσης δημιουργεί τρία επίπεδα συνεχούς δράσης: το ένα αφορά στους συμμετέχοντες στο οικοσύστημα κυβερνοασφάλειας, το δεύτερο στους επαγγελματίες της πληροφορικής και το τρίτο στο σύνολο των πολιτών. Η τριπλή αυτή διάκριση κρίνεται απαραίτητη καθώς η κουλτούρα ασφαλείας έχει περιεχόμενο πολυδιάστατο. Προκρίνεται, εξάλλου, ο ρόλος των ακαδημαϊκών ιδρυμάτων στην εξειδικευμένη εκπαίδευση επαγγελματιών ασφαλείας, βάσει της δημιουργίας συγκεκριμένων επαγγελματικών προφίλ και η συνεχής κατάρτιση και εκπαίδευση των στελεχών του δημόσιου τομέα σε σχέση με τα ζητήματα ασφαλείας.

Στα πλαίσια αυτά η Εθνική Αρχή Κυβερνοασφάλειας έχει εκπονήσει το εγχειρίδιο-οδηγό κυβερνοασφάλειας [50] αλλά και το εργαλείο αυτοαξιολόγησης της Κυβερνοασφάλειας των Οργανισμών. Το εγχειρίδιο προτείνει σειρά βέλτιστων πρακτικών για τη συνολική ασφάλεια των πληροφοριακών συστημάτων, ενώ καθοδηγεί για τη δημιουργία εκπαιδευτικών προγραμμάτων και για την αύξηση της επίγνωσης του προσωπικού σε θέματα κυβερνοασφάλειας. Ειδικότερα ως μέτρα προστασίας σε σχέση με το στόχο της ευαισθητοποίησης προτείνει:

1. Την δημιουργία πολιτικής εκπαίδευσης χρηστών με συγκεκριμένο σκοπό, πεδίο εφαρμογής, ρόλους, ευθύνες και διαδικασίες υλοποίησης.
2. Την οργάνωση εκπαιδευτικών προγραμμάτων ευαισθητοποίησης και επίγνωσης προσωπικού σε θέματα ασφαλείας, περιοδικά επαναλαμβανόμενο και με περιεχόμενο στοχευμένο στις διαφορετικές κατηγορίες υπαλλήλων και στην αλληλεπίδραση χρήστη, συσκευών και δικτύου, στην χρήση ισχυρών κωδικών

[50] (Εθνική Αρχή Κυβερνοασφάλειας, 2021)

πρόσβασης, στους τρόπους ανίχνευσης διαφόρων μορφών επιθέσεων κοινωνικής μηχανικής και στην αναγνώριση παραβίασης του συστήματος.

3. Την ανάλυση γνωσιακών κενών του προσωπικού.
4. Τη διενέργεια ασκήσεων προσομοίωσης περιστατικών κυβερνοασφάλειας.

Το ερωτηματολόγιο αυτοαξιολόγησης[51] για τους Οργανισμούς, αποτελεί ένα εργαλείο προσδιορισμού κενών αλλά και αποτελεσμάτων. Συγκεκριμένα για την επίγνωση θέτει τις παρακάτω ερωτήσεις:

	13. Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας		
	Ερωτήματα	Απαντήσεις	Βαρύτητα
	Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην εκπαίδευση και ευαισθητοποίηση του προσωπικού σε θέματα κυβερνοασφάλειας.	Δεν απαντήθηκε	3
	Ο Οργανισμός διενεργεί σε περιοδική βάση εκπαιδευτικό πρόγραμμα με σκοπό την ευαισθητοποίηση και ανάπτυξη δεξιοτήτων του προσωπικού σε θέματα κυβερνοασφάλειας. Η ύλη των εκπαιδεύσεων περιλαμβάνει:		
1	- Τους τρόπους αλληλεπίδρασης του χρήστη με τα συστήματα, το δίκτυο και τα δεδομένα του Οργανισμού με ασφαλή τρόπο.	Δεν απαντήθηκε	2
2	- Τους τρόπους αναγνώρισης των επιθέσεων κοινωνικής μηχανικής, όπως είναι τα email εξαπάτησης (phishing), οι τηλεφωνικές κλήσεις πλαστοπροσωπίας κ.α.	Δεν απαντήθηκε	3
3	- Τις καλές πρακτικές αυθεντικοποίησης, όπως είναι η δημιουργία ισχυρών κωδικών πρόσβασης και η πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication).	Δεν απαντήθηκε	3
4	- Την αναγνώριση ενδείξεων παραβίασης συστημάτων και περιστατικών που προέρχονται από απειλές εκ των έσω (insider threats).	Δεν απαντήθηκε	2
	Ο Οργανισμός διενεργεί σε περιοδική βάση εκπαιδευτικό πρόγραμμα ευαισθητοποίησης του προσωπικού για θέματα κυβερνοασφάλειας βασισμένο σε διακριτούς ρόλους και στοχευμένο σε διαφορετικές κατηγορίες εργαζομένων με βάση το επιχειρησιακό αντικείμενο και το επίπεδο τεχνικής εξειδίκευσης.	Δεν απαντήθηκε	2
	Ο Οργανισμός έχει διενεργήσει ανάλυση γνωσιακών κενών του προσωπικού (knowledge gap analysis), με σκοπό τη σύνταξη ενός πλάνου δημιουργίας διαδοχικών εκπαιδεύσεων.	Δεν απαντήθηκε	1
	Ο Οργανισμός διενεργεί σε περιοδική βάση ασκήσεις προσομοίωσης περιστατικών κυβερνοασφάλειας και των επιπτώσεών τους, όπως π.χ. το άνοιγμα ενός κακόβουλου αρχείου συνημμένου σε email ή την επίσκεψη σε κακόβουλη ιστοσελίδα.	Δεν απαντήθηκε	1

Εικόνα 11 Ερωτηματολόγιο αυτοαξιολόγησης Εθνική Αρχή Κυβερνοασφάλειας

Στο Εθνικό Σχέδιο Ανάκαμψης και Ανθεκτικότητας[52] στον άξονα της Ψηφιακής Μετάβασης και συγκεκριμένα στον ψηφιακό μετασχηματισμό του κράτους, προτεινόμενη μεταρρύθμιση αποτελεί η εφαρμογή ευρείας κλίμακας στρατηγικών και πολιτικών κυβερνοασφάλειας με επένδυση στη βελτίωση της κυβερνοασφάλειας και τη δημιουργία Εθνικού Κέντρου Κυβερνοασφάλειας, συνολικού κόστους 32 εκ. ευρώ.

Περαιτέρω σημαντικές πρωτοβουλίες αποτελούν τα μαθήματα της Ψηφιακής Ακαδημίας Πολιτών[53] αλλά και το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου[54].

[51] (Εθνική Αρχή κυβερνοασφάλειας, 2022)
[52] (gov.gr)
[53] (NDG)
[54] (Saferinternet4kids)

Πρόσφατα, εξάλλου, δόθηκε η δυνατότητα στους πολίτες να υποβάλλουν ψηφιακά καταγγελίες προς τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος για εγκλήματα στον κυβερνοχώρο μέσω της Ενιαίας Ψηφιακής Πύλης[55]. Παράλληλα, η λειτουργία του ιστοτόπου https://cyberalert.gr/ του Υπουργείου Προστασίας του Πολίτη σε συνεργασία με την ΕΛ.ΛΑΣ, αποτελεί μια καινοτόμο δράση που αφορά και στη δυναμική ενημέρωση και ευαισθητοποίηση των πολιτών.

3.6 Η κουλτούρα ασφαλείας στις στρατηγικές των κρατών -μελών και του Ηνωμένου Βασιλείου: κοινά στοιχεία και βέλτιστες πρακτικές.

Κοινός τόπος στις δράσεις ευαισθητοποίησης και εκπαίδευσης είναι το πρόγραμμα Safer Internet, της Ευρωπαϊκής Επιτροπής. Σχεδόν όλες οι χώρες της ΕΕ έχουν αναπτύξει κάποιο πρόγραμμα ευαισθητοποίησης. Ταυτόχρονα στις περισσότερες από τις εθνικές αρχές CERT, λειτουργούν ιστοσελίδες σε σχέση με την καταγγελία περιστατικών ασφαλείας. Αναφορικά με την ευαισθητοποίηση τονίζεται ότι οι περισσότερες χώρες διεξάγουν ασκήσεις κυβερνοασφάλειας. Παράλληλα, είναι σημαντικό να τονιστεί ότι τα προγράμματα απευθύνονται στο ευρύ κοινό και εδώ σημειώνεται η σημασία επέκτασης των προγραμμάτων τόσο στον επιχειρηματικό κόσμο όσο και στους δημόσιους οργανισμούς.

Την ίδια εικόνα παρουσιάζει, εν γένει και το Ηνωμένο Βασίλειο. Μια από τις πρακτικές μάλιστα εκεί είναι το σημείο WARP[56] (Warning, Advice and Reporting Point), μια υπηρεσία διαμοιρασμού πληροφορίας και γνώσης αναφορικά με τα συμβάντα κυβερνοασφάλειας, υπό την Εθνική Αρχή Κυβερνοασφάλειας.

Μια πρακτική, που εφαρμόζεται σε χώρες της Ευρώπης με ολιστικές προσεγγίσεις ασφαλείας, είναι η διοργάνωση συνεδρίων αναφορικά με τα ζητήματα Κυβερνοασφάλειας, ιδιαίτερα γνωστό είναι το IT Security Incident Management & IT forensics[57], στη Γερμανία. Παράλληλα, στην Ισπανία έμφαση έχει δοθεί στην επικοινωνία και ευαισθητοποίηση των επαγγελματιών πληροφορικής, ενώ η κυβερνητική CERT διεξάγει σεμινάρια και εργαστήρια για την ενίσχυση της ευαισθητοποίησης και την αναβάθμιση γνώσεων του προσωπικού της διοίκησης. Στο Λουξεμβούργο λειτουργεί εθνική διαδικτυακή πύλη για την ασφάλεια πληροφοριών απευθυνόμενη στον ιδιωτικό τομέα παρέχοντας συμβουλές για πρακτικές ασφαλείας, τεχνικά μέσα αλλά και την συμμόρφωση με τα διεθνή πρότυπα. Στην Αυστρία, η Πύλη

[55] (govgr, 2022)
[56] (NCSC.UK)
[57] (IMF)

Ασφαλείας των ΤΠΕ, απευθύνεται σε διαφορετικές κοινωνικές, ηλικιακές και επαγγελματικές ομάδες τόσο του ιδιωτικού όσο και του δημόσιου τομέα παρέχοντας ένα ευρύ φάσμα πληροφόρησης, ενώ διοργανώνει και εργαστήρια σε σχολεία. Ο γαλλικός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριακών Συστημάτων[58] (Anssi) λειτουργεί μια διαδικτυακή Πύλη παροχής πληροφοριών και συμβουλών για τους πολίτες. Στην Πύλη, ο Γάλλος πολίτης δύναται να βρει στοιχεία ορολογίας, κατευθύνσεις για την ορθή ρύθμιση λογισμικών, διαδικτυακά εκπαιδευτικά προγράμματα αλλά και λύσεις για την προστασία των υπολογιστών.

