ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

Ψηφιακή Εγκληματολογία στο Στρατιωτικό Περιβάλλον

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΜΕΛΕΙΑ

Γεώργιος Βάσιος

ΕΠΙΒΛΕΠΩΝ

Κωνσταντίνος Λαμπρινουδάκης, Αναπληρωτής Καθηγητής

Αθήνα, Μάρτιος 2016

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, κ. Κωνσταντίνο Λαμπρινουδάκη για την ανάθεση της διπλωματικής εργασίας. Η εργασία αυτή δεν θα είχε ολοκληρωθεί χωρίς την καθοδήγηση και την πολύτιμη βοήθειά του.

Επίσης, θα ήθελα να ευχαριστήσω τους υπηρεσιακούς μου προϊσταμένους, οι οποίοι με παρότρυναν να παρακολουθήσω το Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων» του Πανεπιστημίου Πειραιά και με υποστήριξαν με κάθε δυνατό τρόπο κατά τη διάρκεια της φοίτησής μου. Ελπίζω το αποτέλεσμα να λειτουργήσει προς όφελος της Υπηρεσίας.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου για τη στήριξή τους σε κάθε απόφασή μου όλα αυτά τα χρόνια και τη συμπαράστασή τους στην εκπλήρωση κάθε στόχου μου.

Περίληψη

Η στρατιωτική λειτουργία έχει εντάξει στους μηχανισμούς της τις τεχνολογίες της Πληροφορικής και του Διαδικτύου, για την κάλυψη των επιχειρησιακών και λειτουργικών της αναγκών. Η χρησιμοποίηση των μέσων αυτών, πέραν των πλεονεκτημάτων, καθιστά τις διακινούμενες πληροφορίες ευάλωτες σε απειλές ενάντια στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητά τους. Στην παρούσα εργασία επιχειρείται μια λεπτομερής περιγραφή των δυνατοτήτων Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας που πρέπει να αναπτυχθούν στο στρατιωτικό περιβάλλον, ώστε να επιτευχθεί η άμεση αντιμετώπιση των περιστατικών ασφαλείας και η εξαγωγή αποδεικτικών στοιχείων για χρήση στις διαδικασίες απόδοσης ευθυνών. Αρχικά, αναφέρονται οι κανονιστικές διατάξεις οι οποίες εμπίπτουν στις έρευνες που περιλαμβάνουν ψηφιακά πειστήρια. Στη συνέχεια, προδιαγράφεται ένα ενιαίο μοντέλο διαδικασιών με αναλυτικές οδηγίες και ενέργειες για κάθε στάδιο. Επιπλέον, περιγράφονται οι απαιτήσεις σε προσωπικό, εξοπλισμό και υποδομές για την αποτελεσματική υλοποίηση των υπόψη δυνατοτήτων, πάντοτε υπό το πρίσμα της στρατιωτικής πραγματικότητας. Τέλος, παρατίθενται συμπεράσματα αναφορικά με την εφαρμογή του μοντέλου στο στρατιωτικό περιβάλλον και προτάσεις για περαιτέρω έρευνα.

Λέξεις κλειδιά : ψηφιακή εγκληματολογία, μοντέλα διαδικασιών, ψηφιακά πειστήρια

Πίνακας Περιεχομένων

Ευρετήριο Εικόνων

Κεφάλαιο 1ο

Ψηφιακή Εγκληματολογία και Στρατιωτικό Περιβάλλον

1.1 Εισαγωγή

Η σύγχρονη τεχνολογική εποχή, με την εξέλιξη των υπολογιστών και τη συνεπαγόμενη ανάπτυξη των δυνατοτήτων τους, πέραν των υπολοίπων οφελών στην ανθρωπότητα, έχει εξυπηρετήσει τόσο τις κυβερνήσεις και τους διάφορους οργανισμούς όσο και τους ίδιους τους μεμονωμένους χρήστες στην εκτέλεση βασικών και αναγκαίων λειτουργιών, οι οποίες τα προηγούμενα χρόνια απαιτούσαν υποχρεωτική παρουσία, μεγάλο κόπο και σε αρκετές των περιπτώσεων υπερβολική γραφειοκρατία. Ταυτόχρονα, η εξάπλωση του Διαδικτύου, το οποίο πλέον βρίσκεται σχεδόν σε κάθε σπίτι, έχει σαν επακόλουθο την εξοικείωση του μεγαλύτερου μέρους της σημερινής κοινωνίας στην απλή χρήση του για την κάλυψη κάθε είδους ανάγκης ή υποχρέωσης.

Το στρατιωτικό περιβάλλον δεν θα μπορούσε να αποτελέσει εξαίρεση και εναρμονισμένο με το σύγχρονο τεχνολογικό ρεύμα έχει πλέον εντάξει στους μηχανισμούς του τις τεχνολογίες της Πληροφορικής και του Διαδικτύου, για την κάλυψη των επιχειρησιακών και λειτουργικών του αναγκών.

Σε άμεση αντιστοιχία με το κοινωνικό περιβάλλον, η ένταξη των μέσων Πληροφορικής στη στρατιωτική λειτουργία, καθιστά τις πληροφορίες που διακινούνται μέσω αυτών ευάλωτες σε όλες τις μορφές των σύγχρονων Κυβερνοεπιθέσεων, θέτοντας σε κίνδυνο την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητά τους. Οι συνέπειες που μπορεί να έχει η διαρροή διαβαθμισμένων πληροφοριών και προσωπικών δεδομένων από τα στρατιωτικά Πληροφοριακά Συστήματα στην εθνική ασφάλεια είναι άκρως σημαντικές και καταδεικνύουν την ανάγκη ανάπτυξης μηχανισμών ασφάλειας Πληροφορικής και εφαρμογής διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας (Incident Response) και Ψηφιακής Εγκληματολογίας (Digital Forensics) για την πρόληψη και αντιμετώπιση, αντίστοιχα, πιθανών περιστατικών.

Σε αντίθεση με τον τομέα της ανάπτυξης και εγκατάστασης μέτρων ασφάλειας Πληροφορικής, όπου παρατηρείται πληθώρα τεχνικών και πρότυπων μεθόδων οι οποίες είναι ευρέως αποδεκτές και εφαρμοζόμενες δύναται να επιτύχουν τα επιδιωκόμενα αποτελέσματα, στον αντίστοιχο της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας η κατάσταση παρουσιάζει προβλήματα.

1.2 Καθορισμός Προβλήματος

Η ισχύουσα νομοθεσία σε κάθε κράτος σχετικά με το δικαίωμα των ατόμων στην ιδιωτικότητα, οι διαφορές στις διατάξεις που αφορούν στη συλλογή, στο χειρισμό και στην εγκυρότητα των ψηφιακών αποδεικτικών στοιχείων στις δικαστικές διαδικασίες, η ποικιλομορφία και ανομοιογένεια των

υποδομών, είτε πρόκειται για υλικό είτε για λογισμικό, η πληθώρα των χρησιμοποιούμενων τεχνικών με τις οποίες οι κακόβουλοι χρήστες εκδηλώνουν τις ενέργειές τους εναντίον της ασφάλειας των πληροφοριών και γενικότερα η μοναδικότητα κάθε περιστατικού ως προς τις ιδιαιτερότητές του έχουν σαν αποτέλεσμα την αδυναμία, και ως εκ τούτου την έλλειψη, προτυποποίησης και δημιουργίας θεωρητικού πλαισίου το οποίο να καθορίζει έναν έγκυρο και αποδεκτό τρόπο ενεργείας.

Τόσο στο στρατιωτικό όσο και στο ευρύτερο τεχνολογικό περιβάλλον, σε αρκετές περιπτώσεις, υιοθετούνται μέθοδοι που προκύπτουν κατά το δοκούν από προσωπικό που πιθανώς να μην πληροί τα απαιτούμενα κριτήρια κατάρτισης, ενώ συχνά χρησιμοποιούνται και αυτοσχέδια εργαλεία λογισμικού. Με τον τρόπο αυτό τα εξαγόμενα αποτελέσματα δεν είναι δυνατόν να χρησιμοποιηθούν στις δικαστικές λειτουργίες ή στις εσωτερικές πειθαρχικές διαδικασίες ενός Οργανισμού, καθώς η γνησιότητά τους μπορεί να αμφισβητηθεί, ενώ επίσης δεν συνεισφέρουν ουσιαστικά στις διαδικασίες τεχνικής ανάλυσης που λαμβάνουν χώρα μετά από τα περιστατικά ασφαλείας, με σκοπό την αναβάθμιση των συστημάτων.

Έχοντας κατά νου όλα τα παραπάνω γίνεται αντιληπτό ότι υφίσταται η ανάγκη προδιαγραφής μιας μεθοδολογίας Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας στο σύνολό της, συμπεριλαμβανομένων τόσο των ενεργειών όσο και των υποδομών και εργαλείων, η οποία θα εξασφαλίζει, στα πλαίσια του δυνατού, την αποτελεσματικότητα και εγκυρότητα των εξαγόμενων στοιχείων για την χρησιμοποίησή τους στις περαιτέρω διαδικασίες απόδοσης τυχόν ευθυνών και επικαιροποίησης των συστημάτων ασφαλείας.

1.3 Δομή Εργασίας

Η προσέγγιση του προβλήματος στην παρούσα εργασία πραγματοποιείται ακολουθώντας την παρακάτω δομή:

Αρχικά, εξετάζεται το ισχύον ελληνικό νομοθετικό πλαίσιο και οι διατάξεις των στρατιωτικών νόμων και κανονισμών, οι οποίοι αποτελούν τις Πολιτικές Ασφαλείας Πληροφοριών στο στρατιωτικό περιβάλλον. Το ενδιαφέρον εστιάζεται στις παραμέτρους οι οποίες είναι εξαιρετικά σημαντικές για τις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας και αφορούν στην ιδιωτικότητα των χρηστών των στρατιωτικών πληροφοριακών συστημάτων, στο δικαίωμα διεξαγωγής ελέγχων από τους υπεύθυνους με σκοπό την ασφάλεια των διακινούμενων πληροφοριών και στο χειρισμό των ψηφιακών στοιχείων που χαρακτηρίζονται ως «πειστήρια» για τις έρευνες ενός περιστατικού ασφαλείας.

Στη συνέχεια αναλύονται οι έννοιες της Αντιμετώπισης Περιστατικών Ασφαλείας και της Ψηφιακής Εγκληματολογίας με αναφορά στα υπάρχοντα μοντέλα διαδικασιών και τους επιδιωκόμενους σκοπούς των διαδικασιών αυτών για τη λειτουργία ενός Οργανισμού. Μέσα από τη σύγκριση των δύο

μοντέλων και λαμβάνοντας υπόψη τις ιδιαίτερες παραμέτρους που χαρακτηρίζουν τη στρατιωτική πραγματικότητα από πλευράς εξειδίκευσης και προσωπικού, προκύπτει η ανάγκη για τη δημιουργία ενός ενιαίου μοντέλου ενεργειών, το οποίο και προδιαγράφεται.

Ακολούθως αναλύονται οι παράγοντες που σχετίζονται με το προσωπικό που θα κληθεί να στελεχώσει τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας ενός Οργανισμού. Επίσης, παρουσιάζεται ο εξοπλισμός που είναι απαραίτητος για την επί τόπου εκτέλεση των καθηκόντων της αντίστοιχης ομάδας, η οποία θα ενεργήσει πρώτη για την αντιμετώπιση ενός περιστατικού με σκοπό να αποκατασταθεί η κανονική ροή λειτουργίας. Ταυτόχρονα, περιγράφεται στο σύνολό του ένα εργαστήριο Ψηφιακών Εγκληματολογικών Ερευνών, το οποίο είναι υπεύθυνο για τη λεπτομερή τεχνική ανάλυση των ψηφιακών πειστηρίων. Η περιγραφή του απαραίτητου προσωπικού και των υποδομών γίνεται πάντοτε με γνώμονα τις ιδιαιτερότητες που παρουσιάζει το στρατιωτικό περιβάλλον.

Τέλος, απαριθμούνται τα συμπεράσματα που εξήχθησαν κατά την εκπόνηση της εργασίας σχετικά με τη δυνατότητα εφαρμογής του προτεινόμενου μοντέλου στο στρατιωτικό περιβάλλον και τα επιμέρους ζητήματα που αφορούν στο προσωπικό και τις υποδομές, ενώ παρουσιάζονται προτάσεις για τη μελλοντική επέκτασή του.

1.4 Συνεισφορά

Η συνεισφορά της παρούσας εργασίας στις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας στο στρατιωτικό περιβάλλον συνίσταται στο ότι συγκεντρώνει και προδιαγράφει το σύνολο των διαδικασιών και των μέσων, προσεγγίζοντας αναλυτικά τα ζητήματα που θα προκύψουν εφόσον αποφασιστεί η ανάπτυξη και ένταξη ανάλογων δυνατοτήτων στη στρατιωτική πραγματικότητα. Αναλυτικότερα:

- Συγκεντρώνει και συγκρίνει τις διατάξεις, τόσο της ελληνικής νομοθεσίας όσο και των πολιτικών ασφαλείας που ισχύουν στο στρατιωτικό περιβάλλον, οι οποίες αφορούν σε ζητήματα που μπορεί να αντιμετωπίσει ο ερευνητής κατά την εκτέλεση των καθηκόντων του. Παρέχει κυρίως μια εικόνα σχετικά με το δικαίωμα των χρηστών στην ιδιωτικότητα και το χειρισμό των ψηφιακών δεδομένων ως αποδεικτικών στοιχείων για τις έρευνες ενός περιστατικού ασφαλείας εντός των στρατιωτικών ορίων. Το αποτέλεσμα της σύγκρισης δεν μπορεί να ληφθεί απαραίτητα ως ορθό, καθώς αποτελεί αντικείμενο τρέχουσας έρευνας και δεν υφίσταται ακόμα επαρκές νομοθετικό πλαίσιο.

- Περιγράφει αναλυτικά ένα ολοκληρωμένο, ενιαίο μοντέλο διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, λαμβάνοντας υπόψη και τους περιορισμούς που θέτει το στρατιωτικό περιβάλλον, το οποίο υιοθετούμενο δύναται να καλύψει την ανάγκη προτυποποίησης στο συγκεκριμένο τομέα.

- Καθορίζει τις απαιτήσεις σε προσωπικό και εξοπλισμό και περιγράφει στο σύνολό της μια πρότυπη υποδομή εργαστηρίου Ψηφιακής Εγκληματολογίας, στοιχεία που δύναται να χρησιμοποιηθούν κατά την αρχική σχεδίαση και τον υπολογισμό των αναγκαίων πόρων για την υλοποίηση των εν λόγω δυνατοτήτων.

Κεφάλαιο 2ο
Ελληνική Νομοθεσία και Πολιτικές Ασφαλείας στο Στρατιωτικό Περιβάλλον

2.1 Εισαγωγή

Η ανάπτυξη της επιστήμης της Πληροφορικής σε συνδυασμό με την ελευθερία που χαρακτηρίζει την πρόσβαση οποιουδήποτε ατόμου στη συγκεκριμένη γνώση, εκτός των αδιαμφισβήτητων ευεργετικών επιτευγμάτων για την ανθρωπότητα, κατέστησε δυνατή και την εκτέλεση ενός ευρέως φάσματος εγκληματικών ενεργειών από κακόβουλους χρήστες, οι οποίοι διαθέτουν την απαιτούμενη εξειδίκευση και τεχνική κατάρτιση. Συνεπακόλουθα, ορισμένα από τα πλέον διαδεδομένα εγκλήματα διαπράττονται πια υπό τη μορφή «κυβερνο-εγκλημάτων», με τους δράστες να εκμεταλλεύονται τα χαρακτηριστικά του νέου χώρου δράσης για να αποφύγουν τον εντοπισμό και τη σύλληψή τους. Η έξαρση του νέου τύπου εγκληματικότητας και οι καταστροφικές συνέπειες που μπορεί να έχει σε κάθε επίπεδο, από κυβερνητικό-εταιρικό έως προσωπικό, καθιστά την αντιμετώπισή της εξαιρετικής σημασίας. Αυτός είναι και ο λόγος που ο τομέας της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας γνωρίζει αντίστοιχη ανάπτυξη με το Κυβερνοέγκλημα.

Το προσωπικό το οποίο επιφορτίζεται με τα καθήκοντα της αντιμετώπισης και διερεύνησης των περιστατικών ασφαλείας, προβαίνει σε ενέργειες αναγνώρισης, συλλογής, εξέτασης και ανάλυσης των κατάλληλων αποδεικτικών στοιχείων, τα οποία εν τέλει θα χρησιμοποιηθούν σε δικαστικές ή εσωτερικές πειθαρχικές διαδικασίες. Οι ενέργειες αυτές είναι ιδιαίτερα πολύπλοκες και επίπονες, ενώ κατά τη διάρκεια υλοποίησής τους οι ερευνητές θα βρεθούν αντιμέτωποι και με προβληματισμούς νομικής φύσεως. Αυτοί συνήθως αφορούν στην εγκυρότητα των ψηφιακών πειστηρίων που συλλέχθηκαν και στην ιδιωτικότητα των χρηστών των Πληροφοριακών Συστημάτων που ελέγχθηκαν. Για να εξασφαλισθεί η αξιοπιστία των μεθόδων συλλογής και ανάλυσης των δεδομένων, η αποδοχή των πειστηρίων από τις δικαστικές λειτουργίες καθώς και για να αποφευχθεί τυχόν παραβίαση του δικαιώματος οποιοδήποτε χρήστη στην ιδιωτικότητα, το προσωπικό που διεξάγει τις έρευνες θα πρέπει να λειτουργεί εντός των καθορισμένων εθνικών νομικών πλαισίων και σύμφωνα με τις πολιτικές ασφαλείας που ισχύουν σε κάθε περιβάλλον, οι οποίες διευκρινίζουν περαιτέρω τα συγκεκριμένα θέματα.

Στη συνέχεια του κεφαλαίου παρουσιάζονται οι διατάξεις της ελληνικής νομοθεσίας που αφορούν στο δικαίωμα ενός ατόμου στην ιδιωτικότητα και στο χειρισμό των στοιχείων που χαρακτηρίζονται ως «πειστήρια» για τις έρευνες ενός περιστατικού ασφαλείας, καθώς πρόκειται για εξαιρετικά σημαντικές παραμέτρους στις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας. Ακολούθως ορίζονται οι Πολιτικές Ασφαλείας Πληροφοριακών Συστημάτων και γίνεται αναφορά στα άρθρα των πολιτικών που ισχύουν στο στρατιωτικό περιβάλλον και τα οποία καθορίζουν

περισσότερες λεπτομέρειες σχετικά με την υποχρέωση ελέγχου των υποδομών από το αρμόδιο προσωπικό Ψηφιακής Εγκληματολογίας και τις απαιτήσεις ιδιωτικότητας των χρηστών των στρατιωτικών Πληροφοριακών Συστημάτων. Τέλος παρατίθενται συμπεράσματα και προβληματισμοί αναφορικά με την εφαρμογή και την πληρότητα των παραπάνω διατάξεων.

2.2 Ελληνική Νομοθεσία

Η Ελλάδα, ως κράτος μέλος της Ευρωπαϊκής Ένωσης, οφείλει να εναρμονίζει τη νομοθεσία της βάσει των κοινοτικών οδηγιών. Το Ηλεκτρονικό Έγκλημα παρουσιάζει πολλές μορφές και η συνεχής εξέλιξη της τεχνολογίας δυσκολεύει τον προσδιορισμό των χαρακτηριστικών κάθε διαφορετικής επίθεσης. Για να αντιμετωπιστεί ο κίνδυνος αυτός, κρίθηκε απαραίτητη η διακρατική συνεννόηση και ο καταρτισμός μιας ενιαίας αποτελεσματικής στρατηγικής. Σε αυτή την κατεύθυνση πραγματοποιήθηκε το 2001 το Συνέδριο για το Ηλεκτρονικό Έγκλημα στη Βουδαπέστη, το οποίο κατέληξε στην αντίστοιχη **Συνθήκη της Βουδαπέστης**, όπου παρατίθενται επεξηγήσεις και ρυθμίσεις για τις περισσότερες μορφές Ηλεκτρονικών Εγκλημάτων. Η Συνθήκη της Βουδαπέστης υπογράφτηκε από είκοσι έξι (26) κράτη μέλη της Ε.Ε., μεταξύ των οποίων και η Ελλάδα, χωρίς όμως μέχρι στιγμής να έχει τεθεί σε ισχύ.

Η προσέγγιση των νομικών θεμάτων που αφορούν στον κυβερνοχώρο παρουσιάζει δυσκολίες, καθώς προϋποθέτει τόσο νομικές όσο και τεχνικές γνώσεις. Στην ελληνική νομοθεσία, ο νόμος **Ν.1805/88** αφορά στα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές, τροποποιώντας και συμπληρώνοντας τις διατάξεις του ποινικού κώδικα (370Β, 370Γ και 386Α) που σχετίζονται με την ηλεκτρονική εγκληματικότητα.

Πιο συγκεκριμένα, το **άρθρο 370Β του ΠΚ** περί «Παραβίασης Απορρήτου» αναφέρει ότι «*όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτο ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών (3) μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους*». Το **άρθρο 370Γ του ΠΚ** περί «Χρήσης Προγραμμάτων Η/Υ» αναφέρει ότι «*όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μηνών και με χρηματική ποινή διακοσίων ενενήντα (290) έως και πέντε χιλιάδων εννιακοσίων (5.900) ευρώ*» και «*όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση ή με χρηματική ποινή. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148 (περί Κατασκοπείας)*». Στο **άρθρο**

386Α του ΠΚ περί «Απάτης με Υπολογιστή» αναφέρεται ότι «*όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με φυλάκιση από τρείς (3) μήνες έως πέντε (5) χρόνια*».

Ανεξάρτητα από το εάν ο συγκεκριμένος νόμος επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της επιστήμης της Πληροφορικής, σίγουρα δεν επαρκεί για να καλύψει τα εγκλήματα που έχουν παρουσιαστεί από τη χρήση του Διαδικτύου. Στην ελληνική έννομη τάξη δεν υπάρχει νόμος που να αναφέρεται σε θέματα Διαδικτύου και ειδικότερα να ρυθμίζει τη συμπεριφορά των χρηστών του από την άποψη του Ποινικού Δικαίου.

Όσον αφορά στην ιδιωτικότητα των χρηστών, ο νόμος **Ν.2472/97** αναφέρεται στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ενώ το 2006 ψηφίστηκε και ο νόμος **Ν.3471/06** για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Αναλυτικότερα, ο Ν.2472/97 ενσωματώνει στο ελληνικό δίκαιο την **οδηγία 46/1995 του Ευρωπαϊκού Κοινοβουλίου** «*για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών*», η οποία επιδίωκε την εναρμόνιση των ευρωπαϊκών νομοθεσιών σε ένα υψηλό επίπεδο προστασίας. Ο συγκεκριμένος νόμος ρυθμίζει την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθορίζοντας τα χαρακτηριστικά τους, τις προϋποθέσεις επεξεργασίας, τις υποχρεώσεις του υπευθύνου επεξεργασίας καθώς και τα δικαιώματα του υποκειμένου των δεδομένων, όπως το δικαίωμα ενημέρωσης, το δικαίωμα πρόσβασης, το δικαίωμα αντίρρησης και το δικαίωμα προσωρινής δικαστικής προστασίας.

Ο Ν.2472/97 τροποποιήθηκε το 2000 και το 2001 και επιβάλλεται από την Αρχή Προστασίας Προσωπικών Δεδομένων (Α.Π.Π.Δ.). Συμπληρώνεται από το νόμο **Ν.2774/99** περί «Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στον Τηλεπικοινωνιακό Τομέα» καθώς και από το νόμο **Ν.3115/03**, ο οποίος προβλέπει τη σύσταση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών.

Τέλος, οι ρυθμίσεις του Ν.2472/97 συμπληρώθηκαν από το νόμο Ν.3471/06 περί «Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών», ο οποίος κατοχύρωσε σημαντικά δικαιώματα των συνδρομητών και χρηστών τηλεπικοινωνιακών υπηρεσιών.

Σε ότι αφορά στα ψηφιακά αποδεικτικά στοιχεία, αυτά σε καμία περίπτωση δεν μπορούν να ταυτιστούν με τα παραδοσιακά αποδεικτικά μέσα. Αυτό συμβαίνει διότι οι αποδείξεις ενός εγκλήματος που λαμβάνει χώρα στο «φυσικό» κόσμο έχουν αντίστοιχα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντιθέτως, τα ηλεκτρονικά πειστήρια δεν είναι χειροπιαστά, υπάρχει περίπτωση να διαχειρίζονται από κάποιο απομακρυσμένο σημείο, ενώ μπορούν να τροποποιούνται με διάφορους τρόπους ή ακόμα και να εξαφανιστούν πολύ εύκολα. Αυτό που μπορεί να γίνει «φυσικά» αντιληπτό είναι η αναπαράστασή τους μέσω προβολής ή εκτύπωσης, χωρίς όμως πάντοτε να είναι δυνατή και αποδοτική αυτή η διεργασία, όπως στην περίπτωση μεγάλων βάσεων δεδομένων.

Οι παραπάνω ιδιαιτερότητες των ψηφιακών πειστηρίων καθιστούν δύσκολη τη δημιουργία ενός αποτελεσματικού πλαισίου το οποίο θα καθορίζει τα χαρακτηριστικά τους, τους νόμιμους τρόπους μεταχείρισής τους και τις προϋποθέσεις εγκυρότητάς τους, ώστε να μπορούν να παρουσιαστούν και να χρησιμοποιηθούν στις δικαστικές διαδικασίες. Το αποτέλεσμα της παραπάνω αδυναμίας είναι η μεταχείρισή τους να γίνεται με τρόπο παρόμοιο με τα παραδοσιακά «φυσικά» αποδεικτικά στοιχεία και αναλόγως κάθε φορά των ιδιαιτεροτήτων της υπόθεσης. Σε κάθε περίπτωση, η συλλογή και προσκόμιση ψηφιακών δεδομένων ως αποδεικτικών στοιχείων για μια υπόθεση υπόκεινται στα όσα αναφέρει η **παράγραφος 3 του άρθρου 19 του Συντάγματος της Ελλάδας** περί «Απορρήτου Επιστολών, Ανταπόκρισης και Επικοινωνίας», στο οποίο αναφέρεται ότι «*απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9Α*». Το **άρθρο 19 του Συντάγματος** αναφέρει ότι «*το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Ο Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων*», ενώ το **άρθρο 9Α του Συντάγματος** ορίζει ότι «*καθένας έχει το δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ο νόμος ορίζει*».

2.3 Πολιτικές Ασφαλείας Πληροφοριακών Συστημάτων

Πέραν των όσων προβλέπονται από την ισχύουσα νομοθεσία μιας χώρας και αφορούν στην προστασία και διακίνηση όλων των τύπων πληροφοριών, ένας Οργανισμός οφείλει να προχωρήσει στη σύνταξη των ιδιαίτερων, για το περιβάλλον του, Πολιτικών Ασφαλείας Πληροφοριών ώστε να καθορίσει περισσότερες λεπτομέρειες σχετικά με το πώς θα προσπαθήσει να επιτύχει το μεγαλύτερο δυνατό επίπεδο ασφάλειας. Όταν η πολιτική ασφαλείας εξειδικεύεται σε θέματα που αφορούν στην ασφάλεια των πληροφοριών που διακινούνται στα Πληροφοριακά Συστήματα του Οργανισμού, τότε αντίστοιχα προκύπτει μια Πολιτική Ασφαλείας Πληροφοριακών Συστημάτων, η οποία συμπληρώνει την Πολιτική Ασφαλείας Πληροφοριών.

Η Πολιτική Ασφαλείας Πληροφοριακών Συστημάτων περιλαμβάνει συνήθως οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν στην προστασία των συστημάτων και με τις οποίες θα επιτευχθούν οι στόχοι ασφαλείας που έχουν ορισθεί. Πολλές από τις διατάξεις της εν λόγω πολιτικής σχετίζονται άμεσα και με τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας ενός Οργανισμού, όπως για παράδειγμα αυτές που καθορίζουν την υποχρέωση ελέγχου των συστημάτων από εξειδικευμένο προσωπικό σε περιπτώσεις περιστατικών ασφαλείας. Η συγκεκριμένη πολιτική πρέπει να γνωστοποιείται σε όλο το προσωπικό που αλληλεπιδρά με τα Πληροφοριακά Συστήματα και συμμετέχει με οποιονδήποτε τρόπο στις διαδικασίες ασφάλειας πληροφοριών, ενώ η εφαρμογή της θα πρέπει να ελέγχεται από τα αρμόδια, για το σκοπό, όργανα και τη Διοίκηση.

Με την εφαρμογή μιας Πολιτικής Ασφαλείας Πληροφοριακών Συστημάτων ένας Οργανισμός εξασφαλίζει την ύπαρξη ενός συστηματικού πλαισίου για την αντιμετώπιση των περιστατικών ασφάλειας πληροφοριών στα υπολογιστικά του συστήματα, καθορίζει τις ευθύνες κάθε οντότητας που συμμετέχει στις διαδικασίες και τον τρόπο επικοινωνίας μεταξύ των διάφορων τμημάτων, συμμορφώνεται με τις νομικές του υποχρεώσεις και ενισχύει την εμπιστοσύνη των συνεργατών του, επιτυγχάνοντας εν τέλει τη δημιουργία κουλτούρας ασφαλείας στο εσωτερικό της υποδομής του.

2.4 Πολιτικές Ασφαλείας Πληροφοριακών Συστημάτων στο Στρατιωτικό Περιβάλλον

Στο ελληνικό στρατιωτικό περιβάλλον, η ασφάλεια των πληροφοριών που διακινούνται στα Πληροφοριακά Συστήματα των Ενόπλων Δυνάμεων περιγράφεται τόσο στον **Εθνικό Κανονισμό Ασφαλείας (Ε.Κ.Α.)** [8], ο οποίος αποτελεί την Εθνική Πολιτική Ασφαλείας, όσο και στον **Στρατιωτικό Κανονισμό (Σ.Κ.) 80-20 «Κανονισμός Ασφαλείας Πληροφοριακών Συστημάτων»** [9], ο οποίος ουσιαστικά αποτελεί την Πολιτική Ασφαλείας Πληροφοριακών Συστημάτων του Στρατού Ξηράς. Επίσης, τα τελευταία χρόνια, οι κεντρικές υποδομές Πληροφορικής Υποστήριξης του Ελληνικού Στρατού έχουν πιστοποιηθεί κατά ISO 27001:2013 για τη λειτουργία Σύστηματος Διαχείρισης Ασφάλειας Πληροφοριών (Σ.Δ.Α.Π.) σύμφωνα με τα όσα ορίζει τα συγκεκριμένο πρότυπο. Τόσο στα αναγραφόμενα στο Σ.Δ.Α.Π. όσο και στα άρθρα των δύο συγγραμμάτων περιέχονται διατάξεις που άπτονται των θεμάτων της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, καθορίζοντας μεταξύ άλλων τον αποδεκτό τρόπο χρήσης των υπηρεσιακών Πληροφοριακών Συστημάτων και τα δικαιώματα των χρηστών καθώς και την υποχρέωση του αρμόδιου προσωπικού για έλεγχο των παρεχόμενων πόρων στις περιπτώσεις εμφάνισης οποιουδήποτε περιστατικού ασφαλείας. Για την πλήρη περιγραφή της λειτουργίας των δυνατοτήτων Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, εφόσον προχωρήσει η υλοποίησή τους στο στρατιωτικό περιβάλλον, θα απαιτηθεί η σύνταξη ιδιαίτερης αντίστοιχης πολιτικής η οποία θα καθορίζει όλες

τις απαραίτητες λεπτομέρειες. Στη συνέχεια της ενότητας παρατίθενται τα άρθρα των υφιστάμενων πολιτικών που αναφέρονται στα παραπάνω θέματα.

2.4.1 Εθνικός Κανονισμός Ασφαλείας (Ε.Κ.Α.)

Ο Εθνικός Κανονισμός Ασφαλείας [8] αποτελεί την Εθνική Πολιτική Ασφαλείας. Στο δεύτερο μέρος του, περιλαμβάνει διατάξεις που αφορούν στα τεχνικά και διαδικαστικά μέτρα ασφαλείας, τα οποία θα πρέπει να εφαρμόζονται και να ισχύουν για όλα τα εθνικά συστήματα και δίκτυα τα οποία διαχειρίζονται διαβαθμισμένες πληροφορίες. Αρκετές από τις διατάξεις του σχετίζονται τις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας. Οι κυριότερες είναι:

- **Άρθρο 51:** Στην παράγραφο 1 αναφέρεται ότι «*Η αυτόματη ή χειρόγραφη καταγραφή ενεργειών διατηρείται ως ημερολόγιο πρόσβασης στις διαβαθμισμένες πληροφορίες*». Τα αρχεία αυτόματης καταγραφής ενεργειών των χρηστών (log files) αποτελούν από τις σημαντικότερες πηγές πληροφοριών κατά τις διαδικασίες Ψηφιακής Εγκληματολογίας.

- **Άρθρο 52:** Στην παράγραφο 1 δηλώνεται η υποχρέωση ελέγχου όλων των μετακινούμενων μέσων αποθήκευσης διαβαθμισμένων πληροφοριών. Συγκεκριμένα αναφέρεται ότι «*Όλα τα μέσα αποθήκευσης που είναι δυνατόν να αφαιρεθούν (π.χ. σκληρός δίσκος, οπτικός δίσκος, μαγνητική ταινία, δισκέτα, κλπ.), όπου πρόκειται να αποθηκευτούν διαβαθμισμένες πληροφορίες, αναγνωρίζονται, σημαίνονται και ελέγχονται κατάλληλα. Η αναγνώριση και οι έλεγχοι περιλαμβάνουν τουλάχιστον τα εξής:*» και συνεχίζοντας στην υποπαράγραφο 1γ «*Περιοδικούς δειγματοληπτικούς ελέγχους και συγκέντρωση των μετακινούμενων μέσων αποθήκευσης για να εξασφαλίζεται η συμμόρφωση με τις υπάρχουσες διαδικασίες αναγνώρισης και ελέγχου. Όλα τα μετακινούμενα μέσα αποθήκευσης συγκεντρώνονται και ελέγχονται τουλάχιστον σε ετήσια βάση από τις αρμόδιες αρχές ασφαλείας*». Πέραν των προγραμματισμένων περιοδικών ελέγχων, γίνεται αντιληπτό ότι κατά τη διάρκεια εμφάνισης ενός περιστατικού ασφαλείας τα υπηρεσιακά μετακινούμενα μέσα αποθήκευσης που συνδέθηκαν με το προσβληθέν σύστημα αποτελούν αντικείμενα έκτακτου ελέγχου.

- **Άρθρο 59:** Το συγκεκριμένο άρθρο περί «Ελέγχου για την παρουσία επιβλαβούς λογισμικού – ιών υπολογιστών» στην παράγραφο 1 αναφέρει ότι «*Ο έλεγχος για την παρουσία επιβλαβούς λογισμικού και ιών υπολογιστών διεξάγεται σύμφωνα με τα αιτήματα της Εθνικής Αρχής Διαπίστευσης Ασφαλείας (Ε.Α.Δ.Α.)*», ορίζοντας την αρμόδια αρχή η οποία θα αιτηθεί τον ανάλογο έλεγχο ενός συστήματος από το εξειδικευμένο προσωπικό, σε περίπτωση υποψίας ή ανίχνευσης ενός περιστατικού ασφαλείας. Επίσης, στην παράγραφο 2 περιγράφεται η υποχρέωση κατά την οποία *«...περιοδικοί έλεγχοι πρέπει να γίνονται στο εγκατεστημένο λογισμικό. Οι έλεγχοι αυτοί πρέπει να γίνονται συχνότερα, εάν το Σύστημα Επικοινωνιών Πληροφορικής (ΣΕΠ) συνδέεται με άλλο ΣΕΠ ή εάν συνδέεται με δίκτυο διαβίβασης δεδομένων*».

- **Άρθρο 65:** Το συγκεκριμένο άρθρο εντάσσει σε παρόμοιους ελέγχους με αυτούς που αναφέρθηκαν στο άρθρο 52 για τα μετακινούμενα μέσα αποθήκευσης και τους μικροϋπολογιστές, αναφέροντας ότι «*Οι μικροϋπολογιστές με ενσωματωμένους σκληρούς δίσκους (ή άλλα μέσα αποθήκευσης σταθερής μνήμης), που λειτουργούν είτε ανεξάρτητα είτε σε δίκτυο και τα φορητά μηχανήματα (για παράδειγμα φορητοί υπολογιστές και ηλεκτρονικά βοηθήματα) με ενσωματωμένους δίσκους, θεωρούνται ως μέσα αποθήκευσης πληροφοριών με την ίδια έννοια όπως οι δισκέτες ή άλλα μετακινούμενα μέσα αποθήκευσης υπολογιστών*».

- **Άρθρο 66:** «*Απαγορεύεται η χρήση ιδιωτικών μέσων αποθήκευσης υπολογιστών, λογισμικού και υλικού ΣΕΠ (για παράδειγμα μικροϋπολογιστές και φορητά μηχανήματα) για αποθήκευση, επεξεργασία και διαβίβαση διαβαθμισμένων πληροφοριών*». Με το παραπάνω άρθρο απαγορεύεται η χρήση οποιουδήποτε προσωπικού εξοπλισμού Πληροφορικής από τους χρήστες για την εκτέλεση των καθηκόντων που σχετίζονται με την μεταχείριση διαβαθμισμένων πληροφοριών. Με αυτόν τον τρόπο θωρακίζεται και διευκολύνεται το έργο του προσωπικού Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, αφού οι υπηρεσιακοί πόροι αποτελούν περιουσία της εκάστοτε υπηρεσίας, παρέχονται για την εκτέλεση συγκεκριμένης υπηρεσιακής εργασίας και υπόκεινται στους άμεσους ελέγχους αυτής από το εξειδικευμένο προσωπικό.

2.4.2 Στρατιωτικός Κανονισμός 80-20

Ο Στρατιωτικός Κανονισμός (Σ.Κ.) 80-20 με τίτλο «Κανονισμός Ασφαλείας Πληροφοριακών Συστημάτων» [9], καθορίζει τις αρχές και την Πολιτική Ασφαλείας Πληροφοριακών Συστημάτων του Στρατού Ξηράς και περιγράφει τις βασικές υποχρεώσεις ασφαλείας που έχει το προσωπικό το οποίο χρησιμοποιεί μέσα πληροφορικής αλλά και γενικότερα όσοι επεξεργάζονται στρατιωτικά δεδομένα και πληροφορίες με αξιοποίηση της τεχνολογίας των πληροφοριών. Ο κανονισμός αυτός συμπληρώνει τον Ε.Κ.Α. στα εξειδικευμένα θέματα της ασφάλειας Πληροφοριακών Συστημάτων και οι χρήστες θα πρέπει υποχρεωτικά να λαμβάνουν γνώση των διατάξεών του. Παρά το γεγονός ότι πραγματεύεται σε γενικότερο πλαίσιο τα θέματα ασφαλείας, αρκετές από τις παραγράφους του σχετίζονται άμεσα με τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας και θα αποτελέσουν τα συνδετικά σημεία στην περίπτωση δημιουργίας ξεχωριστής πολιτικής για τον εν λόγω τομέα. Παρακάτω γίνεται αναφορά σε μερικές από τις παραγράφους που προσεγγίζουν τα θέματα ενδιαφέροντος:

- **Παράγραφος 14:** Στη συγκεκριμένη παράγραφο περιγράφονται οι ειδικές απαιτήσεις τις οποίες πρέπει να πληρούν τα στρατιωτικά επιχειρησιακά Πληροφοριακά Συστήματα. Ειδικότερα, στην πρώτη υποπαράγραφο αναλύεται η απαίτηση για επιβιωσιμότητα, δηλαδή «*η δυνατότητα ενός συστήματος να λειτουργεί ικανοποιητικά και με προκαθορισμένα επίπεδα απόδοσης σε περιπτώσεις εχθρικών πράξεων,*

καταστροφών ή οποιασδήποτε άλλης μορφής αστοχιών και ανθρωπίνων σφαλμάτων». Το χαρακτηριστικό αυτό βρίσκεται σε άμεση σχέση με τους στόχους Επιχειρησιακής Συνέχειας των διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας, όπως αυτοί περιγράφονται στο επόμενο κεφάλαιο. Επιπρόσθετα, στα ενδεικνυόμενα μέτρα για την εξασφάλιση της επιβιωσιμότητας αναφέρεται και η «*δυνατότητα απόκρουσης επιθέσεων άρνησης παροχής υπηρεσιών στα πλαίσια εχθρικών επιχειρήσεων Κυβερνοπολέμου*», η οποία επίσης εντάσσεται στα καθήκοντα της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας.

- **Παράγραφος 15:** Στις αρμοδιότητες και υποχρεώσεις των χρηστών για την ασφάλεια των Πληροφοριακών Συστημάτων περιλαμβάνονται *«…η υποχρέωση και ευθύνη να συμβάλλουν στην επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων Πληροφορικής και να αναφέρουν οποιοδήποτε γεγονός υποπέσει στην αντίληψή τους που μπορεί να οδηγήσει σε παραβίαση της ασφάλειας του συστήματος*» καθώς και *«…η επαγρύπνηση για τον εντοπισμό πιθανής προσπάθειας μη εξουσιοδοτημένης πρόσβασης, στο τμήμα του συστήματος που εργάζονται (αρχεία, προγράμματα κ.α.) και η αναφορά σχετικά*». Πρόκειται για ορισμένους από τους τρόπους με τους οποίους πραγματοποιείται το στάδιο της Ανίχνευσης Περιστατικών σε ένα μοντέλο διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας. Για να εκμεταλλευθούν στο έπακρο οι υποχρεώσεις των χρηστών, στην ιδιαίτερη πολιτική που θα συνταχθεί θα πρέπει να καθοριστεί ο ακριβής τρόπος και οι αναγκαίες πληροφορίες οι οποίες θα πρέπει να αναφέρονται άμεσα στο αρμόδιο προσωπικό, ώστε να προσδιορισθεί όσον το δυνατόν καλύτερα το περιστατικό και να ξεκινήσουν οι προβλεπόμενες ενέργειες αντιμετώπισής του.

- **Παράγραφος 16:** Όσον αφορά στην υπευθυνότητα σχετικά με την πρόσβαση στις πληροφορίες, ο Σ.Κ. 80-20 ορίζει ότι «*Όλα τα δεδομένα του συστήματος ανήκουν στη δικαιοδοσία της Υπηρεσίας η οποία και ευθύνεται, δια των οργάνων ασφαλείας, για την προστασία των διαβαθμισμένων πληροφοριών*» και ότι «*Υπεύθυνος για το σύνολο των δεδομένων του συστήματος είναι ο Διευθυντής ή Διοικητής, ο οποίος έχει και την ευθύνη ασφαλείας των πληροφοριών που απορρέουν από την επεξεργασία τους*». Από τα παραπάνω συμπεραίνεται ότι ο επικεφαλής ενός Οργανισμού ή Υπηρεσίας έχει τη συνολική ευθύνη για τις πληροφορίες που διακινούνται στα Πληροφοριακά Συστήματα και πρέπει να ενεργεί ανάλογα όταν υποπτεύεται ή διαπιστώνει περιστατικά ασφαλείας. Οι διακινούμενες πληροφορίες χαρακτηρίζονται ως ιδιοκτησία της Υπηρεσίας και όχι προσωπικά δεδομένα ενός συγκεκριμένου χρήστη, οπότε μπορούν να συλλεχθούν και να αναλυθούν από το εξειδικευμένο προσωπικό στα πλαίσια των ερευνών ενός περιστατικού ασφαλείας, κατόπιν αιτήσεως του έχοντος την ευθύνη ασφαλείας τους.

- **Παράγραφος 18:** Η πολιτική ασφαλείας, με τη συγκεκριμένη παράγραφο, επιβάλλει την υποχρέωση ύπαρξης Σχεδίου Επαναλειτουργίας για κάθε σύστημα ξεχωριστά. Το παραπάνω σχέδιο δύναται να αποτελεί επιμέρους τμήμα του γενικότερου Σχεδίου Επιχειρησιακής Συνέχειας ενός Οργανισμού, το οποίο με τη σειρά του αποτελεί εργαλείο για την υλοποίηση ενός εκ των

πρωταρχικών στόχων της Αντιμετώπισης Περιστατικών Ασφαλείας που αφορά στην άμεση αποκατάσταση της λειτουργίας των συστημάτων. Συγκεκριμένα, στην πολιτική αναφέρεται ότι «*Επιβάλλεται η ύπαρξη Σχεδίου Επαναλειτουργίας του Συστήματος σε περιπτώσεις που αυτό ή κάποιο μέρος του σταματήσει να λειτουργεί…*» και ότι πρέπει απαραίτητα να προηγηθεί «*Αναγνώριση των πιθανότερων αιτιών μερικής ή ολικής κατάρρευσης του συστήματος. Απαιτείται συγκεκριμένη ανάλυση και προσδιορισμός των αποτελεσμάτων της κάθε αιτίας ξεχωριστά*», ενέργειες που προβλέπονται στο στάδιο Αρχικής Αντιμετώπισης ενός μοντέλου διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας.

- **Παράγραφος 19:** Ανάμεσα στα μέτρα για την ασφάλεια των προσωπικών υπολογιστών, και σε συνέχεια των όσων αναφέρθηκαν στην παράγραφο 16, αναφέρεται η «*Απαγόρευση σύνδεσης σε προσωπικούς υπολογιστές μη εγκεκριμένου υλικού. Ιδιαιτέρως σημαντική είναι η αποτροπή σύνδεσης σε προσωπικούς υπολογιστές κινητών τηλεφώνων, έξυπνων τηλεφώνων, συσκευών αναπαραγωγής μουσικής κλπ. καθώς διαθέτουν αποθηκευτικούς χώρους μεγάλης χωρητικότητας και μπορούν να μεταφέρουν εκούσια ή ακούσια το μεγαλύτερο μέρος των διαθέσιμων δεδομένων ενός προσωπικού υπολογιστή*». Το συγκεκριμένο μέτρο είναι ιδιαιτέρως σημαντικό καθώς, όπως αναφέρθηκε, τα δεδομένα που διακινούνται στα στρατιωτικά Πληροφοριακά Συστήματα αποτελούν ιδιοκτησία της Υπηρεσίας και υπεύθυνος για τις πληροφορίες ο Διοικητής ή Διευθυντής της. Στην περίπτωση κατά την οποία μεταφερθούν υπηρεσιακά δεδομένα σε μια συσκευή προσωπικής ιδιοκτησίας ενός χρήστη, οι διαδικασίες Ψηφιακής Εγκληματολογίας που θα πραγματοποιηθούν στα πλαίσια της έρευνας ενός περιστατικού διαρροής πληροφοριών είναι πιθανό να συναντήσουν εμπόδια νομικής φύσεως σχετικά με την προστασία των προσωπικών δεδομένων του χρήστη.

- **Παράγραφος 80:** Παρά το γεγονός ότι η υποχρέωση τήρησης αναλυτικών αρχείων καταγραφής (log files) τονίζεται σε πολλά σημεία τόσο της παρούσας πολιτικής ασφαλείας όσο και του Ε.Κ.Α., στη συγκεκριμένη παράγραφο, η οποία περιλαμβάνεται στις Βασικές Οδηγίες Ασφαλείας, περιγράφεται αναλυτικά η υποχρέωση στο σύνολό της, αναφέροντας ότι «*Στο σύστημα θα πρέπει να τηρούνται αρχεία που να καταγράφουν κάθε συμβάν σχετικό με την ασφάλεια του συστήματος. Τα αρχεία αυτά θα πρέπει να φυλάσσονται για συγκεκριμένο χρονικό διάστημα, ώστε να είναι δυνατή η αξιοποίησή τους σε ενδεχόμενες έρευνες. Θα πρέπει να περιλαμβάνουν την ταυτότητα των χρηστών, τον ακριβή χρόνο σύνδεσης και αποσύνδεσης των χρηστών, το τερματικό το οποίο χρησιμοποίησε ο χρήστης και τις επιτυχείς και ανεπιτυχείς προσπάθειες του χρήστη να προσπελάσει το σύστημα ή δεδομένα του συστήματος. Κάποια από τα αρχεία που τηρούνται στο σύστημα είναι δυνατό να διατηρούνται για μεγαλύτερα χρονικά διαστήματα, σύμφωνα με τις ανάγκες τις Υπηρεσίας ή τη σχετική νομοθεσία*». Η εφαρμογή της οδηγίας έχει σαν αποτέλεσμα την ύπαρξη μιας σημαντικής πηγής πληροφοριών για τις έρευνες σχετικά με ένα περιστατικό ασφαλείας, ενώ παράλληλα αποτελεί νομική υποχρέωση του Οργανισμού αλλά και σημείο επιθεώρησης κατά της διαδικασίες πιστοποίησης και διαπίστευσής του.

