ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων

«ΚΟΥΛΤΟΥΡΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ»

Η Διπλωματική Εργασία
παρουσιάστηκε ενώπιον του
Διδακτικού Προσωπικού του
Πανεπιστημίου Αιγαίου

Σε Μερική Εκπλήρωση των Απαιτήσεων για το Δίπλωμα
του Μεταπτυχιακού Προγράμματος Σπουδών
Πληροφοριακά και Επικοινωνιακά Συστήματα του
Τμήματος Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

Της:

Μαρίνας – Μαρία Ζηλωτή

ΣΕΠΤΕΜΒΡΙΟΣ 2018

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ ΕΠΙΚΥΡΩΝΕΙ ΤΗ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΤΗΣ:

Μαρίνας – Μαρίας Ζηλωτή – ΑΜ:2016072

X

(Ονοματεπώνυμο 1)
(Ιδιότητα 1)

X

(Ονοματεπώνυμο 2)
(Ιδιότητα 2)

X

(Ονοματεπώνυμο 3)
(Ιδιότητα 3)

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΣΕΠΤΕΜΒΡΙΟΣ 2018

Περίληψη

Στη σύγχρονη εποχή εξαπλώνεται όλο και περισσότερο η χρήση των πληροφοριακών συστημάτων στις λειτουργίες της δημόσιας διοίκησης των ανεπτυγμένων κρατών. Εάν λάβουμε υπόψη τη σημασία των δεδομένων που διαχειρίζονται οι συγκεκριμένες λειτουργίες μπορεί να γίνει εύκολα κατανοητή η σημασία που έχει η ασφάλεια τους. Για την επίτευξη ενός υψηλού επιπέδου ασφαλείας είναι ιδιαιτέρως σημαντική και η στάση των χρηστών, καθώς και η σημασία που αποδίδουν σε αυτόν τον παράγοντα. Με άλλα λόγια, θα μπορούσαμε να κάνουμε λόγο για την ανάπτυξη μίας κουλτούρας ασφαλείας, δηλαδή της υιοθέτησης από τους χρήστες των υπηρεσιών της ηλεκτρονικής διακυβέρνησης ορισμένων στάσεων και συμπεριφορών οι οποίες θα συνέβαλλαν στην αύξηση της ασφάλειας των πληροφοριών που διοχετεύονται και διακινούνται μέσα από τις συγκεκριμένες εφαρμογές.

Ορισμένες πτυχές της κουλτούρας ασφαλείας συνοψίζονται στη δυνατότητα του χρήστη να εντοπίζει δυνητικούς διαδικτυακούς κινδύνους, αλλά και στη γνώση των βέλτιστων πρακτικών αντίδρασης στην περίπτωση κατά την οποία πέσει θύμα διαδικτυακής απάτης. Ιδιαίτερη σημασία βέβαια έχει και η στάση του κράτους (στην εξεταζόμενη περίπτωση, όπου η κουλτούρα ασφαλείας μελετάται στα πλαίσια της σύνδεσης της με την ηλεκτρονική διακυβέρνηση). Ο ρόλος του κράτους σχετίζεται αφενός με το κατά πόσο ενσωματώνει πρακτικές ασφαλείας στις ηλεκτρονικές του εφαρμογές (ούτως ώστε να βελτιώνει τη γενικότερη ασφάλεια των υπηρεσιών του) και αφετέρου με το εαν έχει αναθέσει τη συγκεκριμένη λειτουργία σε κάποιο ανεξάρτητο τμήμα του κρατικού μηχανισμού, το οποίο έχει στη διάθεση του επαρκείς πόρους και προσωπικό και αντικείμενο του είναι η μελέτη και αναβάθμιση των σχετικών συστημάτων. Η ασφάλεια θεωρείται ένας από τους κρίσιμους παράγοντες για την επιτυχημένη υλοποίηση της ηλεκτρονικής διακυβέρνησης. Καθώς αυξάνεται ο αριθμός των σχετικών υπηρεσιών οι οποίες διατίθενται στον χρήστη, αυξάνονται και οι απαιτήσεις σχετικά με την ασφάλεια τους. Ο ανθρώπινος παράγοντας αποτελεί ακρογωνιαίο λίθο των σχετικών διαδικασιών. Συνεπώς για την επίτευξη ενός ικανοποιητικού βαθμού ασφαλείας είναι ιδιαιτέρως σημαντική τόσο η ανάπτυξη και υιοθέτηση αποτελεσματικών σχετικών πρακτικών όσο και η εμφύσηση μίας σχετικής παιδείας στους πολίτες.

Στην παρούσα εργασία αρχικά διεξάγεται μία βιβλιογραφική ανασκόπηση η οποία αποσκοπεί στην αποσαφήνιση των βέλτιστων πρακτικών που έχουν υιοθετηθεί από διάφορες χώρες προς την ανάπτυξη μίας κουλτούρας ασφαλείας, ενώ στη συνέχεια πραγματοποιούνται ορισμένες προτάσεις σχετικά με αντίστοιχες πρωτοβουλίες οι οποίες θα μπορούσαν να υλοποιηθούν στην Ελλάδα προς τη συγκεκριμένη κατεύθυνση. Τα κυριότερα συμπεράσματα συνοψίζονται στην αναγκαιότητα προστασίας των εφαρμογών της ηλεκτρονικής διακυβέρνησης, στη σημασία που έχει η ανάπτυξη μίας κουλτούρας ασφαλείας για τη δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος, στο έλλειμμα ικανοτήτων που παρατηρείται ανάμεσα στους Έλληνες πολίτες σχετικά με την υιοθέτηση των ενδεδειγμένων πρακτικών και συμπεριφορών ασφαλείας, καθώς και στην αναγκαιότητα υλοποίησης εκπαιδευτικών δράσεων, στοχευμένων τόσο προς τους πολίτες όσο και προς το προσωπικό των δημοσίων φορέων, ενισχυτικών δράσεων της κουλτούρας ασφαλείας από τους ελληνικούς δημόσιους οργανισμούς, αλλά και επικοινωνίας των δράσεων και μέτρων ασφαλείας που ακολουθούνται από αυτούς, ούτως ώστε να οικοδομηθεί η εμπιστοσύνη των πολιτών προς το κράτος.

Abstract

In modern times, the use of information systems to the functions of public administration in developed countries is getting rapidly increased. Taking into account the importance of the data manipulated by these functions, it is easy to understand the importance of the security aspect. In order to achieve a high level of security, the users' attitude as well as the importance they give to this factor are of significant importance. In other words, we could speak for the development of a security culture, namely the adoption by users of e-government services of certain attitudes and behaviors that would contribute to the increase of the security of information channeled and shared through related applications.

Some aspects of the security culture are summarized in the user's ability to detect potential online risks, as well as in the knowledge of best practices in managing a case of online fraud. Of particular importance is also the attitude of the state (in our case, where the security culture is studied in relation with e-government). The state's role is related to the extent to which it embeds security practices in its electronic applications (in order to improve the overall security of its services) and, on the other hand, whether it has assigned this function to an independent part of the state apparatus, with sufficient resources and personnel, which has the task of studying and upgrading relevant systems, as well as informing the public.

Security is considered as one of the critical factors for the successful implementation of e-government. As the number of related services increases, there also further security requirements. The human factor is a cornerstone in related processes. Therefore, in order to achieve a satisfactory degree of security, it is particularly important to develop and adopt effective practices and instill a relevant education for the citizens. In the present thesis, is initially carried out a literature review, which aims to clarify the best practices adopted by different countries towards the development of a security culture, and then makes some suggestions regarding the respective initiatives that could be implemented in Greece towards this direction. Our main conclusions can be summarized in the need for the security enhancement of e-government applications, the significance of security culture in fostering a secure cyber environment, the lack of skills among Greek citizens concerning the adoption of the recommended security practices, as well as the need for educational efforts, targeted towards both citizens and

employees of public organizations, enhancement actions for fostering security culture into Greek public services, as well as a communication of security policies and measures, in order to build trust between citizens and state.

Ευχαριστίες

Ευχαριστώ το Πανεπιστήμιο Αιγαίου και τους καθηγητές μου στο Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων για τις πολύτιμες γνώσεις και πληροφορίες καθώς και την κυρία Μαρία Καρύδα για τη στήριξη και την υποστήριξη που μου προσέφερε κατά τη συγγραφή της παρούσας εργασίας.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ.....3

ABSTRACT.....5

ΕΥΧΑΡΙΣΤΙΕΣ.....7

ΚΕΦΑΛΑΙΟ 1 ΕΙΣΑΓΩΓΗ.....10

1.1. Σκοπός της εργασίας.....11

1.2. Χρησιμότητα της εργασίας.....12

1.3. Δομή της εργασίας.....12

ΚΕΦΑΛΑΙΟ 2 Η ΣΗΜΑΣΙΑ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ.....14

2.1. Η έννοια της ηλεκτρονικής διακυβέρνησης.....14

2.2. Εμπόδια και Ευκαιρίες της Ηλεκτρονικής Διακυβέρνησης.....15

2.3. Προϋποθέσεις εφαρμογής της Ηλ. Διακυβέρνησης.....21

2.4. Θέματα ασφάλειας στην ηλεκτρονική διακυβέρνηση.....23

2.4.1. Απαιτήσεις ασφαλείας στην ηλ. Διακυβέρνηση.....23

2.4.2. Κρυπτογραφία και εφαρμογές.....27

2.4.3. Κρυπτογραφία στα πλαίσια της ηλ. Διακυβέρνησης....30

ΚΕΦΑΛΑΙΟ 3 ΚΟΥΛΤΟΥΡΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΗΛ. ΔΙΑΚΥΒΕΡΝΗΣΗ ΣΤΗΝ ΕΥΡΩΠΗ.....35

3.1. Κουλτούρα ασφαλείας οργανισμού.....35

3.2. Η σημασία του ανθρώπινου παράγοντα.....40

3.3. Δυσκολίες και προοπτικές της κουλτούρας ασφαλείας.....42

3.4. Πρακτικές ανάπτυξης κουλτούρας ασφαλείας.....44

3.5. Μελέτες περιπτώσεων ευρωπαϊκών κρατών.....48

3.5.1. Φινλανδία.....48

3.5.2. Γαλλία.....51

3.5.3. Ισπανία.....54

3.5.4. Νορβηγία.....57

ΚΕΦΑΛΑΙΟ 4 ΕΛΛΑΔΑ – ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΚΟΥΛΤΟΥΡΑΣ ΑΣΦΑΛΕΙΑΣ..63

4.1. Η ηλεκτρονική διακυβέρνηση στην Ελλάδα.....63

4.2. Η ελληνική εθνική στρατηγική κυβερνοασφάλειας.....66

4.3. Προφίλ ασφαλείας των Ελλήνων πολιτών.....69

4.4. Προτάσεις για την ενίσχυση της κουλτούρας ασφαλείας.....74

ΣΥΜΠΕΡΑΣΜΑΤΑ.....77
ΒΙΒΛΙΟΓΡΑΦΙΑ.....80

Κεφάλαιο 1

1. Εισαγωγή

Κατά την εποχή μας η κοινωνία διέρχεται από μία γενικότερη φάση ψηφιοποίησης κάθε πτυχής της. Η εξέλιξη αυτή επιβεβαιώνεται από την Παγκόσμια Αναφορά Τεχνολογιών Πληροφορικής του Παγκόσμιου Οικονομικού Φόρουμ για το 2016 (WEF, 2016), σύμφωνα με την οποία οι ψηφιακές τεχνολογίες πλέον έχουν εξελιχθεί σε έναν καθοριστικό παράγοντα για την καινοτομία και γενικότερα οποιαδήποτε πτυχή των σύγχρονων κοινωνιών. Ως εκ τούτου καθίσταται αναγκαία η λήψη κυβερνητικών πρωτοβουλιών σχετικά με την υιοθέτηση καινοτόμων ψηφιακών εφαρμογών στις κρατικές λειτουργίες, ούτως ώστε να υπάρχει σύγκλιση με τις εξελίξεις του κοινωνικού περιβάλλοντος, καθώς και η υιοθέτηση πολιτικών οι οποίες θα θωρακίσουν τις σχετικές εφαρμογές από τους κινδύνους που σχετίζονται με αυτές και θα συμβάλλουν στη βελτίωση της αποτελεσματικότητας τους. Δηλαδή, θα πρέπει να αυξηθεί ο βαθμός της προστασίας από το κυβερνοέγκλημα.

Η ηλεκτρονική διακυβέρνηση (δηλαδή η ψηφιοποίηση των δημοσίων λειτουργιών) θα μπορούσε να συμβάλλει σε μία σημαντική αύξηση της αποτελεσματικότητας τους, καθώς και σε βελτίωση της ικανοποίησης των πολιτών από τις παρεχόμενες υπηρεσίες. Τα οφέλη όμως μπορούν να περιοριστούν σε σημαντικό βαθμό από τους δυνητικούς κινδύνους που εγκυμονεί το διαδίκτυο. Ορισμένα από τα πλέον διαδεδομένα προβλήματα που σχετίζονται με την ασφάλεια μπορούν να συνοψιστούν σε απώλειες χρημάτων, ευαίσθητων δεδομένων, παραβίαση προσωπικών δεδομένων, καταστροφή εξοπλισμού, διακοπή των παρεχόμενων υπηρεσιών, κλπ. Συνεπώς πρέπει να δοθεί ιδιαίτερη σημασία στο κομμάτι της ασφάλειας ούτως ώστε οι σχετικές υπηρεσίες να παραμείνουν αποτελεσματικές (ειδικά εαν ληφθεί υπόψη η σημασία των δεδομένων που διακινούνται από αυτές).

Λόγω της αύξησης της εξάρτησης από τις τεχνολογίες δικτύων, η αποτελεσματική διαχείριση της ασφάλειας των πληροφοριών που διαχέονται μέσα από αυτά, έχει εξελιχθεί σε έναν από τους πλέον κρίσιμους παράγοντες για την επιτυχία των δημοσίων οργανισμών. Γενικότερα, λόγω της ταχείας ανάπτυξης της ηλεκτρονικής

διακυβέρνησης, είναι εξίσου σημαντική η ενίσχυση της επίγνωσης σχετικά με τη σημασία της ασφάλειας των σχετικών συναλλαγών καθώς και η λήψη ισχυρών προληπτικών μέτρων, τόσο από την πλευρά της υλοποίησης σχετικών τεχνολογιών όσο και από την πλευρά της διαχείρισης της ασφάλειας. Η σύνδεση που υπάρχει μεταξύ ζητημάτων ασφαλείας και ηλεκτρονικής διακυβέρνησης έχει καταδειχθεί από μία σειρά σχετικών μελετών (Siponen και Oinas-Kukkonen, 2007, Karyda, 2017, OECD, 2005, Malmedal και Røislien, 2016, Dhillon και Torkzadeh, 2006). Μάλιστα, εξετάζοντας τη σχετική βιβλιογραφία θα μπορούσαμε να συμπεράνουμε ότι τα μη τεχνικά ζητήματα (δηλαδή οι σχετικές στάσεις) είναι εξίσου σημαντικά για τη διαφύλαξη των ευαίσθητων πληροφοριών ενός οργανισμού.

1.1. Σκοπός της εργασίας

Η Ηλεκτρονική Διακυβέρνηση είναι άμεσα συνδεδεμένη με τη μεταρρύθμιση και τον εκσυγχρονισμό της Δημόσιας Διοίκησης μέσω της αξιοποίησης σύγχρονων τεχνολογιών και μεθοδολογιών. Για να καταστεί όμως δυνατή και επιτυχημένη μία τέτοια μετάβαση, δεν αρκεί η αυτοματοποίηση των υπαρχουσών διαδικασιών και η παροχή τους μέσω του διαδικτύου. Η Δημόσια Διοίκηση καλείται να εγκαθιδρύσει και να διατηρήσει καθολικά ένα επίπεδο προστασίας και ασφάλειας, όχι μόνο αντίστοιχο και ισότιμο με αυτό των υπαρχουσών υπηρεσιών, αλλά ικανό να διασφαλίσει ότι τα προσωπικά δεδομένα αξιοποιούνται με τρόπο διαφανή και σύννομο, λαμβάνοντας υπ' όψιν το συμφέρον των πολιτών. Η παρούσα εργασία έχει ως βασικό σκοπό να παρουσιάσει το θέμα της ανάπτυξης της κουλτούρας της ασφάλειας στους πολίτες, με σκοπό την επιτυχημένη εφαρμογή της ηλεκτρονικής διακυβέρνησης.

Ειδικότερα, η εργασία εστιάζει στο τρόπο με τον οποίο διάφορες χώρες εμφυσούν μία κουλτούρα ασφαλείας στους πολίτες τους στις διάφορες υπηρεσίες που παρέχονται στα πλαίσια της ηλεκτρονικής διακυβέρνησης. Μέσα από την μελέτη των πρακτικών και των δράσεων των χωρών, στην Ελλάδα, στην Ευρώπη και σε άλλες χώρες, θα εξαχθούν χρήσιμα συμπεράσματα σχετικά με την ανάπτυξη μίας κουλτούρας ασφαλείας στους πολίτες ούτως ώστε να χρησιμοποιούν σωστά τις

υπηρεσίες ηλεκτρονικής διακυβέρνησης. Επίσης, θα πραγματοποιηθούν ορισμένες προτάσεις πολιτικών προς υλοποίηση οι οποίες θα μπορούσαν να συνδράμουν προς τη συγκεκριμένη κατεύθυνση στον ελληνικό χώρο.

1.2. Χρησιμότητα της εργασίας

Η ασφάλεια των πληροφοριών έχει αποκτήσει σημαίνοντα ρόλο στην εποχή μας. Εάν αναλογιστούμε τη σημασία των πληροφοριών που διοχετεύονται στις υπηρεσίες της ηλεκτρονικής διακυβέρνησης και τις οποίες διαχειρίζονται αυτές, μπορούμε να κατανοήσουμε τη σημασία της προστασίας τους και σε αυτό το επίπεδο. Πέραν των τεχνικών ζητημάτων, η στάση των ατόμων αποτελεί ακρογωνιαίο λίθο για την επίτευξη της ασφάλειας των πληροφοριών. Η κουλτούρα ασφαλείας αποσκοπεί να ενισχύσει ακριβώς αυτή την πτυχή. Επιπρόσθετα, δεν έχει πραγματοποιηθεί κάποια σχετική μελέτη για την Ελλάδα. Η συγκεκριμένη εργασία λοιπόν αποσκοπεί στην κάλυψη, κατά το μέτρο του δυνατού, του συγκεκριμένου κενού. Οι προτάσεις που θα πραγματοποιηθούν κατά τη μελέτη περιπτώσεως της χώρας μας και οι οποίες θα βασιστούν στις βέλτιστες πρακτικές των υπολοίπων χωρών που θα εξεταστούν ευελπιστούμε ότι θα συμβάλουν προς τη συγκεκριμένη κατεύθυνση.

1.3. Δομή της εργασίας

Το κυρίως μέρος της εργασίας αποτελείται από τρία κεφάλαια. Στο δεύτερο κεφάλαιο γίνεται αναφορά στην έννοια της ηλεκτρονικής διακυβέρνησης, τα εμπόδια και τα οφέλη που προκύπτουν από αυτήν, καθώς και τις προϋποθέσεις επιτυχούς εφαρμογής της. Επίσης παρουσιάζονται τα κυριότερα ζητήματα ασφαλείας των σχετικών εφαρμογών.

Το τρίτο κεφάλαιο, εστιάζει στη σύνδεση της κουλτούρας ασφαλείας και της ηλεκτρονικής κυβέρνησης στον ευρωπαϊκό χώρο. Επιπρόσθετα, παρουσιάζονται ορισμένες σχετικές μελέτες περιπτώσεως ούτως ώστε να προσδιοριστούν οι βέλτιστες πρακτικές προς τη συγκεκριμένη κατεύθυνση.

Στο τέταρτο κεφάλαιο, εξετάζεται η κατάσταση που επικρατεί στην Ελλάδα. Στη συνέχεια, πραγματοποιούνται ορισμένες προτάσεις σχετικά με υλοποιήσεις αντίστοιχων πολιτικών.

Στο τέλος της εργασίας παρατίθενται τα συμπεράσματα που αντλήθηκαν μέσα από τη μελέτη.

Κεφάλαιο 2

2. Η Σημασία της Ηλεκτρονικής Διακυβέρνησης

2.1. Η έννοια της ηλεκτρονικής διακυβέρνησης

Η ηλεκτρονική διακυβέρνηση και η ψηφιακή κυβέρνηση είναι όροι που χρησιμοποιούνται για την περιγραφή της εφαρμογής των τεχνολογιών της πληροφορίας και της επικοινωνίας (ΤΠΕ) για τη βελτίωση των δημόσιων υπηρεσιών και την αύξηση της συμμετοχής των πολιτών στη δημοκρατική κυβέρνηση.

Η ηλεκτρονική διακυβέρνηση είναι ο κυρίαρχος όρος που χρησιμοποιείται στη χάραξη πολιτικής στην Ευρωπαϊκή Ένωση (ΕΕ). Αυτός ο όρος δίνει έμφαση στις υπηρεσίες που εστιάζουν στους χρήστες, οι οποίες μπορούν να ενσωματωθούν για να υποστηρίξουν την εύκολη και αποτελεσματική χρήση των δημόσιων υπηρεσιών από τους πολίτες και τις επιχειρήσεις. Πρόσφατα, ωστόσο, επικρατεί και ο όρος «ψηφιακή κυβέρνηση», μια έννοια που επεκτείνει το μοντέλο της ηλεκτρονικής διακυβέρνησης βασιζόμενο στην έννοια των νέων υπηρεσιών που μπορούν να υποστηρίξουν τα «ανοιχτά δεδομένα» του δημόσιου τομέα, καθώς και στη συνεργατική κοινότητα των δημόσιων αρχών, των επιχειρήσεων, και την κοινωνία των πολιτών που μπορεί να τις αναπτύξει.

Η ηλεκτρονική διακυβέρνηση αξιοποιεί το διαδίκτυο ούτως ώστε να προσφέρει πρόσβαση στις κρατικές υπηρεσίες σε όλους τους πολίτες οποιαδήποτε χρονική στιγμή και από οποιαδήποτε τοποθεσία υπάρχει πρόσβαση στο διαδίκτυο. Ένας σχετικός ορισμός είναι εκείνος που την περιγράφει ως «την κυβερνητική χρήση των τεχνολογιών πληροφορικής για τη διεκπεραίωση των εξωτερικών (με τους πολίτες και τις επιχειρήσεις) και των εσωτερικών (με τα άλλα κυβερνητικά τμήματα) επικοινωνιών του δημοσίου τομέα (Ebrahim και Irani, 2005)». Γενικότερα, αναφέρονται τέσσερις υποκατηγορίες της ηλεκτρονικής διακυβέρνησης (Larsen και Milakovich, 2005, Brown, 2003, Palvia και Sharma, 2007):

- Κυβέρνηση προς τον πολίτη (Government to Citizen – G2C) (Larsen και Milakovich, 2005), όπως είναι η δημιουργία ιστότοπων από τους οποίους οι πολίτες μπορούν να κατεβάσουν φόρμες, όπου παρουσιάζονται κυβερνητικές πληροφορίες κλπ.
- Κυβέρνηση προς επιχείρηση (Government to Business – G2B)
- Κυβέρνηση προς κυβέρνηση (G2G)
- Κυβέρνηση προς εργαζόμενους (G2E)

Οι εφαρμογές και οι υπηρεσίες της ηλεκτρονικής διακυβέρνησης έχουν αναφερθεί ως ένας από τους δύο κυριότερους παράγοντες οι οποίοι συμβάλλουν στην ανάπτυξη μίας κουλτούρας ασφαλείας σε εθνικό επίπεδο (OECD, 2005). Ορισμένες από τις πλέον σημαντικές προκλήσεις αναφορικά με την ασφάλεια των υπηρεσιών αυτών μπορούν να συνοψιστούν στον προσδιορισμό των χρηστών, την πιστοποίηση τους, την αποθήκευση δημοσίων και διαβαθμισμένων πληροφοριών στους ίδιους ιστότοπους, τον έλεγχο των εξουσιοδοτήσεων, την επικύρωση των συναλλαγών, τη διατήρηση αντιγράφων των πληροφοριών κοκ. Ορισμένες απαιτήσεις των συστημάτων ηλεκτρονικής διακυβέρνησης θα μπορούσαμε να πούμε ότι είναι οι εξής: η παροχή πολλαπλών μεθόδων πιστοποίησης, η εξουσιοδότηση, η έκδοση και ανάκληση πιστοποιήσεων, η εμπιστευτικότητα, η διαθεσιμότητα, η ιδιωτικότητα, η ακεραιότητα των πληροφοριών, η ανωνυμία, η επεκτασιμότητα κλπ.

2.2. Εμπόδια και Ευκαιρίες στην Υιοθέτηση Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Οι επόμενοι παράγοντες ενδέχεται να εμποδίσουν τη διάδοση των υπηρεσιών της ηλεκτρονικής διακυβέρνησης σε μία χώρα. Μπορούν να διαχωριστούν σε επτά κύριες κατηγορίες (Moon, 2002, Norris et al., 2005, Akman, 2005, Drogkaris et al., 2010, Mahaman, 2005, Hahamis, 2005):

1. Προβλήματα που σχετίζονται με την ηγεσία και άλλα προβλήματα διοικητικής φύσεως: Εντός της συγκεκριμένης κατηγορίας εμπίπτουν εμπόδια τα οποία οφείλονται σην έλλειψη κατάλληλου στρατηγικού σχεδιασμού καθώς και

στην ανεπάρκεια του σχεδιασμού για την εφαρμογή και την προώθηση των υπηρεσιών της ηλεκτρονικής διακυβέρνησης. Είναι ιδιαίτερα συχνό το φαινόμενο της απροθυμίας των κυβερνήσεων να αναλάβουν την υλοποίηση τέτοιων έργων, καθώς είναι ιδιαίτερα απαιτητικά, ενώ πιθανή αποτυχία ή αναποτελεσματική λειτουργία επιφέρει πέραν των δημοσιονομικών προβλημάτων και σημαντικό πολιτικό κόστος. Επιπρόσθετα, αρκετά συχνά οι προωθητικές ενέργειες τόσο νέων όσο και ήδη υπαρχόντων υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι μάλλον ακατάλληλες για την προσέγγιση των πολιτών και των επιχειρήσεων και την παρακίνηση τους στο να χρησιμοποιήσουν τις σχετικές πλατφόρμες.

2. Οικονομικά εμπόδια: Στη συγκεκριμένη κατηγορία εμπίπτουν κατά κύριο λόγο τα έξοδα ανάπτυξης και συντήρησης των υπηρεσιών, τα οποία μάλιστα συχνά υπερβαίνουν τον αρχικό προϋπολογισμό, ενώ υπάρχει και η περίπτωση των ανεπαρκών κονδυλίων για σκοπούς που σχετίζονται με την έρευνα, την ανάπτυξη και την καινοτομία. Εμπόδια της συγκεκριμένης κατηγορίας δημιουργούνται και από τη δυσκολία μέτρησης των εξόδων και οφελών που προκύπτουν από την ηλεκτρονική διακυβέρνηση, λόγω της φύσης των παρεχόμενων υπηρεσιών. Είναι συχνό το φαινόμενο άστοχων αναλύσεων κόστους και οφελών, οι οποίες όμως έχουν ως αποτέλεσμα τον περιορισμό των κονδυλίων που διατίθενται για την υλοποίηση σχετικών μελλοντικών εφαρμογών. Υπάρχει μία ανισορροπία μεταξύ του κόστους ανάπτυξης και συντήρησης και των οφελών, ειδικά στην περίπτωση μας, όπου τα οφέλη είναι κατά κύριο λόγο ποιοτικά. Το γεγονός του ότι τα οφέλη δεν αντισταθμίζονται από τα έξοδα έχει ως αποτέλεσμα ελλειματικούς προϋπολογισμούς, οι οποίοι συχνά καταλήγουν σε περιορισμό ή διακοπή των σχετικών δράσεων. Πέραν του τεχνικού κόστους ανάπτυξης των σχετικών εφαρμογών, προστίθενται επιπρόσθετα έξοδα λόγω των εξόδων που σχετίζονται με την προσαρμογή της νομοθεσίας στην ηλεκτρονική διακυβέρνηση. Εντός της συγκεκριμένης κατηγορίας εμπίπτουν ζητήματα που σχετίζονται με την ελεύθερη διακίνηση των πληροφοριών και την προστασία των προσωπικών δεδομένων.