4 Δημιουργία προγράμματος ευαισθητοποίησης για τους δημόσιους οργανισμούς

Στο παρόν κεφάλαιο διερευνώνται τα βασικά συστατικά της δημιουργίας και διαχείρισης ενός ιστοτόπου που θα προσφέρει ένα πρόγραμμα επίγνωσης ασφαλείας απευθυνόμενο σε δημοσίους υπαλλήλους. Οι προτάσεις βασίστηκαν στην ευέλικτη μεθοδολογία ανάπτυξης έργου αλλά και στις κατευθυντήριες του ENISA και του εγχειριδίου Κυβερνοασφάλειας. Προτεινόμενο εργαλείο διαχείρισης περιεχομένου είναι το Wordpress[59] , ενώ προτείνεται η ένταξη στην Ενιαία Ψηφιακή Πύλη βάσει του νόμου 4727/20.

4.1 Γενικό πλαίσιο της ψηφιακής δράσης «Πρόγραμμα επίγνωσης ασφαλείας στους δημόσιους οργανισμούς».

Η αποτελεσματική δημιουργία ενός προγράμματος επίγνωσης για την ασφάλεια εξαρτάται από πολλούς παράγοντες. Καταρχάς, δομείται επί του γενικού πλαισίου της πολιτικής ασφαλείας του εκάστοτε οργανισμού, λόγω των ιδιαίτερων επιχειρησιακών λειτουργιών, και φυσικά στη βάση των διαδικασιών ασφαλείας. Βασικό ρόλο σε αυτό έχουν οι υπεύθυνοι ασφαλείας, οι οποίοι παρακολουθούν και καταγράφουν το σύνολο αλλά και τα είδη των επιθέσεων στον οργανισμό και εφαρμόζουν τις διαδικασίες ασφαλείας, αξιολογώντας αναλυτικά την αποτελεσματικότητά τους μέσω συγκεκριμένων δεικτών[60]. Οι ηλεκτρονικές βάσεις δεδομένων, τα αποθετήρια γνώσης, τα συστήματα παρακολούθησης των κυβερνοαπειλών, οι γνωσιακές βάσεις για τακτικές και τεχνικές επίθεσης [61] αποτελούν σημαντικούς πόρους διαχείρισης γνώσης και

[58] (SSI)
[59] (WP)
[60] Άρθρο 6 Υπουργική Απόφαση 1027/2019 - ΦΕΚ 3739/Β/8-10-2019 Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α 199).
[61] Για παράδειγμα η γνωσιακή βάση MITRE ATT&CK® αποτελεί ένα τέτοιο εργαλείο https://attack.mitre.org/

δημιουργίας αντιμέτρων. Κατά δεύτερον, οι οικονομικοί πόροι απαιτώνται για την οργάνωση οποιουδήποτε προγράμματος. Εδώ αναφέρονται αφενός πόροι που σχετίζονται με επενδύσεις για την τεχνολογική υποστήριξη της ασφάλειας και αφετέρου πόροι που θα επενδυθούν στην κατάρτιση του προσωπικού αλλά και σε ένα σύστημα κινήτρων και ανταμοιβών, το οποίο χρειάζεται να συνοδεύει οποιοδήποτε πρόγραμμα ανάπτυξης δεξιοτήτων. Κατά τρίτον, η οργανωτική δομή διαδραματίζει σπουδαίο ρόλο στον σχεδιασμό και την υλοποίηση του προγράμματος. Ευνόητα, συνδέεται με την οργανωσιακή δομή του οργανισμού, η οποία και δημιουργεί τους ρόλους, τις αρμοδιότητες και την κατανομή των καθηκόντων, επηρεάζοντας τη ροή της γνώσης εντός του οργανισμού. Ξεκάθαρο πλαίσιο ρόλων και αρμοδιοτήτων, πολυτμηματική συνεργασία και συμπερίληψη των εμπλεκομένων, υποστήριξη και ανάμειξη της ανώτατης διοίκησης και της ηγεσίας του οργανισμού, οργανωσιακή κουλτούρα και κουλτούρα διάχυσης της γνώσης (δίκτυα γνώσης, μέσα ανταλλαγής γνώσης, αξιακό σύστημα) αποτελούν τους βασικούς κρίσιμους παράγοντες επιτυχίας. Κατά τέταρτον, το ανθρώπινο κεφάλαιο του οργανισμού αποτελεί μια σημαντική διάσταση. Εδώ, διερευνάται το ζήτημα της στόχευσης σε σχέση με το ανθρώπινο δυναμικό. Κρίσιμα ερωτήματα που πρέπει να απαντηθούν είναι:

- Το πρόγραμμα στοχεύει στο σύνολο των υπαλλήλων ή σε ομάδες ειδικών;
- Ποιες οι γνώσεις και οι δεξιότητες των υπαλλήλων σε σχέση με τα πληροφοριακά συστήματα;
- Ποιες οι απόψεις και κυρίως ποιες οι συμπεριφορές των υπαλλήλων αναφορικά με την ασφάλεια;
- Πώς οι λύσεις ευθυγραμμίζονται με τις ανάγκες τις επιχειρησιακές, χωρίς να εμποδίζουν τη ροή των εργασιών και κατά συνέπεια μπορούν να πείσουν για τη σημασία της ασφάλειας χωρίς να δημιουργούν «κόπωση ασφαλείας»;
- Υπάρχει στον οργανισμό κουλτούρα ασφαλείας και σε ποιο βαθμό;
- Ποιο το επίπεδο γνώσεων και εκπαίδευσης των εκπαιδευτών ασφαλείας;

Κατά πέμπτον, ένα εξίσου σημαντικό ζήτημα είναι αυτό της ανάπτυξης των μηχανισμών διάχυσης της γνώσης για την ασφάλεια. Οι μηχανισμοί αυτοί δύνανται να είναι επίσημοι ή ανεπίσημοι και να σχετίζονται με την εφαρμογή της τεχνογνωσίας ή με την ενσωμάτωση και ερμηνεία της πληροφορίας. Η δημιουργία των κατάλληλων μηχανισμών σχετίζεται με παράγοντες κοινωνικούς, όπως η επιρροή από τους ομότιμους και η κοινωνική αλληλεπίδραση, περιβαλλοντικούς, για παράδειγμα οι

αλλαγές στην διάταξη και το χώρο, αλλά και με την περιοδικότητα, το περιεχόμενο των προγραμμάτων και τη μέτρηση των αποτελεσμάτων. Κατά συνέπεια τα ζητήματα που πρέπει να απαντηθούν είναι:

- Κάθε πότε και πόσο συχνά θα διενεργείται το πρόγραμμα, έχοντας ως στόχο την συνεχή ενδυνάμωση της κατάλληλης συμπεριφοράς και φυσικά την ανταπόκριση στις εξελισσόμενες απειλές;
- Ποιες πληροφορίες είναι οι κατάλληλες, έχοντας ως στόχο την ανταπόκριση στις ανάγκες του ανθρώπινου κεφαλαίου;
- Ποιες οι δραστηριότητες που θα επιλεγούν και πόσο κοντά θα φέρουν το στόχο;
- Ποιο μήνυμα χρειάζεται να διακινηθεί και πώς θα διακινηθεί; Εδώ, πρέπει να αναζητηθεί η κινητοποίηση μέσω της επιλογής των κατάλληλων μέσων πειθούς και η θετική επικοινωνιακή διάσταση.
- Θα υπάρχουν κίνητρα, ανταμοιβές και ποινές; Και αν ναι σε ποιο πλαίσιο θα λειτουργήσουν;
- Ποιοι και τι είδους δείκτες θα χρησιμοποιηθούν για την αξιολόγηση του προγράμματος;

Ο ανθρωποκεντρικός σχεδιασμός των ψηφιακών υπηρεσιών και οι ευέλικτες μεθοδολογίες ανάπτυξης έργων πληροφορικής δύνανται να απαντήσουν στα παραπάνω ερωτήματα για την αποτελεσματικότερη και παραγωγική ανταπόκριση στις αλλαγές. Ειδικότερα επιλέγεται η διεργασία Scrum[62], ένα δημοφιλές εργαλείο χρησιμοποιούμενο στις υλοποιήσεις για το ελληνικό Δημόσιο[63]. Σε αυτό το πλαίσιο, η σχεδίαση είναι ανθρωποκεντρική, αφορώντας όσους επηρεάζονται από την υπηρεσία, είναι ρεαλιστική, καλύπτοντας πραγματικές και βασισμένες σε δεδομένα ανάγκες, είναι συνεργατική, εμπλέκοντας ενεργά όλους τους συμμετέχοντες, δημιουργεί μια υπηρεσία από την αρχή ως το τέλος με σειρά διαδοχικών βημάτων, είναι ανατροφοδοτούμενη σε όλα τα στάδια και τις φάσεις και ολιστική, προσφέροντας μια ενιαία και ολοκληρωμένη εμπειρία στο χρήστη. Η διαδικασία του σχεδιασμού της ψηφιακής δράσης περνά από διάφορα στάδια εμπλέκοντας σε κάθε φάση τους τελικούς χρήστες, τα μέλη της ομάδας έργου και τον ιδιοκτήτη του έργου ώστε να διασφαλίζεται η κοινή αντίληψη.

Σε πρώτη φάση απαραίτητο στοιχείο είναι η έρευνα, οπότε και καταγράφεται η υφιστάμενη κατάσταση, το θεσμικό και τεχνικό πλαίσιο και τα υφιστάμενα

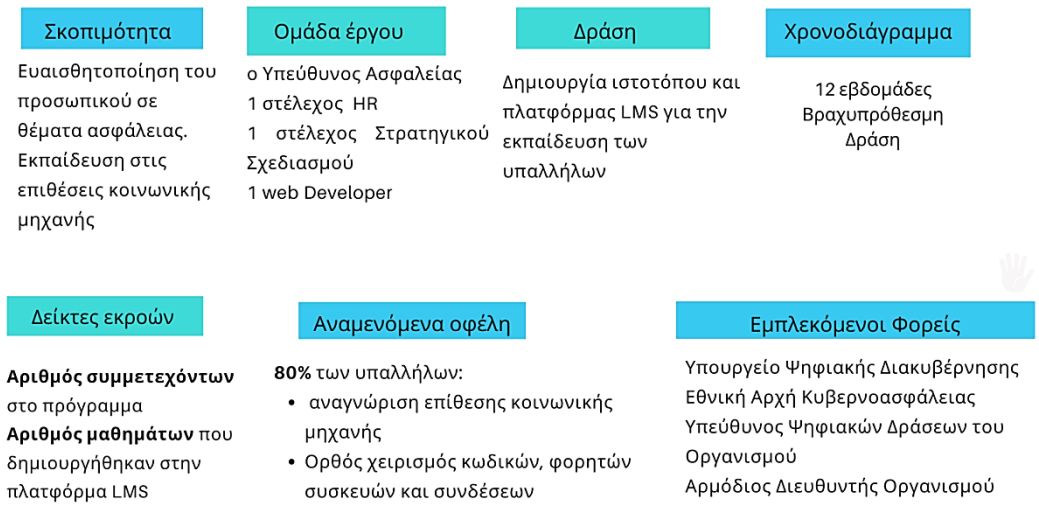
[62] https://scrumguides.org/download.html
[63] Αποτελεί βασικό πλαίσιο των υλοποιήσεων από την ΕΔΥΤΕ https://analysis.digigov.grnet.gr/docs/agile

πληροφοριακά συστήματα. Η έρευνα δύναται να πραγματοποιηθεί με πολλά εργαλεία, και προτείνεται να συνδυάζει ποιοτικές με ποσοτικές αναλύσεις. Στην περίπτωση ενός προγράμματος για την ασφάλεια στους οργανισμούς μπορεί να βασίζεται σε ημιδομημένες συνεντεύξεις με τους υπευθύνους ασφαλείας οργανισμών του Δημοσίου αλλά και απαντήσεις των υπαλλήλων σε ερωτηματολόγια[64], αναφορικά με την κυβερνοασφάλεια. Μπορεί ταυτόχρονα να συμπεριλάβει δεδομένα που σχετίζονται με τις επιθέσεις κοινωνικής μηχανικής και άλλα δεδομένα δευτερογενούς έρευνας. Αναλύοντας τα δεδομένα είναι δυνατό να προχωρήσουμε σε εντοπισμό των εμποδίων και των ευκαιριών ώστε να καθοριστεί η ανάγκη. Παράλληλα, κρίνεται ιδιαίτερα σκόπιμο να καταγραφεί η εμπειρία του χρήστη ώστε η εκπαίδευση να είναι στοχευμένη και να ανταποκρίνεται στις ανάγκες του.