2.4.3 Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών Ε.Σ.

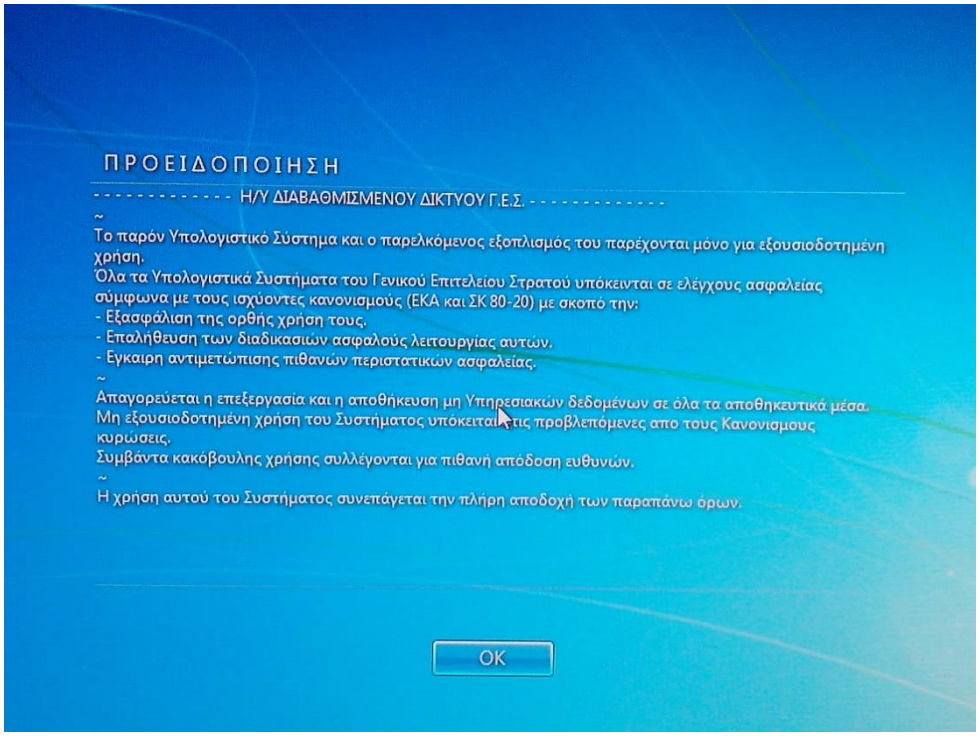
Στην τεκμηρίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Σ.Δ.Α.Π.) του Ε.Σ., περιλαμβάνονται αρκετές διατάξεις οι οποίες αναφέρονται σε θέματα που βρίσκονται σε άμεση σχέση με τις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας. Ειδικότερα, σε ότι αφορά στην ενημέρωση των τελικών χρηστών, οι οποίοι αποτελούν και τη σημαντικότερη παράμετρο για την ασφάλεια ενός Πληροφοριακού Συστήματος, σχετικά με τον τρόπο χρήσης των υπηρεσιακών πόρων αλλά και των υποχρεώσεων και δικαιωμάτων τους, το Σ.Δ.Α.Π. προβλέπει τη συμπλήρωση ειδικού εντύπου αίτησης για τη χορήγηση δικαιωμάτων πρόσβασης στα Πληροφοριακά Συστήματα αλλά και την εμφάνιση ειδικού προειδοποιητικού μηνύματος (warning banner) κατά την έναρξη λειτουργίας ενός συστήματος.

Με το έντυπο αίτησης εισόδου στα υπηρεσιακά Πληροφοριακά Συστήματα επιτυγχάνεται η ταχεία και περιληπτική ενημέρωση κάθε νέου χρήστη σχετικά με τις διατάξεις του Ε.Κ.Α. και του Σ.Κ. 80-20, οι οποίες αφορούν στις υποχρεώσεις των τελικών χρηστών και αναγράφονται υπό την μορφή όρων παροχής πρόσβασης στη συγκεκριμένη αίτηση. Για να χορηγηθεί άδεια πρόσβασης σε ένα χρήστη, μεταξύ άλλων ενημερώνεται ότι:

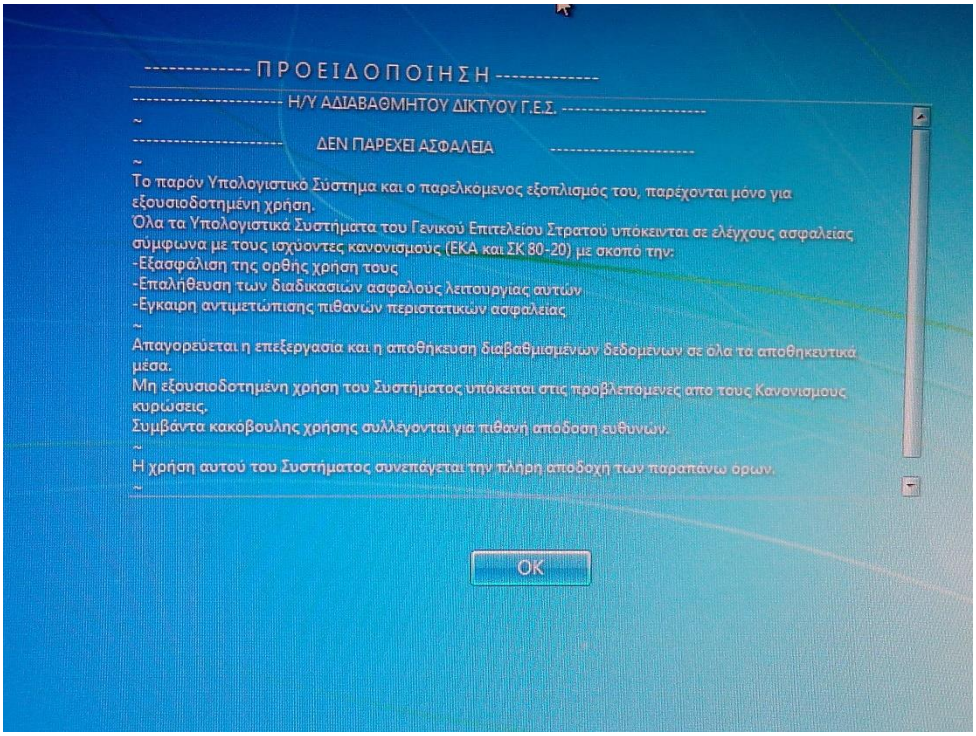
- Αποτελεί υποχρέωσή του να συμβάλλει στην επίτευξη υψηλού επιπέδου ασφάλειας των υπηρεσιακών Πληροφοριακών Συστημάτων.
- Οφείλει να αναφέρει άμεσα οποιοδήποτε γεγονός υποπέσει στην αντίληψή του και το οποίο μπορεί να οδηγήσει σε παραβίαση της ασφάλειας των συστημάτων.
- Είναι υπεύθυνος για την αποκλειστική χρησιμοποίηση των Η/Υ για υπηρεσιακή χρήση και ότι τα αρχεία που δημιουργεί στα συστήματα Πληροφορικής στης Υπηρεσίας παραμένουν στην ιδιοκτησία της.
- Η αποθήκευση εγγράφων προσωπικού ενδιαφέροντος δεν επιτρέπεται στους υπηρεσιακούς Η/Υ.
- Κάθε προσπάθεια παραβίασης της ασφάλειας των Πληροφοριακών Συστημάτων ή πρόσβασης σε μη επιτρεπόμενη περιοχή αρχείων καταγράφεται από τα συστήματα ασφαλείας του δικτύου και της εκάστοτε εφαρμογής.
- Δεν επιτρέπεται η χρησιμοποίηση προσωπικών μέσων αποθήκευσης ή προσωπικών Η/Υ.
- Οφείλει να εξασφαλίζει ότι οι ενέργειές του δεν διακυβεύουν την ασφάλεια των συστημάτων Πληροφορικής και να δέχεται τους προγραμματισμένους ή αιφνιδιαστικούς ελέγχους από το εξουσιοδοτημένο προσωπικό ασφαλείας στους Η/Υ που χρησιμοποιεί.

Τα ειδικά προειδοποιητικά μηνύματα (warning banners) κατά την έναρξη λειτουργίας ενός συστήματος, αποτελούν ακόμα ένα μέτρο ώστε να υπενθυμίζονται οι υποχρεώσεις που αναλαμβάνουν οι χρήστες κάθε φορά που

πρόκειται να χρησιμοποιήσουν τα υπηρεσιακά συστήματα καθώς και το δικαίωμα της Υπηρεσίας να εκτελεί, μέσω του κατάλληλου προσωπικού, τους αναγκαίους ελέγχους ασφαλείας. Οι παρακάτω εικόνες παρουσιάζουν τα προβαλλόμενα μηνύματα τόσο στο εσωτερικό διαβαθμισμένο δίκτυο όσο και στο δίκτυο που παρέχει πρόσβαση στο Διαδίκτυο.



Εικόνα 2.1 : Προειδοποιητικό Μήνυμα Διαβαθμισμένου Δικτύου



Εικόνα 2.2 : Προειδοποιητικό Μήνυμα Αδιαβάθμητου Δικτύου

2.5 Συμπεράσματα

Στο παρόν κεφάλαιο παρουσιάστηκαν οι διατάξεις τόσο της Ελληνικής Νομοθεσίας όσο και των πολιτικών ασφαλείας, που ισχύουν στο ελληνικό στρατιωτικό περιβάλλον, οι οποίες προσεγγίζουν κάποια επιμέρους θέματα που αφορούν στις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας. Τα θέματα αυτά σχετίζονται με την προστασία της ιδιωτικότητας των χρηστών από τη συλλογή και εξέταση δεδομένων προσωπικού χαρακτήρα, το δικαίωμα πραγματοποίησης ελέγχων από έναν Οργανισμό στους πόρους που παρέχει για την εκτέλεση των εργασιών του καθώς και τη μεταχείριση των ψηφιακών δεδομένων ως αποδεικτικών στοιχείων για τις έρευνες ενός περιστατικού ασφαλείας.

Όσον αφορά στο δικαίωμα των χρηστών στην ιδιωτικότητα, αυτό προστατεύεται τόσο από τους ισχύοντες νόμους όσο και από το Σύνταγμα. Συνοπτικά, κάθε πολίτης έχει το δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως αυτά ορίζονται από το νόμο. Στο στρατιωτικό περιβάλλον όμως, σύμφωνα με τις ισχύουσες πολιτικές ασφαλείας, τα υπηρεσιακά συστήματα παρέχονται αυστηρά και μόνο για υπηρεσιακή χρήση και οι πληροφορίες που διακινούνται σε αυτά αποτελούν ιδιοκτησία της Υπηρεσίας. Η αποθήκευση οποιουδήποτε αρχείου προσωπικού ενδιαφέροντος σε αυτά απαγορεύεται, όπως επίσης απαγορεύεται η χρησιμοποίηση οποιασδήποτε προσωπικής συσκευής αποθήκευσης (φορητό μέσο αποθήκευσης, κινητό τηλέφωνο κτλ.) ή προσωπικού υπολογιστή. Κάθε ενέργεια που πραγματοποιείται από τους χρήστες στα υπηρεσιακά συστήματα και στις εφαρμογές καταγράφεται, γεγονός το οποίο αποτελεί απαραίτητη προϋπόθεση για τη χορήγηση δικαιωμάτων χρήσης και τους γνωστοποιείται κάθε φορά που αποκτούν πρόσβαση. Από τα παραπάνω συμπεραίνεται ότι όσον αφορά στα υπηρεσιακά Πληροφοριακά Συστήματα, οι χρήστες δεν μπορούν να έχουν κάποια εύλογη απαίτηση για ιδιωτικότητα αναφορικά με τα δεδομένα που διαχειρίζονται, αφού θεωρείται ότι δεν αποτελούν δεδομένα προσωπικού χαρακτήρα αλλά υπηρεσιακά. Συνεπακόλουθα, στην περίπτωση που το εξειδικευμένο προσωπικό Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας συλλέξει ένα σύστημα για εξέταση, κατόπιν διαταγής και στα πλαίσια εκτέλεσης ερευνών ενός περιστατικού ασφαλείας, δεν παραβιάζεται κάποιο δικαίωμα του χρήστη. Παράλληλα, η ύπαρξη των αρχείων καταγραφής ενεργειών, τα οποία μπορεί να συλλεχθούν για την εξακρίβωση των παραμέτρων ενός περιστατικού, είναι εις γνώση των χρηστών και συχνά αποτελεί λειτουργική απαίτηση ενός συστήματος ή εφαρμογής.

Επίσης, σκοπός της Διοίκησης ενός Οργανισμού, όπως εκφράζεται μέσα από την πολιτική ασφαλείας του, είναι η επίτευξη του μέγιστου δυνατού επιπέδου ασφάλειας στις υποδομές του και από την στιγμή που φέρει την ευθύνη για την ασφάλεια των πληροφοριών που διακινούνται στα Πληροφοριακά Συστήματα ιδιοκτησίας της, έχει το δικαίωμα να πραγματοποιεί τους απαραίτητους ελέγχους μέσω του εξειδικευμένου, για το σκοπό, προσωπικού. Στην ιδιαίτερη περίπτωση του στρατιωτικού περιβάλλοντος,

εφόσον συντρέχουν επαρκείς λόγοι, η διεξαγωγή ερευνών μπορεί να θωρακιστεί νομικά και από το άρθρο 19 του Συντάγματος, για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Τέλος, η μεταχείριση των ψηφιακών δεδομένων ως αποδεικτικών στοιχείων και οι προϋποθέσεις που πρέπει να συντρέχουν ώστε να εξασφαλίζεται η εγκυρότητά τους, δεν προβλέπονται επακριβώς από καμία διάταξη της ελληνικής νομοθεσίας. Το μόνο σημείο που μπορεί να βρει εφαρμογή στη συγκεκριμένη περίπτωση είναι επίσης το άρθρο 19 του Συντάγματος, το οποίο απαγορεύει τη χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση των άρθρων περί προστασίας δεδομένων προσωπικού χαρακτήρα. Η περαιτέρω εξέταση των ψηφιακών αποδεικτικών στοιχείων σχετικά με ένα περιστατικό ασφαλείας γίνεται κατά αναλογία των νομοθετικών διατάξεων που αφορούν στα αποδεικτικά στοιχεία με «φυσική» υπόσταση. Οι Οργανισμοί οφείλουν, μέσα από τις πολιτικές ασφαλείας τους και λόγω ανυπαρξίας των κατάλληλων νόμων, να καθορίσουν τα απαραίτητα κριτήρια για το προσωπικό καθώς και αναλυτικές διαδικασίες αναγνώρισης, συλλογής και εξέτασης των δεδομένων που κρίνονται ως πειστήρια, οι οποίες θα στηρίζονται σε διεθνώς αναγνωρισμένες και αποδεκτές πρακτικές, ώστε να εξασφαλίζουν το μέγιστο δυνατό επίπεδο αξιοπιστίας και εγκυρότητας των αποτελεσμάτων στα οποία καταλήγουν οι έρευνες.

Από τα παραπάνω γίνεται αντιληπτό ότι η απουσία συγκεκριμένης νομοθεσίας που να πραγματεύεται τις παραμέτρους των δυνατοτήτων Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, δημιουργεί συνθήκες αβεβαιότητας και αμφιβολιών, με αποτέλεσμα οι αποφάσεις των αρμόδιων δικαστικών αρχών να μην στηρίζονται σε ένα καθορισμένο πλαίσιο αλλά να προκύπτουν κατά το δοκούν και σύμφωνα με το επίπεδο τεχνικών γνώσεων του εκάστοτε δικαστικού. Ως αποτέλεσμα, οι πολιτικές ασφαλείας που καταρτίζουν οι Οργανισμοί δεν είναι βέβαιο ότι θα είναι σύμφωνες με τις νομικές απαιτήσεις, αφού οι τελευταίες δεν ορίζονται με σαφήνεια. Ως ένα βαθμό το γεγονός αυτό δικαιολογείται από τη δυσκολία του νομοθετικού έργου να ακολουθήσει τις συνεχείς τεχνολογικές εξελίξεις στον τομέα της Πληροφορικής. Παρόλα αυτά, και λόγω της συνεχούς αύξησης του αριθμού των περιστατικών ασφαλείας που ανιχνεύονται σε συστήματα που διαχειρίζονται διαβαθμισμένες πληροφορίες εξαιρετικής σημασίας, όπως τα στρατιωτικά Πληροφοριακά Συστήματα, απαιτείται η συνεργασία νομικών και τεχνικών οργάνων για τη δημιουργία ενός, όσο το δυνατόν, πλήρους νομοθετικού πλαισίου που θα διευκρινίζει και τα θέματα ενδιαφέροντος Ψηφιακής Εγκληματολογίας. Ταυτόχρονα, αντίστοιχη προσπάθεια οφείλει να πραγματοποιηθεί και από τους Οργανισμούς στην κατάρτιση ιδιαίτερων Πολιτικών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, οι οποίες θα περιλαμβάνουν διαδικασίες που θα εξασφαλίζουν την προστασία των δικαιωμάτων των χρηστών, την αξιοπιστία των χρησιμοποιούμενων μεθόδων και την εγκυρότητα των εξαγόμενων συμπερασμάτων.

Κεφάλαιο 3ο
Αντιμετώπιση Περιστατικών Ασφαλείας και Ψηφιακή Εγκληματολογία

3.1 Εισαγωγή

Σύμφωνα με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Η.Π.Α. (National Institute of Standards and Technology – NIST), ως περιστατικό ασφαλείας υπολογιστών δύναται να οριστεί «η παραβίαση ή η απειλή επικείμενης παραβίασης των Πολιτικών Ασφαλείας Υπολογιστών, των Πολιτικών Ορθής Χρήσης ή των καθορισμένων Πολιτικών Ασφαλείας Πληροφοριών» [11].

Λόγω της συνεχούς εξέλιξης της επιστήμης των υπολογιστών και της ανθρώπινης φύσης, ο τύπος και ο τρόπος εκδήλωσης μιας απειλής δεν είναι πάντοτε δυνατό να προβλεφθούν, ώστε να ληφθούν αποτελεσματικά μέτρα ασφάλειας. Οι Οργανισμοί θα πρέπει, σε γενικές γραμμές, να είναι έτοιμοι να αντιμετωπίσουν κάθε περιστατικό ασφαλείας δίνοντας κυρίως έμφαση στην άρτια προετοιμασία τους για την αντιμετώπιση επιθέσεων στις οποίες χρησιμοποιούνται οι πλέον συνηθισμένοι φορείς επιθέσεων, όπως εξωτερικά ή αφαιρούμενα μέσα αποθήκευσης, οι εξαντλητικές δοκιμές (brute force attacks), ο Παγκόσμιος Ιστός, τα μηνύματα ηλεκτρονικού ταχυδρομείου, η παράτυπη χρήση πόρων και η απώλεια ή υποκλοπή πληροφοριών και εξοπλισμού. Η τεχνική ανάλυση που θα πραγματοποιηθεί σε μεταγενέστερο χρόνο στα ευρήματα της επίθεσης μπορεί να οδηγήσει σε σημαντικά συμπεράσματα σχετικά με τον υπεύθυνο και τις αδυναμίες που εκμεταλλεύθηκε για να απειλήσει, ώστε να γίνουν οι κατάλληλες διορθωτικές ενέργειες.

Κατόπιν των παραπάνω, τόσο η Αντιμετώπιση Περιστατικών Ασφαλείας, ως διαδικασία, όσο και η Ψηφιακή Εγκληματολογία αποτελούν αναπόσπαστα κομμάτια του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) ενός Οργανισμού. Η ένταξή τους στις πολιτικές ασφαλείας προϋποθέτει την αλληλεπίδραση και συμμετοχή στις διαδικασίες και των υπολοίπων συστατικών ενός ΣΔΑΠ, όπως το ανθρώπινο δυναμικό και οι υποδομές.

Στο υπόλοιπο του κεφαλαίου αναλύονται οι έννοιες και τα μοντέλα διαδικασιών της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας ξεχωριστά, καθώς και οι σκοποί που επιδιώκονται στα πλαίσια της Πολιτικής Ασφαλείας Πληροφοριών ενός Οργανισμού. Η διαπίστωση ότι πρόκειται για λειτουργίες μερικώς επικαλυπτόμενες, με δυσκολία στην διάκριση των ορίων της καθεμιάς, αλλά και οι περιορισμοί που σχετίζονται κυρίως με το προσωπικό του στρατιωτικού περιβάλλοντος, καταδεικνύουν την ανάγκη για την προδιαγραφή ενός ενιαίου ολοκληρωμένου μοντέλου ενεργειών.

3.2 Αντιμετώπιση Περιστατικών Ασφαλείας (Incident Response)

Η Αντιμετώπιση Περιστατικών Ασφαλείας είναι ο τρόπος με τον οποίο ένας Οργανισμός έχει αποφασίσει να χειρίζεται περιπτώσεις παράνομων ή μη αποδεκτών, βάσει των πολιτικών του, ενεργειών οι οποίες περιλαμβάνουν υπολογιστικά συστήματα ή δικτυακές υποδομές, ώστε να περιορίσει τον αντίκτυπό τους στη λειτουργία του [4].

Στο τυπικό και ευρέως αποδεκτό μοντέλο [1], οι ενέργειες ξεκινούν πριν από την εμφάνιση ενός περιστατικού, με τη διαρκή προετοιμασία του Οργανισμού για την αντιμετώπιση πιθανών απειλών. Πρακτικά αυτό επιτυγχάνεται με την εφαρμογή μέτρων έγκαιρης ανίχνευσης απειλών, όπως για παράδειγμα ένα Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System – IDS). Εκτός από τον παραπάνω τρόπο, η ανίχνευση ενός περιστατικού μπορεί να γίνει κατόπιν παρατήρησης και αναφοράς από οποιονδήποτε χρήστη, με προκαθορισμένες διαδικασίες που προβλέπονται στην ισχύουσα πολιτική ασφαλείας. Στη συνέχεια το προσωπικό που θα χειριστεί το περιστατικό, συνεργαζόμενο με τα επιμέρους τμήματα, συγκεντρώνει πληροφορίες από κάθε διαθέσιμη πηγή, ώστε να σχηματίσει εικόνα για το αν πρόκειται για υπαρκτό συμβάν, ποια συστήματα και χρήστες επηρεάζονται και ποια είναι η πιθανή ζημιά που μπορεί να προκληθεί. Τα παραπάνω, με την έγκριση της Διοίκησης του Οργανισμού και έχοντας υπόψη το ποσοστό ανοχής σε περιστατικά ασφαλείας, συντελούν στο να διαμορφωθεί η κατάλληλη στρατηγική αντιμετώπισης του περιστατικού.

Στο καθαρά τεχνικό μέρος της διαδικασίας, τα ψηφιακά στοιχεία που αφορούν στο συμβάν συλλέγονται, εξετάζονται και αναλύονται χρησιμοποιώντας αποδεκτές μεθόδους και εργαλεία Ψηφιακής Εγκληματολογίας, ώστε να γίνει κατανοητό τι ακριβώς έχει συμβεί, να προκύψει το χρονοδιάγραμμα του περιστατικού και να υιοθετηθεί ή απορριφθεί κάθε πιθανό σενάριο.

Τα αποτελέσματα της έρευνας, όπως και κάθε ενέργεια που πραγματοποιήθηκε από το αρμόδιο προσωπικό, καταγράφονται στην αναφορά που τεκμηριώνει το περιστατικό με τέτοιο τρόπο, ώστε να μπορεί να χρησιμοποιηθεί σε πιθανές δικαστικές λειτουργίες ή εσωτερικές πειθαρχικές διαδικασίες.

Τέλος, κατά την απενημέρωση της υπόθεσης, αποφασίζεται εάν απαιτείται η λήψη επιπλέον μέτρων για τον περιορισμό των περιστατικών ασφαλείας, επιλύονται τα διαπιστωμένα προβλήματα στα Πληροφοριακά Συστήματα που είχαν ως αποτέλεσμα την εμφάνιση του περιστατικού και επικαιροποιούνται οι πολιτικές ασφαλείας και οι προ τυποποιημένες διαδικασίες ώστε να εξασφαλιστεί, στο μέτρο του δυνατού, ότι παρόμοια περιστατικά δεν θα προκύψουν στο μέλλον.

Εκτός από τις ενέργειες που πραγματοποιούνται στο εσωτερικό του Οργανισμού, θα πρέπει να έχουν προβλεφθεί και διαδικασίες που να καθορίζουν τον τρόπο συνεργασίας της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας με την Αστυνομία, εφόσον το συμβάν περιλαμβάνεται στα πλαίσια της δικαιοδοσίας της, καθώς και τον τρόπο χειρισμού και παρουσίασης του περιστατικού στα ΜΜΕ. Ιδιαίτερα στην περίπτωση του στρατιωτικού

περιβάλλοντος, η παραπάνω διαδικασία είναι άκρως σημαντική για την εικόνα και το κύρος των Ενόπλων Δυνάμεων απέναντι στους πολίτες.

Από τα παραπάνω προκύπτει το συμπέρασμα ότι η Αντιμετώπιση Περιστατικών Ασφαλείας αποτελεί κυρίως μια διαχειριστική διαδικασία ενός περιστατικού ασφαλείας, η οποία καθορίζει το πώς τα υπόλοιπα τμήματα εντός (ανθρώπινο δυναμικό, νομικό τμήμα) ή εκτός (αστυνομία, ομάδες άλλων οργανισμών, ΜΜΕ) ενός Οργανισμού θα συνεργαστούν με το αρμόδιο προσωπικό με σκοπό να διαχειριστούν το πρόβλημα, ώστε να περιορίσουν τις επιπτώσεις του και να επαναφέρουν την κανονική ροή λειτουργίας όσο το δυνατόν συντομότερα, τροποποιώντας εφόσον απαιτείται και τις ισχύουσες διαδικασίες. Το τεχνικό μέρος, στο οποίο πραγματοποιείται η ανάλυση των ψηφιακών στοιχείων που έχουν συλλεχθεί, περιλαμβάνεται στη διαδικασία, αλλά δεν είναι πρώτης προτεραιότητας, όπως συμβαίνει στην εξειδικευμένη περίπτωση της Ψηφιακής Εγκληματολογίας. Υπάρχει, για παράδειγμα, η πιθανότητα η πολιτική ενός Οργανισμού να καθορίζει ως αποδεκτή τακτική Αντιμετώπισης Περιστατικών Ασφαλείας την εγκατάσταση των λειτουργικών συστημάτων και εφαρμογών των μηχανημάτων από την αρχή ώστε να αποκατασταθεί άμεσα η κανονική ροή λειτουργίας, αδιαφορώντας για την αιτία που προκάλεσε το περιστατικό.

3.3 Ψηφιακή Εγκληματολογία (Digital Forensics)

Με τον όρο Ψηφιακή Εγκληματολογία περιγράφουμε την εφαρμογή των μέσων της επιστήμης των υπολογιστών στην αναγνώριση, συλλογή, εξέταση και ανάλυση των ψηφιακών δεδομένων που αφορούν σε μια υπόθεση, εξασφαλίζοντας ταυτόχρονα την ακεραιότητα των πληροφοριών και ακολουθώντας τις αυστηρά προκαθορισμένες διαδικασίες τήρησης και χειρισμού των δεδομένων [2].

Η Ψηφιακή Εγκληματολογία χωρίζεται σε κατηγορίες ανάλογα με το τεχνολογικό αντικείμενο το οποίο εξετάζεται, περιέχει τα δεδομένα που σχετίζονται με μια υπόθεση και στο οποίο τελικά θα εφαρμοσθούν οι μέθοδοι συλλογής. Οι όροι «Ασφαλής Ανάκτηση και Ανάλυση Ψηφιακών Δεδομένων», «Συστηματική Διερεύνηση Υπολογιστών» και «Δικανική Υπολογιστών» χρησιμοποιούνται ως συνώνυμα της «Εγκληματολογίας Υπολογιστών» (Computer Forensics), ορίζοντας μια σύγχρονη επιστημονική περιοχή, αντικείμενο της οποίας είναι η έρευνα και ανάλυση των ψηφιακών δεδομένων ενός υπολογιστή, με σκοπό την εξαγωγή ακέραιων, αδιάβλητων και νομικά έγκυρων ηλεκτρονικών ευρημάτων. Η ανάκτηση και ανάλυση αυτών των στοιχείων γίνονται με βάση αυστηρούς κανόνες και τεχνικές και πραγματοποιούνται με τη βοήθεια ειδικού υλικού και λογισμικού.

Αντίστοιχα με τον όρο της «Εγκληματολογίας Υπολογιστών», ως «Ψηφιακή Ιχνηλάτηση Κινητών Συσκευών» (Mobile Forensics) ορίζεται ο κλάδος της Ψηφιακής Εγκληματολογίας, αντικείμενο του οποίου είναι η ανακάλυψη, συλλογή και ανάλυση ψηφιακών αποδεικτικών στοιχείων ή δεδομένων από μια κινητή συσκευή ή συσκευή με δυνατότητες αποθήκευσης και επικοινωνίας ταυτόχρονα όπως ταμπλέτες (tablets) ή Προσωπικοί Ψηφιακοί Οδηγοί (Personal Digital Assistants – PDAs).

Το τυπικό μοντέλο διαδικασιών Ψηφιακής Εγκληματολογίας προβλέπει τέσσερα στάδια:

- **Συλλογή (collection).** Περιλαμβάνει την αναγνώριση, σήμανση, καταγραφή και συλλογή κάθε πιθανής πηγής ψηφιακών πειστηρίων σχετικών με την υπόθεση που διερευνάται, τηρώντας πάντοτε προκαθορισμένες αυστηρές οδηγίες που αφορούν στην τήρηση και στο χειρισμό των δεδομένων και στην εξασφάλιση της ακεραιότητάς τους. Η συλλογή εκτελείται έχοντας πάντοτε κατά νου τον παράγοντα χρόνο, καθώς υπάρχει περίπτωση σημαντικά στοιχεία όπως π.χ. τρέχουσες δικτυακές συνδέσεις να χαθούν από τυχόν καθυστερήσεις.

- **Εξέταση (examination).** Περιλαμβάνει την εξέταση, συνήθως, μεγάλου όγκου δεδομένων με τη χρήση αυτοματοποιημένων και μη διαδικασιών με σκοπό την αξιολόγηση των δεδομένων και εξαγωγή αυτών που παρουσιάζουν το μεγαλύτερο ενδιαφέρον για την εκάστοτε υπόθεση, με κύριο μέλημα πάντοτε την ακεραιότητα των δεδομένων.

- **Ανάλυση (analysis).** Πρόκειται για την ανάλυση των αποτελεσμάτων που προέκυψαν από την φάση της Εξέτασης με τη χρήση νομικά αποδεκτών μεθόδων και τεχνικών με σκοπό να προκύψουν στοιχεία τα οποία θα απαντήσουν στα ερωτήματα που δημιουργήθηκαν κατά τη διάρκεια της έρευνας και θα υποστηρίξουν ή θα απορρίψουν κάθε πιθανή εκδοχή του περιστατικού.

- **Αναφορά (report).** Η τελική φάση της έρευνας περιλαμβάνει την περιγραφή των ευρημάτων της, την καταγραφή των εργαλείων και μεθόδων που χρησιμοποιήθηκαν και τον προσδιορισμό των περαιτέρω ενεργειών που απαιτούνται στη συνέχεια. Τέλος μπορεί να καταλήγει σε προτάσεις για τη βελτίωση των τρεχουσών πολιτικών, διαδικασιών, εργαλείων και λοιπών θεμάτων με σκοπό την αποφυγή παρόμοιων περιστατικών στο μέλλον. Το ύφος συγγραφής της αναφοράς προσδιορίζεται από το είδος της υπόθεσης και την πιθανότητα να συμπεριληφθεί σε δικαστικές ή εσωτερικές πειθαρχικές διαδικασίες.

Τα εργαλεία και οι μέθοδοι Ψηφιακής Εγκληματολογίας χρησιμοποιούνται συνήθως στα πλαίσια ερευνών με σκοπό την εξιχνίαση ηλεκτρονικών εγκλημάτων ή χειρισμό περιστατικών ασφαλείας στα οποία πραγματοποιείται εξέταση των μηχανημάτων που προσβλήθηκαν, συλλογή και τήρηση των ψηφιακών αποδεικτικών στοιχείων και επανάληψη σε ελεγχόμενο περιβάλλον ενός συμβάντος για μελέτη και εξακρίβωση του χρονοδιαγράμματός του. Πέραν των παραπάνω εφαρμογών, οι τεχνικές της Ψηφιακής Εγκληματολογίας δύναται να χρησιμοποιούνται για:

- την αντιμετώπιση προβλημάτων (troubleshooting) κατά τη λειτουργία των Πληροφοριακών Συστημάτων ενός Οργανισμού,

- την ανάλυση των αρχείων καταγραφής (log files) που παράγονται από τα συστήματα και των εντοπισμό τυχόν προβλημάτων ή παραβιάσεων,

- την ανάκτηση δεδομένων (data recovery) που ακούσια ή εκούσια διαγράφτηκαν ή τροποποιήθηκαν,

- την ασφαλή συλλογή δεδομένων (data acquisition) από εξοπλισμό ο οποίος πρόκειται να καταστραφεί ή μεταβιβασθεί και

- τη συμμόρφωση ενός Οργανισμού με τις νομικές και κάθε άλλου είδους κανονιστικές υποχρεώσεις του.

Οι τεχνικές και οι μέθοδοι που χρησιμοποιούνται θα πρέπει να είναι έγκυρες, επαναλαμβανόμενες από τον οποιονδήποτε με τα ίδια δεδομένα εισόδου να παράγουν τα ίδια δεδομένα εξόδου και να τεκμηριώνονται επαρκώς, ώστε να επιτυγχάνεται η αποδοχή των αποτελεσμάτων της έρευνας από τα δικαστικά όργανα και να εξασφαλίζεται η αξιοπιστία των αποδεικτικών στοιχείων.

Γίνεται αντιληπτό ότι το στάδιο της Συλλογής, εξαιτίας του γεγονότος ότι λαμβάνει χώρα επιτόπου στο σημείο και στα μηχανήματα όπου διαπιστώθηκε το περιστατικό ασφαλείας και επειδή τα μέσα και οι ικανότητες που θα διαθέτει το προσωπικό που τη διεξάγει θα είναι περιορισμένα, μπορεί να θεωρηθεί ότι αποτελεί ταυτόχρονα ένα από τα στάδια που αναφέρθηκαν ότι περιλαμβάνει η διαδικασία της Αντιμετώπισης Περιστατικών Ασφαλείας. Η υλοποίηση των υπόλοιπων βημάτων από το προσωπικό της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας υπό κανονικές συνθήκες θα είναι αδύνατη, καθώς για την Εξέταση και την Ανάλυση των ψηφιακών πειστηρίων είναι απαραίτητη η ύπαρξη εξειδικευμένου προσωπικού και η λειτουργία υποδομής εργαστηρίου Ψηφιακής Εγκληματολογίας. Εν κατακλείδι, η διαδικασία Ψηφιακής Εγκληματολογίας που περιεγράφηκε είναι πιο εξειδικευμένη αλλά δεν περιλαμβάνει τις επιμέρους διαδικασίες σε επίπεδο διαχείρισης του Οργανισμού.

3.4 Σύγκριση Μοντέλων

Η περιγραφή των μοντέλων διαδικασιών της Αντιμετώπισης Περιστατικών Ασφαλείας και της Ψηφιακής Εγκληματολογίας κάνει εμφανείς κάποιες διαφορές σχετικά με το που εστιάζει η κάθε διαδικασία και το πως αντιμετωπίζονται συγκεκριμένες παράμετροι.

Στην Αντιμετώπιση Περιστατικών Ασφαλείας δίνεται έμφαση στη διαχειριστική και διοικητική αντιμετώπιση ενός περιστατικού ασφαλείας. Πρωτεύουσας σημασίας είναι η ανάκαμψη του Οργανισμού και η αποκατάσταση της καλής λειτουργίας των συστημάτων σε συνδυασμό με τις μικρότερες δυνατές απώλειες σε κάθε τομέα ξεχωριστά (οικονομικών, δημόσιας εικόνας, εξυπηρέτησης πελατών κτλ). Η τεχνική ανάλυση του περιστατικού περιλαμβάνεται στις διαδικασίες, είναι όμως περιορισμένης έκτασης και κατά τη διαμόρφωση της τακτικής, βάσει της οποίας θα αντιμετωπιστεί το συμβάν, υπάρχει περίπτωση να μείνει και εκτός πλάνου ή να αρκεί μια περιορισμένης έκτασης ανάλυση. Η απόφαση για μια ολοκληρωμένη ή μη εγκληματολογική

ανάλυση στα ψηφιακά στοιχεία καθορίζεται συνήθως από το εκτιμώμενο επίπεδο ικανοτήτων του επιτιθέμενου και την πιθανή, από κάθε άποψη, ζημία στον Οργανισμό.

Αντίθετα, στην Ψηφιακή Εγκληματολογία, οι ερευνητές οι οποίοι είναι επιφορτισμένοι με την τεχνική διερεύνηση ενός περιστατικού ασφαλείας υπολογιστών, εξαίρουν τη σημασία της ένταξης μιας ολοκληρωμένης εγκληματολογικής ανάλυσης των ψηφιακών πειστηρίων στη συνολική έρευνα, ώστε τα αποτελέσματα αυτής να είναι έγκυρα και αποδεκτά σε οποιαδήποτε πιθανή δικαστική λειτουργία ή εσωτερική πειθαρχική διαδικασία. Σκοπός είναι να δοθούν επαρκείς και τεκμηριωμένες εξηγήσεις αναφορικά με τα υποθετικά σενάρια που επικυρώνονται ή απορρίπτονται σχετικά με το συμβάν και όχι μόνο η αποδοχή του προφανούς. Για τον λόγο αυτό, τα στάδια της εξέτασης και ανάλυσης των ψηφιακών αποδεικτικών στοιχείων χαρακτηρίζονται από μεγαλύτερη λεπτομέρεια σε σχέση με την αντίστοιχη φάση ανάλυσης που περιλαμβάνεται στις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας. Η επιστημονική αντιμετώπιση υπερτερεί της διαχειριστικής σε αυτή την περίπτωση.

3.5 Επιλογή Μοντέλου Διαδικασιών για το Στρατιωτικό Περιβάλλον

Ο τρόπος με τον οποίο ένας Οργανισμός θα επιλέξει να αντιμετωπίσει ένα περιστατικό ασφαλείας καθορίζεται επιπλέον, πέραν των όσων αναφέρθηκαν στην προηγούμενη παράγραφο, από την ισχύουσα πολιτική του για την αντιμετώπιση ανάλογων περιπτώσεων και τις νομικές του υποχρεώσεις. Η προκαθορισμένη στρατηγική ασφαλείας πιθανώς να διαφέρει από συμβάν σε συμβάν, αναλόγως της σημασίας του, και η πραγματοποίηση εκτενούς τεχνικής ανάλυσης των παραμέτρων του μπορεί να μην προβλέπεται πάντοτε. Αντίθετα, εάν η πολιτική περιγράφεται ως «μηδενικής ανοχής», είναι σίγουρο ότι κάθε συμβάν θα αναλυθεί λεπτομερώς προκειμένου να μην επαναληφθεί στο μέλλον. Επίσης, η λεπτομερής τεχνική ανάλυση και η προσκόμιση ψηφιακών αποδεικτικών στοιχείων μπορεί να αποτελεί νομική ή άλλης μορφής κανονιστική υποχρέωση, στην οποία ο Οργανισμός δεσμεύεται να προβεί. Η αδυναμία εκπλήρωσης των υπόψη υποχρεώσεων μπορεί να έχει ποικίλες συνέπειες, από περιορισμούς λειτουργίας μέχρι πρόστιμα και διαφυγόντα συμφέροντα.

Στην περίπτωση του στρατιωτικού περιβάλλοντος, η οποία εξετάζεται επί του παρόντος, το αποδεκτό όριο σε ότι αφορά την ανοχή στις συνέπειες κάθε είδους που θα έχει ένα περιστατικό ασφαλείας υπολογιστών είναι πάρα πολύ αυστηρό και μπορεί να χαρακτηριστεί ως «μηδενικής ανοχής». Για το λόγο αυτό τόσο η διαχειριστική όσο και η επιστημονική αντιμετώπιση οφείλουν να διεξάγονται με τον πλέον λεπτομερή και αποτελεσματικό τρόπο.

Παράλληλα, οι απαιτήσεις στελέχωσης των Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας και των ερευνητών Ψηφιακής Εγκληματολογίας είναι μεγάλες. Υπό κανονικές συνθήκες, το προσωπικό που συμμετέχει στις

διαδικασίες της αρχικής επιτόπιας έρευνας του περιστατικού και συλλογής των ψηφιακών πειστηρίων έχει διαφορετικά καθήκοντα και επίπεδο εξειδίκευσης από τους αντίστοιχους ερευνητές του εργαστηρίου Ψηφιακής Εγκληματολογίας, όπου θα καταλήξουν τα συλλεχθέντα στοιχεία για την επιστημονική ανάλυσή τους και την εξαγωγή συμπερασμάτων. Η πρώιμη κατάσταση στην οποία βρίσκεται ο συγκεκριμένος τομέας στο στρατιωτικό περιβάλλον, σε συνδυασμό με την έλλειψη επαρκούς στρατιωτικού προσωπικού τόσο αριθμητικά όσο και από απόψεως εξειδίκευσης για την υλοποίηση των ενεργειών, επιβάλλει την εμπλοκή των ίδιων προσώπων στο σύνολο των διαδικασιών.

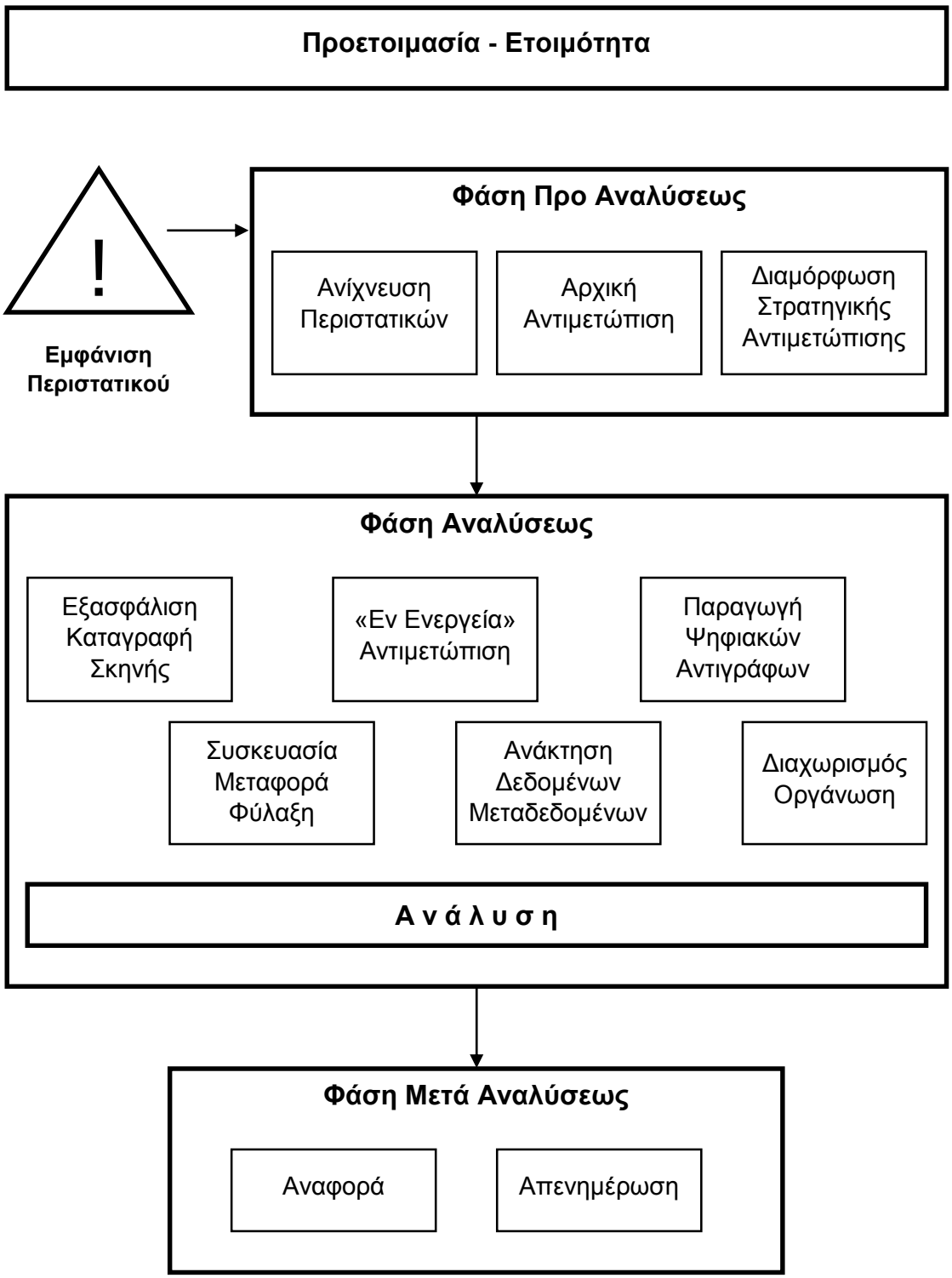
Συμπερασματικά, γίνεται αντιληπτό πως η προδιαγραφή ενός ενιαίου μοντέλου διαδικασιών, το οποίο θα αντιμετωπίζει με την ίδια βαρύτητα κάθε πτυχή ενός περιστατικού ασφαλείας αποτελεί την καταλληλότερη πρόταση όσον αφορά στις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας στο στρατιωτικό περιβάλλον. Ένα τέτοιο μοντέλο διαδικασιών προδιαγράφεται στη συνέχεια.

3.6 Ενιαίο Μοντέλο Διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας

Σε συνέχεια των όσων αναφέρθηκαν έως τώρα στο παρόν κεφάλαιο, παρακάτω προδιαγράφεται ένα ενιαίο μοντέλο διαδικασιών [4], το οποίο ουσιαστικά ενσωματώνει στις διαδικασίες της Αντιμετώπισης Περιστατικών Ασφαλείας μια λεπτομερή τεχνική ανάλυση Ψηφιακής Εγκληματολογίας, ώστε να επιτυγχάνεται μια πιο ολοκληρωμένη αντιμετώπιση, τόσο από διαχειριστική όσο και από τεχνική άποψη.

Οι ενέργειες που περιλαμβάνονται, κατηγοριοποιούνται χρονικά σε τρεις φάσεις: στη φάση Προ Αναλύσεως, στη φάση Αναλύσεως και στη φάση Μετά Αναλύσεως. Με τον όρο «Ανάλυση» ορίζεται η επιστημονική εξέταση, η οποία πραγματοποιείται με αποδεκτές και τεκμηριωμένες μεθόδους και εργαλεία Ψηφιακής Εγκληματολογίας στα ψηφιακά αποδεικτικά στοιχεία, τα οποία έχουν συλλεχθεί από το σημείο όπου έλαβε χώρα το περιστατικό ασφαλείας.