3. Ανισότητες στην εξοικείωση των πολιτών με τις ΤΠΕ: Η διάδοση της ηλεκτρονικής διακυβέρνησης ενδέχεται να περιοριστεί λόγω του ότι δεν έχουν όλα τα άτομα το ίδιο επίπεδο ψηφιακών δεξιοτήτων, του κινδύνου πρόσβασης σε ακατάλληλα συστήματα, των φόβων σχετικά με τη χρήση της τεχνολογίας και της ελλειπούς κατανόησης των συστημάτων. Οι υπηρεσίες της ηλεκτρονικής διακυβέρνησης χρησιμοποιούνται από διάφορες κοινωνικές ομάδες, τα χαρακτηριστικά των οποίων διαφέρουν σημαντικά. Κατά συνέπεια, η ανάπτυξη εφαρμογών οι οποίες θα μπορούν να εξυπηρετήσουν πλήρως όλες τις ομάδες είναι μία αρκετά δύσκολη υπόθεση. Ένα ακόμα ζήτημα το οποίο χρήζει αντιμετώπισης είναι οι δυσκολίες πρόσβασης στα συστήματα που αντιμετωπίζουν ορισμένες κατηγορίες πολιτών, λόγω γεωγραφικών περιορισμών ή σωματικών και πνευματικών ικανοτήτων. Οι πολίτες πρέπει από την πλευρά τους να προσπαθήσουν να καλύψουν τα διάφορα κενά τους, συμμετέχοντας περισσότερο ενεργά στις υπηρεσίες της ηλεκτρονικής διακυβέρνησης.
4. Έλλειψη συντονισμού: ορισμένα εμπόδια που εμπίπτουν στη συγκεκριμένη κατηγορία και ενδέχεται να δημιουργήσουν προβλήματα στη διάδοση της ηλεκτρονικής διακυβέρνησης είναι οι διαφορές που υπάρχουν στη νομοθεσία και τους κανονισμούς τόσο εντός μίας συγκεκριμένης χώρας όσο και μεταξύ διαφορετικών χωρών, οι διαφορετικές προσεγγίσεις που υιοθετούν οι δημόσιοι οργανισμοί σχετικά με την εφαρμογή κοινών συστημάτων ηλεκτρονικής διακυβέρνησης και την παροχή ολοκληρωμένων υπηρεσιών, προβλήματα που σχετίζονται με τη συνεργασία μεταξύ των φορέων, καθώς και κενά στη συνεργασία μεταξύ των κρατών – μελών της Ευρωπαϊκής Ένωσης.
5. Κενά δεξιοτήτων και ευελιξίας στους εργασιακούς χώρους και τους οργανισμούς: Η διοίκηση και το προσωπικό των δημοσίων υπηρεσιών δεν κατέχουν το αναγκαίο επίπεδο δεξιοτήτων και γνώσεων ούτως ώστε να ανταπεξέλθουν άμεσα στις νέες απαιτήσεις που δημιουργούνται από την ηλεκτρονική διακυβέρνηση. Είναι αναγκαία η εκπαίδευση τους, η οποία όμως ορισμένες φορές αποδεικνύεται ανεπαρκής. Τα ανώτερα στελέχη συχνά δεν έχουν το απαραίτητο επίπεδο δεξιοτήτων ούτως ώστε να οργανώσουν τη

μετάβαση προς τις νέες πρακτικές και διαδικασίες. Η αρνητική στάση προς την καινοτομία από τη δημόσια διοίκηση και το προσωπικό τοποθετεί σημαντικά εμπόδια στον ανασχεδιασμό των οργανισμών και των υπηρεσιών στις οποίες εφαρμόζεται η ηλεκτρονική διακυβέρνηση. Ενδέχεται να επηρεαστεί σημαντικά η ανάπτυξη αποτελεσματικών υπηρεσιών, οι οποίες πρέπει πάντοτε να τοποθετούν στο επίκεντρο την εξυπηρέτηση των πολιτών και των επιχειρήσεων. Επιπρόσθετα, σε ορισμένες περιπτώσεις η αλλαγή των πρακτικών εργασίας του προσωπικού παρεμποδίζεται λόγω της ακαμψίας της εργατικής νομοθεσίας.

6. Προβλήματα εμπιστοσύνης και ασφάλειας δεδομένων: Στους πολίτες είναι διάχυτη μία ανησυχία η οποία σχετίζεται με την προστασία της ιδιωτικότητας τους και την καταγραφή προσωπικών τους δεδομένων εν αγνοία τους. Επιπρόσθετα, ανησυχούν για διαδικτυακές απάτες και άλλες παράνομες πράξεις, οι οποίες επηρεάζουν και τις εφαρμογές της ηλεκτρονικής διακυβέρνησης. Επιπρόσθετα, ανησυχίες υφίστανται και όταν ζητούνται κωδικοί πρόσβασης ή ηλεκτρονικό ταχυδρομείο. Ειδικά για την ηλεκτρονική διακυβέρνηση, η ανησυχία αυξάνεται όταν ζητείται η δήλωση ευαίσθητων προσωπικών δεδομένων στις σχετικές εφαρμογές. Το ζήτημα αυτό γίνεται εντονότερο σε περιόδους γενικότερης δυσπιστίας προς την κυβέρνηση ή σε περιπτώσεις κατά τις οποίες οι δημόσιες αρχές αδιαφορούν για τη διαφάνεια και την πληροφόρηση των πολιτών σχετικά με τις δράσεις τους. Οι φορείς υλοποίησης των υπηρεσιών της ηλεκτρονικής διακυβέρνησης θα πρέπει να λαμβάνουν πολύ σοβαρά ζητήματα τα οποία άπτονται της εφαρμογής και προώθησης της ασφάλειας.
7. Τεχνικές παραλείψεις: Ζητήματα τεχνικού σχεδιασμού, όπως είναι η έλλειψη συμβατότητας μεταξύ των συστημάτων που χρησιμοποιούνται, εμποδίζουν τη διακίνηση των πληροφοριών και την επικοινωνία. Είναι αρκετά συχνό το φαινόμενο των κακών επιδόσεων ή της κατάρρευσης συστημάτων ηλεκτρονικής διακυβέρνησης λόγω σχεδιαστικών παραλείψεων. Τα αίτια για αυτά τα περιστατικά βρίσκονται σε ασυμβατότητες μεταξύ του υλισμικού, του λογισμικού και των διαδικτυακών υποδομών μεταξυ των δημοσίων υπηρεσιών. Επιπρόσθετα, υπάρχουν και προβλήματα κατά την επαφή των

χρηστών με τις σχετικές εφαρμογές. Ορισμένες φορές οι εφαρμογές είναι ιδιαίτερα δύσχρηστες, τόσο για το προσωπικό των υπηρεσιών όσο και για τους πολίτες. Ένα ακόμα ζήτημα που θα μπορούσε να τοποθετηθεί στη συγκεκριμένη κατηγορία είναι η απουσία κοινών πρακτικών σε ευρωπαϊκό επίπεδο αναφορικά με την ηλεκτρονική ταυτότητα των πολιτών.

Η διάδοση της ηλεκτρονικής διακυβέρνησης μπορεί να προσφέρει σημαντικές βελτιώσεις στη λειτουργία των δημοσίων οργανισμών. Μέσα από αυτή οφελούνται όχι μόνο οι υπηρεσίες, αλλά και οι πολίτες και οι επιχειρήσεις. Οι κυριότερες ευκαιρίες που προκύπτουν από τις σχετικές εφαρμογές έχουν ως εξής (Γιαμπουράς, 2006, Mahaman, 2005, Torres, 2005):

1. Εξοικονόμηση εξόδων για τις δημόσιες υπηρεσίες.
2. Ποιοτικότερες υπηρεσίες προς τον πολίτη.
3. Αναδιοργάνωση και εξορθολογισμός των διαδικασιών του δημοσίου.
4. Βελτίωση της αποδοτικότητας και της αποτελεσματικότητας των δημοσίων οργανισμών.
5. Μείωση της άμεσης επαφής των πολιτών με τις υπηρεσίες.
6. Συντομότεροι χρόνοι διεκπεραίωσης των συναλλαγών και 24ωρη διαθεσιμότητα των υπηρεσιών.
7. Προώθηση της διαφάνειας και περιορισμός της διαφθοράς.
8. Συμμετοχή των πολιτών στις δημόσιες πολιτικές.
9. Έλεγχος της δημόσιας διοίκησης και απόδοση ευθυνών όταν αυτό είναι αναγκαίο.

Επιπρόσθετα, βελτιώνεται η εξυπηρέτηση ορισμένων αδύνατων κοινωνικών ομάδων (ΑΜΕΑ, άτομα χαμηλότερου μορφωτικού επιπέδου), καθώς η χρήση προσυμπληρωμένων φορμών καθιστά τις λειτουργίες των δημοσίων οργανισμών κατά πολύ ευκολότερες.

Το δημόσιο μπορεί να αποκομίσει σημαντικά οφέλη από την επέκταση της ηλεκτρονικής διακυβέρνησης. Πέραν της βελτίωσης της αποδοτικότητας και της αποτελεσματικότητας, προκύπτει σημαντική εξοικονόμηση πόρων. Μειώνεται τόσο ο χρόνος που χρειάζεται ο κάθε υπάλληλος για να ολοκληρώσει κάποια διαδικασία

όσο και τα λειτουργικά έξοδα, καθώς οι διαδικτυακές συναλλαγές παρουσιάζουν πολύ χαμηλότερο κόστος σε σχέση με τις παραδοσιακές επιτόπιες συναλλαγές (Akman, 2005). Επίπρόσθετα, λόγω των κοινών βάσεων δεδομένων γίνεται κατά πολύ ευκολότερη και γρηγορότερη η αναζήτηση και η επεξεργασία των πληροφοριών από τις δημόσιες υπηρεσίες.

Το κυριότερο όφελος που απολαμβάνουν οι πολίτες από τις εφαρμογές της ηλεκτρονικής διακυβέρνησης είναι οι ποιοτικότερες υπηρεσίες που παρέχονται προς αυτούς. Έχουν τη δυνατότητα 24ωρης πρόσβασης στις υπηρεσίες, εξοικονομούν χρόνο καθώς η διεκπεραίωση των υποθέσεων τους γίνεται σε μεγάλο βαθμό αυτοματοποιημένα, χωρίς να απαιτείται η αναμονή τους σε ουρές ή να χρειάζεται να είναι διαθέσιμος κάποιος υπάλληλος ούτως ώστε να τους εξυπηρετήσει, η αναγκαιότητα της φυσικής τους παρουσίας στις υπηρεσίες συμβάλει στη μείωση του κόστους των συναλλαγών, ενώ εξυπηρετούνται γρηγορότερα και λαμβάνουν συντομότερα απαντήσεις σχετικά με τις υποθέσεις τους. Ακόμα, λαμβάνουν πληρέστερες και ποιοτικότερες υπηρεσίες, μπορούν να ελέγχουν άμεσα την πορεία των αιτημάτων τους, ενώ εξοικονομούν χρόνο, καθώς χάρη στις κοινές βάσεις δεδομένων του δημοσίου δεν είναι αναγκαίο να παρέχουν τις ίδιες πληροφορίες σε κάθε υπηρεσία (Torres, 2005).

Η εξοικονόμηση χρόνου και κόστους οφελεί σημαντικά και τις επιχειρήσεις. Τα οφέλη για αυτές είναι ιδιαίτερα σημαντικά, εάν αναλογιστούμε τον όγκο των συναλλαγών που διατηρούν με το δημόσιο, όπως είναι οι εγγραφές σε διάφορους φορείς, η έκδοση αδειών και πιστοποιητικών, η υποβολή διαφόρων δηλώσεων, καθώς και οι πληρωμές. Η εξοικονόμηση χρόνου που μπορεί να προκύψει από την ηλεκτρονική διεκπεραίωση των παραπάνω διαδικασιών συμβάλει σε σημαντική μείωση των λειτουργικών τους εξόδων, κάτι το οποίο είναι ιδιαίτερα σημαντικό, καθώς αυτά είναι άρρηκτα συνδεδεμένα με τη βιωσιμότητα τους.

2.3. Προϋποθέσεις της επιτυχίας της εφαρμογής της ηλεκτρονικής διακυβέρνησης

Κατά τη διαδικασία υλοποίησης της μετάβασης προς την ηλεκτρονική διακυβέρνηση πρέπει να υπάρχουν ορισμένες ικανότητες, ούτως ώστε η όλη διαδικασία να στεφθεί από επιτυχία. Οι ικανότητες αυτές είναι οι αναλυτικές ικανότητες, οι ικανότητες διαχείρισης πληροφοριών, οι τεχνικές ικανότητες, οι ικανότητες επικοινωνίας και παρουσίασης και οι ικανότητες διαχείρισης έργων (LaVigne, 2001, στου Reffat, 2003).

Οι ικανότητες ερμηνείας και ανάλυσης είναι ιδιαιτέρως σημαντικές σε κάθε επίπεδο της διαδικασίας υλοποίησης της ηλεκτρονικής διακυβέρνησης. Ξεκινούν από τον καθορισμό του προβλήματος, της διαδικασίας μέσω της οποίας ο οργανισμός περιγράφει τα χαρακτηριστικά του και ανακαλύπτει τις διεργασίες, πολιτικές και πρακτικές οι οποίες αποτελούν παράγοντες συνεισφοράς σε αυτά. Σε αυτό το επίπεδο είναι αναγκαίες η ανάλυση των διεργασιών, ο έλεγχος των συστημάτων, η ανάλυση των ενδιαφερομένων, η διεξαγωγή ερευνών ικανοποίησης των συναλλασσομένων, η αξιολόγηση της επίδοσης, η καταγραφή στατιστικών τάσεων και λοιπές παρόμοιες δραστηριότητες. Σε μεταγενέστερα επίπεδα, απαιτούνται η ανάλυση των αναγκών των χρηστών, οι εναλλακτικές των οργανωτικών διαδικασιών, η ροή εργασιών και η ροή της πληροφορίας. Επιπρόσθετα, είναι ιδιαίτερα σημαντική και η διερεύνηση των ενεργειών στις οποίες προβαίνουν άλλοι οργανισμοί για την επίλυση παρομοίων προβλημάτων. Μέσω των αναλύσεων αυτών διευκολύνεται η ανάπτυξη του συστήματος (Reffat, 2003).

Οι ικανότητες που σχετίζονται με τη διαχείριση των πληροφοριών περιλαμβάνουν την αντιμετώπιση της πληροφορίας ως ενός πολύτιμου οργανωτικού πόρου. Το περιεχόμενο, η ποιότητα, η μορφή, η αποθήκευση, η μετάδοση, η προσβασιμότητα, η χρηστικότητα, η ασφάλεια και η διατήρηση των πληροφοριών συνεισφέρουν στην αξία τους. Λόγω του πολύπλευρου χαρακτήρα τους, οι ικανότητες διαχείρισης των πληροφοριών είναι αναγκαίες σε διάφορες εργασίες (Reffat, 2003):

1. Τα στελέχη και το προσωπικό της διαχείρισης του προγραμματισμού πρέπει να έχουν γνώσεις και ικανότητες ούτως ώστε να διασφαλίζουν την εγκυρότητα του περιεχομένου, τη σαφήνεια του ορισμού των δεδομένων, την

αξιοπιστία των μεταδεδομένων και άλλες ποιοτικές απαιτήσεις των δεδομένων.

2. Οι επαγγελματίες των ΤΠΕ πρέπει να είναι ικανοί να δημιουργήσουν τις μορφές, αρχεία και φακέλους που απαιτούνται για την αναπαράσταση και οργάνωση των πληροφοριών. Πρέπει επίσης να βρίσκονται σε θέση να διαχειριστούν τις διεπαφές και τα χαρακτηριστικά ασφαλείας που διασφαλίζουν τη χρηστικότητα και την ακεραιότητα.
3. Οι αρχειοθέτες πρέπει να έχουν τις απαραίτητες γνώσεις διαχείρισης των πληροφοριών, ειδικά όταν πρέπει να εξετάσουν ζητήματα ταξινόμησης, αναζήτησης και συντήρησης.
4. Οι ερευνητές συχνά πρέπει να συνεργάζονται με τους προγραμματιστές, ούτως ώστε να κατασκευάζουν τους ορισμούς των δεδομένων, να σχεδιάζουν τις διεργασίες συλλογής δεδομένων και να υλοποιούν μετρήσεις ποιοτικού ελέγχου. Οι δραστηριότητες αυτές διασφαλίζουν ότι τα δεδομένα είναι κατάλληλα για τις αναλύσεις που επιθυμούν να διεξάγουν.

Επιπρόσθετα, υπάρχει η ανάγκη επικοινωνίας των στόχων, της προόδου, των ζητημάτων που χρήζουν αντιμετώπισης και των αποτελεσμάτων. Ενδέχεται να χρειαστούν συναντήσεις με νομοθετικούς ή εκτελεστικούς φορείς ούτως ώστε να διασφαλιστεί η αρχική και συνεχής υποστήριξη και χρηματοδότηση. Οι συναντήσεις με τους εμπλεκόμενους εξηγούν το πως εκείνοι θα επηρεαστούν από τη μετάβαση στην ηλεκτρονική διακυβέρνηση και ενθαρρύνουν τη συμμετοχή τους σε αυτή. Οι ικανότητες παρουσίασης περιλαμβάνουν την ικανότητα σύνθεσης πολύπλοκων δεδομένων σε πληροφορίες οι οποίες είναι απαραίτητες για κάποιο στοχευμένο κοινό. Η πληροφορία πρέπει να κατηγοριοποιηθεί, να συνοψιστεί και να μετατραπεί σε ενημερωτικό υλικό το οποίο περιλαμβάνει τα σημαντικότερα στοιχεία, χωρίς να υπεραπλουστεύει (Reffat, 2003).

Οι ικανότητες διαχείρισης έργου αφορούν τον σχεδιασμό, την οργάνωση, την εκτίμηση, την ανάθεση πόρων, τη διαπραγμάτευση, την παρακολούθηση της προόδου, τη μέτρηση των αποτελεσμάτων, την επίλυση προβλημάτων και την επικοινωνία. Η διαχείριση έργου περιλαμβάνει τη διαχείριση του πεδίου δράσης, του χρόνου, των εξόδων, της ποιότητας και του κινδύνου. Ασχέτως του μεγέθους του

έργου, οι ικανότητες αυτές πρέπει να μπορέσουν να οδηγήσουν στην υλοποίηση μίας επιτυχούς εφαρμογής της ηλεκτρονικής διακυβέρνησης (Reffat, 2003).

2.4. Θέματα ασφαλείας στην ηλεκτρονική διακυβέρνηση

2.4.1. Απαιτήσεις ασφαλείας στην ηλεκτρονική διακυβέρνηση

Το ζήτημα της προστασίας των δεδομένων αποτελεί αναπόσπαστο στοιχείο των εφαρμογών ηλεκτρονικής διακυβέρνησης. Η προστασία των προσωπικών δεδομένων συνίσταται στην αποφυγή της διαρροής τους με πιθανές αρνητικές επιπτώσεις στο υποκείμενο, καθώς και στην αποφυγή της χρήσης τους για διαφορετικούς σκοπούς από εκείνους της παραχώρησης τους (Γάκης, 2011). Κομβική σημασία για τα δεδομένα των εφαρμογών ηλεκτρονικής διακυβέρνησης έχει επίσης η διασφάλιση της προέλευσης, της πληρότητας και της ακρίβειας τους (Benabdallah, 2002, στου AlKalbani, 2015).

Οι πλατφόρμες της ηλεκτρονικής διακυβέρνησης πρέπει πάντοτε να έχουν ένα υψηλό επίπεδο προστασίας των πληροφοριών τους, λόγω της φύσεως τους. Είναι αναγκαίος ένας σχεδιασμός ασφαλείας ο οποίος θα προβλέπει την αντιμετώπιση διαφόρων απειλών. Αυτός ο στόχος μπορεί να επιτευχθεί μέσα από την εφαρμογή μίας σειράς μέτρων προστασίας, όπως είναι οι πολιτικές, πρακτικές, διαδικασίες, τεχνικές και λειτουργίες λογισμικού και υλικού. Μέσα από τα συγκεκριμένα μέτρα μπορεί να διασφαλιστεί ένα υψηλό επίπεδο ασφάλειας πληροφοριών (Μαυρίδης, 2015).

Ως προσωπικά δεδομένα νοούνται οι πληροφορίες που αναφέρονται και περιγράφουν ένα άτομο (στοιχεία αναγνώρισης, φυσικά χαρακτηριστικά, εκπαίδευση, εργασία, οικονομική κατάσταση, ενδιαφέροντα, δραστηριότητες, συνήθειες). Το άτομο που σχετίζεται με τα δεδομένα αποτελεί το υποκείμενο τους. Ευαίσθητα προσωπικά δεδομένα είναι εκείνα που αφορούν τη φυλετική ή εθνική προέλευση, τις πολιτικές πεποιθήσεις, τις θρησκευτικές και φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, την υγεία, την κοινωνική πρόνοια, την ερωτική ζωή, τις ποινικές διώξεις και καταδίκες και τη συμμετοχή σε ενώσεις προσώπων που σχετίζονται με τα παραπάνω. Τα ευαίσθητα προσωπικά

δεδομένα χαίρουν υψηλότερης νομικής προστασίας σε σχέση με τα απλά (Γάκης, 2011).

Ως επεξεργασία προσωπικών δεδομένων ορίζεται η κάθε εργασία που πραγματοποιείται σε δεδομένα αυτής της κατηγορίας. Ορισμένα σχετικά παραδείγματα είναι η συλλογή, η καταχώρηση, η οργάνωση, η διατήρηση/αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση, η συσχέτιση/συνδυασμός, η διασύνδεση, η δέσμευση, η διαγραφή και η καταστροφή (Γάκης, 2011).

Η αξία ενός αγαθού αφορά τη σημασία που έχει αυτό για την επίτευξη των στόχων του οργανισμού, ενώ μετράται είτε με τη μορφή χρημάτων είτε με άλλους όρους. Ένα υπολογιστικό σύστημα ενδέχεται να έχει ορισμένες αδυναμίες (ευπάθειες), τις οποίες θα μπορούσαν να εκμεταλλευτούν κακόβουλες πλευρές, πραγματοποιώντας επιθέσεις και δημιουργώντας απειλές. Τα αίτια των διαφόρων κινδύνων ενδέχεται να είναι τεχνικά ή ανθρώπινα (εκούσια ή ακούσια), ενώ οι απειλές μπορούν να έχουν είτε σκόπιμο είτε τυχαίο χαρακτήρα. Οι απειλές ενδέχεται να δημιουργήσουν ζημιές. Υπό τον όρο ζημιά νοείται η μείωση της αξίας του αγαθού. Ως επίπτωση ορίζεται μία αλλαγή στον βαθμό επίτευξης των στόχων του οργανισμού (Μαυρίδης, 2015). Η επικινδυνότητα ορίζεται από τα στοιχεία του αγαθού, της ευπάθειας, της απειλής, της ζημιάς και της επίπτωσης. Μέσα από την κατάλληλη αξιολόγηση της επικινδυνότητας οδηγούμαστε στην εκλογή των κατάλληλων μέτρων προστασίας, τα οποία θα συμβάλλουν στην ελαχιστοποίηση της.

Ορισμένοι παράγοντες οι οποίοι επηρεάζουν την ασφάλεια των δεδομένων στις εφαρμογές που εξετάζουμε είναι η υποστήριξη από την ανώτερη διοίκηση, οι νομοθετικές ρυθμίσεις, οι στρατηγικές και πολιτικές ασφαλείας, οι προηγμένες τεχνολογίες ασφαλείας και οι ενδεχόμενες παραβιάσεις (AlKalbani, 2015). Επιπρόσθετα, μία σημαντική πτυχή της εμφύσησης μίας κουλτούρας ασφαλείας είναι και εκείνη της διασφάλισης της δημόσιας εμπιστοσύνης στις σχετικές υπηρεσίες (AlKalbani, 2015), καθώς δεν αναφερόμαστε σε οργανισμούς οι οποίοι απλά πρέπει να ικανοποιήσουν ορισμένες νομικές υποχρεώσεις, αλλά σε δημόσιους οργανισμούς οι οποίοι απευθύνονται σε όλους τους πολίτες μίας χώρας.

Προκειμένου να εκλεγούν τα πλέον αποδοτικά μέτρα προστασίας απαιτείται η διεξαγωγή ενός προσεκτικού και λεπτομερούς σχεδιασμού, ενώ προκειμένου να επιτευχθεί η ασφάλεια των πληροφοριών είναι απαραίτητη η συμμετοχή όλου του προσωπικού του οργανισμού. Επιπρόσθετα, ενδέχεται να χρειαστεί να συνδράμουν και εξωτερικοί συνεργάτες, οι οποίοι ειδικεύονται στο αντικείμενο της ασφάλειας δεδομένων και πληροφοριών (Μαυρίδης, 2015).

Η αποτελεσματική εφαρμογή ενός προτύπου ασφαλείας προϋποθέτει και την ύπαρξη ενός αποτελεσματικού συστήματος διεξαγωγής ελέγχων ασφαλείας. Οι μηχανισμοί ασφαλείας πρέπει να είναι σχεδιασμένοι και να εφαρμόζονται υπό το πρίσμα της υποστήριξης του οργανωτικού στόχου της προώθησης της ασφάλειας των πληροφοριών ενός δημοσίου οργανισμού (AlKalbani, 2015).

Η υιοθέτηση πολιτικών ασφαλείας από έναν δημόσιο οργανισμό επηρεάζεται από τη διοικητική αφοσίωση που υπάρχει προς τη συγκεκριμένη κατεύθυνση (Smith και Jamieson, 2006, στου AlKalbani, 2015). Προκειμένου να γίνει λόγος για την ύπαρξη διοικητικής αφοσίωσης, πρέπει να υπάρχουν ορισμένα χαρακτηριστικά, τα οποία είναι η ορατή συμμετοχή, η συνεχής επικοινωνία και υποστήριξη ούτως ώστε να ενθαρρυνθεί η θετική στάση των εργαζομένων προς την ασφάλεια (Kolkowska και Dillon, 2012, στο AlKalbani, 2015). Έχει δειχθεί (Knapp, 2006, στου AlKalbani, 2015) ότι δεν θα έχει κάποιο αξιοσημείωτο αποτέλεσμα η δημιουργία, εκπαίδευση και ενίσχυση των πολιτικών ασφαλείας χωρίς την υποστήριξη και εμπλοκή της ανώτερης διοίκησης. Η απουσία διοικητικής υποστήριξης αναφέρεται ως ένα κοινό αίτιο για την ασθενή εφαρμογή πολιτικών ασφαλείας πληροφοριών σε έναν οργανισμό (AlKalbani, 2015).

Ιδιαίτερη μνεία πρέπει να γίνει και στον παράγοντα της κοινωνικής πίεσης, η οποία εξωθεί τους δημόσιους οργανισμούς προς την κατεύθυνση της βελτίωσης των πολιτικών ασφαλείας τους. Η κοινωνική πίεση αναφέρεται ως ένας παράγοντας του περιβάλλοντος ο οποίος ενδέχεται να κινητοποιήσει τους οργανισμούς προς την κατεύθυνση της ενσωμάτωσης μηχανισμών ασφαλείας στις καθημερινές τους εργασίες, μέσω της παρότρυνσης υιοθέτησης σχετικών επιτυχημένων πρακτικών (AlKalbani, 2015).

Η κοινωνική πίεση αναφέρεται στην προστασία των κοινωνικά επιθυμητών πληροφοριών στις υπηρεσίες της ηλεκτρονικής διακυβέρνησης. Ένα χαρακτηριστικό παράδειγμα είναι εκείνο της μυστικότητας, της εμπιστοσύνης και της ποιότητας των υπηρεσιών, οι οποίες είναι κοινωνικά επιθυμητές ανάγκες οι οποίες πρέπει να ικανοποιηθούν αποτελεσματικά από τις υπηρεσίες της ηλεκτρονικής διακυβέρνησης. Ορισμένοι δείκτες της κοινωνικής πίεσης είναι οι αντιλήψεις του προσωπικού των δημοσίων υπηρεσιών σχετικά με τις συνέπειες που μπορεί να επιφέρει η αποτυχία συμμόρφωσης με τις κοινωνικές τους υποχρεώσεις, ο βαθμός εξάρτησης των πολιτών από τις τεχνολογικές υπηρεσίες, καθώς και οι προσπάθειες που καταβάλλονται από τους δημόσιους οργανισμούς για την ενίσχυση της ασφάλειας των πληροφοριών που διαχειρίζονται τα συστήματα ηλεκτρονικής διακυβέρνησης ούτως ώστε να ενισχυθεί και η εμπιστοσύνη των πολιτών σε αυτά. Οι κοινωνικές πιέσεις ωθούν τους δημόσιους οργανισμούς στο επίκεντρο της προσοχής, υπενθυμίζοντας τους ότι πρέπει να διατηρήσουν την εμπιστοσύνη των πολιτών καθώς και να διατηρήσουν τη φήμη τους ως υπεύθυνες δημόσιες οντότητες, προστατεύοντας τις πληροφορίες των πολιτών (AlKalbani, 2015).