Σε δεύτερη φάση, η σχεδίαση του έργου περιλαμβάνει το σχεδιασμό της νέας διαδικασίας, την περιγραφή της τεχνικής λύσης, τον προγραμματισμό της ανάπτυξης σε διαδοχικά βήματα με εκτίμηση της χρονικής διάρκειας και των ανθρώπινων και υλικών πόρων και την ευέλικτη ανάπτυξη δηλαδή σε διαδοχές συγκεκριμένου χρονικού διαστήματος.

4.2 Δομή και περιεχόμενο του προγράμματος

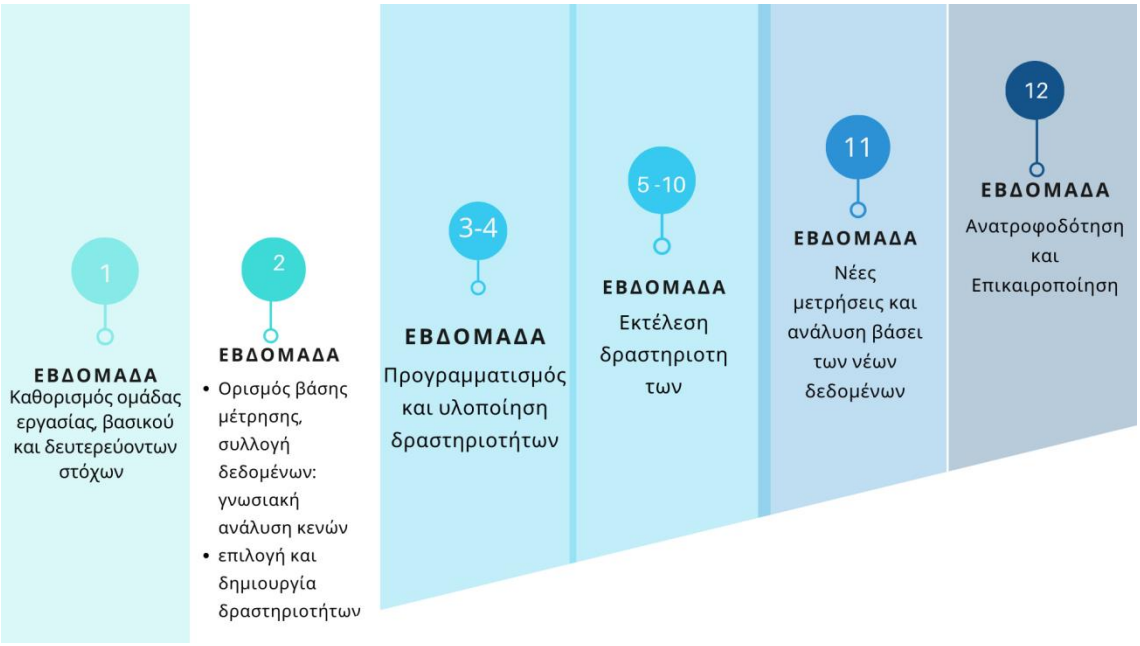
Το γενικό πλαίσιο δημιουργίας του προγράμματος περιγράφεται στην παρακάτω εικόνα:



[64] **ΠΑΡΑΡΤΗΜΑ 1 Ερωτηματολόγιο Αξιολόγησης**

Εικόνα 12 Το πλαίσιο του προγράμματος, ίδια επεξεργασία με Canva

Ο γενικός σχεδιασμός του προγράμματος ακολουθεί τα παρακάτω βήματα εντός του πλαισίου των 12 εβδομάδων:



Εικόνα 13 Πλάνο προγράμματος, ίδια επεξεργασία με Canva

Η εκπαίδευση συνίσταται να οργανωθεί βάσει των θεματικών:

- Βασική ορολογία για την κυβερνοασφάλεια: όροι που αφορούν στην ασφάλεια των πληροφοριακών συστημάτων, βασικές έννοιες, τεχνικά αντίμετρα, είδη επιθέσεων.
- Χρήση και διαχείριση κωδικών πρόσβασης: βέλτιστες πρακτικές για την δημιουργία και διαχείριση κωδικών πρόσβασης.
- Αναγνώριση μιας επίθεσης κοινωνικής μηχανικής: παραδείγματα, τρόποι ανίχνευσης, συστάσεις και βέλτιστες πρακτικές αντιμετώπισης.
- Στρατηγική και πολιτικές ασφαλείας του Οργανισμού με ειδικότερες θεματικές τις πολιτικές: καθαρού γραφείου, ηλεκτρονικού ταχυδρομείου, τηλεργασίας, μέσων κοινωνικής δικτύωσης, χρήσης διαδικτυακών υπηρεσιών του οργανισμού.

- Διαδικασίες ασφαλείας του Οργανισμού με ειδικότερες θεματικές: τη διαδικασία διαχείρισης περιστατικών ασφαλείας και τη διαδικασία αντιμετώπισης περιστατικών παραβίασης προσωπικών δεδομένων.
- Εμπιστευτικότητα πληροφορίας: διαβάθμιση, κανόνες προστασίας της εμπιστευτικής υπηρεσιακής πληροφορίας, εξουσιοδότηση, προστασία ηλεκτρονικής πληροφορίας με κρυπτογράφηση, ψηφιακή υπογραφή, προσωπικά δεδομένα.

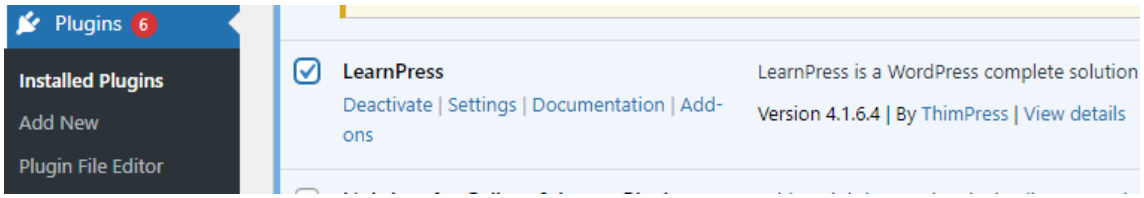
Περαιτέρω το περιεχόμενο δύναται να αναπτυχθεί με πολλαπλές μορφές, κειμένου ή πολυμέσων. Ιδιαίτερα σύγχρονες τάσεις στην εκπαίδευση ασφαλείας θεωρούνται η χρήση ψηφιακού παιχνιδιού αλλά και ασκήσεων προσομοίωσης, αφού αποτελούν μια συμμετοχική και ενεργητική διαδικασία μάθησης εντός ψηφιακού περιβάλλοντος. Είναι αναγκαίο να υπερκεραστεί το παθητικό μέρος της εξ αποστάσεως εκπαίδευσης και να χρησιμοποιηθούν δραστηριότητες που θα δημιουργήσουν περιβάλλον αυτενέργειας, αλληλεπίδρασης και επανάληψης, ώστε ο εκπαιδευόμενος να μην προσπεράσει την ασφάλεια ως απλή οδηγία αλλά να την εμπεδώσει. Καθώς η ανάπτυξη του περιεχομένου θα γίνει μέσω ιστοσελίδας, μπορεί να γίνει διασύνδεση με εξωτερικούς συνδέσμους που προσφέρουν ανοικτά και δωρεάν παιχνίδια και ασκήσεις προσομοίωσης συχνά με την προϋπόθεση της εγγραφής ή και τη δημιουργία ψηφιακών παιχνιδιών με «ανοικτού κώδικα λογισμικό»[65].

4.3 Προτάσεις για τη δημιουργία του προγράμματος

Για την δημιουργία του προγράμματος μπορεί να χρησιμοποιηθεί το ελεύθερο και ανοικτού κώδικα λογισμικό διαχείρισης περιεχομένου WordPress **(ΠΑΡΑΡΤΗΜΑ3 Εγκατάσταση WordPress**), το οποίο δίνει τη δυνατότητα δημιουργίας δυναμικών ή και στατικών ιστοσελίδων, ενώ διαθέτει πρόσθετα που ενισχύουν τη λειτουργικότητα της πλατφόρμας. Τοιουτοτρόπως, δίνεται η δυνατότητα δημιουργίας ενός δικτυακού τόπου για την κυβερνοασφάλεια στον Οργανισμό. Στον ιστότοπο αναρτώνται νέα, άρθρα, θέματα και δράσεις για την κυβερνοασφάλεια, ενώ διατυπώνονται σχόλια και απορίες. Προτείνεται να προσαρμοστεί τεχνικά και σχεδιαστικά, ώστε να ενταχθεί στην Ενιαία Ψηφιακή Πύλη, καλύπτοντας τις βασικές αρχές του πολιτοκεντρικού σχεδιασμού, της διαλειτουργικότητας, και της επαναχρησιμοποίησης δομικών