Η Προ Αναλύσεως φάση περιλαμβάνει τις ενέργειες που λαμβάνουν χώρα πριν την τεχνική ανάλυση των ψηφιακών πειστηρίων, δηλαδή κυρίως διαδικασίες προετοιμασίας, παρακολούθησης και ανίχνευσης συμβάντων. Η φάση Αναλύσεως περιλαμβάνει ουσιαστικά τις διαδικασίες της Εξέτασης και Ανάλυσης, που αναφέρθηκαν στην περιγραφή του μοντέλου της Ψηφιακής Εγκληματολογίας. Η Μετά Αναλύσεως φάση περιλαμβάνει διαδικασίες τεκμηρίωσης του περιστατικού και των ευρημάτων, με τη σύνταξη αντίστοιχης αναφοράς και απενημέρωσης, για την περαιτέρω αξιοποίηση των καταγεγραμμένων αποτελεσμάτων. Σχηματικά το ενιαίο μοντέλο διαδικασιών παριστάνεται ως εξής:



Εικόνα 3.1 : Ενιαίο Μοντέλο Διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας

3.6.1 Προετοιμασία – Ετοιμότητα

Πρόκειται για το στάδιο της διαρκούς επαγρύπνησης στο οποίο βρίσκεται ένας Οργανισμός πριν την εκδήλωση ενός περιστατικού ασφαλείας. Περιλαμβάνει τον καθορισμό της πολιτικής ασφαλείας που αφορά στα Πληροφοριακά του Συστήματα και στις πληροφορίες που διακινούνται μέσω αυτών. Η πολιτική ασφαλείας χρησιμοποιείται ως κριτήριο για το χαρακτηρισμό ενός συμβάντος ως περιστατικού ασφαλείας πληροφοριών ή όχι, περιγράφει το όριο ανοχής του Οργανισμού στις συνέπειες που μπορεί να προκαλέσει το συμβάν και ορίζει τη στρατηγική αντιμετώπισης ανά περίπτωση, περιγράφοντας τον τρόπο με τον οποίο θα ενεργήσουν τα επιμέρους τμήματα σε περίπτωση εκδήλωσης της απειλής.

Στο στρατιωτικό περιβάλλον, η σύνταξη και εφαρμογή τόσο του Εθνικού Κανονισμού Ασφαλείας (Ε.Κ.Α.) [8], ο οποίος αποτελεί την Εθνική Πολιτική Ασφαλείας, όσο και του Στρατιωτικού Κανονισμού περί «Ασφαλείας Πληροφοριακών Συστημάτων» (ΣΚ 80-20) [9], ο οποίος αποτελεί την Πολιτική Ασφαλείας Πληροφοριακών Συστημάτων του Ελληνικού Στρατού, αποτελούν ενέργειες που περιλαμβάνονται στο συγκεκριμένο στάδιο.

3.6.2 Φάση Προ Αναλύσεως

3.6.2.1 Ανίχνευση Περιστατικού

Αμέσως μετά την εκδήλωση ενός περιστατικού ασφαλείας, το στάδιο που ακολουθεί αφορά στην ταχεία ανίχνευσή του. Η ανίχνευση μπορεί να πραγματοποιηθεί είτε από κάποιο μηχανισμό ή μέτρο ασφαλείας είτε από τους ίδιους τους χρήστες. Για το λόγο αυτό είναι αναγκαίο να έχουν προκαθορισθεί οδηγίες και διαδικασίες ειδοποίησης και αναφοράς συμβάντων τα οποία, βάσει των πολιτικών, συνιστούν περιστατικά ασφαλείας.

Η τήρηση προκαθορισμένων διαδικασιών ανίχνευσης και αναφοράς των συμβάντων έχει πολλαπλά οφέλη. Πρωτίστως, ο ορισμός του αποδέκτη και του είδους των πληροφοριών που πρέπει να αναφέρονται κατά την ανίχνευση ενός περιστατικού έχει ως αποτέλεσμα την καλύτερη αρχική ενημέρωση του προσωπικού της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας, μειώνοντας το χρόνο αντίδρασης και περιορίζοντας τις επιπτώσεις από την απειλή. Επίσης, η γνωστοποίηση των κατάλληλων ενεργειών στις οποίες πρέπει να προβαίνει κάθε χρήστης όταν αντιλαμβάνεται ένα συμβάν, συμβάλλει στην αποφυγή της καταστροφής ή τροποποίησης ψηφιακών αποδεικτικών στοιχείων, τα οποία είναι πολύτιμα ώστε να προκύψει το ιστορικό του περιστατικού αλλά και για τη χρησιμοποίησή τους στις δικαστικές και εσωτερικές πειθαρχικές διαδικασίες.

Όσον αφορά στο στρατιωτικό περιβάλλον, η εκκίνηση μιας έρευνας και η κινητοποίηση της αντίστοιχης Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας μπορεί να προκύψει από διάφορες αφετηρίες.

Μια περίπτωση αφορά στην ανίχνευση ενός περιστατικού από τα εγκατεστημένα για τον σκοπό αυτό μέτρα ασφαλείας. Στο στρατιωτικό περιβάλλον εφαρμόζονται όλα τα απαραίτητα μέτρα και οδηγίες για

την έγκαιρη ανίχνευση περιστατικών ασφαλείας, τα οποία περιλαμβάνουν Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems – IDS), συστήματα παρακολούθησης αρχείων καταγραφής δραστηριοτήτων χρηστών (log files monitoring), Συστήματα Ασφάλειας Πληροφοριών και Διαχείρισης Συμβάντων (Security Information and Event Management – SIEM) και προγράμματα ανίχνευσης ιών (antivirus). Μετά την ανίχνευση ενός περιστατικού και σύμφωνα με τα όσα ορίζονται από τις ισχύουσες πολιτικές ασφαλείας (Ε.Κ.Α. και ΣΚ 80-20) που διέπουν τη χρήση των στρατιωτικών Πληροφοριακών Συστημάτων, η αντίστοιχη Διεύθυνση Πληροφορικής διατάζει τη διεξαγωγή ελέγχου στα συστήματα που εμφανίζεται η παραβίαση προς εξακρίβωση και αποκατάσταση του προβλήματος.

Έρευνα, επίσης, μπορεί να διαταχθεί από την αρμόδια Διεύθυνση Ασφαλείας και Πληροφοριών του Γενικού Επιτελείου κατόπιν δικού της ελέγχου ή αιτήματος του Διευθυντή ή Διοικητή μιας υπηρεσίας, στην περίπτωση κατά την οποία έχει περιέλθει εις γνώση του μια παραβίαση των πολιτικών ασφαλείας. Στο σκοπό αυτό συμβάλλουν και οι οδηγίες έγκαιρης αναφοράς περιστατικών ασφαλείας προς τους χρήστες των Πληροφοριακών Συστημάτων του Στρατού. Η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας λειτουργεί ως επιμέρους τμήμα της συνολικής έρευνας, παρέχοντας την τεχνική ανάλυση των δεδομένων του περιστατικού.

Ενδεικτικά, το στάδιο περιλαμβάνει ενέργειες όπως:

- Έλεγχος καλής λειτουργίας και συχνή επικαιροποίηση των μηχανισμών ασφαλείας (IDS, SIEM, antivirus), με σκοπό την έγκαιρη ανίχνευση ύποπτων συμβάντων.

- Έκδοση οδηγιών από τη Διεύθυνση Πληροφορικής προς τους χρήστες των Π.Σ., στις οποίες να περιγράφονται οι ενδείξεις που συνιστούν περιστατικά ασφαλείας, ο τρόπος αναφοράς αυτών στο αρμόδιο προσωπικό και οι άμεσες ενέργειες στις οποίες πρέπει να προβαίνουν οι χρήστες.

- Ενημέρωση και ευαισθητοποίηση των προϊσταμένων σε θέματα που αφορούν στην ασφάλεια Πληροφορικής.

3.6.2.2 Αρχική Αντιμετώπιση

Κατά τη διάρκεια του σταδίου της Αρχικής Αντιμετώπισης, η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας, στηριζόμενη στα στοιχεία που έχει συγκεντρώσει μέχρι εκείνη τη στιγμή αλλά και στην εμπειρία και εξειδίκευση του προσωπικού που την απαρτίζει, προσδιορίζει εάν όντως το αναφερόμενο συμβάν συνιστά περιστατικό ασφαλείας ή εάν πρόκειται για εσφαλμένο είτε μικρής σπουδαιότητας συναγερμό. Τα πρώτα στοιχεία σχετικά με το περιστατικό μπορεί να εξαχθούν από διάφορες πηγές, όπως από την αναφορά των παρατηρήσεων του χρήστη που αντιλήφθηκε την παραβίαση, από τα δεδομένα των συστημάτων παρακολούθησης των δικτύων και των αρχείων καταγραφής (log files) και από λοιπά δεδομένα που παρέχουν οι διαχειριστές των διάφορων δικτύων ενός

Οργανισμού (π.χ. διαβαθμισμένο εσωτερικό δίκτυο ή αδιαβάθμητο δίκτυο πρόσβασης στο Διαδίκτυο).

Εάν το περιστατικό ασφαλείας επιβεβαιώνεται, τότε γίνεται προσπάθεια να προσδιορισθούν το είδος της απειλής και τα συστήματα που πλήττονται. Σκοπός είναι να τεθούν σε εφαρμογή τα κατάλληλα μέτρα ασφαλείας που προβλέπονται από την αντίστοιχη στρατηγική αντιμετώπισης που ορίζει η πολιτική ασφαλείας του Οργανισμού, αναλόγως του περιστατικού.

Από τα παραπάνω προκύπτει ότι κατά το στάδιο της Αρχικής Αντιμετώπισης το αρμόδιο προσωπικό είναι πιθανό να μην έχει έρθει σε επαφή με τον χώρο όπου παρατηρήθηκε το περιστατικό ασφαλείας ή βρίσκεται το μηχάνημα που προσβλήθηκε, καθώς η συγκέντρωση των αρχικών στοιχείων είναι δυνατό να πραγματοποιείται από απόσταση, τηρώντας πάντοτε τις οδηγίες ασφαλούς συλλογής προκειμένου να μην απωλεσθεί οποιοδήποτε στοιχείο από εσφαλμένους χειρισμούς.

Ενδεικτικά, το στάδιο περιλαμβάνει ενέργειες όπως:

- Προσδιορισμός της προέλευσης της απειλής (εντός ή εκτός των ορίων του Επιτελείου) και του τύπου του περιστατικού βάσει των χαρακτηριστικών που ανιχνεύθηκαν.

- Εντοπισμός και καθορισμός της σημαντικότητας των πόρων που έχουν στοχοποιηθεί και των επιπτώσεων σε αυτούς (π.χ. απώλεια εμπιστευτικότητας διαβαθμισμένων πληροφοριών, διακοπή διαθεσιμότητας ενός εξυπηρετητή).

- Λήψη γενικών μέτρων που προβλέπονται από την πολιτική ασφαλείας ανά κατηγορία περιστατικού, όπως απομόνωση ύποπτων ή προσβεβλημένων συστημάτων από τα αντίστοιχα δίκτυα, καταγραφή και παρακολούθηση οποιασδήποτε δικτυακής κίνησης και συλλογή στοιχείων από κεντρικά συστήματα (π.χ. εξυπηρετητές) με μεθόδους «Εν Ενεργεία» συλλογής.

3.6.2.3 Διαμόρφωση Στρατηγικής Αντιμετώπισης

Στο τελευταίο στάδιο της Προ Αναλύσεως Φάσης, καθορίζεται η ακριβής στρατηγική, βάσει της οποίας το εξειδικευμένο προσωπικό θα διαχειριστεί το συγκεκριμένο συμβάν. Επειδή κάθε περιστατικό ασφαλείας παρουσιάζει μοναδικά χαρακτηριστικά, τα οποία μπορεί να οφείλονται, μεταξύ άλλων, σε νέες τεχνολογίες ή στις ιδιαίτερες ικανότητες του επιτιθέμενου, η πολιτική ασφαλείας ενός Οργανισμού δεν μπορεί να προβλέψει κάθε πιθανή μορφή μιας απειλής και ως εκ τούτου να προδιαγράψει μια λεπτομερή στρατηγική αντιμετώπισής της. Αυτό που προδιαγράφεται είναι μια γενική στρατηγική αντιμετώπισης ανά κατηγορία απειλής (π.χ. επιθέσεις μηνυμάτων ηλεκτρονικού ταχυδρομείου, επιθέσεις άρνησης υπηρεσίας κτλ.), ώστε να ορισθούν οι άμεσες ενέργειες και τα μέτρα που απαιτούνται για το προηγούμενο στάδιο της Αρχικής Αντιμετώπισης και στη συνέχεια, μετά τη

συγκέντρωση των απαιτούμενων στοιχείων, καθορίζεται η ακριβής στρατηγική που θα ακολουθηθεί για το τρέχων συμβάν.

Τα στοιχεία που καθορίζουν κάθε φορά την ακολουθούμενη στρατηγική είναι η κρισιμότητα των συστημάτων που προσεβλήθησαν, ο χρόνος που θα απαιτηθεί να μείνουν τα συστήματα εκτός λειτουργίας, οι πιθανοί δράστες και το εκτιμώμενο επίπεδό τους, η εμπειρία και η εξειδίκευση του προσωπικού, οι οικονομικές ζημίες και οι νομικές και λοιπές κανονιστικές υποχρεώσεις του Οργανισμού.

Ενδεικτικά, το στάδιο περιλαμβάνει ενέργειες όπως:

- Εφαρμογή των ενεργειών που προβλέπονται στο Σχέδιο Επιχειρησιακής Συνέχειας του Οργανισμού και αφορούν στους πόρους και τα συστήματα που προσεβλήθησαν και στην αποκατάσταση της κανονικής λειτουργίας τους.

- Καθορισμός του εξειδικευμένου προσωπικού, αναλόγως της φύσης του περιστατικού, το οποίο θα αναλάβει τη συλλογή και εξέταση των ψηφιακών πειστηρίων.

- Έκδοση λεπτομερών οδηγιών (π.χ. καθορισμός εργαλείων λογισμικού, προτεραιότητας συστημάτων) από τον επικεφαλής διαχειριστή περιστατικού προς την Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας σχετικά με τις επιτόπου ενέργειες στο σημείο όπου ανιχνεύθηκε το περιστατικό ασφαλείας.

3.6.3 Φάση Αναλύσεως

Η φάση της Αναλύσεως αποτελεί την κύρια φάση του ενιαίου μοντέλου διαδικασιών και αφορά στο χειρισμό των ψηφιακών πειστηρίων, όπως αυτός περιγράφεται στη στρατηγική που καθορίστηκε στην προηγούμενη φάση. Τα επιμέρους στάδιά της λαμβάνουν χώρα τόσο επί τόπου όσο και στο εξειδικευμένο εργαστήριο Ψηφιακής Εγκληματολογίας. Περιλαμβάνει τις ενέργειες που εκτελεί η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας και αφορούν στην εξασφάλιση, αναγνώριση και καταγραφή της περιοχής όπου ανιχνεύθηκε η παραβίαση και στη συλλογή όλων των ψηφιακών αποδεικτικών στοιχείων που πιθανώς να σχετίζονται με την υπόθεση, καθώς και την εξέταση και ανάλυσή τους από εξειδικευμένους αναλυτές Ψηφιακής Εγκληματολογίας μετέπειτα στο εργαστήριο. Το πλέον σημαντικό στοιχείο της Φάσης Αναλύσεως είναι η υποχρεωτική λεπτομερής καταγραφή οποιασδήποτε ενέργειας εκτελεί το προσωπικό σε οποιοδήποτε στάδιο της έρευνας, όσο ασήμαντη και αν μοιάζει για το σύνολο της διαδικασίας.

3.6.3.1 Εξασφάλιση – Καταγραφή Σκηνής

Το πρώτο μέλημα της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας είναι η εξασφάλιση, από κάθε άποψη, του προσωπικού που ενεργεί και της σκηνής όπου έλαβε χώρα το συμβάν. Με την άφιξη στο σημείο ενδιαφέροντος θα πρέπει να γίνει μια οπτική αναγνώριση της περιοχής, να εντοπισθούν όλες οι πιθανές πηγές ψηφιακών πειστηρίων και να

τεθούν τα όρια της σκηνής. Για την τελευταία ενέργεια μπορούν να χρησιμοποιηθούν υλικά τα οποία περιλαμβάνει η εργαλειοθήκη Αντιμετώπισης Περιστατικών Ασφαλείας, όπως προστατευτική ταινία και σημάνσεις απαγόρευσης εισόδου. Επίσης η σύνθεση της ομάδας, όπως περιγράφεται και στο επόμενο κεφάλαιο, πρέπει να προβλέπει την ύπαρξη ατόμου ή ατόμων τα οποία θα μεριμνήσουν για τη φυσική ασφάλεια των ερευνητών και της περιοχής, απομακρύνοντας μη εξουσιοδοτημένα πρόσωπα από το χώρο που ερευνάται και απαγορεύοντας στον οποιονδήποτε να έρθει σε επαφή με τα ψηφιακά στοιχεία και τους φορείς τους.

Στη συνέχεια ακολουθεί η εξασφάλιση της σκηνής από πιθανή «λογική» απειλή. Οι πηγές ψηφιακών πειστηρίων που αναγνωρίσθηκαν ελέγχονται οπτικά για τη διαπίστωση οποιασδήποτε εξωτερικής ή μη παρέμβασης, η οποία θέτει σε κίνδυνο την ακεραιότητα των δεδομένων. Αυτή η διαδικασία περιλαμβάνει:

- τον ακουστικό και οπτικό έλεγχο για την εξακρίβωση της λειτουργίας ή μη μιας συσκευής (π.χ. ενδεικτικές λυχνίες υπολογιστή ή ήχος ψήκτρας),

- τον οπτικό έλεγχο της οθόνης μιας συσκευής σε λειτουργία για ενδείξεις απομακρυσμένης πρόσβασης από μια άλλη,

- τον οπτικό έλεγχο της οθόνης μιας συσκευής σε λειτουργία για ενδείξεις πιθανής καταστροφής δεδομένων σε εξέλιξη, αναγνωρίζοντας στις τρέχουσες διαδικασίες τις λέξεις «διαγραφή», «διαμόρφωση», «μετακίνηση», «αντιγραφή», «αποκοπή» και «σβήσιμο» (“delete”, “format”, “move”, “copy”, “cut” και “wipe”),

- τον οπτικό έλεγχο της οθόνης μιας συσκευής σε λειτουργία για ενδείξεις επικοινωνιών σε εξέλιξη με τη χρήση εφαρμογών Άμεσων Μηνυμάτων (Instant Messaging) ή συνομιλίας (chat),

- τον οπτικό έλεγχο για την εξακρίβωση της λειτουργίας ή μη συσκευών με δυνατότητα λήψης φωτογραφίας ή βίντεο (ενσωματωμένη κάμερα υπολογιστή) και

- την τοποθέτηση μιας κινητής συσκευής με δυνατότητα επικοινωνίας (π.χ. κινητό τηλέφωνο) σε φορέα Φαραντέι (Faraday), εφόσον διατίθεται, για την αποκοπή της από κάθε δικτυακή πρόσβαση.

Στο συγκεκριμένο στάδιο είναι πιθανό να πραγματοποιηθούν και συνεντεύξεις με τους χρήστες των μηχανημάτων που προσεβλήθησαν ή με άλλα άτομα που εργάζονται και δραστηριοποιούνται στον ίδιο χώρο. Από τις ερωτήσεις που θα γίνουν μπορούν να συγκεντρωθούν στοιχεία σχετικά με τους χρήστες που έχουν πρόσβαση στα μηχανήματα, τα διαπιστευτήρια εισόδου τους (όνομα χρήστη και κωδικός πρόσβασης), τον σκοπό για τον οποίο χρησιμοποιούν τα συστήματα καθώς και λεπτομέρειες σχετικά με τη χρονική εκδήλωση της παραβίασης.

Επίσης είναι δυνατό να συγκεντρωθούν και πληροφορίες που θα βοηθήσουν στην εξέλιξη της έρευνας χωρίς να αποτελούν ψηφιακά δεδομένα όπως χάρτινα αποκόμματα στα οποία αναγράφονται κωδικοί, χειρόγραφες σημειώσεις, προϊόντα εκτύπωσης και εγχειρίδια συσκευών.

Υπενθυμίζεται σε αυτό το σημείο ότι σύμφωνα με τις πολιτικές ασφαλείας που ισχύουν στο ελληνικό στρατιωτικό περιβάλλον [8] [9], όλα τα μέσα Πληροφορικής διατίθενται αυστηρά και μόνο για υπηρεσιακούς σκοπούς και οι διακινούμενες μέσω αυτών πληροφορίες υπόκεινται σε περιορισμούς μόνο λόγω διαβάθμισης του περιεχομένου τους και σε καμία περίπτωση οι χρήστες δεν μπορούν να έχουν αξίωση για ιδιωτικότητα.

Τέλος η περιοχή και κάθε πηγή πληροφοριών που αναγνωρίσθηκε καταγράφονται λεπτομερώς, ώστε να μπορεί μελλοντικά να αναπαρασταθεί επακριβώς η περιοχή στο περιβάλλον ενός εργαστηρίου. Η καταγραφή περιλαμβάνει αρχικά το σχεδιασμό ενός σκαριφήματος της περιοχής υπό διερεύνηση, στο οποίο πρέπει να φαίνονται οι θέσεις των συσκευών που παρουσιάζουν ενδιαφέρον στο χώρο καθώς και τα σημεία σύνδεσης με τα δίκτυα ηλεκτρικού ρεύματος και δεδομένων. Ακολουθεί η καταγραφή κάθε συσκευής ξεχωριστά. Αυτή περιλαμβάνει την απεικόνιση και τη σήμανση όλων των καλωδίων και συνδέσεων από και προς τη συσκευή καθώς και την καταγραφή των αριθμών ονομαστικού κάθε επιμέρους υλικού. Στην τελευταία ενέργεια απαιτείται ιδιαίτερη προσοχή, καθώς η μετακίνηση μιας συσκευής προκειμένου να γίνει ορατός ο αριθμός ονομαστικού μπορεί να προκαλέσει ζημιά στην ίδια τη συσκευή ή στα δεδομένα που φέρει. Συμπληρωματικά, και εφόσον υπάρχει η ανάλογη δυνατότητα, τόσο η σκηνή στο σύνολό της όσο και κάθε υλικό ξεχωριστά μπορούν να φωτογραφηθούν με μια ψηφιακή φωτογραφική μηχανή, ώστε οι φωτογραφίες να συνοδεύσουν τα υπόλοιπα στοιχεία καταγραφής.

Συνοψίζοντας, οι ενέργειες που λαμβάνουν χώρα σε αυτό το στάδιο περιλαμβάνουν:

- Φυσική εξασφάλιση της σκηνής όπου ανιχνεύθηκε το συμβάν από κατάλληλο προσωπικό και σήμανσή της με τα μέσα που περιλαμβάνονται στην εργαλειοθήκη Αντιμετώπισης Περιστατικών Ασφαλείας.

- Αναγνώριση των πιθανών φορέων ψηφιακών πειστηρίων (π.χ. ηλεκτρονικοί υπολογιστές, φορητά μέσα αποθήκευσης, κινητά τηλέφωνα).

- «Λογική» εξασφάλιση των φορέων ψηφιακών πειστηρίων από οποιασδήποτε εξωτερική ή μη παρέμβαση.

- Λεπτομερής καταγραφή, σχεδίαση και, εφόσον είναι δυνατόν, φωτογράφιση της σκηνής.

- Συλλογή λοιπών βοηθητικών στοιχείων (π.χ. αποκόμματα χαρτιού, σημειώσεις, εγχειρίδια συσκευών).

Τονίζεται ότι όλες οι ενέργειες που λαμβάνουν χώρα από το προσωπικό πρέπει να καταγράφονται λεπτομερώς σε κάποιου τύπου Ημερολόγιο Ενεργειών, το οποίο υπάρχει περίπτωση να χρησιμοποιηθεί για τη σύνταξη της τελικής αναφοράς του περιστατικού ή ως αποδεικτικό στοιχείο σε πιθανές δικαστικές ή εσωτερικές πειθαρχικές διαδικασίες.

3.6.3.2 «Εν Ενεργεία» Αντιμετώπιση

Η πρώτη μορφή συλλογής που μπορεί να πραγματοποιηθεί στα συστήματα που έχουν αναγνωρισθεί ως πιθανές πηγές πληροφοριών είναι αυτή η οποία περιλαμβάνει μεθόδους που εντάσσονται στην «Εν Ενεργεία» Ψηφιακή Εγκληματολογία (“Live” Digital Forensics). Κύριο χαρακτηριστικό των μεθόδων αυτών είναι ότι η συσκευή που ερευνάται βρίσκεται σε λειτουργία.

Το πλεονέκτημα της μεθόδου «Εν Ενεργεία» συλλογής ψηφιακών στοιχείων είναι ότι παρέχει τη δυνατότητα συλλογής ευμετάβλητων δεδομένων (volatile data), δεδομένων δηλαδή τα οποία δεν είναι δυνατό να συλλεχθούν μετά τον τερματισμό της λειτουργίας της συσκευής. Ο λόγος για το παραπάνω γεγονός είναι ότι τα συγκεκριμένα δεδομένα χάνονται και δεν μπορούν να αναπαραχθούν με το πέρας της λειτουργίας της συσκευής, όπως συμβαίνει με τις δικτυακές συνδέσεις, τις τρέχουσες διεργασίες αλλά και τα δεδομένα που αποθηκεύονται στους καταχωρητές (registers) ή στη μνήμη RAM. Αντίθετα, το μειονέκτημα που παρουσιάζει συνίσταται στο ότι η χρήση των εργαλείων λογισμικού σε μια συσκευή που βρίσκεται σε λειτουργία μπορεί να παραβιάσει τη θεμελιώδη αρχή της ακεραιότητας των δεδομένων και του περιβάλλοντος του περιστατικού, αφού οι εντολές τους πρέπει να φορτωθούν στη μνήμη για να εκτελεστούν.

Η συλλογή αυτού του τύπου δεδομένων γίνεται συνήθως με κατάλληλα για το σκοπό εργαλεία Ψηφιακής Εγκληματολογίας, τα οποία εκτελούνται είτε από φορητά αφαιρούμενα μέσα αποθήκευσης (USB drives) όπως το **Volatility** είτε από κατάλληλους οπτικούς δίσκους (Live CD π.χ. **Deft 8.2**). Ο τρόπος χρήσης των παραπάνω εργαλείων είναι εκτός του πλαισίου της παρούσας εργασίας.

Αναλυτικός οδηγός ενεργειών που αφορά στη συλλογή ψηφιακών στοιχείων παρατίθεται στο Παράρτημα «Α».

3.6.3.3 Παραγωγή Ψηφιακών Αντιγράφων

Πρόκειται για τη δεύτερη πιθανή επιλογή που μπορεί να έχει η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας για να συλλέξει ψηφιακά πειστήρια σχετικά με το περιστατικό και αφορά σε συστήματα τα οποία βρίσκονται εκτός λειτουργίας. Στο στάδιο αυτό, δημιουργούνται ακριβή αντίγραφα των φορέων των δεδομένων (π.χ. σκληροί δίσκοι, αφαιρούμενα μέσα αποθήκευσης), με κύριο μέλημα την εξασφάλιση της ακεραιότητας. Σε κάθε περίπτωση πρέπει να παράγεται ένα πρωτεύον αντίγραφο (master copy) του αυθεντικού μέσου, το οποίο στη συνέχεια χρησιμοποιείται για την παραγωγή των αντιγράφων εργασίας (work copies), που θα χρησιμοποιηθούν

από τους ερευνητές για την ανάλυση. Στην περίπτωση της «Εν Ενεργεία» συλλογής ψηφιακών στοιχείων, το αρχικό μέσο στο οποίο αποθηκεύτηκαν τα ευμετάβλητα δεδομένα αποτελεί το αντίστοιχο πρωτεύον αντίγραφο. Η πρόσβαση στο αυθεντικό μέσο και στο πρωτεύον αντίγραφο πρέπει να είναι περιορισμένη και να γίνεται μόνο σε άκρως αναγκαίες περιπτώσεις, καθώς η εκ νέου συλλογή των δεδομένων μπορεί να μην είναι δυνατή.

Αντίγραφα μπορεί να ληφθούν από ένα φορέα ψηφιακών στοιχείων ακολουθώντας δύο προσεγγίσεις, τη φυσική και τη λογική.

Στη φυσική προσέγγιση, η συλλογή των στοιχείων γίνεται σε χαμηλό επίπεδο, bit προς bit. Με τον τρόπο αυτό λαμβάνεται ένα ακριβές αντίγραφο του μέσου, το οποίο περιλαμβάνει, εκτός των δεδομένων που είναι ορατά στον απλό χρήστη, τους τομείς που καταλαμβάνουν τα διεγραμμένα αρχεία αλλά και τους μη δεσμευμένους χώρους (unallocated spaces). Η φυσική προσέγγιση μπορεί να καταλήξει σε δύο προϊόντα, το αντίγραφο σε «εικόνα» (image) και το αντίγραφο σε δίσκο. Στην πρώτη περίπτωση, το προϊόν των εργαλείων εγκληματολογίας (forensics tools) που θα χρησιμοποιηθούν είναι ένα αρχείο «εικόνας» (image file), που αναπαριστά επακριβώς το αυθεντικό ψηφιακό αποδεικτικό στοιχείο (π.χ. ένα σκληρό δίσκο). Το αρχείο αυτό μπορεί να «φορτωθεί» σε κάποιο εργαλείο ανάλυσης, το οποίο θα το διαβάσει σαν ένα πραγματικό μέσο, παρέχοντας πρόσβαση σε όλους τους τομείς του και διευκολύνοντας έτσι τα επόμενα στάδια της ανάλυσης. Στη δεύτερη περίπτωση, για λόγους όπως πιθανή ασυμβατότητα λογισμικού και υλικού λόγω παλαιότητας, δεν είναι δυνατή η λήψη αρχείου εικόνας, οπότε η αντιγραφή πραγματοποιείται προς ένα άλλο πραγματικό μέσο (π.χ. έναν δεύτερο σκληρό δίσκο), το οποίο θα είναι και το προϊόν της διαδικασίας.

Η λήψη αντιγράφου ακολουθώντας τη φυσική προσέγγιση είναι η πλέον συνηθισμένη. Δίνει τη δυνατότητα συλλογής ενός πιστού αντίγραφου του μέσου και μάλιστα σε πολλά αντίτυπα, ώστε να διευκολύνονται οι έρευνες χωρίς να απαιτείται η συνεχής εμπλοκή του αυθεντικού, η οποία πρέπει να αποφεύγεται για λόγους ακεραιότητας των αποδεικτικών στοιχείων. Παρόλα αυτά υπάρχουν και ορισμένα μειονεκτήματα. Σε περίπτωση κρυπτογράφησης των δεδομένων του αρχικού μέσου, η ιδιότητα αυτή αναπόφευκτα κληρονομείται και στο αντίγραφο με αποτέλεσμα να μην είναι δυνατή η ανάλυσή του από τα εργαλεία Ψηφιακής Εγκληματολογίας. Το σημαντικότερο όμως μειονέκτημα είναι το χρονοβόρο της διαδικασίας. Στην περίπτωση που υπάρχει χρονικός περιορισμός για την συλλογή και ανάλυση των ψηφιακών στοιχείων, και αναλόγως των απαιτήσεων της υπόθεσης, υπάρχει η εναλλακτική επιλογή της λογικής προσέγγισης για τη λήψη αντιγράφων.

Η λογική προσέγγιση περιλαμβάνει μεθόδους με τις οποίες λαμβάνονται αντίγραφα σε κάποιο εξωτερικό μέσο μόνο των αρχείων και φακέλων που παρουσιάζουν ενδιαφέρον για το περιστατικό που ερευνάται π.χ. αρχεία και φάκελοι όπου αποθηκεύονται δεδομένα ηλεκτρονικής αλληλογραφίας για περιστατικό που αφορά σε εξαπάτηση μέσω μηνυμάτων

ηλεκτρονικού ταχυδρομείου. Επίσης ενδείκνυται για περιπτώσεις κατά τις οποίες τα δεδομένα αποθηκεύονται σε απομακρυσμένες τοποθεσίες (cloud), όπου δεν είναι δυνατή η απευθείας λήψη αντιγράφου. Πλην του προφανούς χρονικού πλεονεκτήματος, με τη λογική προσέγγιση τα δεδομένα που συλλέγονται είναι συνήθως άμεσα αναγνώσιμα και δεν απαιτείται χρήση εξειδικευμένου λογισμικού. Παρόλα αυτά δεν αποτελεί την ενδεδειγμένη τακτική, διότι τα στοιχεία που συγκεντρώνονται είναι περιορισμένα ενώ δεν συλλέγονται και οι περιοχές των μέσων που χαρακτηρίζονται ως μη κατανεμημένες ή περιλαμβάνουν διεγραμμένα αρχεία. Οι συγκεκριμένες περιοχές παρουσιάζουν συνήθως μεγάλο ενδιαφέρον για τις έρευνες.

Από τα παραπάνω συμπεραίνεται ότι η μέθοδος συλλογής που θα ακολουθηθεί κατά τη διάρκεια μιας έρευνας εξαρτάται από:

- το αν η συσκευή που φέρει τα ψηφιακά αποδεικτικά στοιχεία βρίσκεται σε λειτουργία ή όχι,
- το χρονικό περιθώριο που έχει διατεθεί στις έρευνες,
- το μέγεθος της χωρητικότητας των φορέων που έχουν αναγνωρισθεί ότι περιέχουν ψηφιακά αποδεικτικά στοιχεία,
- τη δυνατότητα ή μη συλλογής, μεταφοράς και τήρησης των αυθεντικών μέσων από τις ερευνητικές αρχές και
- τη φυσική θέση όπου βρίσκονται εγκατεστημένες οι συσκευές.

Όπως και στην «Εν Ενεργεία» αντιμετώπιση έτσι και εδώ, κάθε ενέργεια που εκτελεί η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας πρέπει να αποτελεί μέρος μιας προκαθορισμένης διαδικασίας και να καταγράφεται λεπτομερώς σε ένα Ημερολόγιο Ενεργειών.

Για την παραγωγή ψηφιακών αντιγράφων μπορούν να χρησιμοποιηθούν τα εργαλεία **Forensic Tool Kit (FTK) Imager** της AccessData και η εντολή Linux “**dcfldd**”. Ο τρόπος χρήσης των παραπάνω εργαλείων είναι εκτός του πλαισίου της παρούσας εργασίας.

Αναλυτικός οδηγός ενεργειών που αφορά στη συλλογή ψηφιακών πειστηρίων παρατίθεται στο Παράρτημα «Α».

Οι φορείς των ψηφιακών πειστηρίων ή τα ακριβή αντίγραφα αυτών, σε περίπτωση που δεν είναι δυνατή η κράτησή τους, συσκευάζονται και μεταφέρονται στο εργαστήριο για την περαιτέρω ανάλυση.

3.6.3.4 Συσκευασία, Μεταφορά και Φύλαξη Ψηφιακών Πειστηρίων

Τα ψηφιακά αποδεικτικά στοιχεία που έχουν συλλεχθεί είναι πολύτιμα για την εξέλιξη της έρευνας του περιστατικού. Στο πλείστο των περιπτώσεων το προσωπικό που τα συνέλεξε δεν θα έχει τη δυνατότητα να επαναλάβει τη διαδικασία επί τόπου, ενώ και η παρουσία του στη σκηνή όπου

έλαβε χώρα το συμβάν δεν εξασφαλίζει την παραγωγή των ίδιων αποτελεσμάτων. Τα συστήματα που συμμετείχαν μπορεί να έχουν αποκατασταθεί και επανατεθεί σε λειτουργία, τροποποιώντας συνεπακόλουθα όλα τα δεδομένα. Από τα παραπάνω προκύπτει η σπουδαιότητα της συσκευασίας, μεταφοράς και φύλαξης των στοιχείων κάτω από αυστηρές και ελεγχόμενες διαδικασίες.

Από τη στιγμή που οποιαδήποτε συσκευή ή μέσο χαρακτηριστεί ως ψηφιακό πειστήριο για τις έρευνες σχετικά με ένα περιστατικό, καταγράφεται σε ειδικά έντυπα και περιέρχεται σε μια διαδικασία ελέγχου της κυριότητάς του. Η διαδικασία αυτή ονομάζεται «αλυσίδα κυριότητας» (chain of custody) και σκοπός της είναι να εξασφαλίσει την ακεραιότητα των ψηφιακών στοιχείων στην κατάσταση που βρίσκονταν κατά τη διάρκεια της αρχικής συλλογής τους, είτε πρόκειται για τα αυθεντικά μέσα είτε για ακριβή αντίγραφα. Στα έντυπα της αλυσίδας κυριότητας καταγράφονται όλα τα στοιχεία που αφορούν στα πειστήρια, τη διαδικασία συλλογής και τη φύλαξή τους. Ενδεικτικά αναφέρονται ο κατασκευαστής, ο αριθμός ονομαστικού, μια σύντομη περιγραφή (π.χ. εσωτερικός σκληρός δίσκος), η ημερομηνία και ώρα συλλογής, η τοποθεσία συλλογής, το ονοματεπώνυμο του ατόμου που τα συνέλεξε, η χρησιμοποιούμενη μέθοδος και η υπογραφή από αλγορίθμους σύνοψης (hash algorithm digest π.χ. MD5sum) καθώς και η ημερομηνία και ώρα που περιήλθαν στην κατοχή ενός ατόμου μαζί με το ονοματεπώνυμο αυτού και την αιτία. Θα πρέπει να υπάρχει η δυνατότητα τήρησης δύο ειδών εντύπων, ενός συγκεντρωτικού που θα περιλαμβάνει όλα τα συλλεχθέντα αποδεικτικά στοιχεία που αφορούν σε μια υπόθεση και το οποίο θα είναι εύκολα προσβάσιμο από τους ερευνητές, και ενός αναλυτικού εντύπου ανά πειστήριο, το οποίο θα περιέχει περισσότερες λεπτομέρειες και το οποίο θα αποθηκεύεται μαζί με αυτό, ακολουθώντας όλες τις προβλεπόμενες διαδικασίες.

Ένα υπόδειγμα Εντύπου Ψηφιακών Πειστηρίων και Αλυσίδας Κυριότητας παρουσιάζεται στο Παράρτημα «Β».

Μετά την καταγραφή των πειστηρίων στα παραπάνω έντυπα, ακολουθεί η συσκευασία τους. Πρόκειται για ενέργεια που, μαζί με τη μεταφορά τους, απαιτεί μεγάλη προσοχή καθώς οι υψηλές θερμοκρασίες, η υγρασία, οι ισχυροί κραδασμοί, ο στατικός ηλεκτρισμός και τα ηλεκτρομαγνητικά πεδία μπορεί να επηρεάσουν τα μέσα που βρίσκονται αποθηκευμένα τα δεδομένα. Αφού γίνει η καταγραφή, φωτογράφιση και σήμανση των αποδεικτικών στοιχείων, στη συνέχεια κάθε ένα στοιχείο τοποθετείται σε ειδικό φορέα για την μεταφορά του. Τέτοιοι φορείς περιλαμβάνουν αντιστατικές συσκευασίες (π.χ. σακούλες, κουτιά), χάρτινες σακούλες και κιβώτια από χαρτόνι, τα οποία προστατεύουν τα ψηφιακά στοιχεία από την υγρασία και τον στατικό ηλεκτρισμό σε αντίθεση με φορείς που είναι κατασκευασμένοι π.χ. από πλαστικό. Κάθε συσκευασία πρέπει να εξασφαλίζεται ότι δεν θα παραμορφωθεί με οποιονδήποτε τρόπο (π.χ. λύγισμα κατά την αποθήκευση) και να σημαίνεται κατάλληλα. Η σήμανση πρέπει αφενός να αναφέρει το περιεχόμενο της συσκευασίας και αφετέρου να τονίζει την προσοχή κατά τη μεταχείριση (π.χ. σήμανση εύθραυστου). Όπως αναφέρθηκε

και κατά τη διαδικασία της συλλογής, κάθε κινητή συσκευή η οποία βρέθηκε σε λειτουργία πρέπει να εξασφαλιστεί ότι θα παραμείνει ενεργή μέχρι την ανάλυση των δεδομένων της, τα οποία πρέπει επίσης να εξασφαλιστεί ότι δεν θα αλλοιωθούν. Αυτή η επιδίωξη προϋποθέτει την ύπαρξη φορέων τύπου Φαραντέι (Faraday) με δυνατότητα φόρτισης της φορητής συσκευής (εικ. 3.2).

Εικόνα 3.2 : Φορέας Faraday με εξωτερική σύνδεση (Πηγή: www.teeltech.com)

Αφού εξασφαλιστεί ότι όλα τα πειστήρια έχουν συσκευασθεί με τέτοιο τρόπο ώστε να μην υπάρχει κίνδυνος για τα δεδομένα, ακολουθεί η μεταφορά τους στο εργαστήριο ή στο σημείο ασφαλούς αποθήκευσής τους. Κατά τη μεταφορά πρέπει να αποφεύγεται η έκθεσή τους σε ηλεκτρομαγνητικά πεδία, που μπορεί να δημιουργούνται από διάφορες πηγές (π.χ. ασύρματοι αυτοκινήτων), σε περιβαλλοντικές συνθήκες που μπορεί να τα επηρεάσουν (π.χ. υγρασία ή υψηλή θερμοκρασία) καθώς και σε ισχυρούς κραδασμούς.

Τέλος, οι ίδιες προφυλάξεις πρέπει να λαμβάνονται και κατά την αποθήκευση των ψηφιακών αποδεικτικών στοιχείων. Ο χώρος αποθήκευσης πρέπει να παρέχει τη δυνατότητα ελέγχου των περιβαλλοντικών συνθηκών (π.χ. ύπαρξη κλιματισμού) και να είναι κατασκευασμένος έτσι ώστε να παρέχει απομόνωση από ηλεκτρομαγνητικά και άλλου είδους πεδία. Για το σκοπό αυτό μπορεί να χρησιμοποιηθούν και ειδικοί Φωριαμοί Ψηφιακών Πειστηρίων. Τα πειστήρια αποθηκεύονται μαζί με τα προβλεπόμενα έντυπα αλυσίδας κυριότητας που αναφέρονται στο καθένα μεμονωμένα, ενώ το συγκεντρωτικό έντυπο ανά υπόθεση φυλάσσεται σε σημείο με ευκολότερη, αλλά πάντοτε ελεγχόμενη, πρόσβαση από τον ερευνητή. Η πρόσβαση στον χώρο φύλαξης των αποδεικτικών στοιχείων πρέπει να περιορίζεται στο άκρως αναγκαίο προσωπικό και κάθε είσοδος σε αυτόν πρέπει να καταγράφεται λεπτομερώς. Περισσότερες λεπτομέρειες σχετικά με τις προδιαγραφές του χώρου φύλαξης των αποδεικτικών στοιχείων και των Φωριαμών Ψηφιακών Πειστηρίων περιγράφονται στο επόμενο κεφάλαιο.

Συνοψίζοντας, οι ενέργειες που πραγματοποιούνται σε αυτό το στάδιο περιλαμβάνουν:

- Καταγραφή των ψηφιακών πειστηρίων στα Έντυπα Ψηφιακών Πειστηρίων και Αλυσίδας Κυριότητας, σύμφωνα με τις οδηγίες που αναφέρονται στο Παράρτημα «Β».

- Συσκευασία των φορέων των ψηφιακών στοιχείων με κατάλληλο τρόπο και υλικά ώστε να εξασφαλίζεται η ακεραιότητα και καλή κατάστασή τους.

- Φύλαξη των ψηφιακών πειστηρίων και των εντύπων που τα συνοδεύουν σε κατάλληλους χώρους φύλαξης.

Τα στάδια της Φάσης της Ανάλυσης που ακολουθούν υλοποιούνται στο ελεγχόμενο περιβάλλον ενός εργαστηρίου Ψηφιακής Εγκληματολογίας από εξειδικευμένους για τον σκοπό αναλυτές.

3.6.3.5 Ανάκτηση Δεδομένων – Μεταδεδομένων

Στο στάδιο της Ανάκτησης Δεδομένων προκύπτει ο όγκος των δεδομένων, πάνω στα οποία θα εφαρμοστούν οι περαιτέρω διαδικασίες της ανάλυσης.

Τα αντίγραφα εργασίας που παρήχθησαν στα επιμέρους στάδια της συλλογής, εξέρχονται ελεγχόμενα και βάσει προκαθορισμένων διαδικασιών από τον χώρο φύλαξης ώστε να αναλυθούν από τους εξειδικευμένους αναλυτές του εργαστηρίου Ψηφιακής Εγκληματολογίας. Η ανάλυση γίνεται σε συγκεκριμένα μηχανήματα του εργαστηρίου, ώστε να περιοριστεί η πιθανότητα απώλειας της εμπιστευτικότητας και ακεραιότητας των στοιχείων, και από ειδικό λογισμικό, το οποίο έχει τη δυνατότητα να ανακτήσει δεδομένα που έχουν διαγραφεί από τους χρήστες, αλλά καταλαμβάνουν ακόμα χώρο στη μνήμη του αποθηκευτικού μέσου, ή δεδομένα τα οποία βρίσκονται σε τομείς που χαρακτηρίζονται ως «μη δεσμευμένοι χώροι» (unallocated spaces). Τα συγκεκριμένα αυτά μηχανήματα που θα χρησιμοποιηθούν ονομάζονται «Σταθμοί Εργασίας Ψηφιακής Εγκληματολογίας» (Forensics Workstations) και οι προδιαγραφές τους περιγράφονται στο επόμενο κεφάλαιο.

Παράλληλα ο ερευνητής προβαίνει στη συλλογή και προσδιορισμό των μεταδεδομένων (metadata), τα οποία αναφέρονται στα δεδομένα που ανακτήθηκαν από το λογισμικό. Τα μεταδεδομένα περιλαμβάνουν χρονοσφραγίδες, τύπους αρχείων, ιδιότητες και δικαιώματα πρόσβασης, στοιχεία τα οποία μπορούν να χρησιμοποιηθούν ως κριτήρια για την κατηγοριοποίηση και ταξινόμηση του όγκου των δεδομένων που προέκυψε, π.χ. σε μια έρευνα που αφορά σε διαρροή φωτογραφιών ευαίσθητων στρατιωτικών εγκαταστάσεων το ενδιαφέρον εστιάζεται σε αρχεία εικόνων.

Το προϊόν του σταδίου είναι μια ολοκληρωμένη εικόνα των δεδομένων που φέρει το αποδεικτικό στοιχείο, την οποία θα εκμεταλλευθεί

ο εξειδικευμένος ερευνητής προκειμένου να προχωρήσει στο διαχωρισμό των σχετικών από τα μη σχετικά, με το περιστατικό, στοιχείων.

Για την υλοποίηση του σταδίου μπορούν να χρησιμοποιηθούν «ελεύθερα» λογισμικά ανάλυσης δεδομένων, όπως το **Sleuth Kit Autopsy** και το **Pro Discover Basic** της Technology Pathways. Ο τρόπος χρήσης των παραπάνω εργαλείων είναι εκτός του πλαισίου της παρούσας εργασίας.

3.6.3.6 Διαχωρισμός – Οργάνωση

Η επόμενη ενέργεια αφορά στην αναγνώριση των δεδομένων που δεν σχετίζονται με το περιστατικό και την απόρριψή τους από τη συνέχεια της έρευνας και την οργάνωση των υπολοίπων (σχετικών), ώστε να διευκολυνθεί το έργο του ερευνητή. Η ενέργεια του διαχωρισμού και της απόρριψης θα πρέπει να γίνεται σε κάθε περίπτωση στο αντίγραφο εργασίας που εξετάζεται, ώστε σε περίπτωση εσφαλμένης κρίσης του ερευνητή να είναι δυνατή η επαναδημιουργία ενός πλήρους αντιγράφου από το αυθεντικό μέσο ή το πρωτεύον αντίγραφο. Η σημασία του εν λόγω σταδίου είναι μεγάλη, διότι ο διαχωρισμός και η οργάνωση του ελάχιστου δυνατού συνόλου απαραίτητων δεδομένων, τα οποία παρουσιάζουν ενδιαφέρον για την υπόθεση, θα καταστήσει τις έρευνες πιο αποδοτικές και γρήγορες.

Κάθε ενέργεια, όπως και στα προηγούμενα βήματα, καταγράφεται και δικαιολογείται λεπτομερώς.

