ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ

εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΕΣΠΑ 2014-2020
Επιχειρησιακό Πρόγραμμα
ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Οι ψηφιακές τεχνολογίες έχουν αποκτήσει κυρίαρχο ρόλο στη ζωή μας, έχοντας διεισδύσει σε όλους τους τομείς δραστηριότητας μιας σύγχρονης κοινωνίας. Κάθε πολίτης χρησιμοποιεί καθημερινά διάφορες ψηφιακές συσκευές (κινητό τηλέφωνο, ηλεκτρονικός υπολογιστής, tablet) στην εργασία, στο σπίτι, στο χώρο εκπαίδευσης και διαχειρίζεται μεγάλο όγκο δεδομένων τα οποία βρίσκονται σε διαφορετικές βάσεις δεδομένων και χώρους αποθήκευσης (σκληρός δίσκος, CD/DVD, usb stick, storage, υποδομή υπολογιστικού νέφους).

Το ζητούμενο είναι καθένας από εμάς να μπορεί ανά πάσα στιγμή να έχει άμεση πρόσβαση στα δεδομένα του από οποιαδήποτε ψηφιακή συσκευή χρησιμοποιεί τη δεδομένη χρονική στιγμή. Η συγκεκριμένη ανάγκη δημιουργεί μια σειρά από απαιτήσεις ασφάλειας (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) για τα εμπλεκόμενα ψηφιακά συστήματα και τις παρεχόμενες ηλεκτρονικές υπηρεσίες.

Στόχος του κειμένου είναι να εισάγει τους σπουδαστές στην κυβερνοασφάλεια, διευκολύνοντάς τους να αποκτήσουν τις απαραίτητες γνώσεις, δεξιότητες και στάσεις που θα τους επιτρέψουν να ανταποκριθούν με επιτυχία στις υψηλές απαιτήσεις των φορέων της Δημόσιας Διοίκησης που θα κληθούν να στελεχώσουν, οι οποίοι βρίσκονται σε μια συνεχή διεργασία ψηφιακού μετασχηματισμού.

Το στοίχημα είναι να εδραιωθεί από όλους τους πολίτες μία γενικότερη κουλτούρα ασφάλειας, διότι για να μπορέσουμε να αντιμετωπίσουμε αποτελεσματικά και αποδοτικά τις ολοένα και περισσότερο προηγμένες κυβερνοεπιθέσεις στις ψηφιακές υποδομές σε εθνικό και ευρωπαϊκό επίπεδο θα πρέπει να κατανοήσουμε ότι η ασφάλεια είναι ένα θέμα που μας αφορά όλους.

1. ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

1.1. Αρχές και Απαιτήσεις Ασφάλειας

Ο όρος **κυβερνοασφάλεια**, περιλαμβάνει τις δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων.

Η **αρχή της αναλογικότητας (proportionality principle)**, καθοδηγεί την ορθολογική λήψη αποφάσεων στην ασφάλεια και σύμφωνα με την οποία τα μέτρα προστασίας πρέπει να είναι αντίστοιχα των κινδύνων που απειλούν ένα ψηφιακό σύστημα, της πιθανότητας υλοποίησης των απειλών και της σοβαρότητας των αντίστοιχων συνεπειών. Η αρχή της αναλογικότητας σημαίνει ότι οι πόροι και τα μέτρα ασφάλειας που θα πρέπει να εφαρμόσουμε για την προστασία των ψηφιακών μας αγαθών, θα πρέπει να είναι ανάλογα της αξίας τους. Για παράδειγμα, ο προσωπικός μας λογαριασμός ηλεκτρονικού ταχυδρομείου συνήθως προστατεύεται από έναν κωδικό (password), ενώ για να μπορέσουμε να μεταφέρουμε χρήματα μέσω ηλεκτρονικής τραπεζικής εκτός από τον κωδικό θα χρειαστεί να χρησιμοποιήσουμε και έναν επιπλέον κωδικό μιας χρήσης (one time password).

Η **επίτευξη απόλυτης ασφάλειας δεν είναι εφικτός στόχος**, σε πραγματικές συνθήκες. Μία από τις λανθασμένες αντιλήψεις που επικρατεί, μεταξύ των χρηστών ενός πληροφοριακού συστήματος ή εφαρμογής λογισμικού, είναι ότι μπορεί να υπάρξει απόλυτη ασφάλεια. Ευτυχώς για όλους μας η «απόλυτη ασφάλεια» δεν μπορεί να επιτευχθεί και πάντα προσπαθούμε να προσδιορίσουμε ποιο είναι το επίπεδο ή το ποσοστό ασφάλειας (ή αντίστοιχα το ποσοστό επικινδυνότητας) που είμαστε διατεθειμένοι να αποδεχθούμε, εφαρμόζοντας την αρχή της αναλογικότητας. Φανταστείτε έναν κακόβουλο χρήστη, ο οποίος θα μπορούσε να εξαπολύει διαδικτυακές επιθέσεις μένοντας πάντα στο απυρόβλητο, χωρίς δηλαδή να μπορεί να εντοπιστεί και να συλληφθεί. Στόχος μας είναι να θωρακίσουμε τα ψηφιακά μας συστήματα από απειλές και κινδύνους εφαρμόζοντας την αρχή της αναλογικότητας.

Η **αρχή του ελάχιστου προνομίου** δηλώνει ότι κάθε χρήστης πρέπει να έχει τα ελάχιστα δικαιώματα πρόσβασης στα δεδομένα και στους πόρους πληροφορικής που απαιτούνται για την εκπλήρωση των καθηκόντων του, δηλαδή τις ενέργειες για τις οποίες είναι εξουσιοδοτημένος. Ο λόγος επιβολής της αρχής αυτής είναι ότι προστατεύει από εσωτερικές αλλά και εξωτερικές επιθέσεις μη εξουσιοδοτημένης πρόσβασης. Η τακτική που εφαρμόζει συνήθως ένα επιτιθέμενος είναι να αποκτήσει πρόσβαση σε ένα πληροφοριακό σύστημα ή δίκτυο και στη συνέχεια να αναβαθμίσει τα δικαιώματα πρόσβασης που έχει από απλό χρήση σε διαχειριστή, αποκτώντας τον έλεγχο του ψηφιακού συστήματος.

Ιδιαίτερα δύσκολο είναι να θωρακίσουμε ένα ψηφιακό σύστημα το οποίο δεν έχει σχεδιαστεί με γνώμονα την ασφάλεια. Η **αρχή της ασφάλειας από τον σχεδιασμό (security by design)** σημαίνει ότι ένα ψηφιακό σύστημα θα πρέπει να υλοποιείται έχοντας ενσωματώσει στις προδιαγραφές σχεδίασης όλες τις απαιτήσεις ασφάλειας που είναι αναγκαίες για την εύρυθμη λειτουργία του.

Επίσης, η λειτουργία ενός ψηφιακού συστήματος θα πρέπει να χαρακτηρίζεται από την **αρχή της ασφάλειας εξ ορισμού (security by default)**, που σημαίνει ότι όλες οι ρυθμίσεις προστασίας θα πρέπει να είναι εξ ορισμού ενεργοποιημένες και μόνο εφόσον απαιτείται θα πρέπει να απενεργοποιούνται. Για παράδειγμα, σε ένα δικτυακό τείχος προστασίας (firewall) οι θύρες θα πρέπει εξ ορισμού να είναι κλειστές και να ανοίξουν μόνο εκείνες που είναι απαραίτητες για την επικοινωνία με το εξωτερικό δίκτυο.

Δεδομένου ότι το επίπεδο της ασφάλειας ενός ψηφιακού συστήματος εξαρτάται από την ασφάλεια του ασθενέστερου σημείου (**κανόνας του ασθενέστερου κρίκου**), για την αποτελεσματική θωράκιση ενός ψηφιακού συστήματος απαιτείται μία ολιστική προσέγγιση και η χάραξη μιας ενιαίας πολιτικής ασφάλειας σε επίπεδο οργανισμού.

Εξαιρετικά σημαντικό είναι να προσπαθούμε στα ψηφιακά συστήματα να **μειώνουμε την επιφάνεια της επίθεσης**, η οποία αποτελείται από το εύρος των λειτουργικών πόρων που είναι προσπελάσιμοι από έναν επιτιθέμενο. Για παράδειγμα, όσες περισσότερες εφαρμογές λειτουργούν σε ένα πληροφοριακό σύστημα τόσο μεγαλύτερη είναι η επιφάνεια της επίθεσης.

Μία καλή πρακτική που απορρέει από τα παραπάνω, είναι ότι όλες οι εφαρμογές λογισμικού που είναι εγκατεστημένες στις ψηφιακές συσκευές μας να είναι νόμιμες και αναβαθμισμένες με όλες τις κρίσιμες ενημερώσεις ασφάλειας.

Στην κρυπτογραφία εφαρμόζεται η **αρχή του Kerckhoffs**, σύμφωνα με την οποία η ασφάλεια ενός κρυπτοσυστήματος δεν εξαρτάται από τη μυστικότητα του αλγορίθμου κρυπτογράφησης αλλά μόνο από τη διατήρηση της μυστικότητας του κλειδιού κρυπτογράφησης.

Ως βασικές απαιτήσεις ασφάλειας θεωρούνται η **εμπιστευτικότητα**, η **ακεραιότητα** και η **διαθεσιμότητα**. Υπάρχει μία ευρύτερη συζήτηση για το αν η διαθεσιμότητα αποτελεί απαίτηση ασφάλειας ή εάν πρόκειται περισσότερο για λειτουργική απαίτηση ωστόσο, η διακοπή λειτουργίας ενός συστήματος ή/και η διακοπή παροχής μίας ηλεκτρονικής υπηρεσίας αποτελούν αντικειμενικά ένα περιστατικό ασφάλειας. Πρόσθετες απαιτήσεις ασφάλειας θεωρούνται η **αυθεντικοποίηση**, η **εξουσιοδότηση** και η **μη αποποίηση ευθύνης**. Επίσης, εξαιτίας της σπουδαιότητας που έχει αποκτήσει η κυβερνοασφάλεια τα τελευταία χρόνια σε ευρωπαϊκό αλλά και διεθνές επίπεδο, η **ανθεκτικότητα** έχει έρθει να διεκδικήσει τη θέση της ισότιμα με τις υπόλοιπες απαιτήσεις ασφάλειας, όπως φαίνεται στο Σχήμα 1.1.

Σχημα 1.1 Απαιτήσεις ασφάλειας

Στη συνέχεια δίνονται οι ορισμοί των παραπάνω απαιτήσεων ασφάλειας.

- **Εμπιστευτικότητα (Confidentiality)**. Η διασφάλιση ότι μία πληροφορία ή ένας υπολογιστικός πόρος δεν γίνονται διαθέσιμα και δεν αποκαλύπτονται χωρίς την έγκριση του ιδιοκτήτη τους.

- **Ακεραιότητα (Integrity)**. Η διασφάλιση της ακρίβειας και της πληρότητας των πληροφοριών, καθώς και η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.

- **Διαθεσιμότητα (Availability)**. Η διασφάλιση ότι μία πληροφορία ή ένας υπολογιστικός πόρος βρίσκεται πάντοτε στη διάθεση ενός εξουσιοδοτημένου ατόμου όταν τη ζητήσει.

- **Αυθεντικοποίηση (authentication)**. Είναι η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης. Οι χρήστες μπορεί να είναι φυσικά πρόσωπα, υπηρεσίες, διαδικασίες ή υπολογιστές.

- **Εξουσιοδότηση (Authorization)**. Είναι η διαδικασία που διέπει τα μέσα και τις λειτουργίες ελέγχου πρόσβασης σε πόρους από αυθεντικοποιημένους χρήστες. Οι πόροι περιλαμβάνουν αρχεία, βάσεις δεδομένων, πίνακες κ.ά., σε συνδυασμό με πόρους σε επίπεδο συστήματος, όπως κλειδιά μητρώου (registry keys) και δεδομένα ρυθμίσεων (configuration data).

- **Μη-άρνηση της ευθύνης (Non-Repudiation)**. Είναι η αδυναμία αποποίησης (άρνησης) της ευθύνης για την εκτέλεση μίας πράξης (ενέργειας), όπως για παράδειγμα την εκτέλεση μίας ηλεκτρονικής συναλλαγής.

- **Ανθεκτικότητα (Resilience)**. Αναφέρεται στην ικανότητα ενός συστήματος να παράγει συνεχώς το επιδιωκόμενο αποτέλεσμα παρά τα όποια αντίξοα περιστατικά.

Με τον όρο **συνθηματικά (credentials)** προσδιορίζουμε το *όνομα χρήστη (user name)* και τον *κωδικό πρόσβασης (password)* που δίνουμε για να αποκτήσουμε δικαίωμα πρόσβασης (εξουσιοδότηση) σε ένα ψηφιακό σύστημα.

Συχνά δημιουργείται σύγχυση μεταξύ των όρων *ταυτοποίηση* και *αυθεντικοποίηση* στο πλαίσιο λειτουργίας ενός ψηφιακού συστήματος. **Ταυτοποίηση** σημαίνει η διαδικασία αναζήτησης της ύπαρξης του συγκεκριμένου χρήστη στη βάση του συστήματος. Ουσιαστικά, δηλώνεται στο σύστημα το *όνομα χρήστη (user name)*.

Αυθεντικοποίηση είναι η διαδικασία ελέγχου της ταυτότητας του χρήστη. Ζητείται δηλαδή από το χρήστη να αποδείξει ότι είναι ο πραγματικός κάτοχος της ταυτότητας. Για παράδειγμα, εισάγοντας τον κωδικό (*password*) αποδεικνύουμε στο σύστημα ότι είμαστε ο νόμιμος χρήστης με το συγκεκριμένο όνομα *(user name)*.

Εξουσιοδότηση είναι η απονομή στο χρήστη συγκεκριμένων δικαιωμάτων πρόσβασης στο σύστημα. Αφού το σύστημα ελέγξει τα συνθηματικά μας επιτρέπει (εξουσιοδότηση) την πρόσβαση σε συγκεκριμένους πόρους, σύμφωνα με τα δικαιώματα που έχουν δοθεί στον χρήστη. Κατά συνέπεια, η διαδικασία με την οποία αποκτούμε πρόσβαση σε ένα ψηφιακό σύστημα είναι πρώτα η ταυτοποίηση, ακολουθεί η αυθεντικοποίηση και τέλος η εξουσιοδότηση.

<u>Παράδειγμα 1</u>

Ας δούμε για παράδειγμα την ολοκλήρωση μιας τραπεζικής συναλλαγής με τη χρήση μιας εφαρμογής ηλεκτρονικής τραπεζικής. Ας υποθέσουμε ότι θέλουμε να μεταφέρουμε από το λογαριασμό μας 10€ σε λογαριασμό διαφορετικού προσώπου της ίδιας τράπεζας. Αρχικά, θα ανοίξουμε έναν φυλλομετρητή (browser) και θα πλοηγηθούμε στον επίσημο ιστότοπο της τράπεζάς μας. Για να μπορέσουμε να συνδεθούμε στον ηλεκτρονικό μας λογαριασμό θα πρέπει να εισάγουμε τα συνθηματικά μας (όνομα χρήστη και κωδικό πρόσβασης). Θα παρατηρήσετε ότι η διεύθυνση URL της συγκεκριμένης ιστοσελίδας εισαγωγής username και password ξεκινά από (https://) που σημαίνει ότι η μετάδοση των δεδομένων από την ψηφιακή μας συσκευή στον εξυπηρετητή της τράπεζας είναι κρυπτογραφημένη για να μην μπορεί κάποιος κακόβουλος, που ενδεχομένως παρακολουθεί την κίνηση στο δίκτυο να υποκλέψει τα συνθηματικά μας (**εμπιστευτικότητα**).

Εισάγουμε το όνομα χρήστη (**ταυτοποίηση**) και τον κωδικό πρόσβασης (**αυθεντικοποίηση**) και αποκτούμε πρόσβαση στα στοιχεία του τραπεζικού μας λογαριασμού (**εξουσιοδότηση**). Επιλέγουμε να μεταφέρουμε το ποσό των 10€ από τον λογαριασμό μας σε αυτόν του παραλήπτη, επιβεβαιώνοντας τα στοιχεία της συναλλαγής. Για την εκτέλεση της χρηματικής μεταφοράς μας ζητείται να εισάγουμε στο σύστημα έναν επιπλέον κωδικό μιας χρήσης (one time password – otp), τον οποίο λαμβάνουμε στο κινητό μας μέσω sms από την τράπεζα. Πρόκειται για μία αυθεντικοποίηση δύο επιπέδων (two factor authentication), χρησιμοποιώντας κάτι που ξέρω (password) και κάτι που έχω (otp μέσω sms που λαμβάνω στο κινητό μου).

Εφόσον η παραπάνω διαδικασία ολοκληρωθεί με επιτυχία, η συναλλαγή εκτελείται με τη μεταφορά ακριβώς του ποσού που ζητήθηκε από το χρήστη (**ακεραιότητα**). Σε περίπτωση που αμφισβητήσουμε τη εν λόγω συναλλαγή, ισχυριζόμενοι ότι ποτέ δεν δώσαμε συγκατάθεσή για τη μεταφορά χρημάτων από το λογαριασμό μας, η τράπεζα θα παρουσιάσει το αρχείο καταγραφής του συστήματος (log file), αποδεικνύοντας την ολοκλήρωση της συναλλαγής, από τον συγκεκριμένο χρήστη, τη δεδομένη χρονική στιγμή, με τη χρήση των κωδικών μας, καταρρίπτοντας έτσι τον ισχυρισμό μας (**μη αποποίηση ευθύνης**).

Επιπλέον, κατά τη διάρκεια της συναλλαγής μας θα θέλαμε η υπηρεσία ηλεκτρονικής τραπεζικής να βρίσκεται συνεχώς σε λειτουργία (**διαθεσιμότητα**) και το ψηφιακό σύστημα της τράπεζάς μας να παραμένει αξιόπιστο και λειτουργικό σε ενδεχόμενες κυβερνοεπιθέσεις (**ανθεκτικότητα**).

Παράδειγμα 2

Ας εξετάσουμε τις απαιτήσεις ασφάλειας μίας υποθετικής ηλεκτρονικής υπηρεσίας, η οποία θα παρέχεται από την Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης για την υποστήριξη της διαδικασίας υποβολής των εργασιών των σπουδαστών, προς αξιολόγηση από τους εκπαιδευτές, στο πλαίσιο των μαθημάτων.

Το ζητούμενο είναι να μπορεί ένας εκπαιδευτής να κοινοποιεί στους σπουδαστές το κείμενο της εργασίας εξασφαλίζοντας την εγκυρότητα του ηλεκτρονικού εγγράφου. Επίσης, ο εκπαιδευτής μετά από τη διόρθωση των εργασιών, θα πρέπει να έχει τη δυνατότητα να αποστείλει στους σπουδαστές εξατομικευμένες παρατηρήσεις και σχόλια, καθώς και την τελική βαθμολογία της εργασίας, εξασφαλίζοντας το απόρρητο της επικοινωνίας. Συνεπώς, οι απαιτήσεις ασφάλειας της υπηρεσίας είναι η **αυθεντικοποίηση** του συντάκτη, η **ακεραιότητα** του κειμένου και η **εμπιστευτικότητα** της επικοινωνίας.

Στην περίπτωση αποστολής της εργασίας με ηλεκτρονικό ταχυδρομείο, η επιπρόσθετη ψηφιακή υπογραφή του μηνύματος αυθεντικοποιηθεί τον αποστολέα και εξασφαλίζει την ακεραιότητα του περιεχομένου. Επιπλέον, το μήνυμα μπορεί να κρυπτογραφηθεί με το δημόσιο κλειδί του παραλήπτη. Οι σπουδαστές με τη σειρά τους, θα πρέπει να παραδώσουν την εργασία τους στον εκπαιδευτή εντός

καθορισμένης προθεσμίας, αποδεικνύοντας την εγκυρότητα του ηλεκτρονικού εγγράφου, τον χρόνο και την ημερομηνία υπογραφής και επιπλέον εξασφαλίζοντας το απόρρητο της επικοινωνίας. Κατά συνέπεια, οι απαιτήσεις ασφάλειας της υπηρεσίας είναι η **αυθεντικοποίηση** του συντάκτη, η **ακεραιότητα** του κειμένου και η **μη αποποίηση της ευθύνης** αναφορικά με το χρόνο ολοκλήρωσης της εργασίας. Επιπλέον, υπάρχει η απαίτηση της **εμπιστευτικότητας** του περιεχομένου της επικοινωνίας.

Ο εκπαιδευτής συντάσσει το θέμα της εργασίας σε ηλεκτρονικό έγγραφο, το υπογράφει ψηφιακά και στη συνέχεια το αναρτά σε προσυμφωνημένη ιστοσελίδα ή το αποστέλλει στους φοιτητές του επισυναπτόμενο σε μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο υπογράφει επίσης ψηφιακά. Οι σπουδαστές επαληθεύουν το γνήσιο της ψηφιακής υπογραφής του εκπαιδευτή και επιβεβαιώνουν την αυθεντικότητα και την ακεραιότητα του εγγράφου της εργασίας.

Οι σπουδαστές, ολοκληρώνοντας την εργασίας τους την υπογράφουν ψηφιακά με χρονοσήμανση, πετυχαίνοντας την αυθεντικοποίηση, την ακεραιότητα και την μη αποποίηση της ευθύνης για το χρόνο ολοκλήρωσης του εγγράφου. Στη συνέχεια την επισυνάπτουν σε μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο υπογράφουν ψηφιακά με το ιδιωτικό τους κλειδί και κρυπτογραφούν με το δημόσιο κλειδί του εκπαιδευτή τους.

Ο εκπαιδευτής, μοναδικός κάτοχος του ιδιωτικού κλειδιού, είναι ο μόνος που μπορεί να αποκρυπτογραφήσει τα μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνει από τους σπουδαστές του. Στη συνέχεια, επαληθεύει το γνήσιο της ψηφιακής υπογραφής κάθε σπουδαστή, επιβεβαιώνοντας την αυθεντικότητα και την ακεραιότητα των εργασιών. Τέλος, ελέγχει την ώρα και την ημερομηνία δημιουργίας της υπογραφής από τη σχετική χρονοσήμανση και αποδέχεται ή απορρίπτει την εργασία ως εκπρόθεσμη.

Ο εκπαιδευτής, διορθώνει και βαθμολογεί τις εργασίες συντάσσοντας ένα κείμενο αξιολόγησης για κάθε ένα φοιτητή, το οποίο περιέχει παρατηρήσεις, σχόλια, καθώς και την τελική αξιολόγηση. Υπογράφει ψηφιακά το κάθε έγγραφο ξεχωριστά και το επισυνάπτει σε μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο υπογράφει επίσης ψηφιακά και το κρυπτογραφεί με το δημόσιο κλειδί του αντίστοιχου σπουδαστή στον οποίο απευθύνεται. Ο φοιτητής αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί και επαληθεύει το γνήσιο της υπογραφής του καθηγητή, επιβεβαιώνοντας την αυθεντικότητα και την ακεραιότητα του εγγράφου αξιολόγησης της εργασίας.

1.2. Είδη Επιθέσεων

Οι επιθέσεις μπορούν να ταξινομηθούν σε **παθητικές** και **ενεργητικές** επιθέσεις. Η **παθητική επίθεση** στοχεύει στη συλλογή και χρήση πληροφοριών του συστήματος χωρίς να γίνει αντιληπτός και χωρίς να επηρεάσει την ομαλή λειτουργία του. Η

ενεργητική επίθεση έχει στόχο να παρέμβει και να τροποποιήσει τον τρόπο λειτουργίας του συστήματος.

Τα δύο κύρια είδη παθητικής επίθεσης είναι η **υποκλοπή** μηνύματος και η **παρακολούθηση** της κίνησης δεδομένων. **Υποκλοπή μηνύματος** έχουμε για παράδειγμα στην περίπτωση καταγραφής μιας τηλεφωνικής κλήσης, ενός μηνύματος ηλεκτρονικού ταχυδρομείου ή ενός μεταφερόμενου αρχείου. Ένα άλλο παράδειγμα είναι οι **επιθέσεις κρυπτανάλυσης** με τις οποίες γίνεται προσπάθεια να αποκρυπτογραφηθεί ένα κρυπτογραφημένο μήνυμα, χωρίς να είναι γνωστό το κλειδί αποκρυπτογράφησης. Η **ανάλυση κίνησης** εφαρμόζεται στην περίπτωση ανταλλαγής κρυπτογραφημένων δεδομένων, όπου ο επιτιθέμενος προσπαθεί να ανιχνεύσει πρότυπα στη μορφή και τη συχνότητα των μηνυμάτων, ώστε να εξάγει με έμμεσο τρόπο πληροφορίες σχετικά με τη φύση της επικοινωνίας. Οι παθητικές επιθέσεις ανιχνεύονται πολύ δύσκολα επειδή δεν προκαλούν τροποποίηση των δεδομένων. Κατά συνέπεια, αντιμετωπίζονται με αποτρεπτικά μέτρα ασφάλειας όπως για παράδειγμα η κρυπτογράφηση και η ανωνυμοποίηση των δεδομένων.

Οι ενεργητικές επιθέσεις περιλαμβάνουν τη **μεταμφίεση**, την **επανεκπομπή**, την **τροποποίηση**, την **άρνηση υπηρεσίας** και την **εξαντλητική αναζήτηση κωδικού**. Η **μεταμφίεση** μπορεί να αφορά την αλλαγή της IP διεύθυνσης (IP Spoofing) των πακέτων που στέλνει ο επιτιθέμενος ή την αλλαγή της φυσικής (MAC) διεύθυνσης (MAC Address Spoofing) της κάρτας δικτύου του επιτιθέμενου. Η πρώτη περίπτωση εφαρμόζεται κυρίως σε επιθέσεις τύπου Άρνησης Υπηρεσίας, προσφέροντας το επιπλέον πλεονέκτημα ότι αποκρύπτεται η πραγματική διεύθυνση του επιτιθέμενου. Στη δεύτερη περίπτωση ο επιτιθέμενος συνήθως ενδιαφέρεται να λάβει την απάντηση του θύματος, οπότε η τεχνική αυτή χρησιμοποιείται κυρίως για επιθέσεις τύπου Man-In-The-Middle.

Η **επανεκπομπή** (replay attack) συνίσταται αρχικά στην παθητική υποκλοπή ενός μηνύματος και μετέπειτα στην επαναμετάδοσή του ώστε να επιτύχει μία μη εξουσιοδοτημένη ενέργεια.

Η **τροποποίηση μηνυμάτων** ή **επίθεση διαμεσολαβητή** (Man in the Middle attack) εκδηλώνεται όταν ο επιτιθέμενος παρεμβάλλεται στην επικοινωνία μεταξύ δύο κόμβων, υποκλέπτοντας και αλλοιώνοντας τις πληροφορίες που ανταλλάσσονται.

Η **εξαντλητική αναζήτηση κωδικού** (Brute-force attack) εφαρμόζεται στην περίπτωση που ο επιτιθέμενος χρειάζεται να δοκιμάσει όλους τους διαφορετικούς συνδυασμούς πιθανών κωδικών μέχρι να ανακαλύψει τον σωστό. Οι επιθέσεις αυτές βασίζονται σε αυτόματο λογισμικό με χρήση εμπλουτισμένου λεξικού. Αυτός είναι ο λόγος για τον οποίο οι κωδικοί πρόσβασης που επιλέγουμε θα πρέπει να είναι δύσκολο για κάποιον να τους μαντέψει.

Η **Άρνηση Υπηρεσίας** (DoS) και η **Κατανεμημένη Άρνηση Υπηρεσίας** (DDoS) αποσκοπούν στο να θέσουν εκτός λειτουργίας το σύστημα στόχο της επίθεσης, ώστε να μην είναι σε θέση να παρέχει υπηρεσίες στους εξουσιοδοτημένους χρήστες του, αποστέλλοντας έναν μεγάλο αριθμό αιτημάτων εξυπηρέτησης προκαλώντας την

υπερφόρτωση και την κατάρρευσή του. Αν η επίθεση πραγματοποιείται συντονισμένα από πολλές διαφορετικές τοποθεσίες ταυτόχρονα, τότε πρόκειται για μια Κατανεμημένη Άρνηση Εξυπηρέτησης (Distributed Denial of Service).

Υπάρχουν όμως και οι επιθέσεις **Κοινωνικής Μηχανικής** (Social Engineering) που στοχεύουν στον ανθρώπινο παράγοντα, δηλαδή στους ίδιους τους χρήστες των ψηφιακών συστημάτων. Ο επιτιθέμενος προσπαθεί να εκμεταλλευτεί τις αδυναμίες του ανθρώπινου χαρακτήρα χρησιμοποιώντας μεθόδους εκβιασμού, χειραγώγησης ή παραπλάνησης για την επίτευξη του στόχου. Για παράδειγμα, θα μπορούσε κάποιος να καλέσει το υποψήφιο θύμα παριστάνοντας τον διαχειριστή του συστήματος και να του αποσπάσει τους κωδικούς πρόσβασης του συστήματος.

Οι επιθέσεις **Ηλεκτρονικής Εξαπάτησης** (Phishing) βασίζονται στην αποστολή ενός παραπλανητικού μηνύματος ηλεκτρονικού ταχυδρομείου ή μιας παραπλανητικής διαδικτυακής τοποθεσίας με στόχο να ωθήσει τους παραλήπτες θύματα να αποκαλύψουν προσωπικά δεδομένα ή οικονομικά στοιχεία. Οι πληροφορίες αυτές χρησιμοποιούνται συνήθως για υποκλοπή ταυτότητας. Άλλη κλασσική περίπτωση αποτελεί η τοποθέτηση ενός μολυσμένου CD ή USB σε κάποιο πολυσύχναστο σημείο του οργανισμού που αποτελεί στόχο. Η περιέργεια όποιου εργαζομένου τύχει να το βρει θα τον ωθήσει να το συνδέσει στον υπολογιστή του για να δει το περιεχόμενό του. Το αποτέλεσμα είναι να μολυνθεί με ιομορφικό λογισμικό προσφέροντας στον κακόβουλο πρόσβαση στα ψηφιακά συστήματα του οργανισμού.

1.3. Ιομορφικό Λογισμικό

Ιομορφικό ή κακόβουλο είναι το λογισμικό που περιέχει κώδικα εντολών και στοχεύει στην παραβίαση της ασφάλειας (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) ενός ψηφιακού συστήματος.

Στη συνέχεια παρουσιάζονται οι κυριότεροι τύποι ιομορφικού λογισμικού.

- **Virus (Ιός)**. Εκτελέσιμο λογισμικό που ενσωματώνει τον κώδικά του σε ένα πρόγραμμα και αναπαράγεται με την αντιγραφή του εαυτού του σε άλλα προγράμματα.

- **Trojan Horse (Δούρειος Ίππος)**. Πρόγραμμα το οποίο περιέχει πρόσθετη μη αναμενόμενη λειτουργικότητα άγνωστη στον χρήστη του ψηφιακού συστήματος. Σε αντίθεση με τον ιό δεν αναπαράγεται μόνο του.

- **Worm (Αναπαραγωγός).** Αυτόνομο πρόγραμμα που διαδίδει τον εαυτό του σε άλλους υπολογιστές μέσω δικτύου δημιουργώντας αντίγραφα.

- **Backdoors (Κερκόπορτες).** Μετατροπή ενός προγράμματος με τη δημιουργία σημείων εισόδου ώστε να επιτυγχάνεται μη εξουσιοδοτημένη πρόσβαση σε ένα ψηφιακό σύστημα.

- **Logic Bomb (Λογική Βόμβα).** Πρόγραμμα το οποίο ενεργοποιείται υπό συγκεκριμένες συνθήκες (π.χ. ορισμένη λογική συνθήκη, ημερομηνία, ώρα) παραβιάζοντας την ασφάλεια του ψηφιακού συστήματος.

- **Bacteria (Βακτήρια).** Προγράμματα τα οποία αναπαράγονται αυτόνομα, χωρίς να προκαλούν επιβλαβείς ενέργειες, με σκοπό την κατανάλωση πόρων του ψηφιακού συστήματος (επεξεργαστική ισχύ, μνήμη, χώρο στο σκληρό δίσκο). Κατά συνέπεια, μειώνεται η διαθεσιμότητα του συστήματος οδηγώντας το σε κατάρρευση.

1.4. Μελέτη Περίπτωσης

Απαντήστε το ερωτηματολόγιο της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (http://www.adae.gr/quiz/) και στη συνέχεια, απαντήστε το ερωτηματολόγιο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/SELF_ASSESSMENT_TEST/INDEX.HTML) για να αυτο-αξιολογήσετε το επίπεδο γνώσεων που έχετε στην ασφάλεια.

1.5. Βιβλιογραφία

- Network Security Essentials: Applications and Standards (6th Edition), by William Stallings, Pearson Education Limited, 2017.

- Ασφάλεια Πληροφοριακών Συστημάτων, επιστημονική επιμέλεια, Σωκράτης Κάτσικας, Δημήτρης Γκρίτζαλης, Στέφανος Γκρίτζαλης, Εκδόσεις Νέων Τεχνολογιών, 2004.

- Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, επιστημονική επιμέλεια Κωνσταντίνος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας. Εκδόσεις Παπασωτηρίου 2010.

- Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών: http://www.adae.gr/

- Ερωτηματολόγιο της ΑΔΑΕ: http://www.adae.gr/quiz/

- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: http://www.dpa.gr/

- Ερωτηματολόγιο αυτοαξιολόγησης αναφορικά με την υποκλοπή ταυτότητας: https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/SELF_ASSESSMENT_TEST/INDEX.HTML

2. ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Τα περιστατικά κυβερνοασφάλειας που έχουν καταγραφεί τα τελευταία χρόνια αποδεικνύουν ότι οι απειλές στον κυβερνοχώρο είναι εξαιρετικά σοβαρές και υπερβαίνουν τα εθνικά σύνορα, καθώς και τα όρια μεταξύ δημόσιου και ιδιωτικού τομέα. Κατά συνέπεια, η αποτελεσματική αντιμετώπιση των θεμάτων ασφάλειας σε εθνικό αλλά και σε ευρωπαϊκό επίπεδο απαιτεί τη διαμόρφωση στρατηγικών που να καθορίζουν το όραμα, τις βασικές αρχές, τους στόχους, τις προτεραιότητες, τα εμπλεκόμενα μέρη, καθώς και τη δομή διακυβέρνησης, διαμορφώνοντας ένα ολοκληρωμένο και λειτουργικό πλαίσιο για την εδραίωση ενός ανοικτού, ελεύθερου και ασφαλούς κυβερνοχώρου.

2.1. Ευρωπαϊκή Στρατηγική Κυβερνοασφάλειας

Η Ευρωπαϊκή Ένωση (ΕΕ) αναγνωρίζοντας την κρισιμότητα των κυβερνοαπειλών για την ανάπτυξη και ευημερία των κρατών μελών παρουσίασε το 2013 μια στρατηγική για την ασφάλεια στον κυβερνοχώρο καθορίζοντας τους κύριους πυλώνες για την ενίσχυση της ανθεκτικότητας αναφορικά με την ασφάλεια στον κυβερνοχώρο. Οι βασικές αρχές και στόχοι, σχετικά με την εδραίωση ενός αξιόπιστου, ασφαλούς και ανοικτού οικοσυστήματος του κυβερνοχώρου, εξακολουθούν να ισχύουν. Ωστόσο, το διαρκώς εξελισσόμενο τοπίο των εντεινόμενων απειλών καθιστά αναγκαία την ανάληψη περαιτέρω δράσης για την αντιμετώπιση και την αποτροπή επιθέσεων στο μέλλον (European Commission, 2013).

Η Ευρωπαϊκή στρατηγική για την ασφάλεια στον κυβερνοχώρο περιλαμβάνει τις ακόλουθες προτεραιότητες:

- Επίτευξη ανθεκτικότητας στον κυβερνοχώρο.
- Δραστική μείωση της εγκληματικότητας στον κυβερνοχώρο.
- Ανάπτυξη της πολιτικής κυβερνοάμυνας και των ικανοτήτων που σχετίζονται με την Κοινή Πολιτική Ασφάλειας και Άμυνας.
- Ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων για την ασφάλεια στον κυβερνοχώρο.
- Καθιέρωση μιας συνεκτικής διεθνούς πολιτικής κυβερνοχώρου για την Ευρωπαϊκή Ένωση και προώθηση των αξιών της.

2.2. Χάραξη Στρατηγικής Κυβερνοασφάλειας

Ως στρατηγική ορίζεται ένα σχέδιο ενεργειών με σκοπό την επίτευξη ενός μακροπρόθεσμου ή ευρύτερου στόχου. Στόχος μίας στρατηγικής για την ασφάλεια στον κυβερνοχώρο είναι η ενίσχυση της ανθεκτικότητας και της ασφάλειας των εθνικών πόρων ΤΠΕ που υποστηρίζουν κρίσιμες λειτουργίες του κράτους ή της κοινωνίας στο σύνολό της. Ο καθορισμός σαφών στόχων και προτεραιοτήτων είναι επομένως υψίστης σημασίας για την επίτευξη αυτού του στόχου.

Μία στρατηγική κυβερνοασφάλειας θα πρέπει να περιλαμβάνει το όραμα και το σκοπό, να καθορίζει το πεδίο εφαρμογής και να θέτει τους στόχους υψηλού επιπέδου που πρέπει να επιτευχθούν σε ένα συγκεκριμένο χρονικό πλαίσιο. Στο πεδίο εφαρμογής θα πρέπει να αναφέρονται οι επιμέρους τομείς και οι υπηρεσίες που καλύπτονται από την εν λόγω στρατηγική. Η προτεραιότητα υλοποίησης των στόχων καθορίζεται ανάλογα με την επίπτωση που έχουν στην κοινωνία, στην οικονομία και στους πολίτες (ENISA, 2016).