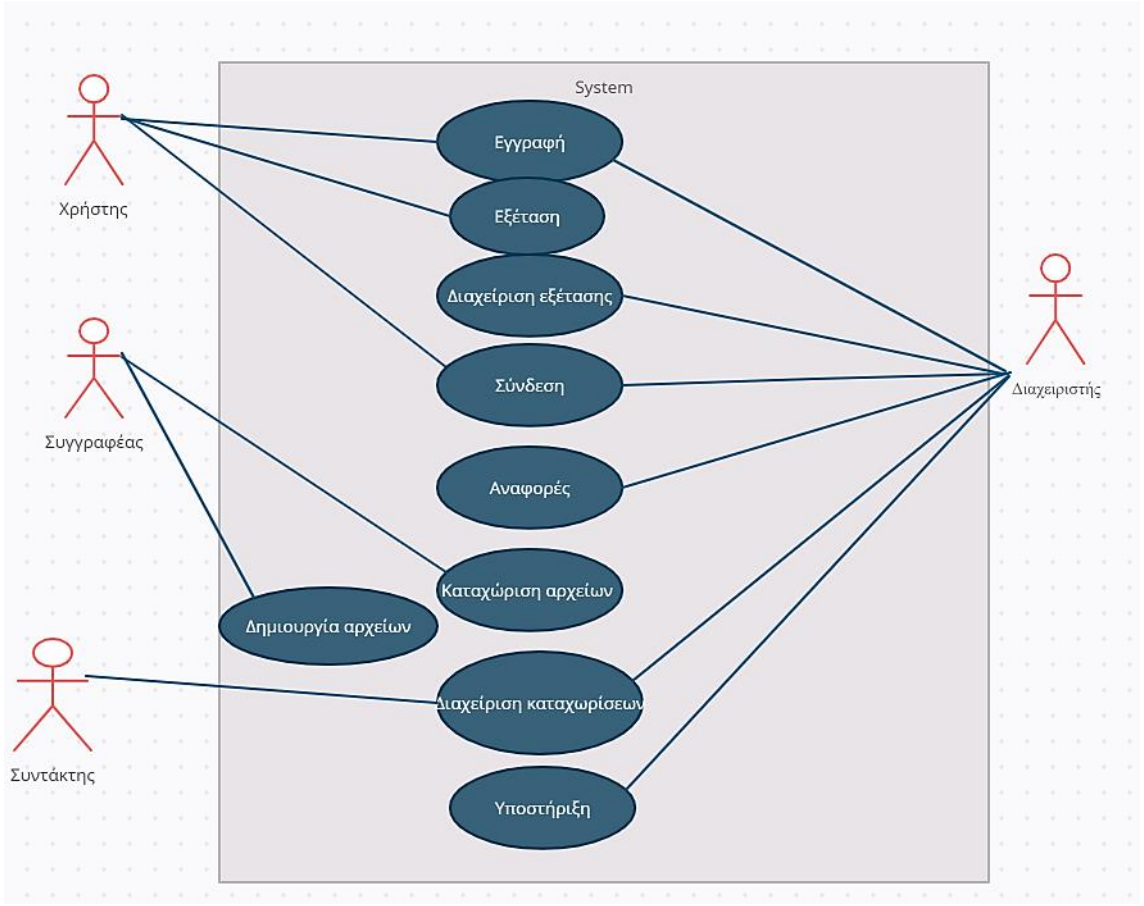
[65] https://www.ibm.com/skills/topics/cybersecurity/ και https://www.informatique-mania.com/el/applications/decouvrez-ces-jeux-open-source-qui-copient-et-ameliorent-les-originaux/

στοιχείων (αυθεντικοποίηση, διαλειτουργικότητα, εξυπηρέτηση, επικοινωνία, μηχανισμός δημιουργίας συμβατός με την προσβασιμότητα). Παράλληλα, από τη λειτουργία των προσθέτων δύναται να εγκατασταθεί ένα σύστημα διαχείρισης μάθησης όπως αυτό που φαίνεται παρακάτω:



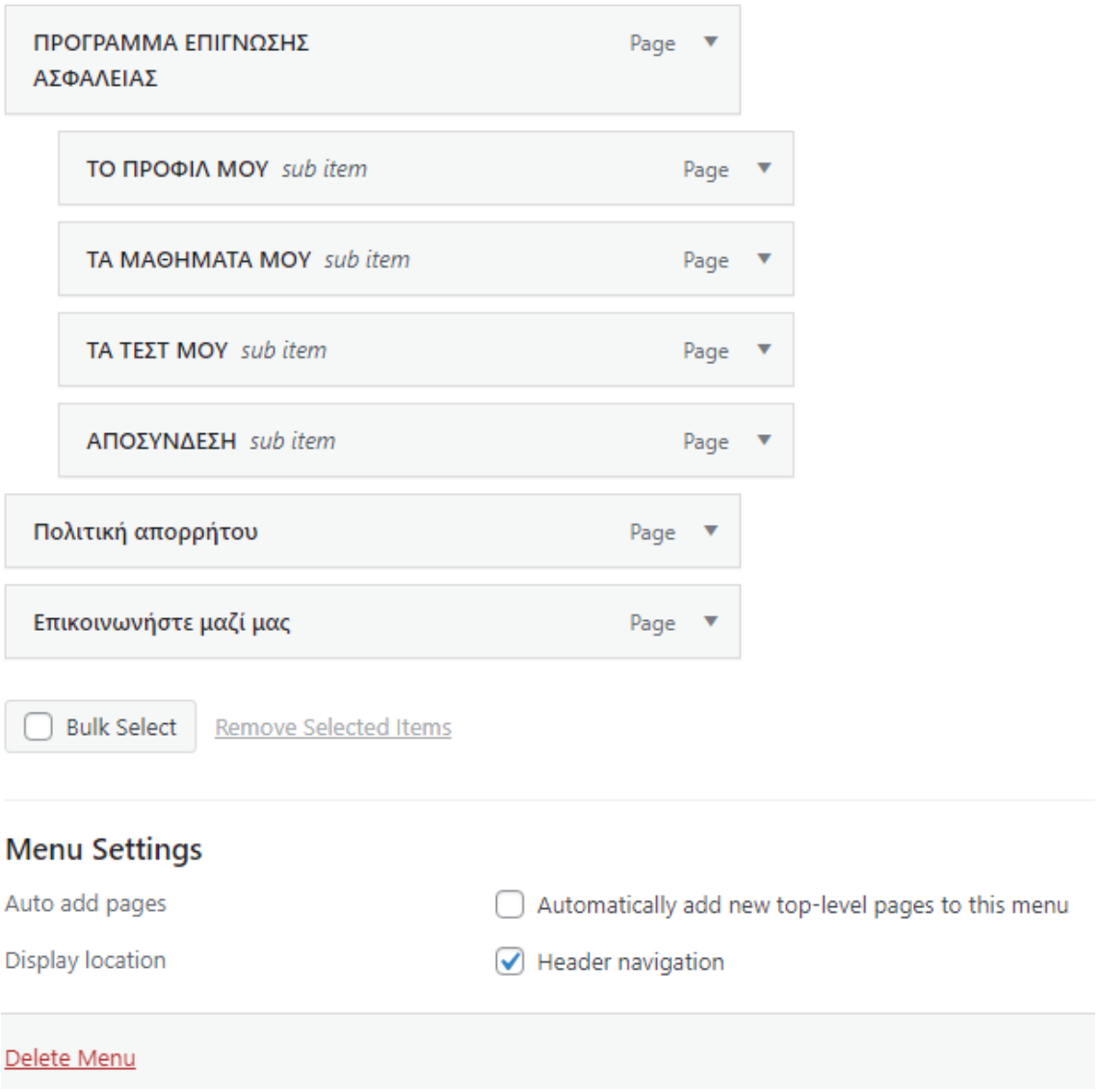
Εικόνα 14 Το πρόσθετο για τη δημιουργία της πλατφόρμας εκπαίδευσης

Η πρόσβαση στο σύστημα διαχείρισης μάθησης θα γίνεται με κωδικούς δημόσιας διοίκησης, αξιοποιώντας την διαδικτυακή υπηρεσία της αυθεντικοποίησης χρηστών δημόσιας διοίκησης (oAuth2.0.PA) της ΓΓΠΣΔΔ. Για τις λειτουργικές απαιτήσεις του συστήματος και την δημιουργία των ρόλων προσδιορίζονται οι χρήστες και η αλληλεπίδρασή τους με το σύστημα ως εξής:

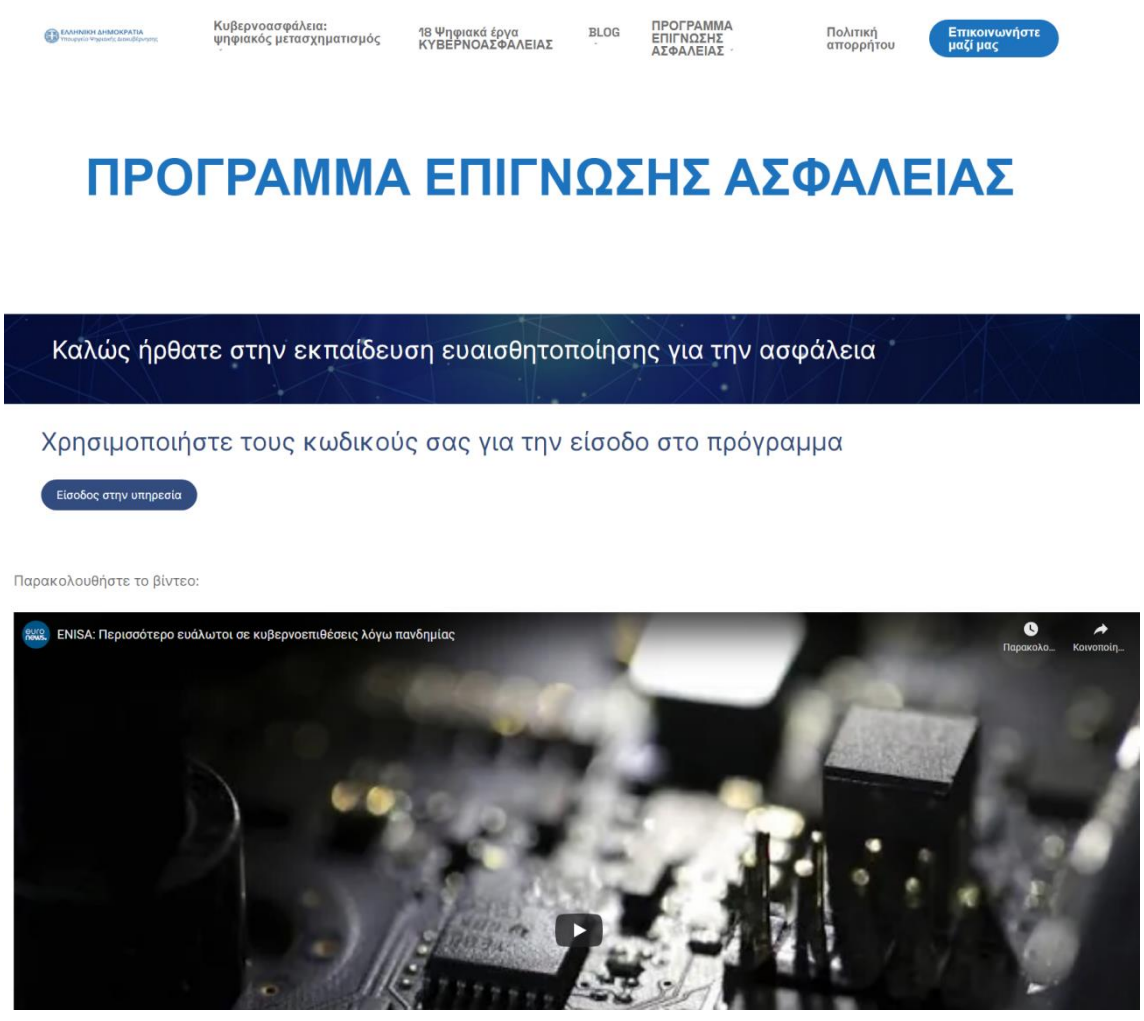


Εικόνα 15 Use case συστήματος διαχείρισης μάθησης, ίδια επεξεργασία με creately

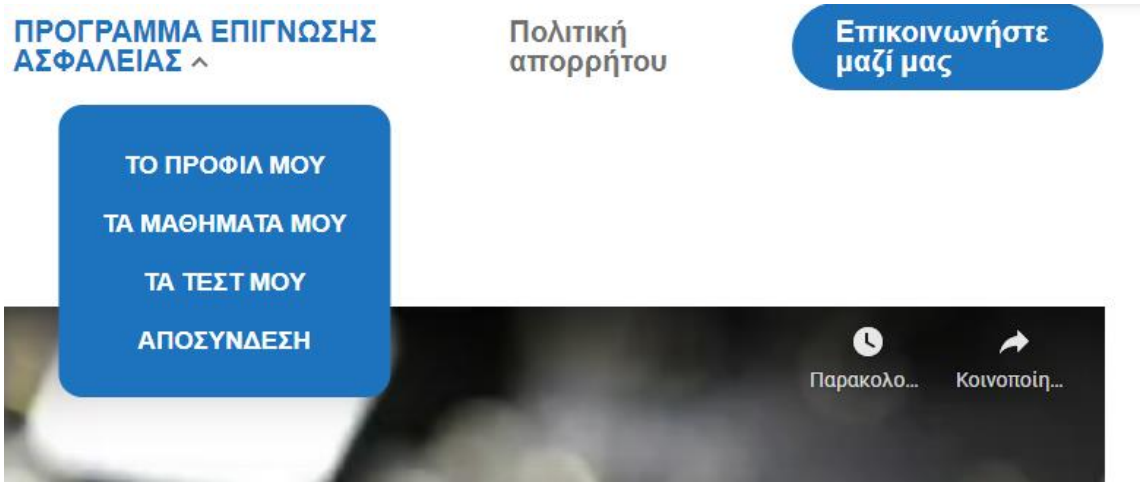
Ο προσδιορισμός των ρόλων και των δικαιωμάτων στο σύστημα είναι ιδιαίτερα σημαντικός, καθώς με αυτό τον τρόπο διασφαλίζονται οι απαιτήσεις αλλά και η ροή του συστήματος. Για αυτό χρησιμοποιούνται διαγράμματα όπως το παραπάνω για την οπτικοποίηση των διαφορετικών χρηστών και την αλληλεπίδρασή τους με το σύστημα. Από τη λειτουργία των σελίδων δημιουργούνται οι σελίδες που εντάσσονται στο κύριο μενού αλλά και η αρχική σελίδα:



Εικόνα 16 Διαχειριστικό περιβάλλον WordPress, δημιουργία menu

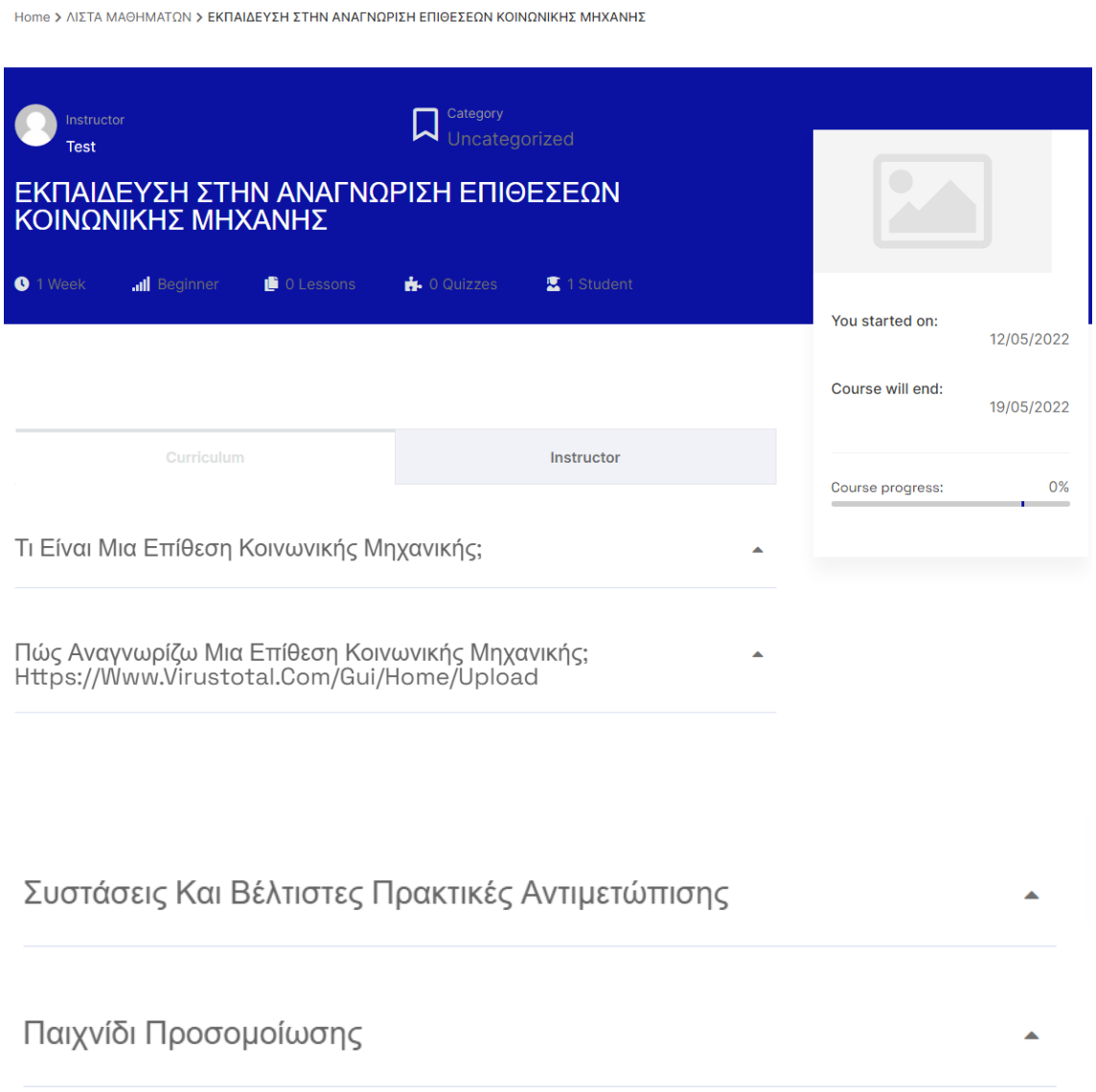


Εικόνα 17 Αρχική σελίδα προγράμματος ευαισθητοποίησης



Εικόνα 18 Το μενού όπως φαίνεται στην αρχική σελίδα.

Οι λειτουργίες του προσθέτου δίνουν τη δυνατότητα κατάταξης των χρηστών σε επίπεδα, δημιουργίας του υλικού των μαθημάτων αλλά και εξαγωγής δεδομένων αναφορικά με την χρήση και τα ποσοστά επιτυχίας των εκπαιδευομένων. Στοιχεία βοηθητικά για την αξιολόγηση και επικαιροποίηση του προγράμματος. Παρακάτω παρουσιάζεται ενδεικτικά η δημιουργία του μαθήματος για την ανίχνευση επιθέσεων κοινωνικής μηχανικής:

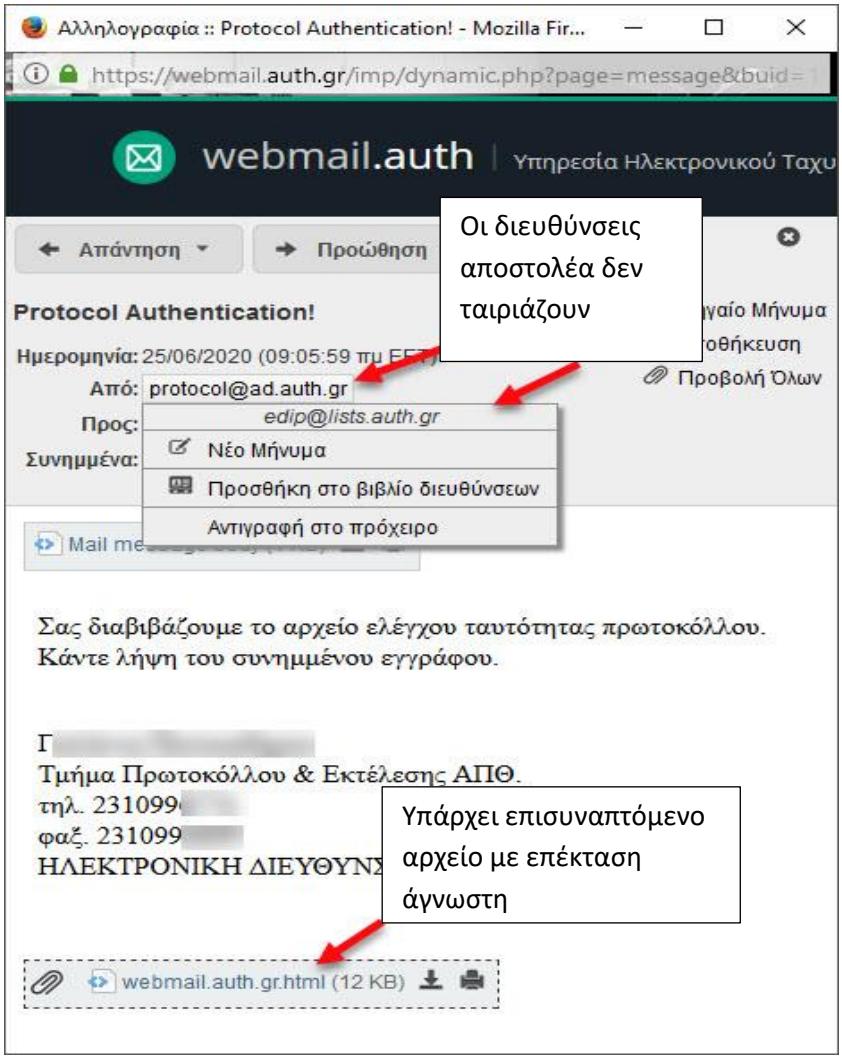


Εικόνα 19 Το μενού του μαθήματος "Εκπαίδευση στην αναγνώριση επιθέσεων κοινωνικής μηχανής"

Περιλαμβάνει τη διάρκεια του μαθήματος, το επίπεδο του χρήστη αλλά και τις τέσσερις βασικές ενότητες για εκπαίδευση διάρκειας μιας εβδομάδας. Ανάμεσα σε αυτά

προτείνεται η ιστοσελίδα https://www.virustotal.com/gui/home/upload για έλεγχο ύποπτων αρχείων και συνδέσμων αλλά και το παιχνίδι «CaPrice Game»[66]

Ενδεικτικά, η αναγνώριση ενός μηνύματος ηλεκτρονικής εξαπάτησης μπορεί να παρουσιαστεί με οπτικοποιημένα παραδείγματα όπως παρακάτω[67]:



Εικόνα 20 Παράδειγμα ύποπτου μηνύματος. Ίδια επεξεργασία από https://it.auth.gr/el/phishing-email

Ολοκληρώνοντας είναι σημαντικό να τονιστεί ότι απαραίτητη προϋπόθεση για την επιτυχία του προγράμματος είναι η τροφοδότηση με υλικό επικαιροποιημένο και αλληλεπιδραστικό, ώστε να δίνεται στον χρήστη η δυνατότητα εμπέδωσης χρήσης των κανόνων ασφαλείας στο σύνολο των κοινωνικών του αλληλεπιδράσεων, προκειμένου να δημιουργηθεί η ενσυνειδησία ασφάλειας.