Ένας κακόβουλος χρήστης επιχειρεί να εκμεταλλευτεί ευπάθειες των συστημάτων ηλεκτρονικής διακυβέρνησης, οι οποίες μπορεί να βρίσκονται τόσο στο σύστημα όσο και στις λειτουργίες εγγραφής, ταυτοποίησης και πιστοποίησης (Palanisamy και Mukerji, 2012). Οι κακόβουλοι χρήστες συνήθως αποσκοπούν στα παρακάτω:

- Αντιποίηση αρχής, εξουσιοδοτημένου χρήστη, οργανισμού.
- Παράνομη πρόσβαση σε πληροφορίες ή υπηρεσίες.
- Παραβίαση της ιδιωτικότητας.
- Μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα και χρήση αυτών.
- Άρνηση παροχής υπηρεσίας (denial of service).

Η σημασία του τομέα της ασφάλειας σχετικά με την εξάπλωση των εφαρμογών της ηλεκτρονικής διακυβέρνησης επιβεβαιώθηκε και από σχετική έρευνα (AlAwadhi και Morris, 2009), η οποία εξέτασε την περίπτωση του Κουβέιτ. Στη μελέτη αυτή η ασφάλεια του διαδικτύου και η εμπιστοσύνη των χρηστών σε αυτό χαρακτηρίζεται ως ένας από τους παράγοντες οι οποίοι επηρεάζουν τη διάδοση των σχετικών

υπηρεσιών. Επιπρόσθετα, αναφέρεται ότι το 64% των ερωτηθέντων εμπιστεύονταν το διαδίκτυο, καθώς θεωρούσαν ότι οι προηγμένες τεχνολογίες ασφαλείας που εφαρμόζονταν σε αυτό μπορούσαν να τους προστατέψουν κατά την ανταλλαγή δεδομένων και τη διεξαγωγή των συναλλαγών τους. Ταυτόχρονα, ένα 30% δήλωσε ότι ζητήματα που σχετίζονται με την ασφάλεια θα μπορούσαν να τους αποτρέψουν από το να εμπιστευτούν και επομένως να χρησιμοποιήσουν τις εν λόγω υπηρεσίες. Οι κυριότερη πηγή ανησυχιών ήταν η υποκλοπή και αλλοίωση ή κακή χρήση των προσωπικών δεδομένων από χάκερς. Κατά συνέπεια, μπορούμε να συμπεράνουμε ότι η διάδοση των υπηρεσιών της ηλεκτρονικής διακυβέρνησης είναι άρρηκτα συνδεδεμένη με τις διαβεβαιώσεις ασφαλείας που παρέχονται στους χρήστες.

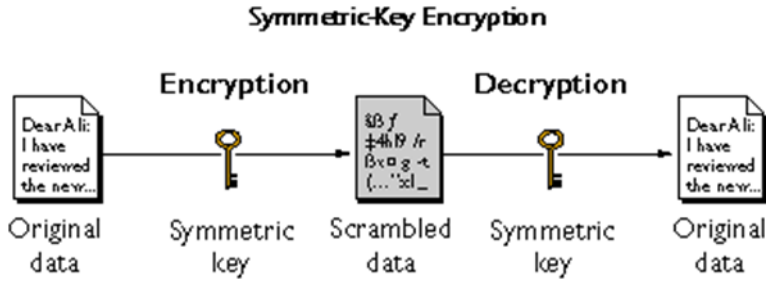
Προς τη συγκεκριμένη κατεύθυνση, σχεδόν όλα τα κράτη – μέλη του ΟΟΣΑ έχουν ενσωματώσει στις εθνικές τους νομοθεσίες ρυθμίσεις για την αντιμετώπιση του διαδικτυακού εγκλήματος (OECD, 2005). Επιπρόσθετα, έχουν θεσμοθετηθεί ειδικά σώματα για την αντιμετώπιση των σχετικών παραβατικών ενεργειών, τα οποία μάλιστα συνεργάζονται τόσο με τον ιδιωτικό τομέα όσο και με αντίστοιχους φορείς άλλων χωρών, καθώς το διαδικτυακό έγκλημα είναι πολυσύνθετο, ενώ έχει διεθνή χαρακτήρα. Επιπρόσθετα, ορισμένες χώρες έχουν θεσμοθετήσει και ομάδες εργασίας τα μέλη των οποίων έχουν ως αντικείμενο τους την άντληση συμπερασμάτων μέσα από την ανάλυση δεδομένων τα οποία σχετίζονται με την ασφάλεια. Η διεθνής συνεργασία των ομάδων αυτών θεωρείται εξέχουσας σημασίας, καθώς καθιστά αποτελεσματικότερη την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών (OECD, 2005).

2.4.2. Κρυπτογραφία και εφαρμογές

Η κρυπτογραφία αποσκοπεί στην τήρηση των απαιτήσεων ασφαλείας που αναφέρθηκαν στο προηγούμενο κεφάλαιο. Έχει τις ρίζες της σε αντίστοιχες τεχνικές οι οποίες χρησιμοποιήθηκαν κατά την αρχαιότητα και τον μεσαίωνα για την προστασία απόρρητων δεδομένων. Ορίζεται ως η επιστήμη της εξεύρεσης τεχνικών μέσω των οποίων τα κείμενα θα μετασχηματιστούν ούτως ώστε να είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα (Γκρίτζαλης, Κάτσικας, Χρυσικόπουλος και Burmester, 2011). Μπορεί να διαχωριστεί σε δύο κύριες διαδικασίες, την κρυπτογράφηση (encryption) και την αποκρυπτογράφηση (decryption). Η πρώτη

διαδικασία μετατρέπει τα δεδομένα σε μη αναγνωρίσιμη ή μη επεξεργάσιμη μορφή, ενώ η δεύτερη τα επαναφέρει στην αρχική τους μορφή. Η όλη διαδικασία υλοποιείται μέσω ειδικών αλγορίθμων. Για την ενεργοποίηση τους χρησιμοποιείται ένα σύνολο χαρακτήρων, το κρυπτογραφικό κλειδί.

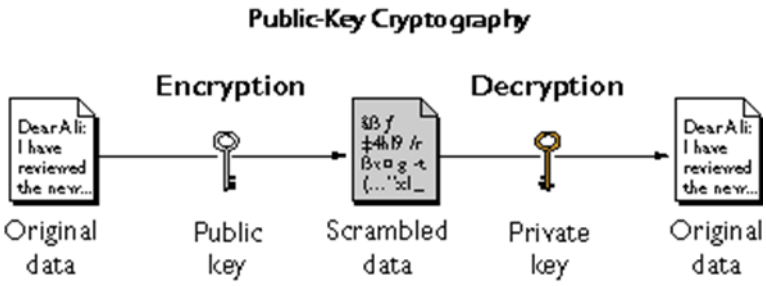
Υπάρχουν δύο κύριες προσεγγίσεις, η συμμετρική και η ασύμμετρη κρυπτογραφία. Στη συμμετρική κρυπτογραφία χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Το κλειδί αυτό ονομάζεται μυστικό κλειδί (secret key), ενώ είναι γνωστό μόνο στους εξουσιοδοτημένους χρήστες (Γκρίτζαλης, Κάτσικας, Χρυσικόπουλος και Burmester, 2011). Η όλη διαδικασία παρουσιάζεται στο επόμενο σχεδιάγραμμα.



Εικόνα 1 – Συμμετρική κρυπτογραφία (IBMa, 2018)

Η συγκεκριμένη τεχνική εφαρμόζεται συνήθως για τη διασφάλιση του ότι δεν θα αποκτήσουν πρόσβαση στα δεδομένα μη εξουσιοδοτημένοι χρήστες (εμπιστευτικότητα), καθώς πρόσβαση σε αυτά έχουν μόνο οι χρήστες που κατέχουν το μυστικό κλειδί. Το σημαντικότερο πλεονέκτημα της είναι η ταχύτητα, ενώ κύριο μειονέκτημα της είναι το ότι στην περίπτωση κατά την οποία έχουμε μεγάλο αριθμό χρηστών δυσκολεύει κατά πολύ η ασφαλής διαχείριση του κλειδιού, καθώς αυτό πρέπει να προωθηθεί σε όλους τους εξουσιοδοτημένους χρήστες με ασφάλεια, ενώ εκείνοι με τη σειρά τους πρέπει να μεριμνήσουν αναλόγως για την προστασία του.

Η προσέγγιση της ασύμμετρης κρυπτογραφίας χρησιμοποιεί δύο κλειδιά, ένα για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση. Τα δεδομένα που έχουν κρυπτογραφηθεί με το ένα κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το δεύτερο κλειδί. Το πρώτο κλειδί (δημόσιο κλειδί) κοινοποιείται σε όλους τους χρήστες, ενώ το δεύτερο (ιδιωτικό κλειδί) είναι απόρρητο. Η όλη διαδικασία παρουσιάζεται στην Εικόνα 2.



Εικόνα 2 – Ασύμμετρη κρυπτογραφία (IBMb, 2018)

Το δημόσιο κλειδί κοινοποιείται μέσω δημοσίων καταλόγων ή δημοσίων βάσεων δεδομένων. Το ιδιωτικό κλειδί έχει απόρρητο χαρακτήρα και το γνωρίζει μόνο ο κάτοχος του ζεύγους των κλειδιών. Σύμφωνα με την προσέγγιση της ασύμμετρης κρυπτογραφίας κάθε χρήστης έχει τουλάχιστον ένα ζεύγος κλειδιών, το οποίο αντιστοιχεί αποκλειστικά σε εκείνον, ούτως ώστε να υπάρχει μονοσήμαντη αντιστοιχία μεταξύ των χρηστών και των ζευγών κλειδιών. Είναι όμως δυνατό ένας χρήστης να έχει περισσότερα από ένα ζεύγη. Το δημόσιο κλειδί ονομάζεται έτσι καθώς κοινοποιείται σε δημόσιους καταλόγους μαζί με τα στοιχεία του κατόχου του (ονοματεπώνυμο, διεύθυνση, κλπ.).

Οι κατάλογοι των δημοσίων κλειδιών είναι προσπελάσιμοι από οποιονδήποτε το επιθυμεί. Το ιδιωτικό κλειδί ονομάζεται έτσι καθώς είναι απόρρητο, δεν δημοσιοποιείται ποτέ στο διαδίκτυο, ενώ το γνωρίζει μόνο ο κάτοχος του. Η συγκεκριμένη προσέγγιση χρησιμοποιείται κατά κύριο λόγο σε δύο περιπτώσεις, στην ανταλλαγή εμπιστευτικών μηνυμάτων και στην επιβεβαίωση της ταυτότητας του αποστολέα (πιστοποίηση). Για τη διαδικασία της ανταλλαγής μηνυμάτων, αρχικά ο αποστολέας κρυπτογραφεί τα δεδομένα με το δημόσιο κλειδί του παραλήπτη και στη συνέχεια ο παραλήπτης τα αποκρυπτογραφεί με το ιδιωτικό του κλειδί. Για την πιστοποίηση του αποστολέα, ο αποστολέας κρυπτογραφεί τα δεδομένα με το ιδιωτικό του κλειδί, ενώ ο παραλήπτης τα αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα.

Η ασύμμετρη κρυπτογραφία μπορεί να χρησιμοποιηθεί σε εφαρμογές ηλεκτρονικής διακυβέρνησης για την παροχή υπηρεσιών όπως είναι η εγγραφή στις πλατφόρμες, η δημιουργία κλειδιών και η πιστοποίηση για όλους τους δημοσίους υπαλλήλους και τους πολίτες που τις χρησιμοποιούν (Kaliontzoglou et al., 2005).

Η ηλεκτρονική υπογραφή αποτελείται από δεδομένα σε ηλεκτρονική μορφή τα οποία συσχετίζονται λογικά με άλλα ηλεκτρονικά δεδομένα και χρησιμοποιείται από τον υπογράφοντα για την τοποθέτηση της υπογραφής του. Έχει την ίδια νομική θέση με τη χειρόγραφη υπογραφή εφόσον ικανοποιεί τις απαιτήσεις του ρυθμιστικού πλαισίου υπό το οποίο δημιουργήθηκε (για την Ευρωπαϊκή Ένωση είναι το πλαίσιο eIDAS) (EU, 2014).

Η ψηφιακή υπογραφή είναι ένα μαθηματικό σχήμα για την τεκμηρίωση της γνησιότητας των ψηφιακών μηνυμάτων ή εγγράφων. Μία έγκυρη ψηφιακή υπογραφή δίδει στον παραλήπτη μία επαρκή εγγύηση για το ότι το μήνυμα έχει δημιουργηθεί από έναν γνωστό αποστολέα (πιστοποίηση), για το ότι ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή του μηνύματος (μη αποκύρηξη), καθώς και για το ότι το μήνυμα δεν αλλοιώθηκε κατά τη μετάδοση του (ακεραιότητα). Οι ψηφιακές υπογραφές αποτελούν συστατικό στοιχείο των περισσότερων κρυπτογραφικών πρωτοκόλλων, ενώ χρησιμοποιούνται συχνά για τη δημιουργία ηλεκτρονικών υπογραφών. Δημιουργούνται με τη βοήθεια της ασύμμετρης κρυπτογραφίας.

2.4.3. Κρυπτογραφία στα πλαίσια της ηλεκτρονικής διακυβέρνησης

Οι Lambrinoudakis et al. (2003) πρότειναν τη χρήση της ασύμμετρης κρυπτογραφίας για την προστασία δεδομένων υπηρεσιών ηλεκτρονικής διακυβέρνησης. Στην προσέγγιση τους θεώρησαν διάφορες υπηρεσίες (μάθηση εξ αποστάσεως, ηλεκτρονική ψηφοφορία, ηλεκτρονική διασύνδεση διαφόρων κυβερνητικών υπηρεσιών μέσω e-mail, τηλεδιασκέψεων, διαμοιρασμένων εγγράφων, συναλλαγές μεταξύ πολιτών και υπηρεσιών, όπως είναι η έκδοση πιστοποιητικών γεννήσεως, η υποβολή φορολογικών δηλώσεων, η πραγματοποίηση ηλεκτρονικών πληρωμών) ως συνιστώσες μίας ενιαίας πλατφόρμας. Με τον τρόπο αυτό επιτυγχάνεται η εισαγωγή μέτρων ασφαλείας τα οποία είναι εφαρμόσιμα για όλη την πλατφόρμα, χωρίς να απαιτείται ξεχωριστός σχεδιασμός για την κάθε συνιστώσα. Η είσοδος στην ενιαία πλατφόρμα πραγματοποιείται μέσω ενός κοινού portal.

Αναφορικά με τον προσδιορισμό των απαιτήσεων ασφαλείας, ακολούθησαν μία μεθοδολογία (Gritzalis et al., 2002, στων Lambrinoudakis et al., 2003), σύμφωνα με την οποία για κάθε επιμέρους υπηρεσία της πλατφόρμας καθορίζεται μία σειρά

κινδύνων, οι οποίοι στη συνέχεια αξιολογούνται ανάλογα με τον βαθμό επικινδυνότητας τους. Οι κυριότερες απαιτήσεις που εντοπίστηκαν παρατίθενται παρακάτω (Lambrinoudakis et al., 2003):

1. Ηλεκτρονική μάθηση:
    - Διασφάλιση της λειτουργικότητας του συστήματος και της εξυπηρέτησης του μέγιστου αριθμού φοιτητών, χωρίς να προκύψουν ζητήματα που σχετίζονται με αδυναμία εξυπηρέτησης ή εξασθένηση των επιδόσεων της σχετικής υπηρεσίας.
    - Υλοποίηση κατάλληλων μηχανισμών πιστοποίησης για τους εξουσιοδοτημένους χρήστες.
    - Διασφάλιση της ακεραιότητας και της εμπιστευτικότητας του εκπαιδευτικού υλικού που παρέχεται στους φοιτητές και προέρχεται από εκείνους, καθώς και των πληροφοριών που δημιουργούνται μέσω της επικοινωνίας των φοιτητών με τη χρήση της πλατφόρμας. Επιπρόσθετα, πρέπει να διασφαλίζεται η προέλευση, η υποβολή και η παράδοση των δεδομένων όταν υπάρχει ανταλλαγή εκπαιδευτικού υλικού μεταξύ των φοιτητών και των εκπαιδευτών. Μία ακόμα απαίτηση είναι η διατήρηση της διάρκειας σύνδεσης του κάθε χρήστη και η καταγραφή των δεδομένων της κάθε συνεδρίας ούτως ώστε να αποφευχθούν πιθανές αμφισβητήσεις των εκπαιδευτικών διαδικασιών.
    - Μετά το πέρας της εκπαιδευτικής διαδικασίας τα προσωπικά δεδομένα των φοιτητών θα πρέπει να αποθηκεύονται ασφαλώς, ούτως ώστε να μην αποκτήσουν πρόσβαση σε αυτά μη εξουσιοδοτημένοι χρήστες.
2. Ηλεκτρονική ψηφοφορία:
    - Προκειμένου να μπορέσει ο οποιοσδήποτε χρήστης (ψηφοφόρος ή μέλος εφορευτικών επιτροπών) να εισέλθει στο σύστημα θα πρέπει να πιστοποιείται. Επιπρόσθετα οι δράσεις των μελών της εφορευτικής επιτροπής καθώς και των κρατικών αξιωματούχων οι οποίοι έχουν

αναλάβει τη διεξαγωγή της ψηφοφορίας θα πρέπει να καταγράφονται.

- Κατά τη φάση της ψηφοφορίας οι κυριότερες απαιτήσεις είναι η διασφάλιση της ανωνυμίας, της εμπιστευτικότητας, της ακεραιότητας και του ότι το κάθε άτομο θα ψηφίσει μόνο μία φορά.
- Κατά τη φάση της καταμέτρησης πρέπει να διασφαλιστεί η ακεραιότητα των δεδομένων. Αυτό μπορεί να επιτευχθεί μέσω της συμμετοχής και παρουσίας αντιπροσώπων όλων των πλευρών που εμπλέκονται στην ψηφοφορία. Μετά την καταμέτρηση πρέπει να διασφαλιστεί η ασφαλής αποθήκευση των αποτελεσμάτων και άλλων στοιχείων της εκλογικής διαδικασίας.

3. Διασύνδεση κυβερνητικών υπηρεσιών: Οι κυριότερες απαιτήσεις ασφαλείας σχετίζονται με τη διαθεσιμότητα του συστήματος, τη διαχείριση των προνομίων πρόσβασης του κάθε χρήστη, την πιστοποίηση, την εμπιστευτικότητα και την ακεραιότητα και την ασφαλή αποθήκευση των δεδομένων.
4. Συναλλαγές μεταξύ πολιτών και υπηρεσιών: Οι κυριότερες απαιτήσεις ασφαλείας σχετίζονται με τη διασφάλιση της διαθεσιμότητας του συστήματος, τη διαχείριση των προνομίων πρόσβασης των χρηστών, την πιστοποίηση, την ακεραιότητα, την εμπιστευτικότητα, τη μη αποκύρηξη ενεργειών που έχουν πραγματοποιηθεί, την καταγραφή των δράσεων των χρηστών, καθώς και την ασφαλή αποθήκευση των δεδομένων.

Οι Lambrinoudakis et al. (2003) αναφέρουν ότι ορισμένες από τις απαιτήσεις της ηλεκτρονικής διακυβέρνησης δεν μπορούν να καλυφθούν από την ασύμμετρη κρυπτογραφία. Προτείνουν (συναρτήσει και των ειδικών απαιτήσεων του περιβάλλοντος) την υιοθέτηση μέτρων όπως είναι η χρήση εφεδρικών servers και τηλεπικοινωνιακών γραμμών, συμβάσεων παροχής υπηρεσιών, διαδικασιών ελέγχου για την επίλυση ζητημάτων που σχετίζονται με την αξιοπιστία του υλισμικού, τους περιορισμένους υπολογιστικούς πόρους, τις υποδομές επικοινωνιών, την αξιοπιστία του λογισμικού, τη συντήρηση. Για την ικανοποίηση των ειδικών απαιτήσεων ασφαλείας των εφαρμογών ηλεκτρονικής ψηφορορίας, όπως είναι η ανωνυμία, το αδιάβλητο της διαδικασίας, η μυστικότητα της ψηφοφορίας και η

επαλήθευση προτείνεται η χρήση ενός ειδικού πρωτοκόλλου ψηφοφορίας το οποίο έχει σχεδιαστεί για τη συγκεκριμένη διαδικασία.

Οι Kaliontzoglou et al. (2005) αναφέρουν ότι η εφαρμογή χαρακτηριστικών ασφαλείας (για παράδειγμα, ψηφιακών υπογραφών) σε ιστοσελίδες εφαρμογών ηλεκτρονικής διακυβέρνησης είναι μία δύσκολη διαδικασία, λόγω της περιορισμένης λειτουργικότητας των διαδικτυακών φυλλομετρητών. Προτείνουν μία διαφορετική προσέγγιση, τη χρήση πλατφορμών ηλεκτρονικής διακυβέρνησης με κατανεμημένες συνιστώσες (όπως είναι ειδικές εφαρμογές, πύλες, εξυπηρετητές εφαρμογών, βάσεις δεδομένων). Η συγκεκριμένη προσέγγιση προσομοιάζει με εκείνη των Lambrinoudakis et al. (2003).

Για την ασφαλή δημιουργία και διανομή των ηλεκτρονικών δημοσίων εγγράφων (όπου χρειάζεται να ικανοποιούνται η πιστοποίηση, η ακεραιότητα, η εμπιστευτικότητα και η μη αποκύρηξη) προτείνεται (Kaliontzoglou et al., 2005) η χρήση εφαρμογών κρυπτογραφίας, πιο συγκεκριμένα των ψηφιακών υπογραφών, της κρυπτογράφησης και της χρονικής σήμανσης. Επιπρόσθετα, χρησιμοποιώντας το ευρωπαϊκό πρότυπο ηλεκτρονικών υπογραφών XAdES παρέχουν διασφάλιση της μακροπρόθεσμης εγκυρότητας των ηλεκτρονικών υπογραφών (κάτι σημαντικό, καθώς τα υπογεγραμμένα δημόσια έγγραφα ενδέχεται να φέρουν υπογραφές οι οποίες διαρκούν για πολλές δεκαετίες). Στον σχεδιασμό τους προβλέπεται και η μακροπρόθεσμη αποθήκευση των ψηφιακών εγγράφων, ούτως ώστε αυτά να είναι διαθέσιμα στο αρχείο για μεγάλες χρονικές περιόδους, με τη χρήση προηγμένων κρυπτογραφικών λειτουργιών στα συστήματα των βάσεων δεδομένων. Με τη χρήση της ασύμμετρης κρυπτογραφίας διασφαλίζεται η εμπιστοσύνη στο σύστημα σε τοπικό, εθνικό και διεθνές επίπεδο. Ένα ακόμα χαρακτηριστικό της είναι ο αυστηρός έλεγχος πρόσβασης, μέσω του οποίου καθορίζεται το ποιοι μπορούν να πραγματοποιήσουν κάθε δράση, το πότε μπορούν να την πραγματοποιήσουν και με τη χρήση ποιών πόρων, ενώ προβλέπεται και μία απλή λειτουργία σύνδεσης, μέσω της οποίας ένας χρήστης μπορεί να συνδεθεί στο σύστημα και να αποκτήσει πρόσβαση σε διάφορες εφαρμογές.

Το πρότυπο XAdES που χρησιμοποιήθηκε για τη δημιουργία των ηλεκτρονικών υπογραφών διασφαλίζει τη μακροπρόθεσμη εγκυρότητα των αποθηκευμένων

εγγράφων, αλλά ενδέχεται να απαιτήσει αυξημένο αποθηκευτικό χώρο. Για την αντιμετώπιση του συγκεκριμένου ζητήματος συνίσταται (Kaliontzoglou et al., 2005) η προσεκτική εξέταση του υλικού που θα αποθηκεύεται ούτως ώστε να υπογράφεται μόνο υλικό το οποίο είναι αναγκαίο να διατηρηθεί για μεγάλες χρονικές περιόδους. Τέτοιου είδους περιορισμοί αποτελούν μέρος των γενικότερων πολιτικών ασφαλείας οι οποίες ρυθμίζουν τη λειτουργία τέτοιου είδους πλατφόρμων και πρέπει να καθορίζονται πριν την ανάπτυξη τους (Kaliontzoglou et al., 2005).

Επίσης, κατά τη συνεργασία των διαφόρων υπηρεσιών ανταλλάσσονται ευαίσθητα δεδομένα ασφαλείας. Προκειμένου να προστατευτούν οι χρήστες από τη διπλή αποστολή των ίδιων δεδομένων ασφαλείας προτείνεται (Kaliontzoglou et al., 2005) η χρήση του προτύπου ανταλλαγής δεδομένων πιστοποίησης και εξουσιοδότησης SAML (Security Assertion Markup Language).

Κεφάλαιο 3

3. Κουλτούρα ασφαλείας και ηλεκτρονική διακυβέρνηση στην Ευρώπη

3.1. Κουλτούρα ασφαλείας οργανισμού

Έχει εξετασθεί εκτενώς ο σημαίνων ρόλος που διαδραματίζουν οι εργαζόμενοι ενός οργανισμού στην επίτευξη ενός συνολικού επιπέδου ασφαλείας σε αυτόν (Karyda, 2010), με αποτέλεσμα να προσδιοριστεί ένα σύνολο παραγόντων οι οποίοι σχηματίζουν τόσο τη συμπεριφορά των εργαζομένων σχετικά με την ασφάλεια (αντιλήψεις, αξίες, συνήθειες, γνώσεις, επίγνωση ασφαλείας κλπ.) όσο και τις συνθήκες του οργανωσιακού περιβάλλοντος (διαθεσιμότητα πόρων, οργανωσιακή αφοσίωση, νόρμες κλπ.).

Σύμφωνα με έναν γενικό ορισμό, κουλτούρα ασφαλείας είναι το σύνολο των απόψεων, αντιλήψεων και αξιών που μοιράζεται το προσωπικό ενός οργανισμού, όπως είναι ένας εργασιακός χώρος ή μία κοινότητα (Cox και Cox, 1991). Η έρευνα της κουλτούρας ασφαλείας σε επίπεδο οργανισμού και επικεντρώνοντας στα πληροφοριακά συστήματα και τις ηλεκτρονικές τεχνολογίες, βασίζεται κατά έναν μεγάλο βαθμό στην υπόθεση του ότι εαν τα διοικητικά στελέχη του οργανισμού έχουν τη δυνατότητα ελέγχου ή πρόβλεψης της κουλτούρας ασφάλειας πληροφοριών του οργανισμού, τότε μπορούν να διαχειριστούν αποτελεσματικότερα την ασφάλεια πληροφοριών του οργανισμού τους (Da Veiga και Eloff, 2009, στης Karyda, 2017), ενώ επικεντρώνει κατά κύριο λόγο στην αλλαγή των βασικών απόψεων των εργαζομένων, ούτως ώστε εκείνοι να ενστερνιστούν τις αξίες ασφαλείας που εφαρμόζονται στις πολιτικές ασφάλειας πληροφοριών (Vroom και Von Solms, 2004, στης Karyda, 2017). Υπό το συγκεκριμένο πρίσμα, η κουλτούρα ασφαλείας έχει περιγραφεί ως η ιδανική κατάσταση συμμόρφωσης με την πολιτική ασφαλείας του οργανισμού (Furnell και Thomson, 2009, στης Karyda, 2017).

Υπό μία διαφορετική οπτική (Martins και Eloff, 2002, Da Veiga et al., 2007, Dhillon, 1997, Helokunnas και Kuusisto, 2003, Straub, 2002, στης Karyda, 2017), η κουλτούρα

ασφαλείας θεωρείται ως το αποτέλεσμα της αλληλεπίδρασης των εργαζομένων με τα στοιχεία ελέγχου της ασφάλειας των πληροφοριών (κωδικοί, αντιϊκά λογισμικά κοκ.). Υπό το συγκεκριμένο πρίσμα η κουλτούρα ασφαλείας πληροφοριών ορίζεται (Martins και Eloff, 2002, Da Veiga, 2007, στης Karyda, 2017) ως οι αντιλήψεις, στάσεις και υποθέσεις που σχετίζονται με την ασφάλεια των πληροφοριών και ενθαρρύνονται και υιοθετούνται σε έναν οργανισμό. Σύμφωνα με τον Dhillon (1997, στης Karyda, 2017) κουλτούρα ασφαλείας είναι οι συμπεριφορές, αξίες και υποθέσεις οι οποίες συμβάλλουν στη διατήρηση της ασφάλειας των πληροφοριών. Οι Helokunnas και Kuusisto (2003, στης Karyda, 2017) προσεγγίζουν το εν λόγω ζήτημα ως ένα σύστημα στο οποίο οι στάσεις, τα κίνητρα, οι γνώσεις και τα νοητικά μοντέλα που σχετίζονται με την ασφάλεια των πληροφοριών αλληλεπιδρούν μεταξύ τους. Ο Straub (2002, στης Karyda, 2017) χρησιμοποιεί τη θεωρία της κοινωνικής ταυτότητας για την κατανόηση της κουλτούρας ασφαλείας, τεκμηριώνοντας το σκεπτικό του με το γεγονός του ότι τα άτομα επηρεάζονται από διαφορετικές κουλτούρες, ενώ αναμένεται να επηρεαστούν και από τις ηθικές αξίες, την εθνική νομοθεσία και την οργανωτική δομή.