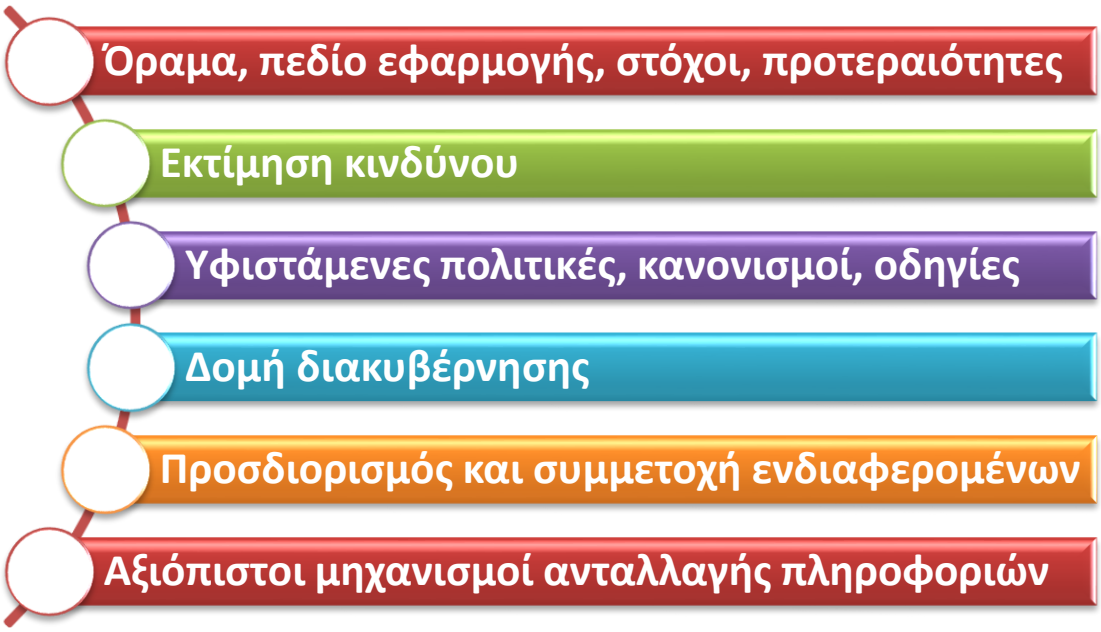
Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (European network and Information Security Agency – ENISA) υποστηρίζει ότι μία στρατηγική κυβερνοασφάλειας μεταξύ των στόχων της θα πρέπει να περιλαμβάνει τα παρακάτω (ENISA, 2016):

- Ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης στον κυβερνοχώρο
- Προστασία κρίσιμων υποδομών
- Διοργάνωση ασκήσεων κυβερνοασφάλειας
- Καθορισμός βασικών μέτρων ασφάλειας
- Καθιέρωση μηχανισμών αναφοράς περιστατικών
- Δράσεις ευαισθητοποίησης των χρηστών
- Ενίσχυση της έρευνας και ανάπτυξης
- Διοργάνωση εκπαιδευτικών και επιμορφωτικών προγραμμάτων
- Ανάπτυξη ικανότητας στην αντιμετώπιση περιστατικών
- Αντιμετώπιση του εγκλήματος στον κυβερνοχώρο
- Διεθνή συνεργασία
- Δημιουργία σύμπραξης δημόσιου-ιδιωτικού τομέα

- Αντιστάθμιση της ασφάλειας με την προστασία της ιδιωτικότητας
- Θεσμοθέτηση της συνεργασίας μεταξύ δημόσιων φορέων
- Παροχή κινήτρων στον ιδιωτικό τομέα για να επενδύσει σε μέτρα ασφάλειας

Μία στρατηγική θα πρέπει να περιλαμβάνει ή να συνοδεύεται από ένα σχέδιο δράσης για την επίτευξη των στόχων της, το οποίο θα πρέπει να περιλαμβάνει: τις επιμέρους δράσεις, που αντιστοιχούν στους στόχους της στρατηγικής και τον τρόπο με τον οποίο θα πραγματοποιηθούν, ένα πλαίσιο διακυβέρνησης για την υλοποίηση, αξιολόγηση και αναθεώρηση της στρατηγικής, καθώς και τη μεθοδολογία αξιολόγησης βάσει της οποίας θα γίνεται η παρακολούθηση της προόδου εφαρμογής της από τον αρμόδιο φορέα (ENISA, 2016).

Ο ENISA για τη σχεδίαση μίας στρατηγικής κυβερνοασφάλειας συνιστά την εφαρμογή μίας διαδικασίας έξι σταδίων (Σχήμα 2.1).



ΣΧΗΜΑ 2.1 Διαδικασία Σχεδίασης Στρατηγικής Κυβερνοασφάλειας

Για τη χάραξη μίας στρατηγικής θα πρέπει να ληφθεί υπόψη το υφιστάμενο θεσμικό πλαίσιο και οι υποχρεώσεις που απορρέουν από κανονισμούς, οδηγίες, νόμους, αρμόδιους φορείς και διεθνείς συνεργασίες (ENISA, 2012a).

Κρίσιμος παράγοντας επιτυχίας μίας στρατηγικής ασφάλειας στον κυβερνοχώρο είναι η ανάπτυξη μίας συνεκτικής δομής συντονισμού. Ένα πλαίσιο διακυβέρνησης καθορίζει τους ρόλους, τις ευθύνες και εξασφαλίζει τη λογοδοσία όλων των ενδιαφερομένων μερών. Ένας δημόσιος φορέας θα πρέπει να οριστεί ως συντονιστής της στρατηγικής με τη συνολική ευθύνη για τον κύκλο ζωής και την τεκμηρίωση της στρατηγικής. Η δομή του συντονιστικού οργάνου, οι ακριβείς αρμοδιότητές του και οι σχέσεις του με τα υπόλοιπα ενδιαφερόμενα μέρη πρέπει να καθοριστούν με λεπτομέρεια. Η επιλεγείσα δομή διακυβέρνησης θα πρέπει να καθορίζεται και να περιγράφεται με σαφήνεια στην εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο μαζί με τα αναμενόμενα οφέλη (ENISA, 2012b).

Ο ENISA με στόχο τον έλεγχο και τη συνεχή βελτίωση μίας στρατηγικής για την ασφάλεια στον κυβερνοχώρο και των συναφών πολιτικών, καθώς και την παρακολούθηση της εφαρμογής της μέσω έργων, δράσεων και διαδικασιών, προτείνει την υιοθέτηση μίας προσέγγισης (Σχήμα 2.2) που βασίζεται στον ακόλουθο κύκλο ζωής (ENISA, 2016):

Σχημα 2.2 Κύκλος Ζωής Στρατηγικής Κυβερνοασφάλειας

Οι κίνδυνοι στον κυβερνοχώρο απειλούν εξίσου κρίσιμες υποδομές του δημόσιου και του ιδιωτικού τομέα. Κατά συνέπεια, κρίνεται σκόπιμος ο εντοπισμός και η συμμετοχή των ενδιαφερομένων, καθώς και η συντονισμένη συνεργασία μεταξύ δημόσιων και ιδιωτικών φορέων. Η ανταλλαγή πληροφοριών μεταξύ ιδιωτικών και δημόσιων φορέων μπορεί να λειτουργήσει ως ένας ισχυρός μηχανισμός για την καλύτερη κατανόηση ενός συνεχώς μεταβαλλόμενου περιβάλλοντος (ENISA, 2014).

Οι ιδιοκτήτες κρίσιμων υποδομών ζωτικής σημασίας θα μπορούσαν ενδεχομένως να μοιραστούν με τις δημόσιες αρχές την ικανότητά τους στον μετριασμό των αναδυόμενων κινδύνων, απειλών και τρωτών σημείων, ενώ οι ενδιαφερόμενοι φορείς του δημόσιου τομέα θα μπορούσαν να παράσχουν πληροφορίες σχετικά με ορισμένες πτυχές που σχετίζονται με την εθνική ασφάλεια, καθώς και στοιχεία που συλλέγονται από μονάδες πληροφοριών και δίωξης του εγκλήματος στον κυβερνοχώρο. Ο συνδυασμός των δύο μερών παρέχει μια πολύ αναλυτική εικόνα για το πώς εξελίσσεται το τοπίο της απειλής (ENISA, 2016).

2.3. Εθνική Στρατηγική Κυβερνοασφάλειας

Η Ελλάδα απέκτησε επίσημα τη δική της Εθνική Στρατηγική Κυβερνοασφάλειας το 2018 με την Υπουργική Απόφαση (ΑΔΑ: Ψ4Ρ7465ΧΘ0-Ζ6Ω), όπου παρουσιάζεται ο κεντρικός σχεδιασμός της Ελληνικής Πολιτείας για τον τομέα της ασφάλειας στον κυβερνοχώρο. Η αρμόδια επιτροπή για τη χάραξη της στρατηγικής έλαβε υπόψη ότι η διάδοση του διαδικτύου και των ψηφιακών συστημάτων αυξάνεται συνεχώς καλύπτοντας κάθε πτυχή των δραστηριοτήτων του δημόσιου και του ιδιωτικού τομέα. Κατά συνέπεια, δόθηκε ιδιαίτερη προσοχή στη δημιουργία ενός ασφαλούς περιβάλλοντος διαδικτύου, υποδομών και υπηρεσιών, που θα τονώσει την εμπιστοσύνη των πολιτών και θα τους οδηγήσει στην περαιτέρω χρήση νέων ψηφιακών προϊόντων και υπηρεσιών.

Το ασφαλές περιβάλλον μαζί με την προώθηση των νέων υπηρεσιών και προϊόντων από τη μια και η διασφάλιση των προσωπικών δεδομένων και των δικαιωμάτων των πολιτών στον νέο ψηφιακό κόσμο από την άλλη, θεωρούνται βασικές προϋποθέσεις τόνωσης και προώθησης της οικονομικής ανάπτυξης στην Ελλάδα (Εθνική Στρατηγική Κυβερνοασφάλειας, 2018).

Με τη θέσπιση της Εθνικής Στρατηγικής Κυβερνοασφάλειας ορίζονται οι βασικές αρχές για τη δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος στην Ελλάδα, τίθενται οι στρατηγικοί στόχοι και το πλαίσιο δράσεων μέσω του οποίου αυτοί θα εκπληρωθούν.

Την εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας αναλαμβάνει η Εθνική Αρχή Κυβερνοασφάλειας, η οποία δημιουργείται για να καλύψει το οργανωτικό και συντονιστικό κενό ανάμεσα στους φορείς που δραστηριοποιούνται στην Ελλάδα στον τομέα της ασφάλειας στον κυβερνοχώρο, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Οι βασικές αρχές της Εθνικής Στρατηγικής Κυβερνοασφάλειας είναι:

1. Η ανάπτυξη και εδραίωση ενός ασφαλούς και ανθεκτικού κυβερνοχώρου ο οποίος θα ρυθμίζεται στη βάση εθνικών, ευρωπαϊκών και διεθνών κανόνων, προτύπων και ορθών πρακτικών και στον οποίο οι πολίτες και οι φορείς του

δημόσιου και ιδιωτικού τομέα θα δραστηριοποιούνται και θα αλληλεπιδρούν με ασφάλεια, σύμφωνα με τις αξίες που διέπουν ένα κράτος δικαίου, όπως, ενδεικτικά, της ελευθερίας, της δικαιοσύνης και της διαφάνειας

2. Η συνεχής βελτίωση των δυνατοτήτων μας στην προστασία από κυβερνοεπιθέσεις με έμφαση στις κρίσιμες υποδομές και η διασφάλιση της επιχειρησιακής συνέχειας

3. Η θεσμική θωράκιση του εθνικού πλαισίου κυβερνοασφάλειας, για την αποτελεσματική αντιμετώπιση περιστατικών κυβερνοεπιθέσεων και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο

4. Η ανάπτυξη ισχυρής κουλτούρας ασφάλειας των πολιτών, του δημόσιου και ιδιωτικού τομέα, αξιοποιώντας τις σχετικές δυνατότητες της ακαδημαϊκής κοινότητας και εν γένει των φορέων του δημόσιου και ιδιωτικού τομέα

Σκοπός της Εθνικής Στρατηγικής Κυβερνοασφάλειας είναι η αναβάθμιση του επιπέδου πρόληψης, αξιολόγησης, ανάλυσης και αποτροπής των απειλών για την ασφάλεια των συστημάτων και υποδομών ΤΠΕ και επιμέρους στόχοι είναι:

1. Ενίσχυση της ικανότητας των φορέων του δημόσιου και ιδιωτικού τομέα στην πρόληψη και την αντιμετώπιση των συμβάντων κυβερνοασφάλειας, στην βελτίωση της ανθεκτικότητας και στη δυνατότητα ανάκτησης των συστημάτων ΤΠΕ έπειτα από κυβερνοεπιθέσεις

2. Η δημιουργία ενός αποτελεσματικού πλαισίου συντονισμού και συνεργασίας με τον καθορισμό των επιμέρους αρμοδιοτήτων και ρόλων των εμπλεκόμενων φορέων του δημόσιου και ιδιωτικού τομέα για την εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας

3. Ενεργό συμμετοχή της χώρας στις διεθνείς πρωτοβουλίες και δράσεις κυβερνοασφάλειας των διεθνών οργανισμών για την ενίσχυση της εθνικής ασφάλειας

4. Ευαισθητοποίηση όλων των κοινωνικών φορέων και ενημέρωση των χρηστών για ασφαλή χρήση του κυβερνοχώρου

5. Συνεχή προσαρμογή του εθνικού θεσμικού πλαισίου στις νέες τεχνολογικές απαιτήσεις και στις Ευρωπαϊκές κατευθύνσεις για την αποτελεσματική καταπολέμηση παράνομων πράξεων που είναι συνυφασμένες με τη δράση στον κυβερνοχώρο

6. Προώθηση της καινοτομίας, της έρευνας και της ανάπτυξης σε θέματα ασφάλειας και της συνεργασίας των εμπλεκομένων φορέων

7. Αξιοποίηση βέλτιστων διεθνών πρακτικών

Η υιοθέτηση, η εφαρμογή και η εποπτεία της Εθνικής Στρατηγικής Κυβερνοασφάλειας θα συμβάλει στη δημιουργία ενός ισχυρού κράτους δικαίου, με υψηλό επίπεδο ασφάλειας και βαθμό ανθεκτικότητας στις κυβερνοαπειλές, με σεβασμό στα προσωπικά δεδομένα, στα ατομικά και κοινωνικά δικαιώματα, το οποίο θα παρέχει ποιοτικές ηλεκτρονικές υπηρεσίες σε πολίτες και επιχειρήσεις ενώ παράλληλα θα λειτουργήσει και σαν μοχλός ανάπτυξης των επιχειρήσεων και της οικονομίας, θέτοντας κοινούς κανόνες προς όλους τους εμπλεκόμενους φορείς.

Η Εθνική Στρατηγική Κυβερνοασφάλειας περιλαμβάνει τη φάση ανάπτυξης και υλοποίησης της Στρατηγικής, καθώς και τη φάση αξιολόγησης και αναθεώρησης. Οι φάσεις αυτές ορίζουν έναν συνεχή κύκλο ζωής, με την έννοια ότι η Εθνική Στρατηγική πρώτα αναπτύσσεται και υλοποιείται, στην συνέχεια αξιολογείται, βάσει προκαθορισμένων δεικτών αξιολόγησης και, εφόσον κριθεί απαραίτητο, αναθεωρείται και επικαιροποιείται.

Η Εθνική Αρχή Κυβερνοασφάλειας υπάγεται απευθείας στον Υπουργό Ψηφιακής Διακυβέρνησης και αποτελεί ένα φορέα υψηλού πολιτικού/ κυβερνητικού επιπέδου με διευρυμένες αρμοδιότητες, παρακολουθεί, υλοποιεί και φέρει τη συνολική ευθύνη της Εθνικής Στρατηγικής Κυβερνοασφάλειας. Στο πλαίσιο των αρμοδιοτήτων της παρακολουθεί, συντονίζει και αξιολογεί το έργο των εμπλεκόμενων φορέων προς επίτευξη των στρατηγικών δράσεων/ στόχων. Το πλαίσιο δράσεων της Εθνικής Στρατηγικής Κυβερνοασφάλειας περιλαμβάνει:

1. Ορισμό των Φορέων που συμμετέχουν στην Εθνική Στρατηγική Κυβερνοασφάλειας – Αποτύπωση φορέων (stake holders)

2. Ορισμό των Κρίσιμων Υποδομών

3. Αποτίμηση Επικινδυνότητας σε Εθνικό Επίπεδο

4. Καταγραφή και βελτίωση Υφιστάμενου Θεσμικού Πλαισίου

5. Εθνικό Σχέδιο Έκτακτης Ανάγκης στον Κυβερνοχώρο

6. Καθορισμό Βασικών Απαιτήσεων Ασφάλειας

7. Αντιμετώπιση Περιστατικών Ασφάλειας

8. Εθνικές Ασκήσεις Ετοιμότητας

9. Ευαισθητοποίηση χρηστών – πολιτών
10. Μηχανισμοί Αξιόπιστης Ανταλλαγής Πληροφοριών
11. Υποστήριξη Ερευνητικών και Αναπτυξιακών Προγραμμάτων και Ακαδημαϊκών Προγραμμάτων Εκπαίδευσης
12. Συνεργασίες σε Διεθνές Επίπεδο
13. Αξιολόγηση και Αναθεώρηση της Εθνικής Στρατηγικής

Συμπερασματικά, η Εθνική Στρατηγική Κυβερνοασφάλειας αναπτύσσεται στη βάση του ανωτέρου πλαισίου δράσεων και ενεργειών το οποίο δημιουργεί τις συνθήκες υλοποίησης του εθνικού στόχου για το επιθυμούμενο επίπεδο κυβερνοασφάλειας. Απαιτείται η ενδυνάμωση της συνεργασίας δημόσιου και ιδιωτικού τομέα, η οποία θεωρείται ιδιαίτερα σημαντική για την επίτευξη του όλου εγχειρήματος αλλά και ιδιαίτερα δυσχερής, δεδομένου του μικρού βαθμού ωρίμανσης και εμπειρίας. Ωστόσο, τα πλεονεκτήματα αυτής της συνεργασίας θα είναι πολλαπλασιαστικά για το κράτος και τη δημόσια διοίκηση, για τους πολίτες και το επίπεδο των παρεχόμενων υπηρεσιών ασφαλείας αλλά και για τον ιδιωτικό τομέα.

2.4. Κριτήρια Αξιολόγησης

Για την αξιολόγηση του επιπέδου ωριμότητας των κρατών μελών αναφορικά με την ασφάλεια στον κυβερνοχώρο, καθώς και τον εντοπισμό βέλτιστων πρακτικών, είναι απαραίτητο να προσδιοριστούν ορισμένα κριτήρια αξιολόγησης. Ο οργανισμός BSA | The Software Alliance προτείνει μία μεθοδολογία αξιολόγησης για την ασφάλεια στον κυβερνοχώρο που βασίζεται στη διερεύνηση 25 στοιχείων, τα οποία καλύπτουν τις παρακάτω 5 ενότητες (BSA | The Software Alliance, 2015):

- Νομικό πλαίσιο κυβερνοασφάλειας
- Επιχειρησιακές ικανότητες
- Συνεργασίες δημόσιου – ιδιωτικού τομέα
- Τομεακά σχέδια κυβερνοασφάλειας
- Εκπαίδευση

Κάθε στοιχείο του ερωτηματολογίου μπορεί να λάβει τις τιμές ακόλουθες τιμές: *"Ναι"*, *"Όχι"*, *"Μερικώς"* ή *"Δεν Εφαρμόζεται"*. Τα 25 κριτήρια αξιολόγησης παρουσιάζονται στον Πίνακα 2.1:

ΠΙΝΑΚΑΣ 2.1 Κριτήρια Αξιολόγησης Επιπέδου Ωριμότητας Κυβερνοασφάλειας

BSA | The Software Alliance, 2015		
Κριτήρια αξιολόγησης του επιπέδου ωριμότητας στην κυβερνοασφάλεια (Επιλογές απόκρισης: *Ναι, Όχι, Μερικώς ή Δεν Εφαρμόζεται*)		
1	Νομικό πλαίσιο κυβερνοασφάλειας	Υπάρχει Εθνική Στρατηγική Κυβερνοασφάλειας;
2		Ποιο έτος υιοθετήθηκε η Εθνική Στρατηγική Κυβερνοασφάλειας;
3		Υπάρχει στρατηγική ή σχέδιο προστασίας των κρίσιμων υποδομών;
4		Υπάρχει νομοθεσία/ πολιτική που να απαιτεί την ανάπτυξη Σχεδίου Ασφάλειας;
5		Υπάρχει νομοθεσία/ πολιτική που να απαιτεί την απογραφή των «συστημάτων» και την κατηγοριοποίηση των δεδομένων;
6		Υπάρχει νομοθεσία/ πολιτική που να απαιτεί την αντιστοίχιση των αντιμέτρων/ απαιτήσεων ασφάλειας με τα επίπεδα επικινδυνότητας;
7		Υπάρχει νομοθεσία/ πολιτική που να απαιτεί τη διεξαγωγή μίας ετήσιας (τουλάχιστον) επιθεώρησης κυβερνοασφάλειας;
8		Υπάρχει νομοθεσία/ πολιτική που να απαιτεί την εκπόνηση έκθεσης για την κυβέρνηση σχετικά με το επίπεδο κυβερνοασφάλειας στο δημόσιο τομέα;
9		Υπάρχει νομοθεσία/ πολιτική που να απαιτεί τον ορισμό σε κάθε φορέα Υπεύθυνου Πληροφορικής (CIO) και Υπεύθυνου Ασφάλειας (CSO);
10		Υπάρχει νομοθεσία/ πολιτική που να καθιστά υποχρεωτική την αναφορά περιστατικών κυβερνοασφάλειας;
11		Υπάρχει νομοθεσία/ πολιτική που να περιλαμβάνει έναν κατάλληλο ορισμό για την «Προστασία Κρίσιμων Υποδομών»;
12		Στο πλαίσιο των δημόσιων και ιδιωτικών συμβάσεων, οι προδιαγραφές για λύσεις κυβερνοασφάλειας βασίζονται σε διεθνή σχήματα διαπίστευσης ή πιστοποίησης, χωρίς επιπρόσθετες εθνικές προδιαγραφές;

13	Επιχειρησιακή επάρκεια	Υπάρχει Εθνική Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (CERT) ή Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας (CSIRT);
14		Ποιο είναι το έτος σύστασης της Ομάδας Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (CERT);
15		Υπάρχει Εθνική Αρχή Κυβερνοασφάλειας σύμφωνα με όσα προβλέπει η Οδηγία Network Security Information (NIS);
16		Υπάρχει πλατφόρμα αναφοράς συμβάντων για τη συλλογή στοιχείων αναφορικά με τα περιστατικά κυβερνοασφάλειας;
17		Διεξάγονται εθνικές ασκήσεις κυβερνοασφάλειας;
18		Υπάρχει εθνικό σχήμα διαχείρισης περιστατικών για την αντιμετώπιση περιστατικών κυβερνοασφάλειας;
19	Συνεργασίες δημόσιου – ιδιωτικού τομέα	Υπάρχει κάποια Σύμπραξη Δημόσιου και Ιδιωτικού Τομέα (ΣΔΙΤ) για την κυβερνοασφάλεια;
20		Οι τομείς της οικονομίας είναι οργανωμένοι (συμβούλια κυβερνοασφάλειας για τις επιχειρήσεις ή τη βιομηχανία);
21		Σχεδιάζονται ή συστήνονται νέες ή υπό σχεδιασμό Σύμπραξεις Δημόσιου και Ιδιωτικού Τομέα (εάν ναι, ποιον τομέα αφορούν);
22	Τομεακά σχέδια κυβερνοασφάλειας	Υπάρχει κάποιο κοινό σχέδιο κυβερνοασφάλειας μεταξύ δημόσιου και ιδιωτικού τομέα;
23		Έχουν οριστεί ανά τομέα συγκεκριμένες προτεραιότητες για την ασφάλεια;
24		Έχουν διεξαχθεί κάποιες τομεακές αξιολογήσεις επικινδυνότητας κυβερνοασφάλειας;
26	Εκπαίδευση	Υπάρχει εκπαιδευτική στρατηγική για τη βελτίωση της γνώσης του κοινού από μικρή ηλικία και την αύξηση της ευαισθητοποίησης για την κυβερνοασφάλεια;

2.5. Μελέτη Περίπτωσης

Μεταβείτε στο διαδραστικό χάρτη του ENISA στον ακόλουθο ηλεκτρονικό σύνδεσμο (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map) και στη συνέχεια επιλέξτε μία χώρα για να μελετήσετε και να αξιολογήσετε την αντίστοιχη εθνική στρατηγική κυβερνοασφάλειας.

2.6.Βιβλιογραφία

- BSA | The Software Alliance (2015). *EU Cybersecurity Dashboard/ A Path to a Secure European Cyberspace*. EU Cybersecurity Maturity Dashboard.
- ENISA (2016). *NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies*. European Network and Information Security Agency. DOI: 10.2824/48036.
- ENISA (2014). *An evaluation Framework for National Cyber Security Strategies*. European Network and Information Security Agency. DOI: 10.2824/3903.
- ENISA (2012a). *National Cyber Security Strategies – Practical Guide on Development and Execution*. European Network and Information Security Agency.
- ENISA (2012b). *National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace*. European Network and Information Security Agency.
- European Commission (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. JOIN(2013) 1 final, Brussels.
- Εθνική Στρατηγική Κυβερνοασφάλειας (2018). Υπουργική Απόφαση αριθμ. πρωτ. 3218/07-03-2018 (ΑΔΑ: Ψ4Ρ7465ΧΘ0-Ζ6Ω).

3. ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

3.1. Εισαγωγή

Σε μία σύγχρονη Δημόσια Διοίκηση η επιχειρησιακή λειτουργία των φορέων και η ποιότητα των παρεχόμενων ηλεκτρονικών υπηρεσιών προς τους πολίτες βασίζονται στην ασφάλεια των πληροφοριακών πόρων που τις υποστηρίζουν. Η θωράκιση των ψηφιακών συστημάτων του δημόσιου τομέα συμβάλει αποφασιστικά στην επίτευξη των στόχων των δημόσιων οργανισμών, διασφαλίζει το κύρος τους και επιτρέπει τη συμμόρφωση με τις νομικές υποχρεώσεις και τα διεθνή πρότυπα.

Η πολυπλοκότητα των ψηφιακών συστημάτων, το ιδιαίτερα δυναμικό περιβάλλον λειτουργίας των φορέων και η επικινδυνότητα των κυβερνοεπιθέσεων, επιβάλουν την υιοθέτηση μίας ολιστικής προσέγγισης μέσα από την εφαρμογή ενός ενιαίου σχεδίου ασφάλειας για την ανάπτυξη, υλοποίηση, λειτουργία, έλεγχο, διαχείριση, παρακολούθηση και βελτίωση των οργανωτικών και τεχνικών μέτρων προστασίας, διασφαλίζοντας την εδραίωση και διατήρηση του επιθυμητού επιπέδου ασφάλειας.

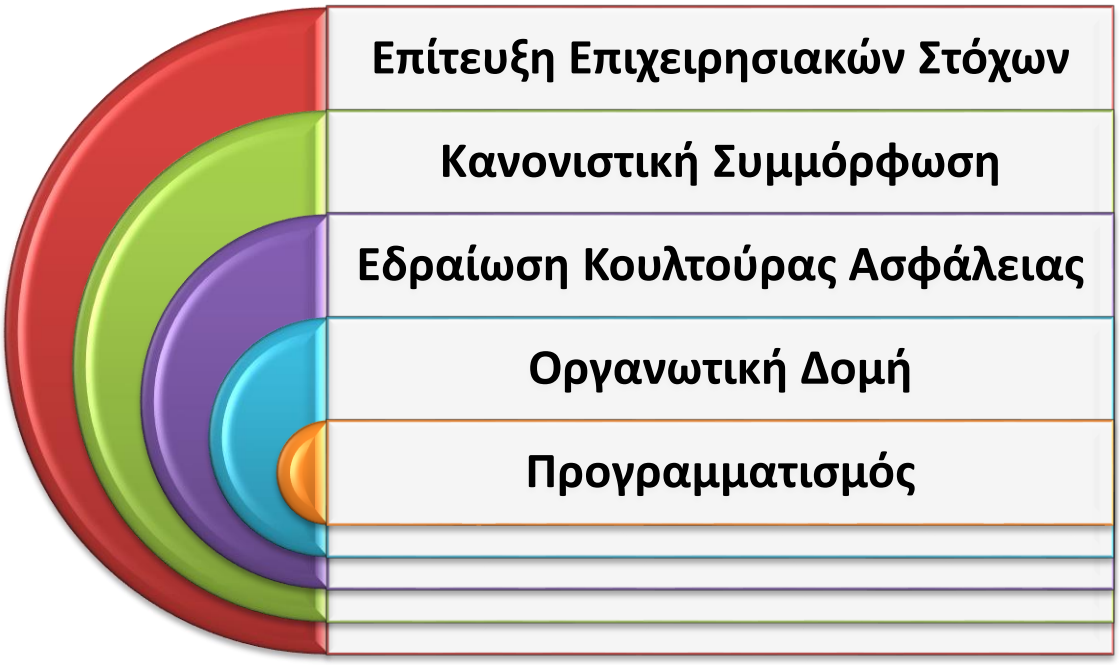
Η διαχείριση της ασφάλειας στοχεύει στην προστασία των ψηφιακών συστημάτων, περιορίζοντας την επικινδυνότητα σε αποδεκτό επίπεδο. Περιλαμβάνει την αξιολόγηση της επικινδυνότητας και προσδιορισμό του αποδεκτού επιπέδου ασφάλειας, την ανάπτυξη και εφαρμογή μιας Πολιτικής Ασφάλειας, τη δημιουργία του κατάλληλου οργανωτικού πλαισίου, την εξασφάλιση των απαιτούμενων πόρων για την εφαρμογή της Πολιτικής Ασφάλειας, καθώς και την εκπαίδευση, ενημέρωση και ευαισθητοποίηση των χρηστών των ψηφιακών συστημάτων.

Η πολιτική ασφάλειας των ψηφιακών συστημάτων αποτυπώνει τη δέσμευση της Διοίκησης του Φορέα και τις βασικές κατευθύνσεις για τον τρόπο διαχείρισης των θεμάτων ασφάλειας. Ειδικότερα, περιλαμβάνει το σκοπό, τους στόχους, τους ρόλους, τις υπευθυνότητες, τους κανόνες, τις οδηγίες και τις διαδικασίες για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών συστημάτων και δικτύων του οργανισμού. Οι οδηγίες και οι διαδικασίες υλοποιούνται με την εφαρμογή των μέτρων ασφάλειας, τα οποία έχουν προκύψει μέσα από μία αξιολόγηση επικινδυνότητας. Η πολιτική ασφάλειας αποτελεί ένα έγγραφο που φέρει την έγκριση της Διοίκησης του Φορέα, είναι δεσμευτική και κοινοποιείται στο σύνολο του προσωπικού.

Η πολιτική ασφάλειας μαζί με τα μέτρα προστασίας ή αντίμετρα ή μέτρα ασφάλειας αποτελούν το σχέδιο ασφάλειας ψηφιακών συστημάτων του οργανισμού.

3.2. Οφέλη Πολιτικής Ασφάλειας

Τα οφέλη που προκύπτουν από τη σχεδίαση και εφαρμογή μίας ολοκληρωμένης πολιτικής ασφάλειας για έναν οργανισμό του δημόσιου τομέα είναι τα παρακάτω (Σχήμα3.1):



ΣΧΗΜΑ 3.1 Οφέλη Πολιτικής Ασφάλειας

- **Επίτευξη επιχειρησιακών στόχων**. Η απρόσκοπτη λειτουργία των ψηφιακών συστημάτων που υποστηρίζουν τις επιχειρησιακές διεργασίες του φορέα, συμβάλει στην επίτευξη των στόχων, καθώς και στην εδραίωση του κύρους και της εμπιστοσύνης των πολιτών.

- **Κανονιστική Συμμόρφωση**. Η πολιτική ασφάλειας διευκολύνει έναν φορέα να συμμορφωθεί με το κανονιστικό – νομικό πλαίσιο που ρυθμίζει τη λειτουργία του. Για παράδειγμα, η θέσπιση και εφαρμογή οργανωτικών και τεχνικών μέτρων ασφάλειας είναι ιδιαίτερα σημαντική για τον Υπεύθυνο Επεξεργασίας δεδομένων, σύμφωνα με όσα προβλέπει ο Γενικός Κανονισμός Προστασίας Δεδομένων. Επίσης, ορισμένοι φορείς είναι υποχρεωμένοι να διαθέτουν πιστοποίηση ασφάλειας σύμφωνα με το πρότυπο ISO 27001.

- **Εδραίωση Κουλτούρας Ασφάλειας.** Η ασφάλεια είναι ένα ζήτημα που μας αφορά όλους. Η πολιτική ασφάλειας δίνει το μήνυμα στο προσωπικό ότι αποτελεί προτεραιότητα για τη Διοίκηση του Φορέα, καθορίζει τους στόχους ασφάλειας, συμβάλει στην επίγνωση των κινδύνων, βοηθά στην ενημέρωση των εργαζομένων για τις διαδικασίες και τα μέτρα προστασίας των ψηφιακών συστημάτων και γενικότερα διευκολύνει την εδραίωση μίας κουλτούρας ασφάλειας.

- **Οργανωτική Δομή.** Η εφαρμογή της πολιτικής ασφάλειας προϋποθέτει τον καθορισμό μίας λειτουργικής οργανωτικής δομής και διακριτών ρόλων για την έγκαιρη αντιμετώπιση και αποτελεσματική διαχείριση των περιστατικών ασφάλειας. Η σχεδίαση, η υλοποίηση, η παρακολούθηση, ο έλεγχος και η αναθεώρηση με σκοπό τη βελτίωση αποτελούν στάδια του κύκλου ζωής μίας πολιτικής ασφάλειας και αντικείμενο εργασίας έμπειρου και καταρτισμένου προσωπικού με αντίστοιχα καθήκοντα και θέσεις ευθύνης.

- **Προγραμματισμός.** Η πολιτική ασφάλειας περιλαμβάνει τους στόχους, τις προτεραιότητες και τους ρόλους για την υλοποίηση του επιθυμητού επιπέδου προστασίας των ψηφιακών συστημάτων του οργανισμού. Κατά συνέπεια, παρέχει τις βασικές κατευθύνσεις για τον προσδιορισμό των πόρων (ανθρώπινο δυναμικό, εξοπλισμός, λογισμικό, υλικοτεχνική υποδομή) που είναι αναγκαίοι για την εφαρμογή των διαδικασιών και μέτρων ασφάλειας. Ουσιαστικά, καθοδηγεί τον φορέα στην ανάπτυξη ενός σχεδίου δράσης για την υλοποίηση της σχεδίου ασφάλειας.

3.3. Ανάπτυξη Πολιτικής Ασφάλειας

Η ασφάλεια ψηφιακών συστημάτων χαρακτηρίζεται από το πλήθος και την ποικιλομορφία των παραγόντων που πρέπει να ληφθούν υπόψη. Οι παράγοντες αυτοί είναι τόσο τεχνικοί, όσο και διοικητικοί – οργανωτικοί. Για το λόγο αυτό, κάθε προσπάθεια προστασίας ενός συστήματος πρέπει να λαμβάνει υπόψη τις εξής γενικές διαπιστώσεις:

- Η ασφάλεια ψηφιακών συστημάτων εξαρτάται από πολλούς παράγοντες και δεν είναι ούτε αποκλειστικά, ούτε κυρίως τεχνικό ζήτημα.

- Η επίτευξη απόλυτης ασφάλειας δεν είναι εφικτός στόχος, σε πραγματικές συνθήκες.

- Για κάθε επίπεδο ασφάλειας υπάρχει ένα αντίστοιχο κόστος που θα πρέπει να καταβληθεί για την επίτευξή του.

- Στο πλαίσιο της αρχής της αναλογικότητας, τα μέτρα προστασίας που θα ληφθούν θα πρέπει να αντιστοιχούν στο επίπεδο και τη φύση των κινδύνων που αντιμετωπίζει το ψηφιακό σύστημα.

Η πολιτική ασφάλειας καταγράφει τις βασικές επιλογές της Διοίκησης και τη βούλησή της για τη θωράκιση των ψηφιακών συστημάτων του οργανισμού. Περιγράφει τις γενικές αρχές πάνω στις οποίες βασίζεται η προστασία των πληροφοριών και προσφέρει μία σειρά από κατευθυντήριες οδηγίες. Κύριο χαρακτηριστικό της πολιτικής ασφάλειας είναι ότι πρέπει να επικυρώνεται από τη Διοίκηση του Φορέα. Σχεδιάζοντας μία πολιτική ασφάλειας υιοθετούμε ολιστική προσέγγιση, λαμβάνουμε υπόψη τις τρέχουσες τεχνολογικές εξελίξεις και ακολουθούμε μία σειρά διαδοχικών σταδίων, με στόχο την κάλυψη όλων των διαστάσεων ασφάλειας των ψηφιακών συστημάτων ενός οργανισμού.

Οι απαιτήσεις για την ασφάλεια των ψηφιακών συστημάτων που πρέπει να ικανοποιεί η πολιτική ασφάλειας προέρχονται από όλους τους εμπλεκόμενους στη χρήση και λειτουργία των συστημάτων ενός οργανισμού και συγκεκριμένα τη Διοίκηση του οργανισμού, τους χρήστες και διαχειριστές των συστημάτων, τις νομικές και κανονιστικές διατάξεις που διέπουν τη λειτουργία του, καθώς και τους πολίτες που είναι οι αποδέκτες των ηλεκτρονικών υπηρεσιών.

Το πρόβλημα που χαρακτηρίζει αρκετούς φορείς του δημόσιου τομέα είναι ότι είτε δεν διαθέτουν πολιτική ασφάλειας, είτε διαθέτουν πολιτικές ασφάλειας για ορισμένα μόνο από τα συστήματα του οργανισμού. Αυτή η αποσπασματική προσέγγιση είναι αναποτελεσματική διότι δεν επιτρέπει την ολοκληρωμένη προστασία των συστημάτων και δημιουργεί προβλήματα και επικαλύψεις στη διαχείριση και στην εφαρμογή διαφορετικών πολιτικών, διαδικασιών και μέτρων ασφάλειας.

Η σχεδίαση της πολιτικής ασφάλειας μπορεί να γίνει εσωτερικά από στελέχη του φορέα που διαθέτουν την εξειδίκευση και την εμπειρία ή εξωτερικά με την ανάθεση του έργου σε κάποιον ειδικό.

Το αρχικό στάδιο ανάπτυξης μίας πολιτικής ασφάλειας αφορά την τεκμηρίωση των ψηφιακών συστημάτων του φορέα. Αναλυτικότερα, περιλαμβάνει τον σκοπό και τους στόχους της πολιτικής, την οριοθέτηση του πεδίου εφαρμογής, την αποτίμηση των αγαθών που χρίζουν προστασίας, καθώς και την καταγραφή των λειτουργικών στοιχείων που συνθέτουν τα ψηφιακά συστήματα του οργανισμού και του περιβάλλοντος λειτουργίας τους. Ως αγαθά ορίζονται τα δεδομένα, οι πληροφορίες και οι υπολογιστικοί πόροι που έχουν αξία (εκφραζόμενη σε χρηματικούς ή άλλους όρους) για το φορέα.

Το επόμενο στάδιο διαμόρφωσης μίας πολιτικής ασφάλειας αφορά την επιλογή της μεθόδου ανάλυσης της επικινδυνότητας (risk analysis) που θα εφαρμοστεί, καθώς και του προτύπου (standard) διαχείρισης της πολιτικής. Η ανάλυση και διαχείριση επικινδυνότητας αποσκοπεί στον εντοπισμό και την αποτίμηση των παραμέτρων που

έχουν σχέση με την ασφάλεια των ψηφιακών συστημάτων, καθώς και στην επιλογή και περιγραφή των απαραίτητων διαδικαστικών και τεχνικών μέτρων για την προστασία τους.

Η αξιολόγηση των αγαθών και κυρίως η αξιολόγηση των δεδομένων αποτελεί βασική δραστηριότητα της μεθόδου ανάλυσης της επικινδυνότητας, καθώς λαμβάνει υπόψη την εκτίμηση για τις πιθανές επιπτώσεις που ενδέχεται να προκύψουν από την απώλεια των βασικών απαιτήσεων ασφάλειας των δεδομένων, δηλαδή από το ενδεχόμενο περιορισμού της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας των δεδομένων.

Η καταγραφή και αποτίμηση τόσο των κινδύνων που υφίστανται τα ψηφιακά συστήματα και οι εγκαταστάσεις τους, όσο και των πιθανών επιπτώσεων που είναι δυνατόν να υποστεί ένας φορέας από ενδεχόμενες κακόβουλες ενέργειες, είναι απαραίτητη προϋπόθεση για την επιλογή των κατάλληλων τεχνολογιών, καθώς και των αντίστοιχων τεχνολογικών μέτρων και των οργανωτικών και διαδικαστικών πρωτοβουλιών και ενεργειών που είναι απαραίτητες για την ασφάλεια των συστημάτων και των εγκαταστάσεων του φορέα.