[66] Το παιχνίδι δημιουργήθηκε από το Εργαστήριο Πληροφοριακών Συστημάτων του Ινστιτούτου Πληροφορικής του Ιδρύματος Τεχνολογίας και Έρευνας https://www.caprice-community.net/game/

[67] (ΑΠΘ)

ΙΙΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

Μελετώντας το ζήτημα της κυβερνοασφάλειας για τους δημόσιους οργανισμούς παρατηρήθηκε ότι πρόκειται για ένα ζήτημα ιδιαίτερα πολύπλοκο και πολυσύνθετο, εξαρτώμενο από ποικίλους εξωτερικούς αλλά και εσωτερικούς παράγοντες. Ο προσδιορισμός του εξωτερικού πλαισίου λαμβάνει υπόψη το νομοθετικό πλαίσιο, υπερεθνικό αλλά και εθνικό, τη δυναμικότητα των τεχνολογικών εξελίξεων, αλλά και την συνεχή εξέλιξη των μέσων και τεχνικών επίθεσης. Παράλληλα, σχετίζεται με παράγοντες οικονομικούς, γεωπολιτικούς και κοινωνικούς αλλά και με το επίπεδο της ψηφιακής ωριμότητας της κοινωνίας και του κράτους. Ταυτόχρονα, η επιρροή από τις εκάστοτε εξωτερικές συνθήκες, όπως για παράδειγμα η πανδημία αλλά και ο πόλεμος, αποτελεί μια παράμετρο που φαίνεται να απαιτεί την συνεχή επικαιροποίηση και τον συνεχή επαναπροσδιορισμό των στρατηγικών σε υψηλό επίπεδο πολιτικής.

Στοιχείο ,εκ των ων ουκ άνευ, στον προσδιορισμό των παραγόντων είναι τα οργανωτικά και λειτουργικά χαρακτηριστικά της διοίκησης που επηρεάζουν τα χαρακτηριστικά των πολιτικών ασφαλείας των οργανισμών. Εστιάζοντας στο εσωτερικό των οργανισμών διαπιστώνεται η προσαρμογή του Σχεδίου Ασφαλείας στις επιχειρησιακές ανάγκες και η συσχέτιση του με την κουλτούρα ασφαλείας, που επικρατεί στον οργανισμό, καθώς θεωρείται όχι μόνο ένα μέσο προστασίας από τους κινδύνους αλλά ένας μηχανισμός διάχυσης της γνώσης και αλλαγής της κουλτούρας κυβερνοασφάλειας.

Η δομική διαπίστωση της ανάγκης για ενίσχυση της επίγνωσης ασφαλείας, συναρτάται με την εξίσου σημαντική ανάγκη για ενίσχυση της ευαισθητοποίησης του συνόλου των πολιτών και σχετίζεται άμεσα με το ρόλο της ανώτερης γραφειοκρατίας αλλά και με την δυναμική ένταξη των δικτύων γνώσης και των επιστημικών κοινοτήτων στην ανάπτυξη της δημόσιας πολιτικής ασφαλείας. Μια ακόμα σημαντική διαπίστωση αποτελεί η ανάγκη για ενίσχυση της εκπαίδευσης ασφαλείας, της περαιτέρω κατάρτισης στον τομέα αυτό και της παραγωγής εξειδικευμένων στελεχών Πληροφορικής, έχοντας πάντα υπόψη τη γεφύρωση του ψηφιακού χάσματος και την ένταξη των «μη ειδικών» στην κουλτούρα της ασφαλείας.

Καθώς η έννοια του πληροφοριακού συστήματος αναφέρεται σε υπολογιστικούς και ανθρώπινους πόρους, συμπεραίνεται ότι η λήψη τεχνικών μέτρων είναι εξίσου σημαντική με την εκπαίδευση του προσωπικού σε ζητήματα κυβερνοασφάλειας, λόγω και του σημαντικού ρόλου του ανθρώπινου παράγοντα για την κυβερνοανθεκτικότητα. Η επίγνωση ασφαλείας προσδίδει προστιθέμενη αξία στην τεχνική θωράκιση των

συστημάτων, την ίδια στιγμή που ενδυναμώνει τη δυνατότητα προσδιορισμού της ατομικής ψηφιακής ταυτότητας και της αυτονομίας στον ψηφιακό κόσμο, προσφέροντας τη γνώση και την ευαισθητοποίηση για τον έλεγχο των δεδομένων, της διακίνησης της υπηρεσιακής πληροφορίας και της ιδιωτικότητας. Ως εκ τούτου, αποτελεί μέρος της γενικότερης ενίσχυσης των ψηφιακών δεξιοτήτων του ανθρωπίνου δυναμικού της Δημόσιας Διοίκησης, συνιστώντας, εν ολίγοις, μέρος της διαδικασίας του επαναπροσανατολισμού των δεξιοτήτων των υπαλλήλων και της δημιουργίας της διοίκησης της γνώσης, την εποχή της ψηφιακής μετάβασης.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

ΑΡΘΡΑ-ΕΚΘΕΣΕΙΣ-ΒΙΒΛΙΑ

Coveware. (2021, Ιούλιος 23). *Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority*. Ανάκτηση Απρίλιος 16, 2022, από https://www.coveware.com/:%20https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority

Dr Amy Ross Arguedas, D. C. (2022, January 19). *Echo chambers, filter bubbles, and polarisation: a literature review*. Ανάκτηση Απρίλιος 29, 2022, από https://reutersinstitute.politics.ox.ac.uk/echo-chambers-filter-bubbles-and-polarisation-literature-review

ENISA. (2017). *Cyber Security Culture in organisations.* European Union Agency for Network and Information Security Science and Technology Park of Crete (ITE).

ENISA. (2018-2021). *Threat landscape.* ENISA.

ENISA. (2021). *ENISA Threat Landscape2021 April 2020 to mid-July 2021 DOI: 10.2824/324797* . ENISA.

European Parliament, . (2015). *Cybersecurity in the European Union and beyond: Exporing the Threats and Policy Responses.* Directorate-General for Internal Policies Policy Department, Publication Office.

Fintech. (2020, February 16). *The 2020 Cybersecurity stats you need to know*. Ανάκτηση Απρίλιος 7, 2022, από https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/

Hadlington, L. (2017, July 1). *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours.* Ανάκτηση Μαϊος 2, 2022, από https://www.cell.com/heliyon/fulltext/S2405-8440(17)30998-2?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2405844017309982%3Fshowall%3Dtrue

IBM. (2019, April). *IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them* . Ανάκτηση Απρίλιος 19, 2022, από https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

INFOCOM. (2021, Οκτώβριος 10). *The State of Cyber Security 2021 by Pylones Hellas: μεγάλη πανελλαδική έρευνα για την κυβερνοασφάλεια και το remote working*. Ανάκτηση Απρίλιος 27, 2022, από https://www.infocom.gr/2021/10/20/the-state-cyber-security-2021-pylones-hellas-megali-panelladiki-erevna-gia-tin-kyvernoasfaleia-kai-remote-working/56369/

ISO/IEC. (2022). *ISO/IEC 27002:2022(en) Information Security, cybersecurity and privacy protection — Information security controls*. Ανάκτηση Απρίλιος 18, 2022, από ISO Online Browsing Platform (OBP): https://www.iso.org/obp/ui#iso:std:iso-iec:27002:ed-3:v2:en:term:3.1.34

ITRC, Identity Theft Resource Center. (2022). *Data Breach Annual Report 2021 in Review*. ITRC.

ITU. (2022). *ITU-T Recommendation series structure*. Ανάκτηση Απρίλιος 27, 2022, από https://www.itu.int/en/ITU-T/publications/Pages/structure.aspx

NIST. (2020, February). *Computer Security Resource Center Glossary*. Ανάκτηση Απρίλιος 18, 2022, από https://csrc.nist.gov/glossary/term/cyber_resiliency

NIST National Institute Of Standards and Technology: NIST. (2021, 6 August). *Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide*. Ανάκτηση Απρίλιος 17, 2022, από https://www.nist.gov/publications/getting-started-nist-cybersecurity-framework-quick-start-guide

NIST. (n.d.). *CYBERSECURITY AND PRIVACY APPLICATIONS*. Ανάκτηση Απρίλιος 17, 2022, από https://www.nist.gov/itl/applied-cybersecurity/cybersecurity-and-privacy-applications

Osterman Research. (2020). *White Paper The Truth About Cybersecurity Training.*

PwC Research . (2021). Global Digital trust Insights Survey 2021 https://www.pwc.com/kz/en/services/global-digital-trust-insights.html#modules.%20UK:%20PWC.

Symmetry Systems και η Osterman Research. (2021). *https://www.symmetry-systems.com/why-zero-trust-is-important*.

The Hague Centre for Strategic Studies, C. K. (2018). *Cybersecurity Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks.* Βρυξέλλες: European Economic and Social Committee, European Union, doi:10.2864/98090.

Tucker Bailey, B. K. (2018, September). *Insider threat: The human element of cyberrisk.* Ανάκτηση Απρίλιος 19, 2022, από https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/insider-threat-the-human-element-of-cyberrisk

Verizon. (2020). *Data Breach Investigations Report.* Verizon.

WHO. (2020, September 23). *Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation.* Ανάκτηση 14 Μαϊος, 2022, από https://www.who.int/news/item/23-09-2020-managing-the-COVID-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation

William, S. (2017). *Network Security Essentials, 6th Edition.* Pearson.

Βαγδατζόγλου, Β. (2018). *Οργανωσιακή κουλτούρα και διαμοίραση της γνώσης στον δημόσιο τομέα:κρίσιμοι παράγοντες επιτυχίας.* Ανάκτηση Απρίλιος 18, 2022, από ΨΗΦΙΔΑ Ιδρυματικό Αποθετήριο/Institutional Repository: https://dspace.lib.uom.gr/handle/2159/21810

Εθνική Αρχή Κυβερνοασφάλειας. (2021, Ιούνιος). *Κυβερνοασφάλεια.* Ανάκτηση Απρίλιος 2, 2022, από https://mindigital.gr/wp-content/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf

Εθνική Αρχή κυβερνοασφάλειας. (2022, Φεβρουάριος). *Οδηγός Αυτοαξιολόγησης – εργαλείο αυτοαξιολόγησης της κυβερνοασφάλειας (cybersecurity self-assessment tool).* Ανάκτηση Απρίλιος 2, 2022, από https://mindigital.gr/kyvernoasfaleia

Ευρωπαϊκή Επιτροπή, Ύ. Ε. (2017). *Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, JOIN(2017) 450 final.* Βρυξέλλες: Ευρωπαϊκή Επιτροπή.

Ιωάννης, Μ. (2015). *Ασφάλεια πληροφοριών στο διαδίκτυο.* Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις https://repository.kallipos.gr/handle/11419/1024

Μπουραντάς Δημήτρης, Π. Ν. (2016). *Διοίκηση Ανθρώπινου Δυναμικού.* Αθήνα: Ε. Μπένου.

Συνέδριο, Ε. Ε. (2019). *Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια.* Λουξεμβούργο: Ευρωπαϊκή Ένωση.