3.6.3.7 Ανάλυση

Στο τελευταίο στάδιο της Φάσης της Ανάλυσης πραγματοποιείται η ουσιαστική ανάλυση του υποσυνόλου των δεδομένων που προέκυψε μετά την εφαρμογή όλων των επιμέρους σταδίων στο αρχικό σύνολο. Τα δεδομένα αυτά θα οδηγήσουν τον ερευνητή στο να καταλήξει σε ένα ιστορικό του περιστατικού, που θα παρουσιάζει τις περισσότερες πιθανότητες να ανταποκρίνεται στην πραγματικότητα. Με τη χρήση των εξειδικευμένων εργαλείων λογισμικού αλλά κυρίως της εμπειρίας του, ο ερευνητής καλείται να εντοπίσει τις σχέσεις ανάμεσα στα διάφορα ψηφιακά στοιχεία και εάν είναι δυνατόν να αναγνωρίσει το δράστη του περιστατικού, καθώς και τις αδυναμίες στην πληροφοριακή υποδομή τις οποίες εκμεταλλεύτηκε.

Προκειμένου να επιτευχθεί ο μεγαλύτερος δυνατός βαθμός αντικειμενικότητας στην ανάλυση και εξαγωγή των συμπερασμάτων, ο ερευνητής πρέπει να εφαρμόσει ευρέως αποδεκτές και τεκμηριωμένες μεθόδους ανάλυσης. Σκοπός του είναι, μέσα από την εξέταση κάθε πιθανής θεωρίας, να αποκλείσει οποιοδήποτε ενδεχόμενο μέχρι να καταλήξει στο σενάριο που θα παρουσιάζει την μεγαλύτερη πιθανότητα να έχει συμβεί, αποφεύγοντας να εστιάσει στο να αποδείξει το προφανές. Η σφαιρική του γνώση σε θέματα πληροφορικής, όπως τα Συστήματα Αρχείων και τα δίκτυα υπολογιστών, καθώς και τα ενδιάμεσα αποτελέσματα στα οποία θα καταλήξει από την εξέταση των δεδομένων, θα τον οδηγήσουν δια της ατόπου απαγωγής

στο να αποκλείσει τις υπόλοιπες εκδοχές και στο να ανακατασκευάσει το περιστατικό όσο το δυνατόν πιο κοντά στην πραγματικότητα.

Από τα παραπάνω γίνεται αντιληπτό ότι δεν υπάρχει ενδεδειγμένη μεθοδολογία η οποία να μπορεί να ακολουθηθεί στο συγκεκριμένο στάδιο της Ανάλυσης. Από τα δεδομένα και τα αποτελέσματα της ανάλυσής τους μέσω των εργαλείων Ψηφιακής Εγκληματολογίας δεν προκύπτει αυτόματα κάποιο συμπέρασμα και η αποτελεσματικότητα της έρευνας εξαρτάται από τις γνώσεις και την εμπειρία του ερευνητή.

Η μεθοδολογία που ακολουθήθηκε πρέπει να μπορεί να επαναληφθεί από οποιονδήποτε στο μέλλον κληθεί να την εφαρμόσει και να οδηγεί στα ίδια αποτελέσματα. Για το λόγο αυτό η λεπτομερής τεκμηρίωση κάθε ενέργειας στην οποία προβαίνει ο ερευνητής είναι απαραίτητη.

Με το πέρας της Ανάλυσης, από το εργαστήριο Ψηφιακής Εγκληματολογίας προκύπτει ένα γραπτό προϊόν, το οποίο ονομάζεται «Έκθεση Πραγματογνωμοσύνης». Αυτή η έκθεση παρουσιάζει με αντικειμενικό τρόπο τα ευρήματα που προέκυψαν από την τεχνική ανάλυση, χωρίς να καταλήγει σε περαιτέρω συμπεράσματα επί της υποθέσεως, και αναφέρει τις μεθόδους και τα εργαλεία που χρησιμοποιήθηκαν. Η κατάρτιση και η εμπειρία των ερευνητών σε συνδυασμό με την ευρεία αποδοχή και αξιοπιστία των μεθόδων και εργαλείων που χρησιμοποιήθηκαν, εξασφαλίζουν το κύρος της έκθεσης. Η Έκθεση Πραγματογνωμοσύνης συνοδεύεται από αντίστοιχο ψηφιακό μέσο (π.χ. οπτικός δίσκος), το οποίο περιλαμβάνει τα ψηφιακά αποτελέσματα της ανάλυσης.

3.6.4 Φάση Μετά Αναλύσεως

Η τρίτη φάση του ενιαίου μοντέλου διαδικασιών αρχίζει όταν όλες οι διαδικασίες ανάλυσης των ψηφιακών πειστηρίων έχουν ολοκληρωθεί και έχει προκύψει το πιθανότερο σενάριο που αφορά στο περιστατικό, ενώ παράλληλα έχουν εκπληρωθεί και οι αντικειμενικοί σκοποί που τέθηκαν κατά τη διαμόρφωση της στρατηγικής αντιμετώπισης. Περιλαμβάνει την αναφορά των αποτελεσμάτων στη διοίκηση και την απενημέρωση σχετικά με το περιστατικό.

3.6.4.1 Αναφορά

Το στάδιο της Αναφοράς περιλαμβάνει τη συγγραφή μιας λεπτομερούς έκθεσης, στην οποία περιγράφεται το ιστορικό του περιστατικού και όλες οι ενέργειες που έλαβαν χώρα κατά τη διάρκεια της αντιμετώπισης και ανάλυσής του.

Κύρια πηγή πληροφοριών για τη συγγραφή της αναφοράς αποτελούν τα Ημερολόγια Ενεργειών της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας και των αναλυτών του εργαστηρίου Ψηφιακής Εγκληματολογίας, σε περίπτωση που δεν τηρείται ένα ενιαίο, η Έκθεση Πραγματογνωμοσύνης που συνέταξε το εργαστήριο, καθώς και οι

μεμονωμένες αναφορές που παράγονται από τα εργαλεία λογισμικού που χρησιμοποιήθηκαν.

Η αναφορά θα πρέπει να είναι γραμμένη με τέτοιο τρόπο, ώστε να μπορεί να γίνει αντιληπτή από αναγνώστες που δεν κατέχουν τις απαραίτητες τεχνικές γνώσεις ή εξειδικευμένες γνώσεις σχετικά με το περιστατικό και τις μεθόδους αντιμετώπισης, όπως για παράδειγμα η Διοίκηση ενός Οργανισμού. Η τεχνική γλώσσα, όπου είναι δυνατόν, πρέπει να αντικαθίσταται από κατανοητές περιγραφικές εκφράσεις και οι εξειδικευμένοι όροι πρέπει να επεξηγούνται σε παράρτημα της αναφοράς. Επίσης θα πρέπει να τηρούνται όλες οι προδιαγραφές, ώστε να είναι δυνατό να χρησιμοποιηθεί σε δικαστικές λειτουργίες ή εσωτερικές πειθαρχικές διαδικασίες ως συμπληρωματικό αποδεικτικό στοιχείο (π.χ. σε μια Ένορκη Διοικητική Εξέταση στο στρατιωτικό περιβάλλον), εφόσον προκύψει αντίστοιχη απαίτηση.

3.6.4.2 Απενημέρωση

Σκοπός του τελευταίου σταδίου του μοντέλου διαδικασιών είναι να περιοριστεί το πρόβλημα, εάν δεν έχει επιλυθεί έως εκείνη τη στιγμή με τα μέτρα που έχουν ληφθεί, ή να επιλυθεί λαμβάνοντας επιπλέον μέτρα ασφαλείας. Απαιτείται προσοχή στη λήψη μέτρων πριν το πέρας της έρευνας, καθώς υπάρχει περίπτωση πιθανά ψηφιακά αποδεικτικά στοιχεία να τροποποιηθούν ή να διαγραφούν προτού περιέλθουν στο εργαστήριο για ανάλυση.

Ιδιαίτερα σημαντικές είναι και οι διαδικασίες ανατροφοδότησης (feedback) και εκμετάλλευσης διδαγμάτων (lessons learned), τα προϊόντα των οποίων γίνονται γνωστά τόσο στη Διοίκηση του Οργανισμού όσο και στα επιμέρους τμήματα. Προτεραιότητα δίνεται στα τμήματα στα οποία παρατηρήθηκαν τα κενά ασφαλείας και απαιτούνται διορθωτικές ενέργειες, ώστε να εξασφαλιστεί ότι δεν θα προκύψει αντίστοιχο πρόβλημα λόγω των ίδιων αδυναμιών στο μέλλον. Τόσο η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας όσο και οι ερευνητές του εργαστηρίου Ψηφιακής Εγκληματολογίας πρέπει να παρουσιάσουν το περιστατικό και το χρονικό της αντιμετώπισής του στο σύνολο του Οργανισμού και, εφόσον απαιτείται, σε συνεργασία με τους αρμόδιους φορείς (π.χ. διαχειριστές δικτύων, υπεύθυνοι ασφαλείας πληροφορικής) να εκδώσουν οδηγίες διόρθωσης και συμμόρφωσης. Η εφαρμογή των νέων μέτρων ασφαλείας και η αποδοτικότητά τους πρέπει να ελέγχονται διαρκώς ώστε να βεβαιωθεί ότι η στρατηγική που ακολουθήθηκε για την αντιμετώπιση του περιστατικού ήταν στο σύνολό της επιτυχής.

3.7 Συμπεράσματα

Το ενιαίο μοντέλο διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας που προδιαγράφηκε στο παρόν κεφάλαιο φαίνεται πως αντιμετωπίζει τους προβληματισμούς που τέθηκαν αρχικά και αποτελεί μια ικανοποιητική λύση, συνυπολογίζοντας τις παραμέτρους που θέτει το στρατιωτικό περιβάλλον.

Οι φάσεις Προ και Μετά Αναλύσεως περιλαμβάνουν επιμέρους στάδια, με τα οποία επιτυγχάνεται η διαχειριστική και διοικητική αντιμετώπιση ενός περιστατικού, όπως ίσχυε και στο μεμονωμένο μοντέλο διαδικασιών της Αντιμετώπισης Περιστατικών Ασφαλείας. Η διαφορά έγκειται στο ότι ενσωματώνεται στη συνολική διαδικασία μια διεξοδική επιστημονική ανάλυση του συμβάντος, ώστε να γίνουν κατανοητές οι τεχνικές λεπτομέρειες του, να βρεθεί ο υπαίτιος και να εξασφαλιστεί η αποφυγή εμφάνισης παρόμοιου προβλήματος στο μέλλον. Η τεχνική ανάλυση των παραμέτρων ενός περιστατικού αποτελεί προ απαιτούμενο στις περιπτώσεις που η πολιτική ασφαλείας χαρακτηρίζεται ως «μηδενικής ανοχής». Η πολιτική που ισχύει στο στρατιωτικό περιβάλλον χαρακτηρίζεται ως τέτοια. Επίσης, η συνεχής ροή των ενεργειών, σε συνδυασμό με τη λεπτομερή περιγραφή τους, καθιστά δυνατή τη διεξαγωγή της έρευνας από το ίδιο προσωπικό στο σύνολό της, όπως καθορίζουν οι τρέχοντες περιορισμοί που σχετίζονται με το στρατιωτικό προσωπικό.

Αντιθέτως, ορισμένα από τα πλεονεκτήματα του μοντέλου έχουν και την αντίστροφη ανάγνωση. Η δέσμευση προσωπικού στη διεξαγωγή του συνόλου μιας έρευνας για μεγάλο χρονικό διάστημα έχει σαν αποτέλεσμα τη μείωση του συνολικού αριθμού των περιστατικών που μπορεί να χειριστεί το αντίστοιχο τμήμα. Επίσης, η συμμετοχή ενός ή μικρού αριθμού ατόμων στο σύνολο μιας έρευνας πιθανώς να θέσει ζητήματα αντικειμενικότητας και αξιοπιστίας, με δεδομένο ότι κανείς ερευνητής δεν είναι δυνατό να έχει εξειδικευμένη γνώση σε όλα τα θέματα και η συνεργασία είναι απαραίτητη.

Έχοντας υπόψη όλα τα παραπάνω, η διαμόρφωση μιας σαφούς εικόνας σχετικά με την καταλληλόλητα ή μη του ενιαίου μοντέλου διαδικασιών στη διαχείριση των περιστατικών ασφαλείας στο στρατιωτικό περιβάλλον προϋποθέτει τη δοκιμή και αξιολόγησή του σε πραγματικές συνθήκες.

Κεφάλαιο 4ο
Προσωπικό – Εξοπλισμός – Υποδομές

4.1 Εισαγωγή

Το Ενιαίο Μοντέλο Διαδικασιών που προδιαγράφηκε στο προηγούμενο κεφάλαιο, προϋποθέτει μια σημαντική παράμετρο ώστε να εφαρμοσθεί και να αποφέρει τα επιδιωκόμενα αποτελέσματα. Αυτή η παράμετρος αφορά στο προσωπικό και στο επίπεδο γνώσεων και εξειδίκευσής του. Στην περίπτωση που δεν εκπληρώνεται η συγκεκριμένη απαίτηση, το προσωπικό που χειρίζεται το περιστατικό έως εκείνη τη στιγμή οφείλει να σταματήσει οποιαδήποτε ενέργεια και να ζητήσει τη συνδρομή ειδικών, ώστε να μην θέσει σε κίνδυνο την ακεραιότητα των ψηφιακών αποδεικτικών στοιχείων. Από τα παραπάνω γίνεται αντιληπτό ότι η εξασφάλιση της πλήρους κατάρτισης και η συνεχής επικαιροποίηση των γνώσεων του προσωπικού που συμμετέχει στις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας πρέπει να αποτελεί κύριο μέλημα της Διοίκησης ενός Οργανισμού και των υπευθύνων του τομέα Ασφάλειας Πληροφορικής.

Παρόλα αυτά, η ύπαρξη μόνο του εξειδικευμένου προσωπικού δεν επαρκεί για τη διεξαγωγή της έρευνας ενός περιστατικού. Συμπληρωματικά, θα πρέπει να παρέχονται και όλα τα απαραίτητα τεχνικά εφόδια και υποδομές, τα οποία θα δώσουν τη δυνατότητα στους ειδικούς να εφαρμόσουν τις γνώσεις τους και να φέρουν σε πέρας, με τρόπο ακριβή και αδιαμφισβήτητο, την τεχνική ανάλυση που απαιτείται για μια ολοκληρωμένη προσέγγιση του συμβάντος. Η ύπαρξη των κατάλληλων εργαλείων, υλικού και λογισμικού, και μιας πρότυπης υποδομής εργαστηρίου Ψηφιακής Εγκληματολογίας θα επιτρέψει στους ερευνητές να υλοποιήσουν το σύνολο των ενεργειών που προβλέπει το Ενιαίο Μοντέλο Διαδικασιών.

Στη συνέχεια του κεφαλαίου αναλύονται οι παράμετροι που αφορούν στο προσωπικό που θα κληθεί να εφαρμόσει τις διαδικασίες της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας μέσα σε έναν Οργανισμό, εστιάζοντας στην ιδιαίτερη περίπτωση του στρατιωτικού περιβάλλοντος. Επίσης, περιγράφεται ο εξοπλισμός που πρέπει να διατίθεται στο προσωπικό που θα ενεργήσει επί τόπου σε μια σκηνή όπου έλαβε χώρα ένα περιστατικό ασφαλείας. Τέλος, παρουσιάζεται η δομή και οι προδιαγραφές που πρέπει να πληροί ένα πρότυπο εργαστήριο Ψηφιακής Εγκληματολογίας και απαριθμούνται τα συμπεράσματα σχετικά με την ένταξη των παραπάνω στοιχείων στη στρατιωτική λειτουργία.

4.2 Προσωπικό

Η πληθώρα των τρόπων με τους οποίους ένας κακόβουλος μπορεί να πλήξει μια εταιρία ή έναν Οργανισμό έχει καταδείξει τη σημασία της ύπαρξης διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας. Όπως αναφέρθηκε και προηγουμένως, εκτός από τις τεχνικές αναλύσεις και την απόδοση τυχόν ευθυνών στα πλαίσια της έρευνας ενός περιστατικού ασφαλείας, οι παραπάνω διαδικασίες διευκολύνουν και μια πληθώρα άλλων τεχνικών λειτουργιών ενός Οργανισμού, όπως η ανάλυση λειτουργικών προβλημάτων, η παρακολούθηση μαζικών αρχείων καταγραφής, η συλλογή και ανάκτηση δεδομένων που δεν χειρίσθηκαν σωστά και η συμμόρφωση με τις νομικές και λοιπές κανονιστικές υποχρεώσεις.

Από τα παραπάνω προκύπτει ότι κάθε Οργανισμός θα πρέπει να έχει, σε κάποιο βαθμό, δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας (Computer Security Incident Response Capability-CSIRC) και Ψηφιακής Εγκληματολογίας είτε σε μεμονωμένο περιβάλλον είτε σε αυτό ενός δικτύου. Η εν λόγω δυνατότητα βρίσκεται σε άμεση συνάρτηση με την ύπαρξη του κατάλληλου προσωπικού.

4.2.1 Κατηγορίες Προσωπικού

Το προσωπικό το οποίο θα κληθεί να υλοποιήσει το σύνολο ή μέρος των ενεργειών που προβλέπονται στο Ενιαίο Μοντέλο Διαδικασιών κατηγοριοποιείται ως εξής [2]:

- **Ομάδες Αντιμετώπισης Περιστατικών Ασφαλείας (Computer Security Incident Response Teams - CSIRT)**. Πρόκειται για το προσωπικό το οποίο καλείται να αντιμετωπίσει άμεσα ένα περιστατικό που έχει ανιχνευθεί από τους μηχανισμούς ασφαλείας ή έχει αναφερθεί από χρήστες και μπορεί να αφορά συνήθως σε μη εξουσιοδοτημένη πρόσβαση, μη προβλεπόμενη χρήση πόρων και διαφόρων τύπων επιθέσεις. Τα μέλη των ομάδων αυτών πρέπει να έχουν επαρκείς γνώσεις σε αντικείμενα όπως οι αρχές της Ψηφιακής Εγκληματολογίας, ευρέως ακολουθούμενες μεθοδολογίες και διαδικασίες, χρήση εξειδικευμένων εργαλείων λογισμικού καθώς και τεχνικές αντιμετώπισης εργαλείων που παρεμποδίσουν τις έρευνες (anti-forensics). Επίσης απαιτείται να γνωρίζουν τεχνικές λεπτομέρειες όπως τα χαρακτηριστικά των λειτουργικών συστημάτων των μηχανημάτων του Οργανισμού που ερευνούν, τα συστήματα αρχείων, τις εκάστοτε εξειδικευμένες εφαρμογές καθώς και τα πρωτόκολλα των δικτυακών υποδομών. Κύριος σκοπός των ομάδων αυτών είναι ο προσδιορισμός του αντίκτυπου του συμβάντος στη λειτουργία του Οργανισμού, ο περιορισμός των ζημιών κάθε είδους και η επαναφορά στην κανονική ροή λειτουργίας. Για να πετύχει τους σκοπούς συνήθως προβαίνει στη συλλογή και μερική ανάλυση των ψηφιακών πειστηρίων από τα μηχανήματα που προσεβλήθησαν και συνεργάζεται με τα αντίστοιχα τμήματα λειτουργίας. Στη συνηθισμένη σύνθεσή της, μια Ομάδα Αντιμετώπισης Περιστατικών αποτελείται από: α) έναν επικεφαλής (team manager) ο οποίος εξασφαλίζει το απαραίτητο προσωπικό και πόρους, αντιμετωπίζει τις κρίσιμες καταστάσεις και αποτελεί το σύνδεσμο με τη διοίκηση

του Οργανισμού, β) έναν επικεφαλής διαχειριστή περιστατικού (incident lead) ο οποίος συντονίζει τις ενέργειες των μελών της ομάδας, ενώ σε περιπτώσεις περιορισμένου προσωπικού δύναται να συμμετέχει και ο ίδιος στις διαδικασίες, γ) έναν τεχνικό επικεφαλής (technical lead) ο οποίος διαθέτει ισχυρές τεχνικές γνώσεις και εμπειρία στην Αντιμετώπιση Περιστατικών Ασφαλείας και ο οποίος είναι υπεύθυνος για το συνολικό τεχνικό έργο της ομάδας (π.χ. ανάλυση ψηφιακών πειστηρίων) και δ) τα λοιπά μέλη της ομάδας (team members), τα οποία εκτελούν το σύνολο των πρακτικών ενεργειών και πρέπει να χαρακτηρίζονται από επάρκεια στις απαραίτητες τεχνικές γνώσεις (εξειδίκευση ανά μέλος αναλόγως του περιστατικού), δυνατότητα επίλυσης προβλημάτων και κριτική σκέψη.

- **Αναλυτές Εργαστηρίου Ψηφιακής Εγκληματολογίας (Digital Forensics Lab Analysts)**. Πρόκειται για ένα σύνολο εξειδικευμένων ερευνητών, χωρίς κάποια ιδιαίτερη δομή ή ιεραρχία πλην του επικεφαλής του εργαστηρίου (lab manager) που έχει τη γενική ευθύνη και ο οποίος επικοινωνεί με τα λοιπά τμήματα του Οργανισμού και τη Διοίκηση. Το λοιπό προσωπικό ασχολείται με τη λεπτομερή τεχνική εξέταση των ψηφιακών πειστηρίων που φτάνουν στο εργαστήριο Ψηφιακής Εγκληματολογίας για ανάλυση. Τα μέλη του εργαστηρίου πρέπει να χαρακτηρίζονται από ισχυρές τεχνικές γνώσεις για μια πληθώρα τομέων της επιστήμης των υπολογιστών και να εξασφαλίζουν την αποτελεσματική αξιοποίηση των εργαλείων υλικού και λογισμικού που τους παρέχονται για την εκτέλεση των καθηκόντων τους. Σκοπός τους είναι, χρησιμοποιώντας επαναλήψιμες, αδιαμφισβήτητες και ευρέως αποδεκτές τεχνικές Ψηφιακής Εγκληματολογίας να απορρίψουν κάθε πιθανό σενάριο και να καταλήξουν στο πλέον πιθανό χρονοδιάγραμμα του περιστατικού. Για το λόγο αυτό συνήθως δεν συμμετέχουν στις λοιπές διαδικασίες των ερευνών, πλην της αναλύσεως των ψηφιακών αποδεικτικών στοιχείων.
- **Επιμέρους Τμήματα Πληροφορικής (IT Professionals)**. Πρόκειται για το προσωπικό των υπόλοιπων τμημάτων του Οργανισμού που φέρουν ευθύνη για τα Πληροφοριακά Συστήματά του, όπως τμήματα και διαχειριστές δικτύων, υπεύθυνοι ασφαλείας πληροφοριών, διαχειριστές ασφαλείας και τεχνικά τμήματα. Σκοπός τους είναι η σωστή λειτουργία των συστημάτων και για το λόγο αυτό συμμετέχουν σε ορισμένα στάδια του Ενιαίου Μοντέλου Διαδικασιών, όπως για παράδειγμα στην Ανίχνευση Περιστατικών μέσω των μηχανισμών παρακολούθησης των αρχείων καταγραφής.

Στο στρατιωτικό περιβάλλον, λαμβάνοντας υπόψη την τωρινή κατάσταση, το προσωπικό που θα συμμετέχει στις Ομάδες Αντιμετώπισης Περιστατικών Ασφαλείας και στους αναλυτές του εργαστηρίου Ψηφιακής Εγκληματολογίας υπάρχει πιθανότητα να είναι το ίδιο. Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, η πρώιμη φάση στην οποία βρίσκεται ο τομέας της Ψηφιακής Εγκληματολογίας σε συνδυασμό με την αριθμητική έλλειψη προσωπικού που κατέχει την απαιτούμενη εξειδίκευση, έχουν σαν αποτέλεσμα την ύπαρξη ενός περιορισμένου συνόλου που δύναται να χρησιμοποιηθεί για να αναπτυχθούν, σύμφωνα με τα πρότυπα, αποτελεσματικές δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας στο στρατιωτικό περιβάλλον.

4.2.2 Μοντέλα Στελέχωσης Προσωπικού

Το προσωπικό που συμμετέχει στις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας μπορεί να έχει τις ακόλουθες μορφές εργασιακής εξάρτησης με τον Οργανισμό που υποστηρίζει [11]:

- **Υπάλληλοι (employees)**. Στη συγκεκριμένη περίπτωση το σύνολο του προσωπικού που υλοποιεί το μοντέλο ενεργειών απαρτίζεται από εργαζόμενους και όλες οι διαδικασίες λαμβάνουν χώρα εντός του Οργανισμού **(in house)**.
- **Μερικής Εξωτερικής Ανάθεσης (partially outsourced)**. Σε αυτή την περίπτωση ο Οργανισμός αναθέτει σε εξωτερικούς συνεργάτες (υπεργολάβους) τμήματα των εργασιών που προβλέπονται από το μοντέλο ενεργειών. Παραδείγματα περιλαμβάνουν την ανάθεση σε πάροχους υπηρεσιών διαχείρισης ασφαλείας (managed security service providers - MSSPs) της παρακολούθησης των συστημάτων και αναφοράς των συμβάντων που συνιστούν περιστατικά ασφαλείας στην Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας του Οργανισμού ή την ανάθεση της αντιμετώπισης εξεζητημένων περιστατικών σε εξειδικευμένους εξωτερικούς συνεργάτες.
- **Πλήρους Εξωτερικής Ανάθεσης (fully outsourced)**. Πρόκειται για την περίπτωση κατά την οποία ο Οργανισμός αναθέτει εξ ολοκλήρου την εφαρμογή των διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας σε κάποιον εξωτερικό συνεργάτη, κυρίως λόγω της έλλειψης επαρκών και εξειδικευμένων εργαζομένων του. Για τη συνεχή και αποτελεσματική εφαρμογή των διαδικασιών απαιτείται ο εξωτερικός συνεργάτης να εγκατασταθεί και να λειτουργεί εντός του Οργανισμού. Το μοντέλο αυτό προϋποθέτει την ταυτόχρονη ύπαρξη εσωτερικών εργαζομένων, οι οποίοι θα επιβλέπουν το έργο του υπεργολάβου.

4.2.3 Επιλογή Μοντέλου Στελέχωσης

Οι παράγοντες που πρέπει να λάβει υπόψη η Διοίκηση ενός Οργανισμού στην απόφασή της για το κατάλληλο μοντέλο στελέχωσης του προσωπικού που θα εμπλέκεται στις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας είναι οι κάτωθι:

- **Διαθεσιμότητα**. Η άμεση διαθεσιμότητα (24/7) του προσωπικού Αντιμετώπισης Περιστατικών Ασφαλείας είναι συχνά απαραίτητη, ώστε να μην χαθούν σημαντικά δεδομένα που σχετίζονται με το συμβάν (κυρίως σε επιθέσεις μέσω δικτύων). Για το λόγο αυτό η άμεση κινητοποίηση του προσωπικού μετά από τηλεφωνική ειδοποίηση μπορεί να μην είναι αρκετή και να απαιτείται η συνεχής παρουσία του στο χώρο του Οργανισμού.
- **Κόστος**. Το κόστος αποτελεί επίσης σημαντική παράμετρο στην επιλογή μοντέλου στελέχωσης. Αρχικά, εφόσον προκύπτει ανάγκη για συνεχή παρουσία και διαθεσιμότητα του προσωπικού επί τόπου (onsite), θα πρέπει να προβλέπεται και η αντίστοιχη αποζημίωση. Επίσης, επειδή το συγκεκριμένο προσωπικό έρχεται σε επαφή με πολλές και διαφορετικές πτυχές της επιστήμης των υπολογιστών, απαιτείται να έχει περισσότερες και

διευρυμένες γνώσεις. Αυτό συνεπάγεται με την ανάγκη για διατήρηση και επέκταση των γνώσεων των μελών του μέσω εκπαιδευτικών προγραμμάτων, σεμιναρίων και πιστοποιήσεων. Τέλος, οικονομικό κόστος μπορεί να προκύπτει και από την κάλυψη αναγκών φυσικής ασφάλειας της ομάδας και εξασφάλισης των μέσων επικοινωνιών που θα χρησιμοποιεί.

- **Πλήρης ή Μερική Απασχόληση**. Στην περίπτωση που δεν υπάρχει το κατάλληλο προσωπικό ή οι απαραίτητοι πόροι για την πλήρη απασχόληση προσωπικού, τότε ο Οργανισμός θα πρέπει να καταφύγει σε λύσεις μερικής απασχόλησης. Παρόλο που η πλήρης απασχόληση είναι η ιδανικότερη επιλογή, τα μέλη της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας δύναται εναλλακτικά να ειδοποιούνται τηλεφωνικά και μέχρι την άφιξή τους ορισμένες ενέργειες να πραγματοποιούνται από προσωπικό του Τμήματος Εξυπηρέτησης (help desk) που θα έχει εκπαιδευτεί καταλλήλως, ώστε να επιτευχθεί ένα μοντέλο μερικής απασχόλησης με τις λιγότερες δυνατές συνέπειες.
- **Εξειδίκευση**. Όπως αναφέρθηκε και παραπάνω, το προσωπικό που συμμετέχει στις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας πρέπει να κατέχει γνώσεις σε πολλούς τομείς της επιστήμης της Πληροφορικής. Το γεγονός αυτό, σε συνδυασμό με την έλλειψη κατάλληλων εργαζομένων εντός του Οργανισμού, πιθανώς να οδηγήσει στη συνεργασία με κάποια υπεργολάβο ομάδα. Επιπρόσθετα, οι πάροχοι υπηρεσιών διαχείρισης ασφαλείας (MSSPs), που πιθανώς να προσληφθούν ως υπεργολάβοι, θα έχουν τη δυνατότητα να συσχετίζουν δεδομένα από διάφορους Οργανισμούς που εξυπηρετούν, ώστε να εντοπίζουν νέες απειλές σε σύντομο χρονικό διάστημα και να αποφεύγεται η προσβολή των υπολοίπων. Παρόλα αυτά, όταν η στελέχωση γίνεται με υπαλλήλους της εταιρίας εξασφαλίζεται η ολοκληρωμένη γνώση των ιδιαιτεροτήτων του περιβάλλοντος του Οργανισμού και προσδιορίζεται καλύτερα κρισιμότητα των υποδομών που προσεβλήθησαν, ώστε να εξασφαλισθούν γρηγορότερα οι σημαντικότεροι πόροι.
- **Ηθικό Εργαζομένων**. Τα καθήκοντα του εν λόγω προσωπικού και η κατάσταση συνεχούς ετοιμότητας στην οποία πρέπει να βρίσκεται μπορεί να αποδειχθούν εξαιρετικά ψυχοφθόρα. Η επιλογή του προσωπικού που θα στελεχώσει τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας ενός Οργανισμού πρέπει να γίνεται έτσι ώστε να βρεθούν κατάλληλα, πρόθυμα, έμπειρα και ικανά στελέχη. Ο ακριβής καθορισμός ρόλων και η ελάφρυνση από τα λοιπά καθήκοντα μπορεί να λειτουργήσει ευεργετικά για το ηθικό του προσωπικού.

Εκτός των προαναφερόμενων παραγόντων, τα κάτωθι πρέπει να ληφθούν σοβαρά υπόψη όταν ένας Οργανισμός προτίθεται να απασχολήσει εξωτερικούς υπεργολάβους:

- **Αποκάλυψη Ευαίσθητων Πληροφοριών**. Για λόγους ιδιωτικότητας αλλά πιθανώς και ασφαλείας, όπως στην περίπτωση του στρατιωτικού περιβάλλοντος, εφόσον απασχολείται εξωτερικός συνεργάτης για τις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής

Εγκληματολογίας θα πρέπει να λαμβάνονται μέτρα ώστε όλες οι ευαίσθητες πληροφορίες να εξασφαλίζονται. Ενδεικτικά, θα πρέπει να υπάρχουν περιορισμοί και έλεγχος των διαδικασιών λήψης αντιγράφων από τους φορείς των ψηφιακών πειστηρίων και να μην δίδεται η δυνατότητα συσχέτισης διαφορετικών συνόλων πληροφοριών (π.χ. έλεγχος ενεργειών χρήστη 1ο_grafeio χωρίς να προκύπτει η πραγματική ταυτότητα του χρήστη). Επίσης οφείλουν να υπογράφονται συμφωνίες τήρησης απορρήτου και εμπιστευτικότητας (nondisclosure agreements – NDAs). Αντίθετα, σε περιπτώσεις που στις έρευνες εμπλέκονται εσωτερικοί εργαζόμενοι του Οργανισμού, η ανάθεση σε εξωτερικό συνεργάτη ενδείκνυται.

- **Ενημέρωση Εσωτερικής Υποδομής**. Για να επιτευχθούν αποτελεσματικά οι σκοποί του Ενιαίου Μοντέλου Διαδικασιών απαιτείται το ιδιαίτερο περιβάλλον ενός Οργανισμού να είναι εις γνώσιν του υπεργολάβου, εφόσον ακολουθείται αυτό το μοντέλο στελέχωσης, ώστε να γίνεται σωστή αξιολόγηση των περιστατικών και να δίνεται προτεραιότητα στην αποκατάσταση των σημαντικότερων πόρων. Αυτό προϋποθέτει τη συχνή επικαιροποίηση των πληροφοριών που διατίθενται στον εξωτερικό συνεργάτη. Μη τήρηση των παραπάνω θα έχει ως αποτέλεσμα μειωμένη απόδοση εξαιτίας της εσφαλμένης διαχείρισης των περιστατικών και διαταραχή των σχέσεων των δυο πλευρών.
- **Χρόνος Αντίδρασης**. Ο χρόνος στον οποίο δύναται να αντιδράσει το προσωπικό που έχει αναλάβει την υλοποίηση των ενεργειών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας αποτελεί σημαντική παράμετρο στην τελική επιλογή του. Στην περίπτωση ενός εξωτερικού υπεργολάβου, θα πρέπει να ληφθούν υπόψη οι δυνατότητες προσέλευσής του στους χώρους του Οργανισμού και η τοποθεσία που είναι εγκατεστημένος. Παρόλο που η πλήρης απασχόληση προσωπικού χαρακτηρίζεται από μειωμένο χρόνο αντίδρασης, στην περίπτωση που οι εγκαταστάσεις ενός Οργανισμού είναι γεωγραφικά διάσπαρτες, η απασχόληση ενός εξωτερικού συνεργάτη, ο οποίος θα εδρεύει κοντά σε κάποιο απομακρυσμένο τμήμα, είναι ενδεικνυόμενη καθώς η επέμβαση της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας από τις κεντρικές εγκαταστάσεις μπορεί να γίνει καθυστερημένα.

Σε κάθε περίπτωση, όποιο μοντέλο στελέχωσης και αν επιλέξει ένας Οργανισμός, θα πρέπει κάποιες υποτυπώδεις δυνατότητες να μπορούν να υλοποιούνται από τον ίδιο εσωτερικά. Η πλήρης εξάρτισή του από τον εξωτερικό υπεργολάβο περιλαμβάνει τον κίνδυνο, σε περίπτωση αδυναμίας εκτέλεσης των συμβατικών υποχρεώσεών του για οποιοδήποτε λόγο, να βρεθεί εκτεθειμένος σε πιθανές απειλές με αποτέλεσμα να προκληθούν σοβαρά προβλήματα στη λειτουργία του. Για τον λόγο αυτό, το τεχνικό προσωπικό θα πρέπει να είναι ενημερωμένο σχετικά με τις καθορισμένες διαδικασίες που προβλέπονται στις πολιτικές ασφαλείας του Οργανισμού ανά περιστατικό, ενώ θα πρέπει επίσης να προβλέπεται και η δημιουργία μιας αντίστοιχης Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας από εσωτερικούς εργαζόμενους για τις περιπτώσεις εκτάκτων αναγκών.

4.2.4. Μοντέλο Στελέχωσης στο Στρατιωτικό Περιβάλλον

Η εξέταση των παραγόντων που προαναφέρθηκαν μέσα από το πρίσμα των παραμέτρων που θέτει το στρατιωτικό περιβάλλον, θα έχει ως αποτέλεσμα να προκύψει ένα μοντέλο στελέχωσης που θα παρουσιάζει τις περισσότερες πιθανότητες να πληροί με τον καλύτερο τρόπο τις απαιτούμενες προϋποθέσεις.

Οι Πολιτικές Ασφαλείας Πληροφοριών που διέπουν τη στρατιωτική λειτουργία [8] [9], προβλέπουν μηδενική ανοχή κατά τη διάρκεια αντιμετώπισης περιστατικών ασφαλείας, τόσο σε ότι αφορά στην αμεσότητα των ενεργειών όσο και στη λεπτομερή ανάλυση των τεχνικών παραμέτρων του συμβάντος. Σε συνδυασμό με τους παράγοντες της άμεσης διαθεσιμότητας και του σύντομου χρόνου αντίδρασης της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας, η συνεχής παρουσία του απαραίτητου εξειδικευμένου προσωπικού στους χώρους των στρατιωτικών Πληροφοριακών Συστημάτων κρίνεται επιβεβλημένη. Η συγκεκριμένη απαίτηση μπορεί να επιτευχθεί είτε με την στελέχωση των ομάδων από κατάλληλο στρατιωτικό προσωπικό (in house), εφόσον υπάρχει, είτε με την πλήρη απασχόληση εξωτερικών υπεργολάβων (outsourced).

Επιπλέον, για την άμεση και αποτελεσματική λειτουργία των Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας απαιτείται να είναι εις γνώση του προσωπικού η εσωτερική υποδομή των Πληροφοριακών Συστημάτων που υποστηρίζει και να περιέρχεται στην κατοχή του μεγάλος όγκος δεδομένων για ανάλυση. Στην περίπτωση απασχόλησης εξωτερικών συνεργατών για την στελέχωση των εν λόγω δυνατοτήτων στο στρατιωτικό περιβάλλον, η παραπάνω απαίτηση θα συνεπαγόταν με την αποκάλυψη ευαίσθητων διαβαθμισμένων πληροφοριών σε αναρμόδια πρόσωπα τα οποία δε φέρουν την ανάλογη εξουσιοδότηση. Παρά το γεγονός ότι στον Εθνικό Κανονισμό Ασφαλείας προβλέπονται διαδικασίες εξουσιοδότησης προσωπικού για χειρισμό απόρρητων πληροφοριών στο στρατιωτικό περιβάλλον, η ευθύνη για την έγκριση μιας τέτοιας εξουσιοδότησης είναι μεγάλη και σε καμία περίπτωση δεν μπορούν να είναι διαθέσιμες όλες οι πληροφορίες σε εξωτερικούς συνεργάτες για προφανείς λόγους εθνικής ασφάλειας. Για το λόγο αυτό ενδείκνυται η στελέχωση των δυνατοτήτων από στρατιωτικό προσωπικό το οποίο θα διαθέτει τα απαιτούμενα προσόντα και το οποίο, λόγω ιδιότητας, είναι ήδη εξουσιοδοτημένο για χειρισμό ευαίσθητων πληροφοριών.

Τέλος, οι Ένοπλες Δυνάμεις, σε άμεση συνάρτηση με τη γενικότερη δυσμενή οικονομική κατάσταση στην οποία βρίσκεται η χώρα, έχουν περιέλθει σε μια κατάσταση οικονομικής λιτότητας. Παρόλο που στη στρατιωτική πραγματικότητα έχει γίνει πλέον αντιληπτή η σημασία της ασφάλειας πληροφοριών και το προσωπικό εμφανίζεται περισσότερο συνειδητοποιημένο από ότι στο πρόσφατο παρελθόν, αναπόφευκτα το μεγαλύτερο μέρος των στρατιωτικών δαπανών αφορά στη διαβίωση του στρατεύσιμου προσωπικού και στις τρέχουσες ανάγκες συντήρησης και

εξοπλισμών και όχι σε αυτές της ασφάλειας πληροφοριών. Μέσα σε αυτά τα πλαίσια, είναι πρακτικά αδύνατο να εξασφαλισθούν και να επενδυθούν μεγάλα ποσά στην Ασφάλεια Πληροφορικής και ειδικότερα σε έναν επιμέρους τομέα, όπως αυτός της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας. Για την ανάπτυξη και διατήρηση όμως πρότυπων τέτοιων δυνατοτήτων, απαιτούνται τόσο εξειδικευμένο προσωπικό όσο και υποδομές και εξοπλισμός, στοιχεία που χαρακτηρίζονται από υψηλό κόστος. Από τα παραπάνω διαπιστώνεται ότι η απασχόληση, μερική ή πλήρης, εξωτερικών υπεργολάβων με επιπλέον κόστος είναι ουσιαστικά αδύνατη και ασύμφορη και οποιαδήποτε επένδυση θα πρέπει να γίνει για την κατάρτιση και εξειδίκευση του υπάρχοντος στρατιωτικού προσωπικού και την παροχή, στο μέτρο του δυνατού, των απαραίτητων εργαλείων υλικού και λογισμικού.

Συμπερασματικά, γίνεται αντιληπτό ότι το μοντέλο στελέχωσης των δυνατοτήτων Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας που ενδείκνυται για το στρατιωτικό περιβάλλον είναι αυτό που περιλαμβάνει προσωπικό που ήδη εργάζεται μόνιμα στις Ένοπλες Δυνάμεις. Ακολουθώντας το συγκεκριμένο μοντέλο επιτυγχάνεται ο περιορισμός του κόστους που θα προέκυπτε από την πρόσληψη εξωτερικών εργαζομένων, ενώ παράλληλα διασφαλίζεται και το απόρρητο των διαβαθμισμένων πληροφοριών. Παρόλα αυτά, για να καταστεί το στρατιωτικό προσωπικό εξειδικευμένο και ικανό στο να υλοποιεί αποτελεσματικά όσα προβλέπονται στις πρότυπες δυνατότητες, απαιτούνται επενδύσεις στην απόκτηση των κατάλληλων γνώσεων και την παροχή των αναγκαίων μέσων.

4.2.5 Ανάπτυξη Δυνατοτήτων Προσωπικού

Όπως αναφέρθηκε στην προηγούμενη υποενότητα, τόσο εξαιτίας των ιδιαιτεροτήτων του στρατιωτικού περιβάλλοντος όσο και της υφιστάμενης οικονομικής κατάστασης, οι προσπάθειες και οι επενδύσεις στον τομέα της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας πρέπει να γίνονται πρωτίστως προς την κατεύθυνση του μόνιμου στρατιωτικού προσωπικού που θα στελεχώσει τις αντίστοιχες δυνατότητες.

Μερικές ενδεικνυόμενες ενέργειες που θα συμβάλλουν στην απόκτηση και την επέκταση των γνώσεων και δυνατοτήτων του προσωπικού είναι οι εξής:

- Εξασφάλιση επαρκών πόρων για τη συντήρηση και επέκταση των γνώσεων του προσωπικού πάνω σε τεχνικά θέματα και θέματα ασφάλειας πληροφοριών, όπως επίσης και σε λοιπά θέματα που άπτονται του αντίστοιχου τομέα, όπως οι νομικές προεκτάσεις των ενεργειών που προβλέπονται από τις προδιαγεγραμμένες διαδικασίες. Το παραπάνω μπορεί να επιτευχθεί με τη συμμετοχή του προσωπικού σε εξειδικευμένες εκπαιδεύσεις και τεχνικά σεμινάρια (workshops) που αφορούν σε νέες μεθοδολογίες, στη χρήση των πιο πρόσφατων εργαλείων λογισμικού και στην απόκτηση πιστοποιήσεων, καθώς και με τη δημιουργία ανάλογης βιβλιοθήκης.

- Ενθάρρυνση του προσωπικού στη δημιουργία εκπαιδευτικού υλικού και τη διεξαγωγή εσωτερικών εκπαιδευτικών δραστηριοτήτων αναλόγως της εξειδίκευσής του, ώστε η συγκεκριμένη γνώση να μεταδίδεται και στα υπόλοιπα μέλη των Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας αλλά και στα ενδιαφερόμενα τμήματα του Οργανισμού. Η συγκεκριμένη δραστηριότητα εντός των Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας είναι άκρως σημαντική, καθώς κάθε μέλος των ομάδων αυτών πρέπει να είναι σε θέση να εκτελέσει οποιαδήποτε ενέργεια της συνολικής διαδικασίας. Η διαθεσιμότητα και αποτελεσματικότητα της εν λόγω ομάδας δεν πρέπει να τίθεται σε αμφιβολία λόγω της απουσίας κάποιου μέλους, ενώ με αυτόν τον τρόπο επιτυγχάνεται και η δυνατότητα δραστηριοποίησης της ομάδας σε περισσότερα του ενός σημεία και εγκαταστάσεις, με την προϋπόθεση ότι διατίθενται τα απαραίτητα τεχνικά μέσα.
- Για τον ίδιο σκοπό, υιοθέτηση μιας πολιτικής εναλλαγής καθηκόντων ανάμεσα στο προσωπικό ανά τακτά χρονικά διαστήματα, ώστε κάθε μέλος να υπηρετήσει το σύνολο των θέσεων εντός της ομάδας. Σε κάθε περίπτωση θα πρέπει να εξασφαλίζεται η αποτελεσματικότητα των δυνατοτήτων της ομάδας.
- Ανάπτυξη υποθετικών σεναρίων και διεξαγωγή ασκήσεων Κυβερνοασφάλειας με τη συμμετοχή και συνεργασία δημόσιων, ιδιωτικών και ακαδημαϊκών φορέων. Με τον τρόπο αυτό θα επιτευχθεί ο διαμοιρασμός της γνώσης κάθε συμμετέχοντα και θα εξαχθούν χρήσιμα συμπεράσματα, τα οποία δύναται να χρησιμοποιηθούν στην επικαιροποίηση και αναβάθμιση των πολιτικών ασφαλείας και των προδιαγεγραμμένων διαδικασιών.
- Επαρκής στελέχωση, στα πλαίσια του δυνατού, των Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας. Το έργο των ομάδων αυτών χαρακτηρίζεται από την κατάσταση συνεχούς ετοιμότητας, πίεσης χρόνου και γενικότερα έντονου άγχους. Παρά τους περιορισμούς που αναφέρθηκαν σχετικά με το υφιστάμενο εξειδικευμένο προσωπικό στο στρατιωτικό περιβάλλον, η φύση των καθηκόντων των συγκεκριμένων ατόμων επιβάλλει την στελέχωση σε τέτοιο βαθμό ώστε, όταν το επιτρέπουν και οι υπηρεσιακές ανάγκες, το προσωπικό να λαμβάνει ανενόχλητα τις απαραίτητες άδειες για ξεκούραση και ανάκαμψη. Επίσης, για την εξασφάλιση της καλύτερης ψυχολογίας και ηθικού, απαιτείται ο ακριβής καθορισμός των καθηκόντων καθενός του προσωπικού και την απεμπλοκή του, στο μέτρο του δυνατού, από λοιπά καθήκοντα εκτός του εξειδικευμένου πεδίου.

4.2.6 Συνεργασία με Λοιπά Τμήματα του Οργανισμού

Εκτός από την εξασφάλιση της πλήρους τεχνικής κατάρτισης του προσωπικού που θα υλοποιεί τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, ιδιαίτερη μέριμνα πρέπει να ληφθεί ώστε η επικοινωνία και η συνεργασία με τα υπόλοιπα τμήματα ενός Οργανισμού να γίνεται με τρόπο αποτελεσματικό. Η ανάγκη αυτή προκύπτει διότι ένα περιστατικό ασφαλείας πιθανώς να επηρεάζει το σύνολο ενός Οργανισμού, από τη λειτουργία του μέχρι την εικόνα του προς το κοινό και τις νομικές του υποχρεώσεις, και διότι για την αντιμετώπισή του, η επιφορτισμένη

με το αντίστοιχο έργο ομάδα, πιθανώς να χρειαστεί τη συνδρομή και των υπόλοιπων τμημάτων.

