ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων σε Μικρομεσαίες Επιχειρήσεις

Ονοματεπώνυμο φοιτητή: Καψαρίδη Παναγιώτα

ΑΜ: 8468

Επιβλέπων καθηγητής: Ντεμίρης Κωνσταντίνος

ΠΑΤΡΑ 2012

ΠΕΡΙΛΗΨΗ

Στην σύγχρονη εποχή, στα πλαίσια του συνεχώς αυξανόμενου ανταγωνισμού στον τομέα των επιχειρήσεων και της επανάστασης της συνδεσιμότητας, η χρήση των *Πληροφοριακών Συστημάτων (Information Systems - IT)* θεωρείται δεδομένη για κάθε οργανισμό. Η ελεύθερη ροή πληροφοριών, οι ευκολίες που παρέχει το Διαδίκτυο (Internet) καθώς και το ηλεκτρονικό εμπόριο έχουν ωθήσει μέχρι και τις μικρότερες επιχειρήσεις να επενδύσουν στην χρήση πληροφοριακών συστημάτων και διαδικτυακών εφαρμογών.

Στο μεγαλύτερο ποσοστό των επιχειρήσεων, η χρήση των πληροφοριακών συστημάτων κρίνεται απολύτως αναγκαία για την βιώσιμη ανάπτυξη και εξέλιξή τους, την επίτευξη των στόχων και της βασικής λειτουργικότητας τους. Ως αποτέλεσμα, η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος, είτε από άμεσες οικονομικές απώλειες, είτε από την αδυναμία της επιχείρησης να λειτουργήσει αποδοτικά. Δίχως αμφιβολία λοιπόν, η ασφάλεια των πληροφοριακών συστημάτων και των δικτύων αποκτά τεράστια σημασία στην σύγχρονη κοινωνία, διαδραματίζοντας πρωτεύον ρόλο κατά την σχεδίαση, συντήρηση και χρήση τους.

Η συγκεκριμένη μελέτη αποτελεί μέρος ενός ευρύτερου ερευνητικού έργου που σκοπό έχει να παράσχει μια απλουστευμένη και συνολική θεώρηση της Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύων στις Μικρομεσαίες Επιχειρήσεις (ΜΜΕ), παρουσιάζοντας μια γενική εικόνα γύρω από το status quo της ασφάλειας.

Η εργασία δεν γράφτηκε με σκοπό να λύσει οποιοδήποτε πρόβλημα ασφάλειας, καθώς δεν αναλώνεται σε τεχνικές αναλύσεις ή διεξοδικές περιγραφές. Είναι γενικής φύσεως και τα περισσότερα θέματα αναλύονται περιληπτικά, έχοντας κατά νου να ευαισθητοποιήσει τον μέσο χρήστη και να του μεταδώσει μια ιδέα γνώσης πάνω στο ενδιαφέρον, πολύπλευρο, συνεχώς μεταβαλλόμενο και πάντα επίκαιρο θέμα της ασφάλειας των πληροφοριακών συστημάτων.

Η εργασία κρίνεται ότι θα έχει εκπληρώσει με επιτυχία το στόχο της, αν το περιεχόμενό της χαρακτηριστεί απλό, κατανοητό και ακριβές από τον αναγνώστη. Εξίσου σημαντικός στόχος είναι η αποδοχή του περιεχομένου της από τους γνωρίζοντες με την πληροφοριακή ασφάλεια, αλλά κυρίως από τους μη ειδικούς.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Πώς έχει επηρεάσει η τεχνολογία των δικτύων και των πληροφοριακών συστημάτων τη ζωή μας και πώς έχει επιδράσει την επιχειρηματικότητα, την οικονομία, την επικοινωνία και την καθημερινότητά μας;

Πολύ θετικά, θα απαντήσουν οι περισσότεροι με μια πρώτη σκέψη. Πράγματι, η θετική επιρροή του Internet, εξαιρετικά δύσκολα μπορεί να αμφισβητηθεί. Οι Αρχαίοι Έλληνες από την άλλη, έλεγαν «ουδέν καλόν αμιγές κακού» για να επιβεβαιωθούν ακόμη και στην περίπτωση των νέων τεχνολογιών. Το Διαδίκτυο έφερε πολλά καλά, και κάπου μέσα σε αυτόν τον σωρό των καλών, έφερε και τα άσχημα.

Η ασφάλεια στο διαδίκτυο οριοθετείται αφενός, όπως και στην πραγματική ζωή, με την επιβολή μέτρων και κανόνων, αφετέρου με τη χρήση του όπλου της τεχνολογίας, αναπτύσσοντας τα κατάλληλα λογισμικά και θέτοντάς τα λειτουργία.

Στην παρούσα εργασία, παρουσιάζονται – ανά κεφάλαιο – τα εξής:

Το πρώτο κεφάλαιο περιέχει μια εκτενής αναφορά σε θέματα γενικά περί ασφάλειας. Περιγράφονται τα πληροφοριακά συστήματα, τα δίκτυα υπολογιστών και οι κυριότερες απαιτήσεις-ανάγκες που καλούνται νια εκπληρώσουν. Εισάγονται οι όροι ασφάλεια, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα και καταγράφονται οι απαιτήσεις σε θέματα ασφαλείας. Επίσης, αναλύεται η έννοια της ανάλυση κινδύνων, οι άξονες στους οποίους κινείται και η βασική μεθοδολογία που υιοθετεί. Τέλος, αναφέρονται κατηγορίες πιθανών περιστατικών παραβίασης ασφαλείας και ενέργειες αντιμετώπισης αυτών.

Το δεύτερο κεφάλαιο περιέχει αναφορά στους κινδύνους ασφαλείας των πληροφοριακών συστημάτων και των δικτύων. Περιγράφονται προβλήματα ασφαλείας και προσδιορίζονται λόγοι και αιτίες που καθιστούν ανασφαλή τα συστήματα υπολογιστών. Περιέχονται αναφορές στους hackers, στους εισβολείς και στις διάφορες κατηγορίες λογισμικού που χρησιμοποιείται για την κατάλυση της ασφάλειας των συστημάτων. Επιπλέον, παρουσιάζονται τρόποι εργασίας και τεχνικές εισβολής με τους οποίες απειλείται η ασφάλεια των δικτύων μιας επιχείρησης.

Το τρίτο κεφάλαιο περιέχει την έννοια της πολιτικής ασφαλείας περιγράφοντας τα βασικά χαρακτηριστικά της και τα περιεχόμενα που πρέπει να διαθέτει. Παρουσιάζονται οι γενικοί άξονες που διαμορφώνουν μια πολιτική ασφαλείας, οι απαιτήσεις που πρέπει να εκπληρώνονται, καθώς και οι εμπλεκόμενοι στη σύνταξη της πολιτικής ασφαλείας μιας επιχείρησης. Γίνεται ιδιαίτερη αναφορά στην εκπαίδευση των χρηστών σε θέματα ασφαλείας, και στη διαχείριση της επιχειρησιακής συνέχειας με τις διαδικασίες που πρέπει να ακολουθούνται. Τέλος, αναφέρονται παράγοντες που εξασφαλίζουν την ασφάλεια δικτύων και πληροφοριών μέσα σε έναν οργανισμό.

Το τέταρτο κεφάλαιο ασχολείται με τις μικρομεσαίες επιχειρήσεις. Περιέχει μια απλουστευμένη και συνολική θεώρηση της διαχείρισης και της εκτίμησης κινδύνων στις μικρομεσαίες επιχειρήσεις. Περιγράφονται προσεγγίσεις ανάθεσης της εκτίμησης κινδύνων, καθώς και μια προτεινόμενη διαδικασία εκτίμησης κινδύνων που διαρθρώνεται μέσω μιας απλουστευμένης προσέγγισης εκτίμησης τεσσάρων φάσεων. Επίσης, παρουσιάζονται απλές συμβουλές και σημαντικές υποδείξεις ασφαλείας για τις μικρομεσαίες επιχειρήσεις.

Το πέμπτο κεφάλαιο περιέχει την έρευνα που πραγματοποιήθηκε για τις ανάγκες της εργασίας. Περιγράφονται οι στόχοι της έρευνας και οι κύριες κατηγορίες θεμάτων που εξετάζει. Αναλύονται τα αποτελέσματα της έρευνας με ιδιαίτερη έμφαση στα μέτρα ασφαλείας, στα προσωπικά δεδομένα και στα οικονομικά στοιχεία που εξάγει.

Το έκτο κεφάλαιο περιλαμβάνει τα συμπεράσματα και τις μελλοντικές επεκτάσεις που πηγάζουν από το σύνολο της εργασίας.

Για την διενέργεια της έρευνας και την επιτυχή εκπλήρωση των σκοπών και επιμέρους στόχων της μελέτης χρησιμοποιήθηκαν τα παρακάτω στοιχεία:

Για την θεωρητική προσέγγιση, χρησιμοποιήθηκε το Διαδίκτυο ως βασικότερο εργαλείο σε συνδυασμό με το σύνολο της υπάρχουσας βιβλιογραφίας και αρθρογραφίας που ήταν δυνατόν να συγκεντρωθεί με κάθε επιφύλαξη ως προς το εύρος πρόσβασης σ’ αυτή.

Για την έρευνα, χρησιμοποιήθηκε ανάλυση περιεχομένου από μικρομεσαίες επιχειρήσεις του ελληνικού επιχειρηματικού τομέα με την ανάλυση και την αξιολόγηση του ερωτηματολογίου που δημιουργήθηκε για το σκοπό της μελέτης.

ΚΕΦΑΛΑΙΟ 1

ΓΕΝΙΚΑ ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ

Η εισαγωγή νέων τεχνολογιών και του διαδικτύου στο παγκόσμιο γίγνεσθαι επέφερε σημαντικές αλλαγές στη ζωή μας τόσο σε επαγγελματικό όσο και σε κοινωνικό επίπεδο. Νέοι τρόποι οργάνωσης της ζωής, επικοινωνίας, πρόσβασης στη γνώση, παραγωγής και επιχειρηματικότητας. Η καθημερινότητά μας πια είναι αναπόσπαστο κομμάτι των νέων τεχνολογιών και η βελτίωση της, τουλάχιστον σε σχέση με αυτά, είναι εμφανής.

Η ψηφιακή εποχή που βιώνουμε σήμερα, είναι η λογική κατάληξη μιας σειράς τεχνολογικών καινοτομιών. Η έξαρση της χρήσης αυτών των καινοτομιών σήμερα έχει ως αποτέλεσμα να ονομάζεται η σημερινή εποχή, ως εποχή των πληροφοριών. Βασικοί προσδιοριστικοί παράγοντες της εποχής αυτής είναι η δυνατότητα διαχείρισης πληροφοριών και γνώσεων.

1.1. Πληροφοριακά συστήματα

Τα πληροφοριακά συστήματα αποτελούν ένα σύνολο διαδικασιών, ανθρώπινου δυναμικού και αυτοματοποιημένων υπολογιστικών συστημάτων, τα οποία προορίζονται για τη συλλογή, επεξεργασία, ανάκτηση, αποθήκευση καθώς και ανάλυση πληροφοριών. Αναγνωρίζονται ως γέφυρα μεταξύ των πρακτικών εφαρμογών της επιστήμης υπολογιστών και του επιχειρηματικού κόσμου, αποτελώντας το μέσο για την αρμονική συνεργασία ανθρώπινου δυναμικού, δεδομένων, διαδικασιών και τεχνολογιών πληροφορίας και επικοινωνιών.

Ένα πληροφοριακό σύστημα μπορεί να περιλαμβάνει υλικό (hardware), λογισμικό (software) και τηλεπικοινωνιακό σκέλος, αντιπροσωπεύει μια σημαντική οικονομική επένδυση μιας επιχείρησης και στηρίζεται στην πληροφορική, έναν τομέα που χαρακτηρίζεται από μεγάλο ρυθμό ανάπτυξης. Καθώς οι εξελίξεις είναι εξαιρετικά γρήγορες, οι κίνδυνοι για τα συστήματα αυτά δεν είναι δυνατό ποτέ να εξαλειφθούν. Η εισαγωγή πληροφοριακών συστημάτων σε ένα περιβάλλον μπορεί μεν να αυξάνει κατακόρυφα την παραγωγικότητα και το κέρδος, αλλά εισάγει νέους κινδύνους που αυξάνουν σημαντικά το ρίσκο και επομένως πρέπει οπωσδήποτε να αναγνωριστούν και να αντιμετωπιστούν ανάλογα.

Τα συστήματα αυτά σχετίζονται διπλά με τον ανθρώπινο παράγοντα, καθώς δημιουργούνται από αυτόν για να τον υπηρετήσουν στη συνέχεια[1]. Η ανθρώπινη φύση όμως προδιαγράφει συμπεριφορές οι οποίες δύσκολα μπορούν να εκτιμηθούν ή να προβλεφθούν, καθώς κανείς δεν μπορεί να εγγυηθεί ότι οι ίδιοι άνθρωποι κάτω από τις ίδιες συνθήκες θα παρουσιάσουν την ίδια συμπεριφορά. Επιπλέον, τα πληροφοριακά συστήματα σχετίζονται με την πληροφορία, ένα αγαθό με ιδιαίτερα μεγάλη ζήτηση που παρουσιάζει την ιδιαιτερότητα ότι μπορεί να αναπαραχθεί άπειρες φορές χωρίς να αλλοιωθεί το πρωτότυπό της. Συνεπώς, οποιαδήποτε κλοπή της πληροφορίας δε μπορεί να γίνει εύκολα αντιληπτή.

Στην δεκαετία του ’80, όταν τα πληροφοριακά συστήματα άρχισαν σιγά σιγά να διεισδύουν στις μεσαίες και μεγάλες επιχειρήσεις, οι άνθρωποι που ήξεραν να τα χειρίζονται ήταν λίγοι και εξειδικευμένοι και τα φαινόμενα παραβίασης της ασφάλειας ήταν σχεδόν ανύπαρκτα. Κατά την διάρκεια της δεκαετίας του ’90 και μέχρι σήμερα, οι νέες τεχνολογίες οδήγησαν σε ευρεία χρήση των ηλεκτρονικών υπολογιστών με αποτέλεσμα ο αριθμός των παραβιάσεων ασφαλείας να ακολουθεί μια συνεχή εκθετική αύξηση.

Η ασφάλεια των υπολογιστικών συστημάτων δεν αποτελεί αυτοσκοπό, αλλά το μέσο για ένα καθολικό σκοπό, την ασφάλεια της πληροφορίας [3]. Δεν αποτελεί ένα σύνολο κόλπων και τεχνικών, αλλά μια αναπτυσσόμενη περιοχή ειδίκευσης [2]. Οι ηλεκτρονικοί παλμοί των άσσων και των μηδενικών τώρα πια συντηρούν την ύπαρξή μας και τα πληροφοριακά συστήματα αποτελούν το ζωοδόχο αίμα της μοντέρνας κοινωνίας. Οι ψηφιακοί αυτοί παλμοί τρέφουν την σχεδόν βιολογική μας εξάρτηση επί της στιγμιαίας ηλεκτρονικής συναναστροφής. Οι ηλεκτρονικοί υπολογιστές έφεραν επανάσταση στον τρόπο σκέψης και στον τρόπο δουλειάς, επηρέασαν σε βάθος την σύγχρονη ζωή και τα συλλογικά ενδιαφέροντα. Πώς θα ήταν δυνατόν να μην επηρεάσουν τις μορφές εγκληματικότητας, το νόμο, αλλά και τα προβλήματα όσων έρχονται αντιμέτωποι με την εγκληματικότητα;

Ο κλάδος της ασφάλειας πληροφοριακών συστημάτων έχει να προσφέρει ευτυχώς μια πληθώρα από αντίμετρα (εργαλεία, μεθόδους, έλεγχους, πολιτικές ασφαλείας) για την αντιμετώπιση κάθε είδους προβλήματος. Η ενσωμάτωση όμως όλων αυτών σε κάθε οργανισμό δεν είναι καθόλου απλή υπόθεση. Αντιθέτως, ο διαφορετικός τρόπος λειτουργίας καθώς και η διαφορετική ανάθεση πόρων για θέματα ασφαλείας δημιουργούν εντελώς διαφορετικές συνθήκες, μοναδικές για κάθε οργανισμό. Η ενσωμάτωση της ασφάλειας λοιπόν δεν πρέπει να θεωρηθεί ως μια απλή διαδικασία, καθώς πρέπει κάθε φορά να λαμβάνονται υπόψη όλοι οι παράγοντες ώστε η ασφάλεια να μην αποτελεί εμπόδιο στην λειτουργία του οργανισμού αλλά να τον υπηρετεί.

1.2. Δίκτυα

Στα πρώτα μοντέλα υπολογιστικών συστημάτων που χρησιμοποιήθηκαν από επιχειρήσεις, ο καθένας από τους υπολογιστές αυτούς μπορούσε να αξιοποιείται ξεχωριστά από τους υπόλοιπους. Με την πάροδο όμως των χρόνων και την αλματώδη ανάπτυξη τόσο της πληροφορικής όσο και των τηλεπικοινωνιών οι επιχειρήσεις και οι άλλοτε μικρομεσαίες επιχειρήσεις άρχισαν να αποκτούν άμεση πρόσβαση στην πληροφορία, να γιγαντώνονται με αποτέλεσμα να προκύπτει το πρόβλημα του ορθού καταμερισμού των πόρων. Οι διοικήσεις αυτών των επιχειρήσεων αποφάσισαν την διασύνδεση όλων των υπολογιστών με στόχο αφενός μεν να καταστούν διαθέσιμα όλα τα προγράμματα, ο εξοπλισμός και προπάντων τα δεδομένα σε οποιονδήποτε στο δίκτυο ανεξαρτήτου φυσικής θέσεως του πόρου και του χρήστη, αφετέρου δε την απόκτηση της δυνατότητας εξαγωγής και συσχέτισης πληροφοριών που αφορούν ολόκληρη την επιχείρηση.

Με τον όρο δίκτυο υπολογιστών εννοείται ένα σύνολο αυτόνομων ή μη αυτόνομων διασυνδεδεμένων υπολογιστών. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι δυνατό κάποιος εξ αυτών να ελέγξει τη λειτουργία κάποιου άλλου. Τα δίκτυα είναι συστήματα μέσω των οποία τα δεδομένα κυκλοφορούν, αποθηκεύονται και υφίστανται επεξεργασία. Αποτελούνται από συστατικά στοιχεία μεταφοράς (καλώδια, δρομολογητές, πύλες, κλπ.), και υπηρεσίες υποστήριξης (σύστημα ονομάτων τομέα και των βασικών εξυπηρετητών, υπηρεσία αναγνώρισης

καλούντος, ελέγχου ταυτότητας κλπ.). Συνδεδεμένο με τα δίκτυα είναι ένα αυξανόμενο ευρύ φάσμα εφαρμογών (συστήματα διανομής ηλεκτρονικού ταχυδρομείου, φυλλομετρητές, κλπ.) και τερματικού εξοπλισμού (τηλεφωνικές συσκευές, υπολογιστές υπηρεσίας, προσωπικοί υπολογιστές, κινητά τηλέφωνα, ηλεκτρονικές ατζέντες. οικιακές συσκευές, βιομηχανικές μηχανές, κλπ.).

Οι κυριότερες απαιτήσεις που καλείται να εκπληρώσει ένα σύγχρονο δίκτυο είναι ο διαμοιρασμός υπολογιστικών πόρων (προγράμματα, δεδομένα, περιφερειακά), η παροχή υψηλής αξιοπιστίας, η μείωση του κόστους και η επικοινωνία μεταξύ των χρηστών. Με την αλματώδη ανάπτυξη της τεχνολογίας σε μέσα μετάδοσης όπως οι οπτικές ίνες, σε ασύρματα δίκτυα, σε τεχνικές μεταγωγής και κόμβους υψηλών ταχυτήτων, δημιουργούνται συνεχώς νέα δίκτυα και υπηρεσίες όπως video on demand, βιντεοτηλεφωνία, επικοινωνίες πολυμέσων κλπ. Η επανάσταση των δικτύων, είναι η επέκταση των ψηφιακών ασύρματων επικοινωνιών υψηλών ταχυτήτων που επιτρέπουν την πρόσβαση σε φορητά τερματικά πολυμέσων, αλλάζοντας την μορφή των δικτύων καθώς τα σύγχρονα τερματικά σημεία τους δεν εξαρτώνται από το που καταλήγει το καλώδιο, αλλά έχουν την ελευθερία κίνησης που προσφέρει η ασύρματη επικοινωνία.

Η μεγάλη ανάπτυξή τους έχει επηρεάσει πλέον την καθημερινή ζωή εκατομμυρίων ανθρώπων μέσα από τη ραγδαία εξάπλωση του Internet. Σήμερα το Internet έχει δημιουργήσει παγκόσμια συνδεσιμότητα, φέροντας σε επαφή εκατομμύρια δικτύων, μεγάλων και μικρών, με εκατοντάδες εκατομμύρια μεμονωμένους προσωπικούς υπολογιστές και, σε αυξανόμενο βαθμό, άλλες διατάξεις. Οι σημερινές τεχνολογικές εξελίξεις επιτρέπουν την υπόθεση ότι ο υπολογιστής του μέλλοντος δεν θα είναι παρά ένα στοιχείο του Διαδικτύου, το οποίο θα παίζει το ρόλο της διασύνδεσης (interface) ανάμεσα στον χρήστη και στο σύνολο των παρεχόμενων από το Διαδίκτυο πληροφοριών, με δυνατότητα πρόσβασης στην "καθολική βιβλιοθήκη της γνώσης".[4] Όμως αυτή η προσφερόμενη δυνατότητα όπου ο καθένας με μια φθηνή τερματική συσκευή όπως ένας υπολογιστής, μπορεί να επικοινωνεί με άλλους υπολογιστές, δημιουργεί και μεγάλα προβλήματα. Απαιτείται μεγάλη προσοχή, σαφείς κανόνες, μεγάλη αυστηρότητα και συνεπώς μεγάλη πολυπλοκότητα για να εξασφαλισθεί η με σαφείς όρους συμμετοχή του καθενός σε ένα τέτοιο δίκτυο. Η φύση του ανθρώπινου παράγοντα εξασφαλίζει ότι τα πράγματα δεν είναι πάντα έτσι.

1.3. Ασφάλεια

Σε γενικές γραμμές, η ασφάλεια αποτελεί μια ανταλλαγή με την ευκολία χρήσης, και οι περισσότεροι άνθρωποι δεν είναι διατεθειμένοι να παραμερίσουν την ευκολία της απομακρυσμένης χρήσης υπολογιστών μέσω δικτύων. Αναπόφευκτα, υποφέρουν από κάποια μορφή απώλειας ασφάλειας[3]. "Ένα πληροφοριακό σύστημα είναι ασφαλές αν μπορείς να εξαρτηθείς από αυτό και το λογισμικό του, και περιμένεις να συμπεριφερθεί όπως θα έπρεπε".

Ο λόγος για τον οποίο παρέχονται μέτρα προστασίας σε ένα δίκτυο είναι ένας και μοναδικός: η ασφάλεια. Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα πληροφοριακά συστήματα και στα δίκτυα υπολογιστών. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως παράλληλα σημαντικά τα προβλήματα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών. Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας όπως η ποιότητα και η απόδοση, για την εξασφάλιση της εύρυθμης λειτουργίας μιας επιχείρησης ή ενός οργανισμού.

Σήμερα όλα σχεδόν τα υπολογιστικά συστήματα είναι δικτυωμένα μέσω του Internet ή μέσω άλλων μικρότερων δικτύων. Αυτή η εξέλιξη εκτός από τα τεράστια πλεονεκτήματα που προφανώς προσφέρει έχει δημιουργήσει και σημαντικούς κινδύνους οι οποίοι εγείρουν το ζήτημα της ασφάλειας των δικτύων και των πληροφοριών που αυτά ανταλλάσσουν. Δεν πρέπει να ξεχνάμε άλλωστε, ότι η πληροφορία είναι ένας πόρος, ένα περιουσιακό στοιχείο, που όπως και όλα τα άλλα περιουσιακά στοιχεία έχει αξία για έναν οργανισμό και κατά συνέπεια χρειάζεται επαρκή προστασία. Η ασφάλεια των πληροφοριών τις προστατεύει από ένα σύνολο απειλών, ώστε να διασφαλίσει την επιχειρησιακή συνέχεια, να ελαχιστοποιήσει τη ζημιά σε μια επιχείρηση και να μεγιστοποιήσει τις επιχειρηματικές ευκαιρίες και την απόδοση. Το θέμα της ασφάλειας, λοιπόν, βρίσκεται πλέον σε κρίσιμο σημείο, συνιστώντας προαπαιτούμενο για την ανάπτυξη των ηλεκτρονικών συναλλαγών και για τη λειτουργία ολόκληρης της οικονομίας.

Αν θέλουμε να δώσουμε έναν ορισμό, τότε θα λέγαμε πως η ασφάλεια πληροφοριακού συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του πληροφοριακού συστήματος, αλλά και το σύστημα ολόκληρο από κάθε σκόπιμη ή τυχαία απειλή[5].

Η έννοια της ασφάλειας ενός δικτύου υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου.

Σύμφωνα με τον προηγούμενο ορισμό της ασφάλειας, η ασφάλεια στα δίκτυα υπολογιστών έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών καθώς και την λήψη μέτρων.

Ποιο συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με[6]:

- *Πρόληψη (prevention)*: την λήψη μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών.
- *Ανίχνευση (detection)*: την λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες.
- *Αντίδραση (reaction)*: την λήψη μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου.

Η ασφάλεια δικτύων και πληροφοριών μπορεί ακόμη να οριστεί ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Συμπερασματικά, η ασφάλεια καθίσταται βασική προτεραιότητα επειδή ακριβώς οι πληροφορίες και οι επικοινωνίες έχουν αποβεί βασικός παράγοντας στην οικονομική και κοινωνική εξέλιξη. Τα πληροφοριακά συστήματα και τα δίκτυα υποστηρίζουν σήμερα υπηρεσίες και μεταφορά δεδομένων σε βαθμό που μέχρι πριν από λίγα χρόνια θεωρείτο αδιανόητος, με την ύπαρξη και τη διάθεσή τους να είναι καθοριστικής σημασίας για άλλες υποδομές. Δεδομένου ότι άπαντες, επιχειρήσεις, ιδιώτες, δημόσιες διοικήσεις, επιθυμούν να εκμεταλλευθούν τις δυνατότητες που παρέχουν τα δίκτυα επικοινωνιών, η ασφάλεια των εν λόγω συστημάτων καθίσταται προαπαιτούμενο της περαιτέρω προόδου.

1.4. Απαιτήσεις Ασφάλειας

1.4.1.Βασικές ιδιότητες ασφάλειας

Είναι γενικά αποδεκτό σήμερα ότι η έννοια της ασφάλειας των δικτύων υπολογιστών αλλά και των πληροφοριακών συστημάτων γενικότερα, συνδέεται στενά με τρεις βασικές έννοιες[7]:

- *Διαθεσιμότητα (Availability):* διασφάλιση της προσπελασιμότητας της πληροφορίας σε εξουσιοδοτημένους χρήστες όποτε απαιτείται. Μία βασική επιδίωξη της πολιτικής προστασίας πρέπει να είναι η εξασφάλιση ότι η πληροφορία είναι πάντα διαθέσιμη για την υποστήριξη της ομαλής εξέλιξης της επιχειρηματικής δραστηριότητας.

- *Εμπιστευτικότητα (Confidentiality)*: διασφάλιση της προσπελασιμότητας της πληροφορίας μόνον από όσους έχουν τα απαραίτητα δικαιώματα. Εξασφαλίζεται έτσι ότι οι πολύτιμες πληροφορίες και τα δεδομένα παραμένουν στην δικαιοδοσία μόνον αυτών που έχουν την εξουσιοδότηση να τα προσπελάσουν.

- *Ακεραιότητα (Integrity)*: διαφύλαξη της ακρίβειας και της πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας αυτής. Η πληροφορία έχει αξία μόνον εάν γνωρίζουμε ότι είναι σωστή και ακριβής. Βασική επιδίωξη της πολιτικής προστασίας είναι ότι δεν πρόκειται η πληροφορία να τροποποιηθεί ή να καταστραφεί με κανέναν τρόπο.

Ασφαλής επικοινωνία μεταξύ δύο μερών νοείται κάθε μορφή επικοινωνίας που γίνεται με χρήση ψηφιακής τεχνολογίας και εξασφαλίζει την διαθεσιμότητα, εμπιστευτικότητα και ακεραιότητα των πληροφοριών που διακινούνται μέσω ενός τηλεπικοινωνιακού δικτύου. Αυτές οι ιδιότητες–απαιτήσεις μπορούν να διατυπωθούν με τα παραπάνω, αλληλένδετα χαρακτηριστικά και έχουν το εξής περιεχόμενο:

α) Διαθεσιμότητα

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Με τον όρο διαθεσιμότητα εννοείται ότι τα δεδομένα είναι προσβάσιμα και οι υπηρεσίες λειτουργούν, παρά τις όποιες τυχόν διαταραχές, όπως διακοπή τροφοδοσίας, φυσικές καταστροφές, ατυχήματα ή επιθέσεις. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των υπολογιστών του δικτύου δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν τους πόρους του δικτύου.

Για τους σκοπούς της ασφάλειας, βασικό μέλημα αποτελεί η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στην παρακώλυση της πρόσβασης των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών. Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο. Η αντιμετώπισή τους αποσκοπεί στο να υπερνικήσει την σκόπιμη, που προκαλείται από κακόβουλα μέρη, παρά τυχαία απώλεια της διαθεσιμότητας.

Παρόλο που η διαθεσιμότητα συχνά αναδεικνύεται στο πλέον σημαντικό χαρακτηριστικό της ασφάλειας, εντούτοις λίγοι μηχανισμοί υπάρχουν για να βοηθήσουν στην υποστήριξή της.

β) Εμπιστευτικότητα

Σε πολλές περιπτώσεις της καθημερινής ζωής οι έννοιες της ασφάλειας και της εμπιστευτικότητας σχεδόν ταυτίζονται, όπως για παράδειγμα σε περιβάλλοντα όπου η ασφάλεια έχει τη σημασία του να κρατούνται μυστικές οι πληροφορίες.

Εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν.

Άλλες εκφάνσεις της εμπιστευτικότητας είναι η ιδιωτικότητα που αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα, και η μυστικότητα που αφορά την προστασία των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση.

γ) Ακεραιότητα

Πρόκειται για την επιβεβαίωση ότι τα δεδομένα που έχουν αποσταλεί, παραληφθεί ή αποθηκευτεί είναι πλήρη και δεν έχουν υποστεί αλλοίωση. Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, που σημαίνει πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων. Αυτό σημαίνει ότι η δημιουργία, μετατροπή και διαγραφή των δεδομένων ενός υπολογιστικού συστήματος, πραγματοποιείται μόνο από εξουσιοδοτημένα μέρη. [6]

1.4.2.Καταγραφή απαιτήσεων ασφάλειας

Προκειμένου μια επιχείρηση να αποκτήσει σαφή εικόνα των κινδύνων ασφαλείας που αντιμετωπίζει το δίκτυο υπολογιστών της, πρωταρχική σημασία έχει η αναγνώριση των υποχρεώσεων και των πραγματικών απαιτήσεων σε θέματα ασφαλείας για την εξασφάλιση ασφαλών επικοινωνιών μέσω του δικτύου της. Υπάρχουν τρεις κύριες πηγές για το σκοπό αυτό [8]:

- Η αποτίμηση των κινδύνων που αντιμετωπίζει η επιχείρηση. Μέσω αυτής της διαδικασίας αναγνωρίζονται οι πιθανές απειλές προς την επιχείρηση, υπολογίζεται η ευπάθεια της στις συγκεκριμένες απειλές, η πιθανότητα υλοποίησής τους καθώς και το κόστος που θα έχουν για την επιχείρηση.

- Το νομικό πλαίσιο και οι συμβατικές υποχρεώσεις της επιχείρησης απέναντι στο κράτος, το προσωπικό και τους συνεργάτες της.

- Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει η ίδια η επιχείρηση σχετικά με την επεξεργασία των πληροφοριών που είναι απαραίτητες στη λειτουργία της.

Ένας αριθμός απαιτήσεων ελέγχου και προστασίας θεωρείται θεμελιώδης για την ασφάλεια των πληροφοριών σε κάθε επιχείρηση. Αυτές, είτε βασίζονται σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική σε θέματα ασφάλειας.

Απαιτήσεις απαραίτητες σε μια επιχείρηση, που βασίζονται στη νομοθεσία, είναι η διαφύλαξη των προσωπικών δεδομένων, η διαφύλαξη των δεδομένων της επιχείρησης και τα δικαιώματα πνευματικής ιδιοκτησίας. Απαιτήσεις που έχουν καθιερωθεί ως κοινή πρακτική είναι η εκπόνηση σχεδίου ασφαλείας, ο καταμερισμός καθηκόντων σχετικών με την ασφάλεια, η εκπαίδευση σε θέματα ασφάλειας, η αναφορά συμβάντων και η διαχείριση της επιχειρησιακής συνέχειας.

Σε περίπτωση που μία επιχείρηση επιθυμεί να καταγράψει και να αντιμετωπίσει τα προβλήματα ασφάλειας που υπάρχουν, μπορεί να ακολουθήσει διάφορες στρατηγικές. Αν η επιχείρηση είναι μικρής κλίμακας, μπορεί να εφαρμόσει κατευθείαν τη βασική προσέγγιση, στα πλαίσια της οποίας επιλέγονται απευθείας βασικά μέτρα προστασίας, τα οποία είναι ευρέως γνωστά από υπάρχοντες κώδικες ακολουθητέας πρακτικής σε διεθνές επίπεδο. Αν η επιχείρηση είναι μεγαλύτερη και τα πληροφοριακά συστήματα έχουν ιδιαίτερη σημασία για τη λειτουργία της, για την αποτελεσματική και ολοκληρωμένη καταγραφή των προβλημάτων ασφαλείας που δυνητικά αντιμετωπίζει, ως επαρκέστερη επιστημονικά μμέθοδος προτείνεται η εκπόνηση λεπτομερούς μελέτης ανάλυσης και διαχείρισης επικινδυνότητας με χρήση πρότυπης αυτοματοποιημένης μμεθοδολογίας, από έμπειρους μελετητές.

Στα πλαίσια της μελέτης αυτής, αρχικά καταγράφονται λεπτομερώς και αποτιμώνται συγκριτικά τα μέλη που περιλαμβάνονται στο δίκτυο της επιχείρησης, μελετώνται διεξοδικά οι απειλές που υφίσταται αυτό και τα σημεία ευπάθειας που παρουσιάζει και ακολούθως υπολογίζεται ο βαθμός επικινδυνότητας του

συστήματος. Τελικά, αναπτύσσεται ένα ολοκληρωμένο σχέδιο ασφάλειας για την επιχείρηση, το οποίο περιλαμβάνει τόσο τα προτεινόμενα αντίμετρα, όσο και την πολιτική ασφαλείας του οργανισμού. Τα προτεινόμενα αντίμετρα μπορεί να είναι κυρίως τεχνικά, αλλά και διοικητικά και οργανωτικά.

1.5. Ανάλυση και Διαχείριση Κινδύνων

Αν και η σημασία της ασφάλειας για όσους ασχολούνται με αυτή είναι γνωστή, η ένταξή της στο πλαίσιο λειτουργίας ενός οργανισμού δεν είναι ούτε εύκολη ούτε αυτονόητη. Ορισμένες δυσκολίες που αντιμετωπίζουν οι άνθρωποι που αναλαμβάνουν την κατοχύρωση της ασφάλειας σε ένα σύστημα είναι μεταξύ άλλων [9]:

- Δυσκολία αιτιολόγησης του κόστους των μέτρων ασφαλείας
- Δυσκολία επικοινωνίας μεταξύ επαγγελματιών της πληροφορικής και των διοικητικών στελεχών επιχειρήσεων και οργανισμών
- Δυσκολία εξασφάλισης της ενεργητικής συμμετοχής των χρηστών στην προστασία του πληροφοριακού συστήματος
- Λανθασμένη επικρατούσα αντίληψη ότι η ασφάλεια αποτελεί αποκλειστικά τεχνικό ζήτημα
- Ο προσδιορισμός και η αποτίμηση των οργανωσιακών επιπτώσεων από την εφαρμογή ενός σχεδίου ασφάλειας

Ορισμένες από τις παραπάνω δυσκολίες είναι εύλογο να προκύπτουν αν αναλογιστεί κανείς την ίδια τη φύση της ασφάλειας. Η ανάγκη για ένα μέτρο προστασίας μπορεί να αποδειχθεί ακόμα και αφού έχει συμβεί κάποια ευπάθεια και είμαστε αναγκασμένοι να υποστούμε τις συνέπειες. Για την επιβολή μέτρων προστασίας είναι απαραίτητη η μελέτη του συστήματος για να εντοπίζονται οι πόροι που χρήζουν προστασίας, τα αδύνατα σημεία και οι ενδεχόμενες απειλές. Ωστόσο, αξίζει να σημειωθεί ότι οι απειλές έχουν δυναμικό χαρακτήρα και χρειάζεται η συνεχής παρακολούθηση της ασφάλειας στο σύστημα.

Η ανάλυση κινδύνων (risk analysis) υποδεικνύει τα μέτρα που θα προσφέρουν προστασία ανάλογη των κινδύνων που απειλούν το σύστημα. Υιοθετεί την έννοια της επικινδυνότητας (προέρχεται από το χώρο της χρηματοοικονομικής διοίκησης), η οποία εξαρτάται από την πιθανότητα πραγματοποίησης ενός επεισοδίου ασφάλειας και από το κόστος που αυτό θα επιφέρει. Η διαχείριση επικινδυνότητας είναι ο αντικειμενικός στόχος και αφορά τον έλεγχο της επικινδυνότητας ώστε να παραμένει σε αποδεκτά επίπεδα. Η επικινδυνότητα μπορεί να μειωθεί (με εφαρμογή των κατάλληλων μέτρων), να μεταβιβαστεί (με ασφάλιση) ή να αναληφθεί (αποδοχή των συνεπειών αν συμβεί επεισόδιο) [9].

Για να μπορέσει να υπολογιστεί ικανοποιητικά η πιθανότητα να συμβεί ένα ανεπιθύμητο γεγονός και το μέγεθος του, πρέπει να υπάρχει μια γνώση των στοιχείων που απαρτίζουν τον κίνδυνο καθώς και των συσχετίσεων μεταξύ τους. Με καλή γνώση του κινδύνου μπορεί κάποιος να αποφασίσει ευκολότερα και σωστότερα για το αν θα αποδεχτεί τον κίνδυνο έτσι όπως έχει αποτιμηθεί ή αν θα προβεί σε ενέργειες που θα τον αποτρέψουν ή θα τον μειώσουν σε αποδεκτά επίπεδα. Αυτός με λίγα λόγια είναι ο σκοπός της ανάλυσης κινδύνων.

Οι απαιτήσεις ασφάλειας του οργανισμού προκύπτουν ύστερα από μεθοδική καταγραφή των κινδύνων που αντιμετωπίζει ο οργανισμός. Το κόστος των μηχανισμών ασφάλειας θα πρέπει να δικαιολογείται από την πιθανή ζημιά στον οργανισμό στην περίπτωση που παραβιασθεί η ασφάλειά του. Τεχνικές αποτίμησης μπορούν να εφαρμοσθούν στο σύνολο του οργανισμού ή μόνο σε επιμέρους τμήματά του, στα οποία έχουν καλύτερη πρακτική εφαρμογή και αποτελέσματα.

Η αποτίμηση κινδύνων είναι μια συστηματική εξέταση των εξής παραγόντων:

- Της ζημιάς που θα υποστεί ο οργανισμός στην περίπτωση που εμφανιστεί ένας κίνδυνος ασφάλειας, συμπεριλαμβανομένων των συνεπειών από την απώλεια της διαθεσιμότητας, της εμπιστευτικότητας ή της ακεραιότητας των πληροφοριών ή άλλων πόρων.
- Της ρεαλιστικής εκτίμησης της πιθανότητας να εμφανιστεί ένας τέτοιος κίνδυνος ασφάλειας σε σχέση με τους υπάρχοντες μηχανισμούς ελέγχου.

Τα αποτελέσματα αυτής της αποτίμησης καθορίζουν τις κατάλληλες ενέργειες και προτεραιότητες του οργανισμού, όπως και τους τρόπους υλοποίησης μηχανισμών ελέγχου της ασφάλειας απέναντι σε αυτούς τους κινδύνους. Ο περιοδικός έλεγχος των κινδύνων ασφάλειας καθώς και των μηχανισμών προστασίας είναι απαραίτητος, προκειμένου να προσαρμόζονται στις ανάγκες και τις προτεραιότητες του οργανισμού, να επεκτείνονται στην προστασία από νέους κινδύνους, καθώς επίσης και να επιβεβαιώνουν την ορθή και αποτελεσματική λειτουργία των υπαρχόντων μηχανισμών προστασίας και ελέγχου.

Οι περιοδικοί έλεγχοι θα πρέπει να διεξάγονται σε διάφορα επίπεδα, ανάλογα με τα αποτελέσματα προηγούμενων ελέγχων και τις αλλαγές στο επίπεδο κινδύνου που είναι αποδεκτό για τον οργανισμό. Συχνά, η αποτίμηση κινδύνου γίνεται αρχικά σε ένα υψηλό επίπεδο για τον καθορισμό προτεραιοτήτων και στη συνέχεια σε πιο αναλυτικά επίπεδα για την καταγραφή και αντιμετώπιση συγκεκριμένων κινδύνων.

1.5.1 Βασική μεθοδολογία ανάλυσης κινδύνων

Προκειμένου να υπάρξουν σωστές αποφάσεις για την αποδοχή, αποτροπή ή μείωση των κινδύνων και την υλοποίηση αποδοτικών οικονομικά (cost effective) λύσεων ασφαλείας, είναι αναγκαία η υιοθέτηση μιας μεθοδολογίας που θα αντιμετωπίζει τα θέματα με βάση το κόστος και το όφελος. Με τον καιρό έχουν δημιουργηθεί μια πληθώρα διαδικασιών που έρχονται να καλύψουν διαφορετικές ανάγκες για ανάλυση κινδύνων. Αν και υπάρχουν πολλές διαφορετικές διαδικασίες, η βασική μέθοδος παραμένει η ίδια.

Ο κίνδυνος στον οποίο εκτίθεται ένα πληροφοριακό σύστημα αποτελεί συνάρτηση:

- Της αξίας των περιουσιακών στοιχείων
- Των ευπαθειών του
- Των πιθανών απειλών και της φύσης τους
- Των επιπτώσεων που μπορεί να προκύψουν

Η βασική μεθοδολογία της ανάλυσης κινδύνων περιλαμβάνει τα παρακάτω βήματα [10]:

Καθορισμός του σκοπού και της εμβέλειας της ανάλυσης

Καθορίζεται τι ακριβώς θα περιληφθεί στην ανάλυση κινδύνων και ποια αποτελέσματα αναμένεται να παραχθούν από αυτήν.

Αναγνώριση και αξιολόγηση των περιουσιακών στοιχείων του πληροφοριακού συστήματος:

Προσπάθεια αναγνώρισης και προσδιορισμός της αξίας τους προς τον οργανισμό, καθώς υπάρχουν πολλά περιουσιακά στοιχεία σε έναν οργανισμό, πολλά από τα οποία δεν είναι εύκολα αναγνωρίσιμα.

Ανάλυση των απειλών προς τα περιουσιακά στοιχεία και των επιπτώσεων που μπορεί να έχουν

Αναγνωρίζονται οι απειλές για κάθε περιουσιακό στοιχείο, ο τρόπος με τον οποίο το απειλούν και οι επιπτώσεις που θα επιφέρει η κάθε απειλή.

Ανάλυση των ευπαθειών

Διευκρινίζεται η ευπάθεια του κάθε περιουσιακού στοιχείου προς κάθε απειλή ξεχωριστά καθώς ένα περιουσιακό στοιχείο μπορεί να είναι λιγότερο ευπαθής προς μια απειλή και περισσότερο προς μια άλλη. Η ευπάθεια ορίζεται επίσης και με τον τύπο *Ευπάθεια = Πιθανότητα να συμβεί μια απειλή* ***x*** *Πιθανότητα να είναι επιτυχής*

Υπολογισμός του κινδύνου

Ο βαθμός του κινδύνου υπολογίζεται ξεχωριστά για κάθε απειλή προς κάθε περιουσιακό στοιχείο. Αποτελεί συνάρτηση όλων των παραπάνω, δηλαδή των επιπτώσεων μιας απειλής (που έχουν σχέση με την αξία του περιουσιακού στοιχείου) και της ευπάθειας του περιουσιακού στοιχείου ως προς την απειλή

Επιλογή τρόπων αντιμετώπισης των κινδύνων

Αναγνωρίζονται τα πιθανά αντίμετρα που μπορούν να εφαρμοστούν και επιλέγονται αυτά που συμφέρουν περισσότερο στον οργανισμό. Υπάρχουν τρεις τρόποι αντιμετώπισης του κινδύνου: (α) Αποφυγή του κινδύνου με πλήρη απόσυρση από μια συγκεκριμένη δραστηριότητα, (β) Αποδοχή του κινδύνου και (γ) Μείωση του κινδύνου με χρήση αντιμέτρων (μέτρων ασφαλείας)

Με τα αντίμετρα μπορούν να επιτευχθούν: (α) Μεταφορά κινδύνου - π.χ. αγορά ασφάλειας, (β) Μείωση ευπάθειας που σημαίνει μείωση πιθανότητας να συμβεί μια απειλή – π.χ. απαγόρευση καπνίσματος σε μια ευαίσθητη περιοχή, ή μείωση πιθανότητας μια απειλή να είναι επιτυχής – π.χ. χρήση firewall, χρήση κρυπτογράφησης, (γ) Μείωση αντίκτυπου – π.χ. σύστημα πυρόσβεσης, (δ) Μέτρα ανάνηψης (επαναφοράς) – π.χ. backup.

Τα επόμενα βήματα

Η ανάλυση κινδύνων και η ασφάλεια των πληροφοριακών συστημάτων γενικότερα είναι μια συνεχόμενη διαδικασία. Μετά την επιλογή των τρόπων αντιμετώπισης και την εφαρμογή τους στον οργανισμό πρέπει να υπάρχει μια συνεχής παρακολούθηση των κινδύνων. Τα δεδομένα σε ένα πληροφοριακό σύστημα αλλάζουν συνεχώς, εισάγονται νέες απειλές, νέες ευπάθειες, νέες επιπτώσεις κτλ. Τα αντίμετρα που έχουν επιλεχθεί ελέγχονται συνεχώς για την αποτελεσματικότητά τους, καθώς πολλά από αυτά σταματούν πλέον να συμφέρουν στον οργανισμό και πρέπει να καταργηθούν ή να αντικατασταθούν από νέα. Το εύλογο ερώτημα βέβαια που τίθεται είναι σε ποιο βαθμό μπορούμε να περιορίσουμε τους κινδύνους και αν μπορούμε εν τέλει να τους εκμηδενίσουμε.

1.5.2. Οφέλη της ανάλυσης κινδύνων

Τα πιο σημαντικά οφέλη που αποκομίζονται από την ανάλυση κινδύνων πληροφοριακών συστημάτων αναφέρονται παρακάτω:

Γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος

Η ανάλυση κινδύνων βοηθάει στην γενικότερη βελτίωση της ασφάλειας του πληροφοριακού συστήματος αναγνωρίζοντας και αντιμετωπίζοντας τους σημαντικότερους κινδύνους που το απειλούν.

Στόχευση της ασφάλειας

Η ασφάλεια πρέπει να στοχεύει κατάλληλα και άμεσα στις πιθανές επιπτώσεις, απειλές και υπάρχουσες ευπάθειες. Η αποτυχία να γίνει αυτό μπορεί να οδηγήσει σε υπερβολικές και μη αναγκαίες δαπάνες. Η ανάλυση κινδύνων προάγει πολύ καλύτερη στόχευση που βοηθά στην εξάλειψη των άσκοπων δαπανών και στην πιο αποτελεσματική αντιμετώπιση των πραγματικών προβλημάτων ασφαλείας.

Βελτίωση της κατανόησης του συστήματος

Κατά την διαδικασία της ανάλυσης κινδύνων βελτιώνεται η γνώση και η κατανόηση του συστήματος ως προς θέματα ασφαλείας. Πρωτίστως αναγνωρίζονται οι διάφορες απειλές και φανερώνονται οι ευπάθειές του. Επίσης κατανοείται η πραγματική αξία των επιμέρους συστημάτων που αποτελούν το πληροφοριακό σύστημα.

Κατανόηση της αναγκαιότητας της ασφάλειας

Η συμμετοχή στην διαδικασία της ανάλυσης κινδύνων διαμορφώνει μια καλύτερη κατανόηση των προβλημάτων ασφαλείας καθώς και των επιπτώσεων που μπορεί να έχουν αυτά. Με αυτό τον τρόπο επιτυγχάνεται καλύτερη επιλογή αντιμέτρων αλλά και μεγαλύτερη αποδοχή των αντιμέτρων που προτείνονται από τους χρήστες. Η κατανόηση της αναγκαιότητας της ασφάλειας έχει ως αποτέλεσμα την αντιμετώπιση των θεμάτων ασφαλείας με την σοβαρότητα που τους αρμόζει.

Δικαιολόγηση δαπανών για την ασφάλεια

Η εισαγωγή ασφάλειας σε ένα πληροφοριακό σύστημα σχεδόν πάντα σημαίνει επιπλέον κόστος. Επειδή όμως δεν οδηγεί άμεσα σε αύξηση των κερδών μιας επιχείρησης, πρέπει να δικαιολογείται οικονομικά. Η ανάλυση κινδύνων δημιουργεί την κατάλληλη δικαιολόγηση για την αναγκαιότητα της ασφάλειας που προτείνεται και του κόστους που αυτή προσθέτει.

1.6. Πιθανά περιστατικά

Η ασφάλεια της επικοινωνίας μεταξύ δύο ή περισσότερων επικοινωνούντων μερών μπορεί να διακυβευτεί με ποικίλους τρόπους. Τα πιθανά περιστατικά που απειλούν ένα δίκτυο μπορούν πολύ χονδρικά να σχηματοποιηθούν στις παρακάτω κατηγορίες:

Διερευνητική επίθεση (Probe)

Μια διερευνητική επίθεση χαρακτηρίζεται από ασυνήθιστες απόπειρες απόκτησης πρόσβασης σε ένα σύστημα ή απόκτησης πληροφοριών σχετικά με το σύστημα. Οι διερευνητικές επιθέσεις ακολουθούνται μερικές φορές από ένα πιο σοβαρό περιστατικό παραβίασης ασφαλείας, αλλά πολύ συχνά είναι αποτέλεσμα περιέργειας ή σύγχυσης.

Σάρωση (Scan)

Μια σάρωση αποτελείται από έναν μεγάλο αριθμό διερευνητικών επιθέσεων που πραγματοποιούνται με τη χρήση ενός αυτόματου εργαλείου. Μερικές φορές μια επίθεση σάρωσης είναι αποτέλεσμα κάποιου σφάλματος, αλλά πολύ συχνά αποτελεί το προοίμιο μιας πιο άμεσης επίθεσης σε συστήματα τα οποία ο εισβολέας έχει βρει ότι είναι ευάλωτα.

Παραβίαση λογαριασμού (Account Compromise)

Ως παραβίαση λογαριασμού χαρακτηρίζεται η μη εξουσιοδοτημένη χρήση ενός λογαριασμού από κάποιον που δεν είναι ο ιδιοκτήτης του λογαριασμού. Το θύμα μπορεί να υποστεί σοβαρή απώλεια δεδομένων, υποκλοπή δεδομένων ή υπηρεσιών.

Παρακολούθηση δικτυακής κίνησης (Packet Sniffer)

Ένα πρόγραμμα παρακολούθησης της δικτυακής κίνησης συλλαμβάνει δεδομένα από πακέτα πληροφοριών μέσα στο δίκτυο μιας επιχείρησης ή στο Internet. Τα δεδομένα αυτά μπορεί να περιλαμβάνουν ονόματα χρηστών, κωδικούς πρόσβασης και άλλα προσωπικά δεδομένα. Με την υποκλοπή εκατοντάδων ή και χιλιάδων κωδικών πρόσβασης, ο εισβολέας είναι στη συνέχεια σε θέση να πραγματοποιήσει εκτεταμένες επιθέσεις στο σύστημα.

Επίθεση απάρνησης παροχής υπηρεσιών (Denial of Service)

Μια επίθεση απάρνησης παροχής υπηρεσιών δεν έχει ως στόχο να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δίκτυα ή δεδομένα, αλλά να αποτρέψει τη χρήση του δικτύου από τους νόμιμους χρήστες του. Μια τέτοια επίθεση μπορεί να έχει πολλές μορφές. Οι εισβολείς μπορεί να κατακλύσουν ένα δίκτυο με μεγάλες ποσότητες δεδομένων, να αποδιοργανώσουν φυσικά στοιχεία του δικτύου ή να ανακατευθύνουν τη μεταφορά των δεδομένων.

Παράδειγμα επίθεσης απάρνησης παροχής υπηρεσιών είναι οι επιθέσεις στην υποδομή του Internet (Internet Infrastructure Attacks). Αυτές οι σπάνιες αλλά σοβαρές επιθέσεις αφορούν περισσότερο σε συστατικά-κλειδιά της υποδομής του παρά σε συγκεκριμένα συστήματα σε αυτό. Τέτοια παραδείγματα είναι παροχείς πρόσβασης στο δίκτυο και μεγάλοι δικτυακοί τόποι αρχείων στους οποίους βασίζονται πολλοί χρήστες. Εκτεταμένες αυτοματοποιημένες επιθέσεις μπορούν επίσης να απειλήσουν την υποδομή του Internet. Γενικά, οι επιθέσεις στην υποδομή επηρεάζουν ένα μεγάλο τμήμα του Internet και παρακωλύουν σε σημαντικό βαθμό την εύρυθμη λειτουργία πολλών δικτυακών τόπων.

Κακόβουλος κώδικας (Malicious Code)

Ο όρος malicious code είναι ένας γενικός όρος που αναφέρεται σε προγράμματα τα οποία όταν εκτελούνται προκαλούν μη επιθυμητά αποτελέσματα σε ένα σύστημα. Οι χρήστες του συστήματος συνήθως δεν γνωρίζουν την ύπαρξη του προγράμματος μέχρι να ανακαλύψουν τη ζημιά. Αυτού του είδους τα προγράμματα μπορούν να οδηγήσουν σε σοβαρή απώλεια δεδομένων, άρνηση υπηρεσίας και άλλα περιστατικά παραβίασης της ασφάλειας.

1.7. Αντιμετώπιση περιστατικών παραβίασης ασφαλείας

Η σωστή και οργανωμένη αντίδραση απέναντι σε ένα περιστατικό παραβίασης της ασφάλειας είναι πολύ σημαντική καθώς μπορεί να κάνει τη διαφορά μεταξύ της πλήρους αποκατάστασης και της ολικής καταστροφής. Παρ' ότι κάθε επίθεση μπορεί να απαιτεί μια διαφορετική αντιμετώπιση σε ορισμένα σημεία, υπάρχει μια γενική αλληλουχία ενεργειών που θεωρούνται απαραίτητες για την επιτυχή αντιμετώπιση οποιουδήποτε είδους επίθεσης:

α) Προετοιμασία

Η διεξοδική αντιμετώπιση του ζητήματος της ασφάλειας περιλαμβάνει όχι μόνο την ανταπόκριση σε ένα πιθανό περιστατικό αλλά και μεθόδους πρόληψής του. Για να ελαχιστοποιηθεί η ζημιά από μια ενδεχόμενη επίθεση είναι απαραίτητο να γίνουν κάποιες ενέργειες προετοιμασίας. Αυτές οι ενέργειες περιλαμβάνουν την αποθήκευση αντιγράφων ασφαλείας όλων των σημαντικών δεδομένων ανά τακτά χρονικά διαστήματα, την παρακολούθηση και συνεχή ενημέρωση του λογισμικού και την δημιουργία και εφαρμογή γραπτής πολιτικής ασφάλειας.

β) Αναγνώριση του είδους της επίθεσης

Η προετοιμασία είναι ζωτικής σημασίας για την ελαχιστοποίηση των συνεπειών μιας επίθεσης. Η πρώτη ενέργεια που πρέπει να πραγματοποιηθεί μετά την εκδήλωση της επίθεσης είναι η αναγνώριση του είδους αυτής. Η αναγνώριση μερικών σημαντικών χαρακτηριστικών της επίθεσης είναι απαραίτητη προτού μπορέσει να γίνει δυνατή η πλήρης αντιμετώπισή της και γίνεται ολοένα και δυσκολότερη όσο μεγαλώνει η πολυπλοκότητα του περιστατικού.

γ) Αντιμετώπιση της επίθεσης

Μετά την αναγνώριση του είδους της επίθεσης, πρέπει να πραγματοποιηθούν οι απαραίτητες ενέργειες για την ελαχιστοποίηση των συνεπειών της. Η αντιμετώπιση της επίθεσης δίνει στον χρήστη ή το διαχειριστή του δικτύου τη δυνατότητα να προστατεύσει άλλα συστήματα και δίκτυα από την επίθεση και να περιορίσει τη ζημιά. Κατά τη φάση της απόκρισης καταγράφονται λεπτομερώς οι μέθοδοι που χρησιμοποιήθηκαν για την αντιμετώπιση της επίθεσης.

δ) Αποκατάσταση και ανάλυση

Η αποκατάσταση και η ανάλυση αποτελούν τις τελευταίες φάσεις που πραγματοποιούνται μετά την αντιμετώπιση της επίθεσης. Η φάση της αποκατάστασης επιτρέπει στους χρήστες να εξακριβώσουν το μέγεθος της ζημιάς που προκλήθηκε, ποια δεδομένα χάθηκαν και ποια είναι η κατάσταση του συστήματος μετά την επίθεση. Όταν έχει πλέον εξασφαλιστεί ότι η επίθεση έχει αντιμετωπιστεί, είναι πολύ χρήσιμο να διεξαχθεί μια ανάλυση της επίθεσης και να απαντηθούν ερωτήματα όπως: Γιατί συνέβη; Αντιμετωπίσθηκε έγκαιρα και σωστά; Θα μπορούσε να αντιμετωπιστεί καλύτερα; Η φάση της ανάλυσης επιτρέπει τον προσδιορισμό των αιτιών για τους οποίους η επίθεση ήταν επιτυχής και τη βέλτιστη σειρά ενεργειών που πρέπει να πραγματοποιηθούν ώστε να προστατευτεί το σύστημα απέναντι σε πιθανές μελλοντικές επιθέσεις.

ΚΕΦΑΛΑΙΟ 2

ΚΙΝΔΥΝΟΙ ΑΣΦΑΛΕΙΑΣ

Στον σημερινό κόσμο των διεθνών δικτύων και του ηλεκτρονικού εμπορίου, κάθε υπολογιστικό σύστημα αποτελεί ένα πιθανό στόχο. Παρόλο που οι ακαδημαϊκοί και οι πρωτοπόροι της βιομηχανίας της πληροφορικής γνώριζαν από παλιά τις θεμελιώδεις ευπάθειες των συνδεδεμένων υπολογιστών στο Internet, τα ελαττώματα αυτά έχουν μάλλον διευθετηθεί παρά διορθωθεί. Σε αποτέλεσμα αυτού, σπάνια πια περνάει ένας ολόκληρος μήνας χωρίς νέα κάποιας παραβίασης της ασφάλειας του υπολογιστικού δικτύου κάποιου οργανισμού ή εταιρείας [2]. Τα τελευταία χρόνια οι παραβιάσεις αυτές έχουν γίνει περισσότερο μοχθηρές καθώς υπολογιστές βγαίνουν εκτός λειτουργίας, εγγραφές αλλοιώνονται, λογισμικό εξοπλίζεται με "πίσω πόρτες", ευαίσθητες πληροφορίες αντιγράφονται χωρίς εξουσιοδότηση και εκατομμύρια προσωπικοί κωδικοί ανταλλάσσουν χέρια.

2.1. Γιατί οι υπολογιστές δεν είναι ασφαλείς

Ένα εύλογο ερώτημα που απασχολεί τον σύγχρονο άνθρωπο ο οποίος βλέπει την τεχνολογία των ηλεκτρονικών υπολογιστών να καλπάζει και να αναπτύσσεται με τρομακτικούς ρυθμούς, είναι το γιατί οι υπολογιστές είναι τόσο ανασφαλείς. Η μεγάλη πλειοψηφία των περιπτώσεων εισβολών σχετίζεται με ένα από τα παρακάτω προβλήματα. [11]

Η Ασφάλεια έχει το κόστος της

Τα χαρακτηριστικά ασφαλείας δεν υλοποιούνται συχνά μέσα σε λειτουργικά συστήματα, επειδή δημιουργούν προβλήματα στους χρήστες. Από την άλλη πλευρά οι χρήστες συχνά παρακάμπτουν την ασφάλεια επιλέγοντας εύχρηστους κωδικούς πρόσβασης, χωρίς να τους αλλάζουν και χωρίς να διστάζουν να τους μοιράζονται με συνεργάτες και άλλους χρήστες. Οι κατασκευαστές παραδίδουν το λογισμικό, με δυνατότητα εγκατάστασης των περισσότερων χαρακτηριστικών του και ανενεργά τα χαρακτηριστικά ασφαλείας του. Με αυτόν τον τρόπο οι άπειροι χρήστες δεν χρειάζεται να κατανοούν και να διαμορφώνουν το λογισμικό σωστά πριν να το χρησιμοποιήσουν, με αποτέλεσμα οι εγκαταστάσεις των υπολογιστών τις περισσότερες φορές να μην είναι σωστά ασφαλισμένες.

Τα χαρακτηριστικά παραδίδονται εσπευσμένα στην αγορά

Οι κατασκευαστές επικεντρώνουν την προσοχή τους στην προσθήκη χαρακτηριστικών που κάνουν το λογισμικό τους περισσότερο χρήσιμο αδιαφορώντας για την παράμετρο της ασφάλειας. Χαρακτηριστικό παράδειγμα είναι η προσθήκη υποστήριξης γλώσσας προγραμματισμού στο Microsoft Outlook και το Outlook Express από την Microsoft, όπου παρά τις πολυάριθμες προειδοποιήσεις από ειδικούς της ασφάλειας υπολογιστών ενσωμάτωσε μια γλώσσα συγγραφής script μέσα στο λογισμικό της για e-mail, παρέχοντας έτσι το κατάλληλο περιβάλλον για την διάδοση ενός "ιού e-mail".

Επισκίαση της ασφάλειας από τον ανταγωνισμό

Το χαρακτηριστικό που κατευθύνει τις εταιρείες να μην δίνουν ιδιαίτερη προσοχή στην ασφάλεια των συστημάτων που παράγουν, είναι η απαξίωση της ασφάλειας από τους ίδιους τους πελάτες. Αν οι πελάτες έδιναν αξία στην ασφάλεια, θα διάλεγαν παλιότερο, καλά δοκιμασμένο, αποδεδειγμένα ασφαλές λογισμικό που θα διέθετε όλα τα χαρακτηριστικά των καινούριων εκδόσεων. Εταιρίες όπως η Microsoft που προσάρμοσαν τα προϊόντα τους ώστε να λειτουργούν για το Διαδίκτυο, αποδεκάτισαν τον ανταγωνισμό. Αν περίμεναν να το κάνουν με ασφάλεια, θα είχαν νικηθεί από κάποιον που δεν θα υλοποιούσε ασφάλεια. Το τελικό αποτέλεσμα είναι τα λιγότερο ασφαλή προϊόντα να καταφθάνουν πάντα πρώτα στην αγορά, να καθιερώνονται και να γίνονται πρότυπά της.

Η ταχύτητα εξέλιξης των υπολογιστών και του λογισμικού

Οι υπολογιστές και η τεχνολογία δικτύωσης εξελίσσονται πολύ γρήγορα και οι εταιρείες δεν μπορούν να προβλέψουν τι θα πάει στραβά. Ο νόμος του Moore αναφέρει ότι το υλικό των υπολογιστών θα διπλασιάζεται σε ισχύ κάθε δύο χρόνια, πρόβλεψη που έχει αποδειχθεί ακριβής για πάνω από τρεις δεκαετίες τώρα. Πρωτόκολλα που δεν αναπτύχθηκαν ποτέ για να είναι ασφαλή υιοθετήθηκαν για άλλες χρήσεις, εκτός αυτών για τις οποίες αναπτύχθηκαν και έγιναν πολύ δημοφιλή σε πολύ μεγαλύτερο κοινό από αυτό που είχαν φανταστεί ποτέ οι δημιουργοί τους.

Η ταχύτητα αυτή της εξέλιξης ευθύνεται και για το γεγονός ότι οι προγραμματιστές δεν μπορούν να προβλέψουν τα προβλήματα με ακρίβεια. Αλλά ακόμη και να προσπαθούσαν να προβλέψουν σφάλματα, δεν θα ήταν ποτέ σε θέση να φανταστούν όλες τις πιθανές επιθέσεις που τα εκατομμύρια εισβολέων θα προσπαθούσαν να κάνουν.

Έλλειψη ποικιλομορφίας στην αγορά λογισμικού

Το μονοπώλιο των λειτουργικών συστημάτων Windows και Unix (καταλαμβάνουν πάνω από το 90% της αγοράς λειτουργικών συστημάτων για τους προσωπικούς υπολογιστές) έχει μειώσει σημαντικά τους στόχους των εισβολέων στις μικρές παραλλαγές αυτών των δύο λειτουργικών συστημάτων. Στις περισσότερες εφαρμογές, ένα από τα δύο προϊόντα κατέχει τη μερίδα του λέοντος, έτσι οι εισβολείς αρκεί να σπάσουν μόνο το ένα για να αποκτήσουν πρόσβαση σε μεγάλο πλήθος υπολογιστών.

Έλλειψη κινήτρου κατασκευαστών για να αποκαλύψουν σφάλματα των προϊόντων τους

Οι κατασκευαστές, για να αποφύγουν προβλήματα με τους πελάτες τους, προσπαθούν να αποκρύψουν τα προβλήματα των λειτουργικών συστημάτων τους αποθαρρύνοντας την συζήτηση των ατελειών τους. Αντίθετα οι εισβολείς, όταν ανακαλύπτουν τυχόν προβλήματα τα κοινοποιούν αμέσως σε όλο τον κόσμο μέσω του Διαδικτύου. Αυτή η διαφορά σημαίνει ότι τα προβλήματα διαχέονται πολύ πιο ευρέα απ' ότι οι λύσεις τους.

Άτακτες διορθώσεις

Όταν ένα λογισμικό παρουσιάσει πρόβλημα ασφαλείας, ο κατασκευαστής θα το διορθώσει, θα δημοσιεύσει μια διόρθωση και θα στείλει ειδοποίηση σε εγγεγραμμένους πελάτες μέσω e-mail. Στην πραγματικότητα, οι περισσότεροι χρήστες δεν εγκαθιστούν ποτέ διορθώσεις ασφάλειας για λογισμικό, εκτός και αν υποστούν εισβολή. Ακόμη χειρότερα, οι διορθώσεις αποστέλλονται βιαστικά σε πελάτες για σφάλματα που δεν έχουν βρεθεί ακόμη, που μπορούν να προκαλέσουν ακόμη μεγαλύτερα προβλήματα στα συστήματα των πελατών και ακόμη και στις καλύτερες περιπτώσεις, να απαιτούν πρόσθετη επεξεργασία για να βρεθούν τα προβλήματα, με αποτελέσματα την επιβράδυνση του συστήματος. Σε κάποιες περιπτώσεις, η θεραπεία είναι χειρότερη από την ασθένεια.

2.2. Hackers

Οι hackers είναι αυτό που έρχεται πρώτο στο νου του κοινού όταν ακούει για ασφάλεια δικτύων υπολογιστών. Υπήρχε μια εποχή κατά την οποία οι ειδικοί σε θέματα ασφάλειας της πληροφορικής μάλωναν για τον όρο hacker. Μερικοί από αυτούς νόμιζαν ότι είναι εξαίρετοι και κάπως παθιασμένοι προγραμματιστές. Άλλοι υποστήριζαν ότι είναι κοινοί εγκληματίες, κρυμμένοι πίσω από ένα πέπλο ανωνυμίας, μια γνώμη που συμμερίζεται με πάθος και η πλειοψηφία των ΜΜΕ. Ένα γεγονός που έκανε τα πράγματα ακόμη δυσκολότερα στο να ερμηνευτούν ήταν ότι πολλοί ειδικοί σε θέματα πληροφορικής ήταν στο παρελθόν οι ίδιοι hackers, εντασσόμενοι και στους δύο παραπάνω ορισμούς. Κάποιοι από αυτούς ήταν ανυπόμονοι να απαλλαγούν από αυτό το προσωνύμιο, ενώ άλλοι επιθυμούσαν να το διατηρήσουν.

Σύμφωνα με την καθαρά τεχνική έννοια του όρου, το hacking πριν την έλευση των υπολογιστών, σήμαινε την επινόηση έξυπνων λύσεων σε δύσκολα τεχνικά προβλήματα. Όταν εμφανίστηκαν για πρώτη φορά υπολογιστές στα πανεπιστήμια, το hacking άρχισε να σημαίνει την επινόηση έξυπνων λύσεων σε δύσκολα προγραμματιστικά προβλήματα.

Η σύγχρονη χρήση της λέξης hacking, σημαίνει την δραστηριότητα με κακόβουλο κίνητρο, όπως οι απόπειρες εισβολής σε υπολογιστικά συστήματα και δίκτυα για την κλοπή ή καταστροφή δεδομένων. Αν και το hacking, μπορεί να έχει πάρα πολλά κίνητρα, όπως απλή περιέργεια, επιθυμία για επίδειξη, κοινωνική διαμαρτυρία κ.α. – είναι οι εγκληματικές δραστηριότητες των hackers αυτές που κερδίζουν την μεγαλύτερη δημοσιότητα από τα μέσα ενημέρωσης. Αυτοί που έχουν αγνότερα κίνητρα συχνά διαμαρτύρονται για αυτήν την σημασιολογική μετατόπιση στην έννοια της λέξης και προτιμούν να προσδιορίζουν την δραστηριότητα του κακόβουλου hacking με άλλους όρους όπως π.χ. cracking. Οι Αρχές αρέσκονται να χρησιμοποιούν τους όρους cybercrime (κυβερνοέγκλημα) και cyberterrorism (κυβερνοτρομοκρατία) για να περιγράψουν τις εγκληματικές δραστηριότητες των hackers.

Μέσα στην κουλτούρα των hackers υπάρχουν πολλοί που πιστεύουν ότι δοκιμάζοντας τα όρια των υπολογιστικών συστημάτων είναι μια ενδιαφέρουσα και διασκεδαστική ενασχόληση. Το να ανακαλύπτεις πώς να εισχωρήσεις σε μέρη υπολογιστικών συστημάτων που είναι "εκτός ορίων" αποτελεί μια συναρπαστική πρόκληση, και αυτοί που το καταφέρνουν συχνά θεωρούνται τοπικοί ήρωες [12]. Η απαγορευμένη γνώση είναι το βασικό νόμισμα στον ψηφιακό υπόκοσμο και η μετάδοση της στους ομόφρονές του θα δώσει στον χάκερ τη φήμη που επιζητά.

Στην πιο στομφώδη εκδοχή τους, οι χάκερς πιστεύουν ότι είναι οι εκλεκτοί πρωτοπόροι του ψηφιακού κόσμου. Το βασικό τους κίνητρο περιγράφεται από την πολύ γνωστή πια φράση –τουλάχιστον στον χώρο της πληροφοριακής ασφάλειας– "η πληροφορία θέλει να είναι ελεύθερη". Και ότι ένα άτομο χρειάζεται πληροφορία για να αποκτήσει πρόσβαση σε περισσότερη πληροφορία. Σ' έναν κόσμο στον οποίο η πληροφορία μπορεί να αντιγραφεί και να μεταδοθεί, αφήνοντας το πρωτότυπο ανέπαφο και λειτουργώντας με το τέλειο αντίγραφο (το οποίο μπορεί πιθανότατα με λίγες υπολογιστικές γνώσεις να γίνει ελαφρώς καλύτερο), η συζήτηση περί ιδιοκτησίας έχει πια τελειώσει.

Η πιο έμπιστη και σεμνή εκδοχή των χάκερς, είναι αυτή κατά την οποία είναι ενεργά πρόθυμοι να ανταλλάξουν τεχνικά τρικ και κόλπα, λογισμικό και υπολογιστικούς πόρους με άλλους χάκερς. Τεράστια δίκτυα όπως το Usenet και ο Παγκόσμιος Ιστός (World Wide Web) μπορούν να λειτουργήσουν χωρίς κεντρικό έλεγχο λόγω αυτού του χαρακτηριστικού. Βασίζονται και ενισχύουν την αίσθηση της κοινότητας που μπορεί να είναι το σημαντικότερο ανέγγιχτο πλεονέκτημα της κουλτούρας των χάκερς.

Σήμερα η σύγχυση γύρω από τον ορισμό hacker[1] φαίνεται να έχει "λυθεί" κατά ένα μεγάλο μέρος. Ενώ μερικοί επαγγελματίες της πληροφορικής συνεχίζουν να αυτοαποκαλούνται hackers, οι περισσότεροι δεν το κάνουν. Στο μυαλό του κοινού, ο ορισμός hacker έχει πια μόνιμα ορισθεί σαν ένα άτομο ιδιαίτερα ταλαντούχο με τους υπολογιστές, το οποίο αρκετά συχνά χρησιμοποιεί αυτό το ταλέντο του για μη ευγενικούς σκοπούς [13].

[1] Σήμερα, ο πιο συνηθισμένος ευφημισμός για τους επαγγελματίες της πληροφοριακής ασφάλειας οι οποίοι εντρυφούν σε δραστηριότητες hacking (για πιθανά) νόμιμους σκοπούς είναι white hats (οι τύποι με τα λευκά καπέλα). Είναι νόμιμοι ειδικοί στην ασφάλεια αλλά με γνώσεις και εμπειρία των μεθόδων της σκοτεινής πλευράς. Αυτός ο ορισμός υπάρχει και στα περισσότερα βιβλία πληροφοριακής ασφάλειας.

Ο Bruce Sterling στο βιβλίο του "The Hacker Crackdown: Law and Disorder on the Electronic Frontier" διατύπωσε ότι [14]:

Ο όρος hacking χρησιμοποιείται σήμερα σε καθημερινή βάση από σχεδόν όλους τους αξιωματικούς επιβολής του νόμου που σχετίζονται επαγγελματικά με την απάτη και κατάχρηση μέσω υπολογιστή. Η αστυνομία περιγράφει σχεδόν κάθε έγκλημα σχετιζόμενο με υπολογιστή σαν hacking.

Επίσης ακόμη πιο σημαντικό είναι το γεγονός ότι οι ίδιοι οι εισβολείς επιλέγουν να αποκαλούν τους εαυτούς τους σαν hackers. Κανένας που εισβάλει σε υπολογιστικά συστήματα δεν περιγράφει ηθελημένα τον εαυτό του σαν εισβολέα, καταχραστή, cracker, hacker της σκοτεινής πλευράς ή γκάνγκστερς υψηλής τεχνολογίας. Αρκετοί άλλοι εξευτελιστικοί όροι έχουν εφευρεθεί σε ελπίδα ότι ο τύπος και το κοινό θα πάψουν να χρησιμοποιούν την πρωταρχική λέξη. Αλλά λίγοι άνθρωποι χρησιμοποιούν πραγματικά αυτούς τους εναλλακτικούς όρους.

2.3. Η σκοτεινή πλευρά: Εισβολείς (Crackers)

Οι crackers είναι αυτοί που έχουν σαν κύρια ασχολία τους την εισβολή σε πληροφοριακά συστήματα. Ο συγκεκριμένος όρος γεννήθηκε το 1985 από χάκερς, σε υπεράσπιση τους, από την λανθασμένη χρήση του όρου hacker από τον έντυπο τύπο. Ο νεολογισμός cracker αντικατοπτρίζει μια ισχυρή αποστροφή ενάντια στην κλοπή και στον βανδαλισμό που διαπράττεται από τις συμμορίες των crackers. Παρόλο που είναι αναμενόμενο οποιοσδήποτε πραγματικός χάκερ να έχει διαπράξει στο παρελθόν, κάποιες "εύθυμες" εισβολές και να γνωρίζει πολλές από τις βασικές τεχνικές εισβολής, οποιοσδήποτε έχει περάσει πια το στάδιο της εφηβείας, αναμένεται να έχει ξεπεράσει την επιθυμία για εισβολή σε συστήματα από απλή ευχαρίστηση εκτός από τις περιπτώσεις που συντρέχουν άμεσοι, ευγενικοί και πρακτικοί λόγοι.

Έτσι, υπάρχει πολύ λιγότερη επικάλυψη ανάμεσα στην κουλτούρα των hackers και την κουλτούρα των crackers. Οι crackers τείνουν να συγκεντρώνονται σε μικρές, μυστικοπαθείς ομάδες που μικρή σχέση έχουν με την τεράστια, ανοικτή κουλτούρα των hackers. Το τυπικό προφίλ του cracker τον περιγράφει σαν γένους αρσενικού, έφηβο ηλικίας μεταξύ 13 και 28 ετών, άτομο έξυπνο, που μαθαίνει γρήγορα.

Από τα κοινά σημεία που υπάρχουν ανάμεσα στις δύο κουλτούρες, ίσως το πιο σημαντικό να είναι αυτό του "ηθικού" cracking, το οποίο περιλαμβάνει την εισβολή σε σύστημα χωρίς την διάπραξη κλοπής, βανδαλισμού ή ρήξη της εμπιστευτικότητας. Στηρίζεται στο σκεπτικό ότι η παραβίαση συστημάτων μπορεί να παρέχει περισσότερο αποτελεσματική ασφάλεια στο μέλλον, έτσι ώστε άλλοι – πιθανώς λιγότερο καλής προθέσεως hackers– να εμποδίζονται από το να προκαλέσουν πραγματική ζημιά. Πάνω σε αυτήν την άποψη, οι crackers υποστηρίζουν ότι ίσως να είναι μια από τις μεγαλύτερες μορφές της χακερίστικης αβροφροσύνης για έναν cracker να: (α) εισβάλει σε κάποιο σύστημα και μετά, (β) να εξηγήσει αναλυτικά στους διαχειριστές του συστήματος πώς ακριβώς επιτεύχθηκε η εισβολή και ποιές αδυναμίες του συστήματος εκμεταλλεύθηκε ο εισβολέας όπως επίσης και τρόπους βελτίωσης της ασφάλειας του πληροφοριακού συστήματος. Με αυτόν τον τρόπο ο εισβολέας λειτουργεί σαν απλήρωτος και αυτόκλητος σύμβουλος ασφαλείας.

Ωστόσο σε κάποιες περιπτώσεις, ο cracker εκτός από την ενημέρωση των διαχειριστών του συστήματος για τις αδυναμίες που ανακαλύπτει θα δημοσιοποιήσει τα ευρήματα του και σε κάποιο δημόσιο φόρουμ (forum) για θέματα πληροφοριακής ασφάλειας. Οι περισσότερες εταιρείες αντιτίθενται σε τέτοιες ενέργειες, υποστηρίζοντας ότι με την δημοσιοποίηση τέτοιου είδους πληροφοριών, οι καλόβουλοι κατά τα άλλα, crackers, δίνουν την ευκαιρία σε άλλους με κακόβουλες προθέσεις να επιχειρήσουν να εισβάλλουν στα δίκτυα τους. Το γεγονός είναι ότι όλο και περισσότερες εταιρείες καταφεύγουν σε δικαστικές ενέργειες ενάντια σε αυτούς που αποκαλύπτουν πληροφορίες οι οποίες μπορούν να υπονομεύσουν την ασφάλεια ή την φήμη τους.

Ο πιο συνηθισμένος σύγχρονος ευφημισμός για τους crackers σήμερα είναι ο όρος "black hat" (ο τύπος με το μαύρο καπέλο), και αυτός ο όρος χρησιμοποιείται σε πολλά (κυρίως καινούργια) βιβλία με θέμα την πληροφοριακή ασφάλεια.

2.4. Τύποι Εισβολέων

Οι εισβολείς ανήκουν στις παρακάτω κατηγορίες, με σειρά αυξανόμενης απειλής [3]:

- Ειδικοί Ασφαλείας
- Έφηβοι Εισβολείς
- Υποαπασχολούμενοι Ενήλικες
- Εισβολείς από Ιδεολογία
- Εγκληματίες Εισβολείς
- Εταιρικοί Κατάσκοποι
- Δυσαρεστημένοι Υπάλληλοι

Ειδικοί Ασφαλείας

Οι περισσότεροι ειδικοί ασφαλείας είναι σε θέση να κάνουν εισβολές αλλά δεν το κάνουν για ηθικούς ή για οικονομικούς λόγους. Γνωρίζουν ότι μπορούν να κερδίσουν περισσότερα χρήματα αποτρέποντας παρά προκαλώντας τις εισβολές, οπότε ξοδεύουν το χρόνο τους παρακολουθώντας τις κοινότητες των εισβολέων και τις τρέχουσες τεχνικές προκειμένου να γίνουν περισσότερο αποτελεσματικοί στη μάχη κατά των εισβολέων. Πολλές εταιρίες που δραστηριοποιούνται στον κυβερνοχώρο προσλαμβάνουν ειδικούς εισβολείς για να ελέγχουν τα συστήματα ασφαλείας τους και των μεγάλων πελατών τους. Αυτοί οι ειδικοί συχνά είναι οι πρώτοι που βρίσκουν νέες μεθόδους εισβολής και συχνά γράφουν λογισμικό για να ελέγχουν ή για να προκαλούν μια κατάσταση.

Έφηβοι Εισβολείς

Οι έφηβοι εισβολείς είναι συνήθως σπουδαστές που κάνουν εισβολές, ενώ βρίσκονται σε κάποια βαθμίδα της εκπαίδευσης – γυμνάσιο, λύκειο ή πανεπιστήμιο. Αυτοί οι εισβολείς μπορούν να χρησιμοποιούν το δικό τους υπολογιστή ή τους ισχυρούς πόρους της σχολής τους για να κάνουν τις εισβολές τους.

Οι έφηβοι εισβολείς κάνουν βόλτες στον κυβερνοχώρο ψάχνοντας για στόχους και ενδιαφέρονται κυρίως για να εντυπωσιάσουν τους φίλους τους και να μην συλληφθούν. Συνήθως δεν βλάπτουν τους στόχους τους ενώ τις περισσότερες φορές η δράση τους δεν γίνεται καν αντιληπτή, εκτός και αν το σύστημα στο οποίο εισβάλουν ανιχνεύσει ασυνήθιστη δραστηριότητα και ειδοποιήσει τον ιδιοκτήτη ή αν ένα firewall καταγράψει την επίθεση ή εκτός και αν κάνουν κάποιο λάθος.

Αν η κοινότητα των εισβολέων θεωρηθεί ως ως μια οικονομική δραστηριότητα, τότε οι έφηβοι εισβολείς είναι οι καταναλωτές. Χρησιμοποιούν τα εργαλεία που παράγονται από άλλους, χαίρονται με τις δραστηριότητές τους και γενικά παράγουν μια βάση διασκέδασης, επάνω στην οποία κάθονται οι σοβαρότεροι έφηβοι εισβολείς και υποαπασχολούμενοι ενήλικες. Καμία σοβαρή προσπάθεια ασφάλειας δεν θα τους βγάλει από το παιχνίδι.

Υποαπασχολούμενοι Ενήλικες

Οι υποαπασχολούμενοι ενήλικες είναι είτε πρώην έφηβοι εισβολείς, οι οποίοι είτε εκδιώχθηκαν από τη σχολή τους, είτε δεν κατάφεραν να βρουν μια εργασία πλήρους απασχόλησης. Συνήθως εργασίες που πληρώνουν μόνο για τις βασικές τους ανάγκες ενώ η πρώτη τους αγάπη είναι η εισβολή. Πολλά από τα εργαλεία που χρησιμοποιούν οι έφηβοι εισβολείς κατασκευάζονται από τους ενήλικες εισβολείς.

Οι ενήλικες εισβολείς δεν είναι εγκληματίες από πρόθεση αφού δεν έχουν σκοπό να κάνουν κακό σε κανέναν. Ωστόσο συχνά δημιουργούν τα σπασίματα που εφαρμόζονται από άλλους εισβολείς για να ξεκλειδώσουν εμπορικό λογισμικό. Επίσης γράφουν τους περισσότερους ιούς λογισμικού και αποτελούν την περιβόητη συμμορία των εισβολέων. Κάνουν τις εισβολές τους για αποκτήσουν φήμη στην κοινότητα των εισβολέων, θέλουν να εντυπωσιάσουν τους όμοιούς τους, να πάρουν πληροφορίες και να κάνουν γνωστή την αντίδρασή τους στην κυβέρνηση και τις επιχειρήσεις. Η ομάδα αυτή αποτελεί το ένα δέκατο της κοινότητας των εισβολέων, αλλά είναι η πηγή του λογισμικού που γράφεται ειδικά για εισβολείς.

Οι υποαπασχολούμενοι ενήλικες αποτελούν κίνδυνο για το δίκτυο μιας εταιρίας αν αυτή κατέχει κάποιο είδος πνευματικής ιδιοκτησίας που θέλει να προστατέψει, μιας και η πνευματική ιδιοκτησία δεν προστατεύεται αρκετά από το νόμο και η εισβολή δεν αποτελεί αδίκημα σε πολλές χώρες του κόσμου.

Εισβολείς από Ιδεολογία

Οι εισβολείς από ιδεολογία είναι αυτοί που κάνουν εισβολές για να προωθήσουν κάποιο πολιτικό σκοπό. Η συγκεκειμένη εισβολή είναι περισσότερο συνηθισμένη σε πολιτικές διαμάχες που αφορούν συνήθως σε θέματα περιβάλλοντος και εθνικισμού. Σε μια προσπάθεια να διαδηλώσουν τις ιδέες τους, αυτοί οι εισβολείς συνήθως καταστρέφουν ιστοσελίδες ή κάνουν επιθέσεις άρνησης παροχής υπηρεσίας εναντίον των ιδεολογικών τους αντιπάλων. Συνήθως προσπαθούν να επιτύχουν ευρεία κάλυψη των κατορθωμάτων τους από τα μέσα και επειδή προέρχονται κυρίως από άλλες χώρες και έχουν την έμμεση υποστήριξη των κυβερνήσεών τους, δεν μπορούν να απαγγελθούν κατηγορίες εναντίον τους.

Αυτό το είδος εισβολής εμφανίζεται κατά κύματα, όταν συμβαίνουν μεγάλα γεγονότα στον πολιτικό στίβο, και πολλές φορές εξαιτίας του ότι αυτού του είδους οι επιθέσεις καταναλώνουν πολύ μεγάλο εύρος ζώνης, προκαλούν χαοτικές καταιγίδες.

Εγκληματίες Εισβολείς

Οι εγκληματίες εισβολείς κάνουν εισβολές είτε για εκδίκηση, είτε για να διαπράξουν κλοπές, είτε απλώς για να ικανοποιηθούν και να προκαλέσουν καταστροφές. Αυτή η κατηγορία εισβολέων δεν αποτελούν ένα ειδικό επίπεδο ηθικού προβλήματος. Οι εγκληματίες εισβολείς είναι αυτοί που ακούγονται στις εφημερίδες να έχουν εισβάλει σε διακομιστές Internet για να κλέψουν αριθμούς πιστωτικών καρτών, για να κάνουν μεταφορές χρημάτων από τράπεζες ή να έχουν εισβάλει στο μηχανισμό τραπεζικών συναλλαγών του Internet για να κλέψουν χρήματα.

Αυτοί οι εισβολείς είναι παρόμοιοι με κάθε άλλο εγκληματία αφού προσπαθούν να κάνουν ζημιά αδιαφορώντας για το ποιος είναι το θύμα. Οι εγκληματίες εισβολείς είναι πολλοί σπάνιοι επειδή η ευφυΐα που απαιτείται για να κάνουν εισβολές συνήθως τους δίνει την ευκαιρία να βρουν κάποιο περισσότερο αποδεκτό κοινωνικά τρόπο ζωής. Παρόλα αυτά, γίνεται όλο και περισσότερο συνηθισμένο το οργανωμένο έγκλημα να απειλεί ότι θα κάνει επιθέσεις άρνησης παροχής υπηρεσιών για να ζητήσει χρήματα προστασίας από εταιρίες τα έσοδα των οποίων προέρχονται από μια δημόσια ιστοθέση. Επειδή οι επιθέσεις άρνησης παροχής υπηρεσιών δεν μπορούν να αποτραπούν, αφού μπορεί για παράδειγμα να εμφανιστούν με την μορφή μιας μεγάλης ποσότητας νόμιμων αιτήσεων, τα θύματα συχνά αισθάνονται ότι δεν έχουν καμία άλλη επιλογή παρά να πληρώσουν.

Εταιρικοί Κατάσκοποι

Οι πραγματικοί εταιρικοί κατάσκοποι είναι πολύ σπάνιοι επειδή είναι πολύ ακριβό και πολύ επικίνδυνο να χρησιμοποιηθούν παράνομες τεχνικές εισβολής εναντίον ανταγωνιστικών εταιριών. Αυτές οι τεχνικές χρησιμοποιούνται τις περισσότερες φορές εναντίον εταιριών υψηλής τεχνολογίας από ξένες κυβερνήσεις. Πολλές εταιρίες υψηλής τεχνολογίας είναι νέες και άπειρες στο θέμα ασφάλειας και έτσι μπορούν εύκολα να επιλεγούν από τους πεπειραμένους πράκτορες ξένων κυβερνήσεων. Αυτές οι υπηρεσίες έχουν ήδη τα χρήματα για να κάνουν κατασκοπία και επιτίθενται σε μερικές επιχειρήσεις μεσαίου μεγέθους για να υποκλέψουν τεχνολογία, η οποία θα δώσει στις εθνικές τους εταιρίες ένα ανταγωνιστικό πλεονέκτημα.

Δυσαρεστημένοι Υπάλληλοι

Οι δυσαρεστημένοι υπάλληλοι είναι οι πιο επικίνδυνοι και οι πιθανότεροι να δημιουργήσουν προβλήματα από όλους τους εισβολείς. Ένας υπάλληλος που θεωρεί ότι δεν του έχει φερθεί καλά η εταιρία στην οποία εργάζεται, έχει και τον τρόπο αλλά και τα κίνητρα να προκαλέσει σοβαρές καταστροφές στο δίκτυό της. Επιθέσεις από δυσαρεστημένους υπαλλήλους δύσκολα ανιχνεύονται πριν να συμβούν, αλλά συνήθως κάποιο είδος συμπεριφοράς δίνει κάποιες γενικές ενδείξεις. Οι επιθέσεις μπορεί να είναι είτε περίπλοκες όπως για παράδειγμα ένας διαχειριστής δικτύου διαβάζει όλα τα e-mail των υπαλλήλων, είτε απλές όπου ένας υπάλληλος κάνει καταστροφές στον διακομιστή της εταιρικής βάσης δεδομένων.

2.5. Κακόβουλα Προγράμματα

Ως *κακόβουλα προγράμματα* (malicious codes) χαρακτηρίζονται τα προγράμματα εκείνα που εκτελούν καταστροφικές ενέργειες σε υπολογιστικά συστήματα. Πρόκειται για προγράμματα που μπορούν να προκαλέσουν ανεπιθύμητα αποτελέσματα, όπως εμφάνιση μηνυμάτων, διαγραφή αρχείων, ακόμη και διαμορφώσεις δίσκων.[3]

Τα κακόβουλα προγράμματα μπορεί να παραμένουν σε αδράνεια στη μνήμη του υπολογιστή για μεγάλο χρονικό διάστημα. Τα αποτελέσματά τους γίνονται αντιληπτά όταν ενεργοποιούνται μετά από κάποιο συμβάν ή σε μια συγκεκριμένη ημερομηνία. Αυτό όμως που κάνει τα κακόβουλα προγράμματα ιδιαίτερα επικίνδυνα είναι η δυνατότητά τους να αντιγράφονται και να εξαπλώνονται από υπολογιστή σε υπολογιστή, αποτελώντας σοβαρές προγραμματιστικές απειλές.