Η ανάλυση επικινδυνότητας παρέχει τη δυνατότητα να εντοπιστούν οι τομείς που απαιτούν τη λήψη μέτρων ασφάλειας (αντιμέτρων) και να προσδιοριστεί το επίπεδο προστασίας που απαιτείται. Το σύνολο των μέτρων ασφάλειας, σε συνδυασμό με την πολιτική ασφάλειας αποτελούν το Σχέδιο Ασφάλειας.

Η αποτελεσματικότητα του σχεδίου ασφάλειας προϋποθέτει την πιστή και συνολική εφαρμογή του. Τα αντίμετρα που προτείνονται βρίσκονται σε αλληλεξάρτηση και η αποτελεσματικότητα ενός αντιμέτρου εξαρτάται συχνά από την υλοποίηση ενός άλλου. Για παράδειγμα, κανένα τεχνικό αντίμετρο δεν πρόκειται να αποδώσει τα αναμενόμενα αποτελέσματα, χωρίς την παράλληλη εφαρμογή ενός κατάλληλου οργανωτικού σχήματος και ενός προγράμματος ευαισθητοποίησης, ενημέρωσης και εκπαίδευσης.

Οι διαδικασίες και τα μέτρα προστασίας που καθορίζει ένα σχέδιο ασφάλειας θα πρέπει να καλύπτουν τις ακόλουθες κατηγορίες απαιτήσεων ασφάλειας:

- **Κανονιστική Συμμόρφωση**. Βασικός στόχος μίας πολιτικής ασφάλειας είναι η συμμόρφωση του οργανισμού με τις νομικές υποχρεώσεις που απορρέουν από το υφιστάμενο κανονιστικό πλαίσιο λειτουργίας του.

- **Οργανωτική Δομή**. Κρίσιμος παράγοντας επιτυχίας για την εφαρμογή ενός σχεδίου ασφάλειας είναι η δημιουργία κατάλληλης οργανωτικής δομής. Η αποτελεσματικότητα της οργανωτικής δομής εξαρτάται από την επαρκή στελέχωση του φορέα και την ανάθεση διακριτών ρόλων και αρμοδιοτήτων σε συγκεκριμένα άτομα που διαθέτουν κατάλληλα τυπικά και ουσιαστικά προσόντα. Επίσης, θα πρέπει να υπάρχουν διαδικασίες για τον εντοπισμό και την αναφορά περιστατικών παραβίασης της

ασφάλειας. Για την υλοποίηση ενός σχεδίου ασφάλειας απαιτούνται δύο βασικοί ρόλοι:

- **Υπεύθυνος Ασφάλειας (Security Officer)**. Είναι αρμόδιος για την για την υλοποίηση και εφαρμογή των μέτρων ασφάλειας και θα πρέπει να διαθέτει επαρκή κατάρτιση και εμπειρία. Για τα θέματα που αφορούν την ασφάλεια αναφέρεται απευθείας στη Διοίκηση του φορέα και συντάσσει σχετικές αναφορές. Είναι υπεύθυνος για το σχεδιασμό και το συντονισμό των δραστηριοτήτων εκπαίδευσης και ενημέρωσης σε θέματα ασφάλειας. Συμμετέχει στο σχεδιασμό κάθε νέου έργου που αφορά την ανάπτυξη εφαρμογών και συστημάτων, ώστε να προσδιορίζει τις σχετικές με την ασφάλεια απαιτήσεις και διεξάγει τακτικούς και έκτακτους ελέγχους για την εφαρμογή του σχεδίου ασφάλειας.

- **Επιτροπή Εποπτείας και Ελέγχου (Steering Committee)**. Έχει ως αρμοδιότητα τη διεξαγωγή ελέγχων τόσο για την εφαρμογή της πολιτικής ασφάλειας, όσο και για την ορθή χρήση των ψηφιακών συστημάτων από το προσωπικό. Επίσης, οφείλει να αναφέρει τις αδυναμίες που εντοπίζει στη λειτουργία των συστημάτων και να προτείνει αλλαγές και βελτιώσεις σε τεχνικό και σε οργανωτικό επίπεδο. Ο Υπεύθυνος Ασφάλειας δεν μπορεί να συμμετέχει στην Επιτροπή Εποπτείας και Ελέγχου μιας και στα καθήκοντά της περιλαμβάνεται ο έλεγχος του έργου του Υπεύθυνου Ασφάλειας του φορέα.

- **Διαχείριση Προσωπικού**. Η καλλιέργεια κουλτούρας ασφάλειας στον φορέα απαιτεί την ενεργό συμμετοχή όλων των υπαλλήλων και κατά συνέπεια, κρίνεται ιδιαίτερα σημαντική η υλοποίηση εκπαιδευτικών παρεμβάσεων ενημέρωσης, ευαισθητοποίησης και απόκτησης δεξιοτήτων σε θέματα ασφάλειας ψηφιακών συστημάτων. Στόχος είναι η είναι η μείωση της επικινδυνότητας που οφείλεται σε ανθρώπινα λάθη, απάτη, κλοπή ή κατάχρηση των πόρων των συστημάτων, καθώς και η αντιμετώπιση και αναφορά περιστατικών παραβίασης της ασφάλειας.

- **Διαχείριση Πολιτικής Ασφάλειας**. Στην πολιτική ασφάλειας θα πρέπει να προσδιορίζονται και οι απαιτούμενες δραστηριότητες για την εφαρμογή της, οι οποίες αφορούν στην αξιολόγηση και αναθεώρηση της πολιτικής, καθώς και στον έλεγχο εφαρμογής της και τον καθορισμό των ενεργειών που προβλέπονται στις περιπτώσεις μη τήρησής της από τους χρήστες των ψηφιακών συστημάτων. Μία πολιτική ασφάλειας θα πρέπει να αναθεωρείται σε τακτά χρονικά διαστήματα και σίγουρα έπειτα από σοβαρά περιστατικά παραβίασης της ασφάλειας, σημαντικές αλλαγές στον εξοπλισμό ή το λογισμικό, καθώς και στην επέκταση ή διασύνδεση των συστημάτων με άλλες εφαρμογές.

- **Έλεγχος Πρόσβασης**. Η πρόσβαση όλων των χρηστών των ψηφιακών συστημάτων στις πληροφορίες, τα υπολογιστικά συστήματα και τις εφαρμογές θα πρέπει να καθορίζεται με βάση τις επιχειρησιακές ανάγκες και τις απαιτήσεις ασφάλειας. Συνήθως εφαρμόζεται αρχή του ελάχιστου προνομίου, σύμφωνα με την οποία κάθε χρήστης πρέπει να έχει τα ελάχιστα δικαιώματα πρόσβασης στις πληροφορίες και στις εφαρμογές που απαιτούνται για την εκπλήρωση των ενεργειών για τις οποίες είναι εξουσιοδοτημένος.

- **Διαχείριση Αλλαγών**. Οποιαδήποτε αλλαγή στην κατάσταση λειτουργιάς των ψηφιακών συστημάτων ενδέχεται να επιφέρει μεταβολή στο επίπεδο ασφάλειας του φορέα. Κατά συνέπεια, για τη διατήρηση του επιθυμητού επιπέδου ασφάλειας, η προμήθεια ή συντήρηση εξοπλισμού και αντίστοιχα η ανάπτυξη εφαρμογών ή οι αναβαθμίσεις λογισμικού θα πρέπει να γίνονται κατόπιν έγκρισης του Υπεύθυνου Ασφάλειας και να προγραμματίζονται αφού έχει καθοριστεί η διαδικασία επαναφοράς του συστήματος στην αρχική του κατάσταση (rollback) σε περίπτωση που παρουσιαστεί οποιαδήποτε δυσλειτουργία.

- **Φυσική Ασφάλεια**. Τα αντίμετρα που υποστηρίζουν τη φυσική ασφάλεια αποσκοπούν στην αποτροπή της μη εξουσιοδοτημένης πρόσβασης στους χώρους των ψηφιακών συστημάτων και της καταστροφής της υλικοτεχνικής υποδομής. Αφορούν στον έλεγχο φυσικής πρόσβασης σε χώρους ζωτικής σημασίας, όπως για παράδειγμα κέντρα υπολογιστικών συστημάτων και δικτύων, και στην προστασία της υγείας των χρηστών.

- **Σχέδιο Συνέχισης Λειτουργίας**. Ανάλογα με τον βαθμό κρισιμότητας των παρεχόμενων υπηρεσιών ενός φορέα και των αντίστοιχων διεργασιών που υποστηρίζει ένα ψηφιακό σύστημα, το σχέδιο ασφάλειας θα πρέπει να περιλαμβάνει οδηγίες που αφορούν τις απαιτούμενες ενέργειες μετά την πραγματοποίηση ενός σημαντικού περιστατικού παραβίασης της ασφάλειας, ώστε οι λειτουργίες του φορέα να εξακολουθήσουν να πραγματοποιούνται με κάποιους εναλλακτικούς τρόπους, έως ότου αντιμετωπιστεί το πρόβλημα ασφάλειας του συστήματος.

Η πολιτική ασφάλειας ενός φορέα απευθύνεται σε κάθε εργαζόμενο που εμπλέκεται στη χρήση ψηφιακών συστημάτων κατά την εκτέλεση της εργασίας του. Κάθε εργαζόμενος που σχετίζεται με τα ψηφιακά συστήματα πρέπει να εκπαιδευτεί στην εφαρμογή της πολιτικής ασφάλειας. Οι εργαζόμενοι που χρησιμοποιούν τα ψηφιακά συστήματα πρέπει να συμμορφώνονται με τις οδηγίες που εμπεριέχονται στην πολιτική ασφάλειας. Η υποχρέωση αυτή ενεργοποιείται από τη στιγμή που η πολιτική έχει εγκριθεί από τη Διοίκηση του φορέα. Η Διοίκηση θα πρέπει να καθορίσει το ακριβές πλαίσιο συμμόρφωσης με την πολιτική ασφάλειας.

Η πολιτική ασφάλειας ενός φορέα διατηρεί την επικαιρότητά της, υπό τη προϋπόθεση ότι δεν έχουν σημειωθεί σημαντικές αλλαγές στο περιβάλλον το οποίο καλύπτει, καθώς και στις αντιλήψεις του οργανισμού σχετικά με την ασφάλεια των ψηφιακών συστημάτων.

Η πολιτική ασφάλειας πρέπει, ανά πάσα χρονική στιγμή, να είναι μία. Άρα η διαχείριση των αλλαγών της πρέπει να τύχει ιδιαίτερης προσοχής, ώστε η έκδοση που χρησιμοποιείται να είναι η ορθή. Είναι εξάλλου σαφές ότι μελλοντικές εξελίξεις θα δημιουργήσουν την ανάγκη για επικαιροποίηση, τουλάχιστον κάποιων σημείων της πολιτικής ασφάλειας.

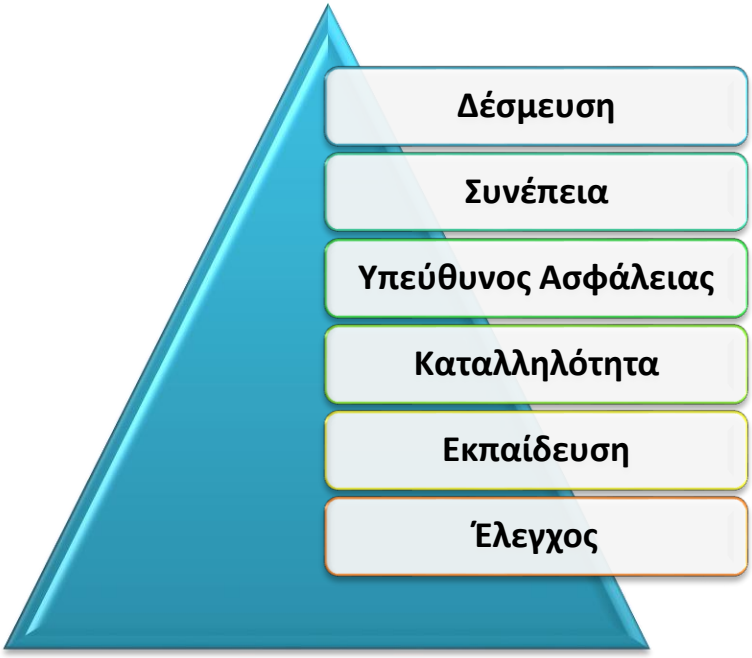
Η πολιτική ασφάλειας θα πρέπει να χαρακτηρίζεται από πληρότητα και να είναι τεχνικά επίκαιρη. Δηλαδή, οι διαδικασίες και τα αντίμετρα να καλύπτουν όλες τις λειτουργίες του ψηφιακού συστήματος, έχοντας λάβει υπόψη όλες τις τρέχουσες τεχνολογικές εξελίξεις. Επίσης, δεν θα πρέπει να ξεχνάμε ότι η πολιτική ασφάλειας απευθύνεται στο σύνολο των εργαζομένων και κατά συνέπεια, θα πρέπει να είναι σαφής και κατανοητή. Η ανάλυση των αντιμέτρων θα πρέπει να είναι τεχνολογικά ανεξάρτητη, χωρίς να περιορίζει τον φορέα σε επιλεγμένες τεχνικές λύσεις και κατασκευαστές. Οι απαιτήσεις ασφάλειας πρέπει να ανταποκρίνονται κατάλληλα στις επιχειρησιακές απαιτήσεις του φορέα και τα αντίμετρα θα πρέπει να μπορούν να είναι εφαρμόσιμα από τους χρήστες με εύχρηστες και αποδοτικές διαδικασίες.

3.4. Κρίσιμοι Παράγοντες Επιτυχίας

Η σχεδίαση, η υλοποίηση, η διαχείριση και ο έλεγχος μίας πολιτικής ασφάλειας αποτελεί γενικά ένα σύνθετο και πολυδιάστατο ζήτημα. Οι κρίσιμοι παράγοντες επιτυχίας για την εφαρμογή της πολιτικής ασφάλειας ενός φορέα του δημοσίου είναι οι παρακάτω (Σχήμα 3.2):

- **Δέσμευση**. Η εφαρμογή της πολιτικής ασφάλειας προϋποθέτει την ισχυρή δέσμευση της Διοίκησης του φορέα, ορίζοντας την κατάλληλη οργανωτική δομή και ρόλους, εξασφαλίζοντας το εξειδικευμένο ανθρώπινο δυναμικό και τους οικονομικούς πόρους που απαιτούνται για την αποτελεσματική διαχείριση της ασφάλειας των ψηφιακών συστημάτων.

- **Συνέπεια**. Η πολιτική ασφάλειας θα πρέπει να είναι συνεπής με το σκοπό και τους στόχους του φορέα. Ουσιαστικά, θα πρέπει να συμβάλει στην ομαλή υλοποίηση της αποστολής του φορέα, να ενισχύει την εμπιστοσύνη των πολιτών στις παρεχόμενες υπηρεσίες, να υποστηρίζει τις επιχειρησιακές διεργασίες, διευκολύνοντας τους χρήστες των ψηφιακών συστημάτων στην ασφαλή και ευέλικτη λειτουργία των εφαρμογών τους.



ΣΧΗΜΑ 3.2 Κρίσιμοι Παράγοντες Επιτυχίας Πολιτικής Ασφάλειας

- **Υπεύθυνος Ασφάλειας**. Αποτελεί το κεντρικό σημείο αναφοράς όλων των χρηστών στο φορέα για την εφαρμογή του σχεδίου ασφάλειας. Θα πρέπει να έχει ως αποκλειστική αρμοδιότητα και αντικείμενο την ασφάλεια των ψηφιακών συστημάτων, να διαθέτει τις απαραίτητες γνώσεις, δεξιότητες και εμπειρία και να υποστηρίζεται από τους διαχειριστές των ψηφιακών συστημάτων στην εκτέλεση των καθηκόντων του.

- **Καταλληλότητα**. Η πολιτική ασφάλειας και οι διαδικασίες υλοποίησης των μέτρων προστασίας θα πρέπει να είναι εύχρηστες και συμβατές με τα ιδιαίτερα χαρακτηριστικά και την κουλτούρα των εργαζομένων, ώστε να μην απαξιωθεί ή απορριφθεί στην πράξη. Θα πρέπει να αποτελεί προστιθέμενη αξία για το φορέα και να υιοθετηθεί από το σύνολο του προσωπικού.

- **Εκπαίδευση**. Η επιμόρφωση του προσωπικού αποσκοπεί στην εδραίωση μιας κουλτούρας ασφάλειας, συμβάλλοντας αποφασιστικά στη διατήρηση του επιθυμητού επιπέδου ασφάλειας και στην επίτευξη των επιχειρησιακών στόχων του φορέα. Η επίγνωση και η ευαισθητοποίηση των εργαζομένων αναφορικά με την ασφάλεια στον κυβερνοχώρο, οδηγεί στην κατανόηση και εφαρμογή του σχεδίου ασφάλειας. Ιδιαίτερα σημαντικό είναι το ποσοστό των περιστατικών ασφάλειας που οφείλεται στους ίδιους τους υπαλλήλους του οργανισμού, οι οποίοι πολλές φορές από έλλειψη σωστής ενημέρωσης, παραβιάζουν τους κανόνες και τις διαδικασίες της πολιτικής ασφάλειας, εκθέτοντας τα ψηφιακά συστήματα σε κίνδυνο ή διαταράσσοντας την ομαλή λειτουργία τους.

- **Έλεγχος**. Για την ορθή εφαρμογή και βελτίωση του σχεδίου ασφάλειας είναι απαραίτητη η διεξαγωγή εσωτερικών αλλά και εξωτερικών ελέγχων (audits), καθώς και ο προγραμματισμός περιοδικών penetration tests. Η αξιολόγηση της αποτελεσματικότητας της πολιτικής ασφάλειας και των αντιμέτρων συνεισφέρει στην αναθεώρησή της και στον έγκαιρο εντοπισμό ευπαθειών.

3.5. Μελέτη Περίπτωσης

1. Σχολιάστε την πολιτική ασφάλειας του ΟΣΕ στον ακόλουθο διαδικτυακό σύνδεσμο: https://www.ose.gr/el/αρχικη/πολιτική-ασφάλειας-πληροφοριών

2. Σχεδιάστε μία εκπαιδευτική παρέμβαση με στόχο την ευαισθητοποίηση και ενημέρωση της Διοίκησης και του προσωπικού ενός φορέα της Δημόσιας Διοίκησης για την πολιτική ασφάλειας που πρόκειται να εφαρμοστεί.

3.6. Βιβλιογραφία

- Network Security Essentials: Applications and Standards (6th Edition), by William Stallings, Pearson Education Limited, 2017.
- Διαχείριση της ασφάλειας πληροφοριών, Σ. Κάτσικας, Εκδόσεις Πολιτεία, 2015, ISBN 9789605464158
- Γκρίτζαλης Σ., Κάτσικας Σ., Γκρίτζαλης Δ., Ασφάλεια Δικτύων Υπολογιστών, Παπασωτηρίου, Αθήνα 2003.
- Κάτσικας Σ., Γκρίτζαλης Δ., Γκρίτζαλης Σ. (επ. επιμ.), Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, Αθήνα 2004.
- Peltier T., Information Security Policies and Procedures, CRC Press, 1999.

4. ΔΙΑΔΙΚΑΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

Σκοπός του κεφαλαίου είναι η αναλυτική περιγραφή επιλεγμένων προτεινόμενων διαδικασιών ασφάλειας στο πλαίσιο εφαρμογής του σχεδίου ασφάλειας ενός υποθετικού οργανισμού της Δημόσιας Διοίκησης με την ονομασία «Φορέας». Αναλυτικότερα, θα παρουσιαστούν τέσσερις ενδεικτικές διαδικασίες που αφορούν την ελεγχόμενη πρόσβαση στο εσωτερικό δίκτυο (network access control), την ελεγχόμενη πρόσβαση στον ιστότοπο (website access control), τη διαδικασία διαχείρισης αλλαγών (change management procedure) και το σχέδιο συνέχισης λειτουργίας (business continuity plan).

4.1. Ελεγχόμενη Πρόσβαση στο Δίκτυο

4.1.1. Στόχος

Βασική διαδικασία ασφάλειας για κάθε φορέα του δημοσίου αποτελεί η ελεγχόμενη πρόσβαση των χρηστών στο εσωτερικό δίκτυο (network access control), διότι πλέον οι περισσότεροι εργαζόμενοι διαθέτουν ηλεκτρονικό υπολογιστή για τη διεκπεραίωση των υπηρεσιακών τους καθηκόντων και τα περισσότερα δεδομένα και οι πληροφορίες βρίσκονται σε ψηφιακή μορφή. Τα αποθηκευμένα δεδομένα στους εξυπηρετητές και στους προσωπικούς υπολογιστές των χρηστών πρέπει να προστατεύονται από τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης.

Η πρόσβαση των χρηστών στο δίκτυο θα γίνεται μέσω προσωπικών λογαριασμών. Η χορήγηση των συνθηματικών θα έγκειται στους γενικούς κανόνες χορήγησης κωδικών όπως αυτές έχουν αποτυπωθεί στη Μελέτη Ασφάλειας. Οι χρήστες είναι υποχρεωμένοι να διαφυλάττουν τους κωδικούς πρόσβασης των συνθηματικών τους ώστε να αποφευχθούν οι πιθανότητες να αποκαλυφθούν σε μη εξουσιοδοτημένα πρόσωπα.

4.1.2. Ρόλοι

Στα περισσότερα ψηφιακά συστήματα οι κωδικοί πρόσβασης αποτελούν την πρώτη δικλείδα ασφαλείας και κατά συνέπεια, είναι σημαντικό η χρήση τους να γίνεται συνειδητά και υπεύθυνα. Οι χρήστες δεν πρέπει να μοιράζονται τους λογαριασμούς και τους κωδικούς τους με συναδέλφους, φίλους, γνωστούς ή συγγενείς, ούτε να τους αποκαλύπτουν μέσω τηλεφώνου ή ηλεκτρονικού ταχυδρομείου.

Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν σε τακτικά διαστήματα, ενώ οι χρήστες των οποίων οι λογαριασμοί ανήκουν σε ομάδες με αυξημένα δικαιώματα, π.χ.

διαχειριστές συστημάτων ή εφαρμογών, θα πρέπει να έχουν ξεχωριστούς κωδικούς για όλους τους υπόλοιπους λογαριασμούς τους. Οι χρήστες δεν θα πρέπει να καταγράφουν τους κωδικούς τους σε χαρτί και να το αφήνουν έκθετο στο γραφείο τους. Ποτέ επίσης δεν θα πρέπει να αποθηκεύονται οι κωδικοί ηλεκτρονικά σε υπολογιστή ή σε κινητό χωρίς κρυπτογράφηση.

Για την καλύτερη διαχείριση και προστασία των δεδομένων θα οριστούν δύο βασικά επίπεδα χρηστών: α) Διαχειριστής και β) Υπάλληλος. Κάθε επίπεδο χρήστη θα έχει ανάλογες δυνατότητες, υποχρεώσεις και δικαιώματα σύμφωνα με τα παρακάτω:

1. Διαχειριστής

Ο λογαριασμός Διαχειριστή θα δοθεί μόνο σε συγκεκριμένους υπαλλήλους που θα είναι υπεύθυνοι για την παραμετροποίηση και επίλυση προβλημάτων δικτύου. Ο λογαριασμός αυτός θα έχει πρόσβαση σε όλους τους φακέλους και τα δεδομένα όλων των εξυπηρετητών και ηλεκτρονικών υπολογιστών. Επίσης, θα έχει τη δυνατότητα εγκατάστασης και απεγκατάστασης προγραμμάτων που είναι χρήσιμα για την καλύτερη λειτουργία του δικτύου. Τέλος, θα είναι υπεύθυνος για την εγκατάσταση των νέων εκδόσεων του αντί-ιομορφικού λογισμικού και την ενημέρωση των λειτουργικών συστημάτων. Ο Διαχειριστής θα έχει επίσης πλήρη έλεγχο σε όλες τις εφαρμογές.

2. Υπάλληλος

Ο συγκεκριμένος λογαριασμός θα δίδεται σε όλους τους υπαλλήλους που θα διαθέτουν ηλεκτρονικό υπολογιστή. Τα δικαιώματα του θα είναι περιορισμένα όσον αφορά την εισαγωγή και επεξεργασία αρχείων. Ο έλεγχος στα τοπικά αρχεία του υπολογιστή του θα είναι πλήρης αλλά δεν θα υπάρχει δυνατότητα εγκατάστασης εφαρμογών λογισμικού ή περιφερειακών συσκευών. Για οποιαδήποτε πρόβλημα ή δυσλειτουργία παρατηρείται θα πρέπει να απευθύνεται στους Διαχειριστές για την επίλυση τους.

Ο κάθε λογαριασμός θα έχει μοναδική ταυτότητα και θα αποτελείται από το *Όνομα Χρήστη* και τον *Κωδικό Πρόσβασης* (*συνθηματικά*). Θα αποδίδεται στον κάθε χρήστη ξεχωριστά και αυτός θα είναι υπεύθυνος για την διαφύλαξη του. Η απόδοση του κάθε λογαριασμού στον αντίστοιχο χρήστη θα βοηθήσει στην ανεύρεση του χωρίς την εμφάνιση του αληθινού του ονόματος και της ιεραρχικής του θέσης. Για την διαφύλαξη αυτών, ο κάθε λογαριασμός θα πρέπει να μην παρέχει ενδείξεις των προνομίων του χρήστη, να μην παρέχει ενδείξεις της ιεραρχικής του θέσης και να μην περιέχει το Ονοματεπώνυμο του.

Η Μονάδα Πληροφορικής είναι αρμόδια για να δημιουργήσει μια αλγοριθμική ακολουθία για την αυτόματη δημιουργία ονομάτων χρηστών και την αποθήκευση τους.

Οι Διαχειριστές θα πρέπει να αλλάξουν αμέσως τον αρχικό λογαριασμό που τους δίνεται από το σύστημα και να τον μετονομάσουν σε λογαριασμό που δεν θα προδίδει την ταυτότητα και τις αρμοδιότητες τους.

Η ομάδα των Διαχειριστών θα είναι υπεύθυνη για την διαχείριση των λογαριασμών των χρηστών, τη δημιουργία νέων και τον έλεγχο για την σωστή τους λειτουργία. Θα είναι επίσης υπεύθυνη για τις ρυθμίσεις και τις ενδεχόμενες αλλαγές που θα αιτηθεί κάποιος χρήστης. Θα είναι τέλος, υπεύθυνη για την ενημέρωση των νέων υπαλλήλων. Οι χρήστες οφείλουν να ακολουθούν πιστά τις διαδικασίες για τη διατήρηση της ασφαλής λειτουργίας του συστήματος.

Σε περίπτωση που κάποιος χρήστης ξεχάσει τα συνθηματικά του η διαδικασία που θα πρέπει να ακολουθηθεί είναι:

- Εάν έχει ξεχάσει το Όνομα Χρήστη, ο Διαχειριστής το αναζητά μέσα από τη βάση χρηστών του συστήματος και ενημερώνει τον χρήστη.
- Εάν έχει ξεχάσει τον Κωδικό Πρόσβασης, ο Διαχειριστής προχωρά στην αρχικοποίηση του κωδικού πρόσβασης του χρήστη, διαγράφοντας τον παλιό κωδικό (που ούτε ο ίδιος δεν τον γνωρίζει) και ορίζοντας έναν καινούργιο. Στη συνέχεια ενημερώνει το χρήστη για τον νέο κωδικό.
- Υποχρέωση του χρήστη, την πρώτη φορά που θα συνδεθεί στο εσωτερικό δίκτυο, πρέπει να είναι η αλλαγή του κωδικού. Σε κάθε περίπτωση ο νέος κωδικός θα πρέπει να ακολουθεί τους κανόνες δημιουργίας κωδικών.

Αναλυτικότερα, οι ρόλοι περιγράφονται παρακάτω:

<u>Μονάδα Πληροφορικής</u>

Η Μονάδα Πληροφορικής, είναι αρμόδια για τον καθορισμό των κανόνων πρόσβασης, καθώς και το σχεδιασμό και την δημιουργία των δικαιωμάτων πρόσβασης που αντιστοιχούν στις υπηρεσιακές ανάγκες των θέσεων σε συνεργασία με τις υπόλοιπες επιχειρησιακές μονάδες του φορέα. Επιπλέον είναι αρμόδια για την εκχώρηση σε κάθε χρήστη, κατόπιν σχετικών αιτιολογημένων αιτημάτων των Προϊσταμένων τους, των δικαιωμάτων πρόσβασης που προβλέπονται για την συγκεκριμένη θέση εργασίας. Ειδικότερα, η Μονάδα Πληροφορικής εκτελεί τις ακόλουθες εργασίες (με προσωπικό διακριτό για την κάθε μία):

- Διαχείριση Αιτημάτων Παροχής Πρόσβασης. Έλεγχος πληρότητας των αιτημάτων χορήγησης ή μεταβολής δικαιωμάτων πρόσβασης που αποστέλλονται από τα Τμήματα του οργανισμού, αρχειοθέτηση των αιτημάτων αυτών και ενημέρωση του αρχείου χρηστών με τα δικαιώματα πρόσβασης που τους εκχωρήθηκαν στα συστήματα του φορέα.

- Εκχώρηση Δικαιωμάτων Πρόσβασης. Υλοποίηση των αιτημάτων παροχής, μεταβολής, αναίρεσης, ή διαγραφής δικαιωμάτων πρόσβασης στο σύστημα.

- Διαγραφή Ανενεργών Λογαριασμών. Διαγραφή λογαριασμών υπαλλήλων που έχουν αποχωρήσει από τον οργανισμό για οποιονδήποτε λόγο (απόσπαση, μετάταξη, συνταξιοδότηση κ.ά.) μετά από ενημέρωση από το αρμόδιο Τμήμα Προσωπικού του φορέα.

Ομάδα Διαχειριστών

Η ομάδα διαχειριστών ορίζεται από τη Μονάδα Πληροφορικής. Είναι υπεύθυνη για την δημιουργία, διαχείριση και έλεγχο όλων των λογαριασμών των χρηστών. Βρίσκεται σε επικοινωνία με τους χρήστες για τυχόν προβλήματα ή παρατηρήσεις. Οι διαχειριστές προτού προβούν σε οποιαδήποτε ενέργεια επαληθεύουν την εγκυρότητα των γραπτών αιτήσεων με τα δεδομένα του συστήματος. Ενεργούν ελέγχους για την πιστοποίηση των λειτουργιών, ενώ είναι υπεύθυνοι για την ενημέρωση των χρηστών σχετικά με τις διαδικασίες ασφάλειας.

Χρήστης

Ο χρήστης είναι υπεύθυνος για την διασφάλιση των συνθηματικών του, τη σωστή εφαρμογή της διαδικασίας πρόσβασης, της ενημέρωσης των διαχειριστών για οποιοδήποτε πρόβλημα προκύψει και την εφαρμογή των οδηγιών χρήσης όπου θα λάβει από τους Διαχειριστές.

4.1.3. Περιγραφή Διαδικασίας

Για τη δημιουργία λογαριασμών χρηστών πρέπει να ακολουθηθούν συγκεκριμένες ενέργειες. Με την τοποθέτηση κάθε χρήστη σε Τμήμα του φορέα, του ανατίθενται συγκεκριμένα καθήκοντα και αρμοδιότητες. Ο Προϊστάμενος Τμήματος θα πρέπει να υποβάλει αίτημα προς στη Μονάδα Πληροφορικής για τις περαιτέρω ενέργειες και την δημιουργία λογαριασμού χρήστη με τις ανάλογες αρμοδιότητες και δικαιοδοσίες οι οποίες αναφέρονται τεκμηριωμένες στην αίτηση.

Η εν λόγω αίτηση αποτυπώνει αναλυτικά και τεκμηριωμένα, τα πλήρη στοιχεία ταυτότητας του χρήστη, την ιεραρχική του θέση, τις αρμοδιότητες του, τα αναγκαία

δικαιώματα πρόσβασης σε δικτυακούς πόρους και τις ανάλογες άδειες για χρήση εφαρμογών λογισμικού.

Σε κάθε χρήστη αναλογούν καθήκοντα και αρμοδιότητες οι οποίες, καθορίζουν το επίπεδο διαβάθμισης της πληροφορίας που θα έχει δικαίωμα να επεξεργαστεί στο σύστημα. Αυτές αναφέρονται στην αίτηση αναλυτικά και αιτιολογημένα ώστε να μπορεί η Μονάδα Πληροφορικής να ορίσει τα κατάλληλα δικαιώματα πρόσβασης για κάθε λογαριασμό. Η εκχώρηση δικαιωμάτων ανά χρήστη δίνεται σύμφωνα με τα στοιχεία της αίτησης του Προϊσταμένου και με τα έγγραφα τεκμηρίωσης που τη συνοδεύουν.

Η αίτηση δημιουργίας νέου λογαριασμού χρήστη, που συμπληρώνεται από τον Προϊστάμενο του αντίστοιχου Τμήματος, προτείνεται να περιλαμβάνει τα παρακάτω στοιχεία για την ενημέρωση του αρχείου τεκμηρίωσης του ψηφιακού συστήματος.

Στοιχεία Ταυτότητας. Αναγράφονται τα στοιχεία ταυτότητας του χρήστη, όπως Όνομα, Επώνυμο, Γενική Διεύθυνση, Διεύθυνση, Τμήμα, email, Τηλέφωνο, κ.ά.

Προσβάσεις & Δικαιώματα. Ορίζονται τα δικαιώματα πρόσβασης στο δίκτυο και σε κοινόχρηστους πόρους, όπως: εξυπηρετητές, εκτυπωτές, κοινόχρηστους φακέλους, εφαρμογές, βάσεις δεδομένων, κ.ά.

Η αίτηση αφού συμπληρωθεί με όλα τα απαραίτητα στοιχεία καθώς και με τα στοιχεία τεκμηρίωσης αποστέλλεται από τον Προϊστάμενο του χρήστη στη Μονάδα Πληροφορικής για τις περαιτέρω ενέργειες, οι οποίες περιλαμβάνουν:

Έλεγχος ταυτότητας. Ελέγχεται η ταυτότητα του χρήστη σύμφωνα με την απόφαση τοποθέτησής του σε συγκεκριμένο Τμήμα του οργανισμού, καθώς και τα σχετικά δικαιώματα πρόσβασης που αντιστοιχούν στη θέση αυτή. Σε περίπτωση διαφορών ενημερώνεται ο αρμόδιος Προϊστάμενος.

Δημιουργία Λογαριασμού. Τα στοιχεία του χρήστη καταχωρούνται στο σύστημα, δημιουργείται ο νέος λογαριασμός και ορίζονται τα δικαιώματα πρόσβασης. Με τη δημιουργία κάθε νέου λογαριασμού συστήματος δίνονται στους χρήστες προσωρινοί κωδικοί μέχρι να συνδεθούν για πρώτη φορά. Μετά την εισαγωγή τους στο σύστημα με τον προσωρινό κωδικό είναι υποχρεωμένοι να τον αλλάξουν σύμφωνα με τις οδηγίες που θα λάβουν για τη δημιουργία νέων κωδικών.

Οι κανόνες δημιουργίας νέων κωδικών πρόσβασης είναι οι παρακάτω:

- Ορισμός κωδικού πρόσβασης μήκους 7 χαρακτήρων για τους χρήστες και 10 χαρακτήρων για τους διαχειριστές. Όσο περισσότερους χαρακτήρες έχει ένας κωδικός τόσο πιο δύσκολο είναι να βρεθεί από εφαρμογή εξαντλητικής αναζήτησης κωδικών.

- Ο κωδικός θα πρέπει να περιέχει ειδικούς χαρακτήρες για την αύξηση του επιπέδου ασφάλειας (! , @ , # , $, % , & , * , +).

- Ο κωδικός θα πρέπει να περιέχει 2 ή περισσοτέρους αριθμούς αλλά πάντα θα υπάρχουν και τουλάχιστον 2 αλφαβητικοί λατινικοί χαρακτήρες.

- Δεν επιτρέπεται ο ορισμός κωδικού που ένας τρίτος θα μπορούσε εύκολα να μαντέψει.

- Η ανανέωση του κωδικού είναι υποχρεωτική κάθε 100 ημέρες. Θα υπάρχει ενημερωτικό μήνυμα για τις τελευταίες 5 ημέρες και εάν δεν αλλαχθεί ο κωδικός, τότε ο λογαριασμός θα κλειδώνει.

- Ο νέος κωδικός δεν επιτρέπεται να είναι επανάληψη κάποιου που έχει ήδη χρησιμοποιηθεί παλαιότερα από τον συγκεκριμένο χρήστη.

- Ο κωδικός είναι αυστηρά προσωπικός και πρέπει να παραμένει μυστικός από συναδέλφους.

Μετά τη δημιουργία και ρύθμιση του νέου λογαριασμού, η Μονάδα Πληροφορικής ενημερώνει το χρήστη με την αποστολή μηνύματος ηλεκτρονικού ταχυδρομείου για τους κανόνες ορθής χρήσης και τις οδηγίες διαχείρισης των συνθηματικών του.

4.2. Ελεγχόμενη Πρόσβαση Ιστότοπου

4.2.1. Στόχος

Η Διαδικασία Ελεγχόμενης Πρόσβασης στον Ιστότοπο του Φορέα (Website Access Control) στοχεύει στη διασφάλιση εξουσιοδοτημένης πρόσβασης στο πολυμεσικό περιεχόμενο του οργανισμού. Ο ιστότοπος του φορέα, εκτός του ενημερωτικού χαρακτήρα, θα παρέχει και ηλεκτρονικές υπηρεσίες προς τους πολίτες.

Η διαδικασία ελεγχόμενης πρόσβασης στον ιστότοπο του φορέα θα ακολουθείται για την δημιουργία νέου λογαριασμού χρήστη, καθώς και για την ταυτοποίηση και αυθεντικοποίηση του χρήστη κάθε φορά που επιθυμεί να συνδεθεί στον ιστότοπο.

Η διαδικασία αυτή θωρακίζει τον ιστότοπο από τη μη εξουσιοδοτημένη πρόσβαση. Η ελεγχόμενη πρόσβαση δεν συμβάλει μόνο στην ασφάλεια των χρηστών και του ιστότοπου αλλά και στην ευκολία πλοήγησης και αναζήτησης πληροφοριών από τους πολίτες.

4.2.2. Ρόλοι

Με τη διαδικασία ελεγχόμενης πρόσβασης στον ιστότοπο θα ταυτοποιούνται και θα αυθεντικοποιούνται οι πολίτες που επιθυμούν να αξιοποιήσουν τις ηλεκτρονικές υπηρεσίες του φορέα. Για την καλύτερη εφαρμογή της διαδικασίας θα πρέπει να γίνει διαχωρισμός των χρηστών, καθώς και μία οριοθέτηση των δικαιωμάτων τους.