Ένας ορισμός της ασφάλειας πληροφοριών ο οποίος θα μπορούσε να συνδεθεί με τις εφαρμογές της ηλεκτρονικής διακυβέρνησης είναι εκείνος ο οποίος την ορίζει ως την αποτελεσματική εφαρμογή προτύπων ασφαλείας και πολιτικών για την προστασία των πληροφοριών των δημόσιων οργανισμών. Η υιοθέτηση ορισμένων σχετικών προτύπων συμμόρφωσης διασφαλίζει ότι οι μηχανισμοί ασφαλείας θα μπορούν να συνεργάζονται και να συντονίζονται μεταξύ τους ούτως ώστε να προστατεύονται οι κρίσιμες πληροφορίες (AlKalbani et al., 2015).

Οι στάσεις και οι συμπεριφορές των εργαζομένων στις υπηρεσίες που εφαρμόζουν την ηλεκτρονική διακυβέρνηση καθορίζονται από οργανωτικούς παράγοντες, όπως είναι η διαδικασία επικοινωνίας και η διαχείριση από την ανώτατη διοίκηση (AlKalbani et al., 2015). Ως περιβαλλοντικός παράγοντας θα μπορούσαν να αναφερθούν οι εξωτερικές πιέσεις που δέχεται ένας δημόσιος οργανισμός σχετικά με τις απαιτήσεις ασφαλείας του κοινού, για να ανταπεξέλθει στις οποίες καταβάλλει εσωτερική προσπάθεια (AlKalbani et al., 2015).

Η κουλτούρα ασφαλείας ενός οργανισμού θα μπορούσε να συνοψιστεί στη διάθεση των εργαζομένων σε εκείνον να συμμορφωθούν με τα εφαρμοζόμενα πρότυπα και πολιτικές που σχετίζονται με την ασφάλεια των πληροφοριών (McIlwraith, 2006, στου AlKalbani, 2015). Ένας σημαντικός κίνδυνος προς την εμφύσηση της είναι το να θεωρήσουν οι εργαζόμενοι την ασφάλεια ως μία απλή πτυχή της καθημερινής τους εργασίας (Oost και Chew, 2007, στου AlKalbani, 2015). Οι τρεις κυριότεροι παράγοντες που συμβάλουν καθοριστικά στον σχηματισμό της κουλτούρας αυτής είναι η αφοσίωση της διοίκησης, η ευθύνη και η ενημέρωση σχετικά με την ασφάλεια των πληροφοριών (AlKalbani, 2015).

Η αφοσίωση της διοίκησης αφορά τις προσπάθειες που καταβάλλονται από την ανώτατη διοίκηση ούτως ώστε να υπάρξει συμμόρφωση με τις απαιτήσεις της ασφάλειας των πληροφοριών (Kajava et al., 2007, στου AlKalbani, 2015). Μπορεί να μετρηθεί εξετάζοντας τις αντιλήψεις των εργαζομένων αναφορικά με τη στάση της διοίκησης πάνω σε αυτό το ζήτημα (διοικητική υποστήριξη και εμπλοκή, ανάθεση στόχων, αποτελεσματικότητα). Η διοικητική υποστήριξη σχετίζεται με τις αποφάσεις, επενδύσεις και δράσεις που έχουν ληφθεί για την εφαρμογή πολιτικών ασφαλείας κατά μήκος ενός οργανισμού. Η διοικητική εμπλοκή αφορά τον βαθμό κατά τον οποίο η ανώτατη διοίκηση συμμετέχει στην επίλυση ζητημάτων τα οποία σχετίζονται με την ασφάλεια. Η ανάθεση στόχων αφορά τη σύνδεση μεταξύ των πολιτικών ασφαλείας πληροφοριών και των οργανωτικών στόχων. Η αποτελεσματικότητα σχετίζεται με τον βαθμό κατά τον οποίο ένας οργανισμός είναι ικανός να διαχειρίζεται δραστηριότητες που σχετίζονται με την ασφάλεια των πληροφοριών, περιλαμβάνοντας τόσο το κατά πόσο οι σχετικές πολιτικές συμβαδίζουν με τις σύγχρονες απαιτήσεις ασφαλείας όσο και την επικοινωνία αυτών των πολιτικών και διαδικασιών στο προσωπικό του οργανισμού (AlKalbani, 2015).

Η αφοσίωση της διοίκησης αποτελεί το σημείο εκκίνησης της διαδικασίας εμφύσησης μίας κουλτούρας ασφαλείας σε έναν οργανισμό. Στη συνέχεια, προσδιορίζονται η τωρινή και η επιθυμητή κατάσταση, υλοποιούνται δράσεις εκπαίδευσης των εργαζομένων και αξιολογείται η αλλαγή των στάσεων μέσα από διάφορους δείκτες (Karyda, 2017). Έχει διατυπωθεί ένα σύστημα μέτρησης της αποτελεσματικότητας της κουλτούρας ασφαλείας, το οποίο περιλαμβάνει την πίστη

στη σημασία της ασφάλειας των πληροφοριών, τους στόχους, τις πολιτικές, τις διαδικασίες και τις διεργασίες συνεχούς βελτίωσης, τη συνεργασία, καθώς και την προσοχή που δίδεται στην παρακολούθηση της ικανοποίησης των στόχων (Chia, 2002, στης Karyda, 2017). Μία άλλη πρόταση συνίσταται στη θεμελίωση μίας κουλτούρας εκπαίδευσης και συνεργασίας με τους εργαζόμενους υπό το πρίσμα της σταδιακής υιοθέτησης της διαχείρισης ασφάλειας, των αξιών και των συμπεριφορών σχετικά με τη χρήση των τεχνολογιών που διέπουν τον οργανισμό (Vroom και Von Solms, 2004, στης Karyda, 2017). Επιπρόσθετα, αναφέρεται (Kolowska, 2011, στης Karyda, 2017) η ύπαρξη διαφορετικών υπό-κουλτουρών ασφαλείας εντός του ιδίου οργανισμού, γεγονός το οποίο αποδίδεται σε διαφορετικές υποβόσκουσες, ακόμα και αντίθετες μεταξύ τους, αξίες.

Η ευθύνη συνίσταται στα μέτρα που έχουν ληφθεί για την προώθηση των ευθυνών που έχουν τα άτομα για την εφαρμογή των προτύπων και πολιτικών ασφαλείας στους οργανισμούς (Herath και Rao, 2009, στου AlKalbani, 2015). Ένας δείκτης της είναι η αντίληψη του προσωπικού του οργανισμού σχετικά με την περιεκτικότητα των πολιτικών που σχετίζονται με την εμφύσηση συμπεριφορών που συνεισφέρουν στην ασφάλεια, τη σαφήνεια και την κατανόηση των ρόλων και των ευθυνών, την καταλληλότητα των κυρώσεων που επιβάλλονται στην περίπτωση της παραβίασης των πολιτικών ασφαλείας, καθώς και την εφαρμογή πολιτικών ασφάλειας πληροφοριών και σχετικών διαδικασιών κατά μήκος του οργανισμού (AlKalbani, 2015).

Η ευθύνη αποτελεί ένα από τα πλέον αποτελεσματικά στοιχεία σχετικά με την εμφύσηση μίας δυναμικής κουλτούρας ασφαλείας στο προσωπικό ενός οργανισμού (Posthumus και Von Solms, 2004, στου AlKalbani, 2015). Εάν οι προβλεπόμενες κυρώσεις δεν εφαρμοστούν αναλόγως, τα άτομα δεν θα αναμένουν κάποια συνέπεια στην περίπτωση κατά την οποία παραβιάσουν τις πολιτικές ασφαλείας (Adams και Sasse, 1999, στου AlKalbani, 2015). Επίσης, τα άτομα με καλά ορισμένους ρόλους και ευθύνες δραστηριοποιούνται περισσότερο ενεργά στη λήψη προληπτικών μέτρων ασφαλείας (Ryan, 2005, στου AlKalbani, 2015).

Η ενημέρωση αφορά την υλοποίηση προγραμμάτων ασφαλείας για την αύξηση των σχετικών γνώσεων του υπαλλήλου που χειρίζεται τις σχετικές εφαρμογές και την

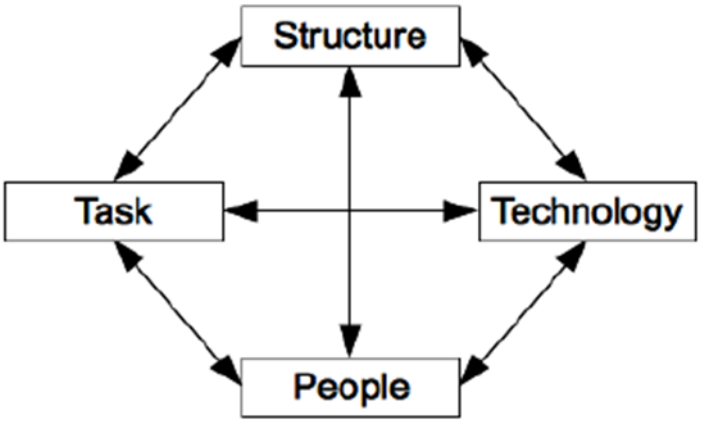
κατανόηση των πολιτικών και μηχανισμών ασφαλείας των οργανισμών (Smith και Jamieson, 2006, στου AlKalbani, 2015). Μπορεί να μετρηθεί μέσω των αντιλήψεων του προσωπικού σχετικά με τα χαρακτηριστικά των σχετικών εκπαιδευτικών προγραμμάτων. Οι αντιλήψεις αυτές αντανακλούν τον αντίκτυπο που έχει δημιουργηθεί από το εύρος και την ποικιλία των προγραμμάτων που έχουν υλοποιηθεί για την υποστήριξη των στόχων ασφαλείας ενός οργανισμού, ενώ η γνώμη τους σχετικά με τη χρησιμότητα των προγραμμάτων αποτελεί έναν δείκτη του κατά πόσο καλά δομημένα και παρουσιασμένα είναι αυτά.

Η ανάπτυξη μίας κουλτούρας ασφαλείας στους πολίτες μίας χώρας διαδραματίζει έναν σημαίνοντα ρόλο στη διαδικασία του τεχνολογικού εκσυγχρονισμού. Σύμφωνα με τους Malmedal και Røislien (2016), δεν αρκούν μόνο οι σχετικές τεχνολογικές εφαρμογές ούτως ώστε να πραγματοποιηθούν βήματα προς τη συγκεκριμένη κατεύθυνση, αλλά αναφέρεται και η σημασία που έχουν οι στάσεις των πολιτών και των εργαζομένων. Ο τρόπος με τον οποίο εκείνοι αντιλαμβάνονται τους κινδύνους που συνδέονται με τις ψηφιακές τεχνολογίες, αλλά και οι στάσεις και οι γνώσεις τους σχετικά με την προστασία από αυτούς συνιστούν έναν κομβικό παράγοντα ο οποίος επηρεάζει σημαντικά τη διαδικασία της ψηφιοποίησης των υπηρεσιών. Η πλέον ανεπιθύμητη εξέλιξη για μία χώρα θα ήταν η διάχυση μίας φοβίας προς την τεχνολογία στον πληθυσμό της, γεγονός το οποίο θα την εμπόδιζε από το να καρπωθεί τα οφέλη που προκύπτουν από αυτήν. Ως σχετικοί κίνδυνοι αναφέρονται (Malmedal και Røislien, 2016) η έλλειψη εμπιστοσύνης προς το δημόσιο αναφορικά με την ικανότητα διαφύλαξης των προσωπικών δεδομένων, καθώς και η αδυναμία κατανόησης των πραγματικών απειλών που σχετίζονται με τις ηλεκτρονικές δραστηριότητες, γεγονός το οποίο θα μπορούσε να οδηγήσει είτε σε υπερβολική χρήση μέτρων ασφαλείας, τα οποία ενδέχεται να αποτελέσουν τροχοπέδη στη διαδικασία της ψηφιακής αναβάθμισης, είτε στη χρήση ανεπαρκών μέτρων λόγω ελλιπούς κατανόησης η οποία οδηγεί σε ανεπαρκή σχεδιασμό. Γενικότερα, τονίζεται η τεράστια σημασία του ανθρώπινου παράγοντα για την ασφάλεια των διαδικτυακών εφαρμογών. Γίνεται αναφορά στη σημασία της διατύπωσης ενός συστήματος μέτρησης του επιπέδου της κουλτούρας ασφαλείας σε εθνικό επίπεδο, ενώ τονίζεται η καθοριστική της συμβολή στην εκμετάλλευση των διευκολύνσεων που μπορούν να

παρέχουν οι ψηφιακές τεχνολογίες από τους πολίτες και στην οικονομική ανάπτυξη μίας χώρας. Ως σύγχρονες προκλήσεις στην αντιμετώπιση των οποίων μπορεί να συμβάλει η ανάπτυξη μίας στέρεας κουλτούρας ασφαλείας αναφέρονται η έλλειψη εμπιστοσύνης στις ψηφιακές υπηρεσίες και ο φόβος του ηλεκτρονικού εγκλήματος (Malmedal και Røislien, 2016).

3.2. Η σημασία του ανθρώπινου παράγοντα στην ανάπτυξη μίας κουλτούρας ασφαλείας

Η εμφύσηση μίας κουλτούρας ασφαλείας στους χρήστες των υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι άρρηκτα συνδεδεμένη με τον ανθρώπινο παράγοντα, καθώς αντικείμενο της είναι τα άτομα που χρησιμοποιούν τις εφαρμογές αυτές και οι στάσεις τους. Προκειμένου να γίνει κατανοητό το παραπάνω και εάν λάβουμε υπόψη μας ότι η ηλεκτρονική διακυβέρνηση αποτελεί συστατικό στοιχείο του κρατικού μηχανισμού, ο οποίος αποτελεί μία οργάνωση, θα παραθέσουμε την έννοια της οργάνωσης σύμφωνα με τον Leavitt (1965). Υπό την προσέγγιση του λοιπόν, μία οργάνωση αποτελείται από τέσσερεις αλληλεπιδρώσες συνιστώσες: τη δομή, την τεχνολογία, τον άνθρωπο και τις διαδικασίες (Leavitt, 1965). Συνεπώς, ο ρόλος του ανθρώπινου παράγοντα είναι θεμελιώδους σημασίας. Σύμφωνα με τη Διεθνή Τηλεπικοινωνιακή Ένωση (International Telecommunication Union – ITU) η δημιουργία μίας κουλτούρας ασφαλείας αποτελεί αναγκαίο παράγοντα για την επίτευξη της ασφάλειας πληροφοριών (Karyda, 2017). Στον οδηγό για τη διαδικτυακή ασφάλεια που εξέδωσε το 2011 προτρέπει τα μέλη των Ηνωμένων Εθνών να στηρίξουν τις στρατηγικές ασφαλείας τους στις εθνικές τους αξίες, καθώς η κουλτούρα και τα εθνικά συμφέροντα επηρεάζουν τον τρόπο με τον οποίο οι άνθρωποι αντιλαμβάνονται τους κινδύνους, ενώ μέσα από τη συγκεκριμένη προσέγγιση θα αυξηθεί η υποστήριξη του δικαστικού σώματος. Για την προώθηση της κουλτούρας ασφαλείας, αλλά και των σχετικών συμπεριφορών και εργαλείων προτείνεται και η σύμπραξη δημοσίου και ιδιωτών.



Εικόνα 3 – Η έννοια της οργάνωσης σύμφωνα με τον Leavitt (Williams et al., 2013)

Η σημασία που δίδεται στον ανθρώπινο παράγοντα δικαιολογείται από το γεγονός του ότι επί της ουσίας η κουλτούρα ασφαλείας είναι άμεσα συνδεδεμένη με τις συμπεριφορές και δράσεις του προσωπικού των οργανισμών (Malmedal και Røislien, 2016). Μάλιστα, κατά τη μέτρηση και αξιολόγηση της θα πρέπει να υπάρχει ξεχωριστός σχεδιασμός ανά κατηγορία ατόμων, καθώς κάθε κατηγορία εμπίπτει σε διαφορετικές πτυχές της κουλτούρας ασφαλείας.

Σε συνέχεια των παραπάνω, έχει αυξηθεί η σημασία που δίδεται στην ανάπτυξη μίας κουλτούρας ασφαλείας (Malmedal και Røislien, 2016), καθώς όλοι οι ειδικοί συμφωνούν ότι οι τεχνολογικές εξελίξεις δεν αρκούν από μόνες τους για τη δημιουργία ενός ασφαλούς περιβάλλοντος. Η αλληλεπίδραση ανθρώπου και τεχνολογίας αποτελεί τον ακρογωνιαίο λίθο για την επίτευξη της ασφάλειας των πληροφοριών. Η κουλτούρα ασφαλείας μπορεί να διαχωριστεί σε δύο κύριες αλληλοσυνδεόμενες πτυχές (Malmedal και Røislien, 2016): σύμφωνα με την πρώτη από αυτές, αποτελεί ένα εργαλείο το οποίο συμβάλλει στη βελτίωση των επιδόσεων του οργανισμού, ενώ σύμφωνα με τη δεύτερη αποτελεί το άθροισμα των τρόπων συμπεριφοράς του προσωπικού του οργανισμού. Υπό ένα γενικότερο πρίσμα, θα μπορούσε να θεωρηθεί ως πρότυπα συμπεριφορών τα οποία επιδέχονται βελτιώσεων ούτως ώστε να αυξηθεί η προστιθέμενη αξία του οργανισμού.

Το Νορβηγικό Κέντρο για την Ασφάλεια των Πληροφοριών διεξήγαγε έρευνα σχετικά με την κουλτούρα διαδικτυακής ασφαλείας στη χώρα αποσκοπώντας στη μέτρηση του επιπέδου της ούτως ώστε να αναπτυχθούν αποτελεσματικές πρακτικές ασφαλείας και να βελτιωθεί η προστασία της χώρας από σχετικούς κινδύνους

(Karyda, 2017). Βρέθηκαν οκτώ κύριοι παράγοντες οι οποίοι καθορίζουν το επίπεδο της κουλτούρας ασφαλείας. Η συλλογικότητα, δηλαδή το κατά πόσο τα άτομα θεωρούν τους εαυτούς τους ως μέλη ενός μεγαλύτερου συνόλου. Η διακυβέρνηση και ο έλεγχος, δηλαδή το ρυθμιστικό πλαίσιο που σχετίζεται με τις Τεχνολογίες Πληροφορίας και Επικοινωνιών. Η εμπιστοσύνη που έχουν οι πολίτες στις κυβερνήσεις, τους οργανισμούς κλπ. Οι αντιλήψεις των κινδύνων, οι οποίες αφορούν την πιθανότητα τα άτομα να υιοθετήσουν επικίνδυνες συμπεριφορές. Η αισιοδοξία σχετικά με τις τεχνολογικές εξελίξεις, η οποία αφορά τις στάσεις των πολιτών προς την ψηφιοποίηση. Οι δεξιότητες, δηλαδή οι ψηφιακές ικανότητες των πολιτών. Το ενδιαφέρον, δηλαδή ο βαθμός κατά τον οποίο οι πολίτες ενδιαφέρονται για τις ΤΠΕ. Τελευταίος παράγοντας ήταν η συμπεριφορά, η οποία αφορά τα πρότυπα συμπεριφορών των πολιτών αναφορικά με τη διαδικτυακή ασφάλεια καθώς και το επίπεδο της εκπαίδευσης πάνω στην ασφάλεια που εκείνου λαμβάνουν. Η έρευνα καταλήγει στο ότι η κατάλληλη εκπαίδευση είναι ιδιαιτέρως σημαντική (μάλιστα αναφέρεται ότι μία από τις σημαντικότερες αδυναμίες της νορβηγικής κυβέρνησης είναι η αποτυχία της να διδάξει την πολύπλοκη αλληλεπίδραση που σημειώνεται μεταξύ της διαδικτυακής ασφάλειας σε ατομικό και κοινωνικό – εθνικό επίπεδο). Τονίζεται η σημασία που έχει η ανάληψη κρατικών πρωτοβουλιών προς τη συγκεκριμένη κατεύθυνση, καθώς η συμμόρφωση των ατόμων με τους εσωτερικούς κανονισμούς ασφαλείας των οργανισμών στους οποίους απασχολούνται δεν συνεπάγεται και ότι θα υιοθετήσουν αντίστοιχες στάσεις στα υπόλοιπα περιβάλλοντα που δραστηριοποιούνται.

3.3. Δυσκολίες και προοπτικές από την ανάπτυξη μίας κουλτούρας ασφαλείας

Έχει προσδιοριστεί (Karyda, 2017) μία σειρά εμποδίων αλλά και ευκαιριών που προέκυψαν σε διάφορους οργανισμούς κατά τη διαδικασία της ανάπτυξης μίας

κουλτούρας ασφαλείας. Τα κυριότερα από αυτά θα παρουσιαστούν σε αυτή την παράγραφο.

Το πρώτο από τα ζητήματα αυτά συνίσταται στο ότι η κουλτούρα ασφαλείας εφαρμόζεται σε διαφορετικά επίπεδα (άτομα, ομάδες εργασίας, ομάδες οι οποίες συνεργάζονται σε διαπροσωπικό ή διαδικτυακό επίπεδο, οργανισμούς, κοινότητες, χώρες). Κατά συνέπεια το περιεχόμενο της κουλτούρας ασφαλείας πρέπει κάθε φορά να προσαρμόζεται στις συνθήκες εφαρμογής του.

Ένα ακόμα ζήτημα που απαντάται συχνά, σύμφωνα με την Karyda (2017), είναι η σύγχυση που σημειώνεται συχνά μεταξύ κουλτούρας και συμπεριφοράς ασφαλείας. Η συμπεριφορά ασφαλείας έχει ως αντικείμενο της κατά κύριο λόγο τη συμμόρφωση με ορισμένους κανόνες και πολιτικές ασφαλείας. Ως εκ τούτου, το βάρος δίδεται εκεί, ενώ αγνοείται η ανάπτυξη μίας κουλτούρας.

Η όλη διαδικασία της ανάπτυξης μίας κουλτούρας ασφαλείας θα μπορούσε να αποτελέσει μία διαδικασία αυτό-μάθησης (Karyda, 2017), καθώς μπορεί να παρέχει σημαντική πληροφόρηση για τις οργανωτικές αξίες, νόρμες κλπ.

Εντός ενός οργανισμού ενδέχεται να υπάρχουν διαφορετικές κουλτούρες ασφαλείας (Kolkowska, 2011, στης Karyda, 2017). Κατά συνέπεια είναι αναγκαίος ο καθορισμός ρόλων και καθηκόντων ανά τμήμα και διοικητικό επίπεδο. Ιδιαίτερα σημαντικός χαρακτηρίζεται ο ρόλος των μεσαίων διοικητικών στελεχών, λόγω του ότι κατά τη διαδικασία λήψης αποφάσεων συχνά αξιολογούν τους κινδύνους ασφαλείας σε συνδυασμό με τα πιθανά επιχειρησιακά κέρδη. Επιπρόσθετα τα στελέχη που απασχολούνται στο τμήμα πληροφορικής πρέπει να έχουν έναν περισσότερο ενεργό ρόλο. Η ανώτατη διοίκηση πρέπει να καταστήσει σαφή τη σημασία της ασφάλειας και να την ενσωματώσει στους στόχους του οργανισμού, ούτως ώστε να προωθήσει μία κουλτούρα ασφαλείας. Στο λειτουργικό επίπεδο, τα άτομα πρέπει να κατανοήσουν τη σημασία της ασφάλειας και να συμπεριφέρονται με γνώμονα εκείνη.

Ένας ακόμα κίνδυνος προκύπτει από την ανάθεση εργασιών σε εξωτερικούς συνεργάτες (outsourcing). Κατά την Karyda (2017), μέσω της συγκεκριμένης πρακτικής οι οργανισμοί σημειώνουν απώλειες σε επίπεδο τεχνολογικής

εξειδίκευσης, γεγονός το οποίο θα μπορούσε να δημιουργήσει προβλήματα στην εμφύσηση μίας κουλτούρας ασφαλείας. Επιπρόσθετα, οι εργαζόμενοι που χρησιμοποιούν τις προσωπικές τους συσκευές κατά την εργασία τους θα πρέπει να εναρμονίσουν τη συμπεριφορά ασφαλείας τους με εκείνη του οργανισμού.

Επιπρόσθετα, πραγματοποιείται αναφορά (Karyda, 2017) στην επίδραση που έχει η εθνική κουλτούρα στη συμπεριφορά ασφαλείας των ατόμων. Ως σχετικό παράδειγμα αναφέρεται η διαφορά μεταξύ των συνεργατικών κοινωνιών (όπου οι εργαζόμενοι επηρεάζονται από τις προσδοκίες των συναδέλφων και ανωτέρων τους) και των ατομικών (όπου συμπεριφέρονται σύμφωνα με τη δική τους γνώμη).

3.4. Καλές πρακτικές για την ανάπτυξη της κουλτούρας ασφαλείας

Οι περισσότερες χώρες (και σχεδόν όλα τα μέλη του ΟΟΣΑ) (OECD, 2005) έχουν υιοθετήσει κάποια εθνική στρατηγική ούτως ώστε να ενισχύσουν την κουλτούρα ασφαλείας σε εθνικό επίπεδο. Οι προσεγγίσεις αυτές διέπονται από δύο κύρια χαρακτηριστικά στοιχεία, μία διεπιστημονική και συνεργατική μεταξύ των διαφόρων φορέων αντιμετώπιση του ζητήματος, καθώς και μία διοικητική δομή υψηλού επιπέδου.

Αναφορικά με το πρώτο χαρακτηριστικό, αποτελεί απόρροια του ότι, σε συμφωνία και με όσα αναφέραμε στις προηγούμενες παραγράφους, η κουλτούρα ασφαλείας δεν αποτελεί απλά ένα τεχνικό ζήτημα, αλλά διέπεται από κοινωνικο-οικονομικές και νομικές πτυχές και ως εκ τούτου είναι αναγκαία η συνεργασία των διαφόρων φορέων. Επιπρόσθετα, καθώς οι κρατικές δομές δεν μπορούν να αναλάβουν μόνες τους την αντιμετώπιση όλων των ζητημάτων που προκύπτουν, κρίνεται αναγκαία η εμπλοκή τόσο του ιδιωτικού τομέα όσο και των πολιτών (OECD, 2005). Ο τρόπος με τον οποίο υλοποιούνται οι συνεργασίες αυτές πάντως διαφέρει σε επίπεδο χωρών, κάτι το οποίο θα εξετάσουμε αναλυτικότερα στις μελέτες περιπτώσεων που θα παραθέσουμε στη συνέχεια της παρούσας εργασίας.

Όσον αφορά το δεύτερο χαρακτηριστικό, μπορεί να συνοψιστεί στο γεγονός του ότι η λήψη των αποφάσεων για την υλοποίηση των σχετικών πολιτικών συνήθως πραγματοποιείται από το υψηλότερο κυβερνητικό επίπεδο. Η αρμοδιότητα της υλοποίησης τους ανατίθεται είτε σε έναν οργανισμό ο οποίος έχει καθοριστεί από τον πρωθυπουργό της χώρας είτε σε κάποιο κυβερνητικό τμήμα ή υπουργείο (OECD, 2005).

Πέραν των νομοθετικών πρωτοβουλιών και της σύστασης ομάδων εργασίας πραγματοποιούνται και δράσεις οι οποίες αποσκοπούν στην αύξηση του κοινού αισθήματος για την αναγκαιότητα της ανάπτυξης μίας κουλτούρας ασφαλείας. Οι δράσεις αυτές συνήθως έχουν τη μορφή της πραγματοποίησης δημοσίων εκδηλώσεων (οι κυριότερες θεματικές ενότητες των οποίων συνήθως είναι η γενική πληροφόρηση σχετικά με ζητήματα ασφαλείας, η διαχείριση κινδύνου, η ηλεκτρονική πιστοποίηση, οι ηλεκτρονικές υπογραφές, αλλά και ο τρόπος λειτουργίας της ασύμμετρης κρυπτογραφίας) και της διανομής υλικού πληροφόρησης. Οι δράσεις αυτές απευθύνονται είτε στο γενικό κοινό είτε και σε περισσότερο στοχευμένες ομάδες, όπως είναι ειδικοί που εργάζονται σε δημόσιους οργανισμούς. Ειδικά για τους δημόσιους υπαλλήλους, οι κυβερνήσεις πραγματοποιούν δράσεις όπως σεμινάρια και συνέδρια (OECD, 2005).