ΝΟΜΟΛΟΓΙΑ

ΝΟΜΟΣ ΥΠ ΑΡΙΘΜ. 4727 (Α΄184/23.9.2020) Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4624 (Α΄ 137/29.08.2019) Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4635 (Α΄ 167/30.10.2019) «Επενδύω στην Ελλάδα και άλλες Διατάξεις»

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4627 (Α΄ 143/25.09.2019) «Κύρωση της Συμφωνίας έδρας μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και του Ευρωπαϊκού Οργανισμού Ασφάλειας Δικτύων και Πληροφοριών (ENISA), - Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας» (ΦΕΚ 143/Α/25-9-2019)

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4619 (Α΄ 95/11.06.2019) Κύρωση του Ποινικού Κώδικα

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4577 (Α΄ 199/03.12.2018) Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις.

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4411 (Α΄142/03.08.2016) Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών. Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις.

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ' ΑΡΙΘΜ. 96 (Α΄ 232/20.11.2020) Τροποποίηση και συμπλήρωση διατάξεων του π.δ. 1/2017 «Οργανισμός της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.)»

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ’ ΑΡΙΘΜ. 84 (Α΄ 123/17.07.2019) Σύσταση και κατάργηση Γενικών Γραμματειών και Ειδικών Γραμματειών/Ενιαίων Διοικητικών Τομέων Υπουργείων.

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ’ ΑΡΙΘΜ. 81 (Α΄ 119/08.07.2019) Σύσταση, συγχώνευση, μετονομασία και κατάργηση Υπουργείων και καθορισμός των αρμοδιοτήτων τους. Μεταφορά υπηρεσιών και αρμοδιοτήτων μεταξύ Υπουργείων.

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ’ ΑΡΙΘΜ. 178 (Α΄281/31.12.2014) Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας.

Υπουργική Απόφαση «Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025» (ΑΔΑ:6ΙΒΕ46ΜΤΛΠ-ΦΜ5)

Υπουργική Απόφαση «Κύρωση του Εθνικού Κανονισμού Ασφαλείας (ΕΚΑ)» (ΦΕΚ 683/Β/27-2-2018)

Υπουργική Απόφαση 1027/8.10.2019 "Θέματα εφαρμογής και διαδικασιών του ν. 4577/ 2018 (Α΄ 199) " (ΦΕΚ 3739/Β/8-10-2019)

Budapest Convention (CETS 185, 23.11.2001, Council of Europe, 2009)

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2019/881 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Απριλίου 2019 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

ΟΔΗΓΙΑ 2018/1972/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 11ης Δεκεμβρίου 2018 για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών

ΟΔΗΓΙΑ 2016/1148/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

ΟΔΗΓΊΑ 2013/40/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων

πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου

ΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ

https://imf-conference.org/imf2018/cfp.html
https://www.ssi.gouv.fr/
https://el.wordpress.org/
https://it.auth.gr/el/phishing-email
https://www.apachefriends.org/download.html
https://nationaldigitalacademy.gov.gr/
https://saferinternet4kids.gr/poioieimaste/
https://greece20.gov.gr/
https://www.gov.gr/updates/services/meso-gov-gr-oi-kataggelies-ste-dioxe-elektronikou-egklematos
https://www.ncsc.gov.uk/
https://creately.com/blog/
https://www.canva.com/el_gr/
https://www.virustotal.com/gui/home/upload
https://www.caprice-community.net/game/
https://scrumguides.org/download.html
https://www.ibm.com/skills/topics/cybersecurity/
https://analysis.digigov.grnet.gr/docs/agile
https://www.informatique-mania.com/el/applications/decouvrez-ces-jeux-open-source-qui-copient-et-ameliorent-les-originaux/
https://attack.mitre.org/
https://ellak.gr/2015/09/ti-ine-to-logismiko-aniktou-kodika-mia-isagogi/
https://www.gsis.gr/dimosia-dioikisi/ked/webservices
https://www.greek-language.gr/greekLang/index.html

https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government
https://joinup.ec.europa.eu/collection/interoperable-europe/news/first-report-berlin-declaration-out

https://www.kathimerini.gr/society/561857965/psifiakes-apates-ta-dolomata-kai-oi-pagides/

ΠΑΡΑΡΤΗΜΑ 1 Ερωτηματολόγιο Αξιολόγησης

Επίγνωση Ασφαλείας

Απαντήστε τσεκάροντας στον αντίστοιχο κύκλο. Υπάρχει η δυνατότητα πολλαπλών απαντήσεων

1. Πόσες "καρτέλες" ανοίγετε συνήθως: *

- Μόνο μια
- Μερικές
- Συνήθως χάνω το μέτρημα
- Τι είναι καρτέλα;

2. Κατά την περιήγηση σας στο Διαδίκτυο, επιλέγετε ιστοτόπους που: *

- Εχουν το στοιχείο htpps στην γραμμή διευθύνσεων
- Εχουν το στοιχείο htpp στην γραμμή διευθύνσεων
- Εχουν ενδιαφέρουσες πληροφορίες
- Εχουν htpps και SSL πιστοποιητικό

3. Τι μοιράζεστε στο Διαδίκτυο; *

- Σχεδόν τα πάντα: φωτογραφίες, profile updates,live stories
- Τίποτα
- Ενδιαφέροντα άρθρα και πληροφορίες
- Σημαντικά Updates

4. Ενημερώσεις έτοιμες προς εγκατάσταση *

- Υπενθύμιση αργότερα
- Να μην ξαναγίνει υπενθύμιση
- Τελειώνω τη δουλειά μου και τις εγκαθιστώ
- Τις εγκαθιστώ άμεσα

5. Χρησιμοποιείτε κάποιο back up για τον υπολογιστή σας: *

- Το cloud
- Δεν χρειάζομαι κάτι τέτοιο
- Χρησιμοποιώ εξωτερικό μέσο αποθήκευσης
- Τι είναι το back up;

6. Πόσα άτομα γνωρίζουν τους κωδικούς σας: *

- Το πιο αγαπημένο μου πρόσωπο
- Ο λογιστής μου/κάποιοι συνάδελφοι
- Κανείς
- Το σύστημα διαχείρισης κωδικών του Υπολογιστή μου

7 Πώς ξεκλειδώνει το τηλέφωνο/ο Υπολογιστής σας:

- Με PIN
- Με δακτυλικό αποτύπωμα ή αναγνώριση προσώπου
- Είναι πάντα ξεκλείδωτο

8 Η επαναχρησιμοποίηση των κωδικών είναι: *

- Μια βοηθητική πρακτική
- Μια καθόλου ορθή πρακτική

9 Πρέπει να συνδεθείτε σε κάποια εφαρμογή ή πρόγραμμα τι από τα παρακάτω κάνετε; *

- Χρησιμοποιώ τον κωδικό και όνομα χρήστη που έχω για όλες τις εφαρμογές
- Χρησιμοποιώ τυχαία στοιχεία (αριθμούς, σύμβολα και γράμματα) κάθε φορά διαφορετικά
- Επιλέγω ανάμεσα σε 2 ή 3 κωδικούς και ονόματα που χρησιμοποιώ συνήθως

10 Κάθε πότε αλλάζετε τους κωδικούς σας; *

- Κάθε έξι μήνες
- Σχεδόν ποτέ
- Αλλάζω μόνο τον κωδικό της τράπεζας, για τους άλλους δεν υπάρχει πρόβλημα

11 Οι κωδικοί μου *

- Βρίσκονται όλοι στο μυαλό μου
- Είναι σε χαρτάκι στο πορτοφόλι/στο συρτάρι του γραφείου/κολλημένο στην οθόνη
- Υπάρχουν στο πρόγραμμα διαχείρισης κωδικών που χρησιμοποιώ

12 Χρησιμοποιείτε προφύλαξη οθόνης στον Υπολογιστή του γραφείου σας: *

- Ναι ώστε να κλειδώνει ο Υπολογιστής μου μετά από 10 λεπτά ανενεργός
- Όχι, δεν χρειάζεται κάτι τέτοιο
- Δεν γνωρίζω τι είναι η προφύλαξη οθόνης

13 Πόσες εφαρμογές και προγράμματα βρίσκονται στον υπολογιστή σας ή στο κινητό σας χωρίς να τα έχετε χρησιμοποιήσει εδώ και καιρό: *

- Κανένα, εφαρμόζω συχνά ελέγχους με την βοήθεια των αντίστοιχων εργαλείων.
- Δεν ξέρω
- Αμέτρητα

14 Το phising είναι μια τεχνική ηλεκτρονικής εξαπάτησης που μας οδηγεί στο να μοιραστούμε προσωπικές πληροφορίες ή να κατεβάσουμε κάποιο κακόβουλο λογισμικό "ιό".

- Σωστό
- Λάθος

15 Γνωρίζω τι είναι το smising;

- Ναι
- Όχι
- Δεν είμαι απόλυτα σίγουρος

16 Γνωρίζω τι είναι το maldvertising:

- Ναι
- Όχι
- Δεν είμαι απόλυτα σίγουρος

17 Γνωρίζω τι είναι το ransomware:

- Ναι
- Όχι
- Δεν είμαι απόλυτα σίγουρος

18 Συνδέεστε από το δίκτυο του Οργανισμού

- Για να περιηγηθείτε στο Διαδίκτυο και στα μέσα κοινωνικής δικτύωσης
- Για να "κατεβάσετε" ταινίες ή μουσική
- Για λόγους που αφορούν στην εργασία σας
- Για όλα τα παραπάνω

19 Λαμβάνετε ένα "ύποπτο" μήνυμα στο υπηρεσιακό mail. Τι κάνετε;

- Το διαγράφετε
- Ενημερώνετε τον υπεύθυνο ασφαλείας του οργανισμού
- Δεν γνωρίζετε τι πρέπει να κάνετε
- Το ανοίγετε...δεν φαίνεται και τόσο ύποπτο

20 Γνωρίζετε και εφαρμόζετε την κρυπτογράφηση των υπηρεσιακών αρχείων και δεδομένων

- Γνωρίζω αλλά δεν εφαρμόζω
- Γνωρίζω και εφαρμόζω
- Ούτε γνωρίζω ούτε εφαρμόζω
- Δε γνωρίζω και δεν ενδιαφέρομαι να μάθω

21 Τι από τα παρακάτω εντάσσεται στην ειδική κατηγορία προσωπικών δεδομένων;

- Ο ΑΦΜ
- Τα ιατρικά αρχεία
- Τα γενετικά δεδομένα
- Ο ΑΜΚΑ

22 Για να περιηγηθείτε σε μια ιστοσελίδα

- Συναινείτε στη χρήση Cookies/χρήσης της τοποθεσίας μου/αποστολής ειδοποιήσεων
- Δε συναινείτε σε κάτι από τα παραπάνω
- Συναινείτε σε κάποια από τα παραπάνω
- Χρησιμοποιείτε παράθυρο ανώνυμης περιήγησης