Για την πρόσβαση στον ιστότοπο ένας πολίτης θα πρέπει να εισάγει όνομα χρήστη και κωδικό, ώστε να επιβεβαιώνεται το δικαίωμα χρήσης των λειτουργιών του ιστότοπου, εκτός των βασικών που η χρήση τους είναι ελεύθερη. Η δυνατότητα δημιουργίας νέων συνθηματικών θα παρέχεται μέσω της ηλεκτρονικής υπηρεσίας δημιουργίας προσωπικού λογαριασμού χρήστη. Για αυτή τη δημιουργία θα πρέπει ο χρήστης να δηλώσει τα στοιχεία του σε μία φόρμα όπου θα δίνεται μέσα από τον ιστότοπο και να κάνει αποδοχή των όρων όπου θα αναφέρονται εκεί, πριν την αποστολή της αίτησης για δημιουργία λογαριασμού στο φορέα.

Επιπλέον, υπάρχει η δυνατότητα πρόσβασης στον ιστότοπο μέσω της ηλεκτρονικής υπηρεσίας αυθεντικοποίησης του συστήματος TAXISnet, χρησιμοποιώντας τα αντίστοιχα συνθηματικά. Ο κάθε λογαριασμός είναι αυστηρά προσωπικός και οι χρήστες είναι υπεύθυνοι για όποιες ενέργειες εκτελεστούν με αυτόν.

Για την ασφάλεια και την ευκολία χρήσης του ιστότοπου θα οριστούν δύο επίπεδα πρόσβασης, των πολιτών και των διαχειριστών του συστήματος διαχείρισης περιεχομένου. Ανάλογα με τα δικαιώματα που θα έχει κάθε χρήστης, θα έχει και τις ανάλογες δυνατότητες πρόσβασης στο σύστημα.

1. Διαχειριστής

Ο χρήστης Διαχειριστής διαθέτει πλήρη δικαιώματα πρόσβασης στο σύστημα διαχείρισης περιεχομένου, με δυνατότητα επεξεργασίας των ιστοσελίδων και των αρχείων του ιστότοπου, καθώς και του προφίλ των χρηστών. Παρακολουθεί και ελέγχει την ομαλή λειτουργία του συστήματος και επικοινωνεί άμεσα με τον Υπεύθυνο Ασφάλειας του φορέα σε περίπτωση περιστατικού ασφάλειας. Επίσης, αποφασίζει ποιες ιστοσελίδες θα πρέπει να μεταδίδουν πληροφορία κρυπτογραφημένη, όπως για παράδειγμα ιστοσελίδες για τη δημιουργία και εισαγωγή κωδικών πρόσβασης.

2. Πολίτης

Ο χρήστης με τα δικαιώματα του πολίτη μπορεί να πλοηγηθεί στον ιστότοπο και να χρησιμοποιήσει τις παρεχόμενες ηλεκτρονικές υπηρεσίες του φορέα. Κάθε χρήστης που έχει δημιουργήσει λογαριασμό και του έχει παραχωρηθεί όνομα χρήστη και αντίστοιχος κωδικός, είναι έτοιμος να κάνει χρήση των δικαιωμάτων του προσωπικού του προφίλ.

4.2.3. Περιγραφή Διαδικασίας

Η Διαδικασία Ελεγχόμενης Πρόσβασης στον Ιστότοπο του Φορέα περιγράφεται στα ακόλουθα βήματα:

Δημιουργία Νέου Λογαριασμού. Στην αρχική ιστοσελίδα θα υπάρχει η επιλογή για σύνδεση στον ιστότοπο με χρήση λογαριασμού ή για την εγγραφή νέου χρήστη. Με την επιλογή δημιουργίας νέου λογαριασμού θα εμφανίζεται μία λίστα καταχώρισης στοιχείων όπου ο χρήστης καλείται να συμπληρώσει με πραγματικά στοιχεία ή θα μπορεί να δημιουργήσει νέο προφίλ με τη χρήση των συνθηματικών του TAXISnet. Για την δημιουργία νέου λογαριασμού, θα χρειαστεί ο χρήστης να δηλώσει κάποια προσωπικά δεδομένα και στοιχεία επικοινωνίας μέσω ειδικής φόρμας τα οποία θα χρησιμοποιηθούν για την ταυτοποίησή του.

Διαδικασία Πρόσβασης. Με την ολοκλήρωση της δημιουργίας του λογαριασμού, ο χρήστης μπορεί να εισάγει τα συνθηματικά του για να συνδεθεί στον ιστότοπο με τον λογαριασμό του χρησιμοποιώντας τις διαθέσιμες ηλεκτρονικές υπηρεσίες.

Διαγραφή Λογαριασμού. Σε περίπτωση που το επιθυμεί ο χρήστης υπάρχει η δυνατότητα αίτησης διαγραφής του λογαριασμού και του προφίλ του. Διαγραφή επίσης θα γίνεται όταν παρατηρηθεί παράνομη χρήση ενός λογαριασμού.

4.3. Διαδικασία Διαχείρισης Αλλαγών

4.3.1. Στόχος

Στόχος της Διαδικασίας Διαχείρισης Αλλαγών (Change Management Procedure) είναι να εξασφαλιστεί η ύπαρξη τυποποιημένης μεθόδου για τον αποτελεσματικό και αποδοτικό χειρισμό όλων των αλλαγών εξοπλισμού και λογισμικού, προκειμένου να ελαχιστοποιηθούν τυχόν επιπτώσεις στην ποιότητα των παρεχόμενων ηλεκτρονικών υπηρεσιών.

Κάθε εξοπλισμός θα φέρει σήμανση όπου θα αναγράφεται ο ειδικός κωδικός από τον οποίο θα γίνεται εύκολα αντιληπτό ο κατασκευαστής, το μοντέλο, τα βασικά χαρακτηριστικά και η ημερομηνία προμήθειας. Αλλαγές γίνονται σε περιπτώσεις αναβάθμισης ή βλάβης. Πριν από την οποιαδήποτε ενέργεια αλλαγής εξοπλισμού ή λογισμικού ενημερώνεται ο Προϊστάμενος της Μονάδας Πληροφορικής για την αιτιολόγηση της αναγκαιότητας της αλλαγής και για να δώσει τη σχετική έγκριση. Επίσης, στην περίπτωση που η αλλαγή αφορά την εγκατάσταση νέου τύπου εξοπλισμού ή λογισμικού απαιτείται επιπλέον η έγκριση του Υπεύθυνου Ασφάλειας.

Μέσω της διαδικασίας διαχείρισης αλλαγών είναι δυνατή η καταγραφή και παρακολούθηση του συνόλου του εξοπλισμού και λογισμικού που εγκαταστάθηκε στο ψηφιακό σύστημα του Φορέα.

4.3.2. Ρόλοι

Η Μονάδα Πληροφορικής θα πρέπει να είναι συνεχώς ενήμερη για όλες τις εξελίξεις σχετικά με τα θέματα αλλαγών εξοπλισμού και λογισμικού, αναλαμβάνοντας την εποπτεία και τον έλεγχο της διαδικασίας. Οι κρίσιμες αλλαγές εξοπλισμού και λογισμικού απαιτούν επιπλέον την έγκριση του Υπεύθυνου Ασφάλειας του φορέα.

Με την ολοκλήρωση της αλλαγής θα πρέπει να ενημερωθεί ο κατάλογος παγίων του φορέα για την καλύτερη τεκμηρίωση της υλικοτεχνικής υποδομής. Ο Υπεύθυνος Παγίων είναι υπεύθυνος για την καταγραφή και παρακολούθηση των παγίων.

4.3.3. Περιγραφή Διαδικασίας

Οι αλλαγές εξοπλισμού ή λογισμικού του φορέα θα πρέπει να υλοποιούνται υπό την εποπτεία της Μονάδας Πληροφορικής, ανεξαρτήτως μεγέθους ή αξίας της αλλαγής και να ορίζεται ο υπεύθυνος διαχειριστής του συστήματος, ο οποίος θα οφείλει να επιτηρεί την διαδικασία και να ελέγχει την ομαλή λειτουργία του συστήματος, ενημερώνοντας σχετικά τον Υπεύθυνο Ασφάλειας.

Η Μονάδα Πληροφορικής λαμβάνει μέριμνα για την αποτροπή κάθε απειλής απώλειας δεδομένων, δυσλειτουργίας του συστήματος ή ασυμβατότητας του νέου εξοπλισμού ή λογισμικού με το υφιστάμενο σύστημα. Τα βήματα που θα πρέπει να ακολουθήσει ο αρμόδιος διαχειριστής για την υλοποίηση της αλλαγής είναι τα παρακάτω:

Αλλαγή Εξοπλισμού

- Διαπιστώνεται η ανάγκη για την αλλαγή του εξοπλισμού.
- Ενημερώνεται η Μονάδα Πληροφορικής.
- Παραλαμβάνεται εξοπλισμός.
- Ελέγχεται ότι καλύπτει πλήρως την ανάγκη.
- Ελέγχεται ότι είναι ασφαλής για τη συγκεκριμένη χρήση.
- Εξετάζονται οι οδηγίες εγκατάστασης/ παραμετροποίησης του εξοπλισμού.
- Γίνονται όλες οι απαραίτητες ενέργειες για τη λήψη αντιγράφων ασφάλειας, εφόσον υπάρχουν χρήσιμα δεδομένα στο υλικό προς αντικατάσταση, για την πρόληψη απώλειας δεδομένων.
- Ελέγχεται ο νέος εξοπλισμός για να διαπιστωθεί η καλή λειτουργία του σε απομονωμένο περιβάλλον τεχνικών δοκιμών.
- Ενημερώνεται η επιχειρησιακή μονάδα του Φορέα που θα επηρεαστεί από την αλλαγή για τυχόν διακοπή λειτουργίας του συστήματος.
- Πραγματοποιείται η αλλαγή.
- Ελέγχεται η ομαλή λειτουργία του συστήματος.
- Επαναφορά των δεδομένων από το αντίγραφο ασφαλείας.
- Δημιουργείται νέο αντίγραφο ασφαλείας.
- Ενημερώνεται η Μονάδα Πληροφορικής για την έκβαση της αλλαγής.
- Καταγραφή της αλλαγής στο ημερολόγιο εργασιών περιγράφοντας τη σειρά των ενεργειών και τα ονόματα των υπευθύνων.

Αλλαγή Λογισμικού

- Αιτιολογείται η ανάγκη αλλαγής του λογισμικού.
- Ενημερώνεται η Μονάδα Πληροφορικής.
- Συντάσσεται τεχνική μελέτη η οποία περιγράφει αναλυτικά τις ανάγκες για το νέο λογισμικό, τις τυχόν επιπτώσεις σε περίπτωση που δεν γίνει η αλλαγή ή γίνει και προκληθούν απώλειες δεδομένων, μία σύντομη περιγραφή του νέου λογισμικού καθώς και η διαπίστωση ότι το νέο λογισμικό καλύπτει όλες τις απαιτήσεις και είναι συμβατό με το σύστημα.
- Αποφασίζεται ποιο λογισμικό καλύπτει πλήρως τις απαιτήσεις.
- Δημιουργείται αντίγραφο ασφαλείας, στο μηχάνημα όπου θα εγκατασταθεί το νέο λογισμικό, για τα δεδομένα όπου δύναται να επηρεασθούν με την αλλαγή του εν λόγω λογισμικού.
- Ελέγχεται η συμβατότητα των αρχείων με το νέο λογισμικό.
- Απεγκατάσταση παλιού λογισμικού.
- Εγκατάσταση νέου.
- Έλεγχος καλής λειτουργίας.
- Επαναφορά αρχείων συστήματος.
- Έλεγχος λειτουργίας αρχείων.
- Δημιουργία νέου αντιγράφου ασφαλείας.
- Ενημερώνεται η Μονάδα Πληροφορικής.
- Καταγραφή της αλλαγής στο ημερολόγιο εργασιών περιγράφοντας τη σειρά των ενεργειών και τα ονόματα των υπευθύνων.

4.4. Σχέδιο Συνέχισης Λειτουργίας

4.4.1. Στόχος

Το Σχέδιο Συνέχισης Λειτουργίας (Business Continuity Plan) θα πρέπει να λαμβάνει υπόψη τις πλέον πρόσφατες εξελίξεις στην πληροφορική στον βαθμό που επηρεάζουν τη λειτουργία του οργανισμού, συμβάλλοντας σημαντικά στην αποτελεσματική διαχείριση του λειτουργικού κινδύνου που σχετίζεται με κάθε ψηφιακό σύστημα.

Η απρόσκοπτη λειτουργία των συστημάτων και η αποτελεσματική υποστήριξή τους είναι παράγοντες κρίσιμοι τόσο για την εύρυθμη λειτουργία του φορέα και τη δημιουργία σχέσεων εμπιστοσύνης με τους (εσωτερικούς και εξωτερικούς) χρήστες, όσο και για την αποτελεσματική αντιμετώπιση του λειτουργικού κινδύνου. Η απρόσκοπτη λειτουργία και η αποτελεσματική υποστήριξη κάθε ψηφιακού συστήματος προϋποθέτουν την τήρηση των πολιτικών, προτύπων και διαδικασιών του φορέα από όλες τις εμπλεκόμενες υπηρεσιακές μονάδες, αλλά και τους παρόχους υπηρεσιών πληροφορικής.

Το Σχέδιο Συνέχισης Λειτουργίας (ΣΣΛ) είναι το έγγραφο που αναφέρεται στα μέτρα, τα οποία εφαρμόζονται σε περιπτώσεις έκτακτης ανάγκης, όπως της καταστροφής ενός υπολογιστικού κέντρου ή την κατάρρευση ενός επιχειρησιακού δικτύου.

Στο Σχέδιο Συνέχισης Λειτουργίας, το οποίο συμπληρώνει το Σχέδιο Ασφαλείας, προβλέπονται μέτρα που στοχεύουν στην ελαχιστοποίηση διακοπών της κανονικής λειτουργίας, στον περιορισμό της έκτασης των ζημιών και καταστροφών, καθώς και στην αποφυγή πιθανής κλιμάκωσης αυτών, στην εκπαίδευση, εξάσκηση και εξοικείωση των εργαζομένων με τις διαδικασίες έκτακτης ανάγκης, στη δυνατότητα γρήγορης αποκατάστασης της ομαλής λειτουργίας, καθώς και στην ελαχιστοποίηση των οικονομικών επιπτώσεων.

Το ΣΣΛ πρέπει να προσδιορίζει τους πιθανούς κινδύνους και γενικότερα τα κριτήρια που καθορίζουν την κατάσταση ως έκτατη και επιβάλλουν την ενεργοποίηση του σχεδίου. Πρέπει να υπάρχουν σαφείς και γραπτές διαδικασίες που να θέτουν τον φορέα σε κατάσταση έκτακτης ανάγκης και να επιτρέπουν εφαρμογή του σχεδίου.

Επιπρόσθετα, το σχέδιο πρέπει να περιέχει μία κατάσταση με τα μέλη του προσωπικού που θα κληθούν στην περίπτωση καταστροφής καθώς και τα τηλέφωνα των προμηθευτών υλικού και λογισμικού, των σημαντικών συνεργατών ή αρμόδιων φορέων που μπορούν να συνδράμουν στη συνέχιση της λειτουργίας του.

Ακόμη, το σχέδιο θα πρέπει να περιέχει διαδικασίες για τον υπολογισμό της ζημιάς από την καταστροφή που συντελέστηκε, ενώ θα πρέπει να περιέχει έναν ρεαλιστικό χρονοπρογραμματισμό με σαφή ανάθεση καθηκόντων για την αποκατάσταση της λειτουργίας της Υπηρεσίας, προτεραιοποιώντας τις κρίσιμες λειτουργίες.

Εκτός των άλλων, πραγματεύεται τη συνέχιση της λειτουργίας της υπολογιστικής και επικοινωνιακής υποδομής μετά από φυσικές καταστροφές (φωτιές, πλημμύρες, σεισμούς, κ.ά.). Για την ταχύτερη δυνατή αντιμετώπιση των έκτακτων περιστατικών, προτείνεται η τοποθέτηση συναγερμών, οι οποίοι χρησιμοποιούνται τόσο για την ανίχνευση (επικείμενης) ζημιάς λόγω των φαινομένων αυτών, αλλά και για την ανίχνευση εισβολών στα συστήματα. Όσον αφορά τις εισβολές, για την ανίχνευση και αντιμετώπισή τους μπορούν να χρησιμοποιηθούν ειδικά συστήματα λογισμικού, τα επονομαζόμενα συστήματα ανίχνευσης εισβολών, τα οποία κάνουν χρήση διαφόρων αισθητήρων και δίνουν τακτικές αναφορές στα κέντρα ελέγχου.

Ως **περιστατικό** είναι το αποτέλεσμα του πιθανού κινδύνου που μπορεί να προκαλέσει ένα έκτατο συμβάν και να ενεργοποιήσει τη διαδικασία για την εφαρμογή του ΣΣΛ. Τα κριτήρια που καθορίζουν μια κατάσταση κινδύνου ως περιστατικό είναι τα παρακάτω:

- Κίνδυνοι ολικής καταστροφής: πυρκαγιά, διαρροή/ πλημμύρα, καταιγίδα με ισχυρούς ανέμους, σεισμός, τρομοκρατικές ενέργειες και δολιοφθορά.
- Κίνδυνοι μερικής καταστροφής: διακοπή ρεύματος, αβλεψία προσωπικού.
- Κίνδυνοι καταστροφής από ιομορφικό λογισμικό: προσβολή ψηφιακού συστήματος από ιομορφικό λογισμικό.
- Κίνδυνοι μη εξουσιοδοτημένης πρόσβασης στο σύστημα: απόπειρα μη εξουσιοδοτημένης πρόσβασης στο σύστημα.

Πρέπει να επισημανθεί, ωστόσο, ότι οι κίνδυνοι αυτού του είδους ελαχιστοποιούνται, αν έχει προηγουμένως καταστρωθεί ένα προσεγμένο σχέδιο ασφάλειας. Το Σχέδιο Συνέχισης Λειτουργίας, άλλωστε, έρχεται να καλύψει τα κενά που πιθανόν να έχει αφήσει το Σχέδιο Ασφάλειας.

4.4.2. Ρόλοι

Ο φορέας θα πρέπει να διαθέτει αρμόδια Μονάδα Πληροφορικής, λειτουργικά και διοικητικά ανεξάρτητη από τους τελικούς χρήστες των υπηρεσιών πληροφορικής, η οποία θα πρέπει να διαθέτει οργανόγραμμα στο οποίο να απεικονίζονται οι επιχειρησιακές και οργανωτικές ανάγκες της Μονάδας και να περιγράφονται με σαφήνεια οι αρμοδιότητες των επί μέρους Τομέων που την αποτελούν. Ιδιαίτερα σημαντικό είναι να εξασφαλίζεται η αναπλήρωση του προσωπικού τουλάχιστον στις κρίσιμες μηχανογραφικές λειτουργίες.

Επίσης, να απεικονίζεται ο διαχωρισμός των καθηκόντων προκειμένου να αποκλείεται η ύπαρξη ασυμβίβαστων ρόλων, να παρέχεται η δυνατότητα καταλογισμού των ευθυνών και να αξιοποιούνται με τον καταλληλότερο τρόπο οι δυνατότητες του προσωπικού. Ειδικότερα, θα πρέπει να διασφαλίζεται ότι διαχωρίζονται πλήρως οι λειτουργίες που σχετίζονται με το σχεδιασμό και την ανάπτυξη των συστημάτων από τις λειτουργίες που αφορούν στην καθημερινή λειτουργία τους.

Η Μονάδα Πληροφορικής θα πρέπει να διαθέτει καταγεγραμμένες και επίσημα εγκεκριμένες περιγραφές θέσεων εργασίας στις οποίες θα περιλαμβάνονται οι αρμοδιότητες, οι υπευθυνότητες και οι δεξιότητες που απαιτούνται για κάθε θέση.

Επιπλέον, ο Υπεύθυνος Ασφάλειας θα πρέπει να υποστηρίζεται στο έργο του από εξειδικευμένη ομάδα έμπειρων στελεχών πληροφορικής, οι οποίοι να έχουν ολοκληρωμένη εικόνα για το επίπεδο ασφάλειας του συστήματος και τους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία του. Στις αρμοδιότητές τους περιλαμβάνονται, μεταξύ άλλων, η συμμετοχή στην αξιολόγηση και διαχείριση των κινδύνων των ψηφιακών συστημάτων, η σύνταξη και ενημέρωση της πολιτικής ασφάλειας, η συμμετοχή στη διαδικασία εύρεσης λύσεων για την κάλυψη κενών ασφάλειας και την αντιμετώπιση έκτακτων περιστατικών κ.ά.

4.4.3. Περιγραφή Διαδικασίας

Ο φορέας θα πρέπει να διαθέτει εγκεκριμένο από τη Διοίκηση Σχέδιο Συνέχειας Λειτουργίας (ΣΣΛ) για τα ψηφιακά συστήματα, έτσι ώστε να εξασφαλίζεται η συνέχεια των κρισιμότερων λειτουργιών τους. Της δημιουργίας ΣΣΛ θα πρέπει να προηγούνται διαδικασίες ανάλυσης επιχειρηματικών επιπτώσεων (business impact analysis) και ανάλυσης κινδύνων (risk assessment).

Βάσει των παραπάνω διαδικασιών θα προσδιορίζονται όλες οι κρίσιμες λειτουργίες καθώς και τα συστήματα – πόροι που χρησιμοποιούν, θα προσδιορίζονται όλοι οι κίνδυνοι που απειλούν τις κρίσιμες λειτουργίες και θα κατατάσσονται σύμφωνα με την πιθανότητα εμφάνισής τους και τις πιθανές επιπτώσεις τους στα συστήματα και τις λειτουργίες και επιπλέον, θα σταθμίζεται το λειτουργικό κόστος από ενδεχόμενη διακοπή των κρίσιμων λειτουργιών και το κόστος ενεργοποίησης του ΣΣΛ για να προσδιορίζονται οι συνθήκες που θα το θέτουν σε εφαρμογή.

Αρχικά θα πρέπει να εξασφαλιστεί η συνέχεια των εργασιών για τις οποίες υπάρχει διαδικασία λήψης και διαχείρισης αντιγράφων ασφαλείας του λογισμικού, των παραμέτρων λειτουργίας και των δεδομένων, καθώς και η ύπαρξη του αναγκαίου εφεδρικού εξοπλισμού, συσκευών παροχής αδιάλειπτης τάσης, ηλεκτρογεννητριών κ.λπ., στους χώρους λειτουργίας των συστημάτων.

Με στόχο την αποτελεσματική και γρήγορη ανάκτηση των δεδομένων και του λογισμικού εφαρμογών, θα πρέπει τα αντίγραφα ασφαλείας να δημιουργούνται με συγκεκριμένες διαδικασίες και με συχνότητα, η οποία να υπαγορεύεται από την κρισιμότητα των πληροφοριών, ώστε να διασφαλίζεται: η ασφαλής αποθήκευση στο χώρο των συστημάτων, η ασφαλής μεταφορά και φύλαξη σε απομακρυσμένο χώρο των επιπλέον αντιγράφων (π.χ. τραπεζική θυρίδα), η επιτυχία των δοκιμών για τη διασφάλιση της ακεραιότητας των δεδομένων, η αρχειοθέτηση με κατάλληλη αναγραφή στα μέσα αποθήκευσης του περιεχομένου και του χρόνου αποθήκευσης των δεδομένων, καθώς και η ανακύκλωση των μαγνητικών μέσων.

Για να θεωρηθεί ολοκληρωμένο και αποτελεσματικό ένα ΣΣΛ για τα ψηφιακά συστήματα, συνιστάται να είναι γραμμένο σε απλή και κατανοητή γλώσσα και να κοινοποιείται επίσημα σε όλο το προσωπικό. Τυχόν διαβαθμισμένες πληροφορίες του σχεδίου, όπως κωδικοί, IP διευθύνσεις κ.λπ., θα πρέπει να γνωστοποιούνται μόνο σε εξουσιοδοτημένα άτομα. Αντίγραφο του ΣΣΛ να φυλάσσεται σε κατάλληλο χώρο και σε ασφαλή απόσταση από το μηχανογραφικό κέντρο.

Ένα τέτοιο σχέδιο θα πρέπει να περιλαμβάνει:

1. Κατάταξη των συστημάτων βάση λειτουργικής ανάγκης.

2. Τη σαφή ιεραρχική δομή των στελεχών που συμμετέχουν στην εφαρμογή του, τις αρμοδιότητές τους, καθώς και τους υπεύθυνους λήψης αποφάσεων σε κάθε ομάδα έκτακτης ανάγκης.

3. Τις διαδικασίες εκτίμησης του εύρους της καταστροφής, με βάση τις οποίες προσδιορίζονται επακριβώς τα τμήματα του σχεδίου τα οποία θα πρέπει να ενεργοποιηθούν.

4. Τις διαδικασίες ενεργοποίησης του σχεδίου, ειδοποίησης των στελεχών και κινητοποίησης των ομάδων έκτακτης ανάγκης.

5. Τις ενέργειες που θα εκτελούνται σε συγκεκριμένες επείγουσες καταστάσεις, οι οποίες μεταξύ των άλλων θα πρέπει να διασφαλίζουν το προσωπικό σε περίπτωση κινδύνου/ καταστροφής (π.χ.: φωτιά, σεισμός κ.λπ.).

6. Κατάλογος προμηθευτών με τους οποίους υπάρχουν συμβάσεις, οι υπηρεσίες που αυτοί προσφέρουν και οι αναμενόμενοι χρόνοι απόκρισής τους σε περίπτωση έκτακτης ανάγκης.

7. Τις διαδικασίες που εξασφαλίζουν ότι το ΣΣΛ συντηρείται, προσαρμόζεται και ενημερώνεται σε κάθε αλλαγή των ροών εργασίας του Φορέα.

8. Τις διαδικασίες εκπαίδευσης του προσωπικού σύμφωνα με τις αρμοδιότητες που αναλαμβάνουν κατά την υλοποίηση του ΣΣΛ.

9. Τις διαδικασίες εκτέλεσης δοκιμών, σύμφωνα με τις οποίες:

   - θα προσδιορίζεται η συχνότητά τους (τουλάχιστον μία φορά το έτος),
   - θα υπάρχουν σαφείς στόχοι εκ των προτέρων, είτε για τον έλεγχο συγκεκριμένων υποσυστημάτων, είτε για τον έλεγχο του συστήματος συνολικά. Η εκτέλεση δοκιμών της τελευταίας κατηγορίας συνιστάται να περιλαμβάνει την πλήρη κάλυψη όλων των κρίσιμων λειτουργιών όπως αναγράφονται στο σχέδιο,
   - θα διεξάγονται υπό συνθήκες που θα προσομοιώνουν περιπτώσεις έκτακτης ανάγκης,
   - θα εξασφαλίζεται η συμμετοχή του Υπεύθυνου Ασφάλειας Ψηφιακών Συστημάτων και της ομάδας υποστήριξής του,
   - θα συντάσσεται έκθεση αποτελεσμάτων μετά την ολοκλήρωσή των δοκιμών,
   - θα γίνονται οι απαραίτητες διορθώσεις στα σχέδια για όλα τα προβλήματα που διαπιστώνονται,
   - θα λαμβάνει γνώση των αποτελεσμάτων η Διοίκηση.

Οι αρχικές προσπάθειες, μετά την εκδήλωση του περιστατικού ασφάλειας, πρέπει να κατευθυνθούν προς την προστασία και διατήρηση των εξαρτημάτων του δικτύου. Ιδιαίτερα πρέπει να ληφθεί μέριμνα ώστε όλα τα μαγνητικά αποθηκευτικά μέσα (σκληροί δίσκοι, μαγνητικές ταινίες, δισκέτες, CD-ROMs, κ.α.) αφού πρώτα αναγνωρισθούν, να προστατευθούν ή ακόμη και να απομακρυνθούν από την τοποθεσία που έχει πληγεί από το περιστατικό σε νέο απομακρυσμένο χώρο.

Η ολοκλήρωση των προσπαθειών για τη διάσωση των πληγέντων χώρων, καθώς και τον καθορισμό των εγκαταστάσεων αποκατάστασης, ακολουθεί η διόρθωση των βλαβών και της δικτυακής υποδομής είτε από το προσωπικό του φορέα, αν αυτό είναι εφικτό, είτε από το ειδικευμένο προσωπικό του κατασκευαστή – προμηθευτή. Περιλαμβάνει τη πλήρη περιγραφή των εξαρτημάτων/ υπολογιστών/ εξυπηρετητών μαζί με το λογισμικό τους, των οποίων πρέπει να αποκατασταθεί η λειτουργία μετά από ένα περιστατικό.

Η διαδικασία αποκατάστασης στηρίζεται στην προϋπόθεση ότι ο προμηθευτής θα έχει την δυνατότητα να αντικαταστήσει άμεσα τα μηχανήματα και τα εξαρτήματα που δεν δύνανται να διασωθούν. Λαμβανομένου υπόψη ότι το παρόν σχέδιο εστιάζει

στη συνέχιση επιχειρησιακής λειτουργίας, πρέπει να είναι δεδομένη η άμεση ανταπόκριση του προμηθευτή σε μηχανήματα και συσκευές που πιθανόν θα απαιτηθούν για το σκοπό αυτό. Για το λόγο αυτό απαιτείται η σύνδεση του παρόντος Σχεδίου Συνέχισης Λειτουργίας με το εκάστοτε σε ισχύ συμβόλαιο συντήρησης του εξοπλισμού του φορέα.

Για να αποφευχθούν προβλήματα και καθυστερήσεις στην αποκατάσταση των ψηφιακών συστημάτων, κάθε προσπάθεια πρέπει να γίνει με σκοπό την επαναφορά τους στην προ της καταστροφής λειτουργική κατάστασή τους. Ωστόσο, είναι πολύ πιθανόν να υπάρξουν περιπτώσεις που συγκεκριμένα εξαρτήματα δεν θα είναι διαθέσιμα ή που ο χρόνος για την προμήθειά τους είναι απαγορευτικά μεγάλος. Η Μονάδα Πληροφορικής θα πρέπει να έχει την απαραίτητη εμπειρία για να αντιμετωπίζει αυτά τα προβλήματα όποτε εμφανιστούν. Αν και η χρησιμοποίηση εξαρτημάτων διαφορετικών από τα προϋπάρχοντα, πιθανόν να απαιτήσει την παρέκκλιση από τις προβλεπόμενες διαδικασίες και ενέργειες, εν τούτοις μπορεί να είναι σκόπιμη η ακόμη και απαραίτητη για την συνέχιση του σχεδίου.

Οι αναπόφευκτες αλλαγές που θα συμβαίνουν στα ψηφιακά συστήματα με τη πάροδο του χρόνου λειτουργίας τους, απαιτούν τη περιοδική αναθεώρηση του ΣΣΛ ώστε ανά πάσα στιγμή να ανταποκρίνεται στη πραγματική κατάσταση. Όπου αυτό είναι δυνατόν, πρέπει να συνάπτονται συμφωνίες με τους προμηθευτές που να περιγράφονται οι διαδικασίες επείγοντος εφοδιασμού με τον απαραίτητο εξοπλισμό.

4.5. Μελέτη Περίπτωσης

1. Σχεδιάστε μία Διαδικασία Αντιμετώπισης Περιστατικών Παραβίασης Ασφάλειας (Security Incident Management Procedure).

2. Σχεδιάστε μία Διαδικασία Ελεγχόμενης Πρόσβασης στο Ολοκληρωμένο Πληροφοριακό Σύστημα (ΟΠΣ) ενός φορέα της Δημόσιας Διοίκησης.

3. Σχεδιάστε τον κανονισμό ορθής πλοήγησης στο Διαδίκτυο.

4. Σχεδιάστε τον κανονισμό ορθής χρήσης του Ηλεκτρονικού Ταχυδρομείου.

5. Σχεδιάστε τη διαδικασία Καθαρής Επιφάνειας Εργασίας (Clean Desk Policy).

4.6. Βιβλιογραφία

- Network Security Essentials: Applications and Standards (6th Edition), by William Stallings, Pearson Education Limited, 2017.
- Διαχείριση της ασφάλειας πληροφοριών, Σ. Κάτσικας, Εκδόσεις Πολιτεία, 2015, ISBN 9789605464158
- Γκρίτζαλης Σ., Κάτσικας Σ., Γκρίτζαλης Δ., Ασφάλεια Δικτύων Υπολογιστών, Παπασωτηρίου, Αθήνα 2003.
- Κάτσικας Σ., Γκρίτζαλης Δ., Γκρίτζαλης Σ. (επ. επιμ.), Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, Αθήνα 2004.
- Peltier T., Information Security Policies and Procedures, CRC Press, 1999.

5. ΝΟΜΙΚΑ ΘΕΜΑΤΑ

5.1. Ασφάλεια Πληροφοριακών Συστημάτων, Δικτύων και Δεδομένων

Με το Νόμο 4577/2018 (ΦΕΚ Α' 199/3-12-2018) ενσωματώθηκε στην ελληνική νομοθεσία η Οδηγία 2016/1148/ΕΕ (Network and Information Security – NIS) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με την οποία, θεσπίζονται μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών.

Η Οδηγία προτείνει ένα ευρύ φάσμα μέτρων για την ενίσχυση του επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών για την εξασφάλιση υπηρεσιών που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία της Ευρωπαϊκής Ένωσης. Στόχος της είναι να εξασφαλίσει ότι οι χώρες της Ε.Ε. είναι καλά προετοιμασμένες και έτοιμες να χειριστούν και να αντιμετωπίσουν επιθέσεις στον κυβερνοχώρο μέσω:

- του διορισμού αρμόδιων αρχών,
- της δημιουργίας ομάδων απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT)[1] και
- της υιοθέτησης εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο.

Η Οδηγία καθορίζει επίσης τη συνεργασία σε επίπεδο Ε.Ε. τόσο σε στρατηγικό όσο και σε τεχνικό επίπεδο.

Ακόμα, εισάγει την υποχρέωση των παρόχων βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών να λαμβάνουν τα κατάλληλα μέτρα ασφαλείας και να ενημερώνουν τις αρμόδιες εθνικές αρχές σχετικά με σοβαρά συμβάντα.

Ένα από τα βασικά σημεία της Οδηγίας αποτελεί η βελτίωση των εθνικών δυνατοτήτων για την ασφάλεια στον κυβερνοχώρο. Οι χώρες της Ε.Ε., μεταξύ αυτών και η Χώρα μας είναι υποχρεωμένες:

[1] Οι CSIRT, γενικά, είναι υπεύθυνες μεταξύ άλλων για: (α) την παρακολούθηση και την αντιμετώπιση συμβάντων ασφαλείας στον κυβερνοχώρο, (β) την παροχή ανάλυσης κινδύνων και συμβάντων και την επίγνωση της κατάστασης, (γ) τη συμμετοχή στο δίκτυο CSIRT, (δ) τη συνεργασία με τον ιδιωτικό τομέα και (ε) την προώθηση της χρήσης τυποποιημένων πρακτικών για τον χειρισμό συμβάντων και κινδύνων και την ταξινόμηση πληροφοριών.

- να ορίζουν μία ή περισσότερες εθνικές αρμόδιες αρχές και CSIRT και να προσδιορίζουν ένα ενιαίο κέντρο επαφής [Εθνική Αρχή Κυβερνοασφάλειας] (σε περίπτωση που υπάρχουν περισσότερες από μία αρμόδιες αρχές),

- να προσδιορίζουν τους παρόχους βασικών υπηρεσιών σε σημαντικούς τομείς, όπως η ενέργεια, οι μεταφορές, η χρηματοδότηση, οι τράπεζες, η υγεία, η ύδρευση και η ψηφιακή υποδομή, στους οποίους μια επίθεση στον κυβερνοχώρο θα μπορούσε να διαταράξει μια βασική υπηρεσία.

Κάθε χώρα της Ε.Ε. οφείλει επίσης να θέσει σε εφαρμογή μια εθνική στρατηγική ασφάλειας του κυβερνοχώρου για τα συστήματα δικτύου και πληροφοριών, που να καλύπτει τα ακόλουθα θέματα:

- την προετοιμασία και την ετοιμότητα να χειρίζονται και να αντιμετωπίζουν επιθέσεις στον κυβερνοχώρο,

- τους ρόλους, τις ευθύνες και τη συνεργασία της κυβέρνησης και άλλων μερών,

- προγράμματα εκπαίδευσης, ευαισθητοποίησης και κατάρτισης,

- την έρευνα και τον σχεδιασμό ανάπτυξης,

- τον σχεδιασμό για τον προσδιορισμό κινδύνων.

Ως ασφάλεια στον κυβερνοχώρο, δε, ορίζεται η ικανότητα των συστημάτων δικτύου και πληροφοριών[2] να ανθίστανται σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των ψηφιακών δεδομένων και των υπηρεσιών που παρέχουν αυτά τα συστήματα.

5.1.1. Εθνική Αρχή Κυβερνοασφάλειας

Με το Ν. 4577/2018 ορίσθηκε για την Ελλάδα ως Εθνικής Αρχής Κυβερνοασφάλειας η Διεύθυνση Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης,

[2] Σύστημα δικτύου και πληροφοριών: ένα δίκτυο ηλεκτρονικών επικοινωνιών ή οποιαδήποτε συσκευή ή ομάδα διασυνδεδεμένων συσκευών που επεξεργάζονται ψηφιακά δεδομένα, καθώς και τα ψηφιακά δεδομένα που έχουν αποθηκευτεί, υποστεί επεξεργασία, ανακτηθεί ή μεταδοθεί.

Τηλεπικοινωνιών & Ενημέρωσης. Η Αρχή αυτή, ως φορέας υψηλού πολιτικού - κυβερνητικού επιπέδου με εξειδικευμένα στελέχη, παρακολουθεί και υλοποιεί τις δράσεις της Εθνικής Στρατηγικής Κυβερνοασφάλειας.

Είναι επίσης, αρμόδια για τον συντονισμό μεταξύ των φορέων που δραστηριοποιούνται στην Ελλάδα στον τομέα της ασφάλειας στον κυβερνοχώρο, τόσο στο δημόσιο [Διεύθυνση Κυβερνοχώρου (ΕΥΠ) – Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT, Διεύθυνση Κυβερνοάμυνας (ΓΕΕΘΑ), Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), Κέντρο Μελετών Ασφαλείας] όσο και στον ιδιωτικό τομέα.

5.1.2. Εθνική Στρατηγική Κυβερνοασφάλειας

Η προαναφερθείσα Εθνική Στρατηγική Κυβερνοασφάλειας, που εγκρίθηκε το Μάρτιο του 2018[3], αποτελεί τον επιτελικό σχεδιασμό της Ελληνικής Πολιτείας για την ασφάλεια στον κυβερνοχώρο. Η σημασία της είναι κρίσιμη με δεδομένη την ολοένα αυξανόμενη χρήση του Διαδικτύου και των Τεχνολογιών Πληροφορικής και Επικοινωνιών σε κάθε πτυχή των δραστηριοτήτων του δημόσιου και του ιδιωτικού τομέα. Στόχος, βεβαίως, είναι η δημιουργία ενός ασφαλούς περιβάλλοντος Διαδικτύου, υποδομών και υπηρεσιών, που θα τονώσει την εμπιστοσύνη των πολιτών και θα τους οδηγήσει στην περαιτέρω χρήση νέων ψηφιακών προϊόντων και υπηρεσιών και στην τόνωσης της οικονομικής ανάπτυξης της Χώρας.