Αναφορικά με τις εκπαιδευτικές πρωτοβουλίες, εκπονούνται από διάφορους φορείς, όπως είναι κυβερνητικές υπηρεσίες οι οποίες ειδικεύονται στην ασφάλεια των πληροφοριών και φορείς εφαρμογής του νόμου οι οποίοι έχουν ως αντικείμενο τους το διαδικτυακό έγκλημα. Επιπρόσθετα, διαμοιράζεται εκπαιδευτικό υλικό, ούτως ώστε να αυξηθεί το ενδιαφέρον του κοινού για ζητήματα ασφαλείας. Σε ορισμένες χώρες έχουν ληφθεί πρωτοβουλίες οι οποίες επικεντρώνουν στους δασκάλους, ούτως ώστε στη συνέχεια εκείνοι να αναλάβουν την επιμόρφωση των μαθητών. Ορισμένες φορές κινητοποιείται και ο ιδιωτικός τομέας (OECD, 2005).

Οι Chang και Lin (2007) θεωρούν ότι τα διοικητικά στελέχη των οργανισμών πρέπει να ενισχύουν τις πρακτικές ασφαλείας των οργανισμών τους μέσα από ενεργητικές, προσεκτικά σχεδιασμένες οδηγίες και κατευθύνσεις. Μέσα από την εμπειρική τους έρευνα εντόπισαν ότι τα χαρακτηριστικά κουλτούρας που είναι προσανατολισμένα προς την άσκηση ελέγχου από τη διοίκηση (η αποτελεσματικότητα και η συνοχή)

συσχετίζονται σημαντικά και θετικά με τις αρχές της ασφάλειας των πληροφοριών. Ο υπερβολικός έλεγχος πάντως αποθαρρύνει έμεσα την ανταλλαγή πληροφοριών μεταξύ του προσωπικού. Η ηγεσία των οργανισμών πρέπει να πραγματοποιεί τις κατάλληλες επιλογές και να υιοθετεί αποτελεσματικές προσεγγίσεις ούτως ώστε να σχηματίζει την κουλτούρα του οργανισμού που διοικεί και να δημιουργεί ένα περιβάλλον το οποίο συμβάλλει στην επιτυχία των πρωτοβουλιών που σχετίζονται με την ασφάλεια των πληροφοριών. Για παράδειγμα, οργανισμοί οι οποίοι διέπονται από κουλτούρες προσανατολισμένες προς την ευελιξία ενδέχεται να μην υποστηρίζουν ένα περιβάλλον το οποίο ευνοεί τις πρακτικές ασφάλειας πληροφοριών και επομένως ίσως είναι επιτακτικό για τα διοικητικά τους στελέχη να προσδιορίσουν και να χρησιμοποιήσουν τις τεχνολογίες ασφαλείας των πληροφοριών και τα αντίστοιχα μέτρα εφαρμογής και διοίκησης για την εφαρμογή όλων των αρχών της διαχείρισης της ασφάλειας των πληροφοριών. Ειδικά για οργανώσεις οι οποίες είναι προσανατολισμένες προς τη συνεργασία, πρέπει να δίδεται ιδιαίτερη προσοχή σε ζητήματα που άπτονται της εμπιστευτικότητας, ούτως ώστε να διασφαλιστεί ότι η διαχείριση της ασφάλειας πληροφοριών θα έχει θετικά αποτελέσματα, καθώς έχει βρεθεί ότι η συνεργατικότητα επιδρά αρνητικά στην εμπιστευτικότητα (Chang και Lin, 2007). Η ασφάλεια των πληροφοριών απαιτεί την εμπλοκή της ανώτατης διοίκησης στη θεμελίωση πολιτικών, διαδικασιών, οργανωτικών δομών και την πρόσληψη προσωπικού και στελεχών έχοντας ως γνώμονα τη βελτίωση της ασφάλειας των πληροφοριών. Επιπρόσθετα, η κουλτούρα ασφαλείας πρέπει να καλλιεργείται ως μέρος της οργανωτικής κουλτούρας και με τέτοιον τρόπο ώστε η ασφάλεια των πληροφοριών να εξελιχθεί σε μία φυσική πτυχή των καθημερινών δραστηριοτήτων όλων των μελών ενός οργανισμού.

Προτείνεται η υιοθέτηση μίας ολοκληρωμένης στρατηγικής, η οποία συνδυάζει τόσο πτυχές της ασφάλειας πληροφοριών όσο και της οργανωτικής κουλτούρας, ενώ δεν επικεντρώνει μόνο στα εξωτερικά πρότυπα συμπεριφοράς, τα οποία είναι ορατά, αλλά στην εσωτερική ανθρώπινη φύση, τις δραστηριότητες και τις σχέσεις, οι οποίες είναι κρυφές και κατά κύριο λόγο ασυνείδητες. Για την κατανόηση και βελτίωση της οργανωσιακής συμπεριφοράς σε κάθε επίπεδο υπό το πρίσμα της ασφάλειας των πληροφοριών, τα διοικητικά στελέχη θα πρέπει να μελετούν την οργανωσιακή

κουλτούρα και να εξετάζουν τον τρόπο με τον οποίο επηρεάζει τις πρακτικές της ασφάλειας των πληροφοριών. Ο πλέον σημαντικός παράγοντας είναι η αξιολόγηση των προαπαιτούμενων κουλτούρας της διαχείρισης ασφαλείας πληροφοριών. Για παράδειγμα, διαφορετικές ομάδες μέσα σε έναν οργανισμό μπορεί να έχουν κάποια κοινά στοιχεία οργανωτικής κουλτούρας, αλλά έχουν επίσης και μία υπό-κουλτούρα η οποία είναι μοναδική για κάποια υπό-ομάδα (Chang και Lin, 2007).

Οι Herath και Rao (2009) εντόπισαν μέσα από εμπειρική έρευνα ότι τα εσωτερικά κίνητρα από τη διοίκηση ενός οργανισμού προς το προσωπικό επηρεάζουν τις συμπεριφορές των εργαζομένων που σχετίζονται με την εφαρμογή των πολιτικών ασφαλείας. Εάν οι εργαζόμενοι αντιλαμβάνονται ότι οι συμπεριφορές που συνδέονται με τη συμμόρφωση στις πολιτικές ασφαλείας έχουν θετικό αντίκτυπο στον οργανισμό είναι περισσότερο πιθανό να τις υιοθετήσουν. Επιπρόσθετα, βρέθηκε ότι οι συμπεριφορές ασφαλείας επηρεάζονται και από την επιρροή της κοινωνίας. Οι τυποποιημένες γνώμες είχαν μία σημαντική επίδραση υποδεικνύοντας ότι οι απόψεις σχετικά με τις προσδοκίες των ανώτερων, της διοίκησης των ΤΠΕ και των συναδέλφων τους έχουν τη μέγιστη επίδραση στις συμπεριφορές ασφαλείας των εργαζομένων. Οι αντιλήψεις των εργαζομένων σχετικά με τη συμμόρφωση των άλλων με τις πολιτικές ασφαλείας επίσης επιδρούν σημαντικά στην πρόθεση τους να συμμορφωθούν και εκείνοι με αυτές.

Η βεβαιότητα του προσωπικού σχετικά με το ότι θα εντοπιστούν πιθανές παραβιάσεις των πολιτικών ασφαλείας επίσης αυξάνει την πιθανότητα συμμόρφωσης με αυτές. Αντιθέτως, η αυστηρότητα των ποινών επιδρά αρνητικά στις προθέσεις υιοθέτησης συμπεριφορών ασφαλείας. Η βαθμιαία προσέγγιση της αξιολόγησης, δηλαδή κυρώσεις και αμοιβές για τις συμπεριφορές βάσει ενός συστήματος πόντων, το οποίο χρησιμοποιείται στη συνολική ετήσια αξιολόγηση του εργαζόμενου, αναφέρεται ως μία καλύτερη εναλλακτική. Οι περισσότεροι εργαζόμενοι δήλωσαν ότι η πιθανότητα να εντοπιστούν εάν παραβιάσουν τους κανονισμούς ασφαλείας είναι περισσότερο πιθανό να οδηγήσει σε συμμόρφωση με αυτούς. Η ύπαρξη και ορατότητα μηχανισμών εντοπισμού είναι μάλλον σημαντικότερη σε σχέση με την αυστηρότητα των ποινών που επιβάλλονται. Τα διοικητικά στελέχη πρέπει να υιοθετούν μηχανισμούς διερεύνησης και αξιολόγησης

των επιδόσεων ασφαλείας των εργαζομένων. Για παράδειγμα, να πραγματοποιούν επιτόπου ελέγχους ούτως ώστε να αξιολογήσουν τις συμπεριφορές στον χώρο εργασίας (Herath και Rao, 2009).

Επίσης είναι ιδιαίτερα σημαντικές τόσο οι τυποποιημένες απόψεις σχετικά με τις προσδοκίες των ανωτέρων σχετικά με τις συμπεριφορές των εργαζομένων, αλλά και το παράδειγμα που δίδουν οι ίδιοι με τη συμπεριφορά τους. Επίσης επιδρούν στη διαμόρφωση της συμπεριφοράς του καθενός και οι συμπεριφορές των συναδέλφων του. Επομένως τα διοικητικά στελέχη μπορούν να ενισχύσουν τη συμμόρφωση με τις πολιτικές ασφαλείας σε έναν οργανισμό ενισχύοντας την κατάλληλη κουλτούρα. Ιδιαίτερη σημασία προς τη συγκεκριμένη κατεύθυνση έχει το να αντιλαμβάνονται οι εργαζόμενοι πως οι δράσεις τους κάνουν τη διαφορά και συμβάλλουν στην επίτευξη της συνολικής ασφάλειας. Δηλαδή, είναι ιδιαίτερα σημαντικές οι προσπάθειες των διοικητικών στελεχών των ΤΠΕ να πείσουν τους εργαζόμενους για τη σημασία των πολιτικών ασφαλείας και για το ότι οι δράσεις του καθενός συνεισφέρουν σημαντικά στην επίτευξη του συνολικού στόχου της ασφάλειας των πληροφοριών (Herath και Rao, 2009).

Ιδιαίτερη σημασία έχει η αναγνώριση της σημασίας των πληροφοριών ως σημαντικού πόρου τόσο από τους εργαζόμενους, αλλά και από την ανώτερη διοίκηση. Η διοίκηση πρέπει να γνωρίζει τη σημασία των σχέσεων που υπάρχουν μεταξύ των οργανωσιακών διεργασιών και των τμημάτων ΤΠΕ όσον αφορά τις ευθύνες σχετικά με την ασφάλεια των πληροφοριών (Smith και Jamieson, 2006). Η δημιουργία ενός αποτελεσματικού σχεδίου είναι αλληλένδετη με την κουλτούρα ασφαλείας, ενώ πρέπει να διεξάγονται συνεχείς αναβαθμίσεις του σχεδίου αυτού, αλλά και έλεγχος του.

3.5. Μελέτες περιπτώσεων ευρωπαϊκών κρατών

3.5.1. Φινλανδία

Η Φινλανδία έχει ενσωματώσει την εθνική της Στρατηγική Διαδικτυακής Ασφαλείας στη Στρατηγική Ασφαλείας για την Κοινωνία που εφαρμόζει, η οποία ορίζει τις αρχές διασφάλισης όλων των κρίσιμων για τη φινλανδική κοινωνία λειτουργιών (διαχείριση

κυβερνητικών υποθέσεων, διεθνών σχέσεων, αμυντική ικανότητα της χώρας, εσωτερική ασφάλεια, λειτουργία της οικονομίας και των υποδομών, διασφάλιση της ευημερίας των πολιτών, ψυχολογική αντοχή στην κρίση). Αναγνωρίζεται η σημασία που έχει η γρήγορη, διαφανής και καλά συντονισμένη ατομική και ομαδική δράση για την επίτευξη της ασφάλειας. Η κυβέρνηση τοποθετείται στην κορυφή της ανάληψης των σχετικών πρωτοβουλιών, έχει την ευθύνη της πολιτικής και στρατηγικής καθοδήγησης, αλλά και της λήψης των αποφάσεων σχετικά με την κατανομή των πόρων (Finnish Secretariat of the Security and Defence Committee, 2013).

Στη στρατηγική της χώρας αναφέρεται ότι ανά πάσα στιγμή πρέπει τόσο η κυβέρνηση όσο και όλοι οι εμπλεκόμενοι παράγοντες να έχουν μία αξιόπιστη εικόνα της ηλεκτρονικής ασφάλειας κάθε χρήσιμης πτυχής της κοινωνίας, καθώς και των πιθανών κινδύνων που ενδέχεται να επηρεάσουν τη λειτουργικότητα τους. Κάθε υπουργείο και κάθε διοικητικό παράρτημα είναι επιφορτισμένο με την ευθύνη της ηλεκτρονικής ασφάλειας και της διαχείρισης των σχετικών κινδύνων εντός του πεδίου αρμοδιότητας του. Δίδεται ιδιαίτερη σημασία στη συνεργασία και στον συντονισμό των σχετικών λειτουργιών. Τα καθήκοντα του κάθε υπουργείου ορίζονται βάσει της ανάλυσης των κινδύνων που έχουν προσδιοριστεί. Επίσης κάθε υπουργείο πρέπει να επιβλέπει την πορεία επίτευξης των στρατηγικών στόχων που έχουν τεθεί. Μία Επιτροπή Ασφαλείας λειτουργεί ως το συντονιστικό σώμα του σχεδιασμού έκτακτων αναγκών (Finnish Secretariat of the Security and Defence Committee, 2013).

Οι διάφοροι φορείς και υπηρεσίες διοργανώνουν συχνά εκπαιδευτικές δράσεις οι οποίες αφορούν την ασφάλεια των πληροφοριών. Με τον τρόπο αυτό βελτιώνεται η χρήση των βέλτιστων πρακτικών ασφαλείας, ενώ στόχος τους είναι η ενίσχυση της ικανότητας των συμμετεχόντων να μπορούν να εντοπίσουν από μόνοι τους πιθανά αδύναμα σημεία τόσο των δράσεων τους όσο και των συστημάτων που χρησιμοποιούν, καθώς και η εν γένει βελτίωση των ικανοτήτων τους (Finnish Secretariat of the Security and Defence Committee, 2013).

Επιπρόσθετα, δίδεται σημασία στο να αποκτήσουν οι εμπλεκόμενοι στις σχετικές εφαρμογές επίγνωση της κατάστασης της διαδικτυακής ασφαλείας (δηλαδή να βρίσκονται σε θέση να την εκτιμούν κατά την εργασία τους ή τη χρήση των

υπηρεσιών), λαμβάνοντας σε πραγματικό χρόνο πληροφορίες σχετικά με τις ευπάθειες, τις διαταραχές και τις επιπτώσεις τους. Για τον σκοπό αυτό έχει δημιουργηθεί ένας κεντρικός φορέας, ο οποίος συλλέγει πληροφορίες από διάφορα συμβάντα, τις αναλύει και στη συνέχεια τις διανέμει στους ενδιαφερόμενους. Στη συνέχεια εκείνοι έχουν τη δυνατότητα να αξιολογήσουν τις πιθανές επιπτώσεις των συμβάντων στο πεδίο εργασίας τους και να λάβουν τις αποφάσεις τους (Finnish Secretariat of the Security and Defence Committee, 2013) .

Οι οργανισμοί στη δομή των υπηρεσιών τους λαμβάνουν υπόψη τις διαδικτυακές απειλές, ενώ φροντίζουν να διατηρούν τα απαραίτητα μέτρα ασφαλείας. Προς τη συγκεκριμένη κατεύθυνση, υλοποιείται σχεδιασμός έκτακτης ανάγκης καθώς και σχετικές ασκήσεις, ενώ οι δράσεις συμπληρώνονται από αναφορές προς τους φορείς ασφαλείας, την παροχή οδηγιών από τους φορείς ασφαλείας προς τους οργανισμούς και την υλοποίηση εκπαιδευτικών δράσεων. Επιπρόσθετα, δίδεται σημασία και στην παροχή κινήτρων (πέραν φυσικά της τεχνικής εκπαίδευσης) στο προσωπικό της αστυνομίας ούτως ώστε να αυξήσει τις προσπάθειες του σχετικά με την πρόληψη του κυβερνοεγκλήματος και την τακτική επεξεργασία και διερεύνηση των σχετικών ψηφιακών στοιχείων. Πέραν των εργαζόμενων στους φορείς που εμπλέκονται με την ηλεκτρονική διακυβέρνηση, η κρατική πολιτική της χώρας περιλαμβάνει και την υλοποίηση δράσεων για τη βελτίωση των γνώσεων όλων των πολιτών σχετικά με τη διαδικτυακή ασφάλεια (Finnish Secretariat of the Security and Defence Committee, 2013) .

Η πορεία της εν λόγω στρατηγικής παρακολουθείται από την κυβέρνηση, τα υπουργεία και τις υπηρεσίες (Finnish Secretariat of the Security and Defence Committee, 2013). Το γεγονός αυτό αποτελεί μία ένδειξη του ότι δίδεται σημασία στην υιοθέτηση των συμπεριφορών που απορέουν από αυτήν. Από την άλλη, θα πρέπει να αναφέρουμε την περιορισμένη σημασία που δίδεται στην υιοθέτηση από τους πολίτες – χρήστες των υπηρεσιών των κατάλληλων συμπεριφορών που προκύπτουν από μία κουλτούρα ασφαλείας ως μειονέκτημα. Η συμμετοχή όλων των φορέων και του προσωπικού τους πάντως στην ασφάλεια των πληροφοριών ενθαρρύνεται σε σημαντικό βαθμό, ενώ δίδεται βαρύτητα στην έμπρακτη κατανόηση

των πρακτικών ασφαλείας, αν αναλογιστούμε τις ασκήσεις και εκπαιδευτικές δράσεις που εφαρμόζονται.

3.5.2. Γαλλία

Η Γαλλία στην Εθνική της Στρατηγική για τη Διαδικτυακή Ασφάλεια αναφέρει ότι στη σύγχρονη εποχή η ασφάλεια των πληροφοριών αποτελεί ευθύνη όλης της κοινωνίας. Διαχωρίζει τους εμπλεκόμενους σε τρεις κατηγορίες. Η πρώτη κατηγορία έχει την ευθύνη της σύστασης και εφαρμογής τεχνολογιών οι οποίες έχουν το αναγκαίο επίπεδο ασφαλείας για τη χρήση που έχουν σχεδιαστεί και τη δυνατότητα αντιμετώπισης των προσδιορισμένων κινδύνων. Αποτελείται από τους ερευνητές, τους σχεδιαστές προϊόντων και υπηρεσιών, τις εταιρείες διαδικτυακής ασφάλειας, τους διαχειριστές των δικτύων επικοινωνίας, τους διαδικτυακούς παρόχους και τις υπηρεσίες απομεμακρυσμένης επεξεργασίας δεδομένων (Premier Ministre, 2015).

Η δεύτερη κατηγορία έχει την ευθύνη της προστασίας της χώρας από κακόβουλους χρήστες του διαδικτύου. Πέραν της εφαρμογής των πολιτικών ασφαλείας, οι στάσεις τις οποίες πρέπει να υιοθετούν όσοι ανήκουν σε αυτήν περιλαμβάνουν την ανάπτυξη των απαιτούμενων τεχνικών ικανοτήτων και την αφοσίωση στη δημιουργία ενός περιβάλλοντος εμπιστοσύνης, το οποίο υποστηρίζει την ψηφιακή μετάβαση, προστατεύοντας τους πολίτες, τις αξίες της χώρας και τα ενδιαφέροντα της στον κυβερνοχώρο. Ανάμεσα στα καθήκοντα της συγκεκριμένης κατηγορίας περιλαμβάνεται η έκφραση της γνώμης του καθενός σχετικά με τις υιοθετούμενες λύσεις ασφαλείας. Αποτελείται από εκλεγμένους αξιωματούχους, την κυβέρνηση, την κεντρική και τις περιφερειακές διοικήσεις και τα συνδικάτα (Premier Ministre, 2015).

Η τρίτη κατηγορία έχει την ευθύνη της σωστής χρήσης των διαθέσιμων υπηρεσιών και τεχνολογιών, της πραγματοποίησης λογικών επιλογών και της αποφυγής επικίνδυνων συμπεριφορών κατά τις ενέργειες της που σχετίζονται με τη χρήση των διαδικτυακών υπηρεσιών. Αποτελείται από όλους τους χρήστες, τα διοικητικά

στελέχη, τους συμμετέχοντες στον δημόσιο βίο και τους πολίτες (Premier Ministre, 2015).

Ανάμεσα στους στόχους που αναφέρονται στη στρατηγική της χώρας, με την κουλτούρα ασφαλείας θα μπορούσαν να συνδεθούν η διασφάλιση της απαραίτητης εκπαίδευσης και κατάρτισης για την επίτευξη της ψηφιακής ασφαλείας και η δημιουργία ενός περιβάλλοντος το οποίο συμβάλλει στην εμπιστοσύνη στις ψηφιακές τεχνολογίες. Ως πρόβλημα αναφέρεται το γεγονός του ότι βάσει των τεχνικών που παρατηρήθηκε ότι χρησιμοποιούνται σε διάφορες κυβερνοεπιθέσεις εναντίον υπηρεσιών, οι χρήστες αντιμετωπίζουν σημαντικές δυσκολίες στο να κατανοήσουν τη σημασία του διαχωρισμού της προσωπικής και της επαγγελματικής τους ζωής κατά τη χρήση του εξοπλισμού και των υπηρεσιών, κάτι το οποίο εκμεταλλεύονται οι κακόβουλες πλευρές ούτως ώστε να αποκτήσουν πρόσβαση στα δεδομένα τους (Premier Ministre, 2015).

Αναφέρεται ότι η Γαλλία υστερεί σε σχέση με τις υπόλοιπες ευρωπαϊκές χώρες σχετικά με την αύξηση της ευαισθητοποίησης των πολιτών της για τους κινδύνους που σχετίζονται με τη χρήση των ψηφιακών τεχνολογιών και την εκπαίδευση τους πάνω σε ζητήματα διαδικτυακής ασφάλειας. Η αύξηση της προσοχής των πολιτών αναφέρεται ως προαπαιτούμενο για τους εκλεγμένους αξιωματούχους, αλλά και τα διοικητικά στελέχη των δημοσίων οργανισμών, οι οποίοι επιπρόσθετα θα πρέπει να βρίσκονται σε θέση να εκτιμούν τους διαδικτυακούς κινδύνους στις σωστές τους διαστάσεις και να επιλέγουν τα κατάλληλα μέτρα για την προστασία των πολιτών που αντιπροσωπεύουν ή των οργανισμών που διοικούν, από την κλοπή πληροφοριών ή προσωπικών δεδομένων, την παραβίαση προσωπικών δεδομένων ή την έκθεση σε ατυχήματα που οφείλονται σε διακοπή των παρεχόμενων υπηρεσιών, καθώς και από τις τεχνολογικές και περιβαλλοντικές επιπτώσεις στις οποίες ενδέχεται να εκτεθούν (Premier Ministre, 2015).

Πραγματοποιείται αναφορά και στο γεγονός του ότι τα τρέχοντα εκπαιδευτικά προγράμματα δεν καλύπτουν το σύγχρονο επίπεδο γνώσεων που απαιτεί η εισαγωγή των ΤΠΕ στις κρατικές υπηρεσίες και ως εκ τούτου προτείνεται η αναβάθμιση τους. Επιπρόσθετα, προτείνεται η δημιουργία εκπαιδευτικού υλικού το οποίο θα απευθύνεται σε όλη την κοινωνία. Η Γενική Γραμματεία Ψηφιακής Τεχνολογίας, σε

συνεργασία με τα αρμόδια υπουργεία, θα υλοποιήσει ειδικά προγράμματα ευαισθητοποίησης για τους εργαζόμενους το αντικείμενο των οποίων απαιτεί μία έμφαση σε ζητήματα διαδικτυακής ασφάλειας σε συνδυασμό με τις κοινωνικές τους ευθύνες. Το Υπουργείο Αποκέντρωσης και Δημοσίων Υπηρεσιών θα διασφαλίσει ότι θα υλοποιηθούν εκπαιδευτικά προγράμματα για τις λειτουργίες των δημοσίων υπηρεσιών, τα οποία θα περιλαμβάνουν και στοιχεία εκπαίδευσης στη διαδικτυακή ασφάλεια. Σε συνεργασία με το Υπουργείο Εσωτερικών θα διασφαλίσει το ότι οι εξετάσεις πρόσληψης των δημοσίων υπαλλήλων οι οποίοι εργάζονται σε υπηρεσίες πληροφοριακών και επικοινωνιακών συστημάτων, αλλά και η εκπαίδευση που παρέχεται στους υπαλλήλους τους θα περιλαμβάνουν ένα τμήμα αφιερωμένο στη διαδικτυακή ασφάλεια. Οι εκπαιδευτικές ανάγκες θα προσδιοριστούν από μία Ειδική Επιτροπή για την Ψηφιακή Εμπιστοσύνη, σε συνεργασία με τους εμπλεκόμενους φορείς της δημόσιας διοίκησης. Επιπρόσθετα, θα κληθούν να συμβάλλουν σε αυτή την προσπάθεια και οι συνδικαλιστικοί φορείς των εργαζομένων, αναπτύσσοντας και υλοποιώντας προγράμματα συνεχούς εκπαίδευσης τα οποία είναι προσαρμοσμένα στις ανάγκες τους (Premier Ministre, 2015).

Αναφέρεται επίσης ότι το γαλλικό δημόσιο θα δώσει το παράδειγμα στο κοινό, ενσωματώνοντας το κατάλληλο επίπεδο κριτηρίων ασφαλείας κατά την επιλογή προϊόντων και υπηρεσιών (Premier Ministre, 2015).

Αξιολογώντας την περίπτωση της Γαλλίας, θα μπορούσαμε να πούμε ότι δίδεται περισσότερη σημασία στην ανάπτυξη μίας κουλτούρας ασφαλείας σε σχέση με τη Φινλανδία. Η χώρα αναγνωρίζει ότι βρίσκεται πίσω σε αυτό το κομμάτι, ενώ ενσωματώνει στη στρατηγική της περισσότερες δράσεις, κατά κύριο λόγο ενημερωτικού και εκπαιδευτικού χαρακτήρα, δίδοντας μεγαλύτερη σημασία και στην εμφύσηση των σχετικών συμπεριφορών στο κοινό που θα χρησιμοποιήσει τις ηλεκτρονικές υπηρεσίες και όχι μόνο στο προσωπικό τους. Σε σχέση με τη Φινλανδία, δίδεται περισσότερη σημασία σε εκπαιδευτικές δράσεις και όχι στις προτάσεις των εργαζομένων στις υπηρεσίες που εφαρμόζουν την ηλεκτρονική διακυβέρνηση. Οι προτάσεις για την υλοποίηση νέων πολιτικών ασφαλείας υλοποιούνται κατά κύριο λόγο από ειδικές επιτροπές και το βάρος δίδεται στο να συνειδητοποιήσουν οι χρήστες των υπηρεσιών και οι φορείς που τις αξιοποιούν τη σημασία της ασφάλειας,

ούτως ώστε να ενστερνιστούν και να εφαρμόσουν στην πράξη τις προτεινόμενες πολιτικές. Το γεγονός αυτό μπορεί να αποδοθεί στο ότι και στη στρατηγική της χώρας δηλώνεται ότι δεν έχει εκτιμηθεί σωστά η σημασία της ασφάλειας από τους πολίτες και τους εργαζόμενους και επομένως πρέπει να πραγματοποιηθούν βήματα προς την ενίσχυση της προσοχής που δίνουν σε αυτήν.

3.5.3. Ισπανία

Η Ισπανία στην Εθνική Στρατηγική Διαδικτυακής Ασφάλειας αναφέρει ότι θέλει να ενθαρρύνει ένα συνεκτικό όραμα προς την κατεύθυνση της ασφαλούς χρήσης του διαδικτύου, ενώ δίδεται έμφαση στη συνεργασία μεταξύ των δημοσίων αρχών, του ιδιωτικού τομέα και των πολιτών. Στις αρχές του σχεδιασμού της χώρας αναφέρεται μεταξύ άλλων η ανάγκη του συντονισμού των ικανοτήτων, των πόρων και των ευθυνών του κάθε εμπλεκόμενου φορέα. Ο πρωθυπουργός αναλαμβάνει το συγκεκριμένο καθήκον, στα πλαίσια του Εθνικού Συμβουλίου Ασφαλείας (Presidencia del Gobierno, 2013).