Εικόνα 21Ερωτηματολόγιο αξιολόγησης

ΠΑΡΑΡΤΗΜΑ 2 Ορολογία

Αλγόριθμοι κρυπτογράφησης	Μέθοδοι κρυπτογράφησης των δεδομένων και των αρχείων.
Ανεπιθύμητη αλληλογραφία, spam	Αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικής αλληλογραφίας σε χρήστες.
Ανοικτού κώδικα λογισμικό	Λογισμικό του οποίου ο πηγαίος κώδικας είναι διαθέσιμος για τροποποίηση ή αναβάθμιση μέσω μιας ελεύθερης άδειας χρήσης.
Αντιϊκό πρόγραμμα, anti-virus software	Λογισμικό προστασίας από ιούς.
Αυθεντικοποίηση πολλών παραγόντων	Μέτρο ασφαλείας που στοχεύει στην προσθήκη επιπλέον επιπέδων προστασίας, πέρα από το όνομα χρήστη και τον κωδικό (αριθμός τηλεφώνου ή βιομετρικά χαρακτηριστικά).
Δημόσιος Τομέας	«Περιλαμβάνει τη Γενική Κυβέρνηση, τα εκτός αυτής νομικά πρόσωπα δημοσίου δικαίου (ΝΠΔΔ), καθώς και τις εκτός αυτής δημόσιες επιχειρήσεις και οργανισμούς Η Γενική Κυβέρνηση περιλαμβάνει τρία υποσύνολα: της Κεντρικής Κυβέρνησης, των Οργανισμών Τοπικής Αυτοδιοίκησης (ΟΤΑ) και των Οργανισμών Κοινωνικής Ασφάλισης (ΟΚΑ). Οι φορείς εκτός Κεντρικής Διοίκησης, που περιλαμβάνονται στους υποτομείς της Γενικής Κυβέρνησης προσδιορίζονται, ανά υποτομέα, από το Μητρώο Φορέων Γενικής Κυβέρνησης, αποτελούν ξεχωριστά νομικά πρόσωπα που εποπτεύονται από φορείς της Κεντρικής Διοίκησης ή από ΟΤΑ». Νόμος υπ΄αριθμ.4270 ΦΕΚ Α΄143/28.6.2014
Διαδικτυακή υπηρεσία,Web Service	Υπηρεσία που παρέχεται μέσω διαδικτύου για τη λειτουργία άλλης υπηρεσίας/προγράμματος.
Διαλειτουργικότητα	«Ικανότητα ανόμοιων και διαφορετικών οργανισμών να αλληλεπιδρούν προς την κατεύθυνση της επίτευξης αμοιβαίως ωφέλιμων και συμφωνημένων κοινών στόχων, οι οποίοι αφορούν την ανταλλαγή πληροφοριών και γνώσεων μεταξύ των εν λόγω οργανισμών διά μέσου των εργασιακών διαδικασιών που υποστηρίζουν, μέσω της ανταλλαγής δεδομένων μεταξύ των αντίστοιχων συστημάτων τους ΤΠΕ».
Δούρειος Ίππος, trojan horse	Κακόβουλο λογισμικό που περιέχει πρόσθετη και μη αναμενόμενη λειτουργικότητα, άγνωστη στον χρήστη.
Εξαντλητική αναζήτηση κωδικού, brute force attack	Ο επιτιθέμενος δοκιμάζει πιθανούς συνδυασμούς κωδικών μέχρι να αποκτήσει πρόσβαση στο σύστημα.
Εσωτερική απειλή, insider threat	Απειλή που προέρχεται από νυν και πρώην στελέχη φορέων αλλά και από εξωτερικούς συνεργάτες, κατεχόντων εσωτερικής πληροφόρησης.
Ιός, virus	Κακόβουλο λογισμικό που ενσωματώνει τον κώδικά του σε ένα πρόγραμμα και αναπαράγεται με την αντιγραφή του σε άλλα προγράμματα.
Κερκόπορτες,backdoors	Κακόβουλο λογισμικό που δημιουργεί σημεία εισόδου ώστε να επιτευχθεί μη εξουσιοδοτημένη πρόσβαση.

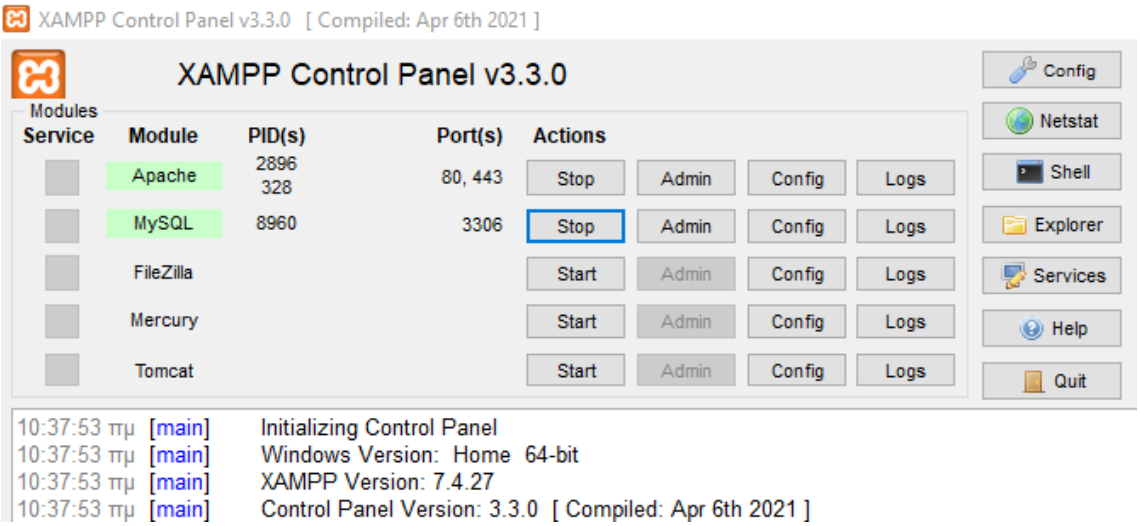
Κυβερνοέγκλημα, cybercrime	• αδικήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των υπολογιστικών δεδομένων και συστημάτων • αδικήματα σχετιζόμενα με τους υπολογιστές • αδικήματα σχετιζόμενα με το περιεχόμενο • αδικήματα αναφερόμενα σε παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας.
Κυβερνοχώρος	Ένας εικονικός, πλασματικός χώρος που δημιουργείται με τη χρήση ηλεκτρονικού υπολογιστή και συνήθως σε σύνδεση με το διαδίκτυο.
Μεταμφίεση	Αλλαγή IP ή MAC διεύθυνσης.
Παραβίαση δεδομένων, data breach	Μη εξουσιοδοτημένος χρήστης αποκτά πρόσβαση στα δεδομένα. Περιλαμβάνει την αποκάλυψη, τη διαρροή, την κλοπή δεδομένων και πληροφοριών.
Προσβασιμότητα	Σχεδιασμός υπηρεσιών ώστε να μπορούν να χρησιμοποιηθούν από ΑμΕΑ.
Υλισμικό	Το υλικό μέρος του υπολογιστή.

5G, δίκτυο	Ασύρματο δίκτυο βελτιωμένης τεχνολογίας.
Bandwidth,εύρος ζώνης	Χωρητικότητα δικτύου/σύνδεσης για μεταφορά δεδομένων.
Business e mail compromise, BEC	Μέθοδος εξαπάτησης μέσω εταιρικού ηλεκτρονικού ταχυδρομείου. Οι δράστες αποκτούν μη εξουσιοδοτημένη πρόσβαση και παρεμβαίνουν σε εταιρικές ηλεκτρονικές συναλλαγές.
Botnet, προελ. "robot"-"network"	«Δίκτυο προγραμμάτων ρομπότ», αριθμός συνδεδεμένων στο διαδίκτυο συσκευών που τρέχουν αυτοματοποιημένα σενάρια προσομοίωσης της ανθρώπινης δραστηριότητας με στόχο την κακόβουλη δραστηριότητα.
Credential stuffing	Μέθοδος κυβερνοεπίθεσης με συλλογή διαπιστευτηρίων για απόκτηση πρόσβασης στο σύστημα.
Cryptojacking, κρυπτοπειρατεία	Χρήση της υπολογιστικής ισχύος για άντληση κρυπτονομισμάτων.
Cyber Kill Chain	Η αλυσίδα ενεργειών των εισβολών.
Distributed Denial Of Service (DDOS), επίθεση κατανεμημένης άρνησης υπηρεσίας	Επίθεση όγκου διαδικτυακής κίνησης με στόχο την διαθεσιμότητα.
Drive by download	Μη ηθελημένη μεταφόρτωση κακόβουλου λογισμικού στο πληροφοριακό σύστημα από κακόβουλο σύνδεσμο/επισυναπτόμενο αρχείο.
Identity theft, κλοπή ταυτότητας	Κλοπή και χρήση στοιχείων ταυτότητας για διάπραξη κυβερνοεγκλήματος.
Malware, ιομορφικό ή κακόβουλο λογισμικό	Λογισμικό σχεδιασμένο για πρόκληση ζημίας στο πληροφοριακό σύστημα.
Malvertising	Η χρήση της διαδικτυακής διαφήμισης για την εξάπλωση κακόβουλου λογισμικού.
Phishing, ηλεκτρονικό ψάρεμα/εξαπάτηση	Μηνύματα ηλεκτρονικού ταχυδρομείου με σκοπό την εξαπάτηση για την υποκλοπή δεδομένων ή την επίθεση με κακόβουλο λογισμικό.
Plugins	Πρόσθετα στοιχεία ενίσχυσης των λειτουργιών του WordPress.
Ransomware, λυτρισμικό	Κακόβουλο λογισμικό που κρυπτογραφεί τα δεδομένα του συστήματος και απαιτεί λύτρα.
Scrum	Διεργασία της ευέλικτης ανάπτυξης έργου πληροφορικής, αποτελεί δάνειο από το rugby, ώστε να δοθεί έμφαση στην ομαδική εργασία.
Smising	Επίθεση ηλεκτρονικού ψαρέματος μέσω SMS.
Social bots	Η τεχνητή νοημοσύνη χρησιμοποιείται για την δημιουργία ψευδών προφίλ και τη διασπορά ψευδών ειδήσεων.
Spear phishing	Επίθεση ηλεκτρονικού ψαρέματος στοχευμένη σε συγκεκριμένους οργανισμούς.
Trending lists, «λίστα τάσεων»	Κορυφαίες/δημοφιλείς αναζητήσεις που εμφανίζονται στα μέσα κοινωνικής δικτύωσης ως προτεινόμενες βάσει αλγορίθμων.
Use case diagram, διάγραμμα περίπτωσης χρήσης	Διάγραμμα στην ανάπτυξη λογισμικού που περιλαμβάνει το σενάριο χρήσης του συστήματος
Web based threats	Ομάδα απειλών που προέρχονται από το διαδίκτυο.
Whaling	Επίθεση ηλεκτρονικού ψαρέματος που στοχεύει σε ανώτερα στελέχη των οργανισμών
Zero trust architecture, Αρχιτεκτονική μηδενικής Εμπιστοσύνης	Μοντέλο ασφαλείας πληροφοριακών συστημάτων

Εικόνα 22 Ορολογία, ίδια επεξεργασία

ΠΑΡΑΡΤΗΜΑ3 Εγκατάσταση WordPress

Η εγκατάσταση πραγματοποιήθηκε τοπικά μέσω της πλατφόρμας XAMPP η οποία περιέχει τον εξυπηρετητή διαδικτύου Apache και τη βάση δεδομένων MySQL.



Εικόνα 23 Η πλατφόρμα XAMPP

Στη συνέχεια έγινε λήψη των αρχείων του WordPress και αποσυμπίεση σε τοπικό φάκελο. Περαιτέρω ακολουθώντας τον οδηγό του WordPress δημιουργήθηκε ο ιστότοπος.

Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης (Ε.Σ.Δ.Δ.Α.)
Πειραιώς 211, ΤΚ 177 78, Ταύρος
τηλ: 2131306349 , fax: 2131306479