Έτσι, το προσωπικό των Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, όποιο μοντέλο στελέχωσης και αν ακολουθείται, πρέπει να είναι σε θέση να συνεργασθεί με τα παρακάτω τμήματα ενός Οργανισμού:

- **Διοίκηση.** Η Διοίκηση ενός Οργανισμού είναι αυτή η οποία καθορίζει την πολιτική ασφαλείας. Στα πλαίσια της ισχύουσας πολιτικής και με βάση τους στόχους και τα όρια που θέτονται σε αυτή, διαθέτει το απαιτούμενο προσωπικό και εξασφαλίζει τους αναγκαίους οικονομικούς πόρους. Η εγκαθίδρυση ενός καναλιού επικοινωνίας, μεταξύ της Διοίκησης και του προσωπικού Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, που θα χαρακτηρίζεται από αμοιβαία κατανόηση και η εξασφάλιση της αμέριστης υποστήριξής της αποτελούν σημαντικούς παράγοντες για την αποτελεσματικότητα του συγκεκριμένου έργου.
- **Τμήμα Ασφάλειας Πληροφορικής.** Κατά τη διάρκεια της έρευνας ενός περιστατικού ασφαλείας είναι εξαιρετικά πιθανό να απαιτηθεί η συνεργασία με το αντίστοιχο τμήμα Ασφάλειας Πληροφορικής του Οργανισμού, εφόσον στις αρμοδιότητές του περιλαμβάνονται καθήκοντα όπως π.χ. η διαχείριση του Τείχους Προστασίας (firewall). Επίσης θα πρέπει να υπάρχει πρόβλεψη και συνεργασία σε θέματα που αφορούν στην υλοποίηση του Σχεδίου Επιχειρησιακής Συνέχειας του Οργανισμού, αφού ένα περιστατικό ασφαλείας πιθανώς να στοχεύει στο να πλήξει την αντίστοιχη δυνατότητα. Τόσο η Αντιμετώπιση Περιστατικών Ασφαλείας όσο και η Επιχειρησιακή Συνέχεια έχουν ως πρωτεύοντα σκοπό την αποκατάσταση της κανονικής ροής λειτουργίας ενός Οργανισμού με τις μικρότερες δυνατές απώλειες, οπότε γίνεται αντιληπτό ότι η συνεργασία μεταξύ των τμημάτων που έχουν αναλάβει τις συγκεκριμένες λειτουργίες είναι επιβεβλημένη.
- **Τμήματα Λειτουργίας Πληροφορικής.** Όπως και στην περίπτωση του τμήματος Ασφάλειας Πληροφορικής, είναι σχεδόν βέβαιο ότι για την συλλογή και ανάλυση ψηφιακών πειστηρίων που σχετίζονται με ένα περιστατικό ασφαλείας θα απαιτηθεί η συνεργασία του αρμόδιου προσωπικού με τα λοιπά τμήματα Λειτουργίας Πληροφορικής. Σε αυτά περιλαμβάνονται κυρίως τα αντίστοιχα τμήματα Διαχείρισης Δικτύων, είτε πρόκειται για εσωτερικό διαβαθμισμένο δίκτυο είτε για αδιαβάθμητο δίκτυο με σύνδεση στο Διαδίκτυο. Από τα συγκεκριμένα τμήματα μπορεί να ζητηθεί η συνδρομή σε ότι αφορά τη συλλογή αρχείων καταγραφής (log files), δεδομένων λογαριασμών χρηστών (user account data) αλλά και η ενημέρωση σχετικά με τις χρησιμοποιούμενες τεχνολογίες και πρωτόκολλα.
- **Νομικό Τμήμα.** Το έργο της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας συχνά θα δημιουργήσει την απαίτηση να συλλεχθούν και αναλυθούν προσωπικά δεδομένα, ενώ η ολοκλήρωση των ερευνών πιθανώς να εκκινήσει νομικές διαδικασίες για την απόδοση ευθυνών ή πειθαρχικό έλεγχο. Από τα παραπάνω συμπεραίνεται ότι υπάρχουν σημαντικές νομικές προεκτάσεις που αφορούν

στη νομιμότητα των ενεργειών της ομάδας και για το λόγο αυτό η συνεργασία και κάλυψη από το νομικό τμήμα του Οργανισμού είναι απαραίτητη.

- **Δημόσιες Σχέσεις.** Μια από τις επιπτώσεις που μπορεί να έχει ένα περιστατικό ασφαλείας σχετίζεται με την απώλεια της καλής φήμης και τη διατάραξη της εμπιστοσύνης του κοινού ή των μετόχων προς τον Οργανισμό. Εξαίρεση δεν θα μπορούσαν να αποτελούν οι Ένοπλες Δυνάμεις, με αποτέλεσμα οποιοδήποτε περιστατικό ασφαλείας να θέτει σε αμφιβολία την αξιοπιστία τους και το αίσθημα ασφάλειας των πολιτών μιας χώρας. Για την άμεση ενημέρωση του κοινού, την αποφυγή διάδοσης αναληθών γεγονότων και την αποκατάσταση της εμπιστοσύνης απαιτείται η αποτελεσματική συνεργασία μεταξύ των τεχνικών ομάδων και του τμήματος Δημοσίων Σχέσεων ενός Οργανισμού.
- **Ανθρώπινο Δυναμικό.** Η συνεργασία με το τμήμα Ανθρωπίνου Δυναμικού μπορεί να απαιτηθεί στις περιπτώσεις που οι έρευνες σχετικά με ένα περιστατικό καταλήξουν στο συμπέρασμα υπάρχουν ευθύνες κάποιου εργαζόμενου του Οργανισμού και απαιτούνται περαιτέρω πειθαρχικές ενέργειες.
- **Φυσική Ασφάλεια.** Όπως αναφέρθηκε και στην περιγραφή του μοντέλου ενεργειών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, υπάρχει περίπτωση κατά τη διάρκεια των ερευνών να απαιτείται η φυσική εξασφάλιση τόσο της σκηνής όπου εντοπίζεται ένα περιστατικό ασφαλείας όσο και του ίδιου του προσωπικού που τις διεξάγει. Επίσης, κατά την αποθήκευση και τήρηση των ψηφιακών αποδεικτικών στοιχείων, η εξασφάλιση της ακεραιότητάς τους, ώστε να δύναται να χρησιμοποιηθούν στις περαιτέρω διαδικασίες, δεν αποτελεί αποκλειστικά ευθύνη του εξειδικευμένου προσωπικού αλλά έγκειται στη γενικότερη φυσική ασφάλεια των εγκαταστάσεων του Οργανισμού. Οι δυο απαιτήσεις που αναφέρθηκαν καταδεικνύουν την ανάγκη συνεργασίας και κοινής σχεδίασης των τμημάτων Φυσικής Ασφάλειας και Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας.

4.2.7 Λοιπές Υπηρεσίες

Πέραν των καθηκόντων που εξ ορισμού έχει το προσωπικό Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, μέσα από την εκτέλεση των ενεργειών του προκύπτουν και ορισμένες επιπλέον υπηρεσίες προς όφελος του Οργανισμού. Συνήθως οι υποδομές και οι μηχανισμοί για την Ανίχνευση Εισβολών (intrusion detection) είτε βρίσκονται εγκαταστημένοι είτε προβάλλονται στις εγκαταστάσεις του, καθιστώντας έτσι το αντίστοιχο τμήμα ως το πρώτο που θα ανιχνεύσει οποιαδήποτε κακόβουλη ενέργεια και θα σημάνει το συναγερμό στα υπόλοιπα. Παράλληλα, οι τεχνικές δυνατότητες που διαθέτει καθώς και οι γνώσεις του προσωπικού, επιτρέπουν τη λεπτομερή ανάλυση των παραμέτρων ενός περιστατικού, τα αποτελέσματα της οποίας μπορούν να χρησιμοποιηθούν σε μεταγενέστερες ενημερώσεις και εκπαιδεύσεις τόσο των άμεσα εμπλεκόμενων τμημάτων όσο και του Οργανισμού συνολικά, ώστε να επιτευχθεί το γενικότερο απαιτούμενο επίπεδο επαγρύπνησης. Επίσης ενεργεί συμβουλευτικά, προτείνοντας τις απαραίτητες

διορθώσεις που πρέπει να γίνουν στις υποδομές και τις εξειδικευμένες εφαρμογές στα αρμόδια τμήματα, ώστε να αποφευχθεί η προσβολή τους σε μελλοντικό χρόνο. Τέλος, διαμοιράζει τη γνώση που αποκτά πάνω σε νέες τεχνολογίες και εργαλεία μετά τη συμμετοχή του σε αντίστοιχες εκπαιδεύσεις και τεχνικά σεμινάρια, διεξάγοντας εσωτερικές εκπαιδευτικές δραστηριότητες για το προσωπικό του Οργανισμού.

4.3 Εξοπλισμός

Το προσωπικό το οποίο θα στελεχώσει τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, πέραν του γνωστικού επιπέδου και των προσόντων που αναφέρθηκαν, θα πρέπει να διαθέτει και τα κατάλληλα μέσα για να εκτελέσει αποτελεσματικά τα καθήκοντά του. Τα μέσα αυτά περιλαμβάνουν τόσο τον εξοπλισμό που θα απαιτηθεί από την Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας προκειμένου να εκτελέσει τις προβλεπόμενες, από το Ενιαίο Μοντέλο Διαδικασιών, ενέργειες επί τόπου στη σκηνή όπου εντοπίστηκε το περιστατικό ασφαλείας, όσο και τη συνολική υποδομή ενός εργαστηρίου Ψηφιακής Εγκληματολογίας, η οποία θα επιτρέψει στους ειδικούς τη λεπτομερή τεχνική ανάλυση των συλλεχθέντων πειστηρίων. Στη συνέχεια της ενότητας περιγράφεται η εργαλειοθήκη που πρέπει να πλαισιώνει τις επιτόπου ενέργειες του αρμόδιου προσωπικού. Η περιγραφή ενός πρότυπου εργαστηρίου ακολουθεί στην επόμενη ενότητα.

4.3.1 Προετοιμασία – Προπαρασκευή

Η σωστή προετοιμασία και μελέτη των παραμέτρων του περιστατικού από το προσωπικό πριν την άφιξή του στη σκηνή, αποτελούν κλειδιά για την επιτυχή αντιμετώπιση του συμβάντος. Όπως προαναφέρθηκε, η στελέχωση της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας προκύπτει, σε ένα βαθμό, αναλόγως της φύσης του περιστατικού. Για παράδειγμα, όταν εντοπίζεται ένα συμβάν που αφορά προσβολή μιας βάσης δεδομένων τύπου Όρακλ (Oracle), είναι αναγκαίο να ενταχθεί στην ομάδα, εάν δεν υπάρχει ήδη, μέλος το οποίο θα είναι εξειδικευμένο στη συγκεκριμένη τεχνολογία.

Παρόμοια, θα πρέπει εκ των προτέρων να εξασφαλιστεί και να διατηρείται από την ομάδα μια εργαλειοθήκη (toolkit), η οποία θα της δίνει τη δυνατότητα να διαχειριστεί οποιοδήποτε περιστατικό συμβεί στα συστήματα που διαθέτει ο Οργανισμός και υπάρχει περίπτωση μελλοντικά να αποτελέσουν αντικείμενο έρευνας. Στο στρατιωτικό περιβάλλον, όπως και στα περισσότερα εταιρικά, τα τεχνικά χαρακτηριστικά αλλά και το λογισμικό που υπάρχει εγκατεστημένο στα μηχανήματα είναι γνωστό, καθορισμένο και ελεγχόμενο. Το γεγονός αυτό αποτελεί σημαντικό παράγοντα για την εξασφάλιση, σε προγενέστερο χρόνο, του απαραίτητου εξοπλισμού που πρέπει να έχει η εργαλειοθήκη της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας και παράλληλα συμβάλλει στην αποφυγή άσκοπων καθυστερήσεων οι οποίες, αναλόγως του περιστατικού, μπορεί να είναι έχουν ανεπανόρθωτες συνέπειες.

4.3.2 Εργαλειοθήκη Αντιμετώπισης Περιστατικών Ασφαλείας

Η εργαλειοθήκη Αντιμετώπισης Περιστατικών Ασφαλείας (IR Toolkit) [10], θα χρησιμοποιηθεί από την αντίστοιχη ομάδα, η οποία θα ενεργήσει στο σημείο όπου ανιχνεύθηκε το περιστατικό ασφαλείας. Τα περιεχόμενά της πρέπει να είναι τέτοια ώστε να επιτρέπουν στο προσωπικό να εκτελέσει τα στάδια της Εξασφάλισης-Καταγραφής Σκηνής, «Εν Ενεργεία» Αντιμετώπισης, Παραγωγής Ψηφιακών Αντιγράφων και Συσκευασίας-Μεταφοράς Ψηφιακών Πειστηρίων της Φάσης Αναλύσεως του Ενιαίου Μοντέλου Διαδικασιών, όπως προδιαγράφηκε στο προηγούμενο κεφάλαιο.

Το σύνολο του προσωπικού της ομάδας θα πρέπει να γνωρίζει τον τρόπο λειτουργίας των περιεχομένων της εργαλειοθήκης, είτε πρόκειται για υλικό είτε για λογισμικό. Κύρια αποστολή της ομάδας είναι η αναγνώριση, η συλλογή και η ασφαλής μεταφορά στο εργαστήριο των ψηφιακών αποδεικτικών στοιχείων με ευρέως αποδεκτές και τεχνικά ακριβείς μεθόδους. Η ευαισθησία και μη αναστρεψιμότητα στην αρχική κατάσταση των ψηφιακών στοιχείων δεν επιτρέπουν λάθη, ακούσια ή εκούσια, από το προσωπικό. Για το λόγο αυτό, κατά την εκτέλεση των διαδικασιών από τα μέλη, θα πρέπει να λαμβάνεται η μέγιστη δυνατή προσοχή και σε καμία περίπτωση δεν πρέπει να πραγματοποιούνται ενέργειες πέραν των ορίων των γνώσεων τους.

Τα απαραίτητα χαρακτηριστικά της εργαλειοθήκης είναι:

- Σχετικά μικρό μέγεθος και τη δυνατότητα φορητότητας λόγω της ανάγκης επιτόπιας χρήσης.
- Τα μέσα της εργαλειοθήκης θα πρέπει να έχουν επιλεγεί έτσι ώστε να αποφεύγεται η παραγωγή ή η μετάδοση, διαμέσου αυτών, φορτίων στατικού ηλεκτρισμού και ηλεκτρομαγνητικών πεδίων, τα οποία μπορεί να αλλοιώσουν τα δεδομένα.
- Το στάδιο της καταγραφής της σκηνής προϋποθέτει την ύπαρξη μέσων τα οποία θα επιτρέψουν την ανακατασκευή της σε μεταγενέστερο χρόνο στο εργαστήριο, όπως ψηφιακές φωτογραφικές μηχανές.
- Για τη συλλογή ευμετάβλητων (volatile) δεδομένων στη διαδικασία της «Εν Ενεργεία» συλλογής, θα πρέπει να έχει προβλεφθεί η ύπαρξη ανάλογου ψηφιακού μέσου με τα αντίστοιχα εργαλεία (bootable live CD ή USB συσκευή αποθήκευσης).
- Το λογισμικό που χρησιμοποιείται για τη συλλογή και παραγωγή ψηφιακών αντιγράφων θα πρέπει είτε να έχει προμηθευτεί και να λειτουργεί με την αντίστοιχη ενεργή και επικαιροποιημένη άδεια είτε εφόσον πρόκειται για Ανοικτού Κώδικα να τυγχάνει ευρείας αποδοχής, χρήσης και ελέγχων από διεθνείς κοινότητες και ιδρύματα. Για την εξασφάλιση μεγαλύτερης αξιοπιστίας, θα πρέπει να χρησιμοποιούνται περισσότερα του ενός λογισμικά παραγωγής αντιγράφων.
- Στην περίπτωση κατά την οποία δεν υπάρχει η δυνατότητα συλλογής και μεταφοράς του αυθεντικού μέσου που περιλαμβάνει τα ψηφιακά πειστήρια, θα πρέπει να έχει ληφθεί μέριμνα ώστε να μπορούν να καλυφθούν

τυχόν εξεζητημένες ανάγκες χωρητικότητας για τη λήψη πρωτεύοντος αντιγράφου.

Επιγραμματικά, τα απαραίτητα συστατικά μιας εργαλειοθήκης Αντιμετώπισης Περιστατικών Ασφαλείας έχουν ως εξής:

- Προστατευτική ταινία (ερυθρόλευκη) και σήμανση απαγόρευσης εισόδου.
- Ψηφιακή φωτογραφική μηχανή ή κάμερα.
- Φακός.
- Μπλοκ μιλιμετρέ ή άλλου τύπου (για τη σχεδίαση της σκηνής).
- Μικρή συλλογή ηλεκτρολόγου.
- Φορητό μέσο (bootable live CD ή USB) που θα φέρει το επιθυμητό λογισμικό συλλογής ψηφιακών στοιχείων.
- Φορητή συσκευή αποθήκευσης μεγάλης χωρητικότητας.
- Φορητός υπολογιστής εξοπλισμένος με εργαλεία συλλογής ψηφιακών στοιχείων και παραγωγής ψηφιακών αντιγράφων.
- Καλωδιοταινία IDE για σκληρούς δίσκους παλαιότερης γενιάς.
- Καλώδιο τύπου SATA για σκληρούς δίσκους νεότερης γενιάς.
- Μετατροπείς συνδέσεων και καλωδίων αναλόγως των απαιτήσεων.
- Συσκευή απαγόρευσης εγγραφής (write blocker) με σύνδεση FireWire ή USB.
- Αντιστατικές σακούλες.
- Πινακίδες, ετικέτες και ταινίες σήμανσης πειστηρίων.
- Έντυπα Ψηφιακών Πειστηρίων.
- Σημειωματάριο ή συσκευή καταγραφής φωνής.
- Γραφική ύλη.

Εικόνα 4.1 : Περιεχόμενα Εργαλειοθήκης Αντιμετώπισης Περιστατικών Ασφαλείας (Πηγή: Nelson B., Guide to Computer Forensics and Investigations, 4th edition)

Πέραν των παραπάνω, και εφόσον υπάρχει η δυνατότητα μεταφοράς επιπλέον αντικειμένων, η εργαλειοθήκη μπορεί να περιλαμβάνει και:

- Τεχνικά εγχειρίδια που αφορούν στα χρησιμοποιούμενα Λειτουργικά Συστήματα, εφαρμογές αλλά και μεθοδολογίες Ψηφιακής Εγκληματολογίας.
- Καλώδια παροχής ηλεκτρικού ρεύματος.
- Επιπλέον φορητούς σκληρούς δίσκους για τη συλλογή δεδομένων και δημιουργία αντιγράφων.
- Φορητούς δίσκους με εξωτερική τροφοδοσία.
- Φορητές συσκευές αποθήκευσης USB διαφόρων χωρητικοτήτων.
- Γάντια δερμάτινα και μιας χρήσης.
- Βουρτσάκι ή φορητό ηλεκτρικό σκουπάκι.
- Εργαλεία (συρματοκοπίδες, λοστούς κλπ).
- Καρότσια μεταφοράς.
- Χαρτοκιβώτια και σακούλες συσκευασίας.
- Λάστιχα ή δεματικά (tire ups).
- Μεγεθυντικό φακό.

Εικόνα 4.2 : Φορητή Συσκευή Προστασίας Εγγραφής (Portable Write Blocker) (Πηγή: www.digitalintelligence.com)

4.3.3 Εργαλεία Λογισμικού

Όπως αναφέρθηκε παραπάνω, η εργαλειοθήκη Αντιμετώπισης Περιστατικών Ασφαλείας θα χρησιμοποιηθεί από την αντίστοιχη ομάδα για την εκτέλεση, μεταξύ άλλων, των ενεργειών που περιλαμβάνονται στο στάδιο της «Εν Ενεργεία» Αντιμετώπισης, με σκοπό τη συλλογή ευμετάβλητων (volatile) δεδομένων. Τα δεδομένα αυτά είναι ιδιαίτερα σημαντικά, διότι δεν είναι δυνατόν να αναπαραχθούν και να συλλεχθούν μετά την παύση της λειτουργίας του υπολογιστή, καθώς είτε πρόκειται για δεδομένα που βρίσκονται στη μνήμη RAM του υπολογιστή είτε αφορούν στην τρέχουσα δικτυακή κίνηση. Για τη συλλογή και ανάλυση αυτών των δεδομένων απαιτούνται συγκεκριμένα εργαλεία λογισμικού, τα οποία πρέπει να περιλαμβάνονται στη συλλογή.

Για τη συλλογή των δεδομένων που βρίσκονται στη μνήμη RAM ενός υπολογιστή, το δημοφιλέστερο εργαλείο που μπορεί να χρησιμοποιηθεί είναι το **Volatility**. Πρόκειται για ένα εργαλείο κατάλληλο για τις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ανάλυσης Κακόβουλου Λογισμικού (Malware Analysis), στις οποίες η διατήρηση του υπολογιστή σε λειτουργία είναι απαραίτητη, καθώς μόνο σε αυτή την κατάσταση μπορεί να παρατηρηθεί και να γίνει κατανοητή η επέμβαση στο σύστημα που έχει προσβληθεί. Το Volatility επιτρέπει την εξαγωγή ευρημάτων και στοιχείων από αποθηκευμένα στιγμιότυπα της μνήμης RAM (memory dumps). Αναλυτικότερα, παρέχει τη δυνατότητα εξαγωγής και παρουσίασης πληροφοριών που αφορούν στις τρέχουσες διαδικασίες, στις ενεργές δικτυακές πόρτες και συνδέσεις, στα εξειδικευμένα αρχεία που έχουν «φορτωθεί» για την εκτέλεση των διαφόρων διαδικασιών, στην ταυτότητα κάθε ενεργής διαδικασίας (process ID) και σε παρόμοια λοιπά δεδομένα. «Ελεύθερη» εκτελέσιμη έκδοση του Volatility κυκλοφορεί για τα Λειτουργικά Συστήματα Windows και Linux.

Για τη συλλογή και ανάλυση δεδομένων της τρέχουσας δικτυακής κίνησης μπορεί να χρησιμοποιηθεί το δωρεάν λογισμικό ανοικτού κώδικα **Wireshark**, το οποίο είναι διαθέσιμο για τα σημαντικότερα Λειτουργικά Συστήματα. Πρόκειται για ένα λογισμικό σύλληψης δικτυακών πακέτων και ανάλυσης πρωτοκόλλων δικτύου υπολογιστών, το οποίο χρησιμοποιείται για τις ενέργειες της παρακολούθησης και ανάλυσης ενός δικτύου και τον εντοπισμό και αντιμετώπιση των προβλημάτων που προκύπτουν. Επιτρέπει στο χρήστη να παρακολουθήσει όλη τη δικτυακή κίνηση που γίνεται στο δίκτυο και όχι μόνο αυτή που αφορά σε μια συγκεκριμένη διεργασία και στη συνέχεια να φιλτράρει τα δεδομένα μέσω πολλών επιλογών ταξινόμησης. Από εκεί και πέρα ο εξειδικευμένος αναλυτής πρέπει να χρησιμοποιήσει τις τεχνικές γνώσεις του για να καταλήξει σε χρήσιμα συμπεράσματα από τα παρεχόμενα στοιχεία.

Τέλος, η εργαλειοθήκη Αντιμετώπισης Περιστατικών Ασφαλείας μπορεί να περιλαμβάνει εκκινήσιμους οπτικούς δίσκους (bootable live CDs) που περιέχουν Λειτουργικά Συστήματα με προεγκατεστημένα εργαλεία Ψηφιακής Εγκληματολογίας, όπως το **Deft** και το **Helix**. Παρόλα αυτά, οι συγκεκριμένοι δίσκοι συχνά απαιτούν την επανεκκίνηση του υπολογιστή, με αποτέλεσμα μέρος των πολύτιμων δεδομένων να απωλεσθεί.

4.4 Εργαστήριο Ψηφιακής Εγκληματολογίας

4.4.1 Γενικά Στοιχεία

Το εργαστήριο Ψηφιακής Εγκληματολογίας είναι ο κατάλληλα διαμορφωμένος και εξοπλισμένος χώρος, στον οποίο καταλήγουν τα ψηφιακά πειστήρια που έχουν συλλεχθεί από την Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας, προκειμένου να υποστούν λεπτομερείς τεχνικές αναλύσεις από τους εξειδικευμένους ερευνητές που το στελεχώνουν. Πιο συγκεκριμένα, στο εργαστήριο λαμβάνουν χώρα τα στάδια της Παραγωγής Ψηφιακών Αντιγράφων (για την παραγωγή των αντιγράφων εργασίας από το αυθεντικό μέσο ή το πρωτεύον αντίγραφο), Φύλαξης Ψηφιακών Πειστηρίων, Ανάκτησης Δεδομένων – Μεταδεδομένων, Διαχωρισμού – Οργάνωσης και Ανάλυσης των Δεδομένων της Φάσης Αναλύσεως του Ενιαίου Μοντέλου Διαδικασιών. Από την τεχνική ανάλυση των στοιχείων αυτών θα προκύψουν τα ευρήματα, τα οποία θα περιγράφονται στην Έκθεση Πραγματογνωμοσύνης που εκπονεί το εργαστήριο και τα οποία θα αποτελέσουν την κύρια πηγή πληροφοριών κατά τη συγγραφή της τελικής αναφοράς, όπου περιγράφεται το ιστορικό του περιστατικού και οι ενέργειες που έλαβαν χώρα κατά τη διάρκεια της αντιμετώπισης και ανάλυσής του.

Στο υπόλοιπο της ενότητας περιγράφονται οι απαιτήσεις που πρέπει να πληρούνται εκ των προτέρων και οι οποίες θα εξασφαλίσουν την ορθή λειτουργία του εργαστηρίου καθώς και οι προδιαγραφές σχετικά με την κατασκευή και τη διαμόρφωσή του [10] [13]. Στη συνέχεια παρουσιάζονται τα χαρακτηριστικά που πρέπει να έχουν οι «Σταθμοί Εργασίας Ψηφιακής Εγκληματολογίας» (Forensics Workstations), οι οποίοι αποτελούν το κύριο εργαλείο ενός τέτοιου εργαστηρίου. Τέλος γίνεται αναφορά σε θέματα που αφορούν στη διαδικασία διαπίστευσης ενός εργαστηρίου Ψηφιακής Εγκληματολογίας.

4.4.2 Λειτουργικές Απαιτήσεις

Στο εργαστήριο Ψηφιακής Εγκληματολογίας λαμβάνουν χώρα οι περισσότερες ενέργειες που σχετίζονται με το χειρισμό και την ανάλυση των δεδομένων που συλλέχτηκαν από τη σκηνή που εντοπίστηκε το περιστατικό ασφαλείας. Επίσης πρόκειται για το χώρο όπου τα αυθεντικά ψηφιακά πειστήρια φυλάσσονται, με σκοπό να εξασφαλισθεί η εμπιστευτικότητα των πληροφοριών και η ακεραιότητα των δεδομένων, ώστε να μπορούν να χρησιμοποιηθούν χωρίς καμία αμφισβήτηση σε νομικές και λοιπές πειθαρχικές διαδικασίες που πιθανώς να έπονται μιας έρευνας. Για να επιτευχθούν τα παραπάνω, το εργαστήριο πρέπει να πληροί ορισμένες προδιαγραφές. Η συμμόρφωση του εργαστηρίου απέναντι σε αυτές τις απαιτήσεις αποτελεί κύριο καθήκον του επικεφαλής του εργαστηρίου (lab manager).

Αρχικά, η λειτουργία του εργαστηρίου θα πρέπει να γίνεται βάσει καθορισμένων πολιτικών και διαδικασιών με σκοπό να επιτευχθούν συγκεκριμένα αποτελέσματα. Ο επικεφαλής του εργαστηρίου είναι υπεύθυνος να καταρτίσει την πολιτική λειτουργίας του τμήματός του και να τη θέσει στη Διοίκηση του Οργανισμού για έγκριση. Στη συνέχεια, εξειδικεύοντας τα όσα

γενικά αναφέρονται στην πολιτική, οφείλει να προδιαγράψει λεπτομερώς τον τρόπο λειτουργίας και τις διαδικασίες αντιμετώπισης αναλόγως του περιστατικού ασφαλείας που ανιχνεύεται κάθε φορά και τις οποίες το προσωπικό του εργαστηρίου θα οφείλει να ακολουθεί επακριβώς. Η περιγραφή, εκτός των τεχνικών λεπτομερειών που σχετίζονται με την ανάλυση και αντιμετώπιση ενός περιστατικού, θα πρέπει να περιλαμβάνει όλο το φάσμα των λοιπών ενεργειών που πραγματοποιούνται στο εργαστήριο, όπως για παράδειγμα την αναφορά και καταγραφή ενός περιστατικού από τη στιγμή της ανίχνευσής του, την παρακολούθηση των ψηφιακών πειστηρίων (αλυσίδα κυριότητας) και τον έλεγχο του εισερχόμενου προσωπικού στο εργαστήριο. Η ύπαρξη και συνεπής τήρηση προδιαγεγραμμένων διαδικασιών εξασφαλίζει την ποιότητα και την αξιοπιστία των αποτελεσμάτων που παρέχει το εργαστήριο στις έρευνες, ενώ αποτελεί και προαπαιτούμενη υποχρέωση στην περίπτωση που η υποδομή υποβληθεί σε διαδικασία πιστοποίησης από αντίστοιχο εξωτερικό φορέα. Στο ελληνικό στρατιωτικό περιβάλλον, η πιστοποίηση των κεντρικών Πληροφοριακών Εγκαταστάσεων τα τελευταία χρόνια σύμφωνα με το διεθνές πρότυπο ISO 27001, που αφορά στα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών, καταδεικνύει ότι ήδη έχουν γίνει ενέργειες προς την κατεύθυνση της προτυποποίησης και τήρησης καθορισμένων διαδικασιών στο στρατό και έχει αποκτηθεί η ανάλογη εμπειρία. Παρόλα αυτά, στην περίπτωση που αποφασιστεί η δημιουργία και λειτουργία δυνατοτήτων Αντιμετώπισης Περιστατικών Ασφαλείας και εργαστηρίου Ψηφιακής Εγκληματολογίας θα πρέπει, όπως αναφέρθηκε και παραπάνω, να καταρτιστεί ιδιαίτερη πολιτική και να προδιαγραφούν ξεχωριστές διαδικασίες, ώστε οι νέες δυνατότητες να καλύπτουν τις απαιτήσεις.

Επιπλέον, απαιτείται να εξασφαλιστεί το κατάλληλο προσωπικό που θα στελεχώσει το εργαστήριο. Έχοντας υπόψη τα όσα καθορίζονται στην πολιτική λειτουργίας σχετικά με την αντιμετώπιση των περιστατικών ασφαλείας, τους επιδιωκόμενους σκοπούς και τα καθορισμένα όρια (χρονικά, οικονομικής ζημίας, ανοχής σε περιστατικά ασφαλείας κτλ.), ο επικεφαλής του εργαστηρίου οφείλει να καθορίσει τα απαιτούμενα προσόντα και να επιλέξει προσωπικό που θα δύναται να ανταποκριθεί στις απαιτήσεις. Σε κάθε περίπτωση, τα μέλη του εργαστηρίου πρέπει να έχουν ισχυρές γνώσεις σε θέματα υλικού και λογισμικού, όπως για παράδειγμα σχετικά με τα Λειτουργικά Συστήματα και τα Συστήματα Αρχείων. Επίσης το προσωπικό θα πρέπει να χαρακτηρίζεται από επαγγελματισμό και θέληση για συνεχή βελτίωση και επέκταση των γνώσεών του. Κάθε στέλεχος πρέπει να παρακολουθείται διαρκώς από τον επικεφαλής και να αξιολογείται από αυτόν και τους συναδέλφους του μέσω διαφανών και αντικειμενικών διαδικασιών για τη διαπίστωση της αποδοτικότητάς του. Τα δεδομένα σχετικά με το προσωπικό που θα στελεχώσει τις εν λόγω δυνατότητες στο στρατιωτικό περιβάλλον αναλύθηκαν λεπτομερώς σε προηγούμενη ενότητα.

Ακολούθως πρέπει να καθοριστούν οι δυνατότητες και τα μέσα του εργαστηρίου. Σε ένα κλειστό και ελεγχόμενο περιβάλλον, όπως το στρατιωτικό, τα τεχνικά χαρακτηριστικά των συστημάτων που υπάρχει

πιθανότητα να προσβληθούν και να αποτελέσουν αντικείμενα ερευνών είναι γνωστά από πριν, όπως γνωστό είναι και το σύνολο του λογισμικού που φέρουν. Επίσης, τα διάφορα τμήματα λειτουργίας τηρούνε στοιχεία που αφορούν στα είδη των περιστατικών που έχουν ανιχνευθεί κατά καιρούς στις υποδομές τους. Οι παραπάνω πληροφορίες είναι άκρως σημαντικές για τον αρχικό προσδιορισμό των δυνατοτήτων του εργαστηρίου, υποδεικνύοντας τα είδη των περιστατικών στα οποία θα πρέπει να δοθεί μεγαλύτερη προσοχή και τα οποία θα πρέπει να αναλύονται στις προδιαγεγραμμένες διαδικασίες. Ο αριθμός και ο τύπος των επιθέσεων θα καθορίσει και την επιλογή του αριθμού και του είδους των τεχνικών μέσων με τα οποία θα εξοπλιστεί το εργαστήριο αλλά και το προσωπικό που θα το στελεχώσει, δίνοντας προτεραιότητα σε άτομα με γνώσεις πάνω στις συγκεκριμένες τεχνολογίες και μεθόδους. Για παράδειγμα, σε ενδεχόμενη προπαρασκευαστική μελέτη για την έναρξη λειτουργίας εργαστηρίου Ψηφιακής Εγκληματολογίας στο ελληνικό στρατιωτικό περιβάλλον, θα πρέπει να ληφθεί υπόψη ότι το σύνολο των μηχανημάτων που υποστηρίζονται φέρει Λειτουργικό Σύστημα τύπου Windows 7, ενώ υπάρχει αριθμός μηχανημάτων με Λειτουργικό Σύστημα Windows XP και κάποιοι εξυπηρετητές που έχουν εγκατεστημένες διανομές του Λειτουργικού Συστήματος Linux. Επίσης η πλειονότητα των συστημάτων χρησιμοποιεί πακέτα εργαλείων γραφείου τύπου Microsoft Office, ενώ οι εκάστοτε εξειδικευμένες εφαρμογές έχουν στο σύνολό τους αναπτυχθεί εντός του στρατού και το μόνιμο προσωπικό Πληροφορικής γνωρίζει τις επιμέρους λεπτομέρειες στη συγγραφή και λειτουργία του κώδικα. Το ίδιο γνωστές είναι και λεπτομέρειες που αφορούν στις δικτυακές υποδομές, είτε πρόκειται για το εσωτερικό δίκτυο είτε για το δίκτυο με πρόσβαση στο Διαδίκτυο. Η υπάρχουσα κατάσταση επιβάλλει τον εξοπλισμό ενός μελλοντικού εργαστηρίου με μηχανήματα και εργαλεία Ψηφιακής Εγκληματολογίας κατάλληλα για τα συγκεκριμένα Λειτουργικά Συστήματα και εφαρμογές, ενώ και το προσωπικό θα οφείλει να επικεντρώσει το ενδιαφέρον του στις χρησιμοποιούμενες τεχνολογίες ώστε να επιτύχει μεγαλύτερο βαθμό εξειδίκευσης και αποδοτικότητας.

Η εξασφάλιση του απαραίτητου προϋπολογισμού αποτελεί εξίσου σημαντική προϋπόθεση για τη λειτουργία του εργαστηρίου. Ο επικεφαλής θα πρέπει έγκαιρα να μελετά το σύνολο των αναγκών ώστε να εξασφαλίζει τα απαραίτητα χρηματικά ποσά. Τα έξοδα του εργαστηρίου περιλαμβάνουν τη συμμετοχή του προσωπικού σε εκπαιδεύσεις και τεχνικά σεμινάρια προκειμένου να εμπλουτιστούν οι γνώσεις του πάνω σε τρέχοντα θέματα ενδιαφέροντος (μεθοδολογίες, νέες τεχνολογίες και εργαλεία, τρέχουσες τάσεις Κυβερνοεπιθέσεων κτλ.), την αναβάθμιση των υπαρχόντων τεχνικών μέσων ή την προμήθεια νέων που να καλύπτουν τις εκάστοτε ανάγκες, την εξασφάλιση, αναλόγως των αναγκών, των απαραίτητων αδειών λειτουργίας του εξειδικευμένου λογισμικού, την πιστοποίηση του προσωπικού αλλά και του εργαστηρίου συνολικά και τις λοιπές τρέχουσες ανάγκες. Στην περίπτωση που δεν εξασφαλιστεί η απαιτούμενη δαπάνη για κάποια από τις παραπάνω ανάγκες, τίθεται σε αμφιβολία η αποτελεσματικότητα του συνολικού έργου του εργαστηρίου. Για τον λόγο αυτό, ο επικεφαλής προσδιορίζει προσεκτικά τις

δυνατότητες που αναφέρθηκαν στην προηγούμενη παράγραφο και καταλήγει στις κατάλληλες ανά περίπτωση οικονομικές απαιτήσεις, τις οποίες και παρουσιάζει λεπτομερώς στη Διοίκηση ώστε να επιτύχει τη ζητούμενη χρηματοδότηση.

Τέλος, για τη σωστή δημιουργία και ομαλή λειτουργία μελλοντικά του εργαστηρίου Ψηφιακής Εγκληματολογίας, ο επικεφαλής πρέπει να έχει εξασφαλίσει τη στήριξη της Διοίκησης. Η εν λόγω απαίτηση είναι και η πλέον σημαντική, καθώς η στήριξη της Διοίκησης είναι προαπαιτούμενη για την κάλυψη όλων των παραπάνω απαιτήσεων. Η έγκρισή της απαιτείται ώστε να διαμορφωθεί και να τεθεί σε ισχύ η προτεινόμενη πολιτική λειτουργίας, ενώ και κατά τη διάρκεια των ελέγχων για την πιστή τήρησή της ο επικεφαλής πρέπει να γνωρίζει ότι ενεργεί έχοντας τη στήριξή της. Επίσης, συνυπολογίζοντας τις εισηγήσεις του υπεύθυνου του εργαστηρίου, η Διοίκηση έχει τον τελευταίο και ουσιαστικότερο λόγο σχετικά με τη στελέχωση του εργαστηρίου από το κατάλληλο προσωπικό. Παράλληλα, καμία δαπάνη δεν μπορεί να πραγματοποιηθεί χωρίς την έγκρισή της και αποτελεί σημαντική πρόκληση για τον υπεύθυνο του εργαστηρίου να πείσει για την αναγκαιότητα των ζητούμενων εξόδων.

4.4.3 Φυσικές Προδιαγραφές

Αφού εξασφαλιστούν όλες οι απαιτήσεις που αναφέρθηκαν προκειμένου να επιτυγχάνεται η σωστή λειτουργία του εργαστηρίου, στη συνέχεια πρέπει να βρεθεί και να διαμορφωθεί ο κατάλληλος χώρος όπου θα στεγασθεί. Επειδή οι πληροφορίες που αναλύονται κατά τη διάρκεια των ερευνών ενός περιστατικού ασφαλείας στο στρατιωτικό περιβάλλον συχνά είναι διαβαθμισμένες, είτε πρόκειται για προσωπικά δεδομένα είτε για πληροφορίες στρατιωτικής αξίας, πέραν του επιπέδου ασφάλειας που προβλέπεται από τις πολιτικές και τις προδιαγεγραμμένες διαδικασίες, θα πρέπει και η ίδια υποδομή να πληροί κάποιες φυσικές προδιαγραφές ώστε να συμβάλλει στην αποφυγή της υποκλοπής ή αλλοίωσης των πληροφοριών αυτών.

4.4.3.1 Κατασκευαστικά Χαρακτηριστικά

Για τις ανάγκες λειτουργίας ενός εργαστηρίου Ψηφιακής Εγκληματολογίας θα πρέπει να διατίθεται απαραίτητα ένας σταθερά περίκλειστος χώρος. Επειδή οι εργασίες που λαμβάνουν χώρα στο εργαστήριο απαιτούν την εξασφάλιση της εμπιστευτικότητας των πληροφοριών από οποιονδήποτε δεν εκτελεί εξουσιοδοτημένη εργασία στα πλαίσια των καθηκόντων του, η υλοποίηση του εργαστηρίου θα πρέπει να γίνει σε χώρο ο οποίος διαχωρίζεται επαρκώς από τις υπόλοιπες εγκαταστάσεις και μπορεί να απομονωθεί. Σε καμία περίπτωση το εργαστήριο δεν μπορεί να οριοθετείται εντός ενός μεγαλύτερου ανοιχτού χώρου και να απομονώνεται με πρόσθετα μετακινούμενα διαχωριστικά. Επειδή η διαδικασία της ανάλυσης των ψηφιακών πειστηρίων που σχετίζονται με τις έρευνες ενός περιστατικού ασφαλείας μπορεί να διαρκέσει για μεγάλο χρονικό διάστημα, το εργαστήριο θα πρέπει να μπορεί λειτουργήσει ως ασφαλής αποθηκευτικός χώρος για τους φορείς των δεδομένων αυτών. Έτσι, ανεξαρτήτως του συνολικού μεγέθους που μπορεί να

έχει, ένα εργαστήριο Ψηφιακής Εγκληματολογίας θα πρέπει κατ' ελάχιστο να διαθέτει τα παρακάτω κατασκευαστικά χαρακτηριστικά:

- Επαρκές δωμάτιο με πραγματικούς (χτιστούς) τοίχους από το πάτωμα μέχρι την οροφή.
- Πρόσβαση μέσω πόρτας που φέρει μηχανισμό ασφαλείας, είτε πρόκειται για κοινή κλειδαριά είτε για ηλεκτρονική κλειδαριά με κωδικό ασφαλείας είτε για σύστημα ελέγχου εισόδου με μαγνητική κάρτα (access control). Σε κάθε περίπτωση απαιτείται προσεκτική διαχείριση των κλειδιών - καρτών ή του κωδικού και διανομή μόνο στο εξουσιοδοτημένο προσωπικό.
- Ύπαρξη χρηματοκιβωτίου ή σταθερού (πακτωμένου) φωριαμού ο οποίος θα φέρει λουκέτο ασφαλείας.

4.4.3.2 Ηλεκτρομαγνητική Προστασία

Όπως αναφέρθηκε, στο μεγαλύτερο μέρος των στρατιωτικών Πληροφοριακών Συστημάτων διακινούνται διαβαθμισμένες πληροφορίες στρατιωτικής αξίας που σχετίζονται με θέματα εθνικής ασφάλειας. Το παραπάνω γεγονός δικαιολογεί το χαρακτηρισμό των ερευνών ενός περιστατικού ασφαλείας στα συστήματα αυτά ως «υψηλού κινδύνου». Όσο η τεχνολογία εξελίσσεται, η διατήρηση της εμπιστευτικότητας των πληροφοριών που αναλύονται σε μια έρευνα Ψηφιακής Εγκληματολογίας γίνεται δυσκολότερη. Κακόβουλοι στοχοποιούν τις αντίστοιχες εγκαταστάσεις όπου λαμβάνει χώρα διακίνηση και ανάλυση δεδομένων και εκμεταλλευόμενοι την πληθώρα και ευκολία προμήθειας συσκευών που μπορούν να υποκλέψουν επικοινωνίες και μεταδόσεις οποιασδήποτε μορφής, αποκτούν μη εξουσιοδοτημένη πρόσβαση σε ένα μέρος των πληροφοριών.

Όλα τα ηλεκτρονικά και ηλεκτρικά συστήματα εκπέμπουν ηλεκτρομαγνητική ακτινοβολία, η οποία διαδίδεται μέσω των αγώγιμων επιφανειών που βρίσκονται κοντά σε αυτές τις συσκευές, αλλά και διαμέσου άλλων καναλιών όπως οι τηλεφωνικές γραμμές, τα καλώδια παροχής ηλεκτρικού ρεύματος και οι διάφορες κεραίες. Αυτή η ακτινοβολία μπορεί να υποκλαπεί από κατάλληλες για το σκοπό συσκευές σε συγκεκριμένη απόσταση από την πηγή, αποκαλύπτοντας με αυτόν τον τρόπο το σύνολο ή μέρος των διακινούμενων πληροφοριών. Γίνεται αντιληπτό ότι οι τεχνικές δυνατότητες που έχει ένας κακόβουλος, η απόσταση στην οποία μπορεί να προσεγγίσει τις εγκαταστάσεις όπου διακινούνται οι πληροφορίες αλλά και η αξία που μπορεί να έχουν οι πληροφορίες για το ίδιο καθορίζουν το μέγεθος της απειλής.

Η διαδικασία αναλύσεως και μελέτης των ανεπιθύμητων και επικίνδυνων για την ασφάλεια διαφευγουσών ακτινοβολιών καλείται TEMPEST [8]. Ο όρος TEMPEST χρησιμοποιείται επίσης για να περιγράψει τα φαινόμενα αυτά καθώς και τους μηχανισμούς καταστολής τους. Στο στρατιωτικό περιβάλλον, το NATO έχει εκδώσει ειδικά εγχειρίδια με οδηγίες για τον τρόπο διεξαγωγής των μετρήσεων TEMPEST, στα οποία αναφέρονται και τα όρια εντός των οποίων οι μετρήσεις θα πρέπει να εμπίπτουν.

Μερικά από τα μέτρα που μπορούν να εφαρμοστούν εναντίον της πιθανότητας ηλεκτρομαγνητικής απειλής είναι τα κάτωθι:

- Σωστή και ασφαλής γείωση των συσκευών.
- Ηλεκτρομαγνητική θωράκιση των διαβαθμισμένων χώρων και συσκευών (πχ. με την τοποθέτηση φύλλων χαλκού σε πόρτες, παράθυρα και οροφές).
- Διαχωρισμός των διαβαθμισμένων από τα αδιαβάθμητα κυκλώματα επεξεργασίας και διαβίβασης πληροφοριών.
- Χρήση φίλτρων για τον περιορισμό ή αποφυγή της εκπεμπόμενης ακτινοβολίας των επικοινωνιακών συσκευών και γραμμών μεταφοράς.
- Αποφυγή τηλεφωνικής εγκατάστασης ή χρησιμοποίηση ειδικών φίλτρων στις τηλεφωνικές γραμμές εντός των χώρων επεξεργασίας διαβαθμισμένων πληροφοριών.
- Αποφυγή τοποθέτησης των συσκευών και των οθονών κοντά σε μεταλλικά έπιπλα και παράθυρα.
- Ύπαρξη ειδικών διαφραγμάτων σε όλους τους αγωγούς θέρμανσης και εξαερισμού ώστε να παγιδεύουν την εκπεμπόμενη ακτινοβολία.
- Πρόσβαση στο διαβαθμισμένο χώρο μέσω δύο θυρών με την ύπαρξη ενδιάμεσου κενού χώρου. Οι θύρες θα είναι επενδυμένες με κατάλληλο υλικό που δεν επιτρέπει τη διαφυγή ακτινοβολίας και κατά την είσοδο θα πρέπει να αποφεύγεται να είναι και οι δύο ταυτόχρονα ανοικτές.

Επειδή η κατασκευή ενός εργαστηρίου σύμφωνα με τις προδιαγραφές TEMPEST μπορεί να είναι αρκετά δαπανηρή, ενώ παράλληλα απαιτεί συχνούς ελέγχους και επιθεωρήσεις για τη διαπίστωση της κατάστασής του, υπάρχει η εναλλακτική λύση της χρησιμοποίησης ειδικών μηχανημάτων τα οποία χαρακτηρίζονται από χαμηλά επίπεδα εκπεμπόμενης ακτινοβολίας. Τα συγκεκριμένα μηχανήματα είναι πιο ακριβά από τους συνηθισμένους υπολογιστές, αλλά σε κάθε περίπτωση πιο οικονομικά από ότι η κατασκευή μιας υποδομής τύπου TEMPEST.

4.4.3.3 Φωριαμοί Ψηφιακών Πειστηρίων

Σύμφωνα με το Ενιαίο Μοντέλο Διαδικασιών, τα ψηφιακά πειστήρια που θα συλλεχθούν από τη σκηνή όπου ανιχνεύθηκε το περιστατικό ασφαλείας θα μεταφερθούν στο εργαστήριο όπου και θα αποθηκευτούν προς φύλαξη, ταυτόχρονα με την ανάλυσή τους. Ο χώρος που θα στεγάσει το εργαστήριο Ψηφιακής Εγκληματολογίας θα πρέπει να είναι εξοπλισμένος με τους κατάλληλους φωριαμούς αποθήκευσης ψηφιακών πειστηρίων, οι οποίοι εκτός των άλλων εντάσσονται στη συνολική διαδικασία της «αλυσίδας κυριότητας». Οι φωριαμοί αυτοί δεν πρέπει να είναι εύκολα προσβάσιμοι σε μη εξουσιοδοτημένο προσωπικό. Τα άτομα τα οποία διαθέτουν την αντίστοιχη εξουσιοδότηση θα πρέπει να τηρούνται στον ελάχιστο αναγκαίο αριθμό και να αναφέρονται σε ειδική κατάσταση που θα βρίσκεται αναρτημένη εντός του εργαστηρίου.

Οι συγκεκριμένοι φωριαμοί είναι κατασκευασμένοι από ατσάλι. Συνήθως παρέχουν ασφάλεια στα αποθηκευμένα μέσα από πυρκαγιά και ταξινομούνται σε κατηγορίες ανάλογα με το χρονικό περιθώριο ασφαλείας που παρέχουν στα περιεχόμενα μέχρι να προκληθεί ζημιά από τη φωτιά. Μπορεί να φέρουν αναδιπλούμενη πρόσοψη ώστε να είναι δυνατός ο γρήγορος οπτικός έλεγχος των αποθηκευμένων μέσων. Επίσης το μέγεθός τους ποικίλει αναλόγως των αναγκών, αφού στα φυλασσόμενα μέσα μπορεί να περιλαμβάνονται από φορητά μέσα αποθήκευσης (εξωτερικοί σκληροί δίσκοι, οπτικοί δίσκοι κτλ.) μέχρι ολόκληρες κεντρικές μονάδες και οθόνες.

Εικόνα 4.3 : Φωριαμοί Αποθήκευσης Ψηφιακών Πειστηρίων (Evidence Lockers) (Πηγή: www.montel.com)

Για την εξασφάλιση των φωριαμών δύναται να χρησιμοποιηθούν ειδικά λουκέτα ασφαλείας υψηλής ποιότητας. Η διανομή των κλειδιών θα πρέπει να γίνεται με μεγάλη προσοχή και εάν είναι δυνατόν θα πρέπει να ακολουθούνται οι παρακάτω πρακτικές:

- Ορισμός ενός εκ των μελών του εργαστηρίου ως υπεύθυνου για τη διανομή των κλειδιών.
- Αρίθμηση των εφεδρικών κλειδιών ανά λουκέτο ασφαλείας.
- Τήρηση μητρώου στο οποίο θα φαίνεται ποιο μέλος έχει χρεωθεί κάθε κλειδί.
- Μηνιαίος έλεγχος πληρότητας κλειδιών.
- Χαρακτηρισμός ασφαλείας και χειρισμός των κλειδιών αναλόγως του βαθμού ασφαλείας των περιεχομένων του αντίστοιχου φωριαμού (πχ. τα κλειδιά φωριαμού που περιέχει απόρρητα δεδομένα χειρίζονται επίσης ως απόρρητα).
- Αναλυτική καταγραφή των κλειδιών όταν εναλλάσσονται τα καθήκοντα του υπεύθυνου διανομής.

- Σε περίπτωση που απωλεσθεί κάποιο κλειδί άμεση αντικατάσταση των λουκέτων στα οποία αντιστοιχεί.
- Αλλαγή λουκέτων και κλειδιών ετησίως.

Εφόσον χρησιμοποιείται σύστημα ασφαλείας με συνδυασμό, αυτός θα πρέπει να φυλάσσεται σε διαφορετικό σημείο. Με το που καθορισθεί ο νέος συνδυασμός, κάθε παλαιότερος πρέπει να καταστρέφεται, ενώ μόνο συγκεκριμένα μέλη του προσωπικού του εργαστηρίου πρέπει να έχουν δυνατότητα να αλλάξουν τους συνδυασμούς (πχ. ο επικεφαλής του εργαστηρίου και ένας υπεύθυνος διανομής).

Κάθε φορά που ανοίγει ένας φωριαμός αποθήκευσης ψηφιακών πειστηρίων καταγράφεται η ημερομηνία και η ώρα, το πρόσωπο που τον άνοιξε, το πειστήριο που εισήλθε ή εξήλθε και ο ακριβής λόγος για τον οποίο πραγματοποιήθηκε η ενέργεια. Το εν λόγω μητρώο αποτελεί αντικείμενο ελέγχων και επιθεωρήσεων, ενώ πρέπει να τηρείται για όσα χρόνια προβλέπεται μετά τη συμπλήρωσή του. Σε καμία περίπτωση δεν θα πρέπει να παραμένει ανοικτός ένας φωριαμός αποθήκευσης ψηφιακών πειστηρίων χωρίς την άμεση επίβλεψη από εξουσιοδοτημένο προσωπικό. Επίσης, το περιεχόμενό των φωριαμών θα πρέπει να ελέγχεται συχνά, ώστε να διαπιστώνεται αν τα ψηφιακά πειστήρια που αφορούν σε παλαιότερες διεκπεραιωμένες υποθέσεις έχουν απομακρυνθεί και αν τα αποθηκευμένα αποδεικτικά στοιχεία συμφωνούν με τα αναγραφόμενα στα Έντυπα Ψηφιακών Πειστηρίων, τα οποία επίσης βρίσκονται εντός των φωριαμών. Οι παραπάνω ενέργειες θα πρέπει να προβλέπονται και να περιγράφονται λεπτομερώς στις προδιαγεγραμμένες διαδικασίες λειτουργίας του εργαστηρίου.

4.4.3.4 Συντήρηση Εγκαταστάσεων

Ιδιαίτερη προσοχή θα πρέπει να δίνεται στη συντήρηση του χώρου όπου στεγάζεται το εργαστήριο Ψηφιακής Εγκληματολογίας. Οι ενέργειες αποκατάστασης οποιασδήποτε φθοράς θα πρέπει να είναι άμεσες, ώστε να μειώνεται οποιοσδήποτε κίνδυνος για την υγεία του προσωπικού και να εξασφαλίζεται η απερίσπαστη εκτέλεση των εργασιών μέσα στις κατάλληλες συνθήκες.

Στα πλαίσια της συντήρησης εντάσσονται και οι ενέργειες αποφυγής της εμφάνισης στατικού ηλεκτρισμού. Ο στατικός ηλεκτρισμός αποτελεί σημαντική απειλή για την ακεραιότητα των ψηφιακών δεδομένων εξαιτίας του φαινομένου της Ηλεκτροστατικής Εκφόρτισης. Συνεπακόλουθα, απαιτείται η εξασφάλιση των κατάλληλων μέσων τα οποία θα εξαλείψουν αυτόν τον κίνδυνο. Οι επιφάνειες εργασίας και τα γραφεία πρέπει να επενδύονται με αντιστατικό υλικό, ενώ κατά τη μεταχείριση των φορέων ψηφιακών πειστηρίων το προσωπικό πρέπει να φέρει κατάλληλα γάντια. Παράλληλα, επειδή η σκόνη ευνοεί την παρουσία στατικού ηλεκτρισμού, θα πρέπει τουλάχιστον μια φορά την εβδομάδα να καθαρίζεται το πάτωμα και η μοκέτα του εργαστηρίου, εφόσον υπάρχει. Σε κάθε περίπτωση, η πολιτική λειτουργίας του εργαστηρίου θα πρέπει να προβλέπει την επίβλεψη του

συνεργείου καθαρισμού από προσωπικό του εργαστηρίου κατά τη διάρκεια καθαρισμού του χώρου.

Επίσης πρέπει να τηρούνται δύο διαφορετικοί τύποι κάδων απορριμμάτων, παρόμοια με τα όσα ορίζονται από τους Στρατιωτικούς Κανονισμούς για την απόρριψη απόρρητων εγγράφων και υλικών. Ο ένας τύπος προορίζεται για υλικό (έγγραφα, μέσα αποθήκευσης κτλ.) που δεν σχετίζεται με το εξειδικευμένο έργο του εργαστηρίου, ενώ ο δεύτερος θα αφορά σημεία όπου θα τοποθετούνται στοιχεία τα οποία σχετίζονται με τις έρευνες ενός περιστατικού ασφαλείας και απαιτούν περαιτέρω ενέργειες καταστροφής, ώστε να εξασφαλισθεί ότι καμία διαβαθμισμένη πληροφορία δεν θα μπορεί να συλλεχθεί από αυτά όταν πλέον δεν θα βρίσκονται κάτω από την φύλαξη και άμεση επίβλεψη του προσωπικού του εργαστηρίου.

4.4.3.5 Φυσική Ασφάλεια

Πέραν του επιπέδου ασφαλείας που εξασφαλίζεται λόγω των χαρακτηριστικών της κατασκευής του εργαστηρίου, θα πρέπει να ληφθούν και ορισμένα επιπλέον μέτρα φυσικής ασφαλείας, είτε αναφέρονται στις πολιτικές λειτουργίας είτε όχι.

Σε κάθε περίπτωση θα πρέπει να τηρείται ένα μητρώο εισερχομένων ατόμων στο εργαστήριο, χειρόγραφο ή ηλεκτρονικό, στο οποίο θα αναγράφεται το ονοματεπώνυμο του επισκέπτη, η ημερομηνία και ώρα άφιξης και αναχώρησης, ο λόγος της επίσκεψης καθώς και το όνομα του συνοδού του από το προσωπικό του εργαστηρίου. Κανένα εισερχόμενο άτομο δεν θα πρέπει να παραμένει στους χώρους του εργαστηρίου χωρίς συνοδεία. Επιπρόσθετα, μπορούν να υιοθετηθούν μέτρα άμεσου οπτικού ελέγχου, όπως η υποχρέωση από τον οποιονδήποτε κυκλοφορεί εντός του εργαστηρίου να φέρει σε εμφανές σημείο ένα διακριτικό ιδιότητας (μέλους ή επισκέπτη), όπως τα ήδη χρησιμοποιούμενα στο στρατιωτικό περιβάλλον Δελτία Εισόδου.

Τέλος, εφόσον διατίθεται η ανάλογη υποδομή, οι χώροι του εργαστηρίου θα πρέπει να παρακολουθούνται και από το Κλειστό Κύκλωμα Τηλεόρασης (Closed Circuit TV - CCTV) του Οργανισμού.

4.4.3.6 Διαμόρφωση Χώρου

Η διαμόρφωση του χώρου που θα στεγάσει το εργαστήριο Ψηφιακής Εγκληματολογίας προκύπτει από τους διαθέσιμους οικονομικούς πόρους, τη συνολική διαθέσιμη επιφάνεια και τους σταθμούς εργασίας που απαιτούνται για τη λειτουργία του. Ο αριθμός των σταθμών εργασίας υπολογίζεται με βάση τον αριθμό των περιστατικών ασφαλείας, τα οποία το εργαστήριο θα κληθεί να αντιμετωπίσει. Κατά τη συνήθη πρακτική, ένα εργαστήριο το οποίο θα αναλύσει τα δεδομένα που αφορούν σε δύο με τρία περιστατικά μηνιαίως, μπορεί να καλύψει τις ανάγκες του με ένα Σταθμό Εργασίας Ψηφιακής Εγκληματολογίας.

Τα τηρούμενα στοιχεία Κυβερνοεπιθέσεων και περιστατικών ασφαλείας στο στρατιωτικό περιβάλλον παρουσιάζουν έναν αρκετά μεγαλύτερο αριθμό συμβάντων. Παρόλα αυτά, σε συνδυασμό με τους

περιορισμούς που αφορούν στο εξειδικευμένο προσωπικό το οποίο δύναται αυτή τη στιγμή να επανδρώσει τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας και τις υπάρχουσες εγκαταστάσεις, η πλέον πιθανή πρόταση σχετικά με τον εξοπλισμό ενός εργαστηρίου τη δεδομένη χρονική περίοδο δεν θα μπορούσε να περιλαμβάνει περισσότερους από τρεις έως τέσσερις εξειδικευμένους σταθμούς εργασίας.

Οι Σταθμοί Εργασίας Ψηφιακής Εγκληματολογίας μπορούν να επικοινωνούν μεταξύ τους μέσω ενός αποκλειστικού, για τις ανάγκες του εργαστηρίου, δικτύου και σε κάθε περίπτωση θα πρέπει να είναι απομονωμένοι από τα υπόλοιπα εσωτερικά και εξωτερικά δίκτυα του Οργανισμού, για λόγους εμπιστευτικότητας και ακεραιότητας των δεδομένων που αναλύονται. Ο χώρος εργασίας για κάθε ένα σταθμό μπορεί να διαχωρίζεται με τους υπόλοιπους μέσω πρόσθετων κουβούκλιων. Εκτός των εξειδικευμένων αυτών σταθμών, το εργαστήριο θα πρέπει να διαθέτει τουλάχιστον έναν υπολογιστή με σύνδεση στο Διαδίκτυο για την κάλυψη διάφορων αναγκών, όπως ηλεκτρονικό ταχυδρομείο και ενημέρωση για τρέχοντα θέματα ενδιαφέροντος, και έναν υπολογιστή συνδεδεμένο στο ευρύτερο εσωτερικό δίκτυο του Οργανισμού για εργασίες όπως αρχειοθέτηση και εσωτερική αλληλογραφία.

Σε ότι αφορά στον υπόλοιπο εξοπλισμό του εργαστηρίου, θα πρέπει να υπάρχει χώρος για την τοποθέτηση των φωριαμών αποθήκευσης ψηφιακών πειστηρίων, ώστε αυτοί να βρίσκονται υπό την άμεση επίβλεψη του αρμόδιου προσωπικού. Στην περίπτωση που ο χώρος δεν επαρκεί, οι φωριαμοί θα πρέπει να τοποθετηθούν σε κατάλληλο σημείο εκτός του εργαστηρίου, το οποίο θα πληροί όλες τις απαιτήσεις φυσικής ασφάλειας.

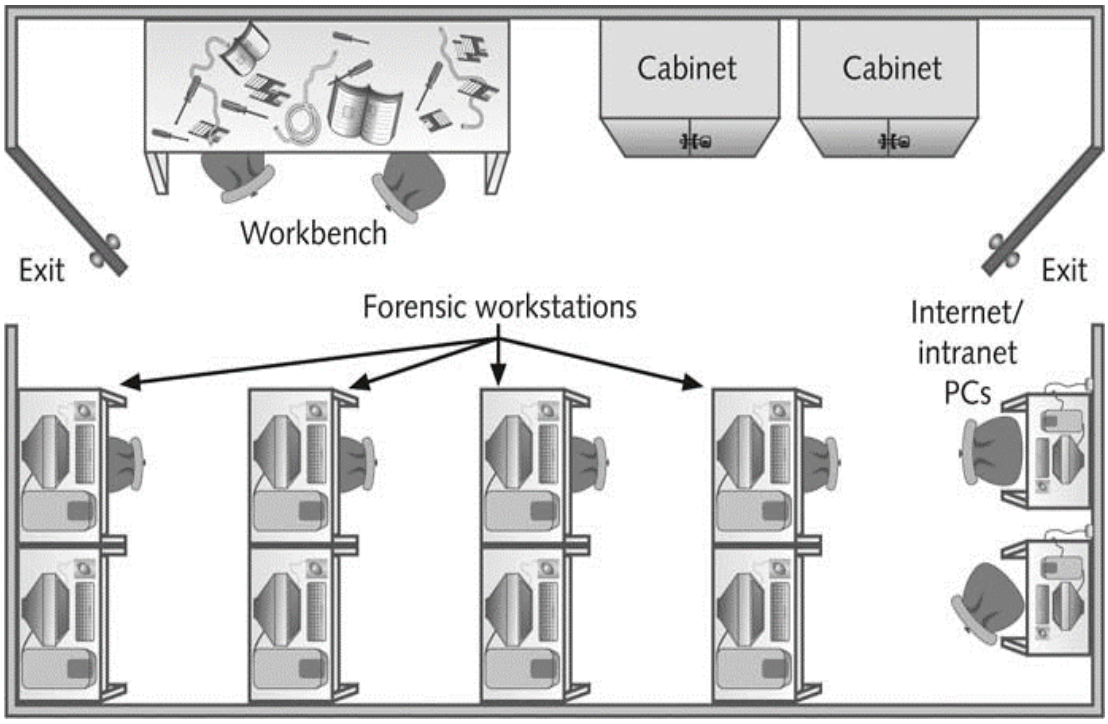
Επίσης, είναι χρήσιμο να εξασφαλιστεί χώρος εντός του εργαστηρίου για την τοποθέτηση ενός πάγκου εργασίας για την εκτέλεση εργασιών όπως η αποσυναρμολόγηση μιας κεντρικής μονάδας που έχει συλλεχθεί ως φορέας ψηφιακών αποδεικτικών στοιχείων ή η καταστροφή ενός ψηφιακού μέσου (πχ. δια θραύσεως). Ο πάγκος, όπως αναφέρθηκε και σε προηγούμενη υποενότητα, θα πρέπει να έχει τις επιφάνειές του καλυμμένες με αντιστατικό υλικό. Παράλληλα, η ύπαρξη μιας βιβλιοθήκης θα λειτουργούσε προς όφελος της συνολικής λειτουργίας του εργαστηρίου, εφόσον εξοπλιζόταν σταδιακά με κατάλληλα για τους σκοπούς συγγράμματα και ενημερωτικό υλικό από εκπαιδεύσεις και τεχνικά σεμινάρια Χρήσιμη θα ήταν και η ύπαρξη αποθηκευτικών χώρων για τα αποθέματα υλικού και λογισμικού.

Στην περίπτωση που οι αναλυτές του εργαστηρίου συμμετέχουν και στις υπόλοιπες διαδικασίες που περιλαμβάνει μια έρευνα σχετικά με ένα περιστατικό ασφαλείας, θα πρέπει να έχει προβλεφθεί χώρος και θέσεις ώστε να μπορεί να λάβει χώρα η εξέταση ενός μάρτυρα ή η ενημέρωση των αρμόδιων προσώπων (πχ. επικεφαλής εργαστηρίου, Διοίκηση κτλ.).

Τέλος, για λόγους ασφαλείας, η πρόσβαση στο εργαστήριο θα πρέπει να μπορεί να γίνει από δύο σημεία. Στην περίπτωση που

το εργαστήριο έχει κατασκευαστεί σύμφωνα με τα πρότυπα TEMPEST, οι δύο είσοδοι θα πρέπει να διαθέτουν δύο πόρτες με ενδιάμεσο κενό χώρο.

Παρακάτω απεικονίζεται η κάτοψη ενός ενδεικτικού εργαστηρίου μεσαίας κλίμακας με τέσσερις Σταθμούς Εργασίας Ψηφιακής Εγκληματολογίας (Forensic workstations), δύο φωριαμούς αποθήκευσης ψηφιακών πειστηρίων (cabinets), έναν πάγκο εργασίας (workbench) και δύο υπολογιστές συνδεδεμένους στο εσωτερικό δίκτυο και το Διαδίκτυο αντίστοιχα (intranet/Internet PCs) [10].



Εικόνα 4.4 : Κάτοψη Εργαστηρίου Ψηφιακής Εγκληματολογίας Μεσαίας Κλίμακας (Πηγή: Nelson B., Guide to Computer Forensics and Investigations, 4th edition)

4.4.4 Σταθμοί Εργασίας Ψηφιακής Εγκληματολογίας (Digital Forensics Workstations)

4.4.4.1 Γενικά

Οι Σταθμοί Εργασίας Ψηφιακής Εγκληματολογίας (Digital Forensics Workstations) αποτελούν το βασικό εργαλείο που χρησιμοποιούν οι αναλυτές του εργαστηρίου Ψηφιακής Εγκληματολογίας για την ανάλυση των ψηφιακών πειστηρίων. Η χρήση του εξειδικευμένου λογισμικού που βρίσκεται εγκατεστημένο στους σταθμούς αυτούς, θα τους επιτρέψει να καταλήξουν στα ευρήματα εκείνα τα οποία θα ενισχύσουν ή θα απορρίψουν κάθε πιθανό σενάριο, ώστε να προκύψει το πιθανότερο ιστορικό του περιστατικού και να εντοπιστούν οι αδυναμίες που επιτρέψανε την εμφάνισή του. Όλα τα παραπάνω, επίσης με τη βοήθεια των σταθμών αυτών, συνοψίζονται σε κατάλληλες αναφορές και συνοδεύουν το αντίστοιχο ψηφιακό υλικό.

Οι συγκεκριμένοι σταθμοί εργασίας δεν αποτελούν εξεζητημένα μηχανήματα που είναι δύσκολο να εντοπιστούν και να προμηθευτούν. Όπως αναφέρθηκε και στην προηγούμενη υποενότητα, τα τεχνικά χαρακτηριστικά τους και το εξειδικευμένο λογισμικό που θα απαιτηθεί προκύπτουν μετά από τον προσδιορισμό των μέσων και των δυνατοτήτων του εργαστηρίου, εκμεταλλευόμενοι το γεγονός ότι το υλικό και το λογισμικό που χρησιμοποιείται σε ένα κλειστό περιβάλλον, όπως το στρατιωτικό, είναι καταγεγραμμένο και ελεγχόμενο. Η πλειονότητα των συστημάτων που λειτουργούν στο εν λόγω περιβάλλον φέρουν Λειτουργικό Σύστημα Windows 7, ενώ υπάρχει και αριθμός μηχανημάτων με Λειτουργικό Σύστημα Windows XP. Εκτός των παραπάνω, ένας αριθμός κεντρικών εξυπηρετητών φέρει διανομές του Λειτουργικού Συστήματος Linux. Η σύνθεση των συστημάτων τα οποία θα κληθεί να ερευνήσει το εργαστήριο καταδεικνύει την ανάγκη να εξασφαλιστούν εργαλεία Ψηφιακής Εγκληματολογίας που θα είναι συμβατά με τα χρησιμοποιούμενα Λειτουργικά Συστήματα. Παράλληλα, για ενέργειες όπως η παραγωγή ψηφιακών αντιγράφων από τα αυθεντικά μέσα αλλά και η ανάλυση φορέων ψηφιακών αποδεικτικών στοιχείων μεγάλης χωρητικότητας, απαιτείται μεγάλη υπολογιστική ισχύς ώστε οι λειτουργίες αυτές να ολοκληρώνονται σε λογικό χρονικό διάστημα και, συνεπακόλουθα, να μην καθυστερούν υπερβολικά οι έρευνες. Η προμήθεια σύγχρονων μηχανημάτων και η συχνή αναβάθμισή τους σύμφωνα με τις τεχνολογικές εξελίξεις αλλά και τις ανάγκες του εργαστηρίου θα διευκολύνει κατά πολύ το έργο των αναλυτών.

Επίσης, μπορεί να ακολουθηθεί και η εναλλακτική λύση της προμήθειας φορητών ηλεκτρονικών υπολογιστών (laptops) ως Σταθμών Εργασίας Ψηφιακής Εγκληματολογίας, αφού πλέον δεν υστερούν τεχνικά από τους αντίστοιχους επιτραπέζιους, ενώ μπορούν να χρησιμοποιηθούν και επιτόπου κατά την πραγματοποίηση των διαδικασιών της Αντιμετώπισης Περιστατικών Ασφαλείας. Παρόλα αυτά θα πρέπει να ληφθεί υπόψη η περιορισμένη δυνατότητα αναβάθμισής τους, η οποία αναπόφευκτα ορίζει μια άτυπη «ημερομηνία λήξης» σε ότι αφορά τη χρησιμοποίησή τους για τους σκοπούς του εργαστηρίου.

Τέλος, ο αριθμός των απαιτούμενων σταθμών εργασίας, όπως περιεγράφηκε παραπάνω, προκύπτει από τα τηρούμενα στοιχεία σχετικά με τον αριθμό των περιστατικών ασφαλείας που ανιχνεύονται μηνιαίως.

4.4.4.2 Τεχνικά Χαρακτηριστικά

Οι κύριες εργασίες για τις οποίες θα χρησιμοποιηθεί ο Σταθμός Εργασίας Ψηφιακής Εγκληματολογίας είναι η παραγωγή ψηφιακών αντιγράφων, η ανάλυση του αντιγράφου «εικόνας» του αυθεντικού μέσου (image copy) και η παραγωγή της αντίστοιχης αναφοράς.

Σε κάθε περίπτωση θα πρέπει να εξασφαλίζεται ότι ο υπολογιστής που θα χρησιμοποιηθεί ως εξειδικευμένος σταθμός εργασίας μπορεί να ανταπεξέλθει σε απαιτητικές, ως προς την κατανάλωση των υπολογιστικών του πόρων, εργασίες, όπως για παράδειγμα η ανάλυση φορέων

ψηφιακών πειστηρίων μεγάλης χωρητικότητας. Επίσης θα πρέπει, σε επίπεδο υλικού, να είναι εξοπλισμένος με όσο το δυνατόν περισσότερες συσκευές και εξαρτήματα τα οποία θα του επιτρέπουν να «διαβάσει» μια ποικιλία ειδών αρχείων και να συνδεθεί με όσο το δυνατόν περισσότερες και διαφορετικές συσκευές. Από τα παραπάνω προκύπτει ότι ο υπολογιστής θα πρέπει να έχει σημαντικές δυνατότητες σε ότι αφορά στην επεξεργαστική του ισχύ, τη μνήμη RAM, την κάρτα γραφικών αλλά και τις κάρτες σύνδεσης με τα διάφορα δίκτυα, ενώ θα πρέπει να φέρει και έναν αριθμό από εξωτερικές θύρες σύνδεσης τύπου USB και FireWire ή θύρες ανάγνωσης εξεζητημένων φορέων αποθήκευσης αρχείων όπως κάρτες μνήμης κινητών τηλεφώνων ή ψηφιακών φωτογραφικών μηχανών (mini και SD cards).

Σε επίπεδο λογισμικού, ο υπολογιστής μπορεί να φέρει οποιοδήποτε Λειτουργικό Σύστημα είναι εξοικειωμένος ο χειριστής του, εκτός και αν ορίζεται διαφορετικά από τις προδιαγεγραμμένες διαδικασίες λειτουργίας του εργαστηρίου. Από εκεί και πέρα, ανάλογα με το Λειτουργικό Σύστημα που θα προτιμηθεί, στο σταθμό εργασίας εγκαθίστανται τα κατάλληλα συμβατά εργαλεία λογισμικού Ψηφιακής Εγκληματολογίας, τα οποία θα καλύψουν το σύνολο των απαιτούμενων λειτουργιών. Αντίθετα με τα Λειτουργικά Συστήματα, όπου πιθανώς να προτιμάται η εργασία με μια συγκεκριμένη έκδοση ή διανομή, στα εξειδικευμένα εργαλεία λογισμικού η δυνατότητα χρησιμοποίησης περισσοτέρων του ενός εργαλείων για την ίδια διαδικασία (πχ. παραγωγή αντιγράφου και σύνοψης) εξασφαλίζει την εξέταση των δεδομένων σε μεγαλύτερο βαθμό και με διαφορετικές προσεγγίσεις, ώστε να αποφευχθεί οποιαδήποτε παράβλεψη. Τα εργαλεία λογισμικού που απαιτείται να εγκατασταθούν σε έναν τέτοιο σταθμό πρέπει πρωτίστως να καλύπτουν τις λειτουργίες συλλογής και ανάλυσης δεδομένων, ενώ εξίσου σημαντική για το έργο των αναλυτών είναι και η εξασφάλιση εργαλείων επεξεργασίας δίσκων (disk editor tools), επεξεργασίας κειμένων (text editor tools) και προβολής αρχείων γραφικών (graphics viewer programs).

Επίσης, κατά την επιλογή Λειτουργικού Συστήματος για τους Σταθμούς Εργασίας Ψηφιακής Εγκληματολογίας, πρέπει να δοθεί προσοχή στα ιδιαίτερα χαρακτηριστικά του όσον αφορά στις εσωτερικές διαδικασίες που λαμβάνουν χώρα κατά την εκκίνηση του συστήματος ή μεταγενέστερα και σχετίζονται με την ακεραιότητα των δεδομένων. Τα Λειτουργικά Συστήματα, κατά την εκκίνησή τους ή μόλις συνδεθεί κάποια εξωτερική συσκευή σε μια από τις θύρες του υπολογιστή (πχ. σύνδεση μέσω θύρας USB συσκευής που περιέχει αντίγραφο «εικόνα» για ανάλυση) εκτελούν αυτόματα διαδικασίες οι οποίες τροποποιούν δεδομένα σε διάφορα σημεία της μνήμης ή της συσκευής. Οι ιδιαιτερότητες αυτές πρέπει να έχουν μελετηθεί και να είναι γνωστές στους αναλυτές του εργαστηρίου, ώστε να προληφθεί το πιθανό ενδεχόμενο αθέμιτης τροποποίησης ή απώλειας των αυθεντικών δεδομένων. Ο παραπάνω σκοπός επιτυγχάνεται με τη χρήση συσκευών ή μεθόδων απαγόρευσης εγγραφής (write blockers). Υπάρχουν διάφοροι τύποι τέτοιων συσκευών οι οποίοι είτε συνδέονται ανάμεσα στο σταθμό εργασίας και το μέσο αποθήκευσης είτε συνδέονται απευθείας σε κάποια θύρα του υπολογιστή (USB ή FireWire). Παράλληλα, υπάρχουν και άλλες ανέξοδες

μέθοδοι με τις οποίες απαγορεύεται η παρέμβαση του Λειτουργικού Συστήματος του Σταθμού Εργασίας Ψηφιακής Εγκληματολογίας. Μια τέτοια μέθοδος περιγράφεται στο Παράρτημα Γ.

Συνοπτικά, τα απαραίτητα τεχνικά χαρακτηριστικά ενός υπολογιστή, σταθερού ή φορητού, ο οποίος θα χρησιμοποιηθεί ως Σταθμός Εργασίας Ψηφιακής Εγκληματολογίας περιλαμβάνουν τα εξής [10]:

- Ηλεκτρονικός Υπολογιστής με Λειτουργικό Σύστημα Windows.
- Συσκευή απαγόρευσης εγγραφής (write blocker).
- Εργαλείο λογισμικού Ψηφιακής Εγκληματολογίας για τη συλλογή δεδομένων (data acquisition tool).
- Εργαλείο λογισμικού Ψηφιακής Εγκληματολογίας για την ανάλυση δεδομένων (data analysis tool).
- Συσκευή αποθήκευσης στην οποία θα αποθηκευτεί το αντίγραφο του αυθεντικού μέσου ή πρωτεύοντος αντιγράφου.
- Επιπλέον θύρες τύπου SATA ή PATA.
- Θύρες τύπου USB.

Επιπλέον χαρακτηριστικά που μπορεί να φανούν χρήσιμα περιλαμβάνουν:

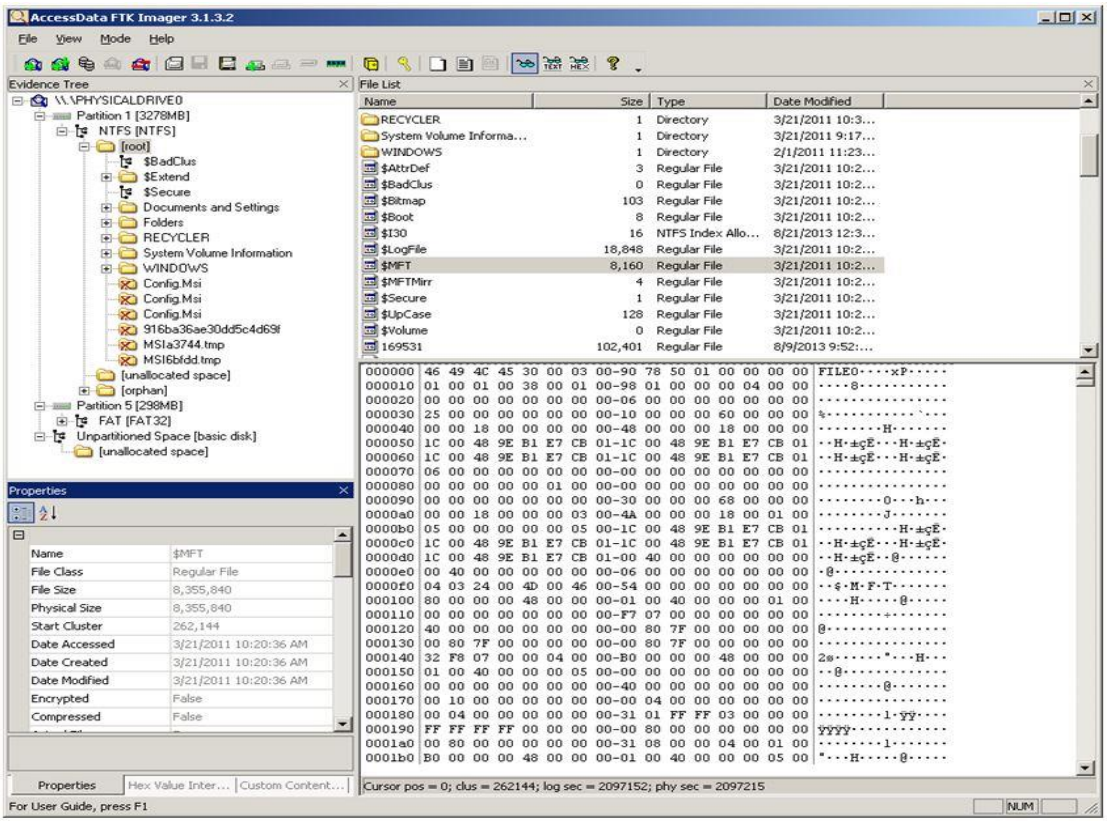
- Κάρτα διασύνδεσης δικτύου (network interface card – NIC).
- Θύρα τύπου FireWire.
- Κάρτα διασύνδεσης τύπου SCSI.
- Εργαλείο επεξεργασίας δίσκων (disk editor tool).
- Εργαλείο επεξεργασίας κειμένων (text editor tool).
- Εργαλείο προβολής αρχείων γραφικών (graphics viewer programs).
- Λοιπά εξειδικευμένα εργαλεία προβολής αρχείων διαφόρων τύπων.

4.4.4.3 Εργαλεία Λογισμικού

Για την κάλυψη των αναγκών που σχετίζονται με το εξειδικευμένο λογισμικό Ψηφιακής Εγκληματολογίας κυκλοφορούν πολλά προϊόντα δωρεάν και επί πληρωμής. Η οικονομική κατάσταση η οποία χαρακτηρίζει τη στρατιωτική αλλά και τη γενικότερη πραγματικότητα επιβάλλει τη στροφή κυρίως στα «ελεύθερα» εργαλεία παρά το γεγονός ότι οι δωρεάν εκδόσεις δεν παρέχουν όλες τις διαθέσιμες δυνατότητες. Σε κάθε περίπτωση θα πρέπει να γίνει προσεκτική επιλογή των εργαλείων που θα εγκατασταθούν στους Σταθμούς Εργασίας Ψηφιακής Εγκληματολογίας, ώστε να χρησιμοποιούνται αυτά που τυγχάνουν της γενικότερης αποδοχής από ίδιου σκοπού υπηρεσίες και ιδρύματα, έχουν υποβληθεί σε ανάλογους ελέγχους από τους κατάλληλους φορείς και τελικά εξασφαλίζουν ότι τα αποτελέσματα που παράγουν μετά την ανάλυση των ψηφιακών πειστηρίων θα είναι ακέραια και αδιαμφισβήτητα.

Όσον αφορά στα εργαλεία συλλογής δεδομένων, δύο ευρέως διαδεδομένα δωρεάν εργαλεία είναι το **Forensic Tool Kit (FTK) Imager** της AccessData και η εντολή Linux "**dcfldd**".

Το FTK Imager είναι ένα εργαλείο προβολής περιεχομένων και παραγωγής αντιγράφων «εικόνας» ενός ψηφιακού μέσου αποθήκευσης (πχ. σκληρού δίσκου, οπτικού δίσκου κτλ.). Έχει τη δυνατότητα παραγωγής και εξαγωγής του αντιγράφου σε μια εξωτερική συσκευή αποθήκευσης, προβολής όλων των περιεχομένων του μέσου, ανάκτησης διαγραμμένων αρχείων εφόσον η μνήμη που απασχολούσαν δεν έχει επανεγγραφεί και παραγωγής σύνοψης μέσω των αλγορίθμων MD5 και SHA1.

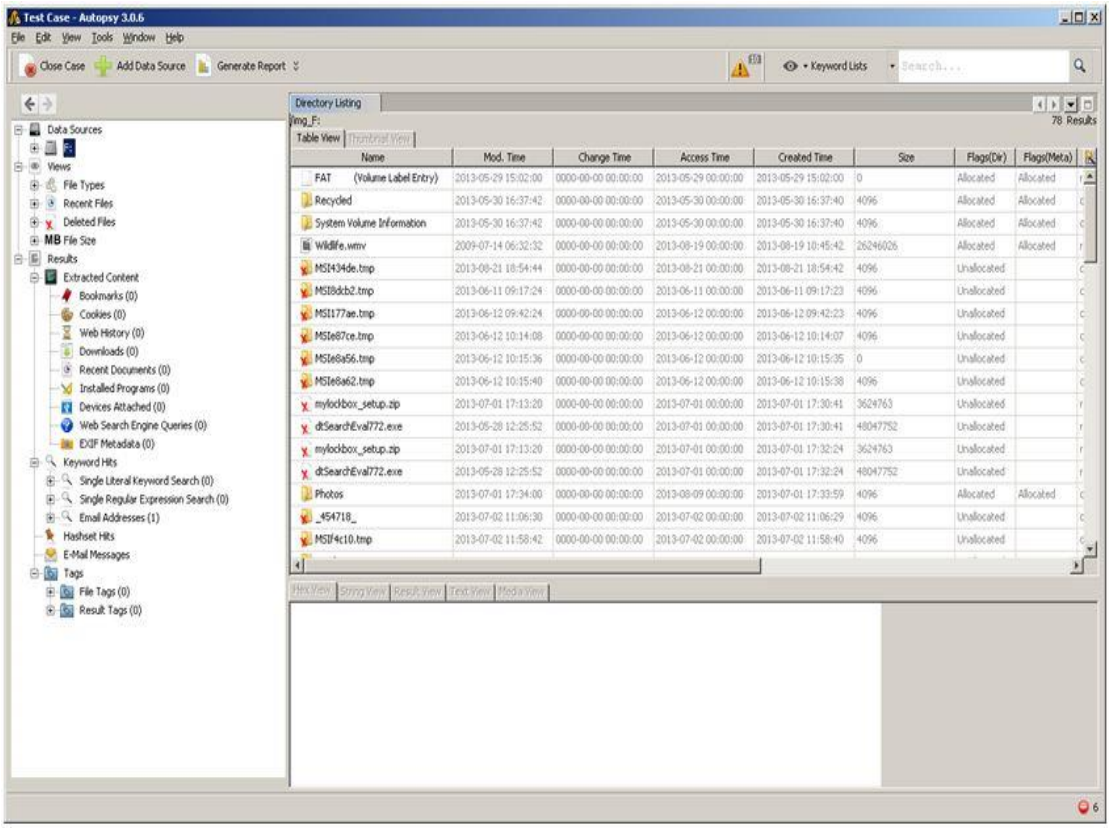


Εικόνα 4.5 : AccessData FTK Imager (Πηγή: www.accessdata.com)

Η εντολή "dcfldd" αποτελεί μια βελτιωμένη έκδοση της αρχικής εντολής παραγωγής ψηφιακών αντιγράφων "dd" του Λειτουργικού Συστήματος Linux από το Εργαστήριο Εγκληματολογίας Υπολογιστών του Υπουργείου Άμυνας των Η.Π.Α (Defense Computer Forensics Lab – dcfl). Η αρχική εντολή ενισχύθηκε για να καλύπτει περισσότερες λειτουργίες σχετικά με τη Ψηφιακή Εγκληματολογία, αφού πέραν της παραγωγής αντιγράφου εκτελεί ενέργειες σύνοψης ταυτόχρονα με τη μετάδοση των δεδομένων (on-the-fly hashing), επιβεβαίωσης της ακεραιότητας του αντιγράφου ως προς το αυθεντικό μέσο, εξαγωγής του αντιγράφου σε περισσότερα του ενός μέσα και διαίρεσή του σε περισσότερα του ενός τμήματα. Η εντολή "dcfldd" κυκλοφορεί και με τη μορφή εκτελέσιμου αρχείου για το περιβάλλον του Λειτουργικού Συστήματος Windows.

Για την ανάλυση των αντιγράφων που παράχθηκαν με τα παραπάνω εργαλεία μπορούν να χρησιμοποιηθούν αντίστοιχα «ελεύθερα» λογισμικά ανάλυσης δεδομένων, όπως το **Sleuth Kit Autopsy** και το **Pro Discover Basic** της Technology Pathways.

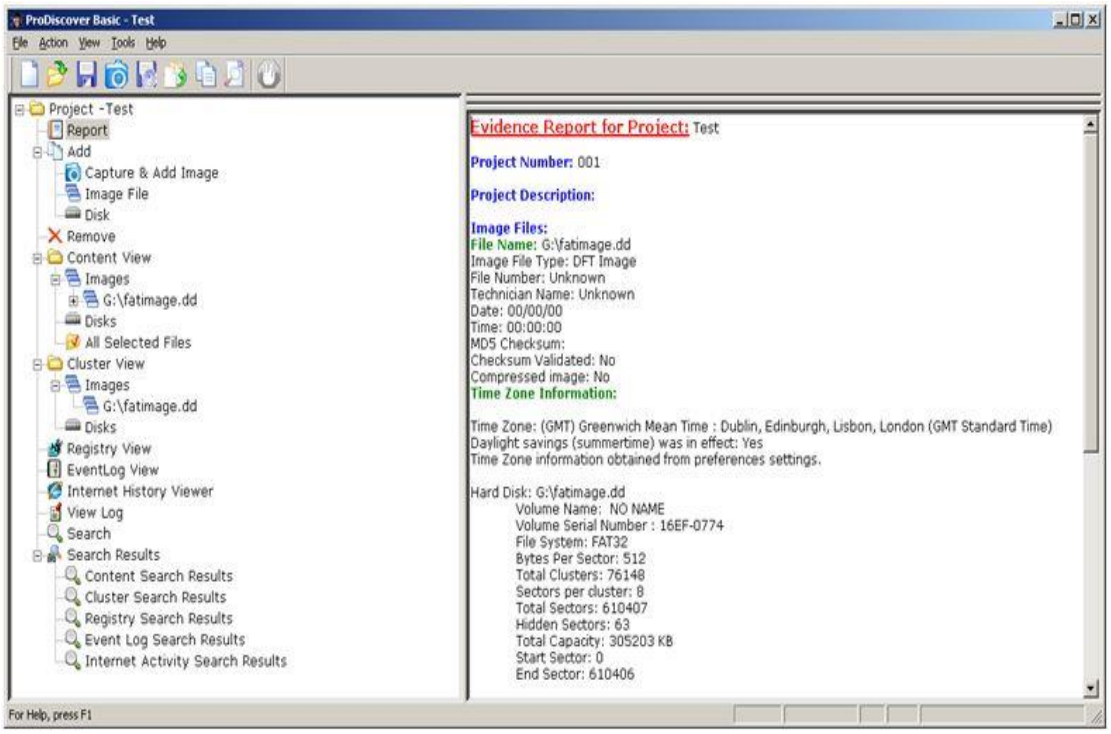
Το Autopsy αφορά στη γραφική διεπαφή χρήστη (Graphical User Interface – GUI) των εντολών του Sleuth Kit και κάποιων άλλων εργαλείων Ψηφιακής Εγκληματολογίας. Συνοδεύεται από λειτουργίες όπως η Ανάλυση Ιστορικού (Timeline Analysis), Ανάλυση Συστήματος Αρχείων (File System Analysis) και Αναζήτησης μέσω Λέξης-Κλειδιού (Keyword Searching), με δυνατότητα προσθήκης και νέων εντολών. Χρησιμοποιείται ευρέως από αστυνομικές και στρατιωτικές υπηρεσίες καθώς και από ιδιωτικούς φορείς που δραστηριοποιούνται στο χώρο. Κατά την εκκίνησή του απαιτεί την είσοδο ενός αντιγράφου «εικόνας» και στη συνέχεια, αναλόγως των προτιμήσεων, εκτελεί τις επιμέρους αναλύσεις.



Εικόνα 4.6 : Sleuth Kit Autopsy (Πηγή: www.sleuthkit.org/autopsy)

Το εργαλείο Pro Discover Basic της Technology Pathways μπορεί να χρησιμοποιηθεί τόσο ως εργαλείο συλλογής όσο και ως εργαλείο ανάλυσης ενός φορέα ψηφιακών πειστηρίων. Μετά την είσοδο ενός αντιγράφου στο λογισμικό, παρέχεται η δυνατότητα στον αναλυτή να ελέγξει τα δεδομένα βάσει του περιεχομένου τους αλλά και ανάλογα με τους τομείς (clusters) του δίσκου που καταλαμβάνουν. Όπως και το Autopsy, επιτρέπει την

εύρεση σημείων ενδιαφέροντος στα δεδομένα μέσω αναζήτησης λέξεων-κλειδιών και άλλων κριτηρίων.



Εικόνα 4.7 : Pro Discover Basic (Πηγή: www.arcgroupny.com)

Εκτός των εξειδικευμένων για τους σκοπούς της Ψηφιακής Εγκληματολογίας εργαλείων, στους σταθμούς εργασίας του εργαστηρίου πρέπει να εγκατασταθούν και άλλα λογισμικά τα οποία θα φανούν χρήσιμα κατά την ανάλυση των ψηφιακών αποδεικτικών στοιχείων. Παρόλο που η σύνθεση των συστημάτων που λειτουργούν στο στρατιωτικό περιβάλλον είναι γνωστή και καταγεγραμμένη, τα περιστατικά ασφαλείας μπορεί να προέρχονται από εξωτερικές πηγές, επεκτείνοντας με αυτόν τον τρόπο το εύρος των χρησιμοποιούμενων μέσων. Έτσι, για την εξέταση των συνηθέστερων φορέων επιθέσεων, όπως τα αρχεία κειμένου και εικόνας, μέσω των οποίων οι κακόβουλοι επιχειρούν να εισέλθουν στα συστήματα που έχουν στοχοποιήσει, απαιτείται η ύπαρξη ποικιλίας προγραμμάτων που μπορούν να τα προβάλλουν αλλά και να παρέχουν στον ερευνητή πληροφορίες για τις κεφαλίδες (headers) και τα μεταδεδομένα τους. Όσον αφορά τα αρχεία κειμένου, εκτός του συνηθέστερου πακέτου του Microsoft Office, θα πρέπει να υπάρχει τουλάχιστον άλλη μια σουίτα αντίστοιχων εφαρμογών όπως το OpenOffice, αλλά και ένα εργαλείο για την δεκαεξαδική ανάλυση του αρχείου σε χαμηλό επίπεδο όπως το **WinHex** της X-Ways Software. Για τα αρχεία εικόνας υπάρχουν εργαλεία τα οποία δεν περιορίζονται μόνο στην προβολή του αντικειμένου αλλά παρουσιάζουν και μεταδεδομένα τα οποία σχετίζονται με την τοποθεσία που λήφθηκε η φωτογραφία, την ημερομηνία και ώρα που πραγματοποιήθηκε η λήψη καθώς και το μοντέλο της ψηφιακής φωτογραφικής μηχανής (Exchangeable Image File data - EXIF data). Το **Exif Viewer** είναι ένα

τέτοιο εργαλείο, ενώ ο ίδιος σκοπός επιτυγχάνεται επίσης με τα εργαλεία που αναφέρθηκε ότι πραγματοποιούν δεκαεξαδική ανάλυση των αρχείων (WinHex).