Γίνεται ιδιαίτερη αναφορά στους πολίτες, οι οποίοι θα πρέπει να αισθάνονται συμμετέχοντες στην υπόθεση της διαδικτυακής ασφάλειας. Προς τη συγκεκριμένη κατεύθυνση, θεωρείται αναγκαίος ο συντονισμός των διαφορετικών σωμάτων των δημοσίων αρχών, σε συνδυασμό με τη συνεργασία ιδιωτικού και δημοσίου τομέα, ούτως ώστε να διασφαλιστεί η συμβατότητα των πρωτοβουλιών που θα λάβει ο κάθε φορέας προς τη συγκεκριμένη κατεύθυνση και να ενισχυθεί η ανταλλαγή πληροφοριών (Presidencia del Gobierno, 2013).

Σύμφωνα με τη στρατηγική της χώρας, οι αρχές θα πρέπει να δώσουν το παράδειγμα της διαχείρισης της διαδικτυακής ασφαλείας. Οι δημόσιες αρχές κατευθύνονται προς την ανάπτυξη δεσμών συνεργασίας με τις εταιρείες διαχείρισης των ΤΠΕ, ούτως ώστε να ανταλλάσσουν σχετικές γνώσεις, να διευκολύνεται ο μεταξύ τους συντονισμός και να αποκτούν μία κοινή κατανόηση του περιβάλλοντος της διαδικτυακής ασφαλείας (Presidencia del Gobierno, 2013).

Γίνεται αναφορά και στη σημασία που έχει η συνεργασία των πολιτών με την αστυνομία για την αντιμετώπιση κυβερνοεπιθέσεων (ανάμεσα στις οποίες ενδέχεται να σημειωθούν και επιθέσεις στις υπηρεσίες της ηλεκτρονικής διακυβέρνησης).

Αναφέρεται ρητά η ανάγκη ενίσχυσης της συμμετοχής των πολιτών και της διευκόλυνσης των διαδικασιών σχετικά με την πρόσβαση και τη μετάδοση σχετικών πληροφοριών προς την αστυνομία (Presidencia del Gobierno, 2013).

Ιδιαίτερη μνεία γίνεται στην ανάληψη κυβερνητικών πρωτοβουλιών οι οποίες αποσκοπούν στην πληροφόρηση και την ευαισθητοποίηση των πολιτών, των επαγγελματιών, των εταιρειών και των δημοσίων φορέων σχετικά με τους κινδύνους των διαδικτυακών εργασιών, αλλά και την απόκτηση των απαραίτητων γνώσεων σχετικά με τα εργαλεία που θα τους προστατέψουν από αυτούς. Επιπρόσθετα, αναφέρεται ότι οι δημόσιες αρχές θα πρέπει να έχουν επίγνωση των ευθυνών διασφάλισης των συστημάτων τους, της προστασίας των πληροφοριών των πλευρών που συναλλάσσονται μαζί τους και της αξιοπιστίας των προσφερόμενων υπηρεσιών. Η διατήρηση της εμπιστοσύνης των πολιτών σε αυτές χαρακτηρίζεται ως ζωτικής σημασίας (Presidencia del Gobierno, 2013).

Αναφέρεται ως απαραίτητη λειτουργία η προώθηση μίας ισχυρής κουλτούρας διαδικτυακής ασφαλείας η οποία θα παρέχει σε όλους τους παράγοντες την απαραίτητη επίγνωση και αυτοπεποίθηση ούτως ώστε να μεγιστοποιήσουν τα οφέλη της κοινωνίας της πληροφορίας και να περιορίσουν στο ελάχιστο δυνατό την έκθεση τους στους κινδύνους του κυβερνοχώρου υιοθετώντας τα κατάλληλα μέτρα για τη διασφάλιση της προστασίας των δεδομένων και την ασφαλή σύνδεση των συστημάτων και του εξοπλισμού τους (Presidencia del Gobierno, 2013).

Η αποτελεσματική διαχείριση των κινδύνων του κυβερνοχώρου θεμελιώνεται επίσης υπό το πρίσμα μίας κουλτούρας διαδικτυακής ασφαλείας. Η προσέγγιση αυτή απαιτεί από τους χρήστες να είναι ευαισθητοποιημένοι σχετικά με τους κινδύνους που περιλαμβάνει η δραστηριοποίηση τους σε αυτό το πεδίο, καθώς και να είναι εξοικειωμένοι με τα εργαλεία προστασίας των πληροφοριών, των συστημάτων και των συσκευών τους (Presidencia del Gobierno, 2013).

Οι παραπάνω στοχεύσεις απαιτούν ένα επίπεδο τεχνικών γνώσεων, ειδικά από το προσωπικό των δημοσίων οργανισμών το οποίο έχει την ευθύνη της κατεύθυνσης, της διοίκησης και της εφαρμογής της διαδικτυακής ασφάλειας. Ως εκ τούτου, δίνεται ιδιαίτερη βαρύτητα στην εκπαίδευση του (Presidencia del Gobierno, 2013).

Προκειμένου να ελέγχεται το κατά πόσο καλά συντονίζονται οι δημόσιοι φορείς για την αντιμετώπιση των απειλών, πραγματοποιούνται ασκήσεις προσομοίωσης περιστατικών ασφαλείας, ώστε να αξιολογηθούν και να βελτιωθούν οι σχετικές δράσεις. Στα πλαίσια της κουλτούρας ασφαλείας, ενισχύονται και εθνικές δραστηριότητες οι οποίες αποσκοπούν στην ανάπτυξη και αξιολόγηση προϊόντων, υπηρεσιών και συστημάτων, τα οποία ικανοποιούν τις ανάγκες ασφαλείας που έχουν προσδιοριστεί. Επιπρόσθετα, υποστηρίζεται η δημιουργία, διάδοση και εφαρμογή των βέλτιστων πρακτικών ασφαλείας στους δημόσιους φορείς (Presidencia del Gobierno, 2013).

Σχετικά με την ενίσχυση της κουλτούρας διαδικτυακής ασφαλείας των πολιτών και των εργαζομένων, ως κύριος στόχος αναφέρεται η αύξηση της επίγνωσης τους σχετικά με τη σημασία της ασφάλειας και την υπεύθυνη χρήση των νέων τεχνολογιών και υπηρεσιών. Προς τη συγκεκριμένη κατεύθυνση η ισπανική κυβέρνηση υλοποιεί τα παρακάτω μέτρα (Presidencia del Gobierno, 2013):

- Προωθούνται δραστηριότητες ευαισθητοποίησης, ούτως ώστε να διασφαλιστεί ότι οι πολίτες και οι επιχειρήσεις έχουν την απαραίτητη πρόσβαση σε πληροφορίες σχετικά με ευπάθειες και διαδικτυακές απειλές καθώς και των βέλτιστων τρόπων προστασίας του τεχνολογικού τους περιβάλλοντος.
- Προωθείται η ανάπτυξη προγραμμάτων αύξησης της επίγνωσης σχετικά με τη διαδικτυακή ασφάλεια, μέσα από συνεργασίες με δημόσιους και ιδιωτικούς φορείς, ενισχύοντας τον απαραίτητο συντονισμό και εξορθολογισμό των προσπαθειών, μέσα από φορείς οι οποίοι ειδικεύονται σε αυτό το πεδίο.

Επιπρόσθετα, θεσμοθετείται μία οργανωτική δομή η οποία έχει ως αντικείμενο της την ασφάλεια και βρίσκεται υπό την εποπτεία του πρωθυπουργού. Η δομή αυτή αποτελείται από το Εθνικό Συμβούλιο Ασφαλείας, την Ειδική Επιτροπή Διαδικτυακής Ασφάλειας και την Επιτροπή Ειδικών Καταστάσεων. Το Εθνικό Συμβούλιο Ασφαλείας βοηθάει τον πρωθυπουργό στην καθοδήγηση της εθνικής πολιτικής ασφαλείας. Η Ειδική Επιτροπή Διαδικτυακής Ασφαλείας υποστηρίζει το Εθνικό Συμβούλιο

Ασφαλείας στη διεκπεραίωση των λειτουργιών του. Ενισχύει τις σχέσεις συντονισμού και συνεργασίας μεταξύ των διαφόρων αρχών και μεταξύ του δημοσίου και του ιδιωτικού τομέα, ενώ αναλύει, μελετά και προτείνει πρωτοβουλίες προς την κατεύθυνση της ασφάλειας. Η σύνθεση της επιτροπής αποτελείται από στελέχη όλων των δημοσίων φορέων οι οποίοι σχετίζονται με ζητήματα τα οποία άπτονται της διαδικτυακής ασφάλειας, ούτως ώστε να επιτυγχάνεται καλύτερος συντονισμός τους. Η Επιτροπή Ειδικών Καταστάσεων έχει ως αντικείμενο της την παροχή υποστήριξης στους δημόσιους οργανισμούς σε περιπτώσεις έκτακτων συμβάντων ασφαλείας (Presidencia del Gobierno, 2013).

Αξιολογώντας την περίπτωση της Ισπανίας, παρατηρούμε ότι έχει τις πλέον ανεπτυγμένες πολιτικές προς την ενίσχυση της κουλτούρας ασφαλείας στη χώρα και στους χρήστες των εφαρμογών της ηλεκτρονικής διακυβέρνησης. Αναγνωρίζεται ο ρόλος του δημοσίου ως του παράγοντα ο οποίος πρέπει να αποτελεί παράδειγμα για την κοινωνία. Υιοθετούνται πολυπλευρες δράσεις για την αύξηση της ευαισθητοποίησης του κοινού και την υιοθέτηση από μέρους του των κατάλληλων συμπεριφορών. Επιπρόσθετα, δίδεται ιδιαίτερη βαρύτητα και στην υιοθέτηση των κατάλληλων συμπεριφορών από το προσωπικό των δημοσίων οργανισμών. Προς τη συγκεκριμένη κατεύθυνση, υλοποιούνται εκπαιδευτικές δράσεις οι οποίες απευθύνονται και σε αυτούς. Ο συντονισμός των διαφόρων φορέων αποτελεί ακρογωνιαίο λίθο της στρατηγικής που ακολουθείται, ενώ δίδεται ιδιαίτερη βαρύτητα και στη συνεργασία δημοσίου και ιδιωτικού τομέα, μέσω της οποίας μπορεί να προκύψει ανταλλαγή πολύτιμων πληροφοριών (Presidencia del Gobierno, 2013).

3.5.4. Νορβηγία

Οι Malmedal και Røislien (2016) πραγματοποίησαν μία εκτεταμένη μελέτη, εξετάζοντας την κουλτούρα ασφαλείας στη Νορβηγία. Αντιμετωπίζουν την εθνική κουλτούρα ασφαλείας ως ένα σύνολο αξιών, αισθημάτων και στάσεων υπό το πρίσμα της διαδικτυακής ασφάλειας. Σύμφωνα με την προσέγγιση τους, η διαδικτυακή ασφάλεια μίας χώρας σχετίζεται με διάφορες πτυχές, από την κυβέρνηση και τον κρατικό έλεγχο έως την ατομική τεχνολογική ικανότητα και πραγματοποίηση επικίνδυνων πράξεων του καθενός. Κατά τη γνώμη τους, η

κουλτούρα διαδικτυακής ασφαλείας αποτελείται από οκτώ κύριες πτυχές, τις οποίες και εξέτασαν στη μελέτη τους:

1. Συλλογικότητα
2. Διακυβέρνηση και έλεγχος
3. Εμπιστοσύνη
4. Αντίληψη του κινδύνου
5. Αισιοδοξία σχετικά με την τεχνολογία και ψηφιοποίηση
6. Ικανότητα
7. Ενδιαφέρον
8. Συμπεριφορά

Η μελέτη πραγματοποιήθηκε με τη χρήση ερωτηματολογίων. Μέσα από τις απαντήσεις διαφαίνεται ένα χαμηλό αίσθημα συλλογικότητας των Νορβηγών αναφορικά με τη χρήση του διαδικτύου (η πλειοψηφία τους απάντησε ότι θα έπρεπε να έχει τη δυνατότητα διατήρησης της ανωνυμίας της στο διαδίκτυο – κάτι το οποίο συνδέεται με κακόβουλες ενέργειες όπως είναι η διαδικτυακή κακοποίηση άλλων χρηστών - , καθώς και ότι η ασφάλεια του διαδικτύου δεν θα βελτιωνόταν ακόμα και εάν ο προσωπικός τους υπολογιστής ήταν ασφαλής. Η συγκεκριμένη απάντηση βέβαια ίσως υποδηλώνει και έλλειψη κατανόησης της πραγματικής σημασίας της διαδικτυακής ασφάλειας (Malmedal και Røislien, 2016).

Σχετικά με τη διακυβέρνηση και τον έλεγχο, οι περισσότεροι ερωτηθέντες διατηρούν μία θετική στάση στην παρακολούθηση των διαδικτυακών τους δραστηριοτήτων από κυβερνητικές υπηρεσίες, λόγω του ότι έτσι βελτιώνεται η διαδικτυακή τους ασφάλεια. Δεν ισχύει όμως το ίδιο σχετικά με την εμπιστοσύνη τους προς την αστυνομία ή άλλες αρχές εφαρμογής του νόμου σε περίπτωση που πέσουν θύματα του κυβερνοεγκλήματος. Επιπρόσθετα, μία σημαντική μερίδα θεωρεί ότι οι ανώνυμοι κυβερνο-ακτιβιστές διαδραματίζουν κάποιον ρόλο στην καταπολέμηση του κυβερνοεγκλήματος. Το γεγονός αυτό υποδεικνύει μία σύγχυση σχετικά με το ποιος και με ποιόν τρόπο πρέπει να ελέγχει το διαδίκτυο. Επιπρόσθετα, οι περισσότεροι θεωρούν ότι η αστυνομία πρέπει να τους προστατεύει από το κυβερνοέγκλημα (κλοπή ταυτότητας – προσωπικών στοιχείων, διαδικτυακές απάτες) καθώς και ότι θα ανέφεραν τέτοια περιστατικά στις αρχές. Οι ερευνητές προτείνουν

τη συστηματική παρακολούθηση αυτών των μέτρων, ώστε να εντοπίζονται εγκαίρως αρνητικές τάσεις και να εφαρμόζονται διορθωτικά μέτρα. Επιπρόσθετα, αναφέρεται ότι οι Νορβηγοί ενδιαφέρονται για την ιδιωτικότητα τους (Malmedal και Røislien, 2016).

Αναφορικά με την εμπιστοσύνη, η πλειοψηφία των ερωτηθέντων θεωρεί ότι οι αρχές θα επεξεργαστούν και θα αποθηκεύσουν τα προσωπικά δεδομένα που έχουν παράσχει κατά έναν ασφαλή τρόπο. Επιπρόσθετα, δηλώνουν ότι αισθάνονται ασφαλείς όταν χρησιμοποιούν τις διαδικτυακές εφαρμογές των δημοσίων υπηρεσιών, ενώ μόνο μία μικρή μειοψηφία θεωρεί ότι αντιμετωπίζει κάποιο κίνδυνο κατά τη χρήση τους (Malmedal και Røislien, 2016).

Σχετικά με την αντίληψη κινδύνου, οι περισσότεροι από τους ερωτηθέντες θεωρούν ότι εκτίθενται σε κίνδυνο όταν χρησιμοποιούν το διαδίκτυο, ενώ θεωρούν ότι ενημερώνονται επαρκώς σχετικά με τις ψηφιακές απειλές. Επιπρόσθετα, δηλώνουν ότι βρίσκονται σε θέση να αξιολογήσουν το ποιες πράξεις είναι ασφαλείς στο διαδίκτυο. Πάνω από τα 2/3 του πληθυσμού προσδιορίζουν ως τον μεγαλύτερο διαδικτυακό κίνδυνο το να πέσουν θύματα κακόβουλης πράξης κάποιου άλλου (για παράδειγμα, ενός χάκερ που επιτίθεται σε ιστότοπο στον οποίο έχουν παράσχει προσωπικά δεδομένα). Γενικότερα, οι Νορβηγοί εμπιστεύονται τις δικές τους ικανότητες, αλλά ανησυχούν σχετικά με τους σκοπούς των άλλων (Malmedal και Røislien, 2016).

Η αντίληψη του κινδύνου και η ικανότητα επικαλύπτονται σε διάφορες περιπτώσεις. Για παράδειγμα, σε ερώτηση σχετικά με το εάν η γνώση των κινδύνων του διαδικτύου έχει οδηγήσει τον συμμετέχοντα στο να μην χρησιμοποιήσει κάποια διαδικτυακή υπηρεσία, οι απαντήσεις μοιράζονται ισόποσα. Γενικότερα, οι πολίτες της χώρας δεν ανησυχούν για τους κινδύνους που σχετίζονται με τις διαδικτυακές δραστηριότητες. Μόλις το 12% εξέφρασε ανησυχίες σχετικά με τη χρήση των υπηρεσιών της ηλεκτρονικής διακυβέρνησης. Επιπρόσθετα, σχετικά με τις προσωπικές τους πρακτικές ασφαλείας, παρουσιάζουν ένα ικανοποιητικό επίπεδο χρήσης των βέλτιστων πρακτικών (Malmedal και Røislien, 2016).

Η νορβηγική κουλτούρα διαδικτυακής ασφαλείας χαρακτηρίζεται από μία γενικότερη θετική στάση προς την τεχνολογία. Η συντριπτική πλειοψηφία των ερωτηθέντων δήλωσε ότι είναι θετικά διακείμενη ως προς τη χρήση νέων τεχνολογιών, καθώς και ότι γνώριζε τι είναι η διαδικτυακή ασφάλεια (Malmedal και Røislien, 2016).

Ο νορβηγικός πληθυσμός είναι μάλλον ικανός όσον αφορά τη διαδικτυακή ασφάλεια. Οι ερωτηθέντες θεωρούν ότι κατέχουν ένα ικανοποιητικό επίπεδο γνώσεων, ενώ μπορούν να λάβουν σημαντικές αποφάσεις και να πραγματοποιήσουν κρίσεις στο πεδίο της διαδικτυακής ασφάλειας. Γενικότερα, θεωρούν ότι γνωρίζουν τα ίδια με τους υπολοίπους ή λίγο περισσότερα. Επιπρόσθετα, θεωρούν ότι λαμβάνουν αρκετές πληροφορίες πάνω στο συγκεκριμένο αντικείμενο (Malmedal και Røislien, 2016).

Η πλειοψηφία δηλώνει ότι ενδιαφέρεται για την τεχνολογία και τις ΤΠΕ. Τα ¾ του πληθυσμού δηλώνουν ότι αξιολογούν μία ιστοσελίδα πριν τη χρησιμοποιήσουν, αλλά μόνο μία μικρή μειοψηφία το κάνει πάντοτε. Επιπρόσθετα, μόνο το 61,1% δήλωσε ότι γνωρίζει πως να πραγματοποιήσει αυτή την αξιολόγηση. Επίσης, μόνο το 18,5% δήλωσε ότι χρησιμοποιεί τον ίδιο κωδικό παντού, κάτι το οποίο αποτελεί επικίνδυνη συμπεριφορά. Μόνο το 9,2% χρησιμοποιεί εργαλεία τα οποία βοηθούν τους χρήστες να χρησιμοποιούν περισσότερο πολύπλοκους κωδικούς. Το 61% όμως χρησιμοποιεί διαφορετικούς κωδικούς για την κάθε διαδικτυακή υπηρεσία, ενώ το 37,8% προσπαθεί να δημιουργήσει ασφαλείς κωδικούς (Malmedal και Røislien, 2016).

Το 18% δηλώνει ότι δεν αναβαθμίζει συστηματικά το λογισμικό του, ενώ το 6% ότι δεν γνωρίζει τις συγκεκριμένες διαδικασίες. Επομένως μία μάλλον σημαντική μερίδα του πληθυσμού παραμένει ευάλωτη στο κυβερνοέγκλημα. Το 14,7% δεν κρατάει ποτέ αρχεία ασφαλείας των δεδομένων του, ενώ το 9,3% δεν γνωρίζει εάν το κάνει ή όχι. Η πλειοψηφία κρατάει αρχείο λιγότερο συχνά από μία φορά το μήνα (Malmedal και Røislien, 2016).

Η συντριπτική πλειοψηφία των ερωτηθέντων χρησιμοποιεί firewall και αντιιικό λογισμικό. Οι υψηλοί αριθμοί βέβαια εξηγούνται από το γεγονός του ότι οι περισσότεροι υπολογιστές που διατίθενται στο εμπόριο έχουν προεγκατεστημένο

λογισμικό ασφαλείας, επομένως δεν είναι απαραίτητα μία επιλογή η οποία εξαρτάται από τον χρήστη. Επιπρόσθετα, το 9.5% του πληθυσμού ορισμένες φορές παραβιάζει σκόπιμα τους κανόνες ασφαλείας (Malmedal και Røislien, 2016).

Οι μισοί συμμετέχοντες έλαβαν κάποια εκπαίδευση σχετικά με τη διαδικτυακή ασφάλεια μέσα στα τελευταία δύο χρόνια. Για τους εργαζόμενους στον δημόσιο τομέα, το συγκεκριμένο ποσοστό ανεβαίνει σε 62%. Η συντριπτική πλειοψηφία δηλώνει ότι η εκπαίδευση αυτή τους βοήθησε να βελτιώσουν τις ικανότητες τους . (Malmedal και Røislien, 2016).

Δεν βρέθηκε πάντως κάποια συσχέτιση μεταξύ της επιμόρφωσης πάνω στη διαδικτυακή ασφάλεια και της άποψης του ότι το διαδίκτυο γίνεται περισσότερο ασφαλές εάν ο υπολογιστής του κάθε ατόμου είναι ασφαλής. Το γεγονός αυτό αποδίδεται στο ότι δεν έχουν καταβληθεί αρκετές προσπάθειες για να εξηγηθεί η πολυπλοκότητα του κυβερνοεγκλήματος και ο τρόπος με τον οποίο οι προσωπικοί υπολογιστές χρησιμοποιούνται σε εγκληματικές αλυσίδες. Οι άνθρωποι κατά κύριο λόγο αποκτούν γνώσεις σχετικά με τη διαδικτυακή ασφάλεια από τρεις πηγές: τους εαυτούς τους, ειδικούς της διαδικτυακής ασφάλειας και φίλους και συναδέλφους (Malmedal και Røislien, 2016).

Η έρευνα καταλήγει στη θετική συσχέτιση της επιμόρφωσης στη διαδικτυακή ασφάλεια και των συμπεριφορικών προτύπων. Εντοπίζει πάντως κενά στη συγκεκριμένη διαδικασία, καθώς επιτελείται κατά κύριο λόγο από ιδιωτικές πρωτοβουλίες. Το γεγονός αυτό έχει ως αποτέλεσμα να υστερούν οι νέοι και οι μεγαλύτερες ηλικίες. Εντοπίζεται μάλιστα ότι εξαιτίας των ελλιπών γνώσεων τους οι μεγαλύτερες ηλικίες φοβούνται να χρησιμοποιήσουν τις εφαρμογές της ηλεκτρονικής διακυβέρνησης (Malmedal και Røislien, 2016).

Το ενδιαφέρον συσχετίζεται ισχυρά με τις στάσεις σχετικά με τη χρήση του διαδικτύου, την αντίληψη του κινδύνου και τα συμπεριφορικά πρότυπα. Ως εκ τούτου και από τη στιγμή που λίγο περισσότερο από το μισό του πληθυσμού της χώρας δεν ενδιαφέρεται για την τεχνολογία και τις ΤΠΕ, πρέπει να καταβληθούν προσπάθειες σχετικά με την αύξηση του ενδιαφέροντος που παρουσιάζει για τον μέσο πολίτη η διαδικτυακή ασφάλεια. Ως μειονέκτημα των εκπαιδευτικών μεθόδων

αναφέρεται το γεγονός του ότι χρησιμοποιούν σε υπερβολικό βαθμό τεχνική γλώσσα και ορολογία. Επομένως προτείνεται ο επαναπροσανατολισμός της μεθόδου επικοινωνίας προς εκείνους οι οποίοι δεν ενδιαφέρονται για την τεχνολογία ούτως ώστε να κατανοήσουν γιατί το ζήτημα της ασφάλειας αφορά και αυτούς (Malmedal και Røislien, 2016).

Κεφάλαιο 4

4. Μελέτη της ελληνικής περίπτωσης – Προτάσεις σχετικά με την ανάπτυξη κουλτούρας ασφαλείας στην Ελλάδα

4.1. Η ηλεκτρονική διακυβέρνηση στην Ελλάδα

Κατά τα τελευταία χρόνια έχει υλοποιηθεί στην Ελλάδα ένας μεγάλος αριθμός εφαρμογών οι οποίες σχετίζονται με την ηλεκτρονική διακυβέρνηση. Στην παράγραφο αυτή θα εξετάσουμε την κάθε μία από αυτές.

Οι λειτουργίες που σχετίζονται με τη φορολογία και τα τελωνεία διεκπεραιώνονται μέσα από τον ιστότοπο gsis.gr, ο οποίος έχει αναπτυχθεί σε συνεργασία της Ανεξάρτητης Αρχής Δημοσίων Εσόδων (ΑΑΔΕ) και της Γενικής Γραμματείας Πληροφορικών Συστημάτων (ΓΓΠΣ). Μέσω του συγκεκριμένου ιστότοπου εξυπηρετούνται πολίτες, επιχειρήσεις, άλλες υπηρεσίες του Υπουργείου Οικονομικών, αλλά και άλλες δημόσιες υπηρεσίες οι οποίες μπορούν να διεκπεραιώσουν ανάγκες οι οποίες σχετίζονται με την πιστοποίηση δεδομένων και στοιχείων. Επιπλέον, η συγκεκριμένη πλατφόρμα είναι ενσωματωμένη στο ενοποιημένο τελωνειακό σύστημα της ΕΕ.

Μία ακόμα εφαρμογή είναι εκείνη του Κτηματολογίου (http://www.ktimatologio.gr). Διεκπεραιώνονται λειτουργίες των κτηματολογικών γραφείων και εξυπηρετούνται πολίτες και επιχειρήσεις.

Οι πολίτες έχουν τη δυνατότητα διεκπεραίωσης των στρατολογικών τους θεμάτων μέσα από τον ιστότοπους https://katataxi.army.gr/ ο οποίος έχει αναπτυχθεί από το Υπουργείο Εθνικής Άμυνας, το Γενικό Επιτελείο Εθνικής Άμυνας και το Γενικό Επιτελείο Στρατού.

Η Διαύγεια (https://diavgeia.gov.gr/) είναι ένας ιστότοπος στον οποίο αναρτώνται οι αποφάσεις και οι διοικητικές πράξεις των δημοσίων φορέων. Εξυπηρετεί τη

διαφάνεια του δημοσίου τομέα και την ενημέρωση των πολιτών. Φορεάς λειτουργίας της είναι το Υπουργείο Διοικητικής Ανασυγκρότησης.

Οι ιστότοποι http://www.opengov.gr και http://data.gov.gr/ διαχειρίζονται από το Υπουργείο Διοικητικής Ανασυγκρότησης και το Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης. Απευθύνονται στους πολίτες , τις επιχειρήσεις και το δημόσιο. Ο πρώτος ιστότοπος χρησιμεύει για τη δημόσια διαβούλευση σχετικά με τα νομοσχέδια, ενώ μέσω αυτού πραγματοποιούνται και προσκλήσεις για θέσεις ευθύνες στο δημόσιο καθώς και αιτήσεις για τις θέσεις αυτές από τους ενδιαφερόμενους. Ο δεύτερος ιστότοπος παρέχει πρόσβαση σε βάσεις δεδομένων των φορέων της ελληνικής κυβέρνησης.

Το Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων (http://www.promitheus.gov.gr) διαχειρίζεται από το Υπουργείο Ανάπτυξης και Ανταγωνιστικότητας και τη Γενική Γραμματεία Εμπορίου. Μέσα από αυτόν τον ιστότοπο το δημόσιο πραγματοποιεί ηλεκτρονικούς διαγωνισμούς για προμήθειες και για την ανάθεση υπηρεσιών σε εξωτερικούς φορείς, για ποσά που υπερβαίνουν τις 60.000 €. Απευθύνεται στους δημόσιους φορείς, τους οικονομικούς φορείς που συμμετέχουν σε διαγωνισμούς του δημοσίου. Επίσης εκεί αναρτώνται και οι δημόσιες συμβάσεις.

Η Εργάνη (https://eservices.yeka.gr) διαχειρίζεται από το Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης και Κοινωνικής Αλληλεγγύης. Απευθύνεται στους πολίτες, τις επιχειρήσεις, τους εργαζόμενους και τους ανέργους. Μέσα από τη συγκεκριμένη πλατφόρμα καθίσταται δυνατή η ηλεκτρονική υποβολή εντύπων που απευθύνονται στο Σώμα Επιθεώρησης Εργασίας (ΣΕΠΕ) (αναγγελίες πρόσληψης, απόλυσης κλπ.), καθώς και τον ΟΑΕΔ (Οργανισμός Απασχόλησης Εργατικού Δυναμικού).