Υπάρχουν πολλά είδη προγραμματιστικών απειλών και οι ειδικοί τις κατηγοριοποιούν ανάλογα με τον τρόπο που συμπεριφέρονται, πως ενεργοποιούνται και πως εξαπλώνονται. Τα τελευταία χρόνια, οι περιπτώσεις που έλαβαν δημοσιότητα, περιγράφτηκαν ενιαία από τα μέσα ενημέρωσης σαν ιοί των υπολογιστών. Ωστόσο οι ιοί αποτελούν μόνο ένα μικρό ποσοστό του κακόβουλου λογισμικού που έχει εφευρεθεί. Το να λέγεται ότι όλες οι προγραμματισμένες απώλειες δεδομένων οφείλονται σε ιούς των υπολογιστών είναι το ίδιο ανακριβές με την δήλωση ότι όλες οι ανθρώπινες παθήσεις οφείλονται σε ιούς.

Οι βασικοί τύποι κακόβουλων προγραμμάτων είναι:

- Ιοί Υπολογιστών (Computer Viruses)
- Δούρειοι Ίπποι (Trojan Horses)
- Σκουλήκια (Worms)

Άλλοι τύποι κακόβουλων προγραμμάτων είναι:

- Λογικές Βόμβες (Logic Bombs): κακόβουλα προγράμματα που «εκρήγνυνται» όταν ικανοποιηθεί μια λογική συνθήκη.
- Χρονικές Βόμβες (Time Bombs): κακόβουλα προγράμματα που ενεργοποιούνται όταν έρθει η κατάλληλη χρονική στιγμή ή μέρα.
- Πίσω πόρτες (Backdoors/Trapdoors): κρυμμένες λειτουργίες προγραμμάτων με τις οποίες παρέχεται η προσπέλαση σε ευαίσθητα δεδομένα.
- Κουνέλια (Rabbits): προγράμματα που αυτο-αντιγράφονται απεριόριστα με σκοπό την υπερβολική κατανάλωση υπολογιστικών πόρων.

2.5.1. Ιοί

Ιοί Υπολογιστών (Computer Viruses) ονομάζονται τα κομμάτια κώδικα που προσαρτώνται σε διάφορα αρχεία, τροποποιούν άλλα προγράμματα και αναπαράγουν πιστά αντίγραφα του εαυτού τους.. Μπορεί να μην κάνουν τίποτε, να μην προκαλούν ζημιές ή να είναι καταστροφικά (π.χ. να μεταβάλλουν και να διαγράφουν αρχεία). Υπάρχουν διάφοροι τύποι ιών όπως:

- Ιοί Εκκίνησης (Bootstrap Viruses): κώδικας που εισάγεται στην διαδικασία εκκίνησης ενός υπολογιστή.
- Παρασιτικοί Ιοί (Parasitic Viruses): μέρη κώδικα που προσαρτώνται σε εκτελέσιμα προγράμματα (αρχεία .com ή .exe).
- Συνοδευτικοί Ιοί (Companion Viruses): εναλλακτικά εκτελέσιμα προγράμματα που εισάγονται στην διαδρομή αναζήτησης κανονικών προγραμμάτων.
- Ιοί Μακροεντολών (Macro Viruses): τμήματα κώδικα που εισάγονται σε αρχεία δεδομένων τα οποία επεξεργάζεται μια εφαρμογή που υποστηρίζει μακροεντολές.

Όσον αφορά τον τρόπο ενεργοποίησής τους, οι ιοί αντιγράφονται από μόνοι τους με δυο βασικούς τρόπους. Όταν εκτελείται ένα μολυσμένο πρόγραμμα είτε μολύνει άμεσα άλλα μέρη του υπολογιστή (π.χ. άλλες τοποθεσίες στο δίσκο ή άλλα προγράμματα), είτε εγκαθίσταται μόνιμα στη μνήμη από μόνο του και κατόπιν μολύνει άλλα προγράμματα που εκτελούνται ή μέσα αποθήκευσης που εισάγονται για χρήση (π.χ. cd/dvd).

2.5.2. Σκουλήκια

Τα σκουλήκια (worms) είναι προγράμματα που εξαπλώνονται μέσω των δικτυωμένων υπολογιστών, αντιγράφοντάς τα ανεξέλεγκτα, χωρίς απαραίτητα να τροποποιούν άλλα αρχεία στους υπολογιστές-στόχους. Μοιάζουν πολύ με τους ιούς στο ότι αντιγράφονται από μόνα τους και επιτίθενται σε συστήματα με σκοπό να επιφέρουν βλάβες. Εξ' ορισμού δεν τροποποιούν άλλα προγράμματα αλλά μπορεί να κουβαλούν μέσα τους κάποιον ιό που μπορεί να το κάνει. Πρόκειται για πλήρως αυτόνομα προγράμματα τα οποία μολύνουν υπολογιστικά συστήματα μόνο μέσω δικτυακών συνδέσεων.

Για τη δημιουργία τους απαιτούνται αρκετές τεχνικές γνώσεις, αλλά ένα καλογραμμένο σκουλήκι έχει τη δυνατότητα να προκαλέσει ανυπολόγιστη ζημιά. Η αυξανόμενη ανάγκη για συμβατότητα μεταξύ υπολογιστικών συστημάτων και εφαρμογών κάνει ευκολότερη την διάδοση των σκουληκιών αλλά και γενικά κάθε είδους κακόβουλου λογισμικού.

Μόλις ένα σκουλήκι μολύνει ένα σύστημα, αναζητεί δραστήρια για πιθανές συνδέσεις με άλλους υπολογιστές, οπότε αν βρει, αμέσως αντιγράφεται σε αυτούς. Όμως, πέρα από την συμπεριφορά αναπαραγωγής τους από σύστημα σε σύστημα, τα σκουλήκια συχνά εκτελούν και κακόβουλες πράξεις, που δεν περιορίζονται μόνο στην καταστροφή αρχείων. Έτσι, μέσω των δικτυακών συνδέσεων μπορούν να υποκλέψουν και να μεταφέρουν προς τους συγγραφείς τους πληροφορίες που αφορούν συνθηματικά χρηστών και άλλες ευαίσθητες αλλά και πολύτιμες πληροφορίες. Επιπλέον, μπορούν να επιφέρουν πλήρη αποδιοργάνωση των λειτουργιών ενός συστήματος ώστε να προκαλείται επίθεση άρνησης εξυπηρέτησης. Αυτό συνήθως προκαλείται από παράλληλες και ανοργάνωτες επιθέσεις περισσότερων του ενός σκουληκιών στο ίδιο σύστημα.

Ο εντοπισμός των σημείων προσβολής είναι δύσκολος, ακριβώς επειδή η μόλυνση από σκουλήκια επιτυγχάνεται μέσω δικτυακών συνδέσεων. Για την αποφυγή της μόλυνσης από σκουλήκια επιβάλλεται ο εντοπισμός και η αντιμετώπιση όλων των ευπαθών σημείων του υπολογιστικού συστήματος. Αυτό σημαίνει ότι ιδιαίτερα πρέπει να προσεχθούν τα αδύνατα σημεία όπως εύκολα συνθηματικά ή ανεξέλεγκτες δικτυακές υπηρεσίες που μπορούν να εκμεταλλευθούν τα σκουλήκια για να εισβάλλουν στο σύστημα από το δίκτυο και να το μολύνουν.

Ένας καλός τρόπος προφύλαξης από τα σκουλήκια είναι η γνώση των μεθόδων που χρησιμοποιούν για τον εντοπισμό και την αξιοποίηση των ευπαθών σημείων του συστήματος. Όπως γίνεται γενικότερα για την πρόληψη εισβολών, η χρήση διατάξεων firewalls και ελέγχου προσπέλασης μπορούν να μειώσουν σημαντικά τους κινδύνους επίτευξης των στόχων των σκουληκιών.

2.5.3. Δούρειοι Ίπποι

Οι Δούρειοι Ίπποι (Trojan Horses) είναι προγράμματα με κρυφές λειτουργίες που δεν περιλαμβάνονται στην τεκμηρίωση που τα συνοδεύει. Τα προγράμματα αυτά ονομάσθηκαν έτσι γιατί λειτουργούν όπως το μυθικό άλογο του Τρωϊκού Πολέμου. Δηλαδή, ενώ επικαλούνται ότι επιτελούν μια χρήσιμη εργασία για τον χρήστη, στην πραγματικότητα εκτελούν μυστικά κάποια διαφορετική λειτουργία με απώτερο σκοπό την κατάλυση της ασφάλειας. Αυτή η λανθάνουσα δραστηριότητα είναι που συνήθως εκτελεί καλυμμένες ενέργειες, όπως η κλοπή των συνθηματικών των χρηστών. Οι Δούρειοι Ίπποι βρίσκονται σε περίοδο μεγάλης εξάπλωσης σήμερα, εκμεταλλευόμενοι της τρωϊκής αφέλειας των άπειρων χρηστών ηλεκτρονικών υπολογιστών.

Υπάρχουν Δούρειοι Ίπποι που η εργασία που υποτίθεται ότι προσφέρουν δεν υπάρχει καν. Έτσι, όταν εκτελούνται απλά προχωρούν στην απροκάλυπτη καταστροφή αρχείων και πόρων του συστήματος. Από την άλλη, υπάρχουν Δούρειοι Ίπποι που λειτουργούν με συγκαλυμμένο τρόπο, έτσι ώστε να επιτελούν την εργασία που επικαλούνται χωρίς να προκαλούν υποψίες. Ως Δούρειοι Ίπποι μπορούν να θεωρηθούν και όσα από τα γνωστά προγράμματα του εμπορίου διαθέτουν λειτουργίες οι οποίες δεν αναφέρονται πουθενά στα εγχειρίδια χρήσης τους, αλλά συνήθως αποκαλύπτονται τυχαία.

Είναι προφανές ότι οι Δούρειοι Ίπποι αποτελούν την πλέον επικίνδυνη κατηγορία κακόβουλων προγραμμάτων, καθώς φανερά επικαλούνται μια δεδομένη λειτουργικότητα ενώ στην πραγματικότητα λειτουργούν λίγο ή πολύ διαφορετικά και μάλιστα χωρίς αυτό να φαίνεται. Έτσι, δεν χρειάζεται να αντιγράφουν τους εαυτούς τους ούτε να αναπαράγονται όπως οι ιοί και τα σκουλήκια. Είναι οι ίδιοι οι χρήστες που βοηθούν τους Δούρειους Ίππους να μολύνουν τα διάφορα υπολογιστικά συστήματα.

Κύριες πηγές Δούρειων Ίππων είναι οι διάφοροι εξυπηρετητές πληροφόρησης (bulletin board servers) και διανομής αρχείων (FTP servers). Σε αυτούς τους τόπους κανείς μπορεί να βρει πληθώρα ελεύθερων (freeware, shareware, demos) και πολλές φορές πειρατικών αντιγράφων προγραμμάτων τα οποία διατίθενται για "κατέβασμα" (download) με μικρή ή καθόλου εγγύηση. Φυσικά με κίνητρο την δωρεάν απόκτηση "χρήσιμου" λογισμικού, οι χρήστες αναλαμβάνουν το ρίσκο να γίνουν οι ίδιοι βοηθοί των συγγραφέων των Δούρειων Ίππων, εγκαθιστώντας τους στους υπολογιστές τους.

Οι πιο χρήσιμοι Δούρειοι ίπποι ονομάζονται πίσω πόρτες. Αυτά τα προγράμματα παρέχουν ένα μηχανισμό με βάση τον οποίο ο εισβολέας μπορεί να ελέγξει απευθείας τον υπολογιστή. Παραδείγματα περιλαμβάνουν κακόβουλα σχεδιασμένα προγράμματα όπως τα NetBus, Back Orifice και BO2K, καθώς και καλοκάγαθα προγράμματα, τα οποία μπορεί να εκμεταλλευθεί κάποιος για να πάρει τον έλεγχο ενός συστήματος, όπως τα netcat, VNC και pcAnywhere. Τα ιδανικά προγράμματα πίσω πόρτας είναι μικρά και γρήγορα εγκαθιστάμενα προγράμματα, τα οποία εκτελούνται διαρκώς. Οι Δούρειοι ίπποι συνήθως μεταφέρονται μέσω ιών που παράγονται από e-mail ή στέλνονται ως συνημμένα σε e-mail.

Η καλύτερη μέθοδος πρόληψης κατά των Δούρειων Ίππων είναι η ενημέρωση των χρηστών. Σε κάθε περίπτωση όμως είναι δύσκολη αλλά όχι αδύνατη η ανίχνευση των Δούρειων Ίππων πριν να εισχωρήσουν σε ένα υπολογιστικό σύστημα. Για το λόγο αυτό επιβάλλεται η καθιέρωση και η συνεπής εφαρμογή από τους διάφορους οργανισμούς συγκεκριμένων πολιτικών εγκατάστασης επίσημα αγορασμένου λογισμικού, καθώς και εκπαίδευσης των χρηστών, έτσι ώστε να αποκτήσουν τα απαραίτητα για να συμμερίζονται τους κινδύνους που αναλαμβάνουν όταν δοκιμάζουν προγράμματα άγνωστης προέλευσης.

2.6. Τρόποι εργασίας των εισβολέων

Τέσσερις είναι οι τρόποι με τους οποίους ένας εισβολέας μπορεί να προσπελάσει το δίκτυο υπολογιστών μιας επιχείρησης:

- Συνδεόμενος μέσω του Internet
- Χρησιμοποιώντας έναν υπολογιστή του ίδιου του δικτύου
- Καλώντας μέσω ενός διακομιστή απομακρυσμένης προσπέλασης (Remote Access Service, RAS)
- Συνδεόμενος μέσω ενός ανασφαλούς ασύρματου δικτύου

Αυτός ο αριθμός τρόπων εισόδου ορίζει και τα όρια του προβλήματος της εισβολής. [3], [11]

2.6.1. Απευθείας Εισβολή

Οι εισβολείς σε πολλές περιπτώσεις εργάζονται στις επιχειρήσεις, διαχειρίζονται κάποιο τοπικό τερματικό ή βρίσκονται μπροστά σε ένα πελάτη δικτύου, διαμορφώνοντας με τον τρόπο αυτό την κατάσταση για περαιτέρω απομακρυσμένη διείσδυση μέσα σε συστήματα.

Σε μεγάλες επιχειρήσεις δεν υπάρχει τρόπος να γνωρίζει η διοίκηση όλους τους ανθρώπους, οπότε ένας άγνωστος εργαζόμενος στο τμήμα πληροφορικής δεν είναι κάτι το ασυνήθιστο ή κάτι το ύποπτο. Σε επιχειρήσεις όπου οι υπάλληλοι δεν έχουν καρτελάκια ή κάρτες εισόδου, δεν είναι δουλειά των υπαλλήλων να ψάξουν τα στοιχεία άλλων υπαλλήλων, οπότε η διείσδυση είναι σχετικά εύκολη.

Η επίλυση του προβλήματος της απευθείας εισβολής είναι εύκολη αφού αρκεί να εφαρμοστεί πολιτική ισχυρής φυσικής ασφάλειας στις εγκαταστάσεις της επιχείρησης και να θεωρηθεί κάθε σύνδεση ή καλώδιο που βγαίνει από το κτήριο της επιχείρησης σαν ένα πρόβλημα ασφαλείας. Αυτό σημαίνει ότι πρέπει να τοποθετηθούν firewalls, που παρακολουθούν κάθε σύνδεση που βγαίνει από το κτήριο, ανάμεσα στις συνδέσεις WAN και στο εσωτερικό δίκτυο της επιχείρησης ή πίσω από ασύρματες συνδέσεις.

2.6.2. Μέσω Τηλεφωνικής Κλήσης

Η εισβολή μέσω τηλεφωνικής κλήσης, μέσω modem, ήταν παλιότερα ο μόνος τρόπος εισβολής, αλλά γρήγορα πήρε τη δεύτερη θέση, μετά από την εισβολή μέσω του Internet, η οποία είναι απλώς ευκολότερη και πιο ενδιαφέρουσα για τους εισβολείς.

Αν και το πρόβλημα της εισβολής μέσω τηλεφωνικής κλήσης σημαίνει συνήθως εκμετάλλευση ενός μόντεμ που είναι συνδεδεμένο σε ένα διακομιστή υπηρεσίας απομακρυσμένης προσπέλασης (RAS), περιλαμβάνει επίσης το πρόβλημα κλήσης προς διακριτούς υπολογιστές. Κάθε μόντεμ που έχει διαμορφωθεί, ώστε να απαντά για να επιτρέπει απομακρυσμένη προσπέλαση ή απομακρυσμένο έλεγχο από τον υπάλληλο που χρησιμοποιεί τον υπολογιστή, αποτελεί ένα πρόβλημα ασφάλειας. Πολλές επιχειρήσεις επιτρέπουν στους υπαλλήλους τους να προσπελαύνουν απομακρυσμένα τους υπολογιστές τους από το σπίτι, χρησιμοποιώντας αυτήν την μέθοδο.

Μία λύση του προβλήματος της εισβολής μέσω τηλεφωνικής κλήσης είναι η τοποθέτηση των διακομιστών RAS έξω από τα firewalls μέσα στη δημόσια ζώνη ασφάλειας και η υποχρεωτική πιστοποίηση των νόμιμων χρηστών στο firewall προκειμένου να εισέλθουν στους πόρους του δικτύου της επιχείρησης.

2.6.3. Internet

Η εισβολή μέσω του Internet είναι η περισσότερο διαθέσιμη, ευκολότερα εκμεταλλεύσιμη και πλέον προβληματική περιοχή εισβολής σε ένα εταιρικό δίκτυο.

Το πρόβλημα της εισβολής μέσω του Internet επιλύεται αν χρησιμοποιηθούν firewalls, οπότε κρίνεται πως δεν υπάρχει λόγος για περαιτέρω συζήτηση αυτού του θέματος εδώ.

2.6.4. Ασύρματα

Η ασύρματη επικοινωνία είναι πλέον φθηνή και χρησιμοποιείται ευρέως στον επιχειρηματικό κόσμο. Το ιδιαίτερα δημοφιλές πρωτόκολλο 802.11b, επιτρέπει σε διαχειριστές να συνδέουν σημεία ασύρματης προσπέλασης (WAP) στα δίκτυά τους και να επιτρέπουν σε χρήστες (συνήθως με φορητούς υπολογιστές) να προσπελαύνουν τα δίκτυά τους και να κυκλοφορούν μέσα στις εγκαταστάσεις χωρίς περιορισμούς. Σε ένα άλλο τρόπο λειτουργίας, δύο WAP μπορούν να συνδέονται μεταξύ τους για να δημιουργήσουν μια ασύρματη γέφυρα ανάμεσα σε κτήρια, κάτι που μπορεί να εξοικονομήσει δεκάδες χιλιάδες ευρώ από μια εταιρεία, σε κόστος κατασκευής ή κόστος κυκλωμάτων.

Το 802.11b δινόταν με ένα πολυδιαφημισμένο σχήμα κρυπτογράφησης, που ονομαζόταν Διασφάλιση Απορρήτου Ισοδύναμη της Ενσύρματης Επικοινωνίας (WEP), το οποίο υποσχόταν ότι θα επιτρέπει τη δικτύωση με την ίδια ασφάλεια που παρέχουν τα ενσύρματα δίκτυα. Η ιδέα ήταν σπουδαία, οι ειδικοί της ασφάλειας χρειάστηκαν όμως λιγότερο από 11 ώρες για να παραβιάσουν το σύστημα. Αρχικά κανένας δεν έδωσε σημασία, οπότε αυτοί οι ειδικοί εξέδωσαν ένα λογισμικό που επέτρεπε την αυτόματη εισβολή. Το WEP έχει παραβιαστεί τόσο πολύ πλέον, που πρέπει να θεωρείται σαν ανασφαλής σύνδεση μέσω του Internet. Όλες οι ασύρματες συσκευές πρέπει να τοποθετούνται στη δημόσια πλευρά του Internet, και οι χρήστες πρέπει να πιστοποιούνται με το firewall της εταιρίας. Η νεότερη υπηρεσία 128-bit WEP είναι περισσότερο ασφαλής, αλλά δεν πρέπει επίσης να θεωρείται ισοδύναμη της ενσύρματης ασφάλειας. Αυτό αφήνει ένα μόνο πρόβλημα που είναι η κλοπή υπηρεσίας. Μπορεί κανείς να πάρει ένα φορητό υπολογιστή μέσα σε μια σύγχρονη μεγαλούπολη και να πιστοποιηθεί σε οποιοδήποτε από τα πολυάριθμα δίκτυα 802.11b που υπάρχουν εκεί.

Σήμερα υπάρχουν ταχύτερα ασύρματα πρωτόκολλα, που περιλαμβάνουν τα 54MB 802.11g και 802.11a, αλλά (ίσως επειδή τα πρωτόκολλα είναι δύο) δεν είναι πιθανό να εκτοπίσουν το 802.11b σε σύντομο χρονικό διάστημα. Το 802.11b είναι φθηνότερο και ταχύτερο από κάθε άλλο κύκλωμα σύνδεσης προς το Internet, οπότε τα πρωτόκολλα μεγαλύτερης ταχύτητας, που λειτουργούν σε μικρότερες αποστάσεις δεν θα μπορέσουν να το αντικαταστήσουν.

2.7. Τεχνικές εισβολής

Οι επιθέσεις εισβολής προχωρούν σε μια σειρά φάσεων, χρησιμοποιώντας διάφορα εργαλεία και τεχνικές. Μια σύνοδος εισβολής αποτελείται από τις παρακάτω φάσεις:

- Επιλογή στόχου
- Συλλογή πληροφοριών
- Επίθεση

Ο εισβολέας προσπαθεί να μάθει στοιχεία για το δίκτυο – στόχο, μέσω κάθε διαδοχικής επίθεσης, οπότε αυτές οι φάσεις παρέχουν στοιχεία στον εισβολέα, ώστε αυτός να μπορεί να συλλέξει πληροφορίες από επιθέσεις που απέτυχαν.

Επιλογή Στόχου

Η επιλογή στόχου είναι η φάση στην οποία ο εισβολέας προσδιορίζει ένα συγκεκριμένο υπολογιστή για να του επιτεθεί. Για να περάσει από αυτήν την φάση, πρέπει να είναι διαθέσιμος κάποιος τρόπος επίθεσης, οπότε το μηχάνημα πρέπει είτε να έχει διαφημίσει την παρουσία του ή να έχει βρεθεί μέσω αναζήτησης. [3],[11]

Συλλογή Πληροφοριών

Η συλλογή πληροφοριών είναι η φάση κατά την οποία ο εισβολέας καθορίζει τα χαρακτηριστικά του στόχου, πριν να του επιτεθεί. Αυτή μπορεί να γίνει είτε μέσω δημόσια διαθέσιμων πληροφοριών, που εκδίδονται για το στόχο ή ερευνώντας το στόχο, χρησιμοποιώντας μη επιθετικές μεθόδους, για να πάρει πληροφορίες από αυτόν. [3], [11]

Επιθέσεις

Οι εισβολείς χρησιμοποιούν διάφορα είδη επιθέσεων εναντίον διαφόρων συστημάτων. Οι περισσότερες από τις επιθέσεις είναι εξειδικευμένες ώστε να εκμεταλλεύονται μια συγκεκριμένη υπηρεσία δικτύου. [3], [11]

2.8. Κίνδυνοι ασφαλείας στο Διαδίκτυο

Το διαδίκτυο σχεδιάστηκε από επιστημονικές και ακαδημαϊκές κοινότητες προκειμένου να επιτευχθεί η ανταλλαγή πληροφοριών μεταξύ έμπιστων οντοτήτων. Το θέμα της ασφάλειας των ευαίσθητων πληροφοριών δεν απασχόλησε αρχικά τους σχεδιαστές του. Ο λόγος είναι ότι κανένας δεν μπορούσε να προβλέψει τότε ότι θα επεκταθεί και θα συνδέσει την πλειοψηφία των δημοσίων και ιδιωτικών δικτύων που υπάρχουν στον κόσμο σήμερα.[11], [15]

Το διαδίκτυο ως μέσο ψηφιακής επικοινωνίας κρύβει έναν αριθμό από σοβαρούς κινδύνους, όπως:

- Έλλειψη εμπιστευτικότητας, αφού τα δεδομένα που διακινούνται είναι χωρισμένα σε πακέτα και μπορούν εύκολα να κλαπούν και να αποκαλυφθεί το περιεχόμενό τους.

- Έλλειψη μηχανισμών για την ταυτοποίηση των χρηστών των συστημάτων. Όλα τα συστήματα που είναι συνδεδεμένα στο διαδίκτυο αναγνωρίζονται από την IP διεύθυνση τους, και το πρωτόκολλο IP δεν παρέχει κάποιο μηχανισμό για την αυθεντικοποίηση των χρηστών του συστήματος.

- Έλλειψη αξιόπιστων μέσων για σύνδεση των IP διευθύνσεων με συγκεκριμένους υπολογιστές.

- Εκτεθειμένοι κωδικοί πρόσβασης. Τα περισσότερα συστήματα χρησιμοποιούν κωδικούς για την ταυτοποίηση των χρηστών, οι οποίοι τις περισσότερες φορές μεταφέρονται στο δίκτυο χωρίς να κρυπτογραφηθούν.

Η υπηρεσία του παγκόσμιου ιστού (WWW) εισάγει ακόμα περισσότερους κινδύνους. Ένας παρουσιαστής ιστοσελίδων (browser) αποτελεί το ιδανικό μέσο για την αυτόματη εκτέλεση προγραμμάτων χωρίς τη γνώση του χρήστη, γνωστών όπως αναφέρθηκε και παραπάνω ως Δούρειοι Ίπποι.

2.8.1. Εγγενή Προβλήματα Ασφάλειας

Το διαδίκτυο δεν πρέπει να αντιμετωπίζεται από άποψη ασφάλειας ως ένα κοινό δίκτυο. Ο κυριότερος λόγος είναι ότι οι μηχανισμοί στους οποίους στηρίζει τη λειτουργικότητα του σχεδιάστηκαν με γνώμονα τη βελτιστοποίησή του στις δυνατότητες διασύνδεσης ετερογενών δικτύων και κοινής εκμετάλλευσης των πληροφοριών/πόρων τους κι όχι στην παρεχόμενη ασφάλεια. Σαν αποτέλεσμα, η ασφάλεια σε κάποιο βαθμό μπορεί να επιτευχθεί μόνο ως ένα πρόσθετο χαρακτηριστικό στην υπάρχουσα υποδομή παρά σαν ένα μέρος του πρωταρχικού δικτυακού σχηματισμού.

Πιο αναλυτικά, στα εγγενή προβλήματα ασφάλειας του διαδικτύου περιλαμβάνονται και τα ακόλουθα:

- Η ετερογένεια των δικτύων που διασυνδέει, η οποία με δεδομένο και το τεράστιο μέγεθος του, έχει το προφανές αποτέλεσμα οι σωστές διαδικασίες διασφάλισης ενός συστήματος σε περιβάλλον διαδικτύου, να απαιτούν μια πληθώρα περίπλοκων ρυθμίσεων και διαμορφώσεων.

- Λόγω της εύκολης και χωρίς περιορισμούς πρόσβασης που προσφέρει σε εκατομμύρια χρήστες, είναι πιο ευάλωτο από κάθε άλλο δίκτυο και αποτελεί στόχο περισσότερων επιθέσεων για επίδοξους εισβολείς.

- Δεν υπάρχει συνολική πολιτική ελέγχου προσπέλασης. Επιπλέον, πολλοί κόμβοι δεν είναι σε θέση για διάφορους λόγους (άγνοια, κόστος, αδιαφορία, κλπ.) να αποκτήσουν τη κατάλληλη διαμόρφωση, έτσι ώστε να μην κινδυνεύουν από την ευρέως ανοικτή σύνδεσή τους στο διαδίκτυο.

- Η φύση του πρωτοκόλλου TCP/IP και των περισσότερων υπηρεσιών που υποστηρίζει, προσθέτουν νέες ευπάθειες και σημεία επιθέσεων. Το γεγονός ότι επιτρέπονται τα πακέτα των δεδομένων να περνούν από μια σειρά απρόβλεπτων ενδιάμεσων υπολογιστών και επιμέρους δικτύων μέχρι να φτάσουν στο τελικό προορισμό τους, δίνει τη δυνατότητα σε ένα τρίτο μέρος να παρέμβει με διάφορους τρόπους στην επικοινωνία δυο νόμιμων μερών.

2.8.2. Απειλές Ασφάλειας

Στις τυπικές απειλές ασφάλειας σε ένα περιβάλλον διαδικτύου, συμπεριλαμβάνονται :

- Βλάβες συστατικών μερών (component failure): Σχεδιαστικά λάθη ή ελαττωματικά μέρη υλικού/λογισμικού, είναι ικανά να προκαλέσουν δυσλειτουργία σε κάποιο συστατικό του συστήματος και να οδηγήσουν έτσι σε άρνηση εξυπηρέτησης ή άλλες καταστάσεις επικίνδυνες για την ασφάλεια.

- Παρουσίαση πληροφοριών (information browsing): Η αποκάλυψη ευαίσθητων πληροφοριών σε μη-εξουσιοδοτημένους χρήστες, είτε είναι εισβολείς είτε είναι νόμιμοι χρήστες που επιχειρούν παράνομους τρόπους προσπέλασης, οδηγεί στην απώλεια εμπιστευτικότητας και μπορεί να προκληθεί από την εκμετάλλευση διάφορων μηχανισμών.

- Μη-εξουσιοδοτημένη διαγραφή, μεταβολή ή εισαγωγή πληροφοριών: Η εκούσια ή και ακούσια πρόκληση ζημιών στα πληροφοριακά αγαθά (information assets) οδηγεί στην απώλεια της ακεραιότητας των λειτουργιών/δεδομένων των οργανισμών και των χρηστών.

- Κατάχρηση (misuse): Η χρήση των πληροφοριακών αγαθών αλλά και των υπόλοιπων πόρων για σκοπούς διαφορετικού από αυτούς που έχουν προκαθορισθεί, προκαλεί άρνηση εξυπηρέτησης, αύξηση κόστους λειτουργίας των συστημάτων και δυσφήμιση των οργανισμών που τα χρησιμοποιούν.

- Διείσδυση (penetration): Οι εισβολείς από μη-εξουσιοδοτημένα πρόσωπα ή συστήματα μπορούν να προκαλέσουν άρνηση εξυπηρέτησης ή να απαιτήσουν σοβαρότατα χρηματικά ποσά για την αντιμετώπιση των συνεπειών από τις παρενοχλήσεις του συστήματος.

- Διαστρέβλωση: Οι προσπάθειες ενός χρήστη που παρανομεί, να μεταμφιεστεί σαν ένας χρήστης με εξουσιοδοτήσεις τέτοιες ώστε να μπορεί να κλέψει πληροφορίες ή να εκμεταλλευτεί υπηρεσίες ή να εκκινήσει συναλλαγές που προκαλούν οικονομικές απώλειες ή δυσχέρειες σε ένα οργανισμό.

Οι πιθανότητες να εκδηλωθούν επιθέσεις και να πραγματοποιηθούν απειλές όπως οι προαναφερθείσες, αυξάνονται όταν προσφέρεται στο διαδίκτυο μια ευδιάκριτη εικόνα της οργάνωσης της δικτυακής υποδομής ενός συστήματος. Πάρα πολλές επιθέσεις στο Internet είναι ευκαιριακής φύσης (opportunistic), με την έννοια ότι δεν έχουν συγκεκριμένο στόχο παραβίασης. Απλά εκδηλώνονται σε ένα συγκεκριμένο σύστημα γιατί εκείνη τη στιγμή το σύστημα αυτό φαντάζει ως ιδανικός στόχος (τελικός ή ενδιάμεσος) για τους επίδοξους εισβολείς.

ΚΕΦΑΛΑΙΟ 3

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Θεωρώντας το σύνολο των προβλημάτων ασφάλειας που καλείται να αντιμετωπίσει σήμερα ένα πληροφοριακό σύστημα και λαμβάνοντας υπόψη τους τρόπους αντιμετώπισης των κινδύνων αυτών, εύκολα αντιλαμβανόμαστε ότι η δημιουργία μιας πολιτικής ασφάλειας που να ανταποκρίνεται στις απαιτήσεις λειτουργίας ενός συστήματος είναι πρωταρχικής σημασίας.

Η ουσία της πολιτικής ασφάλειας εμπεριέχεται στον ορισμό της ο οποίος συμπυκνώνει το νόημά της. Με τον όρο πολιτική ασφαλείας εννοούμε ένα σύνολο κανόνων, οι οποίοι προσδιορίζουν επακριβώς το ρόλο κάθε εμπλεκόμενου μέσα σε μια εταιρεία ή έναν οργανισμό, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του. Πρόκειται στην ουσία για ένα σύνολο από αρχές και οδηγίες υψηλού επιπέδου που αφορούν τη σχεδίαση και διαχείριση συστημάτων ασφαλείας, υποδεικνύοντας με τον τρόπο αυτό πώς πρέπει να λειτουργεί ένας οργανισμός.

3.1. Χαρακτηριστικά πολιτικής ασφάλειας

Τα στοιχεία που πρέπει να περιλαμβάνει μια πολιτική ασφάλειας είναι τα ακόλουθα [16]:

- *Αγαθά*: πρόκειται για τις οντότητες (π.χ. υλικό, λογισμικό, πληροφορίες) του πληροφοριακού συστήματος που έχουν αξία και πρέπει να προστατευθούν.
- *Ρόλοι και αρμοδιότητες*: πρόκειται για τα καθήκοντα, τις αρμοδιότητες, τις ευθύνες του κάθε ρόλου για θέματα που αφορούν το πληροφοριακό σύστημα και την ασφάλειά του.
- *Στόχους*: πρόκειται για τον στόχο ασφάλειας που καθορίζει συνοπτικά την γενικότερη πολιτική και θέτει περιορισμούς.
- *Πεδίο εφαρμογής*: πρόκειται για την εμβέλεια, την έκταση και το χώρο που αφορά η πολιτική ασφαλείας.
- *Οδηγίες κατευθυντήριες γραμμές*.

- *Κουλτούρα, άλλες πολιτικές, νομοθεσία*: πρόκειται για το σύνολο των πεποιθήσεων, αξιών και νόμων που συνθέτουν την κουλτούρα της επιχείρησης και του περιβάλλοντός της και ανατροφοδοτούν τους μηχανισμούς της μέσω μιας διαδικασίας συνεχούς εκμάθησης.

- *Υλοποίηση και εφαρμογή της πολιτικής ασφάλειας – Ενημέρωση και συμμόρφωση*: πρόκειται γα το οργανωτικό πλαίσιο ρόλων, αρμοδιοτήτων, κανονισμών, επιτροπών για την υλοποίηση και εφαρμογή της πολιτικής ασφαλείας, για την ενημέρωση του προσωπικού σχετικά με τη συμμόρφωση και τις ενέργειες που λαμβάνονται στην περίπτωση παραβίασης της πολιτικής ασφαλείας.

- *Επισκόπηση και αναθεώρηση της πολιτικής*: πρόκειται για την τακτική επισκόπηση και αναθεώρηση της πολιτικής όταν αυτό χρειάζεται και καθορίζεται από τις εκάστοτε συνθήκες ώστε να είναι επίκαιρη και να καλύπτει τις απαιτήσεις του πληροφοριακού συστήματος και των διαδικασιών διαχείρισης σε κάθε αλλαγή που μπορεί να παρουσιαστεί και σε κάθε νέα ανάγκη που μπορεί να προκύψει.

3.2. Περιεχόμενα πολιτικής ασφαλείας

Το κείμενο της πολιτικής ασφαλείας θα πρέπει να περιλαμβάνει τουλάχιστον τα παρακάτω:

- Τον ορισμό της ασφάλειας των πληροφοριών, το σκοπό της και τη σπουδαιότητά της ως μηχανισμό που επιτρέπει την ανταλλαγή πληροφοριών.

- Τους σκοπούς της διοίκησης και την υποστήριξή της αναφορικά με την ασφάλεια.

- Την επεξήγηση της πολιτικής ασφαλείας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιήσει η εταιρεία ή οργανισμός, όπως σχετική νομοθεσία, προστασία από ιούς, επιπτώσεις μη συμμόρφωσης με την πολιτική ασφάλειας, διαχείριση επιχειρηματικής συνέχειας κλπ.

- Τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας και την αναφορά συμβάντων.
- Αναφορές σε άλλα κείμενα που μπορούν να υποστηρίξουν την πολιτική ασφαλείας, όπως περιγραφές συγκεκριμένων διαδικασιών και κανονισμών.

3.3. Άξονες πολιτικής ασφάλειας

Πρέπει να γίνει απολύτως σαφές ότι οι πολιτικές ασφαλείας είναι γενικά υποκειμενικές και προσαρμόσιμες στις συγκεκριμένες ανάγκες και τους στόχους κάθε εταιρίας ή οργανισμού αφού οι απαιτήσεις και οι ιδιαιτερότητες που παρουσιάζει κάθε οργανισμός δεν είναι ίδιες. Υπάρχουν ωστόσο κάποιοι γενικοί άξονες που διαμορφώνουν μια πολιτική ασφάλειας και ο κάθε άξονας αντιπροσωπεύει ένα σύνολο από οδηγίες που αφορούν συγκεκριμένους τομείς και ζητήματα τα οποία είναι τόσο σημαντικά που θα πρέπει να αντιμετωπίζονται σε όλες τις πολιτικές ασφαλείας [6].

Φυσική ασφάλεια

Τα μέτρα προστασίας που υποστηρίζουν τη φυσική ασφάλεια έχουν ως κύριο στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στο χώρο του οργανισμού και της καταστροφής των αγαθών του πληροφοριακού συστήματος. Αυτό επιτυγχάνεται με τη δημιουργία επάλληλων περιμέτρων φυσικής ασφάλειας, στη λογική των ομόκεντρων κύκλων, όπου στο κύκλο που βρίσκεται πιο εσωτερικά τοποθετούνται τα αγαθά που πρέπει να προστατευτούν. Χωρίς την εξασφάλιση της φυσικής ασφάλειας, οι βασικές απαιτήσεις για την ασφάλεια των πληροφοριών, δηλαδή η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα θα διατρέχουν σοβαρότατο κίνδυνο. Η ενότητα της πολιτικής ασφαλείας που αφορά τη φυσική ασφάλεια δηλώνει ρητά πώς θα προστατευθούν οι εγκαταστάσεις και ο υλικός εξοπλισμός της εταιρίας. Καθορίζει, επίσης, ποιοι εργαζόμενοι έχουν δικαίωμα πρόσβασης σε απαγορευμένες περιοχές, όπως είναι τα δωμάτια των servers ή οι αποθήκες των καλωδίων. Οι οδηγίες για τη φυσική ασφάλεια μπορεί να αφορούν τον έλεγχο φυσικής πρόσβασης σε κρίσιμους για το πληροφοριακό σύστημα χώρους (π.χ. περιορισμός της κίνησης των επισκεπτών σε συγκεκριμένους χώρους, χρήση ειδικών καρτών για την είσοδο κλπ.).

Ασφάλεια δικτύου

Η ενότητα της ασφάλειας δικτύου δηλώνει τον τρόπο προστασίας των στοιχείων που αποθηκεύονται στο δίκτυο. Μπορεί επίσης να περιλαμβάνει μέτρα ασφάλειας σχετικά με τις τεχνολογίες προστασίας του δικτύου, όπως είναι τα firewalls και τα συστήματα ανίχνευσης επιθέσεων (intrusion detection systems).

Έλεγχος πρόσβασης στα πληροφοριακά συστήματα

Η ενότητα του ελέγχου πρόσβασης καθορίζει ποιος έχει πρόσβαση σε τι. Η πρόσβαση των χρηστών των πληροφοριακών συστημάτων στις πληροφορίες και τις εφαρμογές θα πρέπει να καθορίζεται με βάση τις επιχειρηματικές ανάγκες και τις απαιτήσεις ασφάλειας του εκάστοτε οργανισμού. Πρέπει να υπάρχει μια κατάλληλη διαδικασία που να εξασφαλίζει ότι μόνο οι αρμόδιοι για κάθε υπηρεσία ή πηγή πληροφοριών θα έχουν πρόσβαση σε αυτή. Ο έλεγχος πρόσβασης θα πρέπει να διευκολύνει τους διαχειριστές στη δουλειά τους και να είναι σχετικά εύκολος και κατανοητός ώστε να αποφεύγονται τα λάθη.

Πιστοποίηση

Εκφράζει τον τρόπο που οι χρήστες πιστοποιούν την ταυτότητά τους στο δίκτυο. Ο τύπος της πιστοποίησης που χρησιμοποιείται ποικίλλει ανάλογα με τον τρόπο πρόσβασης των χρηστών στο δίκτυο. Για πρόσβαση από το γραφείο τους, ένα απλό όνομα χρήστη και ένας κωδικός είναι αρκετοί αφού ο έλεγχος πιστοποίησης ενισχύεται από τη φυσική ασφάλεια. Για πρόσβαση όμως στο δίκτυο της επιχείρησης μέσω του Internet μπορεί να χρειαστεί μια πιο περίπλοκη και ασφαλής πιστοποίηση.

Συμμόρφωση με νομικές υποχρεώσεις

Η αναγκαιότητα για τη ύπαρξη της πολιτικής ασφάλειας μπορεί να πηγάζει και από την τυπική υποχρέωση του οργανισμού να ακολουθεί το σχετικό νομικό και κανονιστικό πλαίσιο για τη λειτουργία του. Η ενότητα της συμμόρφωσης επεξηγεί τον τρόπο εφαρμογής της πολιτικής ασφαλείας. Μπορεί επίσης να καθορίζει τις μεθόδους διερεύνησης τυχόν παραβιάσεων της πολιτικής καθώς επίσης και την επιβολή τιμών.

Σχέδιο για την αντιμετώπιση περιστατικών και εκτάκτων αναγκών

Το σχέδιο αυτό εξηγεί τον τρόπο αντιμετώπισης κάθε είδους περιστατικού, από την επίθεση κακόβουλων χρηστών μέχρι μια φυσική καταστροφή. Μπορεί επίσης να απαριθμεί τα μέλη μιας ομάδας αντιμετώπισης έκτακτων περιστατικών που θα διαχειριστούν τέτοια περιστατικά.

Ασφάλεια λογισμικού

Η ενότητα της ασφάλειας λογισμικού επεξηγεί τον τρόπο χρήσης του λογισμικού. Καθορίζει ποιοι έχουν το δικαίωμα να αγοράζουν και να εγκαθιστούν πακέτα λογισμικού στον υλικό εξοπλισμό της εταιρίας, καθώς επίσης και τα μέτρα ασφάλειας όσον αφορά τη λήψη λογισμικού από το Internet.

Σχέδιο συνέχισης λειτουργίας

Μεταξύ άλλων είναι χρήσιμο στην πολιτική ασφάλειας να συμπεριλαμβάνουμε κάποιες οδηγίες για το τι πρέπει να γίνεται μετά την πραγματοποίηση ενός σημαντικού περιστατικού ασφάλειας. Με αυτό τον τρόπο, οι λειτουργίες του οργανισμού που στηρίζονταν στο κομμάτι του πληροφοριακού συστήματος που υπέστη ζημιά θα εξακολουθήσουν να πραγματοποιούνται με κάποιους εναλλακτικούς τρόπους μέχρι την επαναφορά της πλήρους λειτουργικότητας του πληροφοριακού συστήματος.

3.4. Προϋποθέσεις

Εκτός από τα ζητήματα που αντιμετωπίζει, η πολιτική ασφαλείας έχει και κάποιες βασικές προϋποθέσεις που θα πρέπει να εκπληρώνονται ώστε να έχει το επιθυμητό αποτέλεσμα: Τα βασικά χαρακτηριστικά της πολιτικής ασφάλειας εκφράζονται σε έναν αριθμό απαιτήσεων όπως [16]:

- Απαιτεί συμμόρφωση από το προσωπικό της επιχείρησης. Οι κανονισμοί που δηλώνονται μέσω αυτής καθορίζουν οτιδήποτε αφορά την ασφάλεια του πληροφοριακού συστήματος και γι' αυτό το έγγραφο της πολιτικής ασφάλειας θα πρέπει να είναι στη διάθεση όλου του προσωπικού.

- Εκφράζει γενικότερες απόψεις ή αρχές της επιχείρησης. Η υλοποίηση της πολιτικής ασφάλειας επηρεάζεται από την υπάρχουσα κουλτούρα και το γενικότερο σύνολο αρχών και πεποιθήσεων.

- Είναι σαφής ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της, καθώς και εφαρμόσιμη από άποψη κόστους.

- Είναι γενικεύσιμη ώστε η εφαρμογή της να είναι επεκτάσιμη σε μελλοντικά συστήματα που ενδεχομένως ενταχθούν στο πληροφοριακό σύστημα της επιχείρησης.

- Είναι απαλλαγμένη από μη απαραίτητους τεχνικούς όρους και εξειδικευμένες αναφορές ώστε να μην καθίσταται δύσκολη στην εφαρμογή της και εξαρτημένη από τεχνολογικές επιλογές καθώς και να μην τροποποιείται συχνά, παρά μόνο όταν συμβαίνουν σημαντικές αλλαγές στην οργανωτική δομή και στην κουλτούρα της επιχείρησης, στις απαιτήσεις ασφαλείας καθώς και στις τεχνολογικές εξελίξεις.

3.5. Οι εμπλεκόμενοι σύνταξης της πολιτικής ασφαλείας

Ποιοι είναι αυτοί οι οποίοι εμπλέκονται στο δύσκολο έργο της σύνταξης της πολιτικής ασφαλείας μιας επιχείρησης; Ο υπεύθυνος ασφαλείας της επιχείρησης, οι υπεύθυνοι και οι διαχειριστές του δικτύου της εταιρίας, οι υπεύθυνοι των τμημάτων που επηρεάζονται άμεσα ή έμμεσα από την εφαρμογή της συγκεκριμένης πολιτικής ασφαλείας, οι υπεύθυνοι εφαρμογής αντιμέτρων σε περιπτώσεις παραβιάσεων, αντιπρόσωποι από την διοίκηση της επιχείρησης και φυσικά οι νομικοί σύμβουλοι.

3.6. Εκπαίδευση χρηστών

Ακόμα και η καλύτερη δυνατή πολιτική ασφαλείας μπορεί να αποδειχθεί αναποτελεσματική εάν οι χρήστες του δικτύου μιας εταιρίας ή οργανισμού δεν έχουν την κατάλληλη ενημέρωση και εκπαίδευση σε θέματα ασφάλειας. Πολλές φορές οι υπεύθυνοι ασφάλειας σχεδιάζουν την "τέλεια" πολιτική ασφάλειας, αλλά ξεχνούν να συμπεριλάβουν το προσωπικό της εταιρίας στον σχεδιασμό τους με αποτέλεσμα να δημιουργούνται σημαντικά προβλήματα από λάθη που οφείλονται σε άγνοια ή αμέλεια των χρηστών.

Σκοπός της εκπαίδευσης λοιπόν, είναι η εξασφάλιση της ενημέρωσης των χρηστών για τους κινδύνους κατά της ασφάλειας των δικτύων και των πληροφοριακών συστημάτων του οργανισμού και η διασφάλιση ότι είναι κατάλληλα προετοιμασμένοι για την εφαρμογή της πολιτικής ασφαλείας του οργανισμού στην καθημερινή τους εργασία. Οι χρήστες θα πρέπει να εκπαιδεύονται στις διαδικασίες ασφάλειας και τη σωστή χρήση του δικτύου ώστε να ελαχιστοποιηθούν οι πιθανοί κίνδυνοι κατά της ασφάλειας του οργανισμού.

Όλοι οι υπάλληλοι του οργανισμού, και όπου αυτό είναι απαραίτητο και εξωτερικοί συνεργάτες, θα πρέπει να εκπαιδεύονται κατάλληλα και να ενημερώνονται για την πολιτική ασφάλειας και τις όποιες αλλαγές γίνονται σε αυτήν. Θα πρέπει να γνωρίζουν τις διαδικασίες, τις νομικές ευθύνες, τους μηχανισμούς προστασίας και τη σωστή χρήση του δικτύου. Η εκπαίδευση θα πρέπει να γίνεται πριν δοθεί στους χρήστες πρόσβαση στο δίκτυο της εταιρίας.

3.7. Σχέδιο Επιχειρησιακής Συνέχειας

Εκτός από το σχεδιασμό και την εφαρμογή της πολιτικής ασφαλείας, πολύ σημαντική επίσης για την εύρυθμη λειτουργία μιας εταιρίας ή οργανισμού είναι και η διαχείριση της επιχειρησιακής συνέχειας. Σκοπός της είναι η αποτροπή παρεμβολών στις επιχειρηματικές δραστηριότητες του οργανισμού και η προστασία των κρίσιμων διαδικασιών στην περίπτωση μερικών ή ολικών καταστροφών. Για το λόγο αυτό, καταρτίζεται το "Σχέδιο Επιχειρησιακής Συνέχειας" (Business Continuity Plan) το οποίο αποτελεί έναν λεπτομερή οδηγό τόσο για την αντιμετώπιση εκτάκτων περιστατικών που θέτουν σε κίνδυνο την εύρυθμη λειτουργία ενός οργανισμού, όσο και για την ανάκαμψη (recovery) συστημάτων έπειτα από οποιαδήποτε ζημία ή καταστροφή.

Σκοπός της εκπόνησης ενός Σχεδίου Επιχειρησιακής Συνέχειας, είναι η αποτροπή εμποδίων στις επιχειρηματικές δραστηριότητες του οργανισμού και η προστασία των κρίσιμων διαδικασιών στην περίπτωση μερικών ή ολικών καταστροφών στα συστήματά του. Μια διαδικασία διαχείρισης της επιχειρησιακής συνέχειας του οργανισμού (business continuity management process) θα πρέπει να αξιοποιείται για τη μείωση, σε ανεκτό επίπεδο, των επιπτώσεων από καταστροφές και συμβάντα σχετικά με την ασφάλεια του οργανισμού. Τέτοιες καταστροφές μπορεί να είναι αποτέλεσμα φυσικών καταστροφών, αστοχίας υλικών ή σκόπιμων ενεργειών. Επιπλέον θα πρέπει να περιλαμβάνονται και μέτρα για την αποκατάσταση της ομαλής λειτουργίας του οργανισμού. Ο σχεδιασμός για την αντιμετώπιση απρόοπτων γεγονότων θα πρέπει να εξασφαλίζει την αποκατάσταση των επηρεαζόμενων λειτουργιών μέσα σε ένα ρεαλιστικό και αποδεκτό χρονικό πλαίσιο.

Ο οργανισμός θα πρέπει να χρησιμοποιεί μια συγκεκριμένη διαδικασία για το σχεδιασμό και την υλοποίηση της επιχειρησιακής συνέχειας, η οποία θα πρέπει να βασίζεται στα ακόλουθα:

- Την κατανόηση των κινδύνων που ενδέχεται να απειλούν τον οργανισμό, την πιθανότητα να υλοποιηθούν και το κόστος που θα επιφέρουν. Θα πρέπει επίσης να καθοριστούν οι κρίσιμες λειτουργίες του οργανισμού και να κατηγοριοποιηθούν με βάση την προτεραιότητά τους για τον οργανισμό.

- Την κατανόηση των επιπτώσεων κάθε παρεμβολής στη φυσιολογική λειτουργία του οργανισμού. Θα πρέπει να υπάρχει κάποιο σχέδιο αντιμετώπισης τόσο των μικρών, όσο και των σοβαρών συμβάντων.

- Την πιθανή σύναψη κατάλληλου ασφαλιστηρίου συμβολαίου, το οποίο μπορεί να είναι μέρος του σχεδίου επιχειρησιακής συνέχειας.

- Την κατάστρωση μιας στρατηγικής επιχειρησιακής συνέχειας η οποία θα πρέπει να είναι σύμφωνη με τους στόχους και τις προτεραιότητες του οργανισμού.

- Την καταγραφή ενός σχεδίου επιχειρησιακής συνέχειας το οποίο θα υλοποιεί την παραπάνω στρατηγική.

- Τον τακτικό έλεγχο και την τακτική ενημέρωση του σχεδίου και των διαδικασιών που προβλέπονται σε αυτό.

- Την ενσωμάτωση του σχεδίου επιχειρησιακής συνέχειας σε όλες τις λειτουργίες του οργανισμού. Η ευθύνη της υλοποίησης του σχεδίου θα πρέπει να βρίσκεται μέσα στον οργανισμό.

3.8. Παράγοντες εξασφάλισης της ασφάλειας

Οι ακόλουθοι παράγοντες έχουν ιδιαίτερη σημασία στην εξασφάλιση της ασφάλειας δικτύων και πληροφοριών μέσα σε μία επιχείρηση:

- Πολιτική ασφάλειας, στόχοι και δραστηριότητες που αντικατοπτρίζουν τους στόχους της επιχείρησης.

- Εφαρμογή διαδικασιών ασφάλειας με τρόπο συμβατό με την κουλτούρα της επιχείρησης.

- Ενεργή υποστήριξη από τη διοίκηση της επιχείρησης.

- Κατανόηση των απαιτήσεων ασφάλειας, της αποτίμησης κινδύνων και της διαχείρισής τους.

- Κατανόηση από όλο το προσωπικό της επιχείρησης της αναγκαιότητας ύπαρξης και λειτουργίας μηχανισμών ασφάλειας.
- Γνώση της πολιτικής ασφάλειας από όλο το προσωπικό και από τους εξωτερικούς συνεργάτες.
- Εκπαίδευση και επιμόρφωση του προσωπικού.
- Ένα κατανοητό και ισορροπημένο σύστημα μέτρησης που να μπορεί να αξιολογήσει την απόδοση του συστήματος ασφάλειας των πληροφοριών και να προτείνει πιθανές βελτιώσεις.

ΚΕΦΑΛΑΙΟ 4

ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Οι μικρομεσαίες επιχειρήσεις (ΜΜΕ) αποτελούν τομέα προτεραιότητας ενδιαφέροντος στον οποίο επικεντρώνεται η κυβερνητική οικονομική πολιτική κάθε χώρας και θεωρούνται μείζονος σημασίας για την κοινωνικοοικονομική ανάπτυξη στην Ευρωπαϊκή Ένωση. Οι ΜΜΕ συνήθως δημιουργούνται από επιχειρηματικό πάθος και ελλιπή χρηματοδότηση, με επιχειρησιακά συστήματα, τα οποία συχνά είναι ετερογενή και ανεξάρτητα. Επιπρόσθετα, οι υλικοί και άυλοι επιχειρηματικοί πόροι των ΜΜΕ ορίζονται στοιχειωδώς και η αξία αυτών των πόρων, συχνά, είναι γνωστή μόνο εν μέρει. Συνήθως, αυτό συμβαίνει με έναν από τα πιο σημαντικούς πόρους, δηλαδή τις πληροφορίες.

Όπως συμβαίνει με κάθε άλλο επιχειρηματικό πόρο, οι πληροφορίες απαιτείται να διαχειρίζονται και να προστατεύονται με στρατηγική. Ασφάλεια των πληροφοριών θεωρείται η προστασία των πληροφοριών μέσα σε μια επιχείρηση, συμπεριλαμβανομένων των συστημάτων και του υλικού εξοπλισμού που χρησιμοποιούνται για την αποθήκευση, την επεξεργασία και την μετάδοση αυτών των πληροφοριών. Είναι επιβεβλημένο η επιχειρηματική ηγεσία των ΜΜΕ να κατανοήσει την αξία των πληροφοριών, που εμπεριέχονται στα επιχειρησιακά συστήματά τους και να διαθέτει πλαίσιο αξιολόγησης και υλοποίησης της ασφάλειας των πληροφοριών. Πολυάριθμα διεθνώς εγκεκριμένα πλαίσια και προγράμματα ασφάλειας μπορούν να εφαρμοστούν για να προστατεύσουν έναν οργανισμό από την απώλεια πληροφοριών και την ενδεχόμενη ευθύνη. Δεδομένου ότι αυτά τα πλαίσια είναι περίπλοκα, καθολικά και, σε τελευταία ανάλυση, ακριβά στην εφαρμογή τους, υιοθετούνται κυρίως από μεγάλους οργανισμούς.

Συνήθως, λόγω της δυναμικής και της ad hoc ανάπτυξης πολλών ΜΜΕ, δεν αντιμετωπίζονται συστηματικά ούτε τα ζητήματα ενσωμάτωσης ούτε τα θέματα ασφάλειας κατά το στάδιο της δημιουργίας μιας επιχείρησης. Για τον λόγο αυτό, πολιτικές και πλαίσια για τον σχεδιασμό της ασφάλειας πληροφοριών και της ανάκτησης από καταστροφή είναι συνήθως πολύ στοιχειώδεις ή ακόμα και απούσες/απόντα. Συχνά, είναι πιθανό η βασική κατανόηση των κινδύνων που αφορούν στην ασφάλεια των πληροφοριών να μην εκτείνεται πολύ πιο πέρα από

τους ιούς και το αντιικό λογισμικό. Οι ακούσιες απειλές θέτουν ορισμένους από τους υψηλότερους κινδύνους για την ασφάλεια των πληροφοριών στις ΜΜΕ και, επιπλέον, συχνά παραμελούνται η κατάρτιση του προσωπικού και τα προγράμματα ενημέρωσης.

Τα αποτελέσματα των ερευνών αποκαλύπτουν ότι το επίπεδο της ευαισθητοποίησης σε θέματα της ασφάλειας των πληροφοριών μεταξύ ηγετών των ΜΜΕ είναι τόσο μεταβλητό όσο και η κατάσταση των πληροφοριακών συστημάτων, της πληροφορικής τεχνολογίας και της ασφάλειας των πληροφοριών τους. Αν και μια μειονότητα των ΜΜΕ δέχεται ένθερμα πλαίσια ασφάλειας όπως το ISO / IEC 27001 ή το διεθνές ισοδύναμο ISO 17799, τα περισσότερα διοικητικά στελέχη των ΜΜΕ δεν έχουν ακουστά για τα πρότυπα ασφάλειας και θεωρούν την ασφάλεια των πληροφοριών μόνο σαν μια τεχνική παρέμβαση σχεδιασμένη να αντιμετωπίζει τις απειλές από τους ιούς και να επιλαμβάνεται της δημιουργίας εφεδρικών αντιγράφων ασφάλειας δεδομένων [17].

Τα διοικητικά στελέχη όχι μόνον κατηγορούνται για το ότι δεν κατανοούν το καθοριστικό ζήτημα που περιβάλλει την ασφάλεια των πληροφοριών, αλλά οι έρευνες καταλήγουν στο ότι η ηγεσία των ΜΜΕ είναι ανάγκη να καταπιαστεί με, να κατανοήσει και να υλοποιήσει επίσημες διαδικασίες ασφάλειας των πληροφοριών, συμπεριλαμβανομένων των τεχνικών και των οργανωτικών μέτρων. Χωρίς τέτοια μέτρα, οι οργανισμοί τους μπορεί να επηρεαστούν σε υπερβολικό βαθμό από ακούσιες απειλές ή εσκεμμένες επιθέσεις στα συστήματα πληροφοριών τους, που εν τέλει, θα μπορούσαν να οδηγήσουν σε αποτυχία της επιχείρησης.

Βάσει των περιεχομένων αυτού του πακέτου πληροφοριών, οι ΜΜΕ θα είναι σε θέση να διενεργούν εκτιμήσεις κινδύνων στα περιβάλλοντά τους, να επιλέγουν και να εφαρμόζουν κατάλληλα μέτρα για την διαχείριση κινδύνων που σχετίζονται με τη ασφάλεια πληροφοριών.

4.1. Διαχείριση Κινδύνων

Σήμερα, ένα από τα πολυτιμότερα κεφάλαια μιας επιχείρησης είναι η δημιουργία, η επεξεργασία και η χρήση των πληροφοριών. Η δημοσιοποίηση, η διακύβευση ή η μη διαθεσιμότητα αυτού του πόρου μπορεί να έχει σοβαρές συνέπειες για την επιχείρηση, να στοιχειοθετήσει παράβαση νομοθετικών κανόνων και κανονισμών και να επηρεάσει αρνητικά το εμπορικό της σήμα.

Η επαρκής ασφάλεια των πληροφοριών και των συστημάτων επεξεργασίας πληροφοριών αποτελεί θεμελιώδη ευθύνη της διεύθυνσης της επιχείρησης. Οι ιδιοκτήτες και οι υπεύθυνοι λήψης αποφάσεων πρέπει να συνειδητοποιήσουν την τρέχουσα κατάσταση του προγράμματος ασφάλειας των πληροφοριών τους προκειμένου να προβούν σε σωστές κρίσεις και επενδύσεις περιορίζοντας ανάλογα τους κινδύνους σ' ένα αποδεκτό επίπεδο. Οι κίνδυνοι που συνδέονται με τις πληροφορίες μπορούν να οδηγήσουν σε κρίσιμες καταστάσεις όταν παρεκταθούν σε ζωτικής σημασίας εμπορικά και νομικά ζητήματα της επιχείρησης. Συνεπώς, οι κίνδυνοι που συνδέονται με τις πληροφορίες μπορούν να οδηγήσουν σε γενικότερες και κρισιμότερες κατηγορίες κινδύνων όπως [18]:

- *Ο νομικός κίνδυνος / κίνδυνος συμμόρφωσης*: Ο κίνδυνος ο οποίος προκύπτει από παραβιάσεις της νομοθεσίας ή τη μη συμμόρφωση με λογιστικούς κανόνες, κανονισμούς, εναρμονισμένες πρακτικές ή ηθικά πρότυπα. Νομικοί κίνδυνοι ή κίνδυνοι συμμόρφωσης μπορούν να δημιουργήσουν αρνητική δημόσια εικόνα για μία επιχείρηση, να οδηγήσουν στην επιβολή ποινικών και αστικών χρηματικών προστίμων, την καταβολή αποζημίωσης και την ακύρωση συμβολαίων. Η υποκλοπή πληροφοριών που αφορούν πελάτες, όπως πληροφορίες πιστωτικών καρτών, πληροφορίες οικονομικής φύσεως, πληροφορίες για θέματα υγείας ή άλλα προσωπικά δεδομένα μπορούν, επίσης, να εγείρουν πιθανούς κινδύνους από απαιτήσεις τρίτων. Αναγνωρίζοντας την ασφάλεια των πληροφοριών ως ένα πολύπλευρο ζήτημα που προκαλεί ιδιαίτερη ανησυχία και προκειμένου να προστατευθούν τα πολιτικά δικαιώματα και να διασφαλιστεί η εταιρική ευθύνη, οι κυβερνήσεις της ΕΕ και η Ευρωπαϊκή Ένωση έχουν θεσπίσει νόμους και κανονισμούς, οι οποίοι απαιτούν την συμμόρφωση των φορέων ανεξάρτητα από το μέγεθός τους ή τον κλάδο οικονομικής δραστηριότητας στον οποίο ανήκουν. Αυτοί οι κανονισμοί

υποχρεώνουν τις εταιρείες να εφαρμόζουν εσωτερικούς ελέγχους ώστε να προστατευθούν έναντι των κινδύνων που συνδέονται με τις πληροφορίες. Στοχεύουν, επίσης, στην βελτίωση των πρακτικών και των διαδικασιών διαχείρισης κινδύνων.

- *Οι κίνδυνοι οικονομικής σταθερότητας*: Η έλλειψη κατάλληλης παραγωγικής υποδομής, υποδομής διαχείρισης ή προσωπικού για την υλοποίηση της επιχειρηματικής στρατηγικής του φορέα μπορεί να οδηγήσει σε αδυναμία επίτευξης των διακηρυγμένων σκοπών και οικονομικών στόχων που έχουν τεθεί σ' ένα καλά διαχειριζόμενο και ελεγχόμενο περιβάλλον. Η λανθασμένη διαχείριση της ασφάλειας των πληροφοριών μπορεί να επεκταθεί σε κινδύνους που σχετίζονται με την οικονομική σταθερότητα της επιχείρησης. Τέτοιοι κίνδυνοι, με την σειρά τους, μπορούν να οδηγήσουν σε απάτες, ξέπλυμα βρώμικου χρήματος, οικονομική αστάθεια κτλ.

- *Ο κίνδυνος παραγωγικότητας*: Ο κίνδυνος ζημιών εκμετάλλευσης και χαμηλής ποιότητας παροχής υπηρεσιών προς τον πελάτη, σαν συνέπεια της μη απαρέγκλιτης τήρησης βασικών διαδικασιών και ελέγχων επεξεργασίας. Ο κίνδυνος αυτός, συνήθως, αφορά όλες τις συνεργατικές δραστηριότητες παραγωγής, οι οποίες, κατά κάποιο τρόπο, συνεισφέρουν στην συνολική παράδοση ενός προϊόντος ή την συνολική παροχή μιας υπηρεσίας. Ο κίνδυνος παραγωγικότητας δεν περιορίζεται στην χρήση της τεχνολογίας - μπορεί εξίσου να είναι το αποτέλεσμα οργανωτικών δραστηριοτήτων. Ο κίνδυνος που προκύπτει από ανεπαρκή ή ελλιπώς ελεγχόμενα συστήματα και εφαρμογές λογισμικού, τα οποία χρησιμοποιούνται για να υποστηρίξουν το γραφείο εξυπηρέτησης, τις διαδικασίες διαχείρισης κινδύνων, το τμήμα λογιστηρίου ή άλλες μονάδες, υπάγεται σ’ αυτήν την οικογένεια κινδύνων. Η ανεπαρκής διαχείριση της ασφάλειας των πληροφοριών μπορεί να οδηγήσει σε υψηλούς κινδύνους για την παραγωγικότητα συμπεριλαμβανομένων των υψηλών λειτουργικών εξόδων, των φαινομένων δυσλειτουργίας, των αποφάσεων κακής διαχείρισης (τιμή, ρευστότητα και ανοίγματα σε πιστωτικό κίνδυνο) και σε απουσία της ιδιωτικότητας, καθώς και στην διακοπή της παροχής υπηρεσιών προς τους πελάτες.

- *Φήμη και Εμπιστοσύνη Πελατών*: Ενδεχομένως, ο πιο δύσκολος και, ωστόσο, ένας από τους πιο σημαντικούς κινδύνους που πρέπει να γίνει κατανοητός είναι ο κίνδυνος πρόκλησης βλάβης στην φήμη της επιχείρησης, ένας άυλος αλλά σημαντικός πόρος. Θα δώσουν οι πελάτες τους αριθμούς της πιστωτικών καρτών τους σε μια εταιρεία απ' τη στιγμή που θα διαβάσουν στον τύπο ότι κάποιος παρείσφρησε στην βάση δεδομένων της εταιρείας; Θα παραμείνουν οι υψηλά ιστάμενοι υπάλληλοι σε μια τόσο ζημιωμένη εταιρεία; Και, ποια θα είναι η αντίδραση των μετόχων της εταιρείας; Ποια είναι η αναμενόμενη απώλεια των μελλοντικών εσόδων της επιχείρησης; Ποια είναι η αναμενόμενη απώλεια της χρηματιστηριακής κεφαλαιοποίησης;

Πολλοί ιδιοκτήτες ΜΜΕ νομίζουν πως δεν βρίσκονται σε κίνδυνο λόγω του μεγέθους της επιχείρησής τους και των πληροφοριακών τους πόρων. Οι περισσότεροι θεωρούν ότι οι μεγάλες επιχειρήσεις, οι οποίες διαθέτουν περισσότερους πόρους, είναι οι μόνες που κινδυνεύουν. Όμως αυτό δεν είναι αληθές. Πρώτον, η ευαισθησία των πληροφοριών απευθύνεται στην ποιότητα και όχι στην ποσότητα των πληροφοριών. Δεύτερον, οι ΜΜΕ δεν διαθέτουν τους πόρους ή το προσωπικό για να αντιμετωπίσουν το ζήτημα της ασφάλειας με εξίσου εντατικές μεθόδους όπως αυτές που χρησιμοποιούνται στις μεγάλες επιχειρήσεις και, επομένως, είναι περισσότερο εκτεθειμένες. Πράγματι, η νέα τεχνολογία επιτρέπει στις μικρές επιχειρήσεις να χρησιμοποιούν πολλά από τα ίδια πληροφοριακά συστήματα που διαθέτουν οι μεγάλες επιχειρήσεις. Όμως, με τον τρόπο αυτό, οι μικρές επιχειρήσεις εκτίθενται οικειοθελώς σε πολλές απειλές που σχετίζονταν παραδοσιακά με τις μεγάλες επιχειρήσεις. Στην πραγματικότητα, πάνω από το μισό των μικρών επιχειρήσεων αντιμετώπισαν τουλάχιστον ένα συμβάν ασφάλειας κατά τον τελευταίο χρόνο. Δυστυχώς, ένα σημαντικό μέρος των επιχειρήσεων, οι οποίες αντιμετωπίζουν μείζονα βλάβη των υπολογιστικών τους συστημάτων, ποτέ δεν καταφέρνουν να επανακάμψουν και, έτσι, η επιχείρηση καταρρέει από μόνη της. Επομένως, προκειμένου να συνεχίσουν την επιτυχημένη πορεία τους, επιβάλλεται οι ιδιοκτήτες των ΜΜΕ και οι υπεύθυνοι λήψης αποφάσεων να αναγνωρίσουν αυτούς τους σκοπέλους και να λάβουν μέτρα ώστε να αντιμετωπίσουν τα ζητήματα της ασφάλειας των πληροφοριών.

Τα μέτρα (έλεγχοι) περιορισμού των κινδύνων της ασφάλειας των πληροφοριών πρέπει να είναι ανάλογα με τους κινδύνους που αντιμετωπίζουν οι εν λόγω πληροφορίες. Ωστόσο, η διαδικασία καθορισμού σχετικά με το ποιοι έλεγχοι ασφάλειας είναι ενδεδειγμένοι και αποτελεσματικοί από οικονομική άποψη, αρκετά συχνά είναι ένα πολυσύνθετο και, ορισμένες φορές, υποκειμενικό ζήτημα. Μια απ' τις πρωταρχικές λειτουργίες για να τεθεί αυτή η διαδικασία σε μια πιο αντικειμενική βάση είναι η διαρκής εκτίμηση των κινδύνων που συνδέονται με την ασφάλεια.

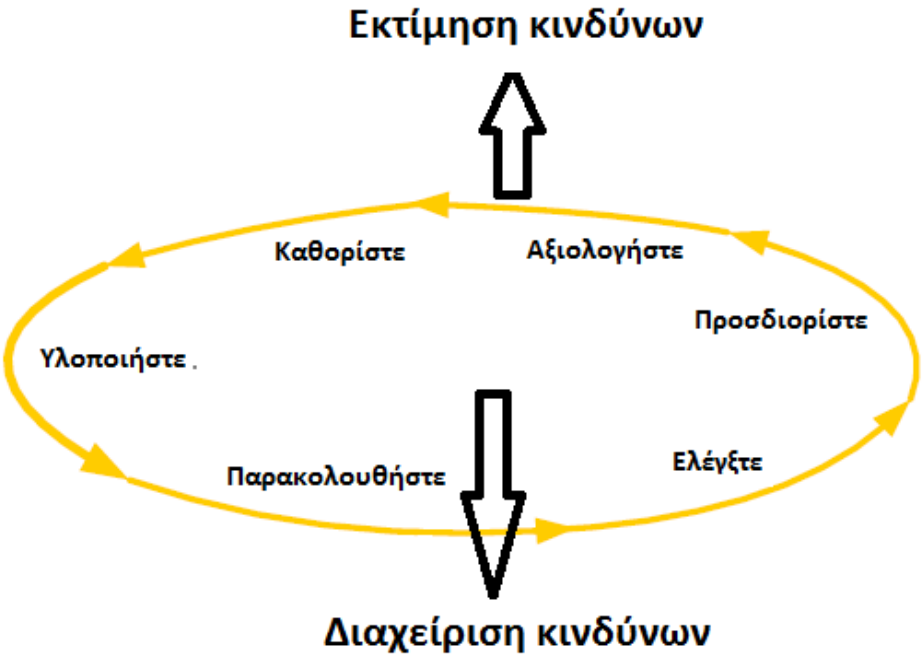
4.2. Εκτίμηση Κινδύνων

Η ασφάλεια των πληροφοριών έχει να κάνει με την αναγνώριση, τον μετριασμό και την διαχείριση κινδύνων που σχετίζονται με τις πληροφορίες. Η εκτίμηση κινδύνων είναι το πρώτο αναγκαίο μέτρο για την κατανόηση των κινδύνων, διεξάγοντας μια συνολική αναγνώριση και αξιολόγηση κινδύνων αναφορικά με τους κινδύνους ασφάλειας των πληροφοριών μιας επιχείρησης. Το αποτέλεσμα αυτής της δραστηριότητας είναι ουσιώδες για την διαχείριση της επιχείρησης καθώς οι ενεχόμενοι κίνδυνοι μπορούν να επηρεάσουν σε σημαντικό βαθμό την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών. Μπορεί, επίσης, να είναι ζωτικής σημασίας για την διατήρηση του ανταγωνιστικού προβαδίσματος, της οικονομικής σταθερότητας, της νομικής συμμόρφωσης και της δυνατής εμπορικής εικόνας της επιχείρησης. Συνεπώς, η εκτίμηση κινδύνων μπορεί να βοηθήσει τους υπεύθυνους λήψης αποφάσεων να:

- Αποτιμήσουν τις οργανωτικές πρακτικές και την τεχνολογική βάση που έχει εγκατασταθεί.
- Ενισχύσουν την προστασία των πληροφοριών βάσει των δυνητικών επιπτώσεων στον οργανισμό.
- Επικεντρώσουν τις ενέργειες για την ασφάλεια σε σημαντικά ζητήματα, εγκαταλείποντας μέτρα που σχετίζονται με αποδεκτούς κινδύνους.
- Διασφαλίσουν ότι τα εφαρμοζόμενα μέτρα και οι υλοποιούμενες δαπάνες είναι πλήρως ανάλογα με τους κινδύνους στους οποίους εκτίθεται ο οργανισμός.

Κατ' αυτόν τον τρόπο, μπορεί να διατηρηθεί ισορροπία μεταξύ των εξόδων αντιμετώπισης ενός κινδύνου και των οφελών που προέρχονται από την αποφυγή της αρνητικής επίπτωσης.

Κατά την διάρκεια μιας εκτίμησης κινδύνων, μία επιχείρηση πραγματοποιεί ενέργειες για να: (α) αναγνωρίσει τους κινδύνους ασφάλειας πληροφοριών, (β) αξιολογήσει τους κινδύνους ώστε να καθορίσει προτεραιότητες και (γ) ορίσει τον τρόπο με τον οποίο θα μετριάσει τους κινδύνους (*Σχήμα 1*).



Σχήμα 1: Δραστηριότητες εκτίμησης κινδύνων σε σχέση με την διαχείριση κινδύνων για την ασφάλεια των πληροφοριών

Ωστόσο, η εκτίμηση κινδύνων για την ασφάλεια των πληροφοριών είναι μόνο το πρώτο βήμα για την διαχείριση κινδύνων ασφάλειας των πληροφοριών, η οποία αποτελεί τη συνεχή διαδικασία αναγνώρισης κινδύνων και εφαρμογής σχεδίων για την αντιμετώπισή τους. Στο Σχήμα 1 απεικονίζεται μια διαδικασία διαχείρισης κινδύνων για την ασφάλεια των πληροφοριών και το 'μερίδιο" της διαχείρισης κινδύνων που συνιστά η εκτίμηση κινδύνων.

Σαφώς, η ίδια η εκτίμηση κινδύνων παρέχει μια κατεύθυνση για τις δραστηριότητες που αφορούν στην ασφάλεια των πληροφοριών ενός οργανισμού ενώ δεν οδηγεί απαραίτητα σε σημαντικές βελτιώσεις εκτός κι αν έχει λάβει χώρα η εφαρμογή μέτρων. Όπως συμβαίνει με κάθε άλλο τομέα διαχείρισης, η υλοποίηση μόνο ενός μέρους του κύκλου ζωής της διαχείρισης δεν φέρνει τα επιθυμητά αποτελέσματα. Καμία αξιολόγηση, ανεξάρτητα από το πόσο εμπεριστατωμένη ή εξειδικευμένη είναι, δε βελτιώνει την θεώρηση της ασφάλειας εκτός αν η επιχείρηση διεκπεραιώνει την εφαρμογή της. Πέρα από την εκτίμηση κινδύνων, η αποτελεσματική διαχείριση κινδύνων περιλαμβάνει τις ακόλουθες ενέργειες:

- Προγραμματισμός του τρόπου με τον οποίο θα εφαρμοστεί η στρατηγική για την προστασία των πληροφοριών και τα σχέδια για τον μετριασμό των κινδύνων από την αξιολόγηση μέσα από την ανάπτυξη αναλυτικών σχεδίων δράσης. Η δραστηριότητα αυτή μπορεί να περιλαμβάνει μια λεπτομερή ανάλυση κόστους–οφέλους ποικίλων στρατηγικών και δράσεων.

- Εφαρμογή των επιλεγμένων αναλυτικών σχεδίων δράσης.

- Παρακολούθηση της προόδου και της αποτελεσματικότητας των σχεδίων. Η δραστηριότητα αυτή περιλαμβάνει την παρακολούθηση οποιονδήποτε μεταβολών των επιπέδων κινδύνων.

- Έλεγχος των αποκλίσεων στην εκτέλεση των σχεδίων με την λήψη των κατάλληλων διορθωτικών μέτρων.

4.3. Ασφάλεια Πληροφοριών

Μέρος της ευθύνης των διευθυντών των μικρομεσαίων επιχειρήσεων είναι να προνοούν για την ασφάλεια του επιχειρηματικού τους περιβάλλοντος. Σύμφωνα με τις περισσότερες ισχύουσες νομικές απαιτήσεις, η ευθύνη για συμβάντα παραβίασης της ασφάλειας βαρύνει αυτούς. Όπως ακριβώς είναι υποχρεωμένοι να παρέχουν ένα ασφαλές και σταθερό φυσικό περιβάλλον, οφείλουν παράλληλα, να διασφαλίζουν ότι οι πληροφορίες της επιχείρησής τους προστατεύονται.

Δεδομένου του γεγονότος, ωστόσο, ότι οι υπολογιστές δεν είναι συσκευές "μιας επισκευής", η προστασία των πληροφοριών αποτελεί σταθερό μέλημα.

Οι υπεύθυνοι λήψης αποφάσεων μπορούν να θέσουν σε εφαρμογή την διαδικασία εκτίμησης κινδύνων για το περιβάλλον τους και να ενεργοποιήσουν την λήψη κατάλληλων μέτρων προκειμένου να αντιμετωπίσουν μη αποδεκτούς κινδύνους. Αυτό αποτελεί προϋπόθεση για την διαχείριση της ασφάλειας των πληροφοριών. Για την διεξαγωγή αυτής της διαδικασίας, μπορούν να εφαρμοστούν ποικίλες προσεγγίσεις σχετικά με την στελέχωση μιας τέτοιας προσπάθειας (επίσης γνωστή ως απόφαση κάποιου να "δημιουργήσει ή να αγοράσει").

Διαφοροποιούμε τρεις προσεγγίσεις:

- *Εσωτερική ανάθεση της εκτίμησης κινδύνων*: η εκτίμηση κινδύνων και ο προσδιορισμός των αναγκαίων μέτρων επιτελούνται από το εσωτερικό προσωπικό της επιχείρησης. Η εκτίμηση βασίζεται στην προσέγγιση εκτίμησης κινδύνων που έχει επιλέξει ο οργανισμός (π.χ. μία ορθή πρακτική, ένα γνωστό πρότυπο κτλ.). Η διαδικασία αυτή θα βοηθήσει την επιχείρηση να αποκτήσει άρτια γνώση της προσέγγισης εκτίμησης για επαναλαμβανόμενες περιπτώσεις εφαρμογής της συγκεκριμένης διαδικασίας.

- *Εξ' ολοκλήρου εξωτερική ανάθεση της εκτίμησης κινδύνων*: σύμφωνα με αυτήν την προσέγγιση, η συνολική εκτίμηση κινδύνων διενεργείται από έναν εξωτερικό ανάδοχο. Η εκτίμηση βασίζεται στην προσέγγιση εκτίμησης κινδύνων που επιλέγει αυτός. Ο ανάδοχος μπορεί επίσης να αναλάβει την διενέργεια επαναλαμβανόμενων μελλοντικών εκτιμήσεων. Δεν προβλέπεται μεταφορά τεχνογνωσίας στο εσωτερικό προσωπικό της επιχείρησης για ολόκληρο τον κύκλο ζωής της εκτίμησης κινδύνων/διαχείρισης κινδύνων της ΜΜΕ.

- *Εν μέρει εξωτερική ανάθεση της εκτίμησης κινδύνων*: σύμφωνα με την προσέγγιση αυτή θεωρείται ότι η αρχική εκτίμηση κινδύνων διενεργείται από μια εξωτερική εταιρεία. Η εκτίμηση βασίζεται σε μια προσέγγιση εκτίμησης κινδύνων που είναι γνωστή στην ΜΜΕ. Κατά συνέπεια, περαιτέρω εκτιμήσεις κινδύνων μπορούν να διενεργηθούν από το προσωπικό της επιχείρησης. Η

αρχική εκτίμηση, η οποία διενεργείται από εξωποριστή, χρησιμεύει ως μεταφορά τεχνογνωσίας στο προσωπικό της ΜΜΕ.

Η προτεινόμενη προσέγγιση εκτίμησης κινδύνων μπορεί να χρησιμοποιηθεί σε αποφάσεις εσωτερικής ανάθεσης και εν μέρει εξωτερικής ανάθεσης ως κατευθυντήρια γραμμή για τις αρχικές και τις μελλοντικές εκτιμήσεις κινδύνων. Κάθε προσέγγιση εκτίμησης κινδύνων, όταν συγκρίνεται με όλες τις άλλες προσεγγίσεις, συνδέεται με πλεονεκτήματα και μειονεκτήματα.

4.3.1. Εσωτερική ανάθεση

Η εσωτερική ανάθεση μπορεί να προσφέρει πολλά πλεονεκτήματα στον φορέα όπως την ανάπτυξη εσωτερικής τεχνογνωσίας και ικανοτήτων για την εκτίμηση και την διαχείριση κινδύνων. Σε αυτό το πλαίσιο, ανάλογα με τις τιμές παροχής συμβουλευτικών υπηρεσιών, που ισχύουν στην αγορά του τομέα της ασφάλειας, αυτή η προσέγγιση μπορεί να οδηγήσει σε μείωση των δαπανών. Η επιλογή αυτή είναι ιδιαίτερα ελκυστική για οργανισμούς με απλή δομή, επιτυχημένο ιστορικό στην εσωτερική υλοποίηση παρόμοιων δραστηριοτήτων (δηλ. ISO9001), επαρκείς ικανότητες και δεξιότητες.

4.3.2. Εξ' ολοκλήρου εξωτερική ανάθεση

Μέσω της εξ' ολοκλήρου εξωτερικής ανάθεσης, μία ΜΜΕ μεταβιβάζει εξολοκλήρου την εκτίμηση και διαχείριση κινδύνων σ' έναν εξωτερικό ανάδοχο. Η εν λόγω ανάθεση μπορεί να περιλαμβάνει αρχικές καθώς και επαναλαμβανόμενες εκτιμήσεις και δραστηριότητες διαχείρισης που καλύπτουν τον συνολικό κύκλο ζωής της διαχείρισης κινδύνων (π.χ. εφαρμογή και διατήρηση μέτρων). Ο ανάδοχος εφαρμόζει την δική του προσέγγιση εκτίμησης κινδύνων/διαχείρισης κινδύνων. Με τον τρόπο αυτό, ο ανάδοχος δεν μεταφέρει τεχνογνωσία στον πελάτη. Σ' αυτό το σημείο πρέπει να σημειωθεί ότι η εξωτερική ανάθεση δραστηριοτήτων εκτίμησης και διαχείρισης δεν απαλλάσσει την διεύθυνση της ΜΜΕ από την ευθύνη της για την ασφάλεια των πληροφοριών.

Ανάλογα με την δομή, την στρατηγική, τους διαθέσιμους πόρους και την κατάσταση της αγοράς, η εξωτερική ανάθεση μπορεί να προσφέρει συγκεκριμένα πλεονεκτήματα. Η απόφαση για την εξωτερική ανάθεση της εκτίμησης κινδύνων των πληροφοριών επιτρέπει στην ΜΜΕ να επικεντρωθεί σε βασικές επιχειρηματικές στρατηγικές ενόσω οι περιφερειακές δραστηριότητες ασκούνται από ένα εξωτερικό εμπειρογνώμονα με εξειδίκευση σε θέματα ασφάλειας των πληροφοριών.

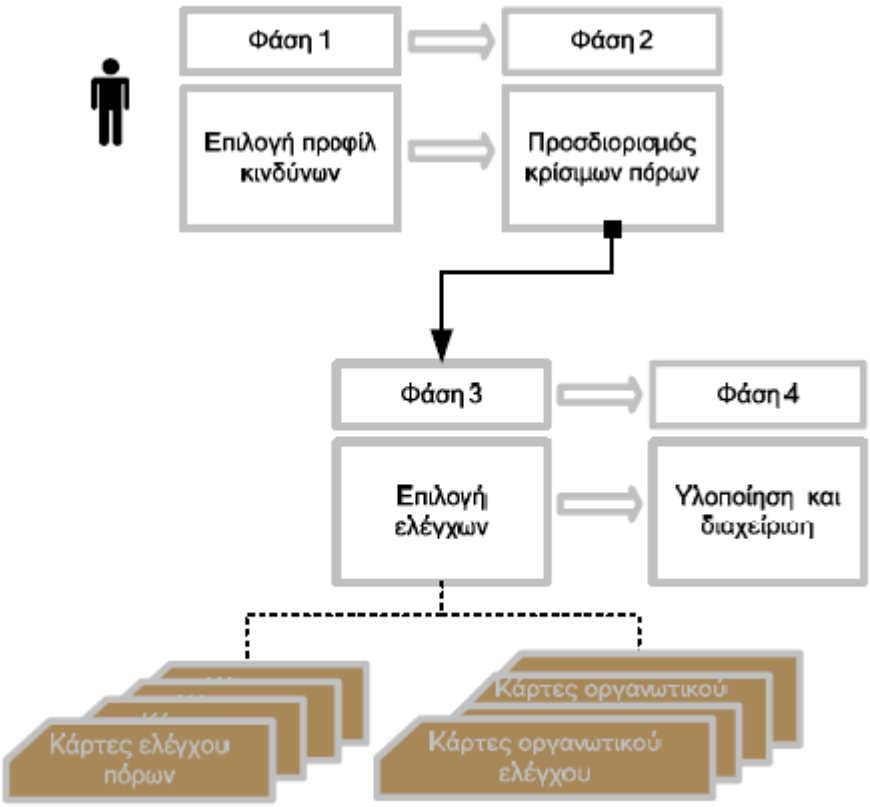
4.3.3. Εν μέρει εξωτερική ανάθεση

Μια λύση μικτών πόρων μπορεί να συνδυάσει τα οφέλη της εσωτερικής αλλά και της εξωτερικής ανάθεσης. Σε μια λύση μικτών πόρων, ο οργανισμός συμμετέχει ενεργά σε μια διαδικασία αυτοαξιολόγησης χρησιμοποιώντας έναν τρίτο ως διαμεσολαβητή. Στο πλαίσιο αυτό, η εκτίμηση βασίζεται σ' ένα υπόδειγμα εκτίμησης κινδύνων που κατανοεί ο πελάτης. Αυτή είναι μια αναγκαία προϋπόθεση προκειμένου να επιτευχθεί η μεταφορά τεχνογνωσίας μεταξύ αναδόχου και πελάτη.

Σ’ αυτή την εκδοχή, η ΜΜΕ αναπτύσσει την ενδοεπιχειρησιακή της ικανότητα ώστε να εκτελεί ορισμένα σημαντικά καθήκοντα σχετικά με θέματα ασφάλειας όταν και όπου αυτό απαιτείται. Μπορούν να προκύψουν καθαρά οφέλη από το γεγονός ότι ο οργανισμός μπορεί να ρυθμίσει και να διαχειριστεί τα μελλοντικά έξοδα του αναδόχου, καθώς και να συνεισφέρει σημαντικά στην εμπειρογνωμοσύνη που παρέχεται από εξειδικευμένο τρίτον.

4.4. Προσέγγιση εκτίμησης κινδύνων

Η προτεινόμενη προσέγγιση εκτίμησης κινδύνων χρησιμοποιεί τέσσερις φάσεις για να εξετάσει οργανωτικά θέματα και ζητήματα ασφάλειας της τεχνολογίας, παρέχοντας έτσι μια περιεκτική ολιστική εικόνα των αναγκών για την ασφάλεια των πληροφοριών. Οι τέσσερις φάσεις για την προτεινόμενη μέθοδο απεικονίζονται στο *Σχήμα 2*.



Σχήμα 2: Οι τέσσερις φάσεις στις οποίες στηρίζεται η προσέγγιση εκτίμησης κινδύνων

Η προσέγγιση αξιολόγησης κινδύνων εξαρτάται από δυο βασικές πτυχές: (α) το προφίλ επιχειρηματικών κινδύνων και (β) τον προσδιορισμό κρίσιμων πόρων.

Την διαδικασία εκτίμησης κινδύνων διαχειρίζεται μια μικρή διεπιστημονική ομάδα αξιολόγησης (από το προσωπικό της ΜΜΕ, από εξωτερικό προσωπικό ή ένα μεικτό σχήμα των δύο), η οποία συγκεντρώνει και αναλύει πληροφορίες και εκπονεί σχέδια μετριασμού με βάση τους κινδύνους για την ασφάλεια του

οργανισμού. Για την αποτελεσματική διενέργεια της εκτίμησης κινδύνων, η ομάδα πρέπει να διαθέτει ευρεία γνώση των επιχειρηματικών δραστηριοτήτων (αναφέρονται και ως επιχειρησιακές διαδικασίες) και της υποδομής της τεχνολογίας των πληροφοριών (ΤΠ) του οργανισμού.

Ως σημείο εκκίνησης, η ομάδα ανάλυσης της ΜΜΕ θα αξιολογήσει το προφίλ κινδύνων ώστε να προσδιοριστεί το προφίλ των επιχειρηματικών κινδύνων. Το επόμενο στάδιο περιλαμβάνει τον προσδιορισμό κρίσιμων πόρων και των συναφών απαιτήσεων διασφάλισης όσον αφορά την διαθεσιμότητα, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων.

Ακολούθως, επιλέγονται οι έλεγχοι (κάρτες ελέγχου). Η διαδικασία επιλογής είναι ριζικά απλοποιημένη με την χρήση τυποποιημένων καρτών ελέγχου. Οι ομάδες ολοκληρώνουν την διαδικασία επιλογής ελέγχων απλώς "τραβώντας" τις κάρτες ελέγχου, που συνδέονται με κινδύνους τόσο για τον οργανισμό όσο και για τους αναγνωρισμένους κρίσιμους πόρους, οι οποίες έχουν δημιουργηθεί για κάθε επίπεδο του προφίλ κινδύνων, κατηγορία πόρου και απαίτηση διασφάλισης (διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα).

Οι κάρτες ελέγχου περιλαμβάνουν ελέγχους από τον κατάλογο των πρακτικών που χρησιμοποιείται σε προσεγγίσεις όπως π.χ. η OCTAVE [18]. Οι εν λόγω έλεγχοι είναι αρκετά απλοί και πιο εύκολα κατανοητοί από μη ειδικούς σε θέματα ασφάλειας. Εναλλακτικά, μπορούν να χρησιμοποιηθούν άλλοι έλεγχοι ασφάλειας. Αυτό ενδεχομένως να είναι απαραίτητο στην περίπτωση που μία ΜΜΕ διαθέτει ήδη μια πολιτική ασφάλειας βάσει ενός άλλου προτύπου (π.χ. ISO 17799).

Κατά το τελευταίο στάδιο, η ομάδα ανάλυσης της ΜΜΕ απασχολείται με την ιεράρχηση των πόρων σύμφωνα με την κρισιμότητά τους, την επίδρασή τους στην επιχείρηση και το σχέδιο προστασίας τους.

Φάση 1 – Επιλογή προφίλ κινδύνων

Κατά την διάρκεια αυτής της φάσης, οι ομάδες αξιολόγησης αξιολογούν το προφίλ επιχειρηματικών κινδύνων τους χρησιμοποιώντας ένα σύνολο προκαθορισμένων ποιοτικών κριτηρίων. Χρησιμοποιώντας έναν πίνακα αξιολόγησης προφίλ κινδύνων, οι ομάδες αξιολόγησης είναι σε θέση να αναγνωρίσουν το γενικό πλαίσιο κινδύνων τους. Το γενικό πλαίσιο κινδύνων συνίσταται στο επιχειρηματικό και εξωτερικό περιβάλλον ενός οργανισμού και μπορεί να κατανεμηθεί σε τέσσερις περιοχές κινδύνων: νομικής και κανονιστικής συμμόρφωσης, φήμη και εμπιστοσύνη πελατών, παραγωγικότητα και οικονομική σταθερότητα.

Κάθε περιοχή ταξινομείται σε τρεις κατηγορίες: υψηλού, μεσαίου και χαμηλού επιπέδου κινδύνων. Αυτές οι κατηγορίες παριστούν ποσοτικά κριτήρια για τον εν λόγω οργανισμό όσον αφορά την περιοχή κινδύνων και βοηθούν στην αναγνώριση ενός επιπέδου κινδύνων. Η ομάδα αξιολογεί τους κινδύνους που αναγνωρίζονται σε κάθε περιοχή έτσι ώστε να δημιουργήσουν το προφίλ κινδύνων του οργανισμού.

Η πείρα λέει ότι ο υψηλότερος κίνδυνος που αναγνωρίζεται σε μια κατηγορία κινδύνων καθορίζει το συνολικό προφίλ επιχειρηματικών κινδύνων. Ένας υψηλός κίνδυνος που φέρεται στην κατηγορία οικονομικών κινδύνων οριοθετεί το προφίλ υψηλών κινδύνων. Επίσης, ένας κίνδυνος μεσαίου επιπέδου οδηγεί σ' ένα προφίλ μεσαίων κινδύνων και οι κίνδυνοι χαμηλού επιπέδου σε προφίλ χαμηλών κινδύνων. Για παράδειγμα, ένας κίνδυνος χαμηλού επιπέδου που φέρεται στην φήμη και την εμπιστοσύνη, στην νομική και κανονιστική συμμόρφωση και στην παραγωγικότητα αλλά είναι υψηλού επιπέδου στην κατηγορία κινδύνων της οικονομικής σταθερότητας καταλήγει σε προφίλ υψηλών κινδύνων για τον οργανισμό.

Ο προσδιορισμός των χαρακτηριστικών (προφίλ) κινδύνων πρέπει να θεωρείται ως πολύ σημαντική απόφαση, η οποία, ακολούθως, οδηγεί στην επιλογή πόρων που σχετίζονται με κινδύνους και στην προστασία τους μέσω καρτών ελέγχου.

Φάση 2 – Προσδιορισμός κρίσιμων πόρων

Κατά τη διάρκεια αυτής της φάσης, η ομάδα αξιολόγησης επιλέγει τους κρίσιμους πόρους βάσει της σχετικής σημασίας για τον οργανισμό και ορίζει τις απαιτήσεις διασφάλισης για κάθε κρίσιμο πόρο.

Κατά κανόνα, η διεύθυνση ενός οργανισμού γνωρίζει ποιοι είναι οι βασικοί πόροι του και μπορεί να χρησιμοποιήσει τα περιορισμένα της μέσα ώστε να επικεντρωθεί στην προστασία αυτών των βασικών πόρων. Η ομάδα αξιολόγησης καθορίζει τι είναι σημαντικό για τον οργανισμό (π.χ. πόροι που συνδέονται με τις πληροφορίες) και επιλέγει εκείνους τους πόρους που είναι μείζονος σημασίας για τον οργανισμό, τα οποία ονομάζονται επίσης και κρίσιμοι πόροι. Δίνεται προσοχή στους πόρους, οι οποίοι χρησιμοποιούνται για να βοηθήσουν τον οργανισμό να ασκήσει τις επιχειρηματικές του δραστηριότητες. Πρέπει να σημειωθεί ότι οι τύποι πόρων μπορούν να απαρτίζονται από άλλους τύπους πόρων. Για παράδειγμα, τα συστατικά μέρη μιας εφαρμογής μπορεί να είναι διακομιστές, σταθμοί εργασίας, δρομολογητές, τμήματα δικτύων κτλ.

Κατά την διαδικασία της αναγνώρισης, είναι ουσιώδες να ληφθούν υπόψη οι απόψεις των διευθυντικών στελεχών (ή του ιδιοκτήτη της επιχείρησης). Η συμμετοχή των υψηλά ιστάμενων στην ανάλυση διασφαλίζει ότι η επιχειρηματική αξία των επιχειρηματικών πόρων πληροφοριών επισημαίνεται δεόντως.

Στην συνέχεια, είναι αναγκαία η αξιολόγηση των απαιτήσεων διασφάλισης για τους πιο σημαντικούς πόρους. Οι απαιτήσεις διασφάλισης σκιαγραφούν τα ποιοτικά χαρακτηριστικά ενός πόρου, τα οποία είναι σημαντικό να προστατευθούν. Κατά την διαδικασία αξιολόγησης εξετάζονται οι ακόλουθες απαιτήσεις διασφάλισης:

- διαθεσιμότητα – η ιδιότητα ενός πόρου να είναι διαθέσιμη κατά τον χρόνο χρήσης του
- εμπιστευτικότητα – η ανάγκη διαφύλαξης του ιδιωτικού χαρακτήρα και της μη προσπέλασης από οποιοδήποτε μη εξουσιοδοτημένο άτομο των πληροφοριών ιδιοκτήτη, των ευαίσθητων πληροφοριών ή των προσωπικών δεδομένων
- ακεραιότητα – η γνησιότητα, η ακρίβεια και η πληρότητα ενός πόρου

Οι απαιτήσεις διασφάλισης των πόρων θα χρησιμοποιηθούν αργότερα κατά την επιλογή των καρτών ελέγχου πόρων. Η επιλογή των απαιτήσεων διασφάλισης έχει αναπτυχθεί ως ένας απλός και πρακτικός οδηγός ώστε να προσδιορίζονται οι ιδιότητες ασφάλειας των κρίσιμων πόρων που επιλέχθηκαν προηγουμένως. Οι απαιτήσεις αναδεικνύουν τη σημασία ενός πόρου και αποτελούν ένα δείκτη του απαιτούμενου επιπέδου προστασίας (π.χ. μέσω της χρήσης κατάλληλων ελέγχων).

Ως αποτέλεσμα αυτής της διαδικασίας, οι ομάδες αξιολόγησης πρέπει να έχουν έναν πίνακα κρίσιμων πόρων ταξινομημένων ανά κατηγορία πόρου και έναν κατάλογο αντίστοιχων απαιτήσεων διασφάλισης, παράλληλα με μία αιτιολόγηση ή συμπληρωματικές πληροφορίες που θα ληφθούν υπόψη κατά την αξιολόγηση. Στην συνέχεια, το αποτέλεσμα θα χρησιμοποιηθεί ως δεδομένο εισόδου από την φάση επιλογής καρτών ελέγχου.

Φάση 3 - Επιλογή Καρτών Ελέγχου

Κατά τη φάση 3, η ομάδα αξιολόγησης επιλέγει τους κατάλληλους ελέγχους βάσει του προφίλ κινδύνων που επιλέγεται για κάθε κατηγορία κινδύνων και της κατάστασης των προσδιορισμένων κρίσιμων πόρων (συμπεριλαμβανομένων των απαιτήσεών τους). Οι έλεγχοι διαχωρίζονται σε δύο κατηγορίες: τους οργανωτικούς ελέγχους και τον έλεγχο βάσει πόρων.

Ολόκληρος ο οργανισμός υποτίθεται ότι αποτελεί ένα ενιαίο περιουσιακό στοιχείο που πρέπει να προστατευθεί. Οι οργανωτικοί έλεγχοι ασφάλειας είναι, κατά κανόνα, περιεκτικοί και εφαρμόζονται στην οργάνωση των πόρων κατά οριζόντιο τρόπο. Αντιθέτως, οι έλεγχοι βάσει πόρων στοχεύουν στην υλοποίηση της προστασίας που απαιτείται από τους πόρους (π.χ. ενισχύοντας τη διαθεσιμότητα ενός συστατικού μέρους ενός κρίσιμου δικτύου).

Οι έλεγχοι ομαδοποιούνται περαιτέρω σε κάρτες ελέγχου. Διατίθενται δύο τύποι καρτών ελέγχου για επιλογή από τις ομάδες που διεξάγουν την αξιολόγηση μιας ΜΜΕ:

- Κάρτες ελέγχου οι οποίες περιλαμβάνουν ελέγχους που εφαρμόζονται οριζόντια στον οργανισμό και σχετίζονται με πρακτικές και διαδικασίες διαχείρισης και

- Κάρτες ελέγχου που εφαρμόζονται σε κρίσιμους πόρους και ταξινομούνται σε συγκεκριμένες κατηγορίες πόρων. Οι κάρτες ελέγχου είναι κατά κύριο λόγο προεπιλεγμένοι – ομαδοποιημένοι έλεγχοι σύμφωνα με τα προφίλ κινδύνων και τις απαιτήσεις διασφάλισης των πόρων.

Αναλόγως, η φάση 3 της προτεινόμενης προσέγγισης εκτίμησης αποτελείται από δύο ξεχωριστά αλλά εξίσου σημαντικά στάδια:

- Στάδιο Α: Επιλογή οργανωτικών ελέγχων
- Στάδιο Β: Επιλογή ελέγχων βάσει πόρων

Κατά τη διάρκεια αυτών των σταδίων, οι έλεγχοι ανατίθενται στον οργανισμό (ως ενιαίο σημαντικό περιουσιακό στοιχείο) και στους προσδιορισμένους κρίσιμους πόρους όπως επισημαίνονται παρακάτω.

Φάση 4 – Υλοποίηση και Διαχείριση

Κατά την φάση 4 και βάσει των αξιολογηθέντων πληροφοριών, η ομάδα αξιολόγησης δημιουργεί σχέδια μετριασμού προκειμένου να αντιμετωπίσει τους κινδύνους για τους κρίσιμους πόρους. Απ' την στιγμή που έχουν προσδιοριστεί το προφίλ κινδύνων του οργανισμού, οι κρίσιμοι πόροι και οι κάρτες ελέγχου, η ομάδα αξιολόγησης σχεδιάζει την εφαρμογή των επιλεγμένων ελέγχων. Είναι αναμενόμενο ότι λόγω των περιορισμένων μέσων τους, οι ΜΜΕ δεν θα είναι σε θέση να εφαρμόσουν όλους τους καθορισμένους ελέγχους για όλους τους κρίσιμους πόρους μια κι έξω. Από την άποψη αυτή, η ιεράρχηση προτεραιοτήτων αποτελεί βασικό στοιχείο για επιτυχημένες προσπάθειες μετριασμού των κινδύνων.

Ένα σχέδιο υλοποίησης ορίζει τον τρόπο με τον οποίον ένας οργανισμός προτίθεται να αυξήσει ή να διατηρήσει το υφιστάμενο επίπεδο ασφάλειάς του. Στόχος του είναι να παράσχει μια κατεύθυνση για μελλοντικές προσπάθειες σχετικά με την ασφάλεια των πληροφοριών μάλλον παρά να βρει μια άμεση λύση σε κάθε ευπάθεια και μέλημα ασφάλειας.

Παρακάτω, μπορούν να βρεθούν ορισμένα κριτήρια για την ιεράρχηση ενεργειών προκειμένου για την υλοποίηση προσδιορισμένων καρτών ελέγχου. Αν και δεν μπορούν όλες να εφαρμοστούν σε όλες τις εταιρείες, μπορούν, ωστόσο, να χρησιμεύσουν ως γενικός οδηγός:

- *Στρατηγική ευθυγράμμιση με τους στόχους του οργανισμού:* Αυτός ο πόρος υποστηρίζει άμεσα τους στόχους του σχεδίου τεκμηριωμένης οργάνωσης και/ή τομεακής εργασίας; Ποιοι σκοποί και/ή στόχοι του σχεδίου εργασίας θα υποστηριχθούν και με ποιόν τρόπο;

- *Συνεχείς προσπάθειες βελτίωσης*: Ο εν λόγω πόρος υποστηρίζει την προσπάθεια συνεχούς βελτίωσης του πόρου ενός τομέα; Ποιος είναι ο πόρος συνεχούς βελτίωσης; Με ποιόν τρόπο ο εν λόγω πόρος υποστηρίζει σκοπούς συνεχούς βελτίωσης;

- *Νομικές ή κανονιστικές εντολές*: Εφόσον είναι απαραίτητο ένας πόρος να ικανοποιεί κανονιστικές απαιτήσεις, αυτό θα αντικατοπτρίζεται στην ιεράρχηση προτεραιοτήτων.

- *Οφέλη του όλου συστήματος*: Τα οφέλη του όλου συστήματος περιλαμβάνουν βελτιωμένη εξυπηρέτηση πελατών για αρκετές ομάδες πελατών. Θα δοθεί μεγαλύτερη προτεραιότητα στις ομάδες πελατών που θεωρούνται κρίσιμες, αλλά όσο μεγαλύτερη είναι η επηρεαζόμενη ομάδα πελατών τόσο μεγαλύτερο θα είναι το όφελος

- *Εξοικονόμηση κόστους/χρόνου*: Οι εκτιμήσεις εξοικονόμησης κόστους και/ή χρόνου περιλαμβάνουν την δαπάνη χρόνου του προσωπικού, την εξοικονόμηση χρόνου των πελατών, την δημιουργία εσόδων και τις άμεσες μειώσεις προϋπολογισμού/κόστους.

- *Μείωση κινδύνων*: Ως αποτέλεσμα ενός έργου, οι πληροφορίες και/ή οι υπηρεσίες θα αποτρέψουν την απώλεια εσόδων και/ή την μη συμμόρφωση με πολιτικές, νομικές και ελεγκτικές απαιτήσεις.

Το επόμενο στάδιο είναι η διαδικασία σχεδιασμού, που υποδεικνύει και παρακολουθεί το ακριβές χρονοδιάγραμμα των εργαλείων ασφάλειας και την υλοποίηση των διαδικασιών.

Μια βασική ερώτηση, σχεδόν σε κάθε υλοποίηση, είναι αν οι ενδοεπιχειρησιακοί πόροι επαρκούν για να εκπληρωθεί το σχέδιο υλοποίησης. Με άλλα λόγια, ενδεχομένως να είναι απαραίτητη η λήψη απόφασης είτε για την εσωτερική είτε για την εξωτερική ανάθεση της σχετικής εργασίας υλοποίησης και διαχείρισης.

4.5. Υποδείξεις ασφαλείας για Μικρομεσαίες Επιχειρήσεις

Τα ακόλουθα συνιστούν τις θεμελιώδεις προϋποθέσεις μέσων άμυνας για την επιχείρηση [20]:

- Διεξαγωγή διαδικασιών ελέγχου με φίλτρα ελέγχου για όλους τους εργαζόμενους και αναδόχους σας (π.χ. βάσει αναφορών ή εισηγήσεων)
- Γνώση και τεκμηρίωση των πολύτιμων πόρων του οργανισμού σας
- Διάθεση σύντομων, αποδοτικών και επαρκώς τεκμηριωμένων διαδικασιών ασφάλειας
- Διεξαγωγή βασικής εκπαίδευσης ευαισθητοποίησης σε θέματα ασφάλειας για τους εργαζόμενούς της επιχείρησης
- Ταχεία ή αυτόματη εφαρμογή προγραμμάτων επιδιόρθωσης τρωτών σημείων λογισμικού μετά από τον έλεγχο της λειτουργικότητάς τους
- Γνώση του διαθέτοντος πρόσβαση στα συστήματα της επιχείρησης και γιατί
- Χρήση δύσκολων συνθηματικών και τακτική αλλαγή τους
- Επιβεβαίωση περί της εφαρμογής αντιικών διεργασιών σε όλους τους υπολογιστές και τις κινητές συσκευές, καθώς και περί της αυτόματης ενημέρωσης του συστήματος για αντιική προστασία
- Χρήση διαφορετικών αντιικών προϊόντων για τους διακομιστές και τους Η/Υ πελάτες του δικτύου της επιχείρησης
- Χρήση συστήματος φιλτραρίσματος για προστασία έναντι του περιεχομένου ανεπίκλητων ηλεκτρονικών μηνυμάτων, μηχανισμού εξαπάτησης, καθώς και κακόβουλου και απαγορευμένου περιεχομένου
- Χρήση τοίχου προστασίας, ιδιαίτερα εάν υπάρχει ευρυζωνική πρόσβαση στο διαδίκτυο
- Χρήση ενός "όλα σε ένα" δικτυακού συστήματος άμυνας με ένα μικρό δίκτυο

Συνθηματικά

Αποτελούν τα κλειδιά για πρόσβαση στις ηλεκτρονικές πληροφορίες, καθώς οποιοσδήποτε μπορεί να προσπελάσει τις πληροφορίες που δεν προστατεύονται με συνθηματικό. Η επιλογή εύκολων συνθηματικών, είναι αρκετά πιθανό να προβλεφθούν ή αποκρυπτογραφηθούν από κάποιον.

Απαράβατοι κανόνες για τα συνθηματικά είναι οι παρακάτω:

- Χρήση τουλάχιστον οχτώ (8) χαρακτήρων
- Αλλαγή σε τακτά χρονικά διαστήματα (π.χ. κάθε μήνα).
- Χρήση διαφορετικών συνθηματικών για διαφορετικά αρχεία (ένα συνθηματικό για κάθε εφαρμογή, όχι το ίδιο παντού).
- Άμεση αλλαγή του παλιού συνθηματικού σε περίπτωση αποχώρησης ενός εργαζομένου.

Επιπλέον, υπάρχουν ορισμένα πράγματα που δεν πρέπει να γίνονται με τα συνθηματικά, όπως:

- Δεν γράφουμε ποτέ ένα συνθηματικό!
- Δεν βασίζεται σε κάτι προφανές (π.χ. το όνομά μας, το όνομα του συντρόφου μας, τα ονόματα των παιδιών μας, τον αριθμό της άδειας κυκλοφορίας του αυτοκινήτου, ημερομηνίες γενεθλίων και οτιδήποτε άλλο είναι ευρέως γνωστά ή που μπορεί εύκολα να αποκρυπτογραφηθούν με λίγο "χειραγώγηση")
- Δεν μοιραζόμαστε το συνθηματικό μας με άλλους

Εν συντομία, το συνθηματικό πρέπει να διαχειρίζεται με προσοχή, να αποτελεί ένα στοιχείο εύκολο στην απομνημόνευση αλλά πολύ δύσκολο στην πρόβλεψη από άλλους. Το συνθηματικό πρέπει να αλλάζει τακτικά και να διαφυλάσσεται σε ασφαλές μέρος.

Ιοί, Σκουλήκια και Δούρειοι Ίπποι

Οι γλωσσαμύντορες θα έλεγαν ότι όλα αυτά είναι διαφορετικά μεταξύ τους αλλά από επιχειρηματική άποψη μπορούν να μεταχειριστούν με τον ίδιο τρόπο. Το κρίσιμο σημείο είναι ότι όλα αυτά μπορούν να προκαλέσουν, και όντως προκαλούν βλάβη, στους υπολογιστές και στις πληροφορίες που αποθηκεύονται σε αυτούς. Ωστόσο, η αποφυγή τους είναι πραγματικά απλή, με τη χρήση αντιιικού λογισμικού. Οποιοδήποτε αντιιικό λογισμικό επαρκεί δεδομένου ότι όλα δουλεύουν, πάνω – κάτω, με τον ίδιο τρόπο και κάνουν την ίδια δουλειά. Το σημαντικότερο όλων είναι απλά η χρήση ενός λογισμικού προγράμματος.

Με ένα αντιιικό λογισμικό ελέγχονται αυτόματα οποιαδήποτε νέα δεδομένα. Με τον τρόπο αυτό, οι πληροφορίες ελέγχονται για την ύπαρξη ή μη ιών πριν αυτοί προκαλέσουν κάποια βλάβη.

Αυτό που οι περισσότεροι άνθρωποι δεν αντιλαμβάνονται είναι ότι το αντιιικό λογισμικό πρέπει να ενημερώνεται διαρκώς. Αυτό σημαίνει διαρκείς, καθημερινές ενημερώσεις, διότι οι συγγραφείς αυτού του λογισμικού ανακοινώνουν νέες εκδόσεις καθημερινά.

Ένας χρυσός κανόνας είναι ότι οποιαδήποτε προσβεβλημένα από ιούς αρχεία ή δεδομένα πρέπει να καταστρέφονται. Ορισμένα αντιιικά λογισμικά διατείνονται ότι απολυμαίνουν αρχεία αλλά αυτό δεν είναι ποτέ εγγυημένο. Η ασφαλέστερη άποψη είναι η καταστροφή των αρχείων που έχουν προσβληθεί από ιό. Εάν πρόκειται για ηλεκτρονικό μήνυμα, αυτό καταστρέφεται χωρίς να ανοιχθεί.

Ανεπίκλητα ηλεκτρονικά μηνύματα (Spam)

Πρόκειται για μηνύματα που θεωρούνται απλώς ένας κακός μπελάς, αλλά – δυστυχώς - κρύβουν εξίσου κινδύνους. Ανεπίκλητα ηλεκτρονικά μηνύματα μπορεί να είναι ένα πρόσχημα γι’ απάτη, ένα επικίνδυνο αλυσιδωτό μήνυμα ηλεκτρονικού ταχυδρομείου, καθώς επίσης μπορεί να περιέχει έναν κρυφό κώδικα ο οποίος μπορεί να αλλάξει τις ρυθμίσεις ενός υπολογιστή ή να μετατρέπει τον υπολογιστή σε φορέα αναμετάδοσης ανεπίκλητων μηνυμάτων.

Στην περίπτωση του κρυφού κώδικα, ο κώδικας αυτός, κατά πάσα πιθανότητα εμπίπτει στην κατηγορία Δούρειος Ίππος και μπορεί να εντοπιστεί από το αντιιικό λογισμικό. Ωστόσο, για την ελαχιστοποίηση οποιονδήποτε κινδύνων, υπάρχουν ορισμένοι κανόνες που χρειάζεται να ακολουθηθούν στην περίπτωση των ανεπίκλητων ηλεκτρονικών μηνυμάτων:

- Διαγραφή χωρίς άνοιγμα ενός ηλεκτρονικού μηνύματος που δεν έχει προφανή αξία ούτε οποιαδήποτε σχέση με την επιχείρηση, είναι ημιαναλφάβητο κλπ.

- Αποφυγή απάντησης σε ανεπίκλητα ηλεκτρονικά μηνύματα. Η διεύθυνση ενός ηλεκτρονικού ταχυδρομείου εντοπίζεται με τον ένα ή τον άλλο τρόπο, και οι αποστολείς ανεπίκλητων ηλεκτρονικών μηνυμάτων δεν γνωρίζουν εάν υπάρχει πραγματικά. Τυχόν απάντηση, επιβεβαιώνει την παρουσία με αποτέλεσμα τη λήψη περισσότερων τέτοιων μηνυμάτων.

- Αποφυγή γνωστοποίησης της ηλεκτρονικής διεύθυνσης οπουδήποτε. Αυτό είναι πολύ δύσκολο όταν ασκείται επιχειρηματική δραστηριότητα. Το ενδεχόμενο τήρησης δύο ηλεκτρονικών διευθύνσεων, μία δημοσιοποιημένη και μία για προσωπική χρήση που να ελέγχεται προσεκτικά, αποτελεί ένα καλό μέτρο προστασίας.

- Αποφυγή χρήσης άγνωστων, αναξιόπιστων ιστοσελίδων, ή ιστοσελίδων που υπόσχονται αφαίρεση από καταλόγους διευθύνσεων ανεπίκλητων ηλεκτρονικών μηνυμάτων.

Το κλείδωμα ανεπίκλητων ηλεκτρονικών μηνυμάτων είναι ένα ενδεχόμενο. Διατίθεται ειδικό λογισμικό κλειδώματος αλλά μπορεί να είναι πολύ ακριβό για μικρές επιχειρήσεις. Είναι πιθανόν να συμφέρει η παροχή κλειδώματος ανεπίκλητων ηλεκτρονικών μηνυμάτων από τον ίδιο τον Πάροχο Υπηρεσιών Διαδικτύου (ISP), έναντι μιας μικρής πρόσθετης αμοιβής, με χρήση δικών του μέσων. Ωστόσο, το κλείδωμα ανεπίκλητων ηλεκτρονικών μηνυμάτων είναι τέχνη όσο και επιστήμη. Εάν τα κριτήρια κατά των ανεπίκλητων ηλεκτρονικών μηνυμάτων είναι πολύ αυστηρά, είναι το ίδιο εύκολο να κλειδωθούν σύννομα ηλεκτρονικά μηνύματα.

Κατασκοπευτικό λογισμικό (Spyware)

Αποτελούν μικρά προγράμματα που παρεισφρύουν στο υπολογιστικό σύστημα προκειμένου να συγκεντρώσουν λαθραία πληροφορίες για τον χρήστη – επιχείρηση χωρίς αυτή να το γνωρίζει. Το μεγαλύτερο μέρος αυτού του λογισμικού αφορά σε διαφημιστικούς σκοπούς αλλά μπορεί επίσης να συγκεντρώσει πληροφορίες για διευθύνσεις ηλεκτρονικού ταχυδρομείου, ακόμα και για συνθηματικά αλλά και στοιχεία για πιστωτικές κάρτες.

Πρόσφατα, δημοσιεύθηκαν επίσημες προειδοποιήσεις σχετικά με το κατασκοπευτικό λογισμικό το οποίο χρησιμοποιείται για την συγκέντρωση ευαίσθητων από εμπορική άποψη δεδομένων, π.χ. στοιχεία συμβάσεων. Το κατασκοπευτικό λογισμικό δεν είναι ότι καλύτερο και ο προσεκτικός χρήστης προσπαθεί να το περιορίσει ή να το αφαιρέσει εντελώς.

Στο Διαδίκτυο διατίθενται καλά πακέτα τα οποία αφαιρούν το κατασκοπευτικό λογισμικό (π.χ. Lavasoft's Ad-Aware, Spybot). Παρόλο που είναι για προσωπική χρήση, οι επιχειρήσεις μπορούν να τα χρησιμοποιήσουν αγοράσουν.

Τοίχοι προστασίας (Firewalls)

Τα συστήματα αυτά πήραν τα όνομά τους από τα φυσικά φράγματα που κατασκευάζονται σε κτίρια για την καταπολέμηση της εξάπλωσης της φωτιάς. Με όρους πληροφορικής, ένα firewall δρα ως φραγμός για την αποτροπή μη εξουσιοδοτημένης χρήσης προς/από ένα ιδιωτικό υπολογιστικό σύστημα. Αποτελεί ένα είδος πόρτας ασφάλειας και αντικλεπτικού συναγερμού για υπολογιστές, βοηθώντας στον περιορισμό εσκεμμένων απειλών.

Ένα firewall θεωρείται σήμερα απαραίτητο σε περίπτωση που ένας ή περισσότεροι υπολογιστές είναι συνδεδεμένοι με το Διαδίκτυο. Μπορεί να είναι είτε ένα τμήμα λογισμικού είτε ένα είδος υλικού. Για την προστασία μεγάλων υπολογιστικών συστημάτων μπορεί να είναι ένας συνδυασμός λογισμικού και υλικού.

Βασικά ένα firewall ελέγχει όλα τα δεδομένα που εισέρχονται ή ακόμη και όσα εξέρχονται από έναν υπολογιστή ώστε να διασφαλιστεί ότι αυτά είναι σύννομα. Συγκεκριμένα αυτό σημαίνει ότι είναι η καλύτερη άμυνα έναντι ενός χάκερ. Για

παράδειγμα, ένα firewall μπορεί να αναχαιτίσει την ανάληψη του ελέγχου του υπολογιστή μέσω μίας έμπιστης τρίτης οντότητας και την ρύθμισή του ως αναμεταδότη ανεπίκλητων μηνυμάτων.

Για καλή τύχη, τα firewalls λογισμικού είναι σήμερα ανέξοδα, εύκολα στην χρήση και εύκολα διαθέσιμα. Σε περίπτωση επιχειρήσεων που διαθέτουν έναν ή περισσότερους υπολογιστές, είναι δυνατή η αγορά ενός συνδυασμού λογισμικών τύπου τοίχου προστασίας και αντιικού σε ένα πακέτο. Κάτι τέτοιο επιφέρει οικονομικά και τεχνικά πλεονεκτήματα για την μικρή επιχείρηση.

Προγράμματα επιδιόρθωσης (Patches)

Τα προγράμματα επιδιόρθωσης είναι λιγότερο γνωστά αλλά είναι πολύ σημαντικά και συνδέονται με ιούς και την ηλεκτρονική παρείσφρηση. Όλα τα προγράμματα λογισμικού παρουσιάζουν προβλήματα και ελαττώματα. Στις περισσότερες περιπτώσεις, τα ελαττώματα είναι τόσο επουσιώδη που μπορούν να αγνοηθούν και ενδεχομένως να μην έχουν κανένα αντίκτυπο στην οποιαδήποτε επιχείρηση. Ορισμένα, ωστόσο, ελαττώματα είναι εξαιρετικά σημαντικά για να αγνοηθούν.

Όλοι οι παραγωγοί λογισμικού παρέχουν προγράμματα επιδιόρθωσης – δηλαδή ενημερώσεις λογισμικού σχεδιασμένες ώστε να αφαιρούν προβλήματα από το λογισμικό τους. Τα ζητήματα αυτά αφορούν κυρίως το λειτουργικό σύστημα του υπολογιστή. Μπορεί να χρησιμοποιείται κάποια έκδοση του Microsoft Windows, ενδεχομένως Apple OSX ή ίσως Unix/Linux. Όλα αυτά τα λειτουργικά συστήματα χρειάζονται, κατά καιρούς, επιδιόρθωση. Παρ' όλα' αυτά πολλές εφαρμογές χρειάζονται επίσης σποραδική επιδιόρθωση. Οι φυλλομετρητές ιστού και τα πακέτα ηλεκτρονικού ταχυδρομείου συχνά χρειάζονται επιδιόρθωση και δεν είναι ασύνηθες για τα συνήθη λογιστικά πακέτα να χρειάζονται ένα πρόγραμμα επιδιόρθωσης.

Η αποφυγή ενημέρωσης των προγραμμάτων επιδιόρθωσης λογισμικού, εγκυμονεί κινδύνους βλάβης του λογισμικού, ή στην περίπτωση φυλλομετρητών ή του ηλεκτρονικού ταχυδρομείου, να επιτρέψει σε κακόβουλο λογισμικό να αλλοιώσει την λειτουργία του υπολογιστή ή σε κακόβουλους χρήστες να αποκτήσουν τον έλεγχο του υπολογιστή.

Οι περισσότεροι κατασκευαστές λογισμικού παρέχουν μία υπηρεσία ειδοποίησης μέσω ηλεκτρονικού ταχυδρομείου που ενημερώνει τους πελάτες τους όταν εκδίδονται νέα προγράμματα επιδιόρθωσης. Συνήθως διαβαθμίζουν σε μία κλίμακα αυτές τις ειδοποιήσεις από κρίσιμες έως αναμενόμενες. Εάν ληφθεί μία προειδοποίηση για ένα πρόγραμμα επιδιόρθωσης ζωτικής σημασίας, το οποίο επηρεάζει ένα τμήμα του λογισμικού στο οποίο στηρίζεται η εύρυθμη λειτουργία της επιχείρησής σας, συνιστάται η εγκατάστασή του το συντομότερο δυνατό. Η συνέχιση των επιχειρηματικών δραστηριοτήτων ενδεχομένως να εξαρτάται από αυτό το γεγονός. Επίσης, μπορεί να ελέγχεται ο ιστότοπος του προμηθευτή του λογισμικού για ενδιαφέρουσες ειδήσεις ή ενημερώσεις. Σήμερα οι περισσότεροι κατασκευαστές λογισμικού προσφέρουν αυτόματες ενημερώσεις μέσω του Διαδικτύου.

Δημιουργία εφεδρικών αντιγράφων (Backup)

Η δημιουργία εφεδρικών αντιγράφων είναι η διαδικασία με την οποία δημιουργείται ένα αντίγραφο ηλεκτρονικών δεδομένων (π.χ. ενός αρχείου λογαριασμών). Τα ηλεκτρονικά δεδομένα είναι πολύ εύκολο να χαθούν, εγκαταλειφθούν από αμέλεια ή να καταστραφούν. Τυχόν απώλεια του μοναδικού αντίγραφου των ηλεκτρονικών λογαριασμών μιας επιχείρησης, θα προκαλέσει πρόβλημα στην διαχείρισή της την επόμενη μέρα.

Ένα τυπικό και αποτελεσματικό καθεστώς δημιουργίας εφεδρικών αντιγράφων θα αποτρέψει μεγάλο μέρος των φυσικών ή τυχαίων απειλών. Τα θεμελιώδους σημασίας δεδομένα μπορούν να αντιγραφούν σε αφαιρούμενους δίσκους (π.χ. cd/dvd, εξωτερικούς σκληρούς)

Το ενδεχόμενο δημιουργίας πολλαπλών εφεδρικών αντιγράφων δεδομένων κρίσιμης σημασίας μπορεί να πραγματοποιηθεί χρησιμοποιώντας μέσα τριών γενιών. Για παράδειγμα, κρατώντας τα δεδομένα “του τέλους της εβδομάδας” των τελευταίων τριών εβδομάδων με κυλιόμενο τρόπο έτσι ώστε να υπάρχουν πάντοτε εφεδρικά αρχεία τριών εβδομάδων (ή γενιών) για κάθε ενδεχόμενο στην περίπτωση που απαιτηθεί η επαναδημιουργία του συστήματος.

Ένα ενδεδειγμένο καθεστώς δημιουργίας εφεδρικών αντιγράφων για μια επιχείρηση είναι:

- Στο τέλος κάθε εργάσιμης ημέρας – δημιουργία εφεδρικών αντιγράφων όλων των αρχείων που αλλάχθηκαν την ημέρα αυτή
- Στο τέλος κάθε εβδομάδας - δημιουργία εφεδρικών αντιγράφων όλων των εφαρμογών (λογαριασμών, αλληλογραφίας κλπ)
- Στο τέλος κάθε μήνα - δημιουργία εφεδρικών αντιγράφων και του λειτουργικού συστήματος επίσης

Αυτό το καθεστώς δημιουργίας εφεδρικών αντιγράφων χρησιμοποιείται από τότε που εφευρέθηκαν οι υπολογιστές και έχει αποδειχθεί ότι είναι αξιόπιστο με την πάροδο του χρόνου. Πιο περίπλοκα καθεστώτα δημιουργίας εφεδρικών αντιγράφων μπορούν να χρησιμοποιηθούν όπου οι αλλαγές δεδομένων γίνονται με ταχύ ρυθμό ή όταν υφίστανται δεδομένα υψηλής αξίας.

Η διατήρηση των εφεδρικών αντιγράφων σε ασφαλή τοποθεσία είναι μείζονος σημασίας. Είναι τόσο πολύτιμα όσο και τα πρωτότυπα δεδομένα, υπόκεινται, δε, στις ίδιες αρχές αναγνώρισης εξουσιοδότησης. Δεν τα αφήνουμε σε μέρη από όπου μπορούν να κλαπούν ή να υποστούν βλάβη, και φυσικά, ποτέ πάνω στον υπολογιστή. Στην ιδανική περίπτωση, η φύλαξη των εφεδρικών αντιγράφων είναι σε ένα εντελώς διαφορετικό κτίριο από αυτό στο οποίο βρίσκονται οι υπολογιστές. Σε περίπτωση που ένα γραφείο υποστεί ολοσχερή καταστροφή από φωτιά, δεν θα έχουν την ίδια μοίρα και τα εφεδρικά αντίγραφα.

Ένα μεγάλο πρόβλημα με τα εφεδρικά αντίγραφα λαμβάνει χώρα όταν ο ιδιοκτήτης λησμονεί να τα επισημάνει δεόντως με την ημερομηνία και το θέμα τους. Στην περίπτωση αυτή όταν το εφεδρικό αντίγραφο χρειαστεί σε συνθήκες βιάσης, θα είναι πολύ χρονοβόρο και ιδιαίτερα δύσκολο να προσδιοριστεί ακριβώς. Μία εναλλακτική επιλογή, εάν υπάρχει μεγάλος αριθμός εφεδρικών αντιγράφων σε διαφορετικά μέσα, είναι η αγορά ενός πυρασφαλούς χρηματοκιβωτίου. Ένα τέτοιο χρηματοκιβώτιο μπορεί να φυλάσσεται στις εγκαταστάσεις της επιχείρησης αλλά μετά από μία πολύ δυνατή φλογερή φωτιά μπορεί να πρέπει να περάσουν δύο έως τρεις ημέρες πριν το χρηματοκιβώτιο έχει κρυώσει αρκετά για να ανοιχθεί.

Υποκλοπή πληροφοριών και ταυτότητας

Πρόκειται για μία από τις γρηγορότερα αναπτυσσόμενες αξιόποινες πράξεις σε πολλές ανεπτυγμένες χώρες. Έχει δοθεί μεγάλη δημοσιότητα στο γεγονός αυτό αλλά το σημαντικό ζητούμενο δεν αναφέρεται. Η υποκλοπή πληροφοριών και στοιχείων ταυτότητας μπορεί να επηρεάσει εξίσου τις επιχειρήσεις και τους ιδιώτες.

Για μία επιχείρηση είναι ζωτικής σημασίας οι παλιές πληροφορίες να καταστρέφονται με ασφαλή τρόπο. Σε αυτό συμπεριλαμβάνονται και τα έγγραφα και τα ηλεκτρονικά αντίγραφα. Δεν είναι κάτι καινούριο για μικρές επιχειρήσεις, οι οποίες διαθέτουν δικές τους ιστοσελίδες, να υποκλέπτονται στοιχεία από τον ιστότοπό τους από κάποιον που έχει κλέψει παλιά επιστολόχαρτα με κεφαλίδες αποστολέα και έχει βρει σε αυτά υπογραφές διευθυντικών στελεχών. Αυτός ο τρόπος χρησιμοποιείται για να χαλκεύονται επιστολές στις υπηρεσίες καταχώρησης ονομασίας στο διαδίκτυο έτσι ώστε να επανακαταχωρηθεί ο ιστότοπος σε μία νέα φυσική διεύθυνση. Στην συνέχεια οργανώνεται μία δόλια επιχείρηση και χορηγούνται έτσι επιχειρηματικά δάνεια.

Μπορεί επίσης να κλαπούν στοιχεία ταυτότητας ιδιωτών με πρόθεση απάτης. Παρά το γεγονός ότι δεν θα καταστεί κάποιος υπόλογος για μία ξεκάθαρη απάτη που διαπράχθηκε από άλλους, το πρόβλημα με την κλοπή στοιχείων ταυτότητας είναι η ανάκτηση της αξιοπιστίας του προσώπου από τράπεζες και άλλους χρηματοοικονομικούς οργανισμούς και ιδιαίτερα από υπηρεσίες/φορείς πιστωτικής αναφοράς.

Ορισμένα πράγματα που πρέπει να γίνονται είναι :

- Αποφυγή δημοσιοποίησης προσωπικών πληροφοριών μέσω του Διαδικτύου, ηλεκτρονικών μηνυμάτων, από τηλέφωνο ή μέσα από επιστολές, σε οποιονδήποτε εκτός εάν υπάρχει βεβαιότητα εμπιστοσύνης.

- Αποφυγή καταστροφής εμπιστευτικών επιχειρηματικών ή προσωπικών εγγράφων πριν τεμαχιστούν πρώτα και, στην ιδανική περίπτωση, με τη χρήση ενός καταστροφέα εγγράφων που έχει διπλή φορά κοπής (εγκάρσια και διαγώνια).

- Ηλεκτρονικό ή μαγνητικό υλικό, που δεν είναι πλέον χρήσιμο, πρέπει να καταστρέφεται με φυσικά τρόπο και έως του σημείου που δεν μπορεί να ξαναχρησιμοποιηθεί.

- Εάν υπάρχουν ανενεργοί επιχειρηματικοί τραπεζικοί λογαριασμοί ή γραμμές συναλλαγής με παλιούς προμηθευτές, αυτοί πρέπει να κλείσουν οριστικά διότι θα μπορούσαν τύχουν εκμετάλλευσης με πρόθεση απάτης.

Σε κάθε περίπτωση, πρέπει να ελέγχονται εξονυχιστικά, τα αντίγραφα κίνησης τραπεζικών λογαριασμών και άλλα οικονομικά έγγραφα. Οποιεσδήποτε ανεπιθύμητες πληρωμές ή χρεωστικές εγγραφές πρέπει να διερευνώνται άμεσα. Οι τράπεζες δεν ενοχλούνται σε περιπτώσεις οποιεσδήποτε απορίων. Ανησυχούν και αυτές, προκειμένου για τον περιορισμό της απάτης. Ένα άλλο θέμα είναι ο περιοδικός έλεγχος περιοδικών ή επαγγελματικών πιστωτικών εγγραφών για τυχόν απροσδόκητα συμβάντα, όπως ερωτήματα σχετικά με την πιστωτική επιφάνεια από εταιρίες με τις οποίες δεν υπήρχε ποτέ καμία συναλλαγή ή δοσοληψία, προσβλητικά σχόλια σχετικά με την πιστωτική επιφάνεια, ειδοποιήσεις αλλαγής διεύθυνσης, ή αναφορές σε αποφάσεις δικαστηρίων κλπ

Ασύρματα Δίκτυα

Τα ασύρματα δίκτυα (WiFi) είναι πολύ ελκυστικά για μικρές επιχειρήσεις, καθώς είναι ανέξοδα στην εγκατάσταση, εύκολα στην διαμόρφωση, παρέχουν ευελιξία και μετριάζουν την δυσκολία και την δαπανηρή διαδικασία καλωδίωσης. Δυστυχώς, είναι επίσης πολύ εύκολο να δημιουργηθεί ένα δίκτυο WiFi που επιτρέπει στον οποιονδήποτε και στον καθένα να διαβάσει τα εμπιστευτικά επιχειρηματικά στοιχεία.

Ο μεγάλος κίνδυνος είναι ότι οποιοσδήποτε εντός της ασύρματης περιοχής μπορεί να χρησιμοποιήσει το WiFi δίκτυό της επιχείρησης. Μπορεί να χρησιμοποιήσει την σύνδεσή της στο Διαδίκτυο δωρεάν, να λάβει γνώση της μεταφοράς δεδομένων της (π.χ. ηλεκτρονικών μηνυμάτων ή συνθηματικών), να έχει πρόσβαση σε αρχεία δεδομένων στους υπολογιστές της ή ακόμη και να ξετρυπώσει τα στοιχεία τραπεζικών της λογαριασμών. Ένα μη ασφαλές δίκτυο WiFi συνιστά μεγάλο κίνδυνο βιομηχανικής κατασκοπίας.

Η δημιουργία δικτύου WiFi στην επιχείρησή απαιτεί προσεκτικό σχεδιασμό και ενδεχομένως να απαιτηθεί βοήθεια από ειδικούς. Η επεξηγηματική αυτή σημείωση δεν μπορεί να αποτελέσει πλήρη οδηγό για την δημιουργία ενός δικτύου. Το σημαντικό σημείο εδώ είναι ότι ένα δίκτυο WiFi μπορεί και πρέπει να δημιουργηθεί με ασφάλεια έτσι ώστε μόνο το προσωπικό της επιχείρησης να μπορεί να το χρησιμοποιεί, να έχει πρόσβαση σε και να διαμοιράζεται δεδομένα.

Οι παρακάτω τεχνικές παρατηρήσεις είναι ουσιώδεις για την ασφάλεια:

- Κάθε μετάδοση δεδομένων πρέπει να είναι κρυπτογραφημένη (χρήση ασύρματης προστατευόμενης πρόσβασης WPA ή WPA2).
- Χρήση προ-μοιρασμένων κλειδιών PSK για την δημιουργία μίας μορφής συνθηματικού ανάμεσα στους υπολογιστές και τον δρομολογητή (συνιστάται η χρήση μίας μακροσκελούς κλείδας).
- Δημιουργία μίας μοναδικής ονομασίας για το WiFi δίκτυο της επιχείρησης μέσω της αντίστοιχης υπηρεσίας.
- Δημιουργία ασφαλής ονομασίας και αναγνωριστικών (SSID).
- Διαμόρφωση του WiFi δρομολογητή έτσι ώστε να μην εκπέμπεται το SSID.
- Αποφυγή χρήσης της προτερόθετης ονομασίας του SSID του κατασκευαστή.
- Καταχώρηση των διευθύνσεων ελέγχου πρόσβασης μέσων (MAC) των υπολογιστών στον δρομολογητή και δημιουργία κανόνα όπου μόνο οι καταχωρημένες διευθύνσεις MAC μπορούν να συνδιαλέγονται με αυτόν.
- Επιβεβαίωση πως τα λειτουργικά συστήματα του διακομιστή και των λοιπών υπολογιστών υποστηρίζουν το WiFi πριν γίνει η αγορά του εξοπλισμού.

Εάν όλα τα παραπάνω ακούγονται κάπως δύσκολα, συνίσταται η εγκατάσταση του WiFi δικτύου της επιχείρησης από έναν ειδικό. Δεν πρέπει να ξεχνάμε ότι τα δεδομένα είναι ενδεχομένως το σημαντικότερο περιουσιακό στοιχείο της επιχείρησης και είναι ανάγκη να προστατευθεί με ένα ασφαλές WiFi. Σε καμία περίπτωση δεν πρέπει να αποτελεί ένα σημείο ελεύθερης πρόσβασης για το κοινό.

Τρίτοι

Σε διάφορες επιχειρηματικές δραστηριότητες, που αφορούν τις ΜΜΕ, εμπλέκονται αρκετά συχνά τρίτοι. Στις συνήθεις δεσμεύσεις τους περιλαμβάνονται η παροχή συμβουλευτικών υπηρεσιών για την διαχείριση εμπορικών υποθέσεων και την εμπορία (marketing), καθώς και η υποστήριξη κρίσιμων συστημάτων της τεχνολογίας των πληροφοριών. Συχνότατα σε αυτούς παρέχεται πρόσβαση σε εμπιστευτικές εταιρικές πληροφορίες ή πρόσβαση σε συστήματα και υποδομή δικτύων για λόγους συντήρησης. Είναι απαραίτητο οι επιχειρήσεις να διασφαλίσουν την εμπιστευτικότητα αυτών των πληροφοριών όχι μόνο συμβατικά αλλά και μέσω μίας διαδικασίας διαχείρισης ελέγχου ενδεδειγμένης πρόσβασης. Οι ΜΜΕ πρέπει, κατ' ελάχιστο, να λάβουν υπόψη τους παρακάτω ελέγχους όταν συναλλάσσονται με τρίτους:

- Σύναψη συμφωνίας εμπιστευτικότητας και τήρησης του απορρήτου.
- Παροχή πρόσβασης σε πληροφορίες, εφόσον συντρέχει λόγος ενημέρωσης, που σημαίνει ότι πρέπει να παρέχεται πρόσβαση σε τρίτους σε πληροφορίες που είναι απολύτως απαραίτητες προκειμένου να εκτελέσουν την εργασία τους.
- Δεν πρέπει να παρέχεται πρόσβαση υποστήριξης τεχνολογίας της πληροφορίας σε τρίτους σε μόνιμη βάση εκτός εάν αυτό είναι αναγκαίο και προβλέπεται ρητά. Η πρόσβαση πρέπει να διακόπτεται άμεσα μετά την ολοκλήρωση των αναγκαίων δραστηριοτήτων. Οι διαδρομές ελέγχου πρέπει να εκτυπώνονται και να ανασκοπούνται προκειμένου να επαληθευθεί ότι οι δραστηριότητες που έλαβαν χώρα περιορίζονταν σε σύννομες διαδικασίες συντήρησης.
- Αίτηση δικαιώματος ελέγχου των μέτρων προστασίας ασφάλειάς του ιδιαίτερα σε περιπτώσεις όπου εταιρικές πληροφορίες χαρακτηρισμένες ως ιδιόκτητες και εμπιστευτικές υπόκεινται σε επεξεργασία στις κτιριακές εγκαταστάσεις του.

Πάροχοι Υπηρεσιών

Οι πάροχοι υπηρεσιών είναι βασικά οι πάροχοι υπηρεσιών διαδικτύου (ISP), οι πάροχοι υπηρεσιών εφαρμογών (ASP) και οι πάροχοι τηλεπικοινωνιακών υπηρεσιών. Πριν την επιλογή ενός παρόχου, τα αρμόδια πρόσωπα πρέπει να ενημερωθούν για τους κανονισμούς που έχουν θεσπιστεί από τον εν δυνάμει υποψήφιο, για παράδειγμα εάν έχουν τεθεί ανώτατα όρια για το εύρος ζώνης , εάν φιλτράρονται τα ηλεκτρονικά μηνύματα και, εάν ναι, σύμφωνα με ποιους κανόνες.

Οι πάροχοι συνήθως αποθηκεύουν δεδομένα χρηστών για σκοπούς τιμολόγησης (επωνυμία, διεύθυνση, αναγνωριστικό χρήστη, τραπεζικό λογαριασμό) καθώς και δεδομένα σύνδεσης και μετάδοσης περιεχομένου (για μια δεδομένη χρονική περίοδο που ποικίλει από τον ένα πάροχο στον άλλο).

Οι χρήστες πρέπει να ζητούν από τους παρόχους τους για ποιο χρονικό διάστημα και ποια στοιχεία των δεδομένων τους παραμένουν αποθηκευμένα. Κατά την επιλογή ενός παρόχου, πρέπει να ληφθεί υπόψη ότι οι πάροχοι στην ΕΕ πρέπει να συμμορφώνονται με τις διατάξεις για την προστασία της ιδιωτικότητας των δεδομένων που ισχύουν για την επεξεργασία των πληροφοριών αυτών.

Μέσω της κρυπτογράφησης, οι χρήστες μπορούν να αποτρέψουν τους παρόχους από το να είναι σε θέση να διαβάσουν το περιεχόμενο των διαβιβαζόμενων δεδομένων.

Πρόσθετοι έλεγχοι αποτελούν τα παρακάτω:

- Σύμφωνα με ποια κριτήρια επιλέγεται ο πάροχος;
- Ποια μέτρα ασφάλειας εφαρμόζει ο πάροχος;
- Σύμφωνα με ποια κριτήρια φιλτράρονται τα ηλεκτρονικά μηνύματα από τον πάροχο (Πάροχοι Ηλεκτρονικού Ταχυδρομείου); Είναι το προσωπικό διαθέσιμο 24 ώρες το 24ωρο για την αντιμετώπιση τεχνικών προβλημάτων και πόσο ικανό είναι;
- Πόσο καλά προετοιμασμένος είναι ο πάροχος για την περίπτωση βλάβης ενός ή περισσότερων πληροφοριακών συστημάτων (σχεδιασμός έκτακτης ανάγκης, αντίληψη για τον τρόπο δημιουργίας αντιγράφων);

- Ποιο επίπεδο διαθεσιμότητας μπορεί να εγγυηθεί ο πάροχος (μέγιστο διάρκειας διακοπής λειτουργίας); Ελέγχει τακτικά το ότι οι συνδέσεις των πελατών παραμένουν σταθερές και εάν έχουν ληφθεί τα μέτρα που απαιτούνται;

- Τι κάνει ο πάροχος για να διαφυλάξει την ασφάλεια των πληροφοριακών συστημάτων και των πελατών του;

Πρέπει να τηρείται η πολιτική ασφάλειας των πληροφοριών και να ακολουθούνται συστηματικά οι κατευθυντήριες γραμμές ασφάλειας κάθε παρόχου. Πρέπει, επίσης, να είναι εφικτό σε εξωτερικούς χρήστες να επιθεωρούν τις κατευθυντήριες γραμμές ασφάλειας. Το προσωπικό του παρόχου πρέπει να είναι ενημερωμένο για τα θέματα της ασφάλειας της τεχνολογίας των πληροφοριών (ΤΠ) και θα υποχρεώνεται να τηρεί τις κατευθυντήριες γραμμές ασφάλειας. Πρέπει, επίσης, να του παρέχεται τακτική εκπαίδευση (όχι μόνο σε θέματα ασφάλειας).

Προστασία και Ιδιωτικότητα Δεδομένων

Πέραν των ανθρώπων που απασχολεί μία επιχείρηση, τι θεωρείται ως βασικό αγαθό της επιχειρηματικής οργάνωσης, το οποίο είναι αθέατο, κατά κύριο λόγο υποτιμημένο, που μπορεί να χρησιμοποιηθεί κατά εσφαλμένο τρόπο από λάθος αποδέκτη και να χαθεί αυτοστιγμεί;

Η πιθανότερη απάντηση είναι οι πληροφορίες. Οι επιχειρηματικές πληροφορίες υπόκεινται σε επιθεώρηση και επεξεργασία, από τα κατάλληλα άτομα τότε που τις χρειάζονται, με βάση την ορθή πολιτική ασφάλειας των πληροφοριών. Σήμερα, η νομοθεσία απαιτεί τη διασφάλιση ότι οι πληροφορίες που τηρούνται για τους ανθρώπους προστατεύονται επαρκώς.

Η νομοθετική πράξη του 1998 περί προστασίας των δεδομένων τέθηκε σε ισχύ την 1^{η} Μαρτίου 2000. Αφορά σε προσωπικά δεδομένα, δηλαδή πληροφορίες σχετικά με αναγνωρίσιμα εν ζωή άτομα ή "υποκείμενα των δεδομένων".

Οι απαιτήσεις της εν λόγω νομοθετικής πράξης μπορούν να συνοψιστούν ως εξής:

- Αξιολόγηση των κινδύνων που αφορούν σε πληροφορίες προσωπικού και ευαίσθητου χαρακτήρα

- Αναγνώριση των αναγκαίων ελέγχων για την προστασία των δεδομένων και της ιδιωτικότητας
- Ανάπτυξη και εφαρμογή πολιτικής ασφάλειας των πληροφοριών

ΚΕΦΑΛΑΙΟ 5

ΕΡΕΥΝΑ

Στα πλαίσια της παρούσας εργασίας και για την όσο το δυνατόν καλύτερη αξιοποίηση της μελέτης, πραγματοποιήθηκε μία έρευνα σε μικρομεσαίες επιχειρήσεις για να διερευνηθεί το επίπεδο ενημέρωσης και δραστηριοποίησης σχετικά με ζητήματα ασφάλειας απέναντι σε περιστατικά παραβίασης δικτύων και επικοινωνιών, τα συνήθη μέτρα που λαμβάνονται για την αντιμετώπιση τέτοιων περιστατικών, καθώς επίσης και οικονομικά στοιχεία σχετικά με την ασφάλεια σε μια προσπάθεια προσέγγισης του οικονομικού αντίκτυπου των ενδεχόμενων επιθέσεων. Για τις ανάγκες της έρευνας επιλέχθηκαν δέκα μικρομεσαίες επιχειρήσεις που δραστηριοποιούνται στην Ελλάδα με κριτήριο την μεγαλύτερη δυνατή πρόσβαση που θα μπορούσαμε να εξασφαλίσουμε τόσο στις επιχειρήσεις, όσο και στις πηγές άντλησης πληροφοριών για αυτές.

5.1. Στόχοι της Έρευνας

Το ερωτηματολόγιο συντάχθηκε με βάση την εμπειρία που αποκομίστηκε μετά από μελέτη της σχετικής διεθνούς βιβλιογραφίας και είχε ως στόχο την εξέταση τεσσάρων κύριων κατηγοριών θεμάτων:

- Την επιχειρηματική προσέγγιση για την αντιμετώπιση απαιτήσεων ασφάλειας, όπως ύπαρξη πολιτικής ασφάλειας και διαχείρισης κινδύνου, ανθρώπινο δυναμικό και διαχείριση έργων ασφάλειας και πλάνο επιχειρησιακής συνέχειας, καθώς επίσης και την πραγματική εμπειρία των ερωτηθέντων από περιστατικά απειλών ασφάλειας και επιθέσεων.

- Την αποτύπωση της παρούσας κατάστασης σχετικά με το επίπεδο ενημέρωσης για τις νομοθετικές ρυθμίσεις και τις πρωτοβουλίες που έχουν αναπτυχθεί τα τελευταία χρόνια στη χώρα μας σχετικά με την ασφάλεια πληροφοριών και επικοινωνιών. Εξετάζεται, επίσης, η πιθανή επίδραση που αυτές οι ρυθμίσεις έχουν στη λειτουργία των οργανισμών καθώς και η σχετική αποτελεσματικότητά τους.

- Τα μέτρα και τις τεχνολογίες που υιοθετούνται για την ασφάλεια πληροφορίας και επικοινωνιών και την αντιμετώπιση πιθανών επιθέσεων στις εξεταζόμενες επιχειρήσεις. Εξετάζονται μέτρα και τεχνολογίες για την ασφάλεια λογισμικού και εφαρμογών, διατήρησης αξιοπιστίας του δικτύου, προστασίας δεδομένων καθώς και η πολιτική αντιμετώπισης πιθανών επιθέσεων. Εξετάζεται, επίσης, η σχετική διαβάθμιση των κινδύνων και των αντίστοιχων μέτρων ασφάλειας που υιοθετούνται.

- Την οικονομική αξιολόγηση των ζητημάτων ασφάλειας για τους εξεταζόμενους οργανισμούς, όπως γενικές επιχειρηματικές επιπτώσεις και σχετικά χρηματοοικονομικά κόστη.

5.2. Προφίλ έρευνας

Η έρευνα πραγματοποιήθηκε την περίοδο Οκτωβρίου-Νοεμβρίου 2012 και διεξήχθη με την πραγματοποίηση δομημένων συνεντεύξεων. Για το σκοπό αυτό συντάχθηκε ένα αναλυτικό ερωτηματολόγιο το οποίο και παρουσιάζεται στο *Παράρτημα Α*. Το ερωτηματολόγιο απεστάλη με e-mail στις επιχειρήσεις λόγω περιορισμένου χρόνου ανάπτυξης της έρευνας. Η διαμόρφωση του ερωτηματολογίου έγινε με τέτοιο τρόπο, ώστε η συμπλήρωσή του να απαιτεί τον ελάχιστο δυνατό χρόνο. Η χρηματική δαπάνη ήταν σχεδόν μηδαμινή, καθώς ο αριθμός συνεντευκτών ήταν μικρός.

Στους συμμετέχοντες στην έρευνα εγγυηθήκαμε την ανωνυμία τους, εξαιτίας του ευαίσθητου και στρατηγικού χαρακτήρα των πληροφοριών που τους ζητήθηκε να καταθέσουν. Οι ερωτήσεις του ερωτηματολογίου ήταν τόσο άμεσες, όσο και έμμεσες. Το ερωτηματολόγιο χωρίστηκε σε τέσσερις ενότητες αντίστοιχες με τα θέματα που περιγράφηκαν και είχε ως εξής:

- Η πρώτη ενότητα αφορούσε γενικές πληροφορίες-στοιχεία για την επιχείρηση (μέγεθος και γεωγραφική περιφέρεια επιχείρησης, κλάδος δραστηριότητας και έτος ίδρυσης, αριθμός υπολογιστικών συστημάτων) ενώ εξετάστηκε και ο βαθμός ενημέρωσης και δραστηριοποίησης σε θέματα ασφάλειας (π.χ. κατάρτιση πολιτικής ασφάλειας).

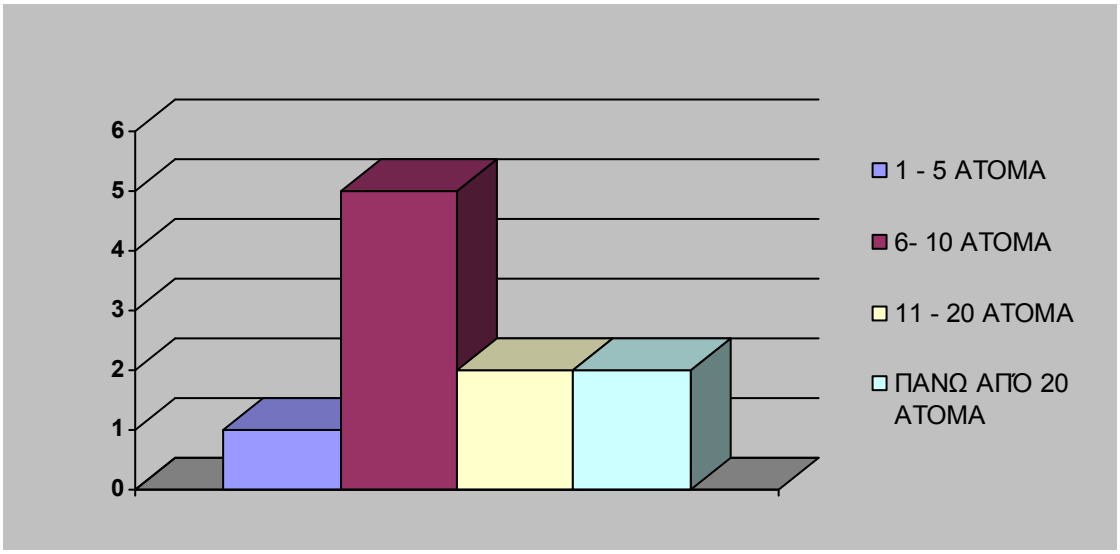
- Η δεύτερη ενότητα αφορούσε τα μέτρα ασφάλειας που κυρίως χρησιμοποιούν, καθώς επίσης και το βαθμό εξοικείωσής τους με τους σημαντικότερους όρους και έννοιες του ζητήματος της ασφάλειας.

- Η τρίτη ενότητα αφορούσε το ζήτημα των προσωπικών δεδομένων των χρηστών και των μέτρων που λαμβάνονται από την επιχείρηση για την εξασφάλισή τους.

- Η τέταρτη ενότητα αφορούσε οικονομικά στοιχεία καθώς εξετάστηκαν οι οικονομικές επιπτώσεις των περιστατικών παραβίασης της ασφάλειας και στοιχεία που αφορούν τα αντίστοιχα τμήματα πρόληψης αυτών των περιστατικών.