Τέλος, ιδιαίτερα χρήσιμη είναι η τήρηση στο εργαστήριο ενός αποθέματος παλαιότερων Λειτουργικών Συστημάτων και εφαρμογών. Στην περίπτωση που ένα περιστατικό ασφαλείας οφείλεται σε κακόβουλες ενέργειες εκτός του παρακολουθούμενου περιβάλλοντος, γίνεται κατανοητό ότι ο επιτιθέμενος μπορεί να χρησιμοποιεί έναν υπολογιστή με εντελώς διαφορετικά τεχνικά χαρακτηριστικά από αυτά που φέρουν τα Πληροφοριακά Συστήματα που υποστηρίζονται. Παρόλο που τα σύγχρονα εργαλεία Ψηφιακής Εγκληματολογίας μπορούν να «διαβάσουν» και να προβάλλουν την πλειοψηφία των αρχείων που έχουν δημιουργηθεί από τις ευρέως χρησιμοποιούμενες εφαρμογές, δεν συμβαίνει το ίδιο με αρχεία που παράχθηκαν από παλαιότερα λογισμικά. Αντίστοιχα, η διαδικασία της αντίστροφης ανάλυσης του κώδικα ενός επικίνδυνου αρχείου για να διαπιστωθεί ο τρόπος λειτουργίας του (reverse engineering), μπορεί να παρουσιάζει δυσχέρειες εφόσον έχει συγγραφεί σε παλαιότερες και ελάχιστα χρησιμοποιούμενες εκδόσεις των διάφορων Γλωσσών Προγραμματισμού. Επικουρικά, εκτός των αποθεμάτων παλαιότερου λογισμικού, το προσωπικό του εργαστηρίου θα πρέπει να παρακολουθεί διαδικτυακά και, εφόσον είναι δυνατόν, να επικοινωνεί με τις λεγόμενες Ομάδες Ειδικών Ενδιαφερόντων (Special Interest Groups – SIGs), οι οποίες διαθέτουν εξειδικευμένες γνώσεις για παλαιότερες τεχνολογίες και να ζητά τη συνδρομή τους σε θέματα που σχετίζονται με το συγκεκριμένο κάθε φορά πεδίο.

4.4.5 Επιχειρησιακή Συνέχεια

Μέχρι αυτό το σημείο έχει γίνει η περιγραφή όλων των απαραίτητων χαρακτηριστικών και προδιαγραφών που πρέπει να πληροί τόσο ο χώρος που θα στεγάσει το εργαστήριο Ψηφιακής Εγκληματολογίας όσο και οι εξειδικευμένοι σταθμοί εργασίας που θα χρησιμοποιηθούν ως το κύριο εργαλείο για την ανάλυση των ψηφιακών πειστηρίων, ώστε να εξασφαλιστεί η ομαλή έναρξη λειτουργίας της συγκεκριμένης υποδομής. Το αμέσως επόμενο μέλημα του επικεφαλής του εργαστηρίου, αλλά και του συνόλου του προσωπικού, είναι να εξασφαλίσουν την επιχειρησιακή συνέχεια της λειτουργίας του εργαστηρίου μετά από οποιαδήποτε πιθανή «καταστροφή».

Ένας από τους κυριότερους λόγους που μπορεί να προκαλέσουν τη μερική ή ολική διακοπή της λειτουργίας του εργαστηρίου Ψηφιακής Εγκληματολογίας είναι τα ακραία φυσικά φαινόμενα (πχ. πλημμύρες, πυρκαγιές, κεραυνοί κτλ.). Το αποτέλεσμα της εμφάνισής τους μπορεί να είναι είτε η πτώση τάσης στις εγκαταστάσεις είτε η άμεση καταστροφή των υποδομών και των δεδομένων. Προβλήματα μπορεί να προκληθούν επίσης από μεταβολές στην παροχή ηλεκτρικού ρεύματος, χωρίς αυτές να οφείλονται σε φυσικά φαινόμενα και εφόσον δεν έχουν ληφθεί τα απαραίτητα μέτρα ασφάλειας, όπως η εξασφάλιση όλων των Πληροφοριακών Συστημάτων με συσκευές Παροχής Αδιάλειπτης Ισχύος (Uninterruptable Power Supply – UPS). Εκτός των παραπάνω, η ομαλή λειτουργία του εργαστηρίου μπορεί να διαταραχθεί από μηχανικά προβλήματα και αστοχίες σε υλικά, όπως για

παράδειγμα η αστοχία ενός σκληρού δίσκου. Τέλος υπάρχει η πιθανότητα να προκληθεί πρόβλημα στους εξειδικευμένους σταθμούς εργασίας στα πλαίσια της διαδικασιών ανάλυσης ενός ψηφιακού πειστηρίου. Για παράδειγμα, κατά τη διάρκεια της εξέτασης του αντιγράφου «εικόνας» του σκληρού δίσκου ενός συστήματος που προσβλήθηκε από έναν ιό, υπάρχει περίπτωση ο ίδιος ιός να μολύνει και το Σταθμό Εργασίας Ψηφιακής Εγκληματολογίας, καθιστώντας τον εκτός λειτουργίας και στερώντας έτσι ένα σημαντικό πόρο από τη λειτουργία του εργαστηρίου.

Το εργαστήριο Ψηφιακής Εγκληματολογίας θα πρέπει να ενταχθεί στο συνολικό Σχέδιο Επιχειρησιακής Συνέχειας του Οργανισμού, εφόσον υπάρχει, και παράλληλα να προβλέψει στην πολιτική λειτουργίας του και τις προδιαγεγραμμένες διαδικασίες κάποιες ιδιαίτερες ενέργειες για την εξασφάλιση της συνέχειας της λειτουργίας του μετά από κάποιο περιστατικό.

Αρχικά θα πρέπει να καθορισθεί η πολιτική σχετικά με τη λήψη και τήρηση των αντιγράφων ασφαλείας (backup policy) των συστημάτων του εργαστηρίου, εφόσον η εν λόγω διαδικασία δεν έχει ενταχθεί στη γενικότερη πολιτική αντιγράφων ασφαλείας του Οργανισμού. Ένα γενικό μέτρο μπορεί να περιλαμβάνει τη λήψη αντιγράφων ασφαλείας από όλα τα μηχανήματα του εργαστηρίου μια φορά την εβδομάδα. Τα συγκεκριμένα αντίγραφα θα πρέπει να αποθηκεύονται σε δύο τοποθεσίες, μια κοντά στην υποδομή, ώστε να είναι δυνατή η άμεση αποκατάσταση των συστημάτων, και μια εναλλακτική μακριά από το εργαστήριο, ώστε να υπάρχει μικρή πιθανότητα να προσβληθεί από την ίδια απειλή (πχ. πτώση τάσης σε μια ευρεία περιοχή). Η επικαιροποίηση των αντιγράφων ασφαλείας και στις δύο τοποθεσίες θα πρέπει να γίνεται σε προκαθορισμένα τακτά χρονικά διαστήματα. Παράλληλα, θα πρέπει να περιγράφεται επακριβώς και η διαδικασία αποκατάστασης ενός Σταθμού Εργασίας Ψηφιακής Εγκληματολογίας μετά τη διακοπή της κανονικής του λειτουργίας (πχ. λόγω της μόλυνσής του κατά την ανάλυση ενός ιού), με τη χρήση των αντιγράφων ασφαλείας.

Σε αντιστοιχία με την παραπάνω διαδικασία, στο Σχέδιο Επιχειρησιακής Συνέχειας του εργαστηρίου πρέπει να περιγράφεται η διαδικασία μετάπτωσης των σταθμών εργασίας σε διάφορες καταστάσεις αναλόγως του περιστατικού που αναλύεται. Πιο συγκεκριμένα, και λόγω των περιορισμένων οικονομικών δυνατοτήτων που αναφέρθηκαν, το εργαστήριο Ψηφιακής Εγκληματολογίας μπορεί να μην διαθέτει τους αντίστοιχους πόρους για τον εξοπλισμό του με επαρκείς και κατάλληλους σταθμούς εργασίας για την ανάλυση διαφορετικών περιστατικών ασφαλείας, με αποτέλεσμα να μην είναι δυνατή η απρόσκοπτη λειτουργία του. Ένα σύστημα μπορεί να απαιτηθεί να χρησιμοποιηθεί για την εξέταση δύο εντελώς διαφορετικών περιστατικών αλλά οι δυνατότητές του (πχ. η διαθέσιμη χωρητικότητα) να μην επιτρέπουν την εγκατάσταση του απαραίτητου λογισμικού. Η δημιουργία εικονικών μέσων (image disks) που θα περιλαμβάνουν το κατάλληλο Λειτουργικό Σύστημα με τα αντίστοιχα εργαλεία Ψηφιακής Εγκληματολογίας αναλόγως του περιστατικού εξασφαλίζει τη δυνατότητα άμεσης μεταβολής των δυνατοτήτων των διαθέσιμων μηχανημάτων ώστε να ανταποκρίνονται στις τρέχουσες ανάγκες.

Τέλος, για την αποκατάσταση των μηχανημάτων του εργαστηρίου στην ίδια κατάσταση με αυτή που βρίσκονταν πριν τη διακοπή της λειτουργίας τους, πρέπει να τηρείται από το προσωπικό ένα μητρώο στο οποίο να καταγράφονται όλες οι τρέχουσες εκδόσεις του συνόλου του λογισμικού σε κάθε χρονική στιγμή. Με τον τρόπο αυτό, στην περίπτωση που δεν υπάρχουν αποθηκευμένα επικαιροποιημένα εικονικά μέσα που να μπορούν να χρησιμοποιηθούν για την ενέργεια αυτή, εξασφαλίζεται ότι η διαδικασία ανάκαμψης, παρά το γεγονός ότι θα είναι πιο επίπονη, θα καταλήξει στην τελευταία λειτουργική κατάσταση των συστημάτων.

4.4.6 Διαπίστευση

4.4.6.1 Η Ανάγκη για Διαπίστευση

Σύμφωνα με τα όσα έχουν αναφερθεί μέχρι αυτό το σημείο προκύπτει πως το έργο του εργαστηρίου Ψηφιακής Εγκληματολογίας, σε γενικές γραμμές, περιλαμβάνει την εφαρμογή εξειδικευμένων επιστημονικών τεχνικών και μεθόδων για τη συλλογή, ανάκτηση και ανάλυση ψηφιακών δεδομένων που έχουν χαρακτηριστεί ως πειστήρια, από τα οποία θα προκύψουν ευρήματα που μπορεί να χρησιμοποιηθούν σε πειθαρχικές ή δικαστικές διαδικασίες. Τα ψηφιακά δεδομένα δεν είναι δυνατόν να γίνουν αντιληπτά με το ανθρώπινο μάτι σε αντίθεση με την αναπαράστασή τους, η οποία μπορεί να αντιστοιχίζεται σε μια φωτογραφία ή έναν αριθμό. Για το λόγο αυτό θα πρέπει να μεταχειρίζονται όπως κάθε φυσικό αντικείμενο που μπορεί να γίνει αντιληπτό με τις ανθρώπινες αισθήσεις και σύμφωνα με τα όσα προβλέπονται από το νόμο σχετικά με αντικείμενα τα οποία έχουν χαρακτηριστεί ως «πειστήρια» για τις έρευνες που σχετίζονται με ένα περιστατικό.

Οι συνεχείς εξελίξεις στον τομέα της Ψηφιακής Εγκληματολογίας έχουν σαν αποτέλεσμα την ύπαρξη πολλών και διαφορετικών μεθόδων και εργαλείων με τα οποία μπορεί να πραγματοποιηθεί το έργο ενός αντίστοιχου εργαστηρίου. Το παραπάνω γεγονός, όμως, θέτει ταυτόχρονα εύλογες αμφιβολίες και προβληματισμούς κατά τη διάρκεια των δικαστικών λειτουργιών, σχετικά με την αποδοχή των ευρημάτων που προέκυψαν ως νόμιμων αποδεικτικών στοιχείων και τη χρησιμοποίησή τους στις εν λόγω λειτουργίες. Τα ευρήματα θα πρέπει να είναι ακριβή, αξιόπιστα και επαναλήψιμα, ενώ υπάρχει περίπτωση ο αναλυτής που τα εξήγαγε να κληθεί να καταθέσει ενώπιων του δικαστηρίου σχετικά με τη διαδικασία που ακολούθησε και τα αποτελέσματα στα οποία κατέληξε, με την κατάθεσή του να είναι εξαιρετικά κρίσιμη για τη διαμόρφωση της τελικής απόφασης. Στη συγκεκριμένη περίπτωση, τόσο το ακροατήριο όσο και οι άμεσοι συμμετέχοντες σε μια δικαστική λειτουργία, πιθανώς να μην διαθέτουν την αντίστοιχη τεχνική κατάρτιση ώστε να αντιληφθούν το σύνολο της κατάθεσης ενός εξειδικευμένου αναλυτή, με αποτέλεσμα να αμφισβητήσουν την ακρίβεια και αξιοπιστία των μεθόδων που ακολουθήθηκαν αλλά και του ίδιου του αναλυτή, προκειμένου να επιτύχουν την απόρριψη των ευρημάτων από τη συνέχεια της διαδικασίας.

Για να εξασφαλιστεί η εγκυρότητα των αποτελεσμάτων και η αξιοπιστία του εργαστηρίου και των αναλυτών του σε ανάλογες περιπτώσεις, απαιτείται η υιοθέτηση ενός Συστήματος Διαχείρισης Ποιότητας, το οποίο ενδεικτικά θα πρέπει να περιλαμβάνει:

- Καταγεγραμμένες πολιτικές λειτουργίας και διαδικασίες για την αναγνώριση, συλλογή, φύλαξη και προστασία των πειστηρίων από πιθανή απώλεια, τροποποίηση ή διαγραφή.
- Καταγεγραμμένες και ελεγμένες, ως προς την απόδοσή τους, τεχνικές διαδικασίες ανάλυσης των ψηφιακών δεδομένων.
- Καθορισμό του απαιτούμενου επιπέδου γνώσεων και των λοιπών επαγγελματικών κριτηρίων που πρέπει να πληροί το προσωπικό που θα στελεχώσει το εργαστήριο.
- Εξασφάλιση της συνέπειας στην υλοποίηση των καταγεγραμμένων καλών πρακτικών και μεθόδων.
- Τήρηση των κατάλληλων προτύπων και ελέγχων κατά τη διάρκεια των εργασιών.
- Καταγεγραμμένα προγράμματα εκπαίδευσης και κατάρτισης του προσωπικού.
- Συμμετοχή κάθε αναλυτή ξεχωριστά σε περιοδικούς ελέγχους της κατάρτισης και των ικανοτήτων του και έλεγχος της αποδοτικότητας του εργαστηρίου συνολικά.
- Συμμετοχή του εργαστηρίου σε διαδικασίες διαπίστευσης από αρμόδιους ανεξάρτητους φορείς.

Όσον αφορά στη διαπίστευση ενός εργαστηρίου, η συγκεκριμένη διαδικασία είναι ιδιαίτερα σημαντική, καθώς αποτελεί την επίσημη αναγνώριση ότι ένα εργαστήριο είναι ικανό να εκτελεί ορισμένες διακριβώσεις και δοκιμές. Στην περίπτωση ενός εργαστηρίου Ψηφιακής Εγκληματολογίας, καθορίζονται τα απαραίτητα κριτήρια που πρέπει να πληρούνται ώστε να εξασφαλίζεται το κατάλληλο επίπεδο αξιοπιστίας σχετικά με τις μεθόδους που χρησιμοποιήθηκαν και τα αποτελέσματα που προέκυψαν. Ενδεικτικά της σπουδαιότητας που έχει η συμμετοχή ενός εργαστηρίου σε διαδικασίες διαπίστευσης είναι τα όσα αναφέρονται στην αναφορά έτους 2009 της Εθνικής Ακαδημίας Επιστημών των Η.Π.Α. [6]. Πιο συγκεκριμένα, στην έβδομη πρόταση διατυπώνονται τα εξής: «*Η διαπίστευση των εργαστηρίων και η πιστοποίηση καθενός του προσωπικού ξεχωριστά θα πρέπει να είναι υποχρεωτική και όλοι οι επαγγελματίες της επιστήμης της Εγκληματολογίας θα πρέπει να έχουν πρόσβαση σε διαδικασίες πιστοποίησης. Στον καθορισμό των απαραίτητων προτύπων για τις διαδικασίες διαπίστευσης και πιστοποίησης, το Εθνικό Ινστιτούτο Εγκληματολογικής Επιστήμης θα πρέπει να λάβει υπόψη του καθορισμένα και διεθνώς αναγνωρισμένα πρότυπα, όπως αυτά που δημοσιεύονται από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization (ISO)). Σε κανένα άτομο δεν θα πρέπει να επιτρέπεται να εφαρμόζει τις Αρχές της Εγκληματολογικής Επιστήμης ή να καταθέτει ως Ειδικός της Εγκληματολογικής Επιστήμης χωρίς να είναι πιστοποιημένος. Οι απαιτήσεις πιστοποίησης θα πρέπει να περιλαμβάνουν κατ'*

ελάχιστον γραπτές δοκιμασίες, πρακτική υπό επίβλεψη, ελέγχους κατάρτισης, διαρκής εκπαίδευση, διαδικασίες επαναπιστοποίησης, συμμόρφωση σε έναν κώδικα ηθικής και αποτελεσματικές πειθαρχικές διαδικασίες. Όλα τα εργαστήρια και οι υποδομές (δημόσιες και ιδιωτικές) πρέπει να διαπιστευτούν και όλοι οι επαγγελματίες της Εγκληματολογικής Επιστήμης πρέπει να πιστοποιηθούν, όπου υπάρχει η αντίστοιχη υποχρέωση, μέσα στο καθορισμένο από το Εθνικό Ινστιτούτο Εγκληματολογικής Επιστήμης χρονικό διάστημα».

Στον ελληνικό χώρο η διενέργεια των ανάλογων επιθεωρήσεων και ελέγχων για τη διαπίστευση ότι ένα εργαστήριο έχει τις τεχνικές και διοικητικές ικανότητες να διεξάγει συγκεκριμένες δοκιμές, μετρήσεις και διακριβώσεις σύμφωνα με συγκεκριμένες πρότυπες ή ενδοεργαστηριακές μεθόδους, με συγκεκριμένο εξοπλισμό και εντός συγκεκριμένων και δηλωμένων ορίων ακριβείας πραγματοποιείται είτε από το Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.) είτε από άλλους ανεξάρτητους επίσημους φορείς σύμφωνα με το πρότυπο ISO 17025:2005.

4.4.6.2 Πρότυπο ISO 17025:2005

Το πρότυπο ISO 17025:2005 του Διεθνούς Οργανισμού Τυποποίησης (International Organization for Standardization - ISO) με τίτλο «*Γενικές απαιτήσεις για την ικανότητα των εργαστηρίων δοκιμών και διακριβώσεων*» [3] καθορίζει, όπως αναφέρεται και στην ονομασία του, τις γενικές απαιτήσεις που πρέπει να πληρούν οι υποδομές εργαστηρίων ανεξαρτήτως εξειδίκευσης, οι οποίες διεξάγουν δοκιμές και διακριβώσεις, συμπεριλαμβανομένων και των δειγματοληψιών, ώστε να χαρακτηριστούν ικανές και επαρκείς. Το πρότυπο καλύπτει τις διαδικασίες που πραγματοποιούνται σε αυτές τις υποδομές και ακολουθούν είτε τις αναγνωρισμένες και προκαθορισμένες μεθόδους είτε τις εξειδικευμένες πρακτικές του εκάστοτε εργαστηρίου. Αφορά όλα τα εργαστήρια τα οποία διεξάγουν δοκιμές και διακριβώσεις, είτε πρόκειται για εσωτερικές υποδομές ενός μεγαλύτερου Οργανισμού είτε για ανεξάρτητους φορείς.

Το πρότυπο αρχικά έφερε την ονομασία ISO/IEC Guide 25 (International Electrotechnical Commission – IEC). Το 1999 εκδόθηκε η πρώτη έκδοση του προτύπου με την ονομασία ISO 17025 από το Διεθνή Οργανισμό Τυποποίησης. Το συγκεκριμένο πρότυπο παρουσιάζει πολλές ομοιότητες με το αντίστοιχο ISO 9000 που αφορά στη Διαχείριση Ποιότητας, με τη διαφορά ότι απευθύνεται στους Οργανισμούς εκείνους οι οποίοι παράγουν αποτελέσματα κατόπιν δοκιμών και διακριβώσεων και εστιάζει στις απαιτήσεις που εξασφαλίζουν την επάρκεια και την ικανότητα τους. Η δεύτερη έκδοση του προτύπου δημοσιεύτηκε το 2005, ώστε να εναρμονίζεται με τις επικαιροποιημένες απαιτήσεις σχετικά με τα Συστήματα Διαχείρισης Ποιότητας, όπως αυτές περιλαμβάνονται στο πρότυπο ISO 9001:2000, εστιάζοντας στις υποχρεώσεις της Διοίκησης και τονίζοντας την υποχρέωση για συνεχή βελτίωση του συστήματος συνολικά.

Οι ενότητες που περιλαμβάνει το πρότυπο ISO 17025 είναι οι εξής πέντε: Αντικείμενο, Τυποποιητικές Παραπομπές, Όροι και Ορισμοί, Απαιτήσεις για τη Διοίκηση και Τεχνικές Απαιτήσεις, με τις δύο τελευταίες να είναι και οι σημαντικότερες [3] [7]. Στην περίπτωση που το επιθεωρούμενο προς διαπίστευση εργαστήριο δεν εφαρμόζει κάποιες από τις περιγραφόμενες λειτουργίες, τότε τα αντίστοιχα μέτρα της κάθε ενότητας δεν εξετάζονται.

Οι Απαιτήσεις για τη Διοίκηση αφορούν στις λειτουργικές παραμέτρους και στις λεπτομέρειες εφαρμογής και αποδοτικότητας του Συστήματος Διαχείρισης Ποιότητας. Οι απαιτήσεις που αναφέρονται στην εν λόγω ενότητα είναι παρόμοιες με αυτές που καθορίζονται στο πρότυπο ISO 9001:2000. Η ενότητα περιλαμβάνει εκατόν τριάντα εννέα (131) δυνητικά εφαρμόσιμα μέτρα. Επιγραμματικά, ορισμένες από τις απαιτήσεις ορίζουν ότι το εκάστοτε εργαστήριο πρέπει:

- Να είναι μια οντότητα που μπορεί να θεωρηθεί νομικά υπεύθυνη.
- Να είναι υπεύθυνο για τη διεξαγωγή δοκιμών, σύμφωνα με το διεθνές πρότυπο και τις ανάγκες των πελατών.
- Να είναι αμερόληπτο έναντι πολιτικών και συμφερόντων που μπορεί να μειώσουν το κύρος του.
- Να είναι εχέμυθο ως προς τα αποτελέσματα.
- Να καθορίζει τις αρμοδιότητες του προσωπικού.
- Να έχει Τεχνικό Υπεύθυνο, ο οποίος θα έχει τη συνολική ευθύνη για τις τεχνικές λειτουργίες και την παροχή των απαιτούμενων πόρων.
- Να έχει Υπεύθυνο Ποιότητας, ο οποίος θα έχει τη συνολική ευθύνη για την παρακολούθηση της σωστής λειτουργίας του συστήματος ποιότητας.
- Να καθορίζει δείκτες βελτίωσης.

Οι Τεχνικές Απαιτήσεις αφορούν στη διασφάλιση της κατάρτισης και επάρκειας του προσωπικού που στελεχώνει την υποδομή, στον έλεγχο των χρησιμοποιούμενων για τις δοκιμές μεθοδολογιών, στον υπάρχοντα εξοπλισμό, στην ύπαρξη μέτρων εξασφάλισης της ποιότητας, στις ενέργειες δειγματοληψίας και ιχνηλασιμότητας των μετρήσεων και τις διαδικασίες αναφοράς των εξαγόμενων αποτελεσμάτων. Το μεγαλύτερο μέρος των απαιτήσεων προέκυψε από τα όσα προβλέπονταν στον αρχικό οδηγό ISO/IEC Guide 25. Η ενότητα περιλαμβάνει εκατόν εβδομήντα (170) δυνητικά εφαρμόσιμα μέτρα.

Το πρότυπο ISO 17025:2005 είναι εφαρμόσιμο σε όλες τις υποδομές εργαστηρίων ανεξαρτήτως μεγέθους και αριθμού απασχολούμενου προσωπικού. Σε κάθε περίπτωση το προσωπικό πρέπει να συμμετέχει στη διαδικασία διαπίστευσης, έστω και αν από τη συμμετοχή του δεν προκύπτει ατομικό όφελος, όπως για παράδειγμα μια προσωπική πιστοποίηση. Κατά τη διάρκεια της επιθεωρήσεως εξετάζονται παράμετροι όπως η επαγγελματική κατάρτιση του προσωπικού και η συνέπεια του κατά την

άσκηση των καθηκόντων σύμφωνα με τα καθορισθέντα, έλεγχοι που δεν μπορούν να πραγματοποιηθούν χωρίς την παρουσία του.

Εν τέλει, οι υποδομές εργαστηρίων χρησιμοποιούν το πρότυπο ISO 17025:2005 με σκοπό να εφαρμόσουν ένα σύστημα ποιότητας, το οποίο θα τους εξασφαλίσει τη δυνατότητα να παράγουν με συνέπεια έγκυρα αποτελέσματα. Επίσης, η συμμόρφωση της λειτουργίας του εργαστηρίου σύμφωνα με τα καθοριζόμενα στο πρότυπο μπορεί να αποσκοπεί στη συμμετοχή σε μια διαδικασία διαπίστευσης, εξασφαλίζοντας έτσι την επίσημη αναγνώριση της ικανότητάς του στο να εκτελεί τις περιγραφόμενες διακριβώσεις και δοκιμές. Σε αυτή την κατεύθυνση θα πρέπει αρχικά να υλοποιηθεί η σύνταξη του Εγχειριδίου Ποιότητας που προβλέπεται από το πρότυπο και, εφόσον κριθεί απαραίτητο, να αναζητηθούν οι υπηρεσίες ενός εξειδικευμένου συμβούλου διαπίστευσης για την αρτιότερη προετοιμασία της υποδομής.

4.5 Συμπεράσματα

Σύμφωνα με τα όσα εξετάστηκαν στο παρόν κεφάλαιο, διαπιστώνεται ότι η επιλογή του κατάλληλου προσωπικού για τη στελέχωση των δυνατοτήτων Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, αποτελεί μια διαδικασία η οποία θα καθορίσει σε μεγάλο βαθμό την αποτελεσματικότητα των εν λόγω δυνατοτήτων. Οι παράγοντες που πρέπει να εξεταστούν είναι πολλοί και καλύπτουν όλες τις παραμέτρους λειτουργίας του Οργανισμού, από την ασφάλεια των διακινούμενων πληροφοριών μέχρι τις οικονομικές δυνατότητες. Τόσο ο επικεφαλής της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας όσο και ο υπεύθυνος του εργαστηρίου Ψηφιακής Εγκληματολογίας, εφόσον οι συνθήκες επιτρέπουν τη στελέχωση των τμημάτων από διαφορετικό προσωπικό, θα πρέπει να καθορίσουν αυστηρά κριτήρια και επαρκείς διαδικασίες για την επιλογή του κατάλληλου προσωπικού, έχοντας υπόψη την πολιτική λειτουργίας και τις κατευθύνσεις της Διοίκησης του Οργανισμού, απέναντι στην οποία είναι οι μοναδικοί υπόλογοι.

Το στρατιωτικό περιβάλλον, λόγω της φύσεώς του, θέτει επιπλέον περιορισμούς και προβληματισμούς κατά την υλοποίηση των παραπάνω διαδικασιών. Η ανάλυση των ιδιαίτερων αυτών παραμέτρων οδηγεί στο συμπέρασμα ότι τα τμήματα που εξετάζονται θα πρέπει να στελεχωθούν από μόνιμο στρατιωτικό προσωπικό, κυρίως για λόγους οικονομίας, αμεσότητας των ενεργειών και εθνικής ασφάλειας. Λόγω όμως του πρώιμου σταδίου στο οποίο βρίσκεται ο συγκεκριμένος τομέας στο στρατιωτικό περιβάλλον, δεν είναι δυνατή η άμεση λειτουργία αποτελεσματικών τέτοιων δυνατοτήτων. Συνεπώς, το μεγαλύτερο μέρος των διατιθέμενων πόρων αλλά και των προσπαθειών του προσωπικού, που θα επωμιστεί αυτές τις ευθύνες, θα πρέπει να επενδυθεί στην επαγγελματική κατάρτιση και τη βελτίωση των ικανοτήτων του, καθώς οι υπηρεσίες που δύναται να προσφέρει στη στρατιωτική λειτουργία είναι πολύτιμες. Η αναβάθμιση του επαγγελματικού επιπέδου του προσωπικού είναι αυτή που θα του επιτρέψει να εκτελέσει αποτελεσματικά τα καθήκοντά του ακόμα και στις περιπτώσεις στις οποίες δεν διατίθεται πληθώρα τεχνικών μέσων.

Πέραν του προσωπικού, η εξασφάλιση του απαραίτητου εξοπλισμού και η δημιουργία της κατάλληλης υποδομής εργαστηρίου θα δώσουν επιπλέον δυνατότητες και θα αυξήσουν την αποδοτικότητα των εμπλεκόμενων τμημάτων. Η σωστή και άρτια προετοιμασία προσωπικού και εξοπλισμού για την πραγματοποίηση των ενεργειών Αντιμετώπισης Περιστατικών Ασφαλείας θα αυξήσει τις πιθανότητες άμεσης αποκατάστασης της λειτουργίας του Οργανισμού, με αντίστοιχο περιορισμό των απωλειών κάθε μορφής. Παράλληλα, με τον τρόπο αυτό, καθίσταται δυνατή και η συγκέντρωση περισσότερων πληροφοριών από το σημείο όπου παρατηρήθηκε το συμβάν, η ανάλυση των οποίων θα βοηθήσει στην εύρεση των αιτιών και την αποφυγή επανάληψης παρόμοιου περιστατικού. Η άμεση αποκατάσταση της ορθής λειτουργίας των Πληροφοριακών Συστημάτων και η μικρότερες δυνατές απώλειες στη δημόσια εικόνα αποτελούν προτεραιότητα για τη στρατιωτική

λειτουργία, ώστε να μη διαταραχθεί η αξιοπιστία και το αίσθημα ασφάλειας των πολιτών.

Τέλος, η δημιουργία μιας πρότυπης υποδομής εργαστηρίου Ψηφιακής Εγκληματολογίας θα πρέπει να αποτελέσει προτεραιότητα στην περίπτωση που αποφασιστεί η ανάπτυξη αντίστοιχων δυνατοτήτων εντός του στρατιωτικού περιβάλλοντος. Η ανάλυση των ψηφιακών πειστηρίων που σχετίζονται με ένα περιστατικό ασφαλείας θα πρέπει να γίνεται βάσει καθορισμένων και αποδεκτών μεθοδολογιών και με τη χρήση αξιόπιστων και ευρέως χρησιμοποιούμενων εργαλείων, ώστε τα ευρήματα που θα εξαχθούν να πληρούν όλα τα χαρακτηριστικά νομικής εγκυρότητας και να μπορούν να παρουσιαστούν σε δικαστικές και λοιπές πειθαρχικές διαδικασίες. Οι παραπάνω προϋποθέσεις καλύπτονται από μια πρότυπη υποδομή εργαστηρίου, πολύ περισσότερο όταν έχει επιθεωρηθεί και διαπιστευθεί για τις λειτουργίες του σύμφωνα με τα διεθνώς καθορισμένα πρότυπα.

Κεφάλαιο 5ο
Επίλογος

5.1 Ανακεφαλαίωση

Στην παρούσα διπλωματική εργασία επιχειρήθηκε μια συνολική προσέγγιση των θεμάτων που αφορούν στις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, μέσα από το πρίσμα και τους περιορισμούς που θέτει το ελληνικό στρατιωτικό περιβάλλον. Η ανάγκη για μια τέτοια μελέτη προέκυψε από την ανυπαρξία μιας προδιαγεγραμμένης μεθοδολογίας, συνοδευόμενης από τις αντίστοιχες προδιαγραφές τεχνικών μέσων και υποδομών, για την αντιμετώπιση των περιστατικών ασφαλείας που ανιχνεύονται στα υπηρεσιακά Πληροφοριακά Συστήματα. Το γεγονός αυτό είχε σαν αποτέλεσμα οι ερευνητές να μην γνωρίζουν τις κανονιστικές διατάξεις βάσει των οποίων ενεργούν, οι ακολουθούμενες μέθοδοι αντιμετώπισης να μην βασίζονται σε ευρέως αποδεκτές αρχές, οι διαδικασίες να πραγματοποιούνται σε χώρους και συστήματα που δεν παρέχουν το απαιτούμενο επίπεδο ασφάλειας για αυτού του είδους τις έρευνες και τελικά να τίθεται σε αμφιβολία η αξιοπιστία και εγκυρότητα των αποτελεσμάτων των ερευνών, προκειμένου αυτά να χρησιμοποιηθούν στις περαιτέρω δικαστικές και εσωτερικές πειθαρχικές λειτουργίες.

Η προσέγγιση του προβλήματος περιέλαβε τα εξής:

- Παρουσίαση των διατάξεων τόσο της ελληνικής νομοθεσίας όσο και των στρατιωτικών πολιτικών ασφαλείας και εξαγωγή συμπερασμάτων σχετικά με τα θέματα ιδιωτικότητας των χρηστών και χειρισμού των ψηφιακών αποδεικτικών στοιχείων, ώστε ο ερευνητής να έχει μια εικόνα του κανονιστικού πλαισίου, εντός του οποίου ενεργεί.

- Προδιαγραφή ενός ενιαίου μοντέλου διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, το οποίο περιλαμβάνει και αναλυτική περιγραφή των ενεργειών ανά στάδιο, το οποίο πρέπει να ακολουθείται επακριβώς από το εξειδικευμένο προσωπικό κατά την αντιμετώπιση οποιουδήποτε περιστατικού, ανεξαρτήτως τρόπου εκδήλωσης και σημασίας, ώστε να εξασφαλίζεται η συνέπεια της διαδικασίας και η εγκυρότητα των αποτελεσμάτων.

- Περιγραφή των χαρακτηριστικών που πρέπει να πληροί το προσωπικό που θα στελεχώσει τις εν λόγω δυνατότητες στο στρατιωτικό περιβάλλον, των απαιτήσεων σε τεχνικά μέσα για την εκτέλεση των ενεργειών του ενιαίου μοντέλου και των προδιαγραφών μιας πρότυπης υποδομής εργαστηρίου Ψηφιακής Εγκληματολογίας στο σύνολό της, ώστε να υπάρχει μια πλήρης εικόνα κατά την αρχική σχεδίαση ανάπτυξης των δυνατοτήτων στο στρατιωτικό περιβάλλον.

5.2 Συμπεράσματα

Τα συμπεράσματα, τα οποία προέκυψαν κατά την εκπόνηση της παρούσας εργασίας, συνοψίζονται στα ακόλουθα:

- Το υφιστάμενο νομοθετικό πλαίσιο παρουσιάζει δυσκολία στο να ακολουθήσει τις τεχνολογικές εξελίξεις στον τομέα της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας. Το νομοθετικό κενό αντιμετωπίζεται εφαρμόζοντας τις διατάξεις που αφορούν στα «φυσικά» αποδεικτικά στοιχεία, οι οποίες ερμηνεύονται αναλόγως της περίστασης και των γνώσεων των δικαστικών αρχών. Απαιτείται η άμεση διαμόρφωση του νομοθετικού πλαισίου το οποίο θα καθορίζει τα θέματα που σχετίζονται με τις εν λόγω δυνατότητες, προκειμένου και οι πολιτικές ασφαλείας που θα συνταχθούν από τους Οργανισμούς να είναι νομικά ορθές.

- Στο στρατιωτικό περιβάλλον, η πραγματοποίηση των ενεργειών που περιλαμβάνονται στις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας και αφορούν στις έρευνες σχετικά με ένα περιστατικό ασφαλείας, καλύπτονται νομικά από το άρθρο 19 του Συντάγματος, εφόσον προκύπτουν λόγοι εθνικής ασφάλειας, αλλά και από τις ισχύουσες πολιτικές ασφαλείας, οι οποίες καθορίζουν το υπηρεσιακό καθεστώς ιδιοκτησίας των Πληροφοριακών Συστημάτων και των διακινούμενων σε αυτά πληροφοριών, καθώς και τους υπεύθυνους ασφαλείας. Παρόλα αυτά, εφόσον μελλοντικά διαμορφωθεί το νομικό πλαίσιο που θα πραγματεύεται τα συγκεκριμένα θέματα, οι πολιτικές ασφαλείας θα πρέπει να αναθεωρηθούν ώστε να συμμορφώνονται με τις αντίστοιχες διατάξεις.

- Το ενιαίο μοντέλο διαδικασιών το οποίο προδιαγράφεται, καλύπτει την ανάγκη προτυποποίησης μιας μεθοδολογίας για την αντιμετώπιση περιστατικών ασφαλείας στο στρατιωτικό περιβάλλον, η οποία στην παρούσα στιγμή απουσιάζει. Με το συγκεκριμένο μοντέλο επιτυγχάνεται τόσο η διαχειριστική όσο και η τεχνική αντιμετώπιση των συμβάντων ενδιαφέροντος, κάτι το οποίο αποτελεί προαπαιτούμενο στις πολιτικές «μηδενικής ανοχής». Η ακολουθία των ενεργειών και η αναλυτική περιγραφή τους καθιστούν τη συνολική υλοποίησή τους δυνατή από το ίδιο προσωπικό, αντιμετωπίζοντας και τους περιορισμούς σε εξειδικευμένο προσωπικό που θέτει η παρούσα στρατιωτική κατάσταση. Το μοντέλο φαίνεται να είναι κατάλληλο συνολικά για το στρατιωτικό περιβάλλον, πλην όμως ασφαλή συμπεράσματα δύναται να εξαχθούν μόνο από την εφαρμογή του σε πραγματικές συνθήκες.

- Το προσωπικό το οποίο θα στελεχώσει τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας αποτελεί τον σημαντικότερο παράγοντα της αποτελεσματικότητάς τους. Εφόσον το ενδεδειγμένο μοντέλο περιλαμβάνει στελέχωση των δυνατοτήτων από μόνιμο στρατιωτικό προσωπικό, απαιτείται να δοθεί ιδιαίτερη μέριμνα για την τεχνική κατάρτισή του και τη συνεχή ανάπτυξη των δυνατοτήτων του, στα πλαίσια που ορίζει και η παρούσα δημοσιονομική κατάσταση.

- Η εξασφάλιση του κατάλληλου εξοπλισμού και η διαπίστευση των υποδομών και των ακολουθούμενων σε αυτές μεθοδολογιών, θα αυξήσει την αποδοτικότητα των διαδικασιών και θα καλύψει τις απαιτήσεις αξιοπιστίας των χρησιμοποιούμενων μεθόδων και εγκυρότητας των εξαγόμενων αποτελεσμάτων. Στην περίπτωση που αποφασιστεί η ανάπτυξη των εν λόγω δυνατοτήτων στο στρατιωτικό περιβάλλον, οι παραπάνω ενέργειες θα πρέπει να αποτελέσουν προτεραιότητες.

5.3 Περαιτέρω Έρευνα

Ο σημαντικότερος τομέας που απαιτεί περαιτέρω έρευνα σχετικά με τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας στο στρατιωτικό περιβάλλον αφορά στη μελέτη της νομικής υπόστασης και εγκυρότητας των χρησιμοποιούμενων μεθόδων, αλλά και της επάρκειας του προσωπικού που τις πραγματοποιεί. Παρόλο που το συγκεκριμένο έργο περιορίζεται από την απουσία σχετικού νομοθετικού πλαισίου, η στρατιωτική πραγματικότητα οφείλει να συμβαδίσει με τις εξελίξεις και να εντάξει όσο το δυνατόν συντομότερα στις λειτουργίες της τις παραπάνω δυνατότητες. Το στρατιωτικό νομικό τμήμα, λόγω της εξειδίκευσής του, θα πρέπει να συνεργαστεί με το αντίστοιχο τεχνικό, το οποίο θα αναλάβει την υλοποίηση των δυνατοτήτων, ώστε να ερευνηθεί η νομιμότητα των διαδικασιών με την παρούσα νομική κατάσταση και να καθοριστούν οι προϋποθέσεις ώστε το εμπλεκόμενο προσωπικό να κρίνεται από τις δικαστικές αρχές ως επαρκές και ικανό.

Η εξειδίκευση του προσωπικού και η ανάπτυξη των δυνατοτήτων του αποτελεί επίσης έναν τομέα όπου απαιτείται περαιτέρω έρευνα. Όπως αναφέρθηκε, το προσωπικό αποτελεί τη σημαντικότερη παράμετρο αποτελεσματικότητας των λειτουργιών. Η κατάρτισή του πρέπει να ελέγχεται διαρκώς, ενώ η επέκταση των δυνατοτήτων και των γνώσεων του συχνά εμποδίζεται από τους οικονομικούς περιορισμούς που χαρακτηρίζουν τη σημερινή κατάσταση στη χώρα. Κατόπιν τούτου, απαιτείται να βρεθούν εναλλακτικές λύσεις, εντός του στρατιωτικού περιβάλλοντος, για τον έλεγχο των γνώσεων και την περαιτέρω εκπαίδευση του προσωπικού.

Σε ότι αφορά στο τεχνικό κομμάτι, οποιαδήποτε μελλοντική εργασία και επέκταση σχετική με τα πραγματευόμενα στην παρούσα εργασία, δε δύναται να προκύψει εάν πρώτα δεν εφαρμοσθούν και ελεγχθούν ως προς την αποδοτικότητά τους οι διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας οι οποίες περιγράφονται. Το παραπάνω προϋποθέτει τη διαμόρφωση της αντίστοιχης πολιτικής στο στρατιωτικό περιβάλλον και την εφαρμογή των διαδικασιών για μια επαρκή χρονική περίοδο, ώστε να προσδιορισθεί ο βαθμός αποτελεσματικότητάς τους.

Αναφορές

1. Mandia K., Prosise C. and Pepe M. (2003) "*Incident Response & Computer Forensics, Second Edition*" McGraw-Hill Co. 2003.
2. Kent K., Chevalier S., Grance T. and Dang H. (2006) "*Guide to Integrating Forensic Techniques into Incident Response*", NIST Special Publication 800-86.
3. Ελληνικός Οργανισμός Τυποποίησης (2006) "*ΕΛΟΤ ΕΝ ISO/IEC 17025 Γενικές Απαιτήσεις για την Ικανότητα των Εργαστηρίων Δοκιμών και Διακριβώσεων, 2η Έκδοση*".
4. Freiling F. and Schwittay B. (2007) "*A Common Process Model for Incident Response and Computer Forensics*", IMF 2007.
5. Mukasey M., Sedgwick J. and Hagy D. (2008) "*Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*", U.S. DoJ, National Institute of Justice.
6. Committee on Identifying the Needs of the Forensic Sciences, National Research Council (2009) "*Strengthening Forensic Science in the United States: A Path Forward*", The National Academy Press.
7. United Nations Industrial Development Organization (2009) "*Complying with ISO 17025: A practical guidebook*", UNIDO 2009.
8. Γενικό Επιτελείο Εθνικής Άμυνας (2009) "*Εθνικός Κανονισμός Ασφαλείας"*.
9. Γενικό Επιτελείο Στρατού, Διεύθυνση Έρευνας και Πληροφορικής (2009) "*Κανονισμός Ασφάλειας Πληροφοριακών Συστημάτων ΣΚ 80-20*", Τυπογραφείο Ελληνικού Στρατού 2009.
10. Nelson B., Phillips A. and Steuart C. (2010) "*Guide to Computer Forensics and Investigations*", Fourth Edition, Cengage Learning 2010.
11. Cichonski P., Milar T., Grance T. and Scarfone K. (2012) "*Computer Security Incident Handling Guide*", NIST Special Publication 800-61 Revision 2.
12. Association of Chief Police Officers (ACPO) (2012) "*ACPO Good Practice Guide for Digital Evidence*", Version 5.0, Police Central E-Crime Unit.
13. Association of Chief Police Officers (ACPO) (2014) "*ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation*", Version 0.1.4, 7Safe Publications 2014.

Παραρτήματα

Παράρτημα «Α»

Οδηγός Ενεργειών Συλλογής Ψηφιακών Αποδεικτικών Στοιχείων

Ο παρακάτω οδηγός περιλαμβάνει μια προτεινόμενη αναλυτική μεθοδολογία [5], η οποία περιγράφει τις διαδοχικές ενέργειες και ελέγχους που πρέπει να υλοποιήσει η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας κατά το στάδιο της συλλογής των ψηφιακών πειστηρίων από τις αντίστοιχες πηγές που αναγνωρίσθηκαν στη σκηνή όπου έλαβε χώρα το περιστατικό ασφαλείας Πληροφορικής.

Στο στρατιωτικό περιβάλλον, η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας θα προχωρήσει στις παρακάτω ενέργειες στο πλαίσιο διαταγής που θα έχει λάβει για έρευνα ενός περιστατικού ασφαλείας, είτε από τη Διεύθυνση Ασφαλείας και Πληροφοριών του Γενικού Επιτελείου, μετά από αντίστοιχη αναφορά ενός συμβάντος, είτε από την οικεία Διεύθυνση Πληροφορικής, μετά την ανίχνευση ενός συμβάντος από τους μηχανισμούς παρακολούθησης και ασφαλείας. Η διαταγή θα πρέπει να καθορίζει, σε συνεννόηση με την οικεία Διοίκηση – Διεύθυνση, εάν υπάρχει δυνατότητα συλλογής και κράτησης των φυσικών αυθεντικών μέσων στο εργαστήριο Ψηφιακής Εγκληματολογίας (π.χ. κεντρικές μονάδες σταθμών εργασίας) ή εάν θα πρέπει να ληφθεί ακριβές αντίγραφο για την διεξαγωγή της έρευνας. Σε κάθε περίπτωση, η αξίωση των χρηστών για ιδιωτικότητα καθορίζεται από την ισχύουσα νομοθεσία και τις πολιτικές ασφαλείας (ΕΚΑ, ΣΚ 80-20) που διέπουν τη χρήση των στρατιωτικών Πληροφοριακών Συστημάτων.

Το προσωπικό της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας πρέπει να κατέχει τις απαιτούμενες γνώσεις και εμπειρία για να προχωρήσει στις ενέργειες που περιγράφονται στον παρακάτω οδηγό. Στην περίπτωση που δεν καλύπτονται αυτές οι προϋποθέσεις από τον ερευνητή, η διαδικασία θα πρέπει να αναβληθεί, διότι υπάρχει ο κίνδυνος είτε να μην συγκεντρωθούν όλα τα διαθέσιμα ψηφιακά στοιχεία είτε να απωλεσθεί η ακεραιότητα και ορθότητα των ήδη συλλεχθέντων. Επίσης, οι πρακτικές που αναφέρθηκαν στο στάδιο της Συσκευασίας, Μεταφοράς και Φύλαξης των Ψηφιακών Αποδεικτικών Στοιχείων της Φάσης Αναλύσεως πρέπει να τηρούνται επακριβώς. Τέλος, υπενθυμίζεται ότι κάθε ενέργεια στην οποία προβαίνει ο ερευνητής πρέπει να καταγράφεται και τεκμηριώνεται λεπτομερώς.

Τα βήματα της μεθοδολογίας για την συνηθέστερη περίπτωση ενός υπολογιστή ως εξεταζόμενη συσκευή έχουν ως εξής:

1. Αναγνώριση Υπάρχουσας Κατάστασης

Αρχικά πρέπει να αναγνωρισθεί η κατάσταση του υπολογιστή, εάν δηλαδή βρίσκεται σε λειτουργία ή όχι. Για τον λόγο αυτό ο ερευνητής ελέγχει εάν είναι αναμμένες οι ενδεικτικές λυχνίες ρεύματος ή απασχόλησης του σκληρού δίσκου. Επίσης για τον ίδιο σκοπό μπορεί να πλησιάσει την κεντρική μονάδα ώστε να ακούσει το κατά πόσο λειτουργεί η ψύκτρα του τροφοδοτικού ή άλλα εξαρτήματα του υπολογιστή. Στην περίπτωση που δεν μπορεί να διαπιστώσει τη λειτουργία του μηχανήματος με τους παραπάνω τρόπους ελέγχει την οθόνη για τον αν είναι σε λειτουργία ή σε κατάσταση ύπνωσης (sleep mode).

1.1 Ενδεχόμενο 1: Η οθόνη βρίσκεται σε λειτουργία και προβάλλει ένα πρόγραμμα, μια εφαρμογή, μια εικόνα, ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή μια ιστοσελίδα.

1.1.1 Ο ερευνητής φωτογραφίζει την οθόνη και καταγράφει όλες τις πληροφορίες που προβάλλονται.

1.1.2 Συνέχεια ενεργειών από 3.«Υπολογιστής σε Λειτουργία».

1.2 Ενδεχόμενο 2: Η οθόνη βρίσκεται σε λειτουργία και προβάλλει μια εικόνα ή βρίσκεται σε λειτουργία προφύλαξης οθόνης (screen saver).

1.2.1 Ο ερευνητής μετακινεί το ποντίκι (mouse) χωρίς να πιέσει κανένα πλήκτρο ή να γυρίσει τη ροδέλα. Στη συνέχεια καταγράφει εάν ο υπολογιστής μεταπίπτει σε οθόνη εισαγωγής διαπιστευτηρίων για είσοδο (login screen) ή επιστρέφει στην επιφάνεια εργασίας και προβάλλει πληροφορίες όμοιες με αυτές στο Ενδεχόμενο 1. Η αλλαγή της κατάστασης καταγράφεται.

1.2.2 Φωτογραφίζει την οθόνη και καταγράφει όλες τις πληροφορίες που προβάλλονται.

1.2.3 Συνέχεια ενεργειών από 3.«Υπολογιστής σε Λειτουργία».

1.3 Ενδεχόμενο 3: Η οθόνη βρίσκεται σε λειτουργία αλλά δεν προβάλλει τίποτα (σαν να είναι κλειστή).

1.3.1 Ο ερευνητής μετακινεί το ποντίκι (mouse) χωρίς να πιέσει κανένα πλήκτρο ή να γυρίσει τη ροδέλα. Η οθόνη μεταπίπτει σε οθόνη εισαγωγής διαπιστευτηρίων για είσοδο (login screen) ή επιστρέφει στην επιφάνεια εργασίας και προβάλλει πληροφορίες όμοιες με αυτές στο Ενδεχόμενο 1. Η αλλαγή της κατάστασης καταγράφεται.

1.3.2 Φωτογραφίζει την οθόνη και καταγράφει όλες τις πληροφορίες που προβάλλονται.

1.3.3 Συνέχεια ενεργειών από 3.«Υπολογιστής σε Λειτουργία».

1.4 Ενδεχόμενο 4α: Η οθόνη είναι εκτός λειτουργίας και δεν προβάλλει τίποτα.

1.4.1 Ο ερευνητής ελέγχει τη θέση του διακόπτη λειτουργίας. Εάν είναι στη θέση «Εκτός» (Off) τότε θέτει σε λειτουργία την οθόνη. Η οθόνη μεταπίπτει σε οθόνη εισαγωγής διαπιστευτηρίων για είσοδο (login screen) ή επιστρέφει στην επιφάνεια εργασίας και προβάλλει πληροφορίες όμοιες με αυτές στο Ενδεχόμενο 1. Η αλλαγή της κατάστασης καταγράφεται.

1.4.2 Φωτογραφίζει την οθόνη και καταγράφει όλες τις πληροφορίες που προβάλλονται.

1.4.3 Συνέχεια ενεργειών από 3.«Υπολογιστής σε Λειτουργία».

1.5 Ενδεχόμενο 4β: Η οθόνη είναι εκτός λειτουργίας και δεν προβάλλει τίποτα.

1.5.1 Ο ερευνητής ελέγχει τη θέση του διακόπτη λειτουργίας. Εάν είναι στη θέση «Εκτός» (Off) τότε θέτει σε λειτουργία την οθόνη. Η οθόνη συνεχίζει να μην προβάλλει τίποτα ούτε εμφανίζει ενδείξεις αλλαγής κατάστασης.

1.5.2 Φωτογραφίζει την κενή οθόνη.

1.5.3 Συνέχεια ενεργειών από 2.«Υπολογιστής εκτός Λειτουργίας».

1.6 Ενδεχόμενο 5: Η οθόνη βρίσκεται σε λειτουργία αλλά δεν προβάλλει τίποτα.

1.6.1 Ο ερευνητής μετακινεί το ποντίκι (mouse) χωρίς να πιέσει κανένα πλήκτρο ή να γυρίσει τη ροδέλα.

1.6.2 Εάν η οθόνη συνεχίζει να μην προβάλλει τίποτα, βεβαιώνεται ότι δεν υπάρχει πρόβλημα με την παροχή ρεύματος της οθόνης. Εάν δεν προκύπτει πρόβλημα τροφοδοσίας της οθόνης, επανελέγχεται η κατάσταση λειτουργίας του υπολογιστή.

1.6.3 Εάν η οθόνη συνεχίζει να μην προβάλλει τίποτα και δεν προκύπτει ότι ο υπολογιστής βρίσκεται σε λειτουργία τότε συνεχίζει τις ενέργειές του από 2.«Υπολογιστής εκτός Λειτουργίας».

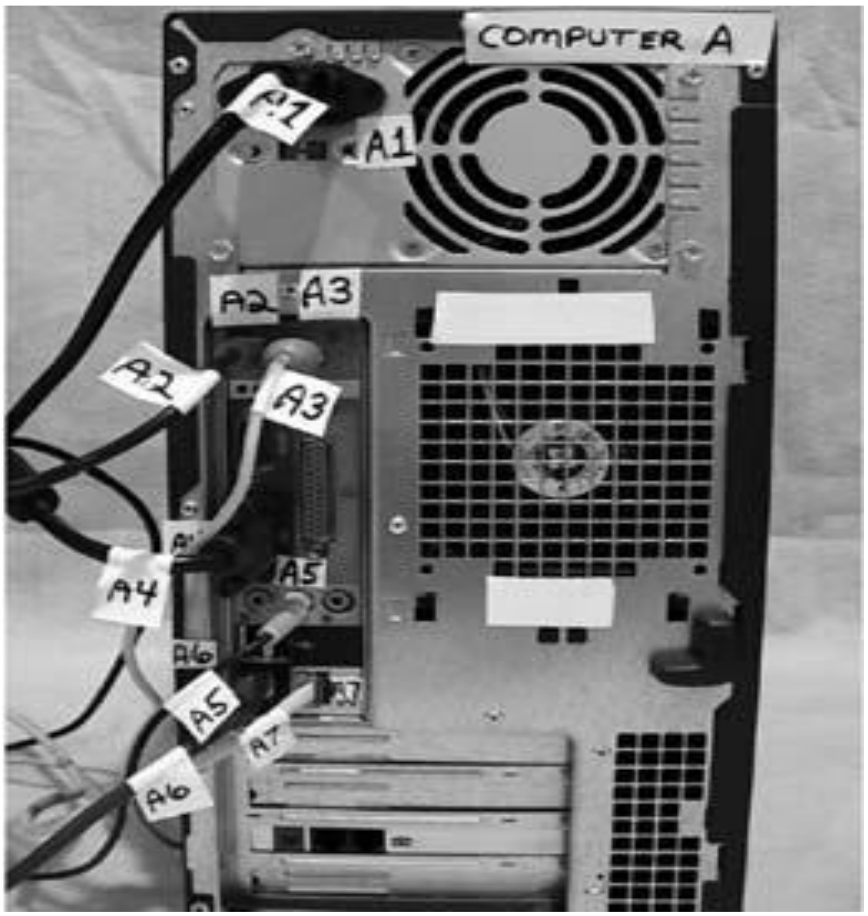
2. Υπολογιστής Εκτός Λειτουργίας

2.1 Για επιτραπέζιους υπολογιστές ο ερευνητής εκτελεί τα εξής:

2.1.1 Φωτογραφίζει, καταγράφει και σχεδιάζει όλα τα καλώδια και τις συνδέσεις που καταλήγουν στον υπολογιστή.

2.1.2 Σημαίνει μοναδικά το καλώδιο παροχής ρεύματος και όλα τα υπόλοιπα καλώδια ή τις συσκευές που είναι συνδεδεμένες στην κεντρική μονάδα, καθώς και την αντίστοιχη θύρα επί του υπολογιστή.

2.1.3 Φωτογραφίζει τον υπολογιστή αφού ολοκληρώσει τις ενέργειες που περιγράφονται στο προηγούμενο βήμα. Το αποτέλεσμα πρέπει να μοιάζει με την εικόνα Α.1.



Εικόνα Α.1 : Φωτογραφία υπολογιστή όπου έχουν σημανθεί τα καλώδια και οι συνδέσεις
(Πηγή: Nelson B., Guide to Computer Forensics and Investigations, 4th edition)

2.1.4 Αφαιρεί το καλώδιο παροχής ρεύματος πρώτα από τον υπολογιστή και στη συνέχεια από την πρίζα ή την συσκευή Αδιάλειπτης Παροχής Ενέργειας (Uninterruptible Power Supply – UPS) και το αποθηκεύει.

2.1.5 Αφαιρεί όλα τα καλώδια που είναι συνδεδεμένα στην κεντρική μονάδα, καταγράφει τις συσκευές στις οποίες καταλήγουν και τα αποθηκεύει.

2.1.6 Τοποθετεί προστατευτική ταινία ώστε να φράξει τον οδηγό δισκέτας, εφόσον υπάρχει.

2.1.7 Ελέγχει εάν ο οδηγός οπτικού δίσκου (CD/DVD), εφόσον υπάρχει, είναι κλειστός και σημειώνει εάν υπάρχει, δεν υπάρχει ή δεν ελέγχθηκε η ύπαρξη δίσκου εντός. Τοποθετεί προστατευτική ταινία ώστε να φράξει τον οδηγό.

2.1.8 Τοποθετεί προστατευτική ταινία πάνω από τον κεντρικό διακόπτη λειτουργίας.

2.1.9 Καταγράφει τη μάρκα, το μοντέλο, τον αριθμό ονομαστικού και οποιοδήποτε διακριτικό έχει τοποθετηθεί μετέπειτα από κάποιον χρήστη.

2.1.10 Καταγράφει όλα τα στοιχεία του υπολογιστή στα χρησιμοποιούμενα από την υπηρεσία έντυπα αλυσίδας κυριότητας με τον τρόπο που έχει προκαθοριστεί.

2.1.11 Συσκευάζει όλα τα αποδεικτικά στοιχεία σύμφωνα με τις προκαθορισμένες διαδικασίες, ώστε να αποφευχθεί οποιαδήποτε φθορά ή καταστροφή των φορέων και απώλεια των δεδομένων κατά τη μεταφορά και φύλαξή τους.

2.2 Για φορητούς υπολογιστές ο ερευνητής εκτελεί τα εξής:

2.2.1 Φωτογραφίζει, καταγράφει και σχεδιάζει όλα τα καλώδια και τις συνδέσεις που καταλήγουν στο φορητό υπολογιστή.

2.2.2 Σημαίνει μοναδικά όλα τα καλώδια ή τις συσκευές που είναι συνδεδεμένες στο φορητό υπολογιστή, καθώς και την αντίστοιχη θύρα επί του υπολογιστή.

2.2.3 Φωτογραφίζει τον υπολογιστή αφού ολοκληρώσει τις ενέργειες που περιγράφονται στο προηγούμενο βήμα.

2.2.4 Αφαιρεί από το φορητό υπολογιστή και αποθηκεύει το καλώδιο τροφοδοσίας και τις μπαταρίες του.

2.2.5 Αφαιρεί όλα τα καλώδια που είναι συνδεδεμένα στον υπολογιστή, καταγράφει τις συσκευές στις οποίες καταλήγουν και τα αποθηκεύει.

2.2.6 Τοποθετεί προστατευτική ταινία ώστε να φράξει τον οδηγό δισκέτας, εφόσον υπάρχει.

2.2.7 Ελέγχει εάν ο οδηγός οπτικού δίσκου (CD/DVD), εφόσον υπάρχει, είναι κλειστός και σημειώνει εάν υπάρχει, δεν υπάρχει ή δεν ελέγχθηκε η ύπαρξη δίσκου εντός. Τοποθετεί προστατευτική ταινία ώστε να φράξει τον οδηγό.

2.2.8 Τοποθετεί προστατευτική ταινία πάνω από τον κεντρικό διακόπτη λειτουργίας.

2.2.9 Καταγράφει τη μάρκα, το μοντέλο, τον αριθμό ονομαστικού και οποιοδήποτε διακριτικό έχει τοποθετηθεί μετέπειτα από κάποιον χρήστη.

2.2.10 Καταγράφει όλα τα στοιχεία του υπολογιστή στα χρησιμοποιούμενα από την υπηρεσία έντυπα αλυσίδας κυριότητας με τον τρόπο που έχει προκαθοριστεί.

2.2.11 Συσκευάζει όλα τα αποδεικτικά στοιχεία σύμφωνα με τις προκαθορισμένες διαδικασίες.

3. Υπολογιστής σε Λειτουργία

Η ξαφνική διακοπή στην τροφοδοσία ενός υπολογιστή που βρίσκεται σε λειτουργία, αφαιρώντας βίαια το καλώδιο παροχής, αποτελεί τη συνηθέστερη μέθοδο αντιμετώπισης στη συγκεκριμένη περίπτωση. Παρόλα αυτά υπάρχουν περιπτώσεις κατά τις οποίες πιθανόν να απαιτηθεί η συνδρομή προσωπικού που είναι εξειδικευμένο στη συλλογή ευμετάβλητων δεδομένων (volatile data) με τις μεθόδους της «Εν Ενεργεία» Ψηφιακής Εγκληματολογίας (“Live” Digital Forensics).

3.1 Στις παρακάτω περιπτώσεις συνίσταται η βίαιη διακοπή της λειτουργίας ενός υπολογιστή:

3.1.1 Από τα προβαλλόμενα στην οθόνη προκύπτει ότι βρίσκεται σε εξέλιξη διαγραφή ή με οποιονδήποτε άλλο τρόπο καταστροφή δεδομένων.

3.1.2 Υπάρχει ένδειξη ότι βρίσκεται σε εξέλιξη μια καταστροφική διαδικασία για τα αποθηκευτικά μέσα του υπολογιστή.

3.1.3 Ο υπολογιστής εμφανίζει ένα τυπικό περιβάλλον Λειτουργικού Συστήματος Microsoft Windows. Η βίαιη διακοπή της λειτουργίας του υπολογιστή θα έχει σαν αποτέλεσμα να διατηρηθούν οι πληροφορίες που αφορούν στον τελευταίο συνδεδεμένο χρήστη του μηχανήματος, στις χρονικές λεπτομέρειες της σύνδεσής του, στα τελευταία αρχεία που είχε πρόσβαση και άλλες σημαντικές πληροφορίες.

3.2 Στις παρακάτω περιπτώσεις ΔΕΝ συνίσταται η βίαιη διακοπή της λειτουργίας ενός υπολογιστή:

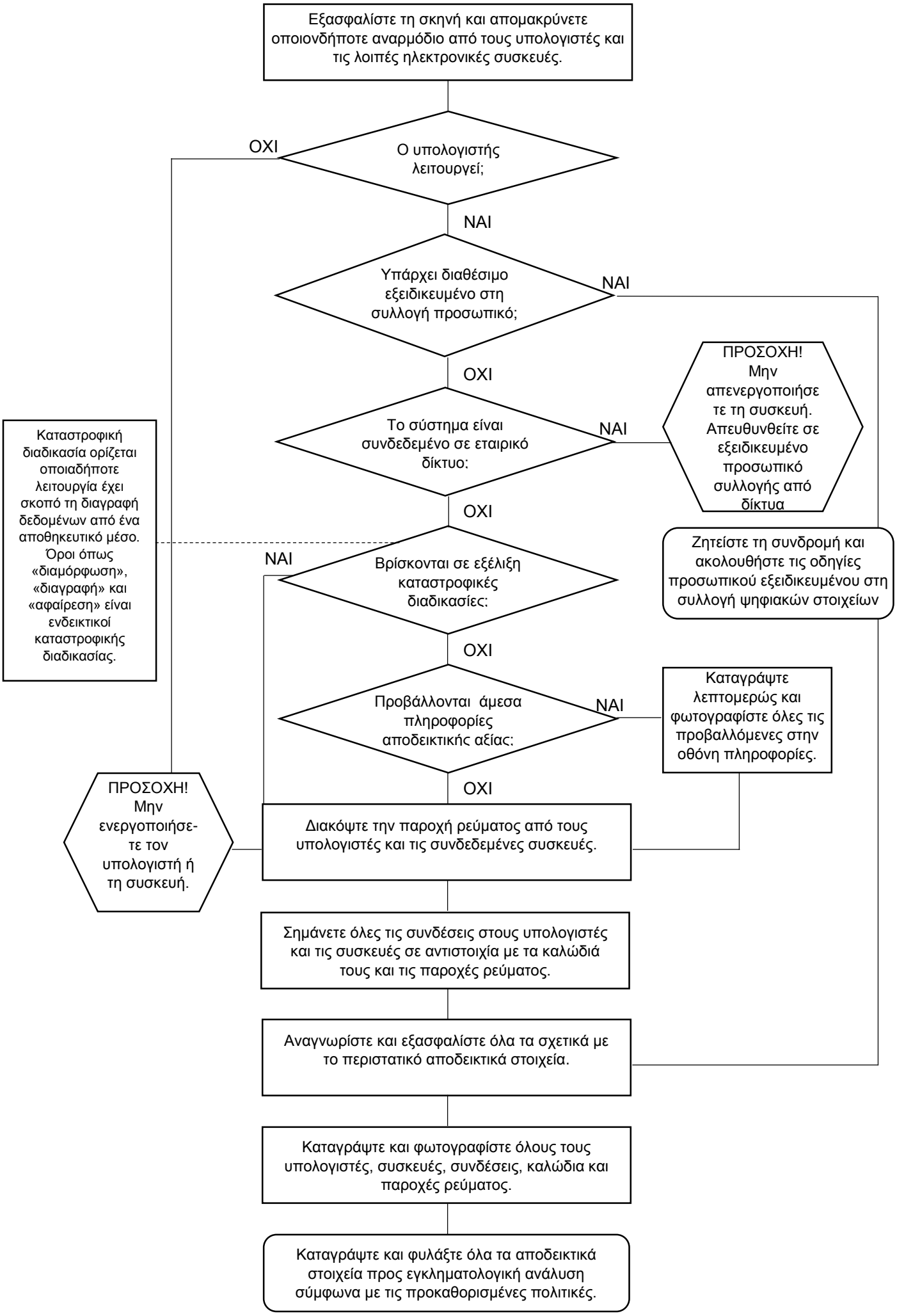
3.2.1 Δεδομένα προφανούς αξίας σχετικά με το περιστατικό ασφαλείας προβάλλονται άμεσα στην οθόνη. Ο ερευνητής, εφόσον δεν έχει τις κατάλληλες γνώσεις, πρέπει να ζητήσει άμεσα τη συνδρομή ειδικού στη συλλογή ευμετάβλητων δεδομένων.

3.2.2 Υπάρχουν ενδείξεις ότι βρίσκονται σε λειτουργία τα εξής:

- Συνεδρίες Άμεσης Συνομιλίας (instant messaging - chat rooms).
- Απομακρυσμένοι αποθηκευτικοί χώροι (remote data storage).
- Ανοιχτά αρχεία επεξεργασίας κειμένου.
- Αρχεία παιδικής πορνογραφίας.
- Διαδικασία παράνομου εμπορίου.
- Διαδικασίες κρυπτογράφησης.
- Προφανείς παράνομες δραστηριότητες.

Εκτός από επιτραπέζιους και φορητούς υπολογιστές, η Ομάδα Αντιμετώπισης Περιστατικών πιθανώς να αναγνωρίσει και άλλες συσκευές ως πηγές ψηφιακών αποδεικτικών στοιχείων. Κινητά τηλέφωνα, ταμπλέτες (tablets), Προσωπικοί Ψηφιακοί Βοηθοί (Personal Digital Assistants - PDAs), δρομολογητές, εκτυπωτές, σαρωτές, φωτοτυπικά μηχανήματα, συσκευές, συσκευές καταγραφής συνομιλίας, συσκευές GPS και ψηφιακά τηλεφωνικά κέντρα μπορεί να περιέχουν δεδομένα σημαντικά για την έρευνα ενός περιστατικού ασφαλείας. Το ίδιο ισχύει και στην περίπτωση που οι υπολογιστές βρίσκονται συνδεδεμένοι σε κάποιο δίκτυο. Εφόσον δεν υπάρχουν οι τεχνικές γνώσεις για τη συλλογή πληροφοριών από αυτές τις συσκευές ή δίκτυα, αυτό που οφείλει να κάνει η ομάδα είναι να εξασφαλίσει, στο βαθμού του δυνατού, ότι οι πληροφορίες δεν θα τροποποιηθούν ή διαγραφούν (π.χ. τοποθέτηση σε φορέα Φαραντέι, απαγόρευση χρήσης από αναρμόδιους). Κάθε ενέργεια θα πρέπει να καταγράφεται λεπτομερώς. Οι διαδικασίες συλλογής ψηφιακών αποδεικτικών στοιχείων από τέτοιες συσκευές είναι εκτός του πλαισίου της παρούσας εργασίας.

Ενδεικτικό Διάγραμμα Ροής Ενεργειών Συλλογής Ψηφιακών Στοιχείων



Παράρτημα «Β»

Έντυπο Ψηφιακών Πειστηρίων και Οδηγίες Συμπλήρωσης

Στο παρόν παράρτημα παρουσιάζεται το υπόδειγμα ενός προτεινόμενου Έντυπου Ψηφιακών Πειστηρίων, το οποίο συμπληρώνεται κατά τη συλλογή των ψηφιακών αποδεικτικών στοιχείων στη σκηνή όπου έλαβε χώρα το περιστατικό ασφαλείας και χρησιμοποιείται κατά τις διαδικασίες ελέγχου κυριότητας των πειστηρίων.

Τα πεδία του εντύπου συμπληρώνονται ως εξής:

(α) Αναγράφεται ο βαθμός ασφαλείας του εγγράφου, σύμφωνα με τα όσα καθορίζονται στον Ε.Κ.Α. περί διαβάθμισης εγγράφων.

(β) Αναγράφεται ο αριθμός υποθέσεως σύμφωνα με τον τρόπο αρίθμησης των υποθέσεων που έχει καθορισθεί από τις εσωτερικές υπηρεσιακές διαδικασίες.

(γ) Αναγράφεται η Υπηρεσία στην οποία ανήκει ο ερευνητής που συλλέγει τα ψηφιακά πειστήρια (π.χ. Κέντρο Πληροφορικής Υποστήριξης Ε.Σ.).

(δ) Αναγράφεται η τοποθεσία όπου συλλέχθηκαν τα πειστήρια (π.χ. Στρδο «Παπάγου»).

(ε) Αναγράφεται το πρόσωπο (π.χ. ιδιοκτήτης συσκευής, χειριστής σταθμού εργασίας) από το οποίο συλλέχθηκαν τα πειστήρια.

(στ) Αναγράφεται η διεύθυνση της τοποθεσίας όπου πραγματοποιήθηκε η συλλογή.

(ζ) Αναγράφεται το ακριβές σημείο που πραγματοποιήθηκε η συλλογή (π.χ. Κεντρικό Κτήριο, 3ος όροφος, Γραφείο 321).

(η) Αναφέρεται η αιτία συλλογής (π.χ. πειστήρια υποθέσεως).

(θ) Αναγράφεται η ημερομηνία και η ώρα που πραγματοποιήθηκε η συλλογή (π.χ. 07 1130-1300 ΔΕΚ 2015).

(ι) Αναγράφεται ο αύξων αριθμός που αντιστοιχίζεται σε κάθε πειστήριο.

(ια) Αναγράφεται η ποσότητα που συλλέχθηκε από το κάθε πειστήριο.

(ιβ) Περιγράφεται το κάθε πειστήριο αναλυτικά. Περιλαμβάνεται ο κατασκευαστής, το μοντέλο, ο αριθμός ονομαστικού, η κατάσταση του πειστηρίου, οποιοδήποτε ιδιαίτερο χαρακτηριστικό και λοιπές τεχνικές λεπτομέρειες (π.χ. εσωτερικός σκληρός δίσκος Western Digital Desktop 1TB S/N:WD123456 MD5sum: BADFE1D9D258E89A6CF0BC7682EBDA6C)

(ιγ) Αναγράφεται ο αύξων αριθμός που αντιστοιχεί στο πειστήριο που παρουσιάζει μεταβολή στην κατάσταση κυριότητάς του.

(ιδ) Αναγράφεται η ημερομηνία που εμφανίζεται η μεταβολή στην κατάσταση κυριότητάς του αντίστοιχου πειστηρίου.

(ιε) Τίθεται η υπογραφή του ατόμου που παραδίδει το ψηφιακό πειστήριο.

(ιστ) Αναγράφονται ο βαθμός και το ονοματεπώνυμο του ατόμου που παραδίδει το ψηφιακό πειστήριο.

(ιζ) Τίθεται η υπογραφή του ατόμου που παραλαμβάνει το ψηφιακό πειστήριο.

(ιη) Αναγράφονται ο βαθμός και το ονοματεπώνυμο του ατόμου που παραλαμβάνει το ψηφιακό πειστήριο.

(ιθ) Αναφέρεται η αιτία μεταβολής της κατάστασης κυριότητας του πειστηρίου (π.χ. αποστολή στο Εργαστήριο Ψηφιακής Εγκληματολογίας για ανάλυση, τελική απόρριψη πειστηρίου).

(κ) Αναγράφεται ο αύξων αριθμός της σελίδας και το σύνολο των σελίδων, σύμφωνα με τα όσα ορίζονται για την αρίθμηση των σελίδων των εγγράφων από τον Διακλαδικό Κανονισμό Στρατιωτικής Αλληλογραφίας (π.χ. Σελίδα 1 από Σελίδες 2).

(κα) Αναγράφεται το άτομο (ιδιοκτήτης ή άλλο πρόσωπο) στο οποίο επιστράφηκε το πειστήριο στα πλαίσια της τελικής απόρριψής του.

(κβ) Αναγράφεται η μέθοδος που χρησιμοποιήθηκε για την καταστροφή του πειστηρίου στα πλαίσια της τελικής απόρριψής του (π.χ. καταστροφή δια πυρός, καταστροφή δια τεμαχισμού).

(κγ) Αναγράφεται οποιαδήποτε άλλη κατάληξη ενός πειστηρίου στα πλαίσια της τελικής απόρριψής του (π.χ. αποθήκευση με τον φάκελο της υπόθεσης όταν πρόκειται για έγγραφα πειστήρια).

(κδ) Η αρχή τελικής απόρριψης (π.χ. υπηρεσία, χειριστής πειστηρίων) καταγράφει τους αύξοντες αριθμούς των πειστηρίων και τον αριθμό της υπόθεσης που αφορούν και βεβαιώνει την καταστροφή τους, σύμφωνα με τα όσα περιεγράφηκαν στην προηγούμενη ενότητα.

(κε) Η διαδικασία τελικής απόρριψης των πειστηρίων, όπως περιεγράφηκε παραπάνω, βεβαιώνεται και από έναν επιπλέον μάρτυρα, για λόγους αξιοπιστίας.

Παρακάτω παρατίθεται το υπόδειγμα του προτεινόμενου Έντυπου Ψηφιακών Πειστηρίων και Αλυσίδας Κυριότητας.

(ΒΑΘΜΟΣ ΑΣΦΑΛΕΙΑΣ) (α)

ΕΝΤΥΠΟ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ ΚΑΙ ΑΛΥΣΙΔΑΣ ΚΥΡΙΟΤΗΤΑΣ	ΑΡΙΘΜΟΣ ΥΠΟΘΕΣΕΩΣ: (β)	
ΠΑΡΑΛΑΜΒΑΝΟΥΣΑ ΥΠΗΡΕΣΙΑ: (γ)	ΤΟΠΟΘΕΣΙΑ: (δ)	
ΠΡΟΣΩΠΟ ΑΠΟ ΤΟ ΟΠΟΙΟ ΣΥΛΛΕΧΘΗΚΕ: (ε)	ΔΙΕΥΘΥΝΣΗ: (στ)	
ΣΗΜΕΙΟ ΣΥΛΛΟΓΗΣ: (ζ)	ΑΙΤΙΑ: (η)	ΗΜΝΙΑ/ΩΡΑ ΣΥΛΛΟΓΗΣ (θ)

Α/Α ΠΕΙΣΤΗΡΙΟΥ	**ΠΟΣΟΤΗΤΑ**	**ΠΕΡΙΓΡΑΦΗ (συμπεριλάβετε κατασκευαστή, μοντέλο, αρ.ονομαστικού, κατάσταση)**
(ι)	(ια)	(ιβ)

ΑΛΥΣΙΔΑ ΚΥΡΙΟΤΗΤΑΣ

Α/Α ΠΕΙΣΤΗΡΙΟΥ	**ΗΜ/ΝΙΑ**	**ΠΑΡΑΔΙΔΩΝ**	**ΠΑΡΑΛΑΜΒΑΝΩΝ**	**ΑΙΤΙΑ ΜΕΤΑΒΟΛΗΣ**
(ιγ)	(ιδ)	ΥΠΟΓΡΑΦΗ (ιε)	ΥΠΟΓΡΑΦΗ (ιζ)	(ιθ)
		ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ (ιστ)	ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ (ιη)	
		ΥΠΟΓΡΑΦΗ	ΥΠΟΓΡΑΦΗ	
		ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	
		ΥΠΟΓΡΑΦΗ	ΥΠΟΓΡΑΦΗ	
		ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	
		ΥΠΟΓΡΑΦΗ	ΥΠΟΓΡΑΦΗ	
		ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	
		ΥΠΟΓΡΑΦΗ	ΥΠΟΓΡΑΦΗ	
		ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	

(ΒΑΘΜΟΣ ΑΣΦΑΛΕΙΑΣ)

		ΥΠΟΓΡΑΦΗ	ΥΠΟΓΡΑΦΗ	
		ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	
		ΥΠΟΓΡΑΦΗ	ΥΠΟΓΡΑΦΗ	
		ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	
		ΥΠΟΓΡΑΦΗ	ΥΠΟΓΡΑΦΗ	
		ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	
		ΥΠΟΓΡΑΦΗ	ΥΠΟΓΡΑΦΗ	
		ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	ΒΑΘΜΟΣ-ΟΝΟΜ/ΜΟ	

ΤΕΛΙΚΗ ΑΠΟΡΡΙΨΗ ΠΕΙΣΤΗΡΙΩΝ

ΕΠΙΣΤΡΑΦΗΚΕ ΣΕ : (κα)

ΚΑΤΑΣΤΡΑΦΗΚΕ : (κβ)

ΑΛΛΟ (ΔΙΕΥΚΡΙΝΗΣΤΕ) : (κγ)

ΑΡΧΗ ΤΕΛΙΚΗΣ ΑΠΟΡΡΙΨΗΣ ΠΕΙΣΤΗΡΙΩΝ (κδ)

ΤΑ ΠΕΙΣΤΗΡΙΑ ΜΕ Α/Α ……ΤΟΥ ΠΑΡΟΝΤΟΣ ΕΝΤΥΠΟΥ ΠΟΥ ΣΥΜΜΕΤΕΧΟΥΝ ΣΤΗΝ ΕΡΕΥΝΑ ΜΕ ΑΡΙΘΜΟ ΥΠΟΘΕΣΕΩΣ …….. ΔΕΝ ΑΠΑΙΤΟΥΝΤΑΙ ΠΛΕΟΝ ΩΣ ΑΠΟΔΕΙΚΤΙΚΑ ΣΤΟΙΧΕΙΑ ΚΑΙ ΔΥΝΑΤΑΙ ΝΑ ΑΠΟΡΡΙΦΘΟΥΝ ΩΣ ΠΕΡΙΓΡΑΦΕΤΑΙ ΑΝΩΤΕΡΩ, ΣΥΜΦΩΝΑ ΚΑΙ ΜΕ ΤΑ ΚΑΘΟΡΙΖΟΜΕΝΑ ΣΤΟΝ Ε.Κ.Α. (ΑΡ. 27 & 28) ΚΑΙ ΤΟΝ Σ.Κ. 80-20 (ΑΡ. 40 & 41).

…… …….. ……..

(βαθμός – ονοματεπώνυμο ολογράφως) *(υπογραφή)* *(ημ/νια)*

ΜΑΡΤΥΡΑΣ ΤΕΛΙΚΗΣ ΑΠΟΡΡΙΨΗΣ ΠΕΙΣΤΗΡΙΩΝ (κε)

ΤΑ ΠΕΡΙΓΡΑΦΟΜΕΝΑ ΣΤΟ ΠΑΡΟΝ ΕΝΤΥΠΟ ΠΕΙΣΤΗΡΙΑ ΜΕ Α/Α .....……. ΚΑΤΑΣΤΡΑΦΗΚΑΝ ΚΑΤΑ ΤΗΝ ΑΝΑΓΡΑΦΟΜΕΝΗ ΗΜΕΡΟΜΗΝΙΑ ΥΠΟ ΤΗΝ ΠΑΡΟΥΣΙΑ ΜΟΥ ΑΠΟ ΤΟΝ ΔΙΑΧΕΙΡΙΣΤΗ ΠΕΙΣΤΗΡΙΩΝ ΩΣ ΠΕΡΙΓΡΑΦΕΤΑΙ ΑΝΩΤΕΡΩ.

…….. ……

(βαθμός – ονοματεπώνυμο ολογράφως) *(υπογραφή)*

Παράρτημα «Γ»

Απαγόρευση Εγγραφής (Write Blocker) με Τροποποίηση της Registry

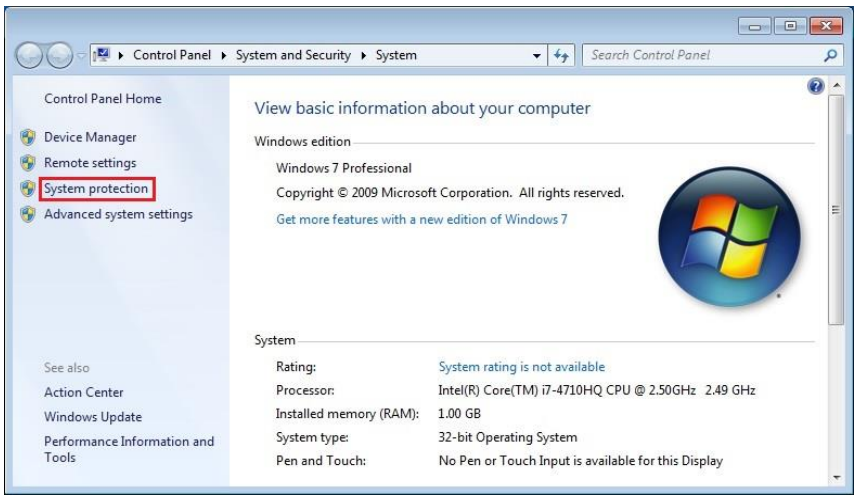
Κατά τη διάρκεια της ανάλυσης των ψηφιακών πειστηρίων, το μέσο αποθήκευσης (πχ. σκληρός δίσκος), μέσω ενός ενδιάμεσου φορέα, θα συνδεθεί σε κάποια θύρα του Σταθμού Εργασίας Ψηφιακής Εγκληματολογίας. Τα Λειτουργικά Συστήματα, κατά την σύνδεση εξωτερικής συσκευής σε μια από τις θύρες του υπολογιστή, εκτελούν συνήθως αυτόματα κάποιες διαδικασίες οι οποίες τροποποιούν δεδομένα σε διάφορα σημεία της μνήμης ή της συσκευής. Για την αποφυγή της αθέμιτης τροποποίησης των δεδομένων που εξετάζονται χρησιμοποιούνται συσκευές ή μέθοδοι απαγόρευσης εγγραφής (write blockers). Υπάρχουν διάφοροι τύποι τέτοιων συσκευών αλλά και κάποιες ανέξοδες μέθοδοι με τις οποίες απαγορεύεται η παρέμβαση του Λειτουργικού Συστήματος του Σταθμού Εργασίας Ψηφιακής Εγκληματολογίας.

Ο παρακάτω οδηγός [10], περιλαμβάνει μια προτεινόμενη σειρά τροποποιήσεων της Registry ενός υπολογιστή που φέρει Λειτουργικό Σύστημα Windows 7, με τις οποίες επιτυγχάνεται η απαγόρευση οποιασδήποτε εγγραφής από το Λειτουργικό Σύστημα του Σταθμού Εργασίας Ψηφιακής Εγκληματολογίας προς ένα μέσο ψηφιακών πειστηρίων το οποίο θα συνδεθεί σε μια θύρα τύπου USB. Πριν την εκτέλεση οποιασδήποτε αλλαγής στη Registry, θα πρέπει να δημιουργηθεί Σημείο Επαναφοράς, ώστε να είναι δυνατή η ανάκαμψη από οποιοδήποτε πρόβλημα.

1. Δημιουργία Σημείου Επαναφοράς

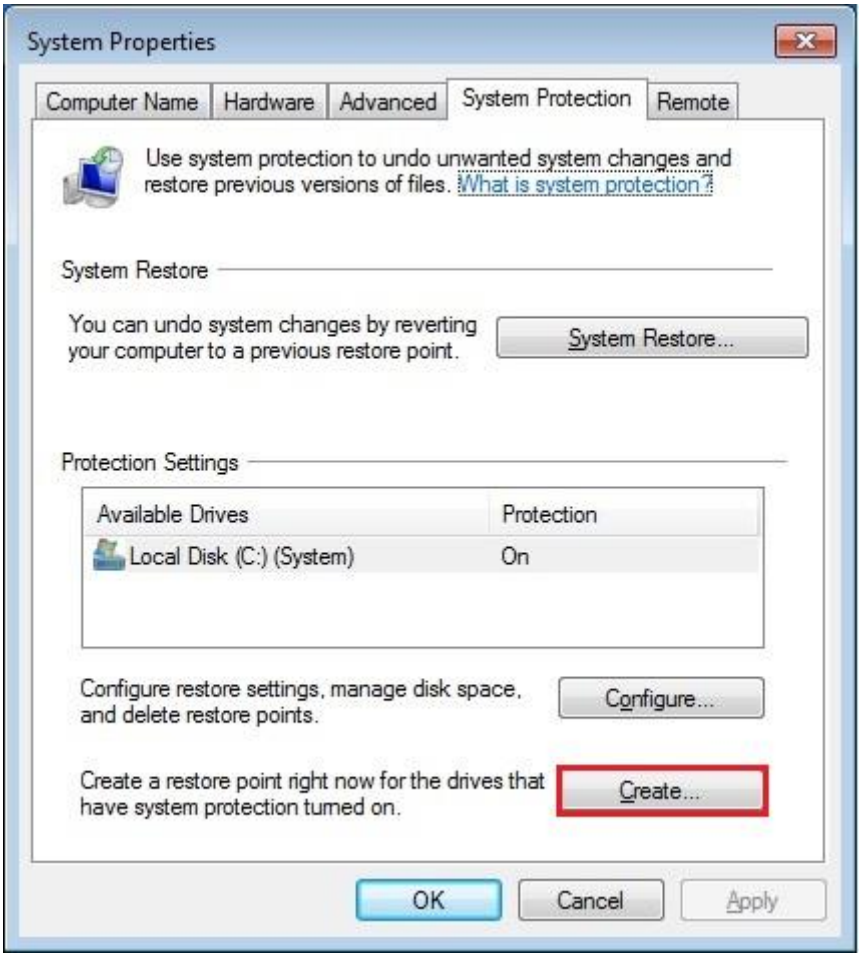
1.1 Επιλογή εικονιδίου **Start** , δεξί κλικ στην επιλογή **Computer** και κλικ στην επιλογή **Properties**.

1.2 Στην οθόνη που θα εμφανιστεί (εικ. Γ.1) επιλογή του **System protection**.



Εικόνα Γ.1 : Οθόνη Properties του Computer

1.3 Στην επόμενη οθόνη, επιλογή του **Create**, εισαγωγή ονόματος για το σημείο επαναφοράς (πχ. Restore point 1) και επιλογή **Close** για να τερματιστεί η διαδικασία.

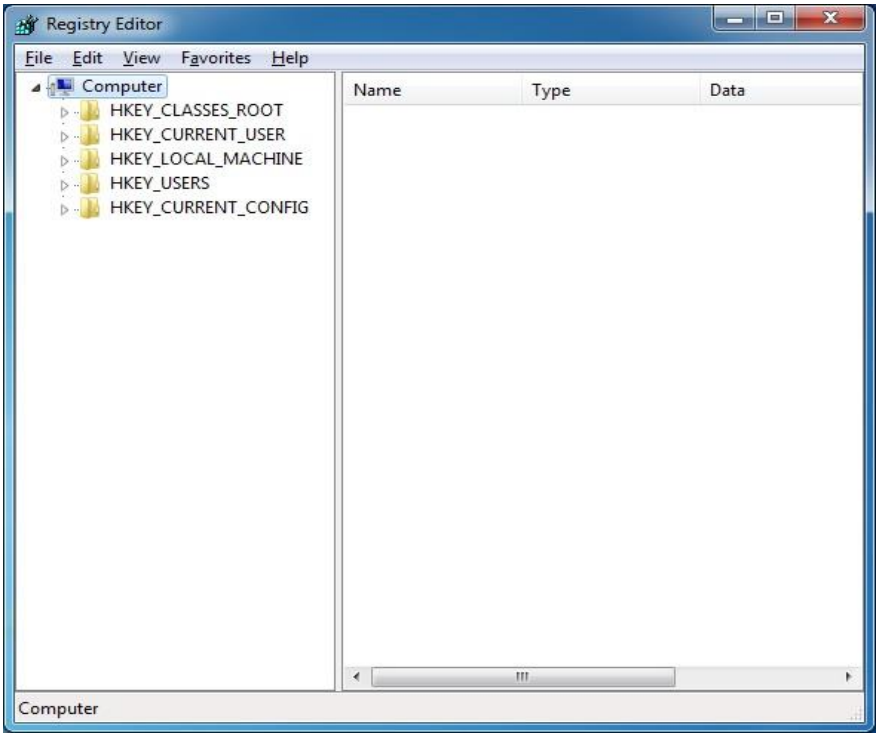


Εικόνα Γ.2 : Επιλογή System Protection και Δημιουργία Σημείου Επαναφοράς

2. Τροποποίηση της Registry

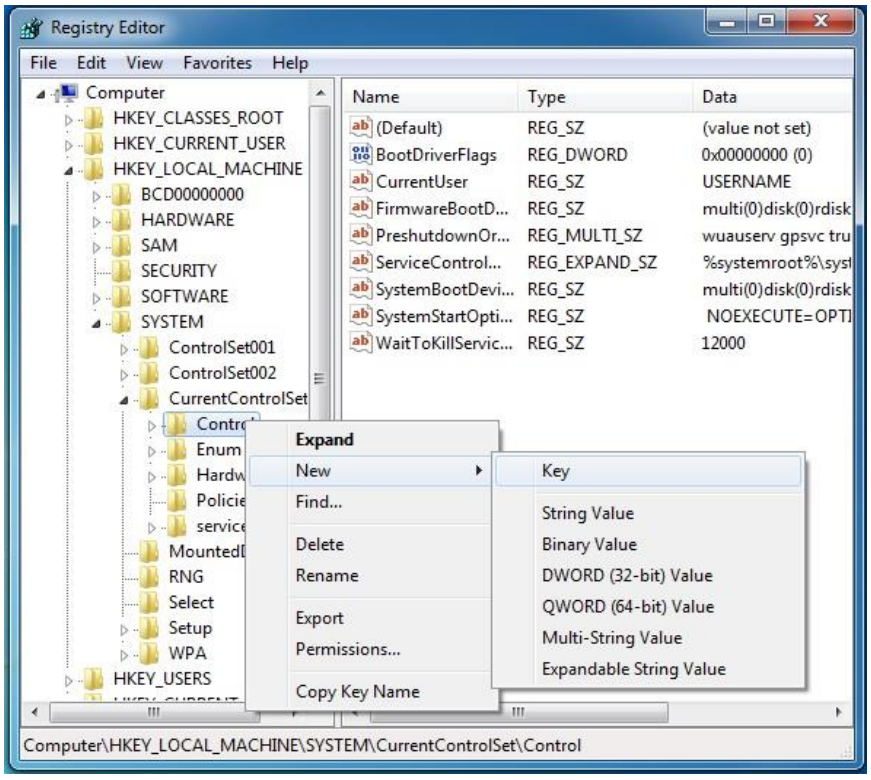
2.1 Επιλογή ξανά του εικονιδίου **Start** και στο πλαίσιο κειμένου πληκτρολόγηση της λέξης "**regedit**" και **Enter**, ώστε να εκκινήσει η λειτουργία του **Registry Editor** (εικ. Γ.3). Σε περίπτωση που εμφανιστεί ειδοποίηση **User Account Control (UAC)**, επιλογή **Yes** για συνέχεια.

2.2 Στον Registry Editor, επέκταση της διαδρομής **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet**.



Εικόνα Γ.3 : Λειτουργία Registry Editor

2.3. Κάτω από την επιλογή CurrentControlSet, δεξί κλικ στην επιλογή **Control** και στη συνέχεια στο υπομενού **New** επιλογή του **Key** (εικ. Γ.4). Πληκτρολόγηση ονόματος για το νέο κλειδί (πχ. StorageDevicePolicies).



Εικόνα Γ.4 : Δημιουργία Νέου Control Key στο CurrentControlSet

2.4 Δεξί κλικ στο νέο κλειδί με όνομα **StorageDevicePolicies** και στο υπομενού **New** επιλογή του **DWORD Value** (32 ή 64 bit ανάλογα την έκδοση του Λειτουργικού Συστήματος που χρησιμοποιείται). Πληκτρολόγηση ονόματος για το νέο χαρακτηριστικό (πχ. WriteProtect).

2.5 Στο δεξιό τμήμα του παραθύρου, δεξί κλικ στο χαρακτηριστικό **WriteProtect** και επιλογή του **Modify**.

2.6 Στο νέο παράθυρο **Edit DWORD Value**, αλλαγή του **Value data** από 0 σε **1**, ώστε να ενεργοποιηθεί η απαγόρευση εγγραφής σε συσκευές που θα συνδεθούν στον υπολογιστή μέσω μιας θύρας USB.

3. Αυτοματοποίηση Διαδικασίας

Προκειμένου να μην εκτελείται το σύνολο της παραπάνω διαδικασίας κάθε φορά που απαιτείται η απαγόρευση εγγραφής σε μια συσκευή, υπάρχει η επιλογή της Εξαγωγής της Registry με τα επιθυμητά κάθε φορά χαρακτηριστικά.

3.1 Δεξί κλικ στο κλειδί **StorageDevicePolicies** και επιλογή του **Export**.

3.2 Στο παράθυρο **Export Registry File** που θα εμφανιστεί, πληκτρολόγηση του ονόματος "**Write Protect USB ON**" και στη συνέχεια αποθήκευση στην Επιφάνεια Εργασίας (Desktop).

3.3 Επανάληψη της διαδικασίας που περιεγράφηκε στο βήμα 2 και στην ενέργεια 2.6 αλλαγή του **Value data** από 1 σε **0**, ώστε να απενεργοποιηθεί η απαγόρευση εγγραφής.

3.4 Δεξί κλικ στο κλειδί **StorageDevicePolicies** και επιλογή του **Export**.

3.5 Στο παράθυρο **Export Registry File** που θα εμφανιστεί, πληκτρολόγηση του ονόματος "**Write Protect USB OFF**" και στη συνέχεια αποθήκευση στην Επιφάνεια Εργασίας (Desktop).

Μετά το πέρας της διαδικασίας έχουν δημιουργηθεί δύο αρχεία τύπου .reg στην Επιφάνεια Εργασίας, τα οποία μπορούν να χρησιμοποιηθούν αναλόγως των αναγκών. Στην περίπτωση που πραγματοποιείται ανάλυση ψηφιακών πειστηρίων μέσω ενός φορέα που θα συνδεθεί σε κάποια από τις θύρες USB του Σταθμού Εργασίας Ψηφιακής Εγκληματολογίας, με τη χρήση του αρχείου Write Protect USB ON απαγορεύεται οποιαδήποτε εγγραφή, εξασφαλίζοντας έτσι την ακεραιότητα των στοιχείων που αναλύονται. Για επαναφορά στην προηγούμενη κατάσταση και άρση της απαγόρευσης επιλέγεται το αρχείο Write Protect USB OFF.