Η εφαρμογή Ήλιος διατίθεται στην ιστοσελίδα του Υπουργείου Εργασίας, Κοινωνικής Ασφάλισης και Κοινωνικής Αλληλεγγύης (http://www.yeka.gr/), ενώ έχει υλοποιηθεί από τον φορέα ΗΔΙΚΑ (Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης). Πρόκειται για ένα ενιαίο σύστημα ελέγχου και πληρωμών συντάξεων. Οι φορείς κύριας ασφάλισης (ΦΚΑ) αποστέλουν σε μηνιαία βάση στην ΗΔΙΚΑ ένα ηλεκτρονικό αρχείο πληρωμών συντάξεων, το οποίο περιέχει αναλυτικά και ανά συνταξιούχο τα

ποσά των συντάξεων που καταβάλει κάθε φορέας, ένδειξη εξαίρεσης από τις μειώσεις που προβλέπονται καθώς και περιοδικότητα καταβολής του ποσού της σύνταξης. Στη συνέχεια ελέγχεται η ακρίβεια και ορθότητα των στοιχείων αυτών, πραγματοποιείται στατιστική επεξεργασία των δεδομένων τους και τα αποτελέσματα δημοσιεύονται σε μηνιαίες εκθέσεις.

Η υπηρεσία «Απλό» (https://aplo.yeka.gr/) διεκπεραιώνει υποθέσεις των πολιτών οι οποίες σχετίζονται με αιτήσεις για βεβαιώσεις ασφάλειας και υγείας. Τη διαχειρίζεται το Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης και Κοινωνικής Αλληλεγγύης.

Η πλατφόρμα του Συστήματος Πρωτοβάθμιας Φροντίδας Υγείας (https://www.e-syntagografisi.gr/p-rv/p) διεκπεραιώνει διαδικασίες ηλεκτρονικής συνταγογράφησης, καθώς και ηλεκτρονικών ραντεβού στις μονάδες πρωτοβάθμιας φροντίδας υγείας. Τη διαχειρίζονται το Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης και Κοινωνικής Αλληλεγγύης και η ΗΔΙΚΑ. Χρησιμοποιείται από γιατρούς, φαρμακοποιούς και πολίτες.

Στον ιστότοπο του Εθνικού Τυπογραφείου (http://www.et.gr/) δίδεται η δυνατότητα αναζήτησης Φύλλων Εφημερίδας Κυβερνήσεως (ΦΕΚ), καθώς και η δυνατότητα ψηφιακά υπογεγραμμένων αρχείων προς δημοσίευση.

Η υπηρεσία ΣΥΖΕΥΞΙΣ (http://www.syzefxis.gov.gr/) αποσκοπεί στη διευκόλυνση της επικοινωνίας μεταξύ των φορέων του δημοσίου, καθώς και στην ενοποιημένη εξυπηρέτηση των πολιτών μέσα από αυτοματοποιημένα και φιλικά προς τον χρήστη συστήματα πληροφόρησης και διεκπεραίωσης συναλλαγών με το δημόσιο. Διαχειρίζεται από το Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης. Απευθύνεται στο Εθνικό Δίκτυο Δημόσιας Διοίκησης.

Το Σύστημα Ηλεκτρονικής Διαχείρισης Εγγράφων – Ψηφιακή Υπογραφή (http://aped.gov.gr/) διαχειρίζεται από το Υπουργείο Διοικητικής Ανασυγκρότησης και την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ). Έχει ως αντικείμενο του την έκδοση δωρεάν ψηφιακών πιστοποιητικών αυθεντικοποίησης/υπογραφής και κρυπτογράφησης. Απευθύνεται σε πολίτες και σε δημοσίους υπαλλήλους.

Το Ηλεκτρονικό Σύστημα του Ανωτάτου Συμβουλίου Επιλογής Προσωπικού (ΑΣΕΠ) βρίσκεται στον ιστότοπο http://www.asep.gr. Απευθύνεται σε πολίτες, οι οποίοι μπορούν μέσα από τη συγκεκριμένη ιστοσελίδα να ενημερώνονται σχετικά με τις προκυρήξεις προσλήψεων προσωπικού στο δημόσιο, να υποβάλουν τις αιτήσεις τους και να ενημερώνονται για τα αποτελέσματα. Αντίστοιχα, οι φορείς του δημοσίου αναρτούν τις προκυρήξεις σχετικά με το προσωπικό που πρόκειται να προσλάβουν.

Μέσω του Ηλεκτρονικού Συστήματος Υποβολής και επεξεργασίας δηλώσεων Πόθεν Έσχες, οι υπόχρεοι έχουν τη δυνατότητα υποβολής της περιουσιακής τους κατάστασης, ενώ δημοσιεύονται και απαντήσεις στις πλέον συχνές ερωτήσεις. Η συγκεκριμένη εφαρμογή βρίσκεται στον ιστότοπο https://www.pothen.gr/pothen/main/, διαχειρίζεται από τους ελεγκτικούς φορείς του δημοσίου, ενώ τη λειτουργία της έχει αναλάβει η ΓΓΠΣ (Γενική Γραμματεία Πληροφοριακών Συστημάτων). Απευθύνεται στους πολίτες οι οποίοι είναι υπόχρεοι υποβολής Πόθεν Έσχες, καθώς και στους ελεγκτικούς φορείς των δηλώσεων.

4.2. Η ελληνική εθνική στρατηγική κυβερνοασφάλειας

Η Ελληνική Εθνική Στρατηγική Κυβερνοασφάλειας αναφέρει ότι πρέπει να δοθεί ιδιαίτερη βαρύτητα στη δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος, στο οποίο συμπεριλαμβάνονται και οι δομές και υπηρεσίες της ηλεκτρονικής διακυβέρνησης και το οποίο θα εξασφαλίσει την εμπιστοσύνη των πολιτών ούτως ώστε να αυξηθεί η χρήση των νέων διαδικτυακών προϊόντων και υπηρεσιών. Η ασφάλεια, σε συνδυασμό με τη διασφάλιση των προσωπικών δεδομένων και των δικαιωμάτων των πολιτών θεωρούνται κομβικής σημασίας και για την οικονομική ανάπτυξη της χώρας. Διαπιστώνεται η ύπαρξη ενός οργανωτικού και συντονιστικού κενού μεταξύ των φορέων της διαδικτυακής ασφάλειας, τόσο ιδιωτικών όσο και δημοσίων. Για την κάλυψη του θεσμοθετείται η Εθνική Αρχή Κυβερνοασφάλειας, η οποία επιφορτίζεται και με τις επιπρόσθετες αρμοδιότητες αποτίμησης, αναθεώρησης και επικαιροποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας τουλάχιστον μία φορά ανά τριετία (ΥΨΗΠΤΕ, 2018).

Η ανάπτυξη μίας ισχυρής κουλτούρας ασφαλείας των πολιτών, του δημοσίου και του ιδιωτικού τομέα αναφέρεται ως μία από τις τέσσερεις βασικές αρχές της Στρατηγικής της χώρας. Προς τη συγκεκριμένη κατεύθυνση προτείνεται η αξιοποίηση των σχετικών δυνατοτήτων της ακαδημαϊκής κοινότητας και γενικότερα των φορέων του δημοσίου και του ιδιωτικού τομέα. Προς τη συγκεκριμένη κατεύθυνση διατυπώνεται ο στόχος της ευαισθητοποίησης όλων των κοινωνικών φορέων και της ενημέρωσης των χρηστών σχετικά με την ασφαλή χρήση του διαδικτύου (ΥΨΗΠΤΕ, 2018).

Ενισχύεται η δυνατότητα ανταλλαγής πληροφοριών μεταξύ των φορέων, ενώ καθίσταται ευκολότερη η αναφορά συμβάντων ασφαλείας καθώς και η εφαρμογή των κοινών πρακτικών ασφαλείας (ΥΨΗΠΤΕ, 2018).

Όλοι οι φορείς που συμμετέχουν στη στρατηγική οφείλουν να λαμβάνουν τα απαραίτητα τεχνικά και οργανωτικά μέτρα ούτως ώστε να διασφαλιστεί η ασφαλής και απρόσκοπτη λειτουργία των συστημάτων επικοινωνίας και πληροφοριών τους, καθώς και να ελαχιστοποιηθούν οι επιπτώσεις των συμβάντων. Τα συγκεκριμένα μέτρα αποτελούνται τόσο από μέτρα πρόληψης όσο και από μέτρα αντιμετώπισης. (ΥΨΗΠΤΕ, 2018).

Σε περίπτωση που προκύψει κάποιο περιστατικό οι φορείς πρέπει να είναι έτοιμοι να αντιδράσουν αποτελεσματικά. Ως εκ τούτου, είναι αναγκαίες οι τεχνικές γνώσεις, η ανάλυση των περιστατικών καθώς και η διάδοση της γνώσης του κάθε φορέα στους υπολοίπους, ούτως ώστε να αυξηθεί τόσο ο βαθμός ετοιμότητας όσο και η ικανότητα αντιμετώπισης συμβάντων όλων των φορέων. Την ευθύνη του συντονισμού των δράσεων κατά την περίπτωση των συμβάντων ασφαλείας φέρουν οι Ομάδες Απόκρισης για Συμβάντα που Αφορούν την Ασφάλεια των Υπολογιστών (ΥΨΗΠΤΕ, 2018).

Προβλέπονται Εθνικές Ασκήσεις Ετοιμότητας, οι οποίες πέραν των υπολοίπων οφελών τους, συνεισφέρουν στην ανταλλαγή πληροφοριών και γνώσεων, τη συνεργασία μεταξύ των φορέων που συμμετέχουν, καθώς και την ενδυνάμωση της κουλτούρας συνεργασίας για τη βελτίωση της διαδικτυακής ασφάλειας στη χώρα. Η γνώση που αποκτάται από τις ασκήσεις αυτές πρέπει να κοινοποιείται πέραν των εμπλεκομένων και στους υπόλοιπους αρμόδιους φορείς. Προς τη βελτίωση των

γνώσεων και ικανοτήτων των φορέων αυτών, επιδιώκεται η συμμετοχή της χώρας και σε διεθνείς και ευρωπαϊκές ασκήσεις ετοιμότητας (ΥΨΗΠΤΕ, 2018)

Η ευαισθητοποίηση των πολιτών και των χρηστών αναφέρεται ως ζωτικής σημασίας για τη χώρα. Προτείνεται η υλοποίηση κατάλληλων και στοχευμένων εκπαιδευτικών και ενημερωτικών εκστρατειών για τους υπαλλήλους των φορέων που συμμετέχουν στη στρατηγική, αλλά και τους υπόλοιπους πολίτες ώστε να ενισχυθούν οι γνώσεις τους σχετικά με τους διαδικτυακούς κινδύνους, κάτι το οποίο θα οδηγήσει στην ενίσχυση της προστασίας από τις πλέον διαδεδομένες απειλές και θα συμβάλει στην αύξηση του επιπέδου διαδικτυακής ασφάλειας της Ελλάδας (ΥΨΗΠΤΕ, 2018).

Οι δράσεις, οι μηχανισμοί και οι μέθοδοι που θα χρησιμοποιηθούν προς την κατεύθυνση της ευαισθητοποίησης πρέπει να είναι προσαρμοσμένοι στο κοινό που απευθύνονται. Τη σχεδίαση, οργάνωση και υλοποίηση του προγράμματος έχει αναλάβει η Εθνική Αρχή Κυβερνοασφαλείας, ενώ μέσα σε αυτό περιλαμβάνονται ενημερωτικές εκστρατείες για τους πολίτες, εκπαιδευτικές πρωτοβουλίες (σε συνεργασία με πανεπιστημιακούς φορείς) οι οποίες απευθύνονται στους διαχειριστές και χρήστες των συστημάτων ΤΠΕ των δημοσίων φορέων, προβολή σχετικού υλικού μέσω ιστοσελίδων (ΥΨΗΠΤΕ, 2018).

Αναφέρεται η ανάγκη συνεργασίας δημοσίων και ιδιωτικών φορέων για την ανταλλαγή πληροφοριών σχετικά με συμβάντα ασφαλείας, ούτως ώστε να ενισχύονται οι γνώσεις και των δύο. Τονίζεται ότι πρέπει να αναπτυχθούν κατάλληλοι μηχανισμοί, οι οποίοι θα ενισχύσουν την αξιόπιστη ανταλλαγή πληροφοριών, ενώ θα διέπονται από αμοιβαία εμπιστοσύνη και σεβασμό μεταξύ των φορέων που συμμετέχουν στη στρατηγική (ΥΨΗΠΤΕ, 2018).

Συνοψίζοντας, βλέπουμε ότι η Ελλάδα προχώρησε τελευταία σε σχέση με τις χώρες που εξετάσαμε στο προηγούμενο κεφάλαιο στην υλοποίηση μίας εθνικής στρατηγικής ασφαλείας. Επιπρόσθετα, εάν συγκριθεί με εκείνη των άλλων κρατών, η συγκεκριμένη στρατηγική φαίνεται μάλλον φτωχή. Δίδεται κατά κύριο λόγο έμφαση στην αύξηση των γνώσεων του προσωπικού των φορέων, δίδεται σημασία στον μεταξύ τους συντονισμό και τη συνεργασία, ενώ προβλέπεται και η ανταλλαγή σχετικών γνώσεων και πληροφοριών μεταξύ των πολιτών. Πραγματοποιείται

αναφορά και στους πολίτες, οι οποίοι αναφέρεται ότι θα πρέπει να αποκτήσουν επίγνωση της σημασίας της ασφάλειας και να υιοθετήσουν τις κατάλληλες συμπεριφορές. Προς τη συγκεκριμένη κατεύθυνση, έχει αναγγελθεί μία σειρά από εκπαιδευτικές δράσεις. Στην επόμενη παράγραφο θα εξετάσουμε το προφίλ ασφαλείας των Ελλήνων πολιτών, ούτως ώστε να προχωρήσουμε και στην υλοποίηση των δικών μας προτάσεων προς τη συγκεκριμένη κατεύθυνση. Για τη διαδικασία της αξιολόγησης θα χρησιμοποιήσουμε τις οκτώ πτυχές της κουλτούρας ασφαλείας που προσδιορίστηκαν από τους Malmedal και Røislien (2016) και παρουσιάστηκαν στη μελέτη περίπτωσης της Νορβηγίας.

4.3. Προφίλ ασφαλείας των Ελλήνων πολιτών

Σε έρευνα του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου αναφέρεται ότι η πλειοψηφία των Ελλήνων πολιτών αγνοεί τους βασικούς κανόνες ασφαλείας κατά τη χρήση του διαδικτύου (Παπαματθαίου, 2015). Το 40% των συμμετεχόντων δήλωσε ότι δεν γνωρίζει το περιεχόμενο της Πολιτικής Απορρήτου ενός ιστότοπου, ενώ το 30% δήλωσε άγνοια σχετικά με το περιεχόμενο των Όρων Χρήσης. Τα αποτελέσματα αυτά υποδεικνύουν ένα έλλειμμα επιμόρφωσης πάνω στον τομέα της ασφάλειας.

Σε δημοσκόπηση η οποία διεξήχθη για λογαριασμό του βρετανικού ειδησεογραφικού πρακτορείου BBC World σε διάφορες χώρες, η Ελλάδα ήταν η χώρα με το μεγαλύτερο ποσοστό πολιτών (84%) το οποίο αντιτίθεται στον έλεγχο του διαδικτύου από τις κυβερνήσεις. Επιπρόσθετα, η πλειοψηφία των Ελλήνων δήλωσε ότι αποφεύγει να εκφράζει ελεύθερα τις απόψεις της στο διαδίκτυο. Επίσης, χαρακτηρίζουν την πρόσβαση σε αυτό θεμελιώδες δικαίωμα (Capital, 2017). Οι απαντήσεις αυτές υποδεικνύουν ένα ενδιαφέρον για τις ΤΠΕ και την τεχνολογία, αλλά και μία αρνητική στάση προς τη διακυβέρνηση και τον έλεγχο, καθώς και μία έλλειψη εμπιστοσύνης προς τις αρχές.

Σε μελέτη της Google και του ΙΟΒΕ σχετικά με το διαδίκτυο στην Ελλάδα (Τσακανίκας, 2013) πάντως αναφέρεται χαμηλότερη χρήση του διαδικτύου σε σχέση με την ΕΕ (53% χρήση του διαδικτύου στην Ελλάδα έναντι 73% του ευρωπαϊκού μέσου όρου), αν και σημειώνονται αυξητικές τάσεις με γρήγορους ρυθμούς. Το διαδίκτυο

αναφέρεται ότι χρησιμοποιούν κατά κύριο λόγο οι νέοι, τα άτομα με υψηλή μόρφωση, υψηλό εισόδημα και οι κάτοικοι των αστικών περιοχών. Επιπρόσθετα, αναφέρεται ότι αυξάνεται η ζήτηση για τις υπηρεσίες της ηλεκτρονικής διακυβέρνησης. Ο πλέον σημαντικός παράγοντας αποτροπής από τη χρήση του διαδικτύου αναφέρεται ότι είναι η ασφάλεια των συναλλαγών. Ως αποτρεπτικοί παράγοντες αναφέρονται η ανησυχία για την ασφάλεια των προσωπικών δεδομένων και η περιορισμένη εμπιστοσύνη (στα πλαίσια της ασφάλειας συναλλαγών), η υστέρηση στην ανάπτυξη των απαραίτητων δεξιοτήτων (στα πλαίσια των κοινωνικών παραγόντων). Τα στοιχεία αυτά μας υποδεικνύουν αφενός το γεγονός του ότι υπάρχουν διαφοροποιήσεις μεταξύ των πολιτών και αφετέρου επιβεβαιώνουν την έλλειψη εμπιστοσύνης αλλά και το έλλειμμα ικανοτήτων. Επιπρόσθετα, υποδεικνύουν και ένα επίπεδο αντίληψης κινδύνου. Εάν λάβουμε υπόψη μας τις ομάδες που αποφεύγουν τη χρήση του διαδικτύου, θα μπορούσαμε να συμπεράνουμε ότι πρέπει να υλοποιηθούν στοχευμένες πολιτικές προς τις συγκεκριμένες κατηγορίες ατόμων.

Σε άλλη έρευνα που διεξήχθη μέσω ερωτηματολογίων (Σκάρτσου, 2018) οι περισσότεροι από τους ερωτηθέντες δήλωσαν ότι έχουν ελάχιστη έως καθόλου γνώση των δικαιωμάτων τους σε σχέση με τις διαδικτυακές εφαρμογές που χρησιμοποιούν. Επιπρόσθετα, θεωρούν ότι δεν πρόκειται να πέσουν ποτέ θύματα του κυβερνοεγκλήματος και σε περίπτωση που πέσουν θα απευθυνθούν στη Δίωξη Ηλεκτρονικού Εγκλήματος. Από την άλλη πλευρά, θεωρούν το νομοθετικό πλαίσιο αδύναμο και τα αρμόδια όργανα ανενημέρωτα σε σχέση με τις εξελίξεις της τεχνολογίας. Επιπρόσθετα, παρατηρούνται και εδώ διαφορές μεταξύ των κοινωνικών ομάδων, με την πλειοψηφία των χρηστών του διαδικτύου να αποτελείται από νέους και αποφοίτους τριτοβάθμιας εκπαίδευσης. Τα συγκεκριμένα αποτελέσματα επιβεβαιώνουν το έλλειμμα ικανοτήτων των Ελλήνων σχετικά με τη διαδικτυακή ασφάλεια. Επίσης, διαφαίνεται μία έλλειψη αντίληψης του κινδύνου. Τέλος, διαφαίνεται μία θετική στάση σχετικά με τη διακυβέρνηση και τον έλεγχο, καθώς υπάρχει διάθεση συνεργασίας με τη Δίωξη Ηλεκτρονικού Εγκλήματος, αλλά και μία έλλειψη εμπιστοσύνης προς τις αρχές, καθώς αμφισβητείται το επίπεδο ικανοτήτων και γνώσεων τους.

Σε μία ακόμα έρευνα που διεξήχθη με τη χρήση ερωτηματολογίων (Κατσαράκη, 2013), λίγοι περισσότεροι από τους μισούς ερωτηθέντες (το 54%) δήλωσαν ότι χρησιμοποιούν το διαδίκτυο για τη διεκπεραίωση των συναλλαγών τους με το δημόσιο. Το 47% των ερωτηθέντων δήλωσε ότι το διαδίκτυο δεν έχει αρκετές δικλείδες ασφαλείας. Αναφορικά με τη χρήση των υπηρεσιών ηλεκτρονικής διακυβέρνησης, το 39,8% θεωρεί ότι το διαδίκτυο αποτελεί ένα ασφαλές περιβάλλον για αυτές, ενώ το 32,7% διαφωνεί και το 27,6% δεν μπορεί να εκφέρει γνώμη. Επιπρόσθετα, το 30% των ερωτηθέντων θεωρεί ότι υπάρχουν κίνδυνοι στο διαδίκτυο, ενώ η συντριπτική πλειοψηφία των ερωτηθέντων θεωρεί ότι και οι ηλεκτρονικές συναλλαγές εμπεριέχουν πολλούς κινδύνους. Το μεγάλο ποσοστό των ατόμων που χρησιμοποιούν το διαδίκτυο για τη διεκπεραίωση συναλλαγών υπονοεί ένα ενδιαφέρον για την τεχνολογία και τις ΤΠΕ. Όσον αφορά την εκτίμηση κινδύνου, τα αποτελέσματα είναι μοιρασμένα. Ειδικά για τις εφαρμογές της ηλεκτρονικής διακυβέρνησης πάντως, η πλειοψηφία των ερωτηθέντων αναγνωρίζει την ύπαρξη κινδύνων, οπότε μπορούμε να πούμε ότι υπάρχει το συγκεκριμένο στοιχείο.

Σε έρευνα για τη διαδικτυακή ασφάλεια της ΕΕ (European Commission, 2015) αναφέρεται ότι το 58% των Ελλήνων χρηστών του διαδικτύου έχει εγκαταστήσει αντιιικό λογισμικό στον υπολογιστή του, το 49% δεν ανοίγει e-mail προερχόμενα από άτομα τα οποία δεν γνωρίζει, το 39% είναι λιγότερο πιθανό να παράσχει προσωπικά δεδομένα σε ιστοσελίδες, το 32% δηλώνει ότι χρησιμοποιεί μόνο τον προσωπικό του υπολογιστή, το 43% ότι επισκέφτεται μόνο ιστότοπους τους οποίους γνωρίζει και εμπιστεύεται, το 16% ότι χρησιμοποιεί διαφορετικούς κωδικούς σε διαφορετικές ιστοσελίδες, το 27% ότι αλλάζει συχνά τους κωδικούς του και το 14% ότι έχει τροποποιήσει τις ρυθμίσεις ασφαλείας του ούτως ώστε να γίνουν περισσότερο αποτελεσματικές. Τα συγκεκριμένα αποτελέσματα αναφέρεται ότι είναι βελτιωμένα σε σχέση με εκείνα προγενέστερης αντίστοιχης έρευνας που είχε πραγματοποιηθεί το 2013. Η Ελλάδα πάντως εξακολουθεί να υστερεί σε σχέση με τον ευρωπαϊκό μέσο όρο σε αρκετές κατηγορίες (χρήση αντιιικού λογισμικού, διαφορετικοί κωδικοί ασφαλείας – το χαμηλότερο ποσοστό σε ευρωπαϊκό επίπεδο, βελτίωση των ρυθμίσεων ασφαλείας), γεγονός το οποίο υποδεικνύει ένα έλλειμμα ικανοτήτων και ενημέρωσης σχετικά με τις πρακτικές ασφαλείας. Το υψηλό ποσοστό ατόμων τα

οποία δεν έχουν εγκατεστημένα αντιιικά λογισμικά στους υπολογιστές τους μας υποδεικνύει ότι ένα μεγάλο ποσοστό των Ελλήνων χρηστών του διαδικτύου είναι ευάλωτοι στο κυβερνοέγκλημα. Επιπρόσθετα, σε ερώτηση σχετικά με την αλλαγή του κωδικού πρόσβασης στις εφαρμογές της ηλεκτρονικής διακυβέρνησης κατά τους τελευταίους μήνες η Ελλάδα είχε ένα από τα χαμηλότερα ποσοστά (μόλις 3% έναντι 8% του ευρωπαϊκού μέσου όρου).

Σχετικά με τους διαδικτυακούς κινδύνους, το 11% θεωρεί ότι έχει άριστο επίπεδο γνώσεων, ενώ το 32% των Ελλήνων θεωρεί ότι είναι καλά πληροφορημένο για αυτούς. Το 23% θεωρεί ότι έχει μέτριο επίπεδο γνώσεων, ενώ το 33% δεν έχει πληροφορηθεί καθόλου. Η χώρα αποδίδει και εδώ κάτω από τον ευρωπαϊκό μέσο όρο (European Commission, 2015). Το έλλειμμα γνώσεων και ικανοτήτων επομένως επιβεβαιώνεται και από εδώ.

Το 83% πάντως δηλώνει ότι κινδυνεύει να πέσει θύμα του κυβερνοεγκλήματος (European Commission, 2015), γεγονός το οποίο υποδεικνύει την ύπαρξη ενός επιπέδου αντίληψης κινδύνου. Επιπρόσθετα, το 84% θεωρεί ότι οι προσωπικές του πληροφορίες δεν διατηρούνται ασφαλείς από τις ιστοσελίδες, γεγονός το οποίο υπονοεί την έλλειψη εμπιστοσύνης. Το ίδιο ισχύει και για τις δημόσιες αρχές (79% δηλώνει ότι δεν θεωρεί πως διατηρούν ασφαλή τα δεδομένα του). Το 71% δηλώνει ότι μπορεί να προστατεύσει επαρκώς τον εαυτό του από το κυβερνοέγκλημα, γεγονός όμως το οποίο έρχεται σε αντίθεση με τις απαντήσεις που δόθηκαν σχετικά με την υιοθέτηση των βέλτιστων πρακτικών ασφαλείας, κάτι το οποίο υποδεικνύει έλλειμμα γνώσεων και ικανοτήτων αυτό-αξιολόγησης. Το επίπεδο αντίληψης κινδύνου επιβεβαιώνεται από το ότι οι Έλληνες θεωρούν ότι κινδυνεύουν από όλες τις κατηγορίες των διαδικτυακών εγκλημάτων περισσότερο σε σχέση με τους Ευρωπαίους. Από την άλλη πλευρά, η πλειοψηφία των πολιτών της χώρας δεν θεωρεί ότι απειλείται από το ενδεχόμενο διακοπής της πρόσβασης της στις διαδικτυακές υπηρεσίες λόγω κυβερνοεπιθέσεων. Το 47% θεωρεί ότι γενικά κινδυνεύει από τις διαδικτυακές απειλές, ποσοστό παρόμοιο του ευρωπαϊκού. Επιπρόσθετα, παρουσιάζεται το δεύτερο μεγαλύτερο ευρωπαϊκό ποσοστό ανησυχίας σχετικά με την προσβολή των συσκευών των χρηστών από κακόβουλο λογισμικό.

Στην περίπτωση κατά την οποία οι ερωτηθέντες λάβουν κάποιο e-mail το οποίο αποσκοπεί στην υποκλοπή των προσωπικών τους στοιχείων, μία σημαντική μερίδα τους δήλωσε ότι θα επικοινωνήσει με τον διαδικτυακό της πάροχο (28%, ένα από τα μεγαλύτερα ποσοστά σε ευρωπαϊκό επίπεδο) και όχι με κάποιον κρατικό φορέα (αστυνομία, οργανισμοί προστασίας του κοινού) (European Commission, 2015). Το ποσοστό αυτό υποδεικνύει μία τάση απόρριψης της διακυβέρνησης και του ελέγχου. Μία παρόμοια τάση (μείωση του ποσοστού που θα επέλεγε την αστυνομία και αύξηση του ποσοστού που θα απευθύνονταν στον διαδικτυακό του πάροχο) για την περίπτωση της παραβίασης του e-mail επεβαιώνει αυτό το χαρακτηριστικό.