Μεταξύ άλλων, στην Εθνική Στρατηγική Κυβερνοασφάλειας περιλαμβάνονται τα εξής:

- πλαίσιο διακυβέρνησης για την επίτευξη των στόχων και των προτεραιοτήτων της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύων και πληροφοριών, συμπεριλαμβανομένων του ρόλου και των αρμοδιοτήτων των κυβερνητικών οργάνων και των λοιπών αρμόδιων φορέων,
- μέτρα ετοιμότητας, απόκρισης και αποκατάστασης, συμπεριλαμβανομένης της συνεργασίας ανάμεσα στο δημόσιο και ιδιωτικό τομέα,
- αναφορά σε προγράμματα εκπαίδευσης, ευαισθητοποίησης και κατάρτισης σε σχέση με την εθνική στρατηγική ασφάλειας δικτύων και συστημάτων πληροφοριών,

[3] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGR.pdf/

- αναφορά στα σχέδια έρευνας και ανάπτυξης σχετικά με την εθνική στρατηγική ασφάλειας συστημάτων δικτύου και πληροφοριών,
- σχέδιο εκτίμησης κινδύνου για τον προσδιορισμό κινδύνων,
- κατάλογος των διαφόρων φορέων που εμπλέκονται στην υλοποίηση της εθνικής στρατηγικής ασφάλειας συστημάτων δικτύου και πληροφοριών.

5.1.3. CSIRT

Ως «Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team – CSIRT)», ορίζεται η Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ). Η ΔΙ.ΚΥΒ. καλύπτει τομείς όπως η ενέργεια, οι μεταφορές, οι τράπεζες, οι υποδομές χρηματοπιστωτικών αγορών, η υγεία, η προμήθεια και διανομή πόσιμου νερού και η ψηφιακή υποδομή, καθώς και υπηρεσίες όπως οι online αγορές, οι online μηχανές αναζήτησης και οι υπηρεσίες cloud (νεφοϋπολογιστική), και είναι υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας.

5.2. Επιθέσεις κατά Συστημάτων Πληροφοριών

Με το Νόμο 4411/2016 (ΦΕΚ 142–Α΄/3-8-2016), η Ελλάδα προέβη στην Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών[4], καθώς και στην ενσωμάτωση της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών (και την αντικατάσταση της απόφασης πλαισίου 2005/222/ΔΕΥ του Συμβουλίου)[5].

Παρόλο που η κύρωση της Σύμβασης και η ενσωμάτωσή της στο εσωτερικό δίκαιο της Χώρας μας, έγινε με μεγάλη καθυστέρηση, ρυθμίζει σειρά κακόβουλων πράξεων που σήμερα ευνοούνται από τη ραγδαία εξέλιξη της τεχνολογίας της πληροφορικής και των ηλεκτρονικών υπολογιστών και την υιοθέτησή τους από εγκληματίες για τη διάπραξη τέτοιων εγκλημάτων.

[4] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[5] https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:32013L0040

5.2.1. Αλλαγές στο Ουσιαστικό Ποινικό Δίκαιο

Το δεύτερο άρθρο του Νόμου 4411/2016, περιλαμβάνει διατάξεις του Ουσιαστικού Ποινικού Δικαίου, που θεσπίστηκαν εξ αρχής ή τροποποιήθηκαν για να εναρμονιστεί η ελληνική νομοθεσία με τη Σύμβαση και ειδικότερα:

Στο άρθρο 13 του Ποινικού Κώδικα (Π.Κ.), εισήχθησαν δύο νέοι ορισμοί και συγκεκριμένα στα εδάφια η΄ και θ΄ εισάγονται οι έννοιες του Πληροφοριακού Συστήματος και των Ψηφιακών Δεδομένων. Οι ορισμοί αυτοί περιλαμβάνονται στο σύνολο του κειμένου της Σύμβασης και στην Οδηγία και είναι απαραίτητοι τόσο για την ερμηνεία των νέων διατάξεων που είτε εισάγονται στο Ποινικό μας Δίκαιο, όσο και αυτών που τροποποιούνται με το Νόμο 4411/2016. Σύμφωνα με τη νέα νομική ορολογία, α) Πληροφοριακό Σύστημα, νοείται οποιαδήποτε συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, από τις οποίες μία ή περισσότερες εκτελούν αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, επεξεργάζονται ή διαβιβάζονται από τη συσκευή με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών και β) Ψηφιακά Δεδομένα νοούνται γεγονότα και πληροφορίες που μπορούν να επεξεργαστούν από πληροφοριακό σύστημα ή πρόγραμμα που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία.

Για την αποτελεσματικότερη προστασία και την ποινική αντιμετώπιση ζητημάτων που αφορούν την δόλια παρακώληση λειτουργίας Πληροφοριακών Συστημάτων, προστέθηκε στον Ποινικό Κώδικα το άρθρο 292Β.

Με το άρθρο αυτό η ελληνική νομοθεσία εναρμονίζεται με τις διατάξεις που περιέχονται στα άρθρα 5 της Σύμβασης και 4 της Οδηγίας, επιδιώκοντας την προσαρμογή της ποινικής προστασίας με την αντίστοιχη ποινική πρόβλεψη για επιθέσεις που εκδηλώνονται κατά συστημάτων τηλεφωνικών επικοινωνιών (άρθρο 292Α Π.Κ.), με γνώμονα την τήρηση της αρχής της αναλογικότητας ως προς το είδος και την ένταση της. Δηλαδή προβλέπονται αυστηρότερες ποινές όταν η κακόβουλη πράξη προκαλεί σημαντική ζημιά σε πληροφοριακά συστήματα με τη χρήση ειδικών για το σκοπό αυτό εργαλείων ή τελείται οργανωμένα από εγκληματική οργάνωση, όπως αυτή ορίζεται στο άρθρο 187 Π.Κ. ή προκαλεί ιδιαίτερα μεγάλη ζημιά ή πλήττει πληροφοριακά συστήματα υποδομής που παρέχουν σημαντικές, ζωτικές υπηρεσίες για την κοινωνία και το Κράτος. Η διάταξη αυτή περιλαμβάνει, προστατεύει και τιμωρεί, αναλογικά (ειδικά και αυστηρότερα), τις επιθέσεις κατά κρατικών πληροφοριακών συστημάτων και κρίσιμων υποδομών της Χώρας που χρησιμοποιούνται ευρύτερα από την κοινωνία και το Κράτος.

Για την εναρμόνιση της ελληνικής νομοθεσίας με το άρθρο 7 της Οδηγίας, προστέθηκε στον Ποινικό Κώδικα το άρθρο 292Γ, με το οποίο νομοθετήθηκε για πρώτη φορά στη Χώρα μας το αξιόποινο προπαρασκευαστικών πράξεων για τη διάπραξη των σχετικών με το άρθρο 292Β αδικημάτων, ανεξαρτήτως αν αυτά τελικά διαπράχθηκαν. Δηλαδή ποινικοποιούνται αυτοτελώς προπαρασκευαστικές ενέργειες και συμπεριφορές που στοχεύουν στην τέλεση των εγκλημάτων που

περιλαμβάνονται στο άρθρο 292Β, όπως η παραγωγή, η πώληση, η εισαγωγή, η κατοχή ή με οποιονδήποτε τρόπο διευκόλυνση αυτών με τη διανομή προγραμμάτων υπολογιστών ή συσκευών. Για τη διασφάλιση και την αποφυγή ποινικοποίησης της επιστημονικής έρευνας, προβλέπεται η τιμωρία της παραγωγής και διάθεσης των σχετικών εργαλείων, υπό την απαραίτητη προϋπόθεση να υπάρχει πρόθεση χρήσης τους για τη διάπραξη σχετικού εγκλήματος.

Για την περεταίρω προστασία των ανηλίκων τροποποιήθηκαν οι διατάξεις περί πορνογραφίας ανηλίκων και ειδικότερα το άρθρο 348Α του Ποινικού Κώδικα, το οποίο σημειωτέων είχε ήδη τροποποιηθεί στη Χώρα μας με το Νόμο 4267/2014, εναρμονίζοντας την ελληνική νομοθεσία με την Οδηγία 2011/93/ΕΕ[6]. Με τη νέα τροποποίηση εισάγεται στις παραγράφους 2 και 5 ο όρος του Πληροφοριακού Συστήματος, όπως ορίζεται στο άρθρο 13 Π.Κ., για να επιτευχθεί ορολογική ομοιογένεια στις διατάξεις του Ποινικού Κώδικα. Επίσης ποινικοποιείται περεταίρω η διαδικτυακή διακίνηση αθέμιτου περιεχομένου, αποσκοπώντας στην προστασία των ανηλίκων από την σεξουαλική κακοποίηση, την σεξουαλική εκμετάλλευση και την προστασία της πνευματικής και της ηθικής τους ανάπτυξης, την προστασία των χρηστών ηθών και της ανθρώπινης αξιοπρέπειας. Οι πράξεις που τιμωρούνται αφορούν τη διακίνηση, τη διάδοση, την προμήθεια του υλικού πορνογραφίας ανηλίκων και τη δημοσίευσή του, μέσω του διαδικτύου.

Για την επίτευξη ορολογικής ομοιογένειας στις διατάξεις του Ποινικού Κώδικα και της απαιτούμενης εννοιολογικής προσέγγισης από τους νομικούς, τροποποιήθηκε και το άρθρο 348Β του Ποινικού Κώδικα, «Προσέλκυση παιδιών για γενετήσιους λόγους», το οποίο συμπληρώθηκε με τον όρο «Πληροφοριακά Συστήματα».

Επίσης τροποποιήθηκε η δεύτερη παράγραφος του άρθρου 370Γ Π.Κ. «Παράνομη πρόσβαση σε πληροφοριακό σύστημα». Η αναδιατυπωμένη διάταξη προβλέπει και τιμωρεί την χωρίς δικαίωμα πρόσβαση σε Πληροφοριακό Σύστημα ή τμήμα αυτού. Ο όρος «πρόσβαση» περιλαμβάνει τη «χωρίς εξουσιοδότηση είσοδο» σε ολόκληρο τον ηλεκτρονικό υπολογιστή ή σε μέρος αυτού, (όπως π.χ. σε επιμέρους αρχεία και φακέλους). Δεν περιλαμβάνει όμως τη χωρίς δικαίωμα αποστολή ηλεκτρονικών μηνυμάτων ή φακέλων. Για τη θεμελίωση της υποκειμενικής υπόστασης απαιτείται πρόθεση, όπως αυτή προσδιορίζεται σύμφωνα με το εσωτερικό δίκαιο κάθε Κράτους Μέλους. Οι περισσότερες νομοθεσίες των Κρατών Μελών του Συμβουλίου της Ευρώπης, περιλαμβάνουν διατάξεις σχετικές με την παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή. Με τη διάταξη αυτή ουσιαστικά ποινικοποιείται το γνωστό κατά στη γλώσσα των δραστών «computer hacking». Ο δικαιολογητικός λόγος ποινικοποίησης της παράνομης πρόσβασης συνίσταται στο γεγονός ότι ο κάθε κάτοχος ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος τα άτομα που μπορούν να έχουν πρόσβαση ή εξουσία χρήσης του υπολογιστή ή του

[6] Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 2011 σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου.

συστήματος υπολογιστή, καθώς επίσης και να ορίζει εξατομικευμένα τα δικαιώματα πρόσβασης και διαχείρισης των δεδομένων που περιλαμβάνει και τιμωρεί, σε βαθμό Πλημμελήματος, κάθε υπαίτια παράβαση των απαγορεύσεων ή των μέτρων ασφαλείας που έχει λάβει ο νόμιμος κάτοχός τους. Εφόσον ο χρήστης έχει την ιδιότητα του υπαλλήλου σε σχέση με τον κάτοχο, η πράξεις αυτές τιμωρούνται μόνο εφόσον προβλέπονται ρητά από εσωτερικό κανονισμό ή μέτρα ασφαλείας που έχει λάβει αρμόδιος για το σκοπό αυτό υπάλληλος ή ο κάτοχος του υπολογιστή ή του συστήματος υπολογιστών.

Προστέθηκε νέα διάταξη και συγκεκριμένα το άρθρο 370Δ Π.Κ., με το οποίο ποινικοποιείται και τιμωρείται αυτοτελώς η παραβίαση του απορρήτου των επικοινωνιών με τη χρήση τεχνικών μέσων και πληροφοριακών συστημάτων, καθώς και η χρήση από τον ίδιο ή η διαβίβαση των πληροφοριών αυτών σε τρίτα πρόσωπα, με ποινές αντίστοιχες της παραβίασης του απορρήτου των τηλεφωνικών επικοινωνιών που προβλέπονται στη διάταξη του άρθρου 370Α Π.Κ. (κάθειρξη μέχρι δέκα χρόνια). Σε περίπτωση που οι πράξεις αυτές έχουν ως αποτέλεσμα την παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους σε καιρό πολέμου, τιμωρούνται σε βαθμό κακουργήματος, με τις προβλεπόμενες στο άρθρο 146 Π.Κ. ποινές «Παραβίαση Μυστικών της Πολιτείας». Με τη διάταξη αυτή ποινικοποιείται περεταίρω η ακρόαση και ο έλεγχος του περιεχομένου των επικοινωνιών και παροχή του περιεχομένου των δεδομένων είτε άμεσα, με πρόσβαση και χρήση των συστημάτων πληροφοριών, είτε έμμεσα με τη χρήση ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα. Σχετικά ποινικά αδικήματα προβλέπονται στα άρθρα 292Α, 370Α, 370Β και 370Γ ΠΚ, στο άρθρο 15 του Ν. 3471/2006 για πράξεις αφαίρεσης, αλλοίωσης, καταστροφή δεδομένων συνδρομητών ή χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών, στα άρθρα 22 § 4 Ν 2472/1997 και 4 και 15 Ν 3471/2006 αναφορικά με δεδομένα προσωπικού χαρακτήρα, στο άρθρο 10 του Ν. 3115/2003 για την παραβίαση του απορρήτου των επικοινωνιών.

Προστέθηκε νέα διάταξη και συγκεκριμένα το άρθρο 370Ε Π.Κ., με το οποίο ποινικοποιείται και τιμωρείται αυτοτελώς η εισαγωγή, η διανομή, η κατοχή, ο σχεδιασμός και η με οποιοδήποτε τρόπο διάθεση μηχανογραφικών εφαρμογών και προγραμμάτων λογισμικού, συσκευών ή τεχνικών μέσων, με τα οποία ευνοείται και καθίσταται δυνατή η δόλια πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος, με σκοπό τη διάπραξη εγκλημάτων που περιλαμβάνονται στις διατάξεις των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ του Π.Κ..

Επίσης, προστέθηκε στον Ποινικό Κώδικα το άρθρο 381Α Π.Κ., για την εναρμόνιση της ελληνικής νομοθεσίας με το άρθρο 4 της Σύμβασης και το άρθρο 5 της Οδηγίας. Περιλαμβάνει διατάξεις που εξειδικεύουν το αντικείμενο της φθοράς των Ψηφιακών Δεδομένων ενός Συστήματος Πληροφοριών και ποινικοποιούν ειδικά την με δόλο και χωρίς δικαίωμα «Φθορά Ηλεκτρονικών Δεδομένων». Με την προσθήκη του άρθρου αυτού καλύπτεται και συμπληρώνεται η ελληνική νομοθεσία, ως προς την αυτοτελή

προστασία των Ψηφιακών Δεδομένων, από πράξεις καταστροφής, απόκρυψης ή ανέφικτης χρήσης τους, διαγραφής ή αλλοίωσής τους.

Έτσι, τα Ψηφιακά Δεδομένα προστατεύονται αυτοτελώς και όχι αυτοματοποιημένα με βάση το βαθμό και την έκταση που πλήττεται ο υλικός τους φορέας (σκληρός δίσκος, εξωτερική φορητή μνήμη κ.λπ.). Στις παραγράφους 2 και 3 του εν λόγω άρθρου προβλέπονται διακεκριμένες παραλλαγές σύμφωνα με τις ρυθμίσεις της Οδηγίας και ειδικότερα προβλέπονται και τιμωρούνται βαρύτερα οι επιθέσεις που έγιναν με τη χρήση ειδικού για το σκοπό αυτό εργαλείου ή στρέφονται κατά μεγάλου αριθμού Πληροφοριακών Συστημάτων ή προκαλούν ζημιές ευρείας έντασης και έκτασης ή τελέστηκαν κατά Πληροφοριακών Συστημάτων που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες, όπως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια ή τελέστηκαν από δομημένη και με διαρκή δράση ομάδα τριών ή περισσότερων προσώπων, που επιδιώκουν την τέλεση τέτοιων εγκλημάτων μαζικά. Τα παραπάνω διώκονται σε βαθμό Πλημμελήματος γενόμενης μνείας ότι τα αναφερόμενα στην πρώτη παράγραφο διώκονται εφόσον υποβληθεί έγκληση κατά κανόνα του παθόντος, ενώ τα αναφερόμενα στις παραγράφους δύο και τρία αυτεπαγγέλτως. Με τη διάταξη αυτή ποινικοποιούνται οι επιθέσεις κατά πληροφοριακών συστημάτων με ιομορφικό λογισμικό, πράξεις που πριν την ψήφιση του Νόμου αντιμετωπίζονταν ποινικά ως φθορά ξένης ιδιοκτησίας, άρθρο 381 Π.Κ..

Προστέθηκε το άρθρο 381Β Π.Κ., για την ενσωμάτωση στην ελληνική νομοθεσία των διατάξεων του άρθρου 7 της Οδηγίας. Στο νέο άρθρο περιλαμβάνονται διατάξεις που ποινικοποιούν την ευθύνη των προσώπων που δρουν με σκοπό την τέλεση αξιόποινων πράξεων, κυρίως αυτών που προβλέπονται στο άρθρο 381Α Π.Κ. και αφορούν την αγορά, την πώληση, την προμήθεια, την κατοχή και διακίνησης συσκευών και προγραμμάτων υπολογιστών και των συνθηματικών ή κωδικών εισόδου, προκειμένου αυτά να χρησιμοποιηθούν με δόλο για την επίτευξη παράνομης πρόσβασης σε μέρος ή στο σύνολο ενός Πληροφοριακού Συστήματος.

Τροποποιήθηκε το άρθρο 386Α Π.Κ. (Απάτη με Υπολογιστή), κατά τα οριζόμενα στο άρθρο 8 της Σύμβασης. Η τροποποιημένη διάταξη διαφοροποιεί την κλασική – συμβατική Απάτη από την Απάτη με Υπολογιστή, η οποία πλέον ποινικοποιεί την χωρίς δικαίωμα χρήση ψηφιακών δεδομένων και στοιχείων άλλου προσώπου, όπως π.χ. η δόλια χρήση από το δράστη του παράνομα αποκτηθέντος ονόματος διαδικτυακού χρήστη και του κωδικού χρήσης υπηρεσιών διαδικτύου του δικαιούχου. Το νέο στοιχείο που εισάγεται στην Απάτη με Υπολογιστή και τη διαχωρίζει από την απλή είναι ότι ο δράστης για να προσπορίσει στον εαυτό του ή άλλον παράνομο περιουσιακό όφελος, επηρεάζει το αποτέλεσμα μιας διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή, είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων, είτε με τη χωρίς δικαίωμα χρήση δεδομένων, είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα. Η περιουσιακή βλάβη υφίσταται ακόμα και στην περίπτωση που τα πρόσωπα που την υπέστησαν είναι άδηλα ή στρέφονται κατά μεγάλου ή

αορίστου αριθμού ατόμων, ενώ για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα. Ως προς τις ποινές η πράξη αντιμετωπίζεται και τιμωρείται σύμφωνα με τα προβλεπόμενα στο Άρθρο 386 Π.Κ..

5.2.2. Άρση Απορρήτου σε Περιπτώσεις Κυβερνοεγκλημάτων

Στις ηλεκτρονικές επικοινωνίες, σύμφωνα με τη νομοθεσία, απόρρητα θεωρούνται:

- Το περιεχόμενο της επικοινωνίας (περιεχόμενο τηλεφωνικών κλήσεων, ηλεκτρονικού ταχυδρομείου και γενικά οποιασδήποτε επικοινωνίας φωνής, εικόνας, δεδομένων).
- Η ταυτότητα του καλούντος και του καλουμένου.
- Η ταυτότητα του αποστολέα και του παραλήπτη ηλεκτρονικού ταχυδρομείου.
- Τα δεδομένα θέσης της τερματικής συσκευής (γεωγραφικός εντοπισμός).

Οι πάροχοι ηλεκτρονικών επικοινωνιών είναι υπεύθυνοι να λαμβάνουν όλα τα αναγκαία μέτρα για τη διασφάλιση του απορρήτου των επικοινωνιών τους στο δημόσιο τηλεπικοινωνιακό δίκτυο τους (δίκτυα κορμού και πρόσβασης). Οι συνδρομητές και οι χρήστες οφείλουν να μεριμνούν για το απόρρητο της επικοινωνίας στα ιδιωτικά δίκτυα τα οποία περιλαμβάνουν τις διατάξεις μεταγωγής (αν υπάρχουν) όπως και τις καλωδιώσεις στα κτίρια, τα εσωτερικά δίκτυα (LAN) και τις τερματικές συσκευές (σταθερά ενσύρματα και ασύρματα τηλέφωνα, κινητά τηλέφωνα, fax, προσωπικοί υπολογιστές).

Φορείς του δικαιώματος του άρθρου 19 του Συντάγματος είναι όλα τα φυσικά πρόσωπα, ανεξαρτήτως ιθαγένειας και εθνικότητας και ανεξαρτήτως εάν πρόκειται για επικοινωνία εντός της χώρας ή με το εξωτερικό. Φορείς του ως άνω δικαιώματος είναι επίσης όλα τα νομικά πρόσωπα ιδιωτικού δικαίου καθώς και τα νομικά πρόσωπα δημοσίου δικαίου στο βαθμό που είναι φορείς συνταγματικών δικαιωμάτων. Σχετικά με τα νομικά πρόσωπα ιδιωτικού δικαίου (π.χ. επιχειρήσεις), η προστασία του απορρήτου της επικοινωνίας συνδέεται με τη διασφάλιση και άλλων δικαιωμάτων, όπως είναι για παράδειγμα η ελεύθερη επιχειρηματική δράση τους.

Αποδέκτες του δικαιώματος είναι τόσο τα όργανα της κρατικής εξουσίας, όσο και οι ιδιώτες, φυσικά ή νομικά πρόσωπα όπως για παράδειγμα εταιρίες σταθερής ή κινητής τηλεφωνίας κ.λπ.. Αντικείμενο της προστασίας του απορρήτου θεωρείται η ελευθερία της επικοινωνίας και το απόρρητο όλων των μορφών επικοινωνίας.

Νομοθετικές ρυθμίσεις που αφορούν στο απόρρητο των ηλεκτρονικών επικοινωνιών

Καταρχήν το απόρρητο των επικοινωνιών προστατεύεται από το άρθρο 19 του Συντάγματος, με το οποίο προβλέφθηκε και η σύσταση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Σε νομοθετικό επίπεδο σχετικές με το απόρρητο των επικοινωνιών είναι οι ρυθμίσεις του Ν. 2225/1994 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας, οι διατάξεις του Ν. 3115/2003, με τον οποίο συστάθηκε η ΑΔΑΕ, του Ν. 3471/2006, όπως τροποποιήθηκε και ισχύει, με το οποίο ρυθμίζονται θέματα προστασίας δεδομένων προσωπικών χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και οι διατάξεις του Ν. 3674/2008 σχετικά με τη διασφάλιση του απορρήτου της τηλεφωνικής επικοινωνίας. Σχετικά είναι και τα οριζόμενα στις διατάξεις του Ν. 4070/2012, η απόφαση υπ' αριθμ. 99/2017 (ΦΕΚ 4073/Β'/23.11.2017), ο Ν. 4411/2016, καθώς και ο Ν. 4055/2012.

Άρση του απορρήτου των επικοινωνιών

Η άρση του απορρήτου των επικοινωνιών είναι μια κατ' εξαίρεση επιτρεπόμενη διαδικασία, βάσει της οποίας τα στοιχεία της επικοινωνίας, τα οποία είναι καταρχήν απόρρητα, καθίστανται γνωστά σε συγκεκριμένες Αρχές και για συγκεκριμένους λόγους.

Σύμφωνα με τη διάταξη του άρθρου 19 παρ. 1 του Συντάγματος, η άρση αυτή είναι δυνατόν να ισχύσει για τη δικαστική αρχή και όχι έναντι της διοίκησης για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Οι προαναφερθέντες λόγοι εξειδικεύονται με τις διατάξεις του ν. 2225/1994, όπως ισχύει, ο οποίος περιλαμβάνει και κατάλογο των εγκλημάτων για τη διακρίβωση των οποίων μπορεί να διαταχθεί με διάταξη του αρμόδιου δικαστικού συμβουλίου η άρση του απορρήτου.

Τις διαδικασίες, τις τεχνικές και τις οργανωτικές ρυθμίσεις για την άρση του απορρήτου των επικοινωνιών προβλέπουν, εξειδικεύοντας τη διάταξη του άρθρου 19 του Συντάγματος, οι διατάξεις του ν. 2225/1994 και του ΠΔ 47/2005, όπως ισχύουν.

Ειδικότερα ο ν. 2225/1994, όπως ισχύει, προβλέπει τους λόγους για τους οποίους η άρση του απορρήτου επιτρέπεται, τα όργανα που μπορούν να τη διατάξουν, τα χρονικά όρια εντός των οποίων μπορεί η άρση να πραγματώνεται, καθώς και τη διαδικασία που πρέπει να ακολουθείται σε κάθε περίπτωση.

Το ΠΔ 47/2005, όπως ισχύει, προβλέπει τα είδη αλλά και τα επιμέρους στοιχεία της επικοινωνίας, τα οποία μπορεί να αφορά η άρση του απορρήτου. Προβλέπει επίσης τα μέσα και τις μεθόδους πραγμάτωσης της άρσης, καθώς και τις σχετικές υποχρεώσεις των παρόχων υπηρεσιών και δικτύων επικοινωνίας.

Η ΑΔΑΕ παραλαμβάνει τις διατάξεις του αρμόδιου δικαστικού συμβουλίου που επιβάλλουν την άρση του απορρήτου και ελέγχει την τήρηση των όρων και της διαδικασίας.

5.2.3. Κυβερνοέγκλημα, Κυβερνοεπιθέσεις και Δίκτυο 24/7

Τόσο στη Σύμβαση της Βουδαπέστης όσο και στην Οδηγία 2013/40/ΕΕ προβλέπεται το κάθε Κράτος να ορίσει ένα «Σημείο Επαφής 24/7», που θα ανταποκρίνεται σε αιτήματα των αντίστοιχων Σημείων Επαφής των άλλων Κρατών για θέματα που αφορούν το κυβερνοέγκλημα και τις κυβερνοεπιθέσεις. Έτσι, έχει δημιουργηθεί ένα «Δίκτυο 24/7», για την άμεση συνεργασία μεταξύ των Κρατών, με δεδομένο άλλωστε ότι το κυβερνοέγκλημα δεν περιορίζεται εδαφικά, διαπράττεται ταχύτατα και μπορεί να υπάρξουν θύματα ταυτόχρονα σε πολλά σημεία του κόσμου (π.χ. κακόβουλο λογισμικό που αποστέλλεται με email σε εκατομμύρια παραλήπτες).

Με το έκτο άρθρο του Νόμου 4411/2016, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙ.Δ.Η.Ε.) της Ελληνικής Αστυνομίας, ορίσθηκε ως σημείο επαφής που λειτουργεί σε 24ωρη βάση, επτά ημέρες την εβδομάδα, παρέχοντας άμεση συνδρομή σε περιπτώσεις έρευνας και δίωξης αδικημάτων σχετικών με υπολογιστικά συστήματα και δεδομένα, υπό την εποπτεία Εισαγγελέα Εφετών.

Στο πλαίσιο αυτό, η ΔΙ.Δ.Η.Ε. ως αρμόδιο σημείο επαφής παρέχει τεχνικές συμβουλές, προβαίνει σε ενέργειες διατήρησης ψηφιακών δεδομένων σε κατεπείγουσες περιπτώσεις, τη συλλογή των αποδεικτικών στοιχείων, την παροχή νομικής ενημέρωσης και τον εντοπισμό των υπόπτων, επικοινωνώντας για το σκοπό αυτό με οποιοδήποτε σημείο επαφής άλλου Κράτους.

5.3. ENISA

Πρόσφατα δημοσιεύθηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ο Κανονισμός 2019/881 σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και την Πράξη για την Κυβερνοασφάλεια [7] . Ο συγκεκριμένος Κανονισμός περιλαμβάνει και διατάξεις σχετικά με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ).

Οργανισμός της Ε.Ε. για την Κυβερνοασφάλεια

[7] https://eur-lex.europa.eu/eli/reg/2019/881/oj

Ο ENISA[8], που έχει έδρα στην Ελλάδα, συμβάλλει στην ασφάλεια των δικτύων και πληροφοριών της ΕΕ από τότε που ιδρύθηκε το 2004. Με τους νέους κανόνες παρέχεται στον ENISA μόνιμη εντολή και αποσαφηνίζεται ο ρόλος του ως οργανισμού της ΕΕ για την κυβερνοασφάλεια.

Ανατέθηκαν, πλέον, στον ENISA νέα καθήκοντα για την παροχή στήριξης στα κράτη μέλη, τα θεσμικά όργανα της ΕΕ και άλλους φορείς σε ζητήματα κυβερνοχώρου. Ο ENISA θα προωθήσει την υιοθέτηση του νέου συστήματος πιστοποίησης, ενώ θα οργανώνει τακτικές ασκήσεις ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ καθώς και μια μεγάλης κλίμακας γενική άσκηση ανά διετία.

Στον Κανονισμό προβλέπεται επίσης ένα δίκτυο εθνικών υπαλλήλων-συνδέσμων με σκοπό τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ του ENISA και των κρατών μελών.

Η πρώτη νομοθετική πράξη της ΕΕ στον τομέα της κυβερνοασφάλειας - η οδηγία του 2016 σχετικά με την ασφάλεια δικτύων και πληροφοριών (NIS) - είχε ήδη προσδώσει στον ENISA βασικό ρόλο στη στήριξη της εφαρμογής της οδηγίας. Για παράδειγμα, ο ENISA καλύπτει τη γραμματειακή υποστήριξη του δικτύου των ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT) που συγκροτήθηκε δυνάμει της οδηγίας για την ασφάλεια δικτύων και πληροφοριών και υποστηρίζει ενεργά τη συνεργασία μεταξύ των ομάδων CSIRT.

Κοινή πιστοποίηση της κυβερνοασφάλειας

Στον Κανονισμό προβλέπεται επίσης η θέσπιση μηχανισμού για τη δημιουργία ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας για ειδικές διαδικασίες, προϊόντα και υπηρεσίες ΤΠΕ. Τα πιστοποιητικά που εκδίδονται στο πλαίσιο των συστημάτων θα ισχύουν σε όλες τις χώρες της ΕΕ, ώστε να είναι ευκολότερο για τους χρήστες να αποκτήσουν εμπιστοσύνη στην ασφάλεια των τεχνολογιών αυτών και για τις εταιρείες να διεξαγάγουν τις επιχειρηματικές τους δραστηριότητες πέραν των συνόρων. Οι πιθανές χρήσεις για τα εν λόγω πιστοποιητικά ποικίλλουν σε μεγάλο βαθμό, από τα συνδεδεμένα παιχνίδια και τις έξυπνες φορητές συσκευές έως τα συστήματα βιομηχανικού αυτοματισμού και ελέγχου και τα έξυπνα ενεργειακά δίκτυα.

Τα σημερινά συστήματα πιστοποίησης θα βασιστούν σε ό,τι ήδη υπάρχει σε διεθνές, ευρωπαϊκό και εθνικό επίπεδο. Τα συστήματα θα εγκρίνονται από την Επιτροπή και θα εφαρμόζονται και θα επιβλέπονται από τις εθνικές αρχές πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

Η πιστοποίηση θα είναι προαιρετική, εκτός αν άλλως ορίζεται στη νομοθεσία της ΕΕ ή των κρατών μελών. Η Επιτροπή θα παρακολουθεί τακτικά τον αντίκτυπο των

[8] https://www.enisa.europa.eu/

συστημάτων πιστοποίησης και θα αξιολογεί το βαθμό χρήσης τους από τους κατασκευαστές και τους παρόχους υπηρεσιών.

Θα υπάρχουν τρία διαφορετικά επίπεδα διασφάλισης, με βάση το επίπεδο του κινδύνου που συνδέεται με την προβλεπόμενη χρήση του προϊόντος. Για το πλέον βασικό επίπεδο, οι κατασκευαστές ή οι πάροχοι υπηρεσιών θα μπορούν να διενεργήσουν οι ίδιοι αξιολόγηση της συμμόρφωσης.

5.4.Γενικός Κανονισμός Προσωπικών Δεδομένων

Από τις 25 Μαΐου 2018 τέθηκε σε ισχύ σε επίπεδο Ευρωπαϊκής Ένωσης ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (και την κατάργηση της οδηγίας 95/46/ΕΚ).

Ο Κανονισμός επιτρέπει στους πολίτες της ΕΕ, να ελέγχουν καλύτερα τα προσωπικά τους δεδομένα. Εκσυγχρονίζει επίσης και ενοποιεί τους κανόνες που επιτρέπουν στις επιχειρήσεις να μειώσουν τη γραφειοκρατία και να επωφεληθούν από τη μεγαλύτερη εμπιστοσύνη των καταναλωτών.

Ο Κανονισμός ρυθμίζει την επεξεργασία από άτομο, εταιρεία ή οργανισμό των δεδομένων προσωπικού χαρακτήρα που αφορούν άτομα στην ΕΕ. Δεν υπάγεται σε αυτόν η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποθανόντων προσώπων ή νομικών προσώπων.

Οι κανόνες δεν εφαρμόζονται σε δεδομένα που υποβάλλονται σε επεξεργασία από ένα άτομο για αυστηρά προσωπικούς λόγους ή για δραστηριότητες που διενεργούνται κατ' οίκον, υπό την προϋπόθεση ότι δεν συνδέονται με κάποια επαγγελματική ή εμπορική δραστηριότητα. Όταν ένα άτομο χρησιμοποιεί δεδομένα προσωπικού χαρακτήρα εκτός της ιδιωτικής σφαίρας, παραδείγματος χάρη για κοινωνικοπολιτιστικές ή χρηματοοικονομικές δραστηριότητες, τότε το δίκαιο περί προστασίας δεδομένων πρέπει να τηρείται.

Δεδομένα προσωπικού χαρακτήρα

Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα.

Ο ΓΚΠΔ προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται βάσει προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά). Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε σύστημα τεχνολογίας πληροφοριών, μέσω βιντεοεπιτήρησης ή σε έντυπη μορφή. Σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που προβλέπει ο ΓΚΠΔ.

Παραδείγματα δεδομένων προσωπικού χαρακτήρα:

- όνομα και επώνυμο
- διεύθυνση κατοικίας
- ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com•
- αναγνωριστικός αριθμός κάρτας
- δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
- διεύθυνση διαδικτυακού πρωτοκόλλου (IP)
- αναγνωριστικό cookie

Επεξεργασία δεδομένων προσωπικού χαρακτήρα

Ο όρος «επεξεργασία» καλύπτει ευρύ φάσμα πράξεων που πραγματοποιούνται σε δεδομένα προσωπικού χαρακτήρα, είτε με χειροκίνητα είτε με αυτοματοποιημένα μέσα. Περιλαμβάνει τη συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή δεδομένων προσωπικού χαρακτήρα.

Ο Κανονισμός εφαρμόζεται στην εξ ολοκλήρου ή μερική επεξεργασία δεδομένων προσωπικού χαρακτήρα με αυτοματοποιημένα μέσα καθώς και στη μη αυτοματοποιημένη επεξεργασία, εάν αποτελεί μέρος διαρθρωμένου συστήματος αρχειοθέτησης.

Παραδείγματα επεξεργασίας:

- διαχείριση προσωπικού και μισθοδοσία
- προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα
- αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων
- δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου σε ιστότοπο
- αποθήκευση διευθύνσεων IP ή διευθύνσεων MAC
- μαγνητοσκόπηση (τηλεόραση κλειστού κυκλώματος)

Υπεύθυνος Προστασίας Δεδομένων – Data Protection Officer

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων εισάγει για πρώτη φορά αναλυτικές διατάξεις για τον ρόλο, τις παρεχόμενες εγγυήσεις και τα καθήκοντα του Υπευθύνου Προστασίας Δεδομένων (άρθρα 37-40), ο οποίος βρίσκεται πλέον στο επίκεντρο του νέου νομικού πλαισίου.

Ειδικότερα, ορίζεται ότι υπό συγκεκριμένες προϋποθέσεις, ορισμένοι υπεύθυνοι αλλά και εκτελούντες την επεξεργασία[9] υποχρεούνται πλέον να ορίζουν υπεύθυνο προστασίας δεδομένων.

Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων). Ο ρόλος του είναι συμβουλευτικός (όχι αποφασιστικός) και δεν φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό.

Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία.

Προβλέπονται συγκεκριμένα καθήκοντα του DPO και αντίστοιχες υποχρεώσεις του εργοδότη του. Παράβαση των σχετικών με τον DPO διατάξεων επιφέρει κυρώσεις (βλ. άρθρα 37-38 και 83 σε συνδυασμό με αιτιολογική σκέψη 97 ΓΚΠΔ).

[9] «**υπεύθυνος επεξεργασίας**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα
«**εκτελών την επεξεργασία**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

Τέλος, ορίζεται ρητά ότι τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων πρέπει να δημοσιοποιούνται προκειμένου να διασφαλίζεται η απρόσκοπτη επικοινωνία με τα υποκείμενα των δεδομένων.

Επιπλέον, προβλέπεται υποχρέωση για τον υπεύθυνο και εκτελούντα την επεξεργασία να ανακοινώνουν στην εποπτική αρχή στοιχεία που αφορούν στον ορισμό του υπευθύνου προστασίας δεδομένων.

Ασφάλεια επεξεργασίας

Οι υποχρεώσεις του υπευθύνου επεξεργασίας σχετικά με την ασφάλεια της επεξεργασίας προσδιορίζονται ρητά στο άρθρο 32 ΓΚΠΔ, ενώ η γενικότερη ευθύνη του για τον προσδιορισμό των κατάλληλων τεχνικών και οργανωτικών μέτρων προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει τη νομιμότητα μιας επεξεργασίας πηγάζει και από το άρθρο 24 ΓΚΠΔ. Επίσης, στον ΓΚΠΔ για πρώτη φορά προσδιορίζεται ρητά αυτοτελής υποχρέωση και των εκτελούντων την επεξεργασία για λήψη μέτρων ασφάλειας.

Παραδοσιακά, ο όρος **ασφάλεια πληροφορίας/ δεδομένων** (information/ data security), χρησιμοποιείται για να περιγράψει τη μεθοδολογία, καθώς και τις μεθόδους και τεχνικές που ακολουθούνται προκειμένου να επιτευχθούν οι εξής στόχοι:

- Εμπιστευτικότητα (confidentiality): Τα δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
- Ακεραιότητα (integrity): Τα δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα.
- Διαθεσιμότητα (availability): Τα δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

Πλήγμα σε οποιοδήποτε από τα ανωτέρω –από τυχαία ή εσκεμμένη ενέργεια– συνιστά, γενικά, περιστατικό ασφάλειας.

Στον ΓΚΠΔ προτείνονται τα ακόλουθα «ενδεδειγμένα» τεχνικά και οργανωτικά μέτρα ασφάλειας:

- Ψευδωνυμοποίηση και Κρυπτογράφηση.

- Διασφάλιση Απορρήτου, Ακεραιότητας, Διαθεσιμότητας και Αξιοπιστίας.
- Αποκατάσταση Διαθεσιμότητας και της πρόσβασης σε περίπτωση συμβάντος.
- Δοκιμή, εκτίμηση και διαρκής αξιολόγηση της αποτελεσματικότητας των μέτρων.
- Χρήση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης για την απόδειξη της συμμόρφωσης.

Τα μέτρα ασφάλειας μπορεί να τεκμηριώνονται σε επιμέρους διαδικασίες ή σε γενικότερες πολιτικές ασφάλειας. Η επιλογή των κατάλληλων μέτρων ασφάλειας γίνεται λαμβάνοντας υπόψη (πρβλ. άρθρα 25 και 32 ΓΚΠΔ) τις τελευταίες εξελίξεις, το κόστος εφαρμογής, καθώς και τα χαρακτηριστικά της επεξεργασίας (φύση - πεδίο εφαρμογής - πλαίσιο – σκοποί). Σε κάθε περίπτωση, πριν τον καθορισμό των μέτρων ασφάλειας που θα υιοθετηθούν, προέχει η σωστή αξιολόγηση των κινδύνων και των πιθανών συνεπειών τους για τα υποκείμενα των δεδομένων. Τέλος, σε κάθε περίπτωση, τα υλοποιημένα μέτρα πρέπει να υποβάλλονται σε περιοδική, τουλάχιστον, αναθεώρηση, αλλά και να είναι αποδεδειγμένα επικυρωμένα από την διοίκηση του υπευθύνου ή του εκτελούντος την επεξεργασία.

Γνωστοποίηση περιστατικών παραβίασης δεδομένων

Σύμφωνα με το άρ. 33 του Κανονισμού, οι υπεύθυνοι επεξεργασίας, σε περίπτωση που συμβεί περιστατικό παραβίασης προσωπικών δεδομένων από το οποίο ενδέχεται να προκληθεί κίνδυνος στα δικαιώματα και τις ελευθερίες των προσώπων τα οποία αφορά το περιστατικό, οφείλουν να γνωστοποιήσουν το εν λόγω περιστατικό στην εθνική Αρχή που είναι αρμόδια για την προστασία των δεδομένων προσωπικού χαρακτήρα [(στην Ελλάδα η Αρχή αυτή είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)].

Η γνωστοποίηση αυτή πρέπει να γίνεται αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που ο υπεύθυνος επεξεργασίας ενημερωθεί για το περιστατικό. Η γνωστοποίηση πρέπει να περιέχει σύνολο σχετικών πληροφοριών (φύση/έκταση του περιστατικού, κατηγορίες προσώπων που επλήγησαν, αιτία και συνέπειες αυτού, ενέργειες που έγιναν προς αντιμετώπισή του, κ.ά.). Ακόμα και αν οι σχετικές αυτές πληροφορίες δεν είναι όλες διαθέσιμες κατά την υποβολή της γνωστοποίησης, αυτή θα πρέπει να υποβληθεί ως αρχική και να ακολουθήσει στο μέλλον, χωρίς αδικαιολόγητη καθυστέρηση, επικαιροποίησή της (με υποβολή συμπληρωματικής γνωστοποίησης).

Επισημαίνεται ότι ακόμα και αν το περιστατικό δεν μπορεί να προκαλέσει κίνδυνο για τα φυσικά πρόσωπα που αφορά, οπότε και δεν απαιτείται η υποβολή της ως άνω γνωστοποίησης στην Αρχή, ο υπεύθυνος επεξεργασίας οφείλει σε κάθε περίπτωση να τηρεί δικό του εσωτερικό σχετικό αρχείο.

Περαιτέρω, σύμφωνα με το άρ. 34 του Κανονισμού, όταν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων τα οποία αφορά το περιστατικό, τότε ο υπεύθυνος επεξεργασίας οφείλει να ανακοινώνει αμελλητί την παραβίαση και στα πρόσωπα αυτά. Αυτή η ανακοίνωση είναι ανεξάρτητη της προαναφερθείσας γνωστοποίησης στην Αρχή (η οποία γνωστοποίηση στην Αρχή υποβάλλεται ακόμα και αν ο σχετικός κίνδυνος δεν κρίνεται ως υψηλός). Η ανακοίνωση στα φυσικά πρόσωπα θα πρέπει να γίνει με τον πλέον πρόσφορο και αποτελεσματικό τρόπο, με τη μορφή προσωποποιημένης πληροφόρησης και όχι μέσω κάποιας γενικού χαρακτήρα ανακοίνωσης, στο βαθμό που αυτό είναι εφικτό.

Σημειώνεται ότι η Αρχή δύναται σε κάθε περίπτωση να δώσει εντολή στον υπεύθυνο επεξεργασίας να ενημερώσει τα φυσικά πρόσωπα για το περιστατικό (άρ. 58 παρ. 2 ε' Κανονισμού).

5.5.Αρμόδιοι φορείς και Αρχές

5.5.1. Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας

Με το Π.Δ. 178/2014 προβλέφθηκε η ίδρυση και η διάρθρωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙ.Δ.Η.Ε.) με έδρα την Αθήνα και η ίδρυση και διάρθρωση Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα τη Θεσσαλονίκη.

Η αποστολή της ΔΙΔΗΕ συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Στην εσωτερική της δομή αποτελείται από πέντε τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από:

- Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών,
- Τμήμα Καινοτόμων Δράσεων και Στρατηγικής,
- Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας λογισμικού και Πνευματικών Δικαιωμάτων,

- Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και
- Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων.

5.5.2. Εθνική Υπηρεσία Πληροφοριών – Διεύθυνση Κυβερνοχώρου

Η Διεύθυνση Κυβερνοχώρου της Εθνικής Υπηρεσίας Πληροφοριών[10] είναι αρμόδια:

- για τεχνικής φύσεως θέματα ασφάλειας πληροφοριών (INFOSEC) και ειδικότερα για την ασφάλεια των εθνικών επικοινωνιών, των συστημάτων τεχνολογίας πληροφοριών καθώς και για την αξιολόγηση και πιστοποίηση των διαβαθμισμένων συσκευών και συστημάτων ασφάλειας επικοινωνιών και πληροφορικής,
- για τη συλλογή, την επεξεργασία δεδομένων και την ενημέρωση των αρμόδιων φορέων καθώς και για την, κατά περίπτωση, στατική και ενεργητική αντιμετώπιση των ηλεκτρονικών επιθέσεων κατά των κρίσιμων υποδομών της χώρας και ειδικότερα κατά των δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής,
- για τον έλεγχο και την αξιολόγηση ασφάλειας συστημάτων καθώς και για τη συλλογή, εξόρυξη (data mining) και εκμετάλλευση δεδομένων.

5.5.3. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει ως αποστολή της την εποπτεία της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων, του νόμου 4624/2019, του νόμου 3471/2006 και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά[11].

η Αρχή είναι επιφορτισμένη μεταξύ άλλων να (άρθρο 57 ΓΚΠΔ):

[10] Π.Δ. 1/2017, όπως τροπ. και ισχύει
[11] https://www.dpa.gr/

- Παρακολουθεί και επιβάλλει την εφαρμογή του ΓΚΠΔ.
- Προωθεί την ευαισθητοποίηση του κοινού στα ζητήματα προστασίας προσωπικών δεδομένων και των υπευθύνων και εκτελούντων επεξεργασίας σχετικά με τις υποχρεώσεις τους δυνάμει του ΓΚΠΔ. Ειδική προσοχή αποδίδεται σε δραστηριότητες που απευθύνονται ειδικά σε παιδιά.
- Συμβουλεύει το εθνικό κοινοβούλιο, την κυβέρνηση και άλλα όργανα και οργανισμούς για νομοθετικά και διοικητικά μέτρα που σχετίζονται με την προστασία των προσωπικών δεδομένων.
- Παρέχει κατόπιν αιτήματος πληροφορίες στα υποκείμενα των δεδομένων σχετικά με την άσκηση των δικαιωμάτων τους.
- Χειρίζεται τις υποβληθείσες για παράβαση διατάξεων του ΓΚΠΔ καταγγελίες.
- Διενεργεί έρευνες σχετικά με την εφαρμογή του ΓΚΠΔ.
- Συνεργάζεται με άλλες εποπτικές αρχές μέσω ανταλλαγής πληροφοριών και να παρέχει αμοιβαία συνδρομή σε αυτές με σκοπό τη διασφάλιση της συνεκτικότητας εφαρμογής του ΓΚΠΔ.

Η Αρχή καταρτίζει ετήσια έκθεση των δραστηριοτήτων της, την οποία υποβάλλει στο εθνικό κοινοβούλιο, την κυβέρνηση και άλλες αρχές και την καθιστά διαθέσιμη στο κοινό, την Επιτροπή και το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

5.5.4. Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) είναι μια από τις συνταγματικά καθιερωμένες Ανεξάρτητες Αρχές με διοικητική αυτοτέλεια, η οποία συστάθηκε ως ειδικός εποπτεύων φορέας για να προστατεύει το απόρρητο της επικοινωνίας[12].

Η Αρχή συστάθηκε με το Ν.3115/2003 κατ' εφαρμογή της συνταγματικής επιταγής του άρθρου 19 παρ. 2 του Συντάγματος. Με τον παραπάνω νόμο ρυθμίζονται τα θέματα της συγκρότησης, των αρμοδιοτήτων και της λειτουργίας της ΑΔΑΕ, ενώ με το ΠΔ 40/2005 ρυθμίζεται η εσωτερική της διάρθρωση.

Η ΑΔΑΕ, στο πλαίσιο των αρμοδιοτήτων της, έχει ως σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με

[12] http://www.adae.gr/

οποιονδήποτε άλλο τρόπο. Επιπλέον, στις αρμοδιότητές της περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου που προβλέπονται από το νόμο.

Η ΑΔΑΕ έχει ελεγκτικές, γνωμοδοτικές και κανονιστικές αρμοδιότητες, ενώ παράλληλα συλλέγει πληροφορίες σχετικές με την αποστολή της και επιβάλλει κυρώσεις σε περιπτώσεις παραβάσεως της σχετικής κείμενης νομοθεσίας.

Πιο συγκεκριμένα, μεταξύ άλλων, η ΑΔΑΕ έχει, σύμφωνα με το άρθρο 6 του ν. 3115/2003, όπως ισχύει, τις παρακάτω αρμοδιότητες:

- Διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας τακτικούς και έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της ΕΥΠ, άλλων δημοσίων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημοσίου τομέα, καθώς και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία. Οι έλεγχοι διενεργούνται από τα μέλη και το προσωπικό της ΑΔΑΕ προκειμένου να διαπιστωθεί η σωστή εφαρμογή των πολιτικών ασφάλειας που επιβάλλεται να εφαρμόζουν οι πάροχοι ή για τη διαπίστωση παραβίασης του απορρήτου της επικοινωνίας.

- Λαμβάνει πληροφορίες σχετικές με την αποστολή της από τις προαναφερθείσες υπηρεσίες, οργανισμούς και επιχειρήσεις, καθώς και από τους εποπτεύοντες Υπουργούς.

- Καλεί σε ακρόαση τις παραπάνω υπηρεσίες, οργανισμούς, νομικά πρόσωπα και επιχειρήσεις και κάθε άλλο πρόσωπο, που κρίνει ότι μπορεί να συμβάλει στην εκπλήρωση της αποστολής της.

- Προβαίνει σε κατάσχεση των μέσων παραβίασης του απορρήτου που υποπίπτουν στην αντίληψή της κατά την ενάσκηση του έργου της και ορίζεται μεσεγγυούχος αυτών μέχρι να αποφανθούν τα αρμόδια δικαστήρια. Προβαίνει επίσης στην καταστροφή πληροφοριών ή στοιχείων ή δεδομένων, τα οποία αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.

- Εξετάζει καταγγελίες σχετικά με την προστασία των δικαιωμάτων των αιτούντων, όταν θίγονται από τον τρόπο και τη διαδικασία άρσης του απορρήτου.

- Συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών, καθώς και με ευρωπαϊκούς και διεθνείς οργανισμούς, για θέματα της αρμοδιότητάς της.

- Γνωμοδοτεί και απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και τη διαδικασία άρσης του.

- Εκδίδει κανονιστικές πράξεις που δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως με τις οποίες ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις ανωτέρω αρμοδιότητές της καθώς και με την εν γένει διασφάλιση του απορρήτου των επικοινωνιών.

5.5.5. Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είναι Ανεξάρτητη Διοικητική Αρχή. Αποτελεί τον Εθνικό Ρυθμιστή που ρυθμίζει, εποπτεύει και ελέγχει: (α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρίες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και (β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρίες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς.

Ειδικότερα, σύμφωνα με το νομικό πλαίσιο που τη διέπει, η ΕΕΤΤ, μεταξύ άλλων:

- Ρυθμίζει τα θέματα που αφορούν τον α) καθορισμό σχετικών αγορών, προϊόντων ή υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ελληνική Επικράτεια, β) τον ορισμό και τις υποχρεώσεις Παρόχων με Σημαντική Ισχύ στις ανωτέρω σχετικές αγορές σύμφωνα με την εθνική και κοινοτική νομοθεσία.

- Εποπτεύει και ελέγχει τους παρόχους δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, επιβάλλει τις σχετικές κυρώσεις, τηρεί και διαχειρίζεται το Μητρώο Παρόχων Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών.

- Εκδίδει Κώδικες Δεοντολογίας για την παροχή δικτύων και υπηρεσιών των ηλεκτρονικών επικοινωνιών.

- Μεριμνά για την τήρηση της νομοθεσίας περί ηλεκτρονικών επικοινωνιών και επιβάλει σχετικές κυρώσεις.

- Ρυθμίζει τα θέματα ονομάτων χώρου στο Διαδίκτυο με κατάληξη ".gr" και είναι αρμόδια για θέματα ονομάτων χώρου με κατάληξη ".eu".

- Ρυθμίζει θέματα προστασίας του καταναλωτή στον τομέα των ηλεκτρονικών επικοινωνιών και στον τομέα παροχής ταχυδρομικών υπηρεσιών.

Ονόματα χώρου ".gr"

Ένα όνομα χώρου (domain name) είναι μία λέξη που επιλέγουμε προκειμένου να μπορούμε με εύκολο τρόπο να συνδεθούμε με έναν υπολογιστή στο διαδίκτυο. Η λέξη αυτή πάντα προσδιορίζεται περαιτέρω από μία κατάληξη που χαρακτηρίζει κατά κάποιο τρόπο την "περιοχή" του δικτύου στην οποία ανήκει. Έτσι, για παράδειγμα για τον χώρο ονομάτων με κατάληξη .gr, ένα domain name θα έχει τη μορφή onoma.gr και επισκεπτόμαστε τις ιστοσελίδες που του αντιστοιχούν γράφοντας σε κάποιο πρόγραμμα πλοήγησης (browser) μια διεύθυνση της μορφής http://www.onoma.gr.

Η βάση δεδομένων που περιλαμβάνει το σύνολο των καταχωρηθέντων ονομάτων χώρου με κατάληξη .gr και .ελ και των ονομάτων χώρου με κατάληξη .gr ή .ελ που τυχόν αποτελούν αντικείμενο δηλώσεων καταχώρησης, με τα στοιχεία τα οποία αντιστοιχούν σε κάθε ένα από αυτά, όπως κατά καιρούς τα στοιχεία αυτά καθορίζονται από την ΕΕΤΤ με Απόφασή της. Επιπλέον, ο φορέας που διαχειρίζεται το Μητρώο είναι υπεύθυνος για τη διαχείριση των εξυπηρετητών ονομάτων και των αρχείων ζώνης (zone files) που είναι απαραίτητα για τη σωστή λειτουργία των ονομάτων χώρου με κατάληξη .gr και .ελ. Το Μητρώο ανήκει στην ΕΕΤΤ, η οποία είναι υπεύθυνη για τη σωστή και σύμφωνη με την κείμενη νομοθεσία χρήση του.

Για να εκχωρηθεί ένα όνομα χώρου με κατάληξη .gr ή .ελ θα πρέπει κάποιος να καταθέσει σχετική δήλωση σε κάποιον καταχωρητή. Στην ιστοσελίδα της ΕΕΤΤ, έχει αναρτηθεί Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου με κατάληξη .gr ή .ελ, ο οποίος έχει συνταχθεί από την ΕΕΤΤ και καθορίζει τις προϋποθέσεις και τη διαδικασία για κάθε νέα εκχώρηση .

Πέραν της εκχώρησης ονομάτων χώρου με κατάληξη .gr και .ελ (ονόματα 2ου επιπέδου), εκχώρηση ονομάτων χώρου μπορεί να γίνει και στα ακόλουθα subdomains του .gr (ονόματα 3ου επιπέδου):

- com.gr για όσους ασκούν εμπορική δραστηριότητα
- edu.gr για εκπαιδευτικούς οργανισμούς
- net.gr για παρόχους υπηρεσιών διαδικτύου (Internet Service Providers - ISPs) και παρόχους
- org.gr για μη κερδοσκοπικούς οργανισμούς
- gov.gr αποκλειστικά για κυβερνητικούς οργανισμούς

5.6.Μελέτη Περίπτωσης

- Στο Γενικό Κανονισμό Προστασίας Δεδομένων (2016/679/ΕΕ) περιγράφονται οι υποχρεώσεις του Υπεύθυνου Επεξεργασίας. Τεκμηριώστε πως η πολιτική ασφάλειας συμβάλει στην καλύτερη συμμόρφωση του φορέα με τον Κανονισμό.

- Στο Νόμο 3979/2011 (ΦΕΚ 138 Α'/16-6-2011), "Για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις", αναζητήστε τα άρθρα που αναφέρονται στα θέματα της ασφάλειας και τεκμηριώστε ποιες είναι οι υποχρεώσεις των φορέων του δημοσίου.

5.7.Βιβλιογραφία

- Νόμος 4577/2018 (ΦΕΚ Α' 199/3-12-2018). Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις.

- Γερμανός, Γ. και Παπαθανασίου, Α. (2017). *Νομοθεσία για το έγκλημα στον κυβερνοχώρο και την ψηφιακή εγκληματικότητα*. Εκδόσεις Αντ. Ν. Σάκκουλα Ε.Ε.

- Νόμος 4411/2016 (ΦΕΚ Α' 142/3-8-2016). Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων

Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης - πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις.

- Κανονισμός 2016/679/ΕΕ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων (Γενικός Κανονισμός Προστασίας Δεδομένων).

- Νόμος 3979/2011 - (ΦΕΚ 138 Α/16-6-2011). "Για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις".

6. ΑΣΦΑΛΕΙΑ ΚΟΙΝΩΝΙΚΩΝ ΔΙΚΤΥΩΝ

Ο όγκος των προσωπικών δεδομένων που διακινούνται καθημερινά μέσα από μία Εφαρμογή Κοινωνικής Δικτύωσης (ΕΚΔ) είναι εντυπωσιακά μεγάλος. Λαμβάνοντας υπόψη ότι ένας χρήστης χρησιμοποιεί πολλαπλές εφαρμογές κοινωνικής δικτύωσης διευρύνονται ακόμα περισσότερο τα όρια έκθεσης της ιδιωτικής ζωής του ατόμου.

Δεδομένου ότι η εμπορική επιτυχία μιας ΕΚΔ εξαρτάται σε μεγάλο βαθμό από τον αριθμό των χρηστών που προσελκύει, οι πάροχοι σχεδιάζουν τις εφαρμογές τους έτσι ώστε να ενθαρρύνουν συμπεριφορές οι οποίες αυξάνουν τον αριθμό των χρηστών και των μεταξύ τους συνδέσεων. Το αποτέλεσμα αυτής της τακτικής είναι να γίνονται οι χρήστες πιο δεκτικοί στα «αιτήματα φιλίας» που λαμβάνουν και τελικά να μη συνειδητοποιούν το μέγεθος ή το είδος του κοινού το οποίο έχει πρόσβαση στα δεδομένα του προφίλ τους.

Ο Mark Zuckerberg, ιδρυτής του Facebook, υποστήριξε σε μία ομιλία του ότι «η ιδιωτικότητα δεν αποτελεί πλέον κοινωνική νόρμα». Ισχύει άραγε κάτι τέτοιο ή μήπως οι περισσότεροι από εμάς δεν έχουμε συνειδητοποιήσει τις επιπτώσεις αυτής της υπέρμετρης κοινωνικότητας. Στη συνέχεια εξετάζονται οι βασικότεροι κίνδυνοι για την ασφάλεια και την ιδιωτικότητα ενός τακτικού χρήστη του Facebook και του Twitter αλλά και τα αντίμετρα τα οποία μπορούν να ληφθούν για την αντιμετώπισή τους.

Η κοινωνική δικτύωση, είναι μια μορφή συγκέντρωσης ατόμων σε «κοινότητες», κάτι αντίστοιχο με την έννοια της γειτονιάς, με στόχο την διαμόρφωση κοινωνικών σχέσεων. Τα κοινωνικά δίκτυα στο Διαδίκτυο, είναι άτυπα εργαλεία διαχείρισης ταυτότητας που υποστηρίζουν την κοινωνική δικτύωση και χαρακτηρίζονται από ευκολία στη χρήση, διευκολύνουν τη δημιουργία αυθόρμητων σχέσεων, διευρύνουν την αλληλεπίδραση και την επικοινωνία μεταξύ των χρηστών τους.

Υπάρχει μια πληθώρα δυνατοτήτων, που κάθε ΕΚΔ διαθέτει, όπου ένας χρήστης μπορεί, να δημιουργεί και να συντηρεί, χωρίς ιδιαίτερες τεχνικές γνώσεις: Ένα δημόσιο ή ημι-δημόσιο προφίλ, μια λίστα φίλων (friendslist), πρόσβαση στη λίστες των φίλων και χρήση διαφόρων υπηρεσιών και εργαλείων.

Οι εμπλεκόμενοι/ οντότητες στις ΕΚΔ διακρίνονται στις ακόλουθες τρεις κατηγορίες:

- ΠΑΡΟΧΟΙ ΥΠΗΡΕΣΙΩΝ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ (ΙΔΙΕΣ ΕΤΑΙΡΕΙΕΣ). Προσφέρουν τα μέσα και τις δυνατότητες για την επεξεργασία των δεδομένων των χρηστών.

- ΧΡΗΣΤΕΣ. Χρησιμοποιούν τις υπηρεσίες και αλληλεπιδρούν με τους άλλους χρήστες.

- ΤΡΙΤΕΣ ΟΝΤΟΤΗΤΕΣ. Οι τρίτες οντότητες μπορεί να είναι πάροχοι εφαρμογών, άλλων υπηρεσιών κ.ά.

6.1. Κίνδυνοι Ασφάλειας και Ιδιωτικότητας στις ΕΚΔ

Οι κίνδυνοι ασφάλειας και ιδιωτικότητας στις Εφαρμογές Κοινωνικής Δικτύωσης συνοψίζονται στις ακόλουθες κατηγορίες:

- **Κλοπή Ταυτότητας**. Πρόκειται για την περίπτωση όπου κάποιος χρήστης των ΕΚΔ παριστάνει ψευδεπίγραφα κάποιον άλλον χρήστη και μπορεί να εκδηλωθεί με: α) την κλοπή της γνήσιας διαδικτυακής ταυτότητας (προφίλ), β) τη δημιουργία ενός νέου προφίλ που θα περιλαμβάνει, αυθαίρετα, προσωπικά δεδομένα χρήστη εν αγνοία του (π.χ. ονοματεπώνυμο ή φωτογραφίες).

- **Έκθεση μεγάλου αριθμού προσωπικών δεδομένων και χρήση της πληροφορίας για άλλο σκοπό**. Στις ΕΚΔ ο χρήστης εκθέτει, καταχωρεί και δημοσιεύει μεγάλο αριθμό προσωπικών του στοιχειών, ενώ παράλληλα έχει λανθασμένη αίσθηση ότι οι πληροφορίες που ανεβάζει είναι διαθέσιμες μόνο στους φίλους του.

- **Παρενόχληση – Stalking – Cyberbullying**. Όταν οι χρήστες των ΕΚΔ δημοσιοποιούν προσωπικές πληροφορίες (π.χ. αριθμό τηλεφώνου, διεύθυνση οικίας κ.ά.) μπορούν να χρησιμοποιηθούν από κακόβουλους χρήστες, για διαδικτυακή παρακολούθηση, παρενόχληση, ηλεκτρονικό εκφοβισμό (Cyberbullying).

- **Εντοπισμός – Προσδιορισμός θέσης**. Πολλοί χρήστες επιλέγουν να δημοσιεύσουν στις ΕΚΔ το που βρίσκονται κάθε στιγμή. Αυτό γίνεται είτε συνειδητά ή αυτόματα, με χρήση κατάλληλων εφαρμογών, πλην όμως αυτή η πληροφορία μπορεί να χρησιμοποιηθεί από χρήστες με κακόβουλους σκοπούς (π.χ. διαρρήκτες) και να δημιουργηθεί κίνδυνος για την φυσική ασφάλεια του χρήστη.

- **Δημοσιοποίηση προσωπικών δεδομένων από τρίτους χρήστες**. Όσο προσεκτικός είναι ένας χρήστης σχετικά με τις πληροφορίες που δημοσιοποιεί στις ΕΚΔ, δεν είναι σε θέση να ελέγξει πληροφορίες, που άλλοι χρήστες

δημοσιοποιούν για αυτόν (π.χ. ανέβασμα μιας φωτογραφίας χωρίς γνώση λοιπών εικονιζόμενων).

- **Παραχώρηση των δεδομένων** των χρηστών από τις ίδιες τις εταιρίες των ΕΚΔ σε τρίτες εταιρίες, για στοχευμένη διαφήμιση.
- **Παραχώρηση στοιχείων σε εφαρμογές**, οι οποίες όμως δεν πιστοποιούνται πάντα για την ασφάλειά τους (ενδέχεται να αποκτούν πρόσβαση σε προσωπικές πληροφορίες ή να περιέχουν ιομορφικό λογισμικό).
- **Εξειδικευμένες απάτες**. Οι πληροφορίες που δημοσιεύουν οι χρήστες μπορεί να χρησιμοποιηθούν για επιθέσεις ηλεκτρονικής εξαπάτησης (phishing) ή κοινωνικής μηχανικής (social engineering).

Επιπρόσθετα μπορεί να ανακύψουν και άλλοι δευτερεύοντες κίνδυνοι όπως:

- Εύκολη μετάδοση επιβλαβούς ηλεκτρονικού περιεχόμενου (όπως ιομορφικό λογισμικό, πορνογραφικό υλικό κ.ά.),
- Πιθανά προβλήματα στην αγορά εργασίας (π.χ. ένα βίντεο σπουδαστή σε εύθυμη κατάσταση μπορεί να σταθεί εμπόδιο σε μια μελλοντική προσπάθεια εύρεσης εργασίας).
- Οι ΕΚΔ μπορεί να γίνουν πολύ εθιστικές, οδηγώντας σταδιακά σε κοινωνική απομόνωση.
- Οι όροι χρήσης μπορούν να αλλάξουν οποτεδήποτε το έχει αποδεχτεί ο χρήστης κατά την εγγραφή στον κοινωνικό δίκτυο. Συνήθως ζητείται συγκατάθεση άλλα η εξάρτηση είναι τέτοια που πρακτικά γίνεται αποδοχή χωρίς επαρκή μελέτη των αλλαγών. Η ίδια η μελέτη των όρων είναι πολύ χρονοβόρα και δυσνόητη.
- Οι χρήστες αποποιούνται των πνευματικών τους δικαιωμάτων για οτιδήποτε ανεβάζουν, αφού πλέον ανήκει στο κοινωνικό δίκτυο.

6.2.Facebook

Το Facebook, η πιο γνωστή ΕΚΔ, ξεκίνησε το 2004 και ανήκει στην εταιρεία Facebook, Inc., που εδρεύει στις ΗΠΑ. Οι κυριότερες απειλές είναι οι ακόλουθες:

1. **Δημιουργία ψηφιακού φακέλου**. Τα προφίλ των χρηστών μπορούν να συγκεντρωθούν από τρίτους οι οποίοι θα δημιουργήσουν έναν ψηφιακό φάκελο προσωπικών δεδομένων που θα περιλαμβάνει στιγμιότυπα του κάθε προφίλ σε βάθος χρόνου (Acquisti & Gross, 2006 · ENISA, 2007).

2. **Συλλογή δευτερευόντων πληροφοριών**. Πέραν των πληροφοριών που ο χρήστης εν γνώσει του κοινοποιεί μέσω του προφίλ του, το Facebook είναι σε θέση να συλλέγει πληροφορίες που προκύπτουν από τη χρήση της υπηρεσίας, όπως για παράδειγμα το χρόνο και τη διάρκεια συνδέσεων στην υπηρεσία, τη θέση (διεύθυνση IP) του χρήστη, τα προφίλ χρηστών που επισκέπτεται και τα μηνύματα που ανταλλάσσει. Επίσης, η δυνατότητα αυθεντικοποίησης των χρηστών σε συνεργαζόμενους ιστότοπους χρησιμοποιώντας το λογαριασμό τους στο Facebook, διευρύνει τις δυνατότητες παρακολούθησης των ενεργειών τους (Acquisti & Gross, 2006 · ENISA, 2007).

3. **Αναγνώριση προσώπου**. Οι φωτογραφίες που δημοσιεύονται στο προφίλ του χρήστη συνδέονται είτε άμεσα, μέσω των ετικετών που προσαρτώνται σε κάθε πρόσωπο της φωτογραφίας, είτε έμμεσα με τον κάτοχο του προφίλ και αποτελούν ένα ψηφιακό αναγνωριστικό του χρήστη, το οποίο δίνει τη δυνατότητα συσχέτισης διαφορετικών προφίλ του Facebook ή και διαφορετικών ΕΚΔ. Το αποτέλεσμα είναι η δυνατότητα συλλογής περισσότερων πληροφοριών για έναν χρήστη από αυτές που ο ίδιος επιθυμεί να αποκαλύψει (ENISA, 2007).

4. **CBIR (Content-based Image Retrieval)**. Το CBIR είναι μία τεχνολογία βάσει της οποίας είναι εφικτή η διασταύρωση χαρακτηριστικών από διαφορετικές φωτογραφίες με σκοπό τον εντοπισμό χρηστών. Επιτρέπει την εξαγωγή δεδομένων θέσης από φαινομενικά ανώνυμα προφίλ και δίνει τη δυνατότητα άσκησης επιθετικού μάρκετινγκ ή άλλων ενεργειών που συνδέονται με την ακούσια αποκάλυψη δεδομένων θέσης (ENISA, 2007).

5. **Δυσκολία πλήρους διαγραφής προφίλ**. Το Facebook παρέχει τη δυνατότητα στο χρήστη να απενεργοποιήσει εύκολα το προφίλ του μέσω του μενού «Account Settings». Δεν ισχύει όμως το ίδιο για την πλήρη διαγραφή του προφίλ, καθώς η δυνατότητα διαγραφής δεν είναι εξίσου ορατή και άμεση. Επιπρόσθετα, δευτερεύουσες πληροφορίες του χρήστη που συνδέονται με το προφίλ του, όπως τα σχόλια που έχει κάνει στα προφίλ τρίτων, είναι πρακτικά αδύνατον να αφαιρεθούν, αφού ο χρήστης θα πρέπει να τα εντοπίσει και να τα αφαιρέσει χειροκίνητα. Το αποτέλεσμα είναι να χάνει ο χρήστης τον έλεγχο της ηλεκτρονικής του ταυτότητας και να αποδυναμώνεται η δυνατότητα άμυνάς του έναντι της δημιουργίας του ψηφιακού του φακέλου (ENISA, 2007).

6. **SPAM**. Πολλοί spammers προσπαθούν να επωφεληθούν από την τεράστια ανάπτυξη του Facebook και τη δυνατότητα ελεύθερης διακίνησης μηνυμάτων που παρέχει, προκειμένου να διαδίδουν ανεπιθύμητα μηνύματα. Μία συνήθης

τακτική είναι η χρήση ειδικού λογισμικού που αυτοματοποιεί την αποστολή αιτημάτων φιλίας και τη δημοσίευση σχολίων, στοχεύοντας σε προφίλ με συγκεκριμένα δημογραφικά χαρακτηριστικά. Τα σχόλια που δημοσιεύουν περιλαμβάνουν συνήθως συνδέσμους προς ιστότοπους που έχουν σχεδιαστεί για την προώθηση προϊόντων και υπηρεσιών. Επίσης, χρησιμοποιούν συνήθως ελκυστικά προφίλ προκειμένου να πείσουν το θύμα να δεχτεί το αίτημα φιλίας που του αποστέλλουν και στη συνέχεια δημοσιεύουν τα σχόλιά τους στις δημόσιες περιοχές σχολίων των φίλων των θυμάτων (ENISA, 2007 · Dinerman, 2011).

7. **Ευπάθειες κώδικα και ιομορφικό λογισμικό**. Λόγω της υψηλής δημοτικότητάς του, το Facebook έχει αποτελέσει κατά καιρούς μέσο εξάπλωσης ιομορφικού λογισμικού το οποίο μπορεί να εκμεταλλευτεί ευπάθειες του κώδικα της πλατφόρμας της υπηρεσίας, των εφαρμογών τρίτων που χρησιμοποιούνται μέσα από αυτή, του συστήματος του χρήστη, ή την άγνοια των χρηστών σχετικά με τις μεθόδους προστασίας (ENISA, 2007 · McDowell & Morda, 2011 · McCarthy, Watson & Weldon-Siviy, 2011).

8. **Διαρροή προσωπικών δεδομένων μέσω της χρήσης τρίτων εφαρμογών**. Η χρήση των εφαρμογών που παρέχονται μέσω του Facebook ενδέχεται να δίνει τη δυνατότητα σε τρίτους να αποκτήσουν πρόσβαση στα προσωπικά στοιχεία του χρήστη (McDowell & Morda, 2011 · Dinerman, 2011).

9. **Ηλεκτρονική εξαπάτηση και κοινωνική μηχανική**. Το Facebook μπορεί να χρησιμοποιηθεί από έναν επιτιθέμενο ως εργαλείο συλλογής πληροφοριών για έναν χρήστη-στόχο, οι οποίες θα του επιτρέψουν να εξαπολύσει μία στοχευμένη επίθεση ηλεκτρονικής εξαπάτησης. Επίσης, το ίδιο το Facebook μπορεί να χρησιμοποιηθεί ως μέσο διάδοσης συνδέσμων ηλεκτρονικής εξαπάτησης. Η τακτική που συνήθως χρησιμοποιείται είναι η δημοσίευση δελεαστικών συνδέσμων, οι οποίοι αν ακολουθηθούν οδηγούν σε σελίδες που είναι αντίγραφα της αρχικής σελίδας σύνδεσης του Facebook με στόχο την υποκλοπή των συνθηματικών του χρήστη (ENISA, 2007 · McDowell & Morda, 2011 · McCarthy, Watson & Weldon-Siviy, 2011).

10. **Διείσδυση σε δίκτυα που οδηγεί σε διαρροή πληροφοριών**. Ορισμένες πληροφορίες είναι διαθέσιμες μόνο σε Φίλους και μέλη μίας περιορισμένης ομάδας ανθρώπων. Λόγω του ότι κάποιος μπορεί να κερδίσει εύκολα τη «φιλία» ενός χρήστη, αυτός ο μηχανισμός προστασίας δεν είναι ιδιαίτερα αποτελεσματικός. Ουσιαστικά, για την επικοινωνία μεταξύ των χρηστών δεν παρέχεται καμιά εγγύηση ως προς την ασφάλεια και την ιδιωτικότητα Επίσης, τα κριτήρια που χρησιμοποιούνται για την αποδοχή της συμμετοχής ενός χρήστη σε ένα δίκτυο είναι πολύ γενικά (ENISA, 2007).

11. **Πλαστοπροσωπία**. Η υλοποίηση αυτής της επίθεσης στο Facebook δεν απαιτεί ιδιαίτερες γνώσεις, αφού οποιοσδήποτε χρήστης μπορεί να δημιουργήσει ένα

προφίλ, παρέχοντας στη συνέχεια τα στοιχεία του προσώπου που θέλει να υποδυθεί. Παραλλαγές της επίθεσης αυτής είναι η κλωνοποίηση προφίλ και η μεταφορά υπάρχοντος προφίλ σε άλλες ΕΚΔ (ENISA, 2007).

12. **Πειρατεία προφίλ**. Ο επιτιθέμενος αποκτά τον πλήρη έλεγχο του προφίλ ενός χρήστη, χρησιμοποιώντας διάφορες τεχνικές και εκμεταλλευόμενος ευπάθειες όπως αδύναμα συνθηματικά και ελλιπή μέτρα προστασίας (McDowell & Morda, 2011).

13. **Παρακολούθηση και καταδίωξη**. Πρόκειται για επιθετικές συμπεριφορές ατόμων τα οποία επιδιώκουν να έρθουν σε επικοινωνία και φυσική επαφή με το θύμα. Το Facebook ενθαρρύνει τη δημοσίευση προσωπικών πληροφοριών τα οποία αποκαλύπτουν τη θέση του χρήστη, τη συμπεριφορά του ή ακόμα και το αν είναι συνδεδεμένος με την υπηρεσία (ENISA, 2007).

14. **Εκφοβισμός**. Το Facebook διαθέτει ορισμένα χαρακτηριστικά που το καθιστούν ένα πολύ χρήσιμο εργαλείο για έναν επιτιθέμενο ο οποίος επιθυμεί να εκφοβίσει το θύμα του. Ορισμένα από αυτά τα χαρακτηριστικά είναι η ευκολία με την οποία ο επιτιθέμενος μπορεί να παραμείνει ανώνυμος (χρησιμοποιώντας ένα ψεύτικο προφίλ), καθώς και η δυνατότητα χρήσης πολλαπλών καναλιών επικοινωνίας μέσα από την ίδια πλατφόρμα (ENISA, 2007).

15. **Απειλή «εκ των έσω»**. Το Facebook αντλεί το μεγαλύτερο ποσοστό των κερδών του από τη διαφήμιση, γεγονός που αποτελεί το σημαντικότερο κίνδυνο κατά της ιδιωτικότητας. Ο χρήστης δε διαθέτει τη δυνατότητα να διασφαλίσει ότι ο πάροχος δεν θα καταχραστεί τα δεδομένα του ή ότι εφαρμόζει την πολιτική ιδιωτικότητας που ανακοινώνει.

Μέσα σε παρένθεση αναφέρεται ο αριθμός της απειλής που αντιμετωπίζεται από το κάθε αντίμετρο (Facebook).

a) Χρήση ισχυρών συνθηματικών και υιοθέτηση βέλτιστων πρακτικών διαχείρισής τους (13).

b) Αποσύνδεση του χρήστη από το Facebook όταν δεν το χρησιμοποιεί (13).

c) Έλεγχος της αυθεντικότητας της αρχικής σελίδας σύνδεσης (10,13). Ιδιαίτερη προσοχή απαιτείται στην περίπτωση υπηρεσιών συντόμευσης συνδέσμων (π.χ. tinyurl).

d) Αποφυγή εισαγωγής τμημάτων κώδικα στη διεύθυνση του προγράμματος περιήγησης (10,13).

e) Χρήση αναβαθμισμένων εκδόσεων του περιηγητή και του λογισμικού ασφάλειας (8).

f) Αποφυγή εγκατάστασης και χρήσης εφαρμογών τρίτων που παρέχονται μέσω του Facebook οι οποίες δεν προέρχονται από αξιόπιστες πηγές (9).

g) Χρήση της εφαρμογής «Web Of Trust», ως μέσο άμυνας έναντι συνδέσμων που οδηγούν σε κακόβουλες σελίδες και επιθέσεις clickjacking (8, 10).

h) Χρήση του πρωτοκόλλου SSL για την κρυπτογραφημένη μετάδοση δεδομένων (13).

i) Χρησιμοποίηση συνθηματικών μίας χρήσης, ιδιαίτερα όταν η σύνδεση του χρήστη γίνεται από κοινόχρηστο υπολογιστή (13). Ο χρήστης, εφόσον έχει γνωστοποιήσει στην υπηρεσία το κινητό του τηλέφωνο, μπορεί να αποστείλει τη λέξη «otp» σε έναν πενταψήφιο αριθμό τηλεφώνου προκειμένου να λάβει ένα συνθηματικό χρήσης με διάρκεια ζωής 20 λεπτών.

j) Παρακολούθηση της δραστηριότητας του λογαριασμού (13).

k) Απόρριψη αιτημάτων φιλίας από άγνωστους χρήστες (1,7,11,14,15) .

l) Προσοχή κατά τη δημοσίευση πληροφοριών (1,3,4,5,10,14).

m) Έλεγχος επιπέδου πρόσβασης για την κάθε πληροφορία που δημοσιεύεται, χρησιμοποιώντας των ενσωματωμένο επιλογέα επιπέδου πρόσβασης (1,3,4,5,10,14).

n) Προσοχή σε παράξενες και δελεαστικές δημοσιεύσεις, ακόμα και αν αυτές προέρχονται από Φίλους (7,8,10).

o) Αποφυγή συνδέσμων οι οποίοι οδηγούν σε διεύθυνση διαφορετική από αυτή που εμφανίζεται στο χρήστη, ή που χρησιμοποιούν εικόνες για την αναπαράσταση λεκτικών συνδέσμων (10).

p) Αποφυγή χρήσης του λογαριασμού Facebook για τη σύνδεση σε άλλους ιστότοπους (2).

q) Αναφορά ενός προφίλ για πλαστοπροσωπία, παρενόχληση ή εκφοβισμό (12, 14, 15).

r) Επανάκτηση ενός προφίλ το οποίο έχει δεχτεί πειρατεία (13).

s) Χρήση τεχνικών ανωνυμοποίησης φωτογραφιών, οι οποίες περιορίζουν τη δυνατότητα αυτόματης αναγνώρισης προσώπων, αφαιρώντας της πληροφορίες που είναι απαραίτητες για την αναγνώριση (3,4).

t) Μελέτη της πολιτικής «Ιδιωτικότητας» του Facebook (Όλες).

6.3. Twitter

Το Twitter γνωστή ΕΚΔ, ιδρύθηκε το 2006 και επιτρέπει στους χρήστες του να στέλνουν και να διαβάζουν σύντομα μηνύματα (Tweets) μέχρι 140 χαρακτήρες. Οι κυριότερες απειλές είναι οι ακόλουθες:

1. **Διαρροή προσωπικών δεδομένων και συμπεριφοράς**. Ο χρήστης είτε εσκεμμένα είτε ακούσια μπορεί να αποκαλύψει προσωπικά δεδομένα ή ευαίσθητες πληροφορίες για τον ίδιο ή και για άλλους χρήστες με πιθανά δυσάρεστα αποτελέσματα, όπως για παράδειγμα εγκληματικές ενέργειες, αποκλεισμός από ασφαλιστικές εταιρίες ή ενοχλητική στοχευόμενη διαφήμιση (Huina Mao, Xin Shuai & Apu Kapadia, 2011 · Humphreys, Gill & Krishnamurthy, 2010). Επίσης, η δυνατότητα προώθησης μηνυμάτων (retweeting) αυξάνει τον κίνδυνο αποκάλυψης ευαίσθητων προσωπικών δεδομένων (Meeder, B., Tam, J.. Kelley, P. G. & Cranor, L. F., 2010 · Java, A., Song, X., Finin, T. & Tseng, B., 2007 · Krishnamurthy, B., Gill, P. & Arlitt, M., 2008 · De Cristofaro, E., Soriente, C., Tsudik, G. & Williams, A., 2012).

2. **Εντοπισμός θέσης**. Η δυνατότητα εντοπισμού της ακριβούς τοποθεσίας ενός χρήστη και η παρακολούθησή του ανά πάσα στιγμή.

3. **SPAM**. Αποστολή συνδέσμων σε ιστοσελίδες με διαφημιστικό περιεχόμενο, phishing και ιομορφικό λογισμικό (Griery, Thomas, Paxsony & Zhang, 2010 · Benevenuto, Magno, Rodrigues, & Almeida, 2010 · Irani, Webb, Pu & Li, 2010).

4. **Πειρατεία λογαριασμού**. Ο επιτιθέμενος αποκτά πρόσβαση στον λογαριασμό ενός χρήστη, χρησιμοποιώντας διάφορες τεχνικές και εκμεταλλευόμενος ευπάθειες όπως αδύναμα συνθηματικά και ελλιπή μέτρα προστασίας (Griery, Thomas, Paxsony & Zhang, 2010).

5. **Πλαστοπροσωπία**. Ένας κακόβουλος χρήστης μπορεί να δημιουργήσει λογαριασμό στο Twitter, προβάλλοντας τις ιδιότητες ενός άλλου προσώπου που θέλει να υποδυθεί.

6. **Trolls**. Ανώνυμοι χρήστες με πονηρά προκλητικές, σκόπιμα ανόητες ή επιτηδευμένα εκτός θέματος παρεμβάσεις, με πρωταρχική πρόθεση να προκαλέσουν αλυσίδα αντιδράσεων από άλλους χρήστες. Αποτελεί συνηθισμένο λάθος, ειδικά ανάμεσα στους αρχάριους χρήστες, η προσπάθεια να απαντήσουν σε ή να κάνουν διάλογο με επιθετικά ή αγενή trolls.

Μέσα σε παρένθεση αναφέρεται ο αριθμός της απειλής που αντιμετωπίζεται από το κάθε αντίμετρο.

Προσεκτική αξιολόγηση των πληροφοριών πριν τη δημοσίευσή τους. Αποφυγή κοινοποίησης ευαίσθητων πληροφοριών (1), (2).

a. Χρήση ψευδωνύμων (1), (2), (5), (6).

b. Χρησιμοποίηση των επιλογών ασφάλειας στο μενού ρυθμίσεις (1), (2), (3), (4), (5).

c. Χρήση ισχυρών συνθηματικών και τακτική αλλαγή του κωδικού πρόσβασης (4), (5).

d. Χρήση διαφορετικών συνθηματικών στους λογαριασμούς των Facebook και Twitter (4), (5).

e. Χρήση διαφορετικών λογαριασμών ηλεκτρονικού ταχυδρομείου κατά την εγγραφή στο Facebook και Twitter (4), (5).

f. Χρήση ενημερωμένου λογισμικού προστασίας από ιούς (antivirus, antispam, antispyware) και κατάλληλα παραμετροποιημένου δικτυακού τείχους προστασίας (firewall) με αυστηρή πολιτική ασφάλειας (3), (4), (5).

g. Αγνοήστε τα μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν «ύποπτες» συνδέσεις, καθώς και τα μηνύματα spam στο Twitter (3).

h. Μην εμπιστεύεστε αυτούς που θα ήθελαν να σας ακολουθήσουν χωρίς έλεγχο (1), (3), (5).

i. Μην εγκρίνετε σε εφαρμογές να χρησιμοποιήσουν το λογαριασμό σας χωρίς έλεγχο (1), (2), (3), (4).

j. Αποσύνδεση του χρήστη από το Twitter όταν δεν το χρησιμοποιεί (4).

k. Έλεγχος της πολιτικής ιδιωτικότητας και των όρων χρήσης.

l. Επίγνωση και τακτική ενημέρωση πάνω σε θέματα ασφάλειας και ιδιωτικότητας με στόχο τη δημιουργία μιας κουλτούρας προσανατολισμένη στην ασφάλεια της πληροφορίας. Ιδιαίτερη προσοχή πρέπει να δίνεται στην αγωγή και εκπαίδευση των παιδιών (Όλες).

6.4. Γενικές Οδηγίες

Ένας τακτικός χρήστης υπηρεσιών κοινωνικής δικτύωσης θα πρέπει:

1. Να εξετάζει πάντα όλες τις ρυθμίσεις που παρέχονται από την εκάστοτε εφαρμογή, επιλέγοντας αυτές που παρέχουν το μέγιστο βαθμό προστασίας.

2. Να αξιολογεί τις πληροφορίες και να ελέγχει τα μεταδεδομένα των αρχείων που δημοσιεύει.

3. Να έχει εγκατεστημένο ένα αξιόπιστο αντι-ιομορφικό λογισμικό το οποίο να ενημερώνεται τουλάχιστον καθημερινά.

4. Να έχει εγκατεστημένο ένα δικτυακό τείχος προστασίας (firewall) κατάλληλα παραμετροποιημένο βάσει μιας αυστηρής πολιτικής. Να παρακολουθεί και να ελέγχει τις καταγραφές του συστήματος.

5. Να ενημερώνεται για τις ευπάθειες των ΕΚΔ που χρησιμοποιεί και να αναβαθμίζει τις εκδόσεις του λογισμικού.

6. Να εφαρμόζει τις βέλτιστες πρακτικές για την προστασία του από επιθέσεις κοινωνικής μηχανικής.

7. Να χρησιμοποιεί ισχυρά συνθηματικά και να αλλάζει τακτικά τους κωδικούς πρόσβασης.

8. Να ενημερώνει τους συνανθρώπους στο κοινωνικό του περιβάλλον αναφορικά με τα θέματα ασφάλειας και ιδιωτικότητας, προάγοντας μια κουλτούρα προσανατολισμένη στην προστασία της πληροφορίας.

9. Να αναφέρει στους διαχειριστές συστημάτων και στις αρμόδιες αρχές περιστατικά ασφάλειας και απειλές που πρέπει να αντιμετωπιστούν σε ευρύτερη κλίμακα.

10. Να ελέγχει προσεκτικά την πολιτική ιδιωτικότητας και τους όρους χρήσης μιας ΕΚΔ.

6.5. Συμπεράσματα

Από την παραπάνω ανάλυση γίνεται αντιληπτό, ότι η δημοσίευση ορισμένων τύπων πληροφοριών θέτει σε κίνδυνο την επαγγελματική σταδιοδρομία, τις προσωπικές σχέσεις και την ασφάλεια όσων χρησιμοποιούν ΕΚΔ. Η δημοσίευση εταιρικών δεδομένων μπορεί να έχει σημαντικά αρνητικές επιπτώσεις για την εταιρεία αλλά και

για τον εργαζόμενο που τις δημοσίευσε. Επίσης, ανάρμοστες δημοσιεύσεις ή φωτογραφίες είναι δυνατόν να θέσουν σε κίνδυνο τις σπουδές ή την καριέρα ενός χρήστη, αφού πολλά πανεπιστήμια και εργοδότες ελέγχουν τα προφίλ όσων υποβάλλουν αιτήσεις ή είναι υπάλληλοί τους.

Οι προσωπικές σχέσεις επίσης μπορεί να διαταραχθούν από σχόλια για τα οποία κάποιος μπορεί στη συνέχεια να μετανιώσει. Ακόμα και αν αποσυρθούν αυτά τα σχόλια ή οι φωτογραφίες, μπορεί να είναι πολύ αργά για να επανορθωθεί η ζημιά, αφού δεν υπάρχει η δυνατότητα να ελεγχθεί ποιος τα βλέπει και που τα αναδιανέμει.

Ακόμα και η προσωπική ασφάλεια των χρηστών τίθεται σε κίνδυνο δημοσιεύοντας ορισμένα είδη πληροφοριών. Για παράδειγμα, αποκαλύπτοντας ένας χρήστης ότι θα απουσιάζει από το σπίτι του, ιδιαίτερα αν έχει συμπεριλάβει στο προφίλ του και τη διεύθυνση κατοικίας του, αυξάνει τον κίνδυνο διάρρηξης. Αντίστοιχα, η δημοσίευση φωτογραφιών και λεπτομερειών που αφορούν τα παιδιά ενός χρήστη θέτει πιθανόν σε κίνδυνο την ασφάλειά τους.

Προτείνεται, ως βέλτιστη τακτική ενάντια στις απειλές, η υλοποίηση εκστρατειών ενημέρωσης και ευαισθητοποίησης των χρηστών σε θέματα ασφάλειας και προστασίας της ιδιωτικότητας. Επίσης, ιδιαίτερα σημαντική είναι η ανάπτυξη εξειδικευμένων εργαλείων για την προστασία όσων χρησιμοποιούν ΕΚΔ, όπως για παράδειγμα η αυτοματοποιημένη διαγραφή δευτερευουσών πληροφοριών που συνδέονται με το προφίλ του χρήστη.

Τέλος, προτείνεται η επανεξέταση του κανονιστικού πλαισίου που διέπει τη λειτουργία των ΕΚΔ και η αναθεώρησή του όπου αυτό κρίνεται απαραίτητο, ούτως ώστε να αντιμετωπιστούν ζητήματα όπως η δυνατότητα μεταφοράς ενός προφίλ από μία ΕΚΔ σε μία άλλη.

6.6. Μελέτη Περίπτωσης

Επιλέξτε μία εφαρμογή κοινωνικής δικτύωσης που χρησιμοποιείτε και εξετάστε τους κινδύνους για την ασφάλεια των χρηστών.

6.7. Βιβλιογραφία

- Acquisti, A. and Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. Privacy Enhancing Technologies (PET) Lecture Notes in Computer Science, 4258:36–58.
- ENISA Position Paper No.1 (2007). *Security Issues and Recommendations for Online Social Networks.* European Network and Information Security Agency.
- McDowell, M. and Morda, D. (2011). *Socializing Securely: Using Social Networking Services*. Produced for United States Computer Emergency Readiness Team (US-CERT) by Carnegie Mellon University.
- McCarthy, L., Watson, K. and Weldon-Siviy, D. (2011). *Own Your Space: A Guide to Facebook Security*. Facebook.
- Dinerman, B. (2011). *Social networking and security risks*. GFI White Paper, GFI Software.
- Facebook (2010). *Facebook Privacy & Security Guide*. Secure State and SocialMediaSecurity.com. http://socialmediasecurity.com/downloads/Facebook_Privacy_and_Security_Guide.pdf
- Facebook (2012). *Facebook Security Best Practices*. Sophos. http://www.sophos.com/en-us/security-news-trends/best-practices/facebook.aspx
- Huina Mao, Xin Shuai, Apu Kapadia, (2011). *Loose Tweets: An Analysis of Privacy Leaks on Twitter*. Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, WPES'11, pp. 1-12.
- Humphreys, L., Gill, P. and Krishnamurthy, B. (2010). *How much is too much? Privacy issues on Twitter*. In Conference of International Communication Association, Singapore.
- Meeder, B., Tam, J.. Kelley, P. G. and Cranor, L. F. (2010). *RT@ IWantPrivacy: Widespread violation of privacy settings in the Twitter social network*. In Web 2.0 Privacy and Security Workshop, IEEE Symposium on Security and Privacy.
- Java, A., Song, X., Finin, T. and Tseng, B. (2007). *Why we twitter: understanding microblogging usage and communities*. WebKDD/SNA-KDD '07: Proceedings of

the 9th WebKDD and 1st SNA-KDD 2007 workshop on Web mining and social network analysis. New York, NY, USA: ACM, pp. 56–65.

- Krishnamurthy, B., Gill, P. and Arlitt, M. (2008). *A few chirps about twitter*. WOSP '08: Proceedings of the first workshop on Online social networks. New York, NY, USA: ACM, pp. 19–24.

- Griery, C., Thomas, K., Paxsony V., and Zhang, M. (2010). *@spam: The Underground on 140 Characters or Less*. Proceedings of the 17th ACM conference on Computer and communications security, pp. 27-37.

- Benevenuto, F., Magno, G., Rodrigues, T., and Almeida, V. (2010), *Detecting Spammers on Twitter*. Seventh annual Collaboration, Electronic messaging, AntiAbuse and Spam Conference CEAS.

- Irani, D., Webb, S., Pu, C. and Li, K. (2010). *Study of TrendStuffing on Twitter through Text Classification*. Seventh annual Collaboration, Electronic messaging, AntiAbuse and Spam Conference CEAS.

- De Cristofaro, E., Soriente, C., Tsudik, G., Williams, A. (2012) Hummingbird: privacy at the time of Twitter. 33th IEEE Symposium on Security and Privacy.

7. ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΕΥΡΕΙΑΣ ΚΛΙΜΑΚΑΣ

Τα τελευταία χρόνια έχουν παρουσιαστεί ανησυχητικές περιπτώσεις διάδοσης ιομορφικού λογισμικού, το οποίο έχει τη δυνατότητα να προκαλέσει τη δυσλειτουργία κρίσιμων πληροφοριακών συστημάτων και υποδομών ή να υποκλέψει εμπιστευτικές πληροφορίες και κρατικά μυστικά. Περιστατικά παραβίασης της ασφάλειας εθνικών υποδομών θα μπορούσαν να προκαλέσουν σημαντικές καταστροφές, απώλειες ανθρώπινης ζωής και να οδηγήσουν σε θερμά επεισόδια μεταξύ κρατών με ανυπολόγιστες συνέπειες. Επίσης, η συσχέτιση που υπάρχει μεταξύ των κρίσιμων υποδομών σε εθνικό επίπεδο, η τιμή της οποίας είναι γενικά δύσκολο να εκτιμηθεί, λειτουργεί πολλαπλασιαστικά στο μέγεθος μιας πιθανής επίπτωσης και καθιστά επιτακτική την εύρεση και ανάπτυξη μέτρων προστασίας.

Μεταξύ των κυριότερων κυβερνοεπιθέσεων που εκδηλώθηκαν τα τελευταία χρόνια συγκαταλέγονται οι ακόλουθες περιπτώσεις:

- **WannaCry**. Αποτελεί ίσως τη διασημότερη κυβερνοεπίθεση της δεκαετίας, προσβάλοντας πάνω από 230.000 υπολογιστές σε περισσότερα από 150 κράτη το 2017, στοχεύοντας το λειτουργικό σύστημα των Windows. Το συγκεκριμένο ransomware προκάλεσε σημαντικά προβλήματα στο Εθνικό Σύστημα Υγείας της Αγγλίας. Η ιομορφή κρυπτογραφούσε τα δεδομένα του υπολογιστή ζητώντας Bitcoins.

- **Sony**. Το 2014 σημειώθηκε υποκλοπή δεδομένων από τους εξυπηρετητές της Sony Pictures από τους hackers Guardians of Peace. Τα δεδομένα αφορούσαν προσωπικά στοιχεία εργαζομένων, μηνύματα ηλεκτρονικού ταχυδρομείου, αρχεία μισθοδοσίας και υλικό ταινιών που δεν είχαν ακόμη βγει στην αγορά. Στη συνέχεια οι δράστες ζήτησαν να μην προβληθεί στις αίθουσες η ταινία «The Interview», που αφορούσε τη δολοφονία του ηγέτη της Βόρειας Κορέας.

- **Stuxnet**. Κυβερνοεπίθεση το 2010 με στόχο τα βιομηχανικά συστήματα αυτοματισμού SCADA του πυρηνικού προγράμματος του Ιράν. Η ιομορφή προσβάλει το λειτουργικό σύστημα των Windows με στόχο λογισμικό λειτουργίας των συσκευών φυγοκέντρισης της Siemens. Αρχικά διαδίδεται μέσω USB και εξαπλώνεται μέσω δικτύου.

- **Yahoo**. Το 2016 η εταιρία ανακοίνωσε πως το 2014 σημειώθηκε περιστατικό παραβίασης 500 εκ. λογαριασμών χρηστών. Ο επιτιθέμενος απέσπασε ονόματα χρηστών, κωδικούς πρόσβασης και στοιχεία επικοινωνίας. Η Yahoo προέτρεψε τους χρήστες των υπηρεσιών της να δημιουργήσουν νέους κωδικούς πρόσβασης.

- **Εσθονία**. Κυβερνοεπίθεση DDoS ευρείας κλίμακας στην Εσθονία το 2007, διάρκειας τριών εβδομάδων, με στόχο την πλήρη κατάρρευση των υποδομών του κράτους. Η επίθεση αποδόθηκε στη Ρωσία, ωστόσο δεν ήταν δυνατόν να εξακριβωθεί εάν πίσω από αυτήν βρισκόταν η ρωσική κυβέρνηση ή hackers που έδρασαν αυτόνομα.

Σκοπός της παρούσας ενότητας είναι η αναλυτική παρουσίαση του ιομορφικού λογισμικού Flame, που αποτελεί ένα από τα πιο εξελιγμένα κακόβουλα προγράμματα που έχουν γραφτεί ποτέ. Χρησιμοποιήθηκε ως ένα ολοκληρωμένο εργαλείο διεθνής κατασκοπείας στον κυβερνοχώρο. Μεταδίδεται μέσω τοπικών δικτύων υπολογιστών ή μέσω USB sticks και μπορεί να καταγράψει ήχο, οθόνη, πληκτρολόγηση και δικτυακή κίνηση. Επίσης, μπορεί να καταγράψει συζητήσεις που διεξάγονται μέσω Skype.

Συγκεκριμένα, θα προσδιορισθούν τα ιδιαίτερα χαρακτηριστικά του και θα ταξινομηθεί βάσει των ιδιοτήτων του. Θα γίνει μια διεξοδική μελέτη της συμπεριφοράς και των στοιχείων που έχουν καταγραφεί για τον Flame σε διεθνές επίπεδο με στόχο τη διεξαγωγή πολύτιμων συμπερασμάτων, η αξιοποίηση των οποίων θα μπορέσει να συμβάλει στη σχεδίαση και ανάπτυξη αποτελεσματικών μέτρων αντιμετώπισης. Επίσης, η ανάλυση της δομής, των λειτουργιών και των μηχανισμών που χρησιμοποιήθηκαν για την κατασκευή και εξάπλωσή του, θα οδηγήσει σε τεχνικά συμπεράσματα απαραίτητα για τον προσδιορισμό των κατάλληλων τεχνολογιών για την αποτελεσματική προστασία των πληροφοριακών συστημάτων και δικτύων που υποστηρίζουν κρίσιμες υποδομές από ανάλογες επιθέσεις.

7.1. Ιομορφικό Λογισμικό Flame

Η ραγδαία εξέλιξη των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) έχει συμβάλει αποφασιστικά στην πρόοδο και ανάπτυξη του επιπέδου και της ποιότητας ζωής του ανθρώπου σε όλους τους τομείς δραστηριοτήτων. Ο βαθμός εξάρτησης της λειτουργίας των κρίσιμων υποδομών, στις οποίες στηρίζεται η ύπαρξη και η ευημερία μιας σύγχρονης κοινωνίας, από πληροφορικά συστήματα και δίκτυα δεδομένων, αναδεικνύει την ανάγκη αποτελεσματικής προστασίας από διάφορες απειλές, οι οποίες μπορούν να προέλθουν από καλά οργανωμένες ομάδες οικονομικών συμφερόντων σε διεθνές επίπεδο ή από ξένες μυστικές κρατικές υπηρεσίες, έχοντας ως στόχο την καταστροφή υλικοτεχνικών υποδομών, την αποσταθεροποίηση της οικονομίας, τον εκφοβισμό, ή την υποκλοπή πολύτιμων πληροφοριών.

Η ανακάλυψη του ιομορφικού λογισμικού Flame και ειδικότερα η πολυπλοκότητα και τα ιδιαίτερα χαρακτηριστικά του, αποδεικνύουν περίτρανα ότι το διαδίκτυο αποτελεί πλέον το πέμπτο πεδίο συγκρούσεων και επίδειξης ισχύος σε διεθνή κλίμακα, το

οποίο έρχεται να προστεθεί στα τέσσερα παραδοσιακά πεδία πολεμικών επιχειρήσεων: ξηρά, θάλασσα, αέρας και διάστημα. Οι ικανότητες, η οργάνωση, τα κίνητρα, η τεχνογνωσία και οι πόροι που απαιτούνται για τη σχεδίαση και ανάπτυξη ιομορφικού λογισμικού ανάλογου επιπέδου, το οποίο να μπορεί να χρησιμοποιηθεί σε γεωγραφικά και εθνικά στοχευόμενες επιθέσεις και κατασκοπεία, υποδεικνύουν ότι απαιτείται μια νέα μεθοδολογική προσέγγιση στην προστασία της πληροφορίας η οποία θα πρέπει να περιλαμβάνει διαφορετικές διαστάσεις σε πολιτικό, νομικό, οργανωτικό και τεχνολογικό επίπεδο.

Ο Flame αποκαλύφθηκε το Μάιο του 2012 όταν η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union – ITU), η οποία είναι η ειδικευμένη υπηρεσία του ΟΗΕ υπεύθυνη για τις ΤΠΕ, ζήτησε από την εταιρία Kaspersky να εξετάσει αναφορές από χώρες της Μέσης Ανατολής σχετικά με περιστατικά προσβολής της ασφάλειας πληροφοριακών συστημάτων από ιομορφικό λογισμικό. Οι ερευνητές της Kaspersky ονόμασαν την ιομορφή που εντόπισαν Flame από το όνομα μίας από τις κύριες λειτουργικές της μονάδες. Υπολογίζεται ότι ο Flame χρησιμοποιήθηκε αρχικά το 2010, αλλά οι δημιουργοί του συνεχίζουν έως σήμερα την ανάπτυξη διαφόρων τμημάτων του κώδικα διατηρώντας την ίδια αρχιτεκτονική. Επίσης, φαίνεται ότι η ανάπτυξη της πλατφόρμας του κώδικα των Command & Control (C&C) servers ξεκίνησε το 2006 (Gostev, 2012a).

7.2. Ανάλυση Χαρακτηριστικών και Ταξινόμηση

Ο Flame είναι ένα εργαλείο κατασκοπείας στον κυβερνοχώρο, το οποίο δίνει τη δυνατότητα στον επιτιθέμενο να υποκλέψει μία πληθώρα δεδομένων από το στόχο του. Τα κύρια χαρακτηριστικά του είναι τα ακόλουθα (Bencsáth, Pék, Buttyán & Félegyházi, 2012 · Bit9 Threat Advisor, 2012 · Gostev, 2012a · sKyWIper Analysis Team, 2012 · Symantec Official Blog, 2012 · Symantec Security Response, 2012):

1. Διαθέτει μία αρθρωτή δομή που περιλαμβάνει μία πλούσια συλλογή τεχνολογιών κατασκοπείας σε μία και μόνο ιομορφή.

2. Στοχεύει σε συστήματα με λειτουργικό σύστημα Microsoft Windows και ενσωματώνει πολλαπλές τεχνικές διάδοσης, επίθεσης και ενσωμάτωσης κώδικα.

3. Έχει τη δυνατότητα αποτύπωσης πληκτρολογήσεων, στιγμιότυπων της οθόνης ανά τακτά χρονικά διαστήματα ανάλογα με την εφαρμογή που χρησιμοποιεί το θύμα, ενεργοποίησης του μικροφώνου και της κάμερας του υπολογιστή στόχου για την καταγραφή ήχου και εικόνας, καθώς και αναζήτησης στα αποθηκευτικά μέσα συνδεδεμένα με τον υπολογιστή.

4. Έχει τη δυνατότητα παρακολούθησης και αποτύπωσης της δικτυακής κίνησης, προκειμένου να υποκλέψει διακινούμενους κωδικούς και συνθηματικά λογαριασμών.

5. Είναι σε θέση να ενεργοποιήσει τον πομποδέκτη Bluetooth, προκειμένου να καταγράψει τις παρακείμενες ενεργοποιημένες συσκευές Bluetooth. Επιπρόσθετα, δίνει τη δυνατότητα χρησιμοποίησης του Bluetooth για την αποστολή δεδομένων σε μία παρακείμενη συσκευή Bluetooth η οποία ελέγχεται από τον επιτιθέμενο.

6. Λόγω του ότι καταλαμβάνει μεγάλο χώρο στο δίσκο, προστίθεται στο σύστημα στόχο τμηματικά. Το κύριο συστατικό του που προσβάλει ένα σύστημα έχει μέγεθος 6 MB και περιλαμβάνει μία σειρά από λειτουργικές μονάδες σε συμπιεσμένη μορφή. Μετά την εγκατάσταση του κύριου συστατικού στο σύστημα, αυτό αποκρυπτογραφεί και αποσυμπιέζει τις λειτουργικές μονάδες που περιλαμβάνει και τις τοποθετεί σε διάφορα σημεία του δίσκου. Ο αριθμός των λειτουργικών μονάδων της κάθε μόλυνσης εξαρτάται από τους σκοπούς της παρακολούθησης του κάθε στόχου. Στην πλήρη ανάπτυξή της η ιομορφή μπορεί να φτάσει έως και τα 20 MB.

7. Χρησιμοποιεί τεχνικές συμπίεσης και κρυπτογράφησης προκειμένου να αποκρύψει τα αρχεία του. Συγκεκριμένα, έχουν εντοπιστεί 5 διαφορετικές μέθοδοι κρυπτογράφησης (και παραλλαγές τους), 3 διαφορετικές τεχνικές συμπίεσης και τουλάχιστον 5 διαφορετικές μορφές αρχείων.

8. Χρησιμοποιεί βάσεις δεδομένων SQLite και τις άγνωστες βάσεις δεδομένων CLAN, για την αποθήκευση ορισμένων από τις πληροφορίες που συγκεντρώνει.

9. Χρησιμοποιεί μηχανισμούς ενσωμάτωσης κώδικα στις εκτελούμενες διεργασίες του συστήματος (όπως winlogon, services και explorer), οι οποίες δεν επιτρέπουν τον εντοπισμό του ενσωματωμένου κώδικα με τη χρήση κλασσικών μεθόδων, όπως την απαρίθμηση των λειτουργικών μονάδων της κάθε διεργασίας. Ταυτόχρονα οι σελίδες της μνήμης που χρησιμοποιεί είναι προστατευμένες με δικαιώματα READ, WRITE και EXECUTE έτσι ώστε να είναι απροσπέλαστες από τις εφαρμογές των χρηστών.

10. Ελέγχει την παρουσία περισσοτέρων από 300 προϊόντων ασφάλειας τα οποία θα μπορούσαν να τον ανιχνεύσουν και τροποποιεί ανάλογα τη συμπεριφορά του, έτσι ώστε να αποφευχθεί ο εντοπισμός του. Για παράδειγμα, ενώ συνήθως χρησιμοποιεί την επέκταση .ocx, στην περίπτωση που είναι εγκατεστημένο το McAfee Shield αλλάζει τις επεκτάσεις των αρχείων του σε .tmp.

11. Διαθέτει ποικίλες μορφές αυτοαναπαραγωγής και εξάπλωσης σε τοπικά δίκτυα και USB sticks, οι οποίες περιγράφονται στη συνέχεια αναλυτικά.

12. Δημιουργεί λογαριασμούς κερκόπορτες στους μολυσμένους υπολογιστές, εφόσον είναι διαθέσιμα τα απαραίτητα δικαιώματα.

13. Τα δεδομένα που συγκεντρώνει αποστέλλονται κρυπτογραφημένα σε απομακρυσμένους Command & Control (C&C) Servers χρησιμοποιώντας το πρωτόκολλο SSL, εφόσον υπάρχει διαθέσιμη διαδικτυακή σύνδεση. Σε αντίθετη περίπτωση, τα συγκεντρωμένα δεδομένα μπορούν να αποσταλούν σε USB sticks, μέσω των οποίων μπορούν να μολυνθούν άλλοι υπολογιστές των οποίων η διαδικτυακή σύνδεση χρησιμοποιείται για την επικοινωνία με τους C&C Servers. Ο κώδικας της ιομορφής περιλαμβάνει μία προκαθορισμένη λίστα C&C τομέων, καθώς και μία δυναμική λίστα στην οποία οι επιτιθέμενοι μπορούν να προσθέσουν νέους τομείς στην περίπτωση που οι αρχικοί τομείς εγκαταλειφθούν.

14. Αξιοποιεί την scripting γλώσσα προγραμματισμού LUA για τη συγγραφή τμημάτων της ιομορφής και ενσωματώνει έναν διερμηνέα της γλώσσας, που επιτρέπει στους επιτιθέμενους να εμπλουτίσουν την λειτουργικότητά της μέσω διαφόρων scripts τα οποία αποστέλλονται από τους C&C Servers στους μολυσμένους υπολογιστές.

15. Οι επιτιθέμενοι είναι σε θέση να αποστείλουν μία λειτουργική μονάδα “αυτοκτονίας” της ιομορφής, στην περίπτωση που αυτό καταστεί αναγκαίο. Η λειτουργική αυτή μονάδα (browse32) εντοπίζει όλα τα ίχνη της ιομορφής, περιλαμβανομένων των αρχείων που περιλαμβάνουν τα δεδομένα που έχουν υποκλαπεί, και τα καταστρέφει.

Οι λειτουργικές μονάδες που περιλαμβάνει ο Flame έχουν τη δυνατότητα να συγκεντρώσουν έναν εξαιρετικά μεγάλο όγκο πληροφοριών από τον υπολογιστή που έχει προσβάλει, ο οποίος υπερβαίνει κατά πολύ τον όγκο πληροφοριών που μπορεί να συγκεντρωθεί από ιομορφές του παρελθόντος. Επίσης, δίνεται η δυνατότητα στον επιτιθέμενο να συλλέξει ορισμένες πρώτες πληροφορίες ούτως ώστε να προχωρήσει στη συνέχεια στη συλλογή περισσότερων στοιχείων. Για παράδειγμα, ο Flame μπορεί να συλλέξει μεταδεδομένα αρχείων και στη συνέχεια ο επιτιθέμενος, βάσει αυτών των πληροφοριών, να επιλέξει να υποκλέψει μόνο τα αρχεία που τον ενδιαφέρουν. Το τεράστιο εύρος των λειτουργιών και το μέγεθός του τον κάνει να ξεχωρίζει από άλλα εργαλεία κατασκοπείας.

Η αρχική εστία μόλυνσης δεν έχει έως τώρα εντοπιστεί. Συνεπώς, δεν είναι γνωστή η μέθοδος που χρησιμοποιήθηκε για τη μόλυνση του πρώτου υπολογιστή. Από τη στιγμή όμως που θα μολύνει έναν υπολογιστή, διαθέτει ποικίλες μορφές αυτοαναπαραγωγής και εξάπλωσης σε τοπικά δίκτυα και USB sticks. Για τη μόλυνση μέσω USB sticks χρησιμοποιεί τις μεθόδους Autorun (Autorun.inf) και Euphoria (MS10-046). Για την εξάπλωσή του σε τοπικά δίκτυα χρησιμοποιεί την ευπάθεια MS10-061 που εμφανίζεται σε υπολογιστές με διαμοιραζόμενο εκτυπωτή,

απομακρυσμένες εργασίες ή εφόσον εκτελείται από ένα χρήστη που διαθέτει δικαιώματα διαχειριστή τομέα, μπορεί να επιτεθεί εναντίον άλλων υπολογιστών του δικτύου, δημιουργώντας λογαριασμούς με προκαθορισμένο συνθηματικό που θα χρησιμοποιηθούν στη συνέχεια ως κερκόπορτα για την αντιγραφή του.

Η εξάπλωσή του Flame δεν πραγματοποιείται αυτόματα. Οι μηχανισμοί εξάπλωσης είναι εξ' ορισμού απενεργοποιημένοι και πρέπει να ενεργοποιηθούν από τους επιτιθέμενους κατά παραγγελία. Στόχος αυτού του χαρακτηριστικού είναι η ελεγχόμενη εξάπλωση και η μείωση της πιθανότητας εντοπισμού.

Εκτός από τις παραπάνω μεθόδους εξάπλωσης, ο Flame είναι σε θέση να μετατρέψει έναν μολυσμένο υπολογιστή σε ένα πλαστό proxy server για το μηχανισμό Windows Update. Με αυτό τον τρόπο οι υπολογιστές του τοπικού δικτύου προσπαθούν να αποκτήσουν ενημερώσεις των Windows από τον μολυσμένο υπολογιστή, ο οποίος αντί αυτών των ενημερώσεων τους αποστέλλει την ιομορφή.

Όπως προαναφέρθηκε, ο Flame είναι σε θέση να υποδυθεί έναν proxy server για το μηχανισμό Windows Update και έτσι να μεταδοθεί σε ένα τοπικό δίκτυο ως μία υπογεγραμμένη ενημέρωση του λειτουργικού συστήματος Windows. Για την επιτυχία της επίθεσης, το πρόγραμμα που εγκαθιστά την ιομορφή θα πρέπει να είναι ψηφιακά υπογεγραμμένο από τη Microsoft. Οι επιτιθέμενοι χρησιμοποίησαν μία τεχνική με την οποία δημιούργησαν ένα ιδιωτικό κλειδί υπογραφής και ένα πλαστό πιστοποιητικό για το αντίστοιχο δημόσιο κλειδί, το οποίο οδηγεί ιεραρχικά στην Αρχή Πιστοποίησης Ρίζας της Microsoft και μπορεί να χρησιμοποιηθεί για την επαλήθευση της ψηφιακής υπογραφής του κώδικα.

Για τη δημιουργία πλαστού ψηφιακού πιστοποιητικού, οι επιτιθέμενοι χρησιμοποίησαν την υποδομή Microsoft Terminal Services Licensing, η οποία επιτρέπει στους Licensing Servers να αποκτήσουν, με μία πλήρως αυτοματοποιημένη διαδικασία, ένα ψηφιακό πιστοποιητικό από έναν Activation Server της Microsoft. Βάσει αυτής της διαδικασίας, ο Licensing Server δημιουργεί ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού και αποστέλλει στον Activation Server το δημόσιο κλειδί και τις επιπρόσθετες πληροφορίες που απαιτούνται για τη δημιουργία ενός πιστοποιητικού. Ο Licensing Server είναι στη συνέχεια σε θέση να χρησιμοποιήσει το ιδιωτικό κλειδί για την υπογραφή αδειών χρήσης για τους clients, προκειμένου αυτοί να μπορούν να έχουν πρόσβαση σε διάφορες υπηρεσίες τερματικών σταθμών. Η εγκυρότητα των αδειών μπορεί να επαληθευθεί μέσω του ελέγχου της υπογραφής του Licensing Server και του πιστοποιητικού που αποκτήθηκε από τον Activation Server (Bencsáth, Pék, Buttyán & Félegyházi, 2012 · Sotirov, 2012).

Ο παραπάνω μηχανισμός έχει δύο αδυναμίες που εκμεταλλεύτηκαν οι επιτιθέμενοι:

1. Η υπογραφή που περιλαμβάνεται στο πιστοποιητικό που εκδίδεται από τον Activation Server παράγεται χρησιμοποιώντας τη συνάρτηση σύνοψης MD5, η οποία είναι αποδεδειγμένα ευάλωτη σε επιθέσεις σύγκρουσης.

2. Το πιστοποιητικό που εκδίδεται από τον Activation Server δεν περιλαμβάνει επεκτάσεις οι οποίες να περιορίζουν τους τρόπους χρήσης του ιδιωτικού κλειδιού, με αποτέλεσμα να είναι δυνατό να χρησιμοποιηθεί για την υπογραφή κώδικα.

Ωστόσο, το παραγόμενο πιστοποιητικό περιλαμβάνει ορισμένες επεκτάσεις MS Hydra οι οποίες είναι χαρακτηρισμένες ως κρίσιμες και οι οποίες δεν υποστηρίζονται από τα λειτουργικά συστήματα Windows Vista και Windows 7. Προκειμένου να ξεπεράσουν αυτό το εμπόδιο, οι επιτιθέμενοι εκμεταλλεύτηκαν την αδυναμία της συνάρτησης σύνοψης MD5 πραγματοποιώντας μία επίθεση σύγκρουσης επιλεγμένου προθέματος (chosen-prefix collision attack). Μέσω αυτής της επίθεσης απέκτησαν μία έγκυρη υπογραφή από τον Activation Server της Microsoft επί ενός χαλκευμένου πιστοποιητικού, το οποίο περιελάμβανε ένα δημόσιο κλειδί του οποίου το αντίστοιχο ιδιωτικό κλειδί ήταν γνωστό στους επιτιθέμενους και στο οποίο οι επεκτάσεις Hydra είχαν υπερκαλυφθεί από ένα ασυνήθιστα μεγάλο πεδίο IssuerUniqueID. Έτσι, κατά την επαλήθευση του πλαστού πιστοποιητικού δεν γινόταν αντιληπτή η παρουσία των επεκτάσεων Hydra και το πιστοποιητικό μπορούσε να χρησιμοποιηθεί για την υπογραφή εφαρμογών ακόμα και σε λειτουργικά συστήματα Windows Vista και Windows 7 (Bencsáth, Pék, Buttyán & Félegyházi, 2012 · Sotirov, 2012).

Ο στόχος μίας επίθεσης σύγκρουσης σε μία συνάρτηση σύνοψης είναι η παραγωγή της ίδιας σύνοψης από δύο διαφορετικές εισόδους της συνάρτησης. Στην περίπτωση της επίθεσης σύγκρουσης επιλεγμένου προθέματος, ο επιτιθέμενος ξεκινά με δύο επιλεγμένες εισόδους που έχουν γνωστές διαφορές και στη συνέχεια προσθέτει και στις δύο περαιτέρω πληροφορίες (γνωστές ως near collision blocks), έως ότου οι τροποποιημένες είσοδοι οδηγήσουν στην ίδια σύνοψη. Στη συνέχεια, μπορεί ο επιτιθέμενος αν το επιθυμεί, να επεκτείνει τις δύο συγκρουόμενες εισόδους, προσθέτοντας τις ίδιες επιπρόσθετες πληροφορίες. Η συνάρτηση MD5 που χρησιμοποιούσε η Microsoft ήταν γνωστό ήδη από το 2008 ότι είναι ευάλωτη σε αυτού του τύπου τις επιθέσεις (Stevens, 2012 · Sotirov, Stevens, Appelbaum, Lenstra, Molnar, Osvik, De Weger, 2008).

Στην περίπτωση του Flame, οι δύο είσοδοι ήταν δύο πιστοποιητικά. Το πρώτο περιελάμβανε έναν σειριακό αριθμό, την περίοδο ισχύος, το λεκτικό “MS” ως το όνομα του υποκειμένου του πιστοποιητικού και το δημόσιο κλειδί του επιτιθέμενου ως επιλεγμένο πρόθεμα. Το αδόμητο και μεγάλο πεδίο IssuerUniqueID χρησιμοποιήθηκε για την προσθήκη των near collision blocks. Το δεύτερο πιστοποιητικό περιελάμβανε και αυτό έναν σειριακό αριθμό και την περίοδο ισχύος, το λεκτικό “Terminal Services LS” ως το όνομα του υποκειμένου του πιστοποιητικού και τμήμα ενός τυχαίου δημόσιου κλειδιού ως επιλεγμένο πρόθεμα. Το υπόλοιπο τμήμα του δημόσιου κλειδιού χρησιμοποιήθηκε για τα near collision blocks. Τελικά, και τα δύο πιστοποιητικά περιελάμβαναν τις επεκτάσεις Hydra, αλλά στο πρώτο

πιστοποιητικό το μήκος του IssuerUniqueID ήταν τέτοιο που υπερκάλυπτε αυτές τις επεκτάσεις (Bencsáth, Pék, Buttyán & Félegyházi, 2012 · Sotirov, 2012).

Μετά την εύρεση ενός συγκρουόμενου ζεύγους πιστοποιητικών, οι επιτιθέμενοι έστειλαν στον Activation Server ένα αίτημα έκδοσης πιστοποιητικού, χρησιμοποιώντας το τυχαίο δημόσιο κλειδί του δεύτερου πιστοποιητικού. Ο Activation Server δημιούργησε αυτό το δεύτερο πιστοποιητικό προσθέτοντας έναν σειριακό αριθμό και μία περίοδο ισχύος που κατάφεραν να προβλέψουν οι επιτιθέμενοι, τις επεκτάσεις Hydra και την υπογραφή επί της σύνοψης MD5. Ωστόσο, εφόσον το πρώτο και το δεύτερο πιστοποιητικό είχαν την ίδια σύνοψη MD5, η υπογραφή του δεύτερου πιστοποιητικού ήταν έγκυρη και για το πρώτο, το οποίο οι επιτιθέμενοι ήταν σε θέση να χρησιμοποιήσουν για την υπογραφή της ιομορφής (Bencsáth, Pék, Buttyán & Félegyházi, 2012 · Sotirov, 2012).

Η μεγαλύτερη πρόκληση που είχαν να αντιμετωπίσουν οι επιτιθέμενοι ήταν να καταφέρουν να στείλουν το αίτημα έκδοσης πιστοποιητικού την κατάλληλη στιγμή, έτσι ώστε ο server να δημιουργήσει ένα πιστοποιητικό με το σειριακό αριθμό και την περίοδο ισχύος που χρησιμοποίησαν κατά την επίθεση σύγκρουσης. Τόσο ο σειριακός αριθμός όσο και η περίοδος ισχύος εξαρτώνται από το χρόνο παραλαβής του αιτήματος, και με δεδομένο τον τρόπο υπολογισμού τους οι επιτιθέμενοι είχαν ένα χρονικό διάστημα διάρκειας ενός χιλιοστού του δευτερολέπτου για την αποστολή του αιτήματος. Είναι συνεπώς πολύ πιθανό το να χρειάστηκε να πραγματοποιήσουν πολλές προσπάθειες έως ότου το επιτύχουν και για κάθε προσπάθεια θα έπρεπε να παράγουν ένα διαφορετικό ζεύγος σύγκρουσης. Το συμπέρασμα είναι ότι οι επιτιθέμενοι είτε έχουν στη διάθεσή τους εξαιρετικά μεγάλη υπολογιστική ισχύ είτε έχουν στην κατοχή τους μία νέα και γρήγορη μέθοδο παραγωγής συγκρούσεων MD5. Κρυπτογράφοι ερευνητές επιβεβαιώνουν ότι η επίθεση σύγκρουσης επιλεγμένου προθέματος που χρησιμοποιήθηκε για το Flame έγινε χρησιμοποιώντας μία νέα άγνωστη παραλλαγή της έως τώρα γνωστής μεθόδου (Bencsáth, Pék, Buttyán & Félegyházi, 2012 · Sotirov, 2012 · Stevens, 2012).

Ο Flame διαθέτει τρεις λειτουργικές μονάδες που εμπλέκονται στην εξάπλωσή του μέσω του μηχανισμού Windows Update. Αυτά είναι τα SNACK, MUNCH και GADGET.

Ο Internet Explorer κατά την εκκίνησή του χρησιμοποιεί το πρωτόκολλο WPAD (Web Proxy Auto-Discovery Protocol) προκειμένου να ενημερωθεί για τις ρυθμίσεις proxy του τομέα στον οποίο ανήκει. Εάν για παράδειγμα το όνομα του υπολογιστή είναι computerX.ds.unipi.gr, ο Internet Explorer θα ζητήσει ένα αρχείο ρυθμίσεων wpad.dat από τον υπολογιστή wpad.ds.unipi.gr ή wpad.unipi.gr. Αν ο DNS Server δεν διαθέτει αυτές τις εγγραφές, ο Internet Explorer θα χρησιμοποιήσει το WINS ή το NetBIOS για την επίλυση αυτών των ονομάτων. Το SNACK ανιχνεύει τα αιτήματα WPAD, υποδύεται τον WPAD server και παρέχει ένα πλαστό αρχείο wpad.dat. Έτσι, ο υπολογιστής που λαμβάνει αυτό το αρχείο, ορίζει ως proxy τον μολυσμένο υπολογιστή και όλη η διαδικτυακή του κίνηση ανακατευθύνεται προς αυτόν (Symantec Official Blog, 2012).

Το MUNCH είναι ένας Web Server του Flame που λαμβάνει την ανακατευθυνόμενη κίνηση και ελέγχει για αιτήματα Windows Update, οπότε και αποστέλλει με τη βοήθεια του GADGET το φαινομενικά υπογεγραμμένο από τη Microsoft εκτελέσιμο TumblerEXE.exe, το οποίο και εκτελείται. Το Tumbler πραγματοποιεί ορισμένους ελέγχους, συμπεριλαμβανομένων των ελέγχων ύπαρξης λογισμικού ασφαλείας και επικοινωνεί με το MUNCH του πλαστού proxy, προκειμένου να λάβει το αρχείο mssecmgr.ocx. Με τη λήψη και εκτέλεση αυτού του αρχείου ο υπολογιστής μολύνεται από τον Flame (Symantec Official Blog, 2012).

Ο Flame είναι μία καλοσχεδιασμένη πλατφόρμα η οποία περιλαμβάνει μία πληθώρα λειτουργικών μονάδων. Τα άρθρα (Antiy Labs, 2012 · Bencsáth, Pék, Buttyán & Félegyházi, 2012 · sKyWIper Analysis Team, 2012) περιλαμβάνουν μία εκτενή λίστα με τις περίπου 20 λειτουργικές μονάδες και τα αρχεία του Flame που έχουν μελετηθεί έως σήμερα. Η βασικότερη λειτουργική μονάδα του είναι το mssecmgr.ocx, που αποτελεί το πρώτο στοιχείο της ιομορφής που εκτελείται σε έναν υπολογιστή. Το αρχείο αυτό περιλαμβάνει ένα μεγάλο αριθμό επιμέρους υπομονάδων.

Οι περισσότερες υπομονάδες, συμπεριλαμβανομένων των διαφόρων scripts, είναι αποθηκευμένες σε ένα κρυπτογραφημένο τμήμα του mssecmgr.ocx, το οποίο στην αρχή του περιλαμβάνει ένα ευρετήριο για τη γρήγορη αναζήτησή τους. Εκτός αυτού του κρυπτογραφημένου τμήματος υπάρχουν τμήματα κώδικα τα οποία υλοποιούν έναν HTTP Server, έναν SOCKS Proxy, SSH, DB Server και τον διερμηνέα της γλώσσας LUA (Symantec Official Blog, 2012).

Το msgsecmgr.ocx μπορεί να ενεργοποιηθεί με δύο διαφορετικές μεθόδους (sKyWIper Analysis Team, 2012):

1. Τροποποιώντας το registry έτσι ώστε κατά την εκκίνηση του συστήματος να φορτώνεται το msgsecmgr.ocx, ως τμήμα της διαδικασίας αυθεντικοποίησης

2. Εκτελώντας την κύρια λειτουργική του μονάδα msgsecmgr.ocx, χρησιμοποιώντας το rundll32 και την παρακάτω εντολή: start /wait rundll32.exe c:\windows\system32\mssecmgr.ocx,DDEnumCallback

Κατά την εκκίνηση του συστήματος και την αυθεντικοποίηση του χρήστη, το mssecmgr.ocx φορτώνεται ως LSA (Local Security Authority) Authentication Package. Στη συνέχεια χρησιμοποιεί διάφορες περίπλοκες τεχνικές προκειμένου να ενσωματωθεί στις εκτελούμενες διεργασίες.

Αρχικά αποσυμπιέζει και εκτελεί το advnetcfg.ocx. Στη συνέχεια, το mssecmgr.ocx περνά το nteps32.ocx στο advnetcfg.ocx, το οποίο με τη σειρά του ενσωματώνει το nteps32.ocx στην εκτελούμενη διεργασία του shell32.dll. Στη συνέχεια, το mssecmgr.ocx ξεκινά το βασικό LUA script, το οποίο ελέγχει αν πρέπει να κατεβάσει

κάποια νέα ή ενημερωμένη λειτουργική μονάδα από τους C&C Servers, δημιουργεί διάφορα αρχεία βάσεων δεδομένων για την αποθήκευση δεδομένων υποκλοπής και εκκινεί διάφορες άλλες λειτουργικές μονάδες (Symantec Official Blog, 2012).

Οι C&C Servers διαθέτουν μία διαδικτυακή εφαρμογή που ονομάζεται Newsforyou. Η εφαρμογή διαχειρίζεται την αλληλεπίδραση με τον Flame και διαθέτει μία απλή κονσόλα διαχείρισης που επιτρέπει στους επιτιθέμενους να ανεβάζουν καινούργια πακέτα κώδικα, να τα προωθούν στους μολυσμένους υπολογιστές, αλλά και να κατεβάζουν πακέτα με δεδομένα υποκλοπής. Η εφαρμογή αυτή δε φαίνεται να χρησιμοποιείται μόνο από τον Flame, καθώς περιλαμβάνει λειτουργικότητα η οποία επιτρέπει την επικοινωνία με υπολογιστές οι οποίοι έχουν μολυνθεί από ιομορφές οι οποίες χρησιμοποιούν διαφορετικά πρωτόκολλα. Μάλιστα, από τα πρωτόκολλα και τους τύπους clients που βρέθηκαν να υποστηρίζονται, διαπιστώνεται ότι πρέπει να υπάρχει μία ακόμα ενεργή ιομορφή η οποία παραμένει άγνωστη (Symantec Security Response, 2012).

Η εξέταση των C&C Servers παρείχε χρήσιμες πληροφορίες όχι μόνο για την αρχιτεκτονική της ιομορφής, αλλά και για την οργανωτική δομή των επιτιθέμενων. Διαπιστώθηκε ότι ο κώδικας των C&C Servers γράφτηκε και συντηρήθηκε από τουλάχιστον τέσσερα άτομα, γεγονός που καταδεικνύει μία συνεχή προσπάθεια υποστήριξης του Flame, καθώς και πιθανών νέων απειλών παρόμοιας φύσης. Η ανάπτυξη του λογισμικού τους διήρκησε πολλά χρόνια, ξεκινώντας πιθανότατα από το 2006, αρκετό δηλαδή διάστημα πριν από την πρώτη γνωστή μεταγλώττιση του Flame που έγινε το 2010 (Symantec Security Response, 2012).

Επίσης, η οργάνωση του συστήματος είναι τέτοια που υποστηρίζει μία σαφή διάκριση ρόλων. Οι ρόλοι που αναγνωρίστηκαν είναι οι εξής (Symantec Security Response, 2012):

- Διαχειριστές, με αρμοδιότητα την εγκατάσταση του server.
- Χειριστές, με αρμοδιότητα την προσθήκη λειτουργικών μονάδων και λήψη των δεδομένων υποκλοπής, χωρίς όμως να είναι σε θέση να τα αποκρυπτογραφήσουν.
- Συντονιστές, οι οποίοι κατείχαν το ιδιωτικό κλειδί και είχαν τη δυνατότητα να αποκρυπτογραφήσουν τα δεδομένα υποκλοπής.

Από αυτή τη σαφή διάκριση ρόλων γίνεται φανερό ότι πίσω από τον Flame βρίσκεται μία εξαιρετικά ιεραρχικά οργανωμένη ομάδα. Το γεγονός αυτό, σε συνδυασμό με τη διαπίστωση ότι ο μηχανισμός Windows Update παραβιάστηκε από έμπειρους κρυπταναλυτές, ενισχύει την άποψη ότι ο Flame είναι αποτέλεσμα εργασίας μίας μεγάλης και καλά χρηματοδοτούμενης ομάδας.

Βάσει των παραπάνω χαρακτηριστικών, προκύπτει το συμπέρασμα ότι ο Flame μπορεί να ταξινομηθεί κυρίως ως Αναπαραγωγός, λόγω του ότι διαθέτει το χαρακτηριστικό της αυτοαναπαραγωγής, ενώ ταυτόχρονα δεν απαιτείται για την αναπαραγωγή του η ενεργοποίηση κάποιου άλλου λογικού αντικειμένου (ξενιστής). Ταυτόχρονα όμως εξαιτίας της δυνατότητάς του να δημιουργεί λογαριασμούς κερκόπορτες, διαθέτει και τα χαρακτηριστικά κερκόπορτας, ενώ η δυνατότητα που έχει να εξαπλώνεται μέσω της παραβίασης του μηχανισμού Windows Update του προσδίδει και τα χαρακτηριστικά Δούρειου Ίππου.

7.3. Συμπεράσματα

Ο Flame επιβεβαίωσε ότι οι παραδοσιακοί μηχανισμοί και μέτρα ασφάλειας δεν επαρκούν για την προστασία της πληροφορίας από προηγμένες στοχευόμενες επιθέσεις. Στη συνέχεια αναλύονται τα συμπεράσματα που προκύπτουν από τη μελέτη του Flame, καθώς και τα μέτρα που θα μπορούσαν να ληφθούν για την αντιμετώπιση ανάλογων ιομορφών.

Ο Flame είναι προϊόν μιας νέας εποχής που ανατέλει στο χώρο του κυβερνοπολέμου. Πρόκειται για μία ιομορφή η οποία είναι 40 φορές μεγαλύτερη από τον Stuxnet, ο οποίος θεωρούνταν το πιο προηγμένο ιομορφικό λογισμικό που έχει εμφανιστεί. Ο Stuxnet εντοπίστηκε περίπου δύο χρόνια πριν από τον Flame και αν και διαπιστώθηκε ότι χρησιμοποιεί διαφορετική πλατφόρμα από τον Flame, εντούτοις βρέθηκε τουλάχιστον μία λειτουργική μονάδα η οποία ήταν κοινή και στις δύο ιομορφές. Από την έως τώρα ανάλυση των δύο ιομορφών προκύπτει το συμπέρασμα ότι οι ομάδες ανάπτυξής τους είναι διαφορετικές και η κάθε ομάδα ανέπτυσσε ανεξάρτητα την πλατφόρμα της, έως περίπου το 2007-2008. Το 2009, μέρος του πηγαίου κώδικα της πλατφόρμας του Flame χρησιμοποιήθηκε από το Stuxnet. Από το 2010 και μετά οι δύο πλατφόρμες αναπτύχθηκαν ανεξάρτητα, αν και αξιοποιήθηκαν και από τις δύο κοινές ευπάθειες. Με βάση τα παραπάνω, προκύπτει το συμπέρασμα ότι πρόκειται για δύο έργα τα οποία εκτελέστηκαν παράλληλα, από διαφορετικές ομάδες αλλά πιθανότητα από κοινό συντονιστή (Gostev, 2012b).

Ο Flame είναι μία χαρακτηριστική περίπτωση ανάδειξης της ανεπάρκειας που διακρίνει τα παραδοσιακά συστήματα ασφάλειας, τουλάχιστον όταν πρόκειται για την προστασία κρίσιμων υποδομών. Το κυβερνοέγκλημα εξελίσσεται διαρκώς και επινοεί νέους τρόπους παράκαμψης των μηχανισμών ασφάλειας. Οποιαδήποτε ιομορφή είναι καινούργια και άγνωστη, είναι πολύ πιθανό να καταφέρει να παρακάμψει τα παραδοσιακά συστήματα ασφάλειας. Στην περίπτωση μάλιστα του Flame υπήρχε επιπλέον η εγγύηση της ηλεκτρονικής υπογραφής της Microsoft. Η πρακτική της λήψης μέτρων προστασίας κατόπιν της αναγνώρισης και επιβεβαίωσης των ιομορφικών προσβολών είναι ένα ξεπερασμένο μοντέλο, καθώς δίνει τη δυνατότητα στους επιτιθέμενους που χρησιμοποιούν μία νέα μέθοδο να πραγματοποιούν με επιτυχία τις επιθέσεις τους έως ότου γίνουν αντιληπτοί,

αναγνωριστούν οι τεχνικές δράσης τους και ληφθεί ένα νέο μέτρο ασφάλειας. Μέχρι τότε όμως η ζημιά έχει ήδη γίνει.

Ο ενδεδειγμένος τρόπος αντιμετώπισης, τουλάχιστον όταν πρόκειται για την προστασία κρίσιμων υποδομών, είναι η υιοθέτηση μίας προληπτικής προσέγγισης, μέσω του αυστηρού ελέγχου των εφαρμογών που εγκαθίστανται και εκτελούνται στα συστήματα και διατήρησης μίας whitelist με τις εγκεκριμένες εφαρμογές. Υιοθετώντας μία προσέγγιση άρνησης εκτέλεσης εξ ορισμού οποιουδήποτε λογισμικού δεν περιλαμβάνεται στη λίστα των εγκεκριμένων εφαρμογών, δεν θα επέτρεπε την εκτέλεση ιομορφών όπως ο Flame, ανεξάρτητα εάν αυτές εμφανίζονται ως αξιόπιστες και ψηφιακά υπογεγραμμένες. Σε αντίθεση με τη λογική των παραδοσιακών ανιχνευτών ιών, η προσέγγιση του whitelist δίνει τη δυνατότητα στους διαχειριστές να ελέγχουν με λεπτομέρεια τις εφαρμογές που εκτελούνται σε κάθε σύστημα (Munro, 2012).

Η υπογραφή του κώδικα συμβάλει στην αυθεντικοποίηση του κατασκευαστή του λογισμικού και στην ακεραιότητα του κώδικα. Ωστόσο, η εγκυρότητα της ψηφιακής υπογραφής δεν εξασφαλίζει την αξιοπιστία του κώδικα ή του κατασκευαστή του. Οι δημιουργοί του Flame μπόρεσαν να κατασκευάσουν ένα πλαστό πιστοποιητικό διότι η Microsoft χρησιμοποιούσε ακόμα τη συνάρτηση κατακερματισμού MD5 για την έκδοση των πιστοποιητικών παρόλο που οι ευπάθειές της είναι γνωστές από το 2008. Γενικότερα, η υπογραφή του κώδικα είναι μια καλή τεχνική για τη δημιουργία εμπιστοσύνης για την προέλευση του λογισμικού, όμως προϋποθέτει τη χρήση ισχυρών αλγορίθμων κρυπτογράφησης, καθώς και μια αυστηρή διαχείριση και έλεγχο των ιδιωτικών κλειδιών (Bencsáth, Pék, Buttyán & Félegyházi, 2012 · Munro, 2012).

Η παραδοσιακή τεχνική ανίχνευσης ιομορφικού λογισμικού με τη χρήση υπογραφών είναι αναποτελεσματική στην προστασία από άγνωστες ιομορφές. Άλλωστε, ο δημιουργός μιας στοχευόμενης επίθεσης θα φροντίσει να ξεπεράσει όλα τα γνωστά προϊόντα ανιχνευτές ιών. Μία αξιόλογη λύση θα μπορούσε να είναι η ανάπτυξη συστημάτων αναγνώρισης προτύπων με χρήση τεχνητής νοημοσύνης για την ανίχνευση ύποπτης συμπεριφοράς που αν και αποτελεί ακόμη ανοιχτό πεδίο έρευνας θα μπορούσε να συμβάλει στην αντιμετώπιση νέων επιθέσεων (Bencsáth, Pék, Buttyán & Félegyházi, 2012 · Bit9 Threat Advisor, 2012, · Marks, 2012 · Goyal, Sharma, Bevinakoppa, Watters, 2012). Η παραγωγή πολλών “false positives” ειδοποιήσεων από συστήματα αυτού του είδους, είναι κάτι που μπορεί να είναι ανεκτό όταν πρόκειται για την προστασία κρίσιμων πληροφοριακών συστημάτων και υποδομών.

Εξετάζοντας την περίπτωση του Flame, παρατηρείται ένα μεγάλο χάσμα αναφορικά με τις πληροφορίες και γνώσεις που έχουν στη διάθεσή τους οι επιτιθέμενοι σε σχέση με τα θύματα της επίθεσης. Η εγκατάσταση και λειτουργία ενός κατανεμημένου δικτύου από honeypots θα μπορούσε να συμβάλει στην ανίχνευση συντονισμένων επιθέσεων με τη συλλογή στοιχείων αναφορικά με τις νέες ιομορφικές προσβολές που θα εντοπίζονται εγκαίρως (Bencsáth, Pék, Buttyán & Félegyházi, 2012).

Ο Flame αποτελεί τμήμα μιας ευρύτερης επίθεσης και παρέμεινε ενεργός για ένα μεγάλο χρονικό διάστημα πριν αποκαλυφθεί από τους ερευνητές. Αυτό οφείλεται στο γεγονός ότι δεν προκαλεί ορατές επιπλοκές στα συστήματα που προσβάλει, χρησιμοποιώντας παράλληλα τεχνικές συμπίεσης και κρυπτογράφησης. Ο Flame υποκλέπτει πληροφορίες με πολλαπλούς τρόπους και χρησιμοποιεί διάφορα εναλλακτικά μέσα επικοινωνίας για τη μετάδοση των πληροφοριών που συλλέγει στους επιτιθέμενους, καθώς και την αποστολή από αυτούς νέων τμημάτων κώδικα και εντολών. Ωστόσο, ένας έμπειρος διαχειριστής με τη χρήση κατάλληλων εργαλείων θα μπορούσε να είχε εντοπίσει τις ανωμαλίες που επιφέρει η εγκατάσταση του Flame στα συστήματα που έχει υπό την εποπτεία του. Συνεπώς, η αυστηρή συνεχής παρακολούθηση και οι τακτικοί έλεγχοι ορθής λειτουργίας πληροφοριακών συστημάτων και δικτύων αποτελούν βασική γραμμή άμυνας έναντι των κυβερνοεπιθέσεων (Bencsáth, Pék, Buttyán & Félegyházi, 2012).

Οι δημιουργοί του Flame, όπως άλλωστε είναι φυσικό σε περιπτώσεις κυβερνο-κατασκοπείας, παραμένουν άγνωστοι. Σε διεθνές επίπεδο τα άτομα που δραστηριοποιούνται στην ανάπτυξη και χρήση ιομορφικού λογισμικού μπορούν να κατηγοριοποιηθούν σε τρεις κύριες ομάδες: ακτιβιστές, οργανωμένο κυβερνο-έγκλημα και ορισμένα τεχνολογικά προηγμένα κράτη. Εφαρμόζοντας ως συλλογιστική μέθοδο την εις άτοπο απαγωγή, διαπιστώνεται ότι ο Flame δεν αποτελεί το χαρακτηριστικό είδος εργαλείου που θα χρησιμοποιούσε ένας ακτιβιστής. Επίσης, ο Flame δεν έχει σχεδιαστεί για παράνομη μεταφορά χρημάτων από τραπεζικούς λογαριασμούς. Κατά συνέπεια, δεδομένης της πολυπλοκότητας της ιομορφής και της γεωγραφικής τοποθεσίας των στόχων, η πιο λογική εξήγηση είναι ο Flame να έχει αναπτυχθεί κατά παραγγελία από κάποιο κράτος με σημαντικά στρατηγικά και οικονομικά συμφέροντα στη Μέση Ανατολή (Boothby, Von Heinegg, Michael, Schmitt, Wingfield, 2012 · Gostev, 2012a).

Γεγονός είναι ότι ο Flame αποτελεί ένα μόνο από τα κομμάτια του πάζλ των επιχειρήσεων κυβερνοπολέμου που βρίσκονται σε εξέλιξη τα τελευταία χρόνια στην ευρύτερη γεωγραφική περιοχή της Μέσης Ανατολής. Αναλυτικότερα, παρατηρείται ότι οι επιθέσεις με ιομορφικό λογισμικό παρουσιάζονται χρονικά κατά κύματα. Η στρατηγική φαίνεται να είναι ότι το πρώτο κύμα των επιθέσεων έχει σκοπό να μολύνει όσο το δυνατό περισσότερους στόχους που παρουσιάζουν δυνητικό ενδιαφέρον. Το δεύτερο κύμα αποσκοπεί στη συλλογή δεδομένων από τους υπολογιστές των θυμάτων για να επιτρέψει την κατηγοριοποίηση των πληροφοριακών συστημάτων και τον προσδιορισμό των σημαντικότερων στόχων της επίθεσης. Τέλος, το τρίτο κύμα αφορά την προσβολή της ασφάλειας των επιλεγμένων συστημάτων με εξειδικευμένο ιομορφικό λογισμικό που θα εκτελέσει την τελική φάση της επίθεσης η οποία θα μπορούσε να είναι η παρακολούθηση, η υποκλοπή εμπιστευτικών πληροφοριών, η τροποποίηση παραμέτρων ή ακόμη και η φυσική καταστροφή του συστήματος.

Μεγάλο πρόβλημα στην έγκαιρη ανίχνευση μιας ιομορφής και στον περιορισμό της διάδοσής της αποτελεί η απροθυμία των οργανισμών θύματα της επίθεσης να

ενημερώσουν τη διεθνή επιστημονική κοινότητα και να παρέχουν στοιχεία που θα βοηθήσουν στην αντιμετώπιση της απειλής. Στην προσπάθειά τους να προασπίσουν τη φήμη και την ιδιωτικότητα των ευαίσθητων δεδομένων τους δυσχεραίνουν το έργο της συνολικής καταπολέμησης της εξάπλωσης του ιομορφικού λογισμικού. Η αποτελεσματική αντιμετώπιση των κυβερνοεπιθέσεων προϋποθέτει τη συνεργασία και την ανταλλαγή πληροφοριών σε διεθνές επίπεδο μεταξύ οργανισμών, κρατικών υπηρεσιών, εταιριών ανάπτυξης προϊόντων ασφάλειας και ερευνητικής κοινότητας (Bencsáth, Pék, Buttyán & Félegyházi, 2012).

Οι κυβερνοεπιθέσεις μεταξύ κρατών εγείρουν νομικά θέματα που ενδεχομένως να μην καλύπτονται από το υφιστάμενο διεθνές δίκαιο. Ο ιδρυτικός χάρτης των Ηνωμένων Εθνών, ο οποίος υπογράφηκε στις 26 Ιουνίου 1945 και λειτουργεί σαν είδος συντάγματος, στο άρθρο 2(4) αναφέρει ότι *«Όλα τα κράτη-μέλη στις διεθνείς τους σχέσεις θα απέχουν από την απειλή ή τη χρήση στρατιωτικής δύναμης κατά της εδαφικής ακεραιότητας και της πολιτικής ανεξαρτησίας άλλου κράτους»*. Επίσης, στο άρθρο 51 αναφέρεται ότι *«Τίποτε στο χάρτη αυτό δεν περιορίζει το δικαίωμα της ατομικής ή συλλογικής αυτοάμυνας, όταν μια ένοπλη επίθεση λαμβάνει χώρα εναντίον μέλους των Ηνωμένων Εθνών, έως ότου το Συμβούλιο Ασφαλείας πάρει τα αναγκαία μέτρα για τη διατήρηση της διεθνούς ειρήνης και ασφάλειας»*.

Ο νομοθέτης το 1945 δεν μπορούσε να φανταστεί ότι το κύριο πεδίο μαχών στον 21ο αιώνα θα ήταν ο κυβερνοχώρος. Το ερώτημα που τίθεται είναι εάν το Ιράν έχει το δικαίωμα αυτοάμυνας ενάντια στους επιτιθέμενους. Η απάντηση προκύπτει από την ερμηνεία του κατά πόσο ο Flame αποτελεί ή όχι ένοπλη επίθεση. Η τεχνική ανάλυση δείχνει ότι συμπεριφέρεται ως ένα εργαλείο κατασκοπείας και δεν προκαλεί καταστροφές τέτοιας κλίμακας που να μπορεί να θεωρηθεί αιτία πολέμου. Αποτελεί περισσότερο ένα μήνυμα απειλητικής προειδοποίησης παρά μία ένοπλη επίθεση (Boothby, Von Heinegg, Michael, Schmitt, Wingfield, 2012 · Jolley, 2012).

Η νέα χιλιετία ανοίγει τις πόρτες της στην ανάπτυξη μιας νέας βιομηχανίας παραγωγής ιομορφικού λογισμικού για την επιβολή και διατήρηση της κυριαρχίας των τεχνολογικά ανεπτυγμένων κρατών. Οι κυβερνοεπιθέσεις είναι πολύ πιθανό ότι θα πληθύνουν τα επόμενα χρόνια και θα γίνονται ολοένα και πιο στοχευόμενες και αποτελεσματικές. Δεν αποκλείεται μάλιστα κάποιες από αυτές να οδηγήσουν σε σημαντικές φυσικές καταστροφές κρίσιμων υποδομών με απώλειες ανθρώπινων ζωών.

Οι ανεπτυγμένες σε ΤΠΕ χώρες θα πρέπει να συμφωνήσουν σε ορισμένες βασικές αρχές που να περιορίζουν την ένταση και το εύρος των κυβερνοεπιθέσεων. Η υπογραφή μιας τέτοιας συνθήκης ή έστω μιας συμφωνίας σε επίπεδο Ηνωμένων Εθνών θα ήταν το πρώτο βήμα για τη δημιουργία ενός ρυθμιστικού πλαισίου για τον έλεγχο των συνεπειών από ιομορφικές προσβολές.

Οι παραδοσιακές πολεμικές επιχειρήσεις που έχουν λάβει χώρα τα τελευταία έτη στην ευρύτερη περιοχή της Μέσης Ανατολής και Βόρειου Αφρικής, είχαν ως κύριο στόχο τη διατήρηση του ελέγχου από τις μεγάλες δυνάμεις των ενεργειακών

αποθεμάτων αυτής της ευαίσθητης και στρατηγικής γεωγραφικά ζώνης του πλανήτη. Το κόστος αυτών των συρράξεων και η μετέπειτα διατήρηση των νέων καθεστώτων στην εξουσία, αποδείχθηκε για τους επιτιθέμενους δυσβάσταχτο τόσο σε χρήμα όσο και σε ανθρώπινες ζωές και απώλεια του κύρους και της λαϊκής υποστήριξης των κυβερνήσεων που τις σχεδίασαν και τις υποστήριξαν.

Ο κυβερνοπόλεμος μπορεί να επιτύχει τους ίδιους στόχους (επίδειξη τεχνολογικής υπεροχής, υποκλοπή κρατικών μυστικών, ανατροπή κυβερνήσεων, υποκίνηση εσωτερικών ταραχών και επαναστάσεων, καταστροφή κρίσιμων εθνικών υποδομών) χωρίς ο επιτιθέμενος να χρειαστεί να αναλάβει την ευθύνη της επίθεσης και να εμπλέξει τα στρατεύματά του σε πολεμικές συρράξεις. Η στρατηγική των κυβερνοεπιθέσεων μπορεί να αποφέρει ως κέρδος την υποκλοπή κρατικών μυστικών, τον αποσυντονισμό της λειτουργίας κρίσιμων υποδομών και την απόδειξη της τεχνολογικής υπεροχής των επιτιθέμενων, που μπορεί να αποτελέσει ένα σημαντικό ηθικό πλήγμα και μια έμπρακτη απειλή για τις συνέπειες μιας ενδεχόμενης συνολικής σύγκρουσης δυνάμεων. Συνεπώς, ο αντίπαλος υπό την απειλή της εξαπόλυσης μιας συντονισμένης και μεγάλης κλίμακας κυβερνοεπίθεσης σε εθνικό επίπεδο, είναι πολύ πιθανό να υποκύψει στις εξωτερικές πιέσεις και να συμμορφωθεί με τις κατευθύνσεις και τις συστάσεις της διεθνής διπλωματίας.

Η απειλή των κυβερνοεπιθέσεων αποτελεί ένα πολύ αποτελεσματικό και αποδοτικό διπλωματικό όπλο για την άσκηση εξωτερικής πολιτικής από τις χώρες που διαθέτουν την ανάλογη τεχνολογική υπεροχή στον τομέα αυτό.

7.4. Μελέτη Περίπτωσης

Εφαρμογή συμμετρικής κρυπτογράφησης με τη χρήση του εργαλείου 7-zip.

7.5. Βιβλιογραφία

- Bencsáth B., Pék G., Buttyán L., Félegyházi M. (2012). *The Cousins of Stuxnet: Duqu, Flame, and Gauss*. Future Internet, 4(4), pp.971-1003.
- Munro K. (2012). *Deconstructing Flame: the limitations of traditional defenses*. Elsevier, Computer Fraud & Security Volume 2012, Issue 10, pp. 8–11.
- Bit9 Threat Advisor (2012). *Don't get burned by Flame*. Vol. 1, No. 3.
- Boothby W.H., von Heinegg W.H., Michael J.B., Schmitt M.N., Wingfield T.C. (2012). *When Is a Cyberattack a Use of Force or an Armed Attack?*. IEEE Computer, Volume 45, Issue 8, pp. 82-84.
- Marks P. (2012). *Why we may never know who created Flame virus*. New Scientist, Volume 214, Issue 2868, pp. 24.
- Jolley J. D. (2012). *Article 2(4) and Cyber Warfare: How Do Old Rules Control the Brave New World?*. Social Science Electronic Publishing, Inc.
- Goyal R., Sharma S., Bevinakoppa S., Watters P. (2012). *Obfuscation of Stuxnet and Flame Malware*. Proceedings of the 3rd International conference on Applied Informatics and Computing Theory (AICT '12). Latest Trends in Applied Informatics and Computing, Barcelona, Spain.
- Symantec Official Blog (2012). *W32.Flamer: Enormous Data Collection*. http://www.symantec.com/connect/blogs/w32flamer-enormous-data-collection
- Symantec Official Blog (2012). *Painting a Picture of W32.Flamer*, http://www.symantec.com/connect/blogs/painting-picture-w32flamer
- Symantec Official Blog (2012) "W32.Flamer: Microsoft Windows Update Man-in-the-Middle", http://www.symantec.com/connect/blogs/w32flamer-microsoft-windows-update-man-middle
- Symantec Security Response (2012). *W32.Flamer*, http://www.symantec.com/security_response/writeup.jsp?docid=2012-052811-0308-99
- sKyWIper Analysis Team (2012). *sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks*. Budapest University of Technology and Economics, Department of Telecommunications, v1.05.

- Gostev A. (2012a), "The Flame: Questions and Answers", Kaspersky Lab, http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

- Gostev, A. (2012b). *Back to Stuxnet: the missing link.* Kaspersky Lab, https://www.securelist.com/en/blog/208193568/Back_to_Stuxnet_the_missing_link

- Sotirov A. (2012). *Analyzing the MD5 Collision in Flame*, https://speakerdeck.com/asotirov/analyzing-the-md5-collision-in-flame

- Stevens M. (2012). *Attacks on Hash Functions and Applications.* Mathematical Institute, Leiden University.

- Sotirov A., Stevens M., Appelbaum J., Lenstra, A., Molnar D., Osvik, D.A., De Weger B. (2008). *MD5 considered harmful today - Creating a rogue CA certificate.* Presented at 25th Chaos Communications Congress, Berlin, Germany.

- Stevens M. (2012). *Technical Background on the Flame Collision Attack*". CWI (Centrum Wiskunde & Informatica) News.

- Antiy Labs (2012). *Analysis Report on Flame Worm Samples.* Version 1.3.0.

- Symantec Security Response (2012). *Have I Got Newsforyou: Analysis of Flamer C&C Server*.