Εξετάζοντας τα αποτελέσματα των παραπάνω ερευνών μπορούμε να σκιαγραφήσουμε ορισμένα χαρακτηριστικά του προφίλ ασφαλείας των Ελλήνων πολιτών. Εάν αναλογιστούμε ότι οι υπηρεσίες ηλεκτρονικής διακυβέρνησης χρησιμοποιούνται από τους πολίτες αυτούς (τόσο ως υπαλλήλους όσο και ως συναλλασσόμενους), μπορούμε να αντιληφθούμε ότι τα χαρακτηριστικά αυτά θα μας βοηθήσουν να προτείνουμε ορισμένες πολιτικές οι οποίες θα συμβάλλουν στην αύξηση της κουλτούρας ασφαλείας στο συγκεκριμένο πεδίο εφαρμογής. Κυριότερο χαρακτηριστικό που διαφαίνεται από τα παραπάνω είναι η έλλειψη γνώσεων και ικανοτήτων σχετικά με τη διαδικτυακή ασφάλεια. Το γεγονός αυτό αφήνει ένα μεγάλο ποσοστό των Ελλήνων χρηστών του διαδικτύου ευάλωτο σε κακόβουλες ενέργειες, καθώς δεν γνωρίζει πως να προστατευτεί. Επιπρόσθετα, διαφαίνεται ένα έλλειμμα εμπιστοσύνης προς τις αρχές, τόσο όσον αφορά τον τρόπο με τον οποίο θα επεξεργαστούν τα δεδομένα των πολιτών όσο και για την ασφάλεια των συστημάτων τους. Οι πολίτες φαίνεται ότι αντιλαμβάνονται πως η χρήση του διαδικτύου εγκυμονεί αρκετούς κινδύνους. Όσον αφορά τη διακυβέρνηση και τον έλεγχο, τείνουν να έχουν μία αρνητική στάση αν και όχι τόσο απόλυτη, καθώς εκφράστηκαν αντιθέσεις τόσο σχετικά με τον έλεγχο του διαδικτύου από το κράτος, ενώ όσον αφορά τη συνεργασία με τη Δίωξη Ηλεκτρονικού Εγκλήματος έχουν εκφραστεί τόσο θετικές όσο και αρνητικές γνώμες. Επίσης, εκδηλώνεται ένα ενδιαφέρον για τις ΤΠΕ και την τεχνολογία, εάν αναλογιστούμε το ότι σημειώνονται μεγάλα ποσοστά χρήσεως του διαδικτύου και των εφαρμογών της ηλεκτρονικής διακυβέρνησης. Ένα ακόμα στοιχείο που πρέπει να ληφθεί υπόψη μας είναι τα κοινωννικά

χαρακτηριστικά των χρηστών, οι οποίοι κατά κύριο λόγο είναι νέοι, άτομα με υψηλή μόρφωση και/ή υψηλό εισόδημα και κάτοικοι αστικών περιοχών.

4.4. Προτάσεις για την ενίσχυση της κουλτούρας ασφαλείας στην Ελλάδα

Τα ευρήματα της προηγούμενης παραγράφου καθιστούν ξεκάθαρη την ανάγκη υλοποίησης πολιτικών ούτως ώστε να ενισχυθεί η κουλτούρα ασφαλείας των Ελλήνων πολιτών. Η συγκεκριμένη ανάγκη άλλωστε αναφέρεται και στη Στρατηγική της χώρας για την Κυβερνοασφάλεια. Προς τη συγκεκριμένη κατεύθυνση θα μπορούσαν να υλοποιηθούν συνεργασίες μεταξύ του δημοσίου και ιδιωτικών φορέων και επιχειρήσεων (όπως συμβαίνει και στις χώρες του εξωτερικού που εξετάσαμε). Τον κυριότερο ρόλο όμως θα πρέπει να διαδραματίσει η κυβέρνηση, καθώς με τον τρόπο αυτό θα διασφαλιστεί μία σωστά συντονισμένη, ενοποιημένη και αποτελεσματική προσέγγιση η οποία θα απαντήσει κατά τον βέλτιστο δυνατό τρόπο στο πρόβλημα. Δεν είναι τυχαίο άλλωστε, ότι και στις υπόλοιπες χώρες οι σχετικές διαδικασίες συντονίζονται από την κυβέρνηση, ενώ κάτι τέτοιο προβλέπεται και από την ελληνική στρατηγική. Η σημασία της ηγεσίας της κυβέρνησης στην εν λόγω προσπάθεια ενισχύεται από το γεγονός του ότι αναφερόμαστε στις υπηρεσίες της ηλεκτρονικής διακυβέρνησης, δηλαδή τη διεκπεραίωση των λειτουργιών της κρατικής μηχανής με τη βοήθεια του διαδικτύου. Βάσει των προηγούμενων ευρημάτων θα μπορούσαμε να προτείνουμε τις επόμενες πολιτικές προς υλοποίηση:

1. Διαφαίνεται ξεκάθαρα ότι υπάρχει ένα τεράστιο έλλειμμα επιμόρφωσης και γνώσεων σχετικά με τη διαδικτυακή ασφάλεια. Το όποιο περιεχόμενο των εκπαιδευτικών προγραμμάτων σε σχολεία κλπ. αποδεικνύεται μάλλον άστοχο. Από την άλλη πλευρά οι χρήστες φαίνεται ότι κατανοούν πως το διαδίκτυο εγκυμονεί κινδύνους. Επίσης παρουσιάζουν ενδιαφέρον για τις ΤΠΕ και τη νέα τεχνολογία. Ως εκ τούτου, θα μπορούσαμε να υποθέσουμε ότι είναι θετικά διακείμενοι σε εκπαιδευτικές δράσεις. Οι δράσεις αυτές βέβαια θα πρέπει να είναι στοχευμένες προς τις διάφορες ομάδες που χρησιμοποιούν το διαδίκτυο (οι οποίες παρουσιάζουν ορισμένες διαφοροποιήσεις).

Επιπρόσθετα, θα μπορούσαν να υλοποιηθούν και εκπαιδευτικές δράσεις για τις ομάδες που προς το παρόν απέχουν από τη χρήση του. Οι δράσεις που θα σχεδιαστούν για τη δεύτερη υπό-ομάδα πολιτών, πέραν της διάστασης της επιμόρφωσης στην ασφάλεια θα πρέπει να επεξηγήσουν και τα οφέλη που προκύπτουν για τους πολίτες από την ηλεκτρονική διακυβέρνηση ούτως ώστε να την καταστήσουν ελκυστική προς αυτούς. Γενικότερα, θα πρέπει να υιοθετηθούν πολυδιάστατες εκπαιδευτικές μέθοδοι και προοπτικές, ούτως ώστε να καλυφθούν οι ανάγκες όλων των ομάδων, κάτι το οποίο είναι μάλλον αδύνατο να γίνει εάν εφαρμοστεί μία μονοδιάστατη προσέγγιση. Αρχικά, θα πρέπει να πραγματοποιηθούν εκπαιδευτικές δράσεις για τους νέους, στα πλαίσια της ανάπτυξης υπεύθυνων πολιτών. Πέραν της χρήσης της τεχνολογίας, θα πρέπει να διδάσκονται και το πως να συμπεριφέρονται με ασφάλεια σε ένα περιβάλλον όπου η χρήση των ΤΠΕ σταδιακά καθίσταται ραγδαία. Προς τη συγκεκριμένη κατεύθυνση, πρέπει να εμπλουτιστούν κατάλληλα τα σχολικά προγράμματα. Επιπρόσθετα, πρέπει να υλοποιηθούν στοχευμένα εκπαιδευτικά προγράμματα για την κάθε ομάδα που χρησιμοποιεί τις εφαρμογές των υπηρεσιών της ηλεκτρονικής διακυβέρνησης.

2. Η αρνητική στάση προς τη διακυβέρνηση και τον έλεγχο, αλλά και η έλλειψη εμπιστοσύνης προς τους κρατικούς φορείς είναι επίσης ένα ζήτημα το οποίο χρήζει αντιμετώπισης. Θα πρέπει να οικοδομηθεί η εμπιστοσύνη των πολιτών προς το κράτος, από τη στιγμή που αυτό έχει την αρμοδιότητα της άσκησης εξουσίας στο διαδίκτυο και της ρύθμισης του. Οι πολίτες θεωρούν ανεπαρκές το επίπεδο των γνώσεων και ικανοτήτων των αντίστοιχων φορέων. Εάν λάβουμε υπόψη και το κενό γνώσεων που παρατηρείται γενικότερα στην ελληνική κοινωνία, θα μπορούσαμε να προτείνουμε την υλοποίηση κατάλληλων εκπαιδευτικών πολιτικών για το προσωπικό των δημοσίων οργανισμών, αλλά και την αστυνομία, καθώς και την παροχή του κατάλληλου εξοπλισμού ούτως ώστε να είναι σε θέση να εντοπίζουν πιθανές απόπειρες πραγματοποίησης κακόβουλων ενεργειών στα συστήματα που διαχειρίζονται, να εφαρμόζουν αποτελεσματικά τις πολιτικές ασφαλείας των οργανισμών που εργάζονται και η αστυνομία να είναι σε θέση να

καταπολεμάει αποφασιστικά κάθε περίπτωση διαδικτυακού εγκλήματος. Γενικότερα, πρέπει να δοθεί προτεραιότητα σε δράσεις αυτού του είδους, καθώς και να επικοινωνηθούν κατάλληλα προς τους πολίτες, ούτως ώστε να ανακτηθεί η εμπιστοσύνη τους. Επιπρόσθετα, πρέπει να παρακολουθείται ανά τακτά χρονικα διαστήματα η γνώμη των πολιτών πάνω στα συγκεκριμένα ζητήματα καθώς και να τους δοθεί η δυνατότητα να εκφράζουν διάφορες παρατηρήσεις σε κατάλληλα όργανα, ούτως ώστε αυτές να αξιολογούνται και εάν κρίνεται αναγκαίο να λαμβάνονται επιπρόσθετες δράσεις.

3. Πρέπει να ενεργοποιηθούν τα διοικητικά στελέχη των δημοσίων οργανισμών ώστε να λάβουν μέρος στη διαδικασία της ενίσχυσης της κουλτούρας ασφαλείας. Προς τη συγκεκριμένη κατεύθυνση, θα πρέπει να θέσουν το ζήτημα της διαδικτυακής ασφάλειας ως μείζονος σημασίας κατά μήκος του οργανισμού που διοικούν. Επιπρόσθετα, μία αποδοτική πρακτική θα ήταν η ανάθεση του συγκεκριμένου ζητήματος σε ένα ανώτερο διοικητικό στέλεχος, το οποίο είτε θα είναι μέλος της διοίκησης του οργανισμού είτε θα αναφέρεται άμεσα σε αυτήν. Αναγκαία είναι και η παροχή τακτικών αναφορών προς τη διοίκηση, ούτως ώστε να αξιολογείται το επίπεδο της κουλτούρας ασφαλείας κατά μήκος του οργανισμού και να προτείνονται πολιτικές και πόροι που θα κατευθύνονται προς τον συνεχή σηματισμό και τη διατήρηση της. Τα στελέχη των οργανισμών πρέπει να δρουν σύμφωνα με το συγκεκριμένο πλαίσιο, αποτελώντας παραδείγματα για τους υπαλλήλους και επιλύοντας οποιαδήποτε απορία έχουν.
4. Προς την οικοδόμηση μίας κουλτούρας ασφαλείας θα μπορούσε να συμβάλλει και η ανταλλαγή γνώσεων με χώρες οι οποίες έχουν μεγαλύτερη εμπειρία σε σχέση με την Ελλάδα πάνω στο συγκεκριμένο ζήτημα, ούτως ώστε να αξιοποιηθούν οποιαδήποτε σημεία της προϋπάρχουσας γνώσης ταιριάζουν με τη χώρα μας.

Συμπεράσματα

Η Ηλεκτρονική Διακυβέρνηση συνίσταται στη διεκπεραίωση των λειτουργιών του δημοσίου μέσω των ηλεκτρονικών υπολογιστών και με τη βοήθεια του διαδικτύου. Προσφέρει σημαντικά οφέλη στην κοινωνία, καθώς οδηγεί σε εξοικονόμηση πόρων,

καλύτερη εξυπηρέτηση των συναλλασσόμενων με τις υπηρεσίες, βελτίωση της διαφάνειας και πάταξη της διαφθοράς. Για την επιτυχία των σχετικών εφαρμογών πάντως απαιτείται κατάλληλος σχεδιασμός, εξέταση διαφόρων παραμέτρων (που απευθύνεται η εφαρμογή, ποιους εξυπηρετεί, φιλοσοφία οργανισμού κλπ.) και κατάλληλος συντονισμός και συνεργασία μεταξύ των ειδικών των ΤΠΕ που θα αναλάβουν την υλοποίηση τους και του φορέα ο οποίος θα τη διαχειρίζεται. Οι σχετικές πλατφόρμες γνωρίζουν ολοένα και μεγαλύτερη διάδοση, ενώ θα μπορούσαμε να αποτολμήσουμε και κάποια πρόβλεψη σχετικά με το ότι σε μακροπρόθεσμο χρονικό ορίζοντα θα κυριαρχήσουν ολοκληρωτικά στις συναλλαγές πολιτών – επιχειρήσεων και δημοσίου.

Από τη στιγμή που οι σχετικές υπηρεσίες διασυνδέονται και λειτουργούν βασιζόμενες πάνω στο διαδίκτυο δεν μπορεί να αγνοηθεί και το ζήτημα της ασφάλειας, ειδικά εάν αναλογιστούμε τη σημασία των δεδομένων που διαχειρίζονται και που αποθηκεύονται σε αυτές. Υπάρχει ένα πλήθος τεχνικών μεθόδων και πολιτικών για την προστασία από τους διαδικτυακούς κινδύνους, αλλά δεν μπορούν να αποδώσουν από μόνες τους. Το σημαντικότερο στοιχείο για την επίτευξη της ασφάλειας, από τη στιγμή που την εφαρμογή των μεθόδων αναλαμβάνουν άνθρωποι, είναι οι στάσεις και οι συμπεριφορές των χρηστών τους. Η κουλτούρα ασφαλείας περιγράφει ακριβώς αυτές τις συμπεριφορές. Συνοψίζεται στην υιοθέτηση μίας υπεύθυνης στάσης σχετικά με τη χρήση του διαδικτύου, στον σεβασμό των πολιτικών ασφαλείας, την υιοθέτηση των εφαρμοζόμενων μέτρων και πολιτικών, καθώς και τη συνεχή επιμόρφωση σχετικά με τους νέους κινδύνους και τις μεθόδους αντιμετώπισης τους. Υπό το πρίσμα της ηλεκτρονικής διακυβέρνησης, αφορά την κυβέρνηση μίας χώρας (καθώς εποπτεύει όλους τους δημοσίους οργανισμούς και την εφαρμογή πολιτικών και στρατηγικών), τα διοικητικά στελέχη των δημοσίων οργανισμών (οι οποίοι έχουν την ευθύνη της εμφύσησης της στον οργανισμό που διοικούν, καθώς και το καθήκον του να αποτελούν ένα θετικό παράδειγμα προς τους υφισταμένους τους), τους υπαλλήλους (οι οποίοι διαχειρίζονται τα συστήματα του οργανισμού και πρέπει να ενστερνίζονται και να υλοποιούν τις πολιτικές ασφαλείας του, καθώς και να συμμετέχουν σε ενημερωτικές δράσεις) και βέβαια τους πολίτες (οι οποίοι συναλλάσσονται με τις υπηρεσίες της

ηλεκτρονικής διακυβέρνησης και οφείλουν να υιοθετούν μία εν γένει ασφαλή διαδικτυακή συμπεριφορά). Ο ρόλος των πολιτών είναι ιδιαίτερα σημαντικός στο πεδίο της ηλεκτρονικής διακυβέρνησης, καθώς έρχονται σε επαφή με τις πλατφόρμες του δημοσίου μέσα από τους προσωπικούς τους υπολογιστές, επομένως πρέπει να υιοθετούν μία γενικότερη ασφαλή διαδικτυακή συμπεριφορά, καθώς ένα άτομο είναι σε θέση να επηρεάσει την ελαστικότητα ενός ολόκληρου διαδικτυακού συστήματος. Η σχέση ατόμου και συνόλου έχει παρομοιαστεί με εκείνη της διάδοσης των ιών και της αντιμετώπισης τους στη θεωρία του εμβολιασμού στην ιατρική (Malmedal και Røislien, 2016). Επομένως γίνεται ξεκάθαρη η σημασία της τήρησης των κανόνων ασφαλής πλοήγησης από τον κάθε πολίτη ξεχωριστά.

Η σημασία της κουλτούρας ασφαλείας γίνεται κατανοητή και από το ότι όλες οι χώρες που εξετάσθηκαν στις μελέτες περιπτώσεων ενσωματώνουν στις εθνικές τους στρατηγικές διαδικτυακής ασφαλείας πτυχές της, δίδοντας μάλιστα ιδιαίτερη σημασία στην ευαισθητοποίηση του κοινού σχετικά με τους διαδικτυακούς κινδύνους. Η στρατηγική της Ελλάδας είναι λιγότερο περιεκτική σε σχέση με εκείνη των άλλων χωρών, κάτι το οποίο μπορούμε να αποδώσουμε στο ότι εκπονήθηκε με κάποια καθυστέρηση σε σχέση με εκείνες, οπότε δεν υπάρχει κάποια πρότερη εμπειρία. Η ανάπτυξη μίας κουλτούρας ασφαλείας πάντως στη χώρα αναφέρεται ξεκάθαρα στις στοχεύσεις της. Επιπρόσθετα, κατά τα τελευταία χρόνια έχει αναπτυχθεί μία πληθώρα εφαρμογών οι οποίες εντάσσονται στα πλαίσια της ηλεκτρονικής διακυβέρνησης. Το κοινό της χώρας πάντως θα μπορούσε να χαρακτηριστεί διαδικτυακά ανώριμο. Από τη μία εκδηλώνει ενδιαφέρον για τις σύγχρονες τεχνολογίες, ενώ χρησιμοποιεί κατά ένα συνεχώς αυξανόμενο ποσοστό τις νέες εφαρμογές για τη διεκπεραίωση των συναλλαγών του με το δημόσιο. Από την άλλη όμως διαπιστώνεται ένα ξεκάθαρο κενό γνώσεων και ικανοτήτων αντιμετώπισης των διαδικτυακών απειλών, καθώς και ένα έλλειμμα εμπιστοσύνης προς τους αρμόδιους φορείς αντιμετώπισης τους και το κράτος, το οποίο διαδραματίζει τον θεσμικό ρόλο της εποπτείας και ρύθμισης του διαδικτύου. Οι πολίτες αναγνωρίζουν πάντως τους κινδύνους που εγκυμονεί η χρήση των διαδικτύων, οπότε μπορούμε να διακρίνουμε ένα ευνοϊκό κλίμα για την καλλιέργεια μίας κουλτούρας ασφαλείας. Προς τη συγκεκριμένη κατεύθυνση θεωρούμε ότι θα

πρέπει να υλοποιηθεί μία πληθώρα εκπαιδευτικών δράσεων, στοχευμένων στις διάφορες ομάδες που χρησιμοποιούν το διαδίκτυο, οι οποίες διέπονται από διαφορετικά χαρακτηριστικά. Επιπρόσθετα, πρέπει να υλοποιηθούν δράσεις ενίσχυσης του προσωπικού των δημοσίων φορέων και της αστυνομίας τόσο από πλευράς παροχής πόρων όσο και από την πλευρά της κατάλληλης επιμόρφωσης τους, ενώ παράλληλα θα πρέπει να επικοινωνηθεί στο κοινό η αναβάθμιση των ικανοτήτων των αρμόδιων φορέων, καθώς και των μέτρων προστασίας που λαμβάνουν ούτως ώστε να οικοδομηθεί η εμπιστοσύνη των πολιτών προς αυτούς. Ταυτόχρονα, τα διοικητικά στελέχη των οργανισμών πρέπει να δώσουν ιδιαίτερη σημασία στην ανάπτυξη της κουλτούρας ασφαλείας στους φορείς που εποπτεύουν, τόσο υλοποιώντας σχετικές διαδικασίες όσο και δίδοντας οι ίδιοι το παράδειγμα προς το προσωπικό. Τέλος, ο διάλογος με τρίτες χώρες, οι οποίες έχουν σημειώσει επιτυχίες σε αυτόν τον τομέα θα μπορούσε να συμβάλλει σημαντικά προς την κατεύθυνση της ανάπτυξης κουλτούρας ασφαλείας, μέσα από την απόκτηση έμπρακτων γνώσεων, εμπειριών και συμβουλών.

Βιβλιογραφία

Akman, I., Yazici, A., Mishra, A., and Arifoglu, A. (2005). E-Government: A global view and an empirical evaluation of some attributes of citizens. *Government Information Quarterly*, 22, pp. 239-257

AlAwadhi, S., and Morris, A. (2009). Factors Influencing the Adoption of E-government Services. *Journal of Software*, 4(6), pp. 584-590

AlKalbani, A., Deng, H., Kam, B. (2015). Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure. PACIS 2015 Proceedings 65.

Brown, M.M. (2003). Electronic Government. In: Jack Rabin (Ed.), *Encyclopedia of Public Administration and Public Policy*. pp. 427 – 432, New York: Marcel Dekker

Capital. (2017). Αυξάνονται οι ανησυχίες για τις ψευδείς ειδήσεις στο Διαδίκτυο. Διαθέσιμο στο link: http://www.capital.gr/technology/3241908/auxanontai-oi-anisuxies-gia-tis-pseudeis-eidiseis-sto-diadiktuo. Προσπελάστηκε στις: 6/8/2018.

Chang, S.E., and Lin, C.S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems,* 107(3), pp. 438-458

Cox, S., and Cox, T. (1991). The structure of employee attitudes to safety - a European Example. *Work and Stress*, 5, pp. 93-106

Dhillon, G, and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), pp. 293-314

Drogkaris, P., Gritzalis, S., and Lambrinoudakis, C. (2010). Transforming the Greek E-Government Environment towards the E-Gov 2.0 Era. In: R. Wagner (Editor), *EGOVIS' 10 International Conference on Electronic Government and the Information Systems Perspective,* Berlin: Springer

Ebrahim, Z., and Irani, Z. (2005). E-government adoption: architecture and barriers. *Business Process Management Journal*, 11 (5), pp. 589-611

European Commission. (2015). Cyber Security Report. Διαθέσιμο στο link: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf. Προσπελάστηκε στις: 7/8/2018.

European Union (E.U.). (2014). Regulation (EU) No 910/2014. Διαθέσιμο στο link: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG. Προσπελάστηκε στις: 30/6/2018

Finnish Secretariat of the Security and Defence Committee. (2013). Finnish National Cyber Security Strategy. Διαθέσιμο στο link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/finlands-cyber-security-strategy. Προσπελάστηκε στις: 5/8/2018.

Hahamis, P., Iles, J., and Healy, M. (2005). E-Government in Greece: Opportunities for Improving the Efficiency and Effectiveness of Local Government. Proceedings of the 5th European Conference on E-Government, Antwerp, Belgium.

Herath, T., and Rao, H.R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), pp. 106-125

IBMa. Symmetric cryptography. Διαθέσιμο στο link: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7symm.html. Προσπελάστηκε στις: 4/6/2018

IBMb. Public key cryptography. Διαθέσιμο στο link: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/s7pkey.html. Προσπελάστηκε στις: 10/7/2018

Kaliontzoglou, A., Sklavos, P., Karantjias, T., and Polemi, D. (2005). A secure e-Government platform architecture for small to medium sized public organizations. *Electronic Commerce Research and Applications*. 4, pp. 174–186

Karyda, M. (2017). Fostering Information Security Culture in Organizations: A research Agenda. The 11th Mediterranean Conference on Information Systems (MCIS), Genoa, Italy.

Lambrinoudakis, C., Gritzalis, S., Dridi, F., and Pernul, G. (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer Communications*, 26, pp. 1873-1883

Larsen, B., and Milakovich, M. (2005). Citizen Relationship Management and E-Government. *Lecture Notes in Computer Science*, 3591, pp. 57–68

Leavitt, H.J. (1965). *Applied Organizational Change in Industry*. Chicago: Rand McNally

Mahaman, B.D., Ntaliani, M.S., and Costopoulou, C.I. (2005). E-Government for Rural Development: Current Trents and Opportunities for Agriculture. Proceedings of the 005 EFITA/WCCA Joint Congress on IT in Agriculture, Vila Real, Portugal.

Malmedal, B., and Røislien, H.E. (2016). The Norwegian Cybersecurity culture. Gjøvik: Norwegian Centre for Information Security (NorSIS)

Moon, M.J. (2002). The evolution of e-government among Municipalities: Rhetoric or Reality? *Public Administration Review,* 62(4), pp. 424-433

Norris, F.D., and Moon, M.J. (2005). Advancing E-Government at the Grassroot: Tortoise or Hare? *Public Administration Review,* 65(1), pp. 64-75

OECD. (2005). The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries. *OECD Digital Economy Papers*, No. 102, Paris: OECD Publishing

Palanisamy, R. and Mukerji, B. (2012). Adoption of Open Source Software for Enhancing Customer Satisfaction: A Case Study from Canadian Educational Sector. *Journal of Services Research*, 12(2), pp. 7-27

Palvia, S.C.J. and Sharma, S.S. (2007). E-Government and E-Governance: Definitions/Domain Framework and Status around the World. Available at: https://www.researchgate.net/publication/268411808_E-Government_and_E-Governance_DefinitionsDomain_Framework_and_Status_around_the_World. Accessed at: 10/7/2018

Premier Ministre. (2015). French National Digital Security Strategy. Διαθέσιμο στο link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-

map/strategies/information-systems-defence-and-security-frances-strategy. Προσπελάστηκε στις: 3/6/2018.

Presidencia del Gobierno. (2013). Spanish National Cyber Security Strategy. Διαθέσιμο στο link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/the-national-security-strategy. Προσπελάστηκε στις: 19/6/2018.

Reffat, R. (2003). Developing a Successful E-Government. Proceedings of the Symposium on E-Government: Opportunities and Challenge, Muscat, Oman

Smith, S., Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. *Information Systems Management,* 23(2), pp. 23-32

Torres, L., Pina, V., and Royo, S. (2005). E-government and the transformation of public administrations in EU countries: Beyond NPM or just a second wave of reforms? *Online Information Review*, 29 (5), pp.531-553

WEF (World Economic Forum). (2016). The Global Information Technology Report 2016. Διαθέσιμο στο link: ://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf. Προσπελάστηκε στις: 1/7/2018

Williams, T.L., Becker, D., Redman, T.C., and Talburt, J. (2013). Modeling and Simulating the Impact of Social Issues on Information Quality: Literature Review. Conference Paper, International Conference on Information Quality, At Little Rock, November 2013

Γάκης, Κ. (2011). *Καλλικράτης: Ηλεκτρονική Διακυβέρνηση στην Αυτοδιοίκηση*. Αθήνα: ΕΕΤΑΑ

Γιαμπουράς, Γ.Μ. (2006). Η ηλεκτρονική διακυβέρνηση ως εργαλείο ελέγχου και χρηστής διαχείρισης, ο ρόλος των επιστημόνων Τεχνολογιών, Πληροφορικής και Επικοινωνιών. Πρακτικά του συνεδρίου Ηλεκτρονική Διακυβέρνηση κατά της Κακοδιαχείρισης και της Διαφθοράς, Αθήνα, Ελλάδα.

Γκρίτζαλης, Σ., Κάτσικας, Σ., Χρυσικόπουλος, Β., και Burmester, Μ. (2011). *Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές*. Αθήνα: Παπασωτηρίου

Κατσαράκη, Ε. (2013). *Η Στάση Πολιτών στην Ηλεκτρονική Διακυβέρνηση. Η Περίπτωση του Δήμου Ηρακλείου.* Πτυχιακή Εργασία, Καλαμάτα: ΑΤΕΙ Καλαμάτας

Μαυρίδης, Ι. (2015). *Ασφάλεια πληροφοριών στο διαδίκτυο*. Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών

Παπαματθαίου, Μ. (2015). Οι Ελληνες αγνοούν στοιχειώδεις κανόνες ασφαλείας στο Internet. *Το Βήμα.* Διαθέσιμο στο link: http://www.tovima.gr/2015/04/28/society/oi-ellines-agnooyn-stoixeiwdeis-kanones-asfaleias-sto-internet/. Προσπελάστηκε στις: 19/6/2018.

Σκάρτσου, Α. (2018). *Το θεσμικό πλαίσιο του διαδικτύου στην Ελλάδα.* Πτυχιακή Εργασία, Πύργος: ΤΕΙ Δυτικής Ελλάδας

Τσακανίκας, Α. (2013). *Το Διαδίκτυο στην Ελλάδα: Εμπόδια και Προοπτικές. Ίδρυμα Οικονομικών και Βιομηχανικών Ερευνών (ΙΟΒΕ) – Google*. Διαθέσιμο στο link: https://www.e-kyklades.gr/images/TODIADIKTYOSTINELLADA_F2791.pdf. Προσπελάστηκε στις: 13/6/2018.

Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης (ΥΨΗΠΤΕ). (2018). Εθνική Στρατηγική Κυβερνοασφάλειας. Διαθέσιμο στο link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGR.pdf. Προσπελάστηκε στις: 18/8/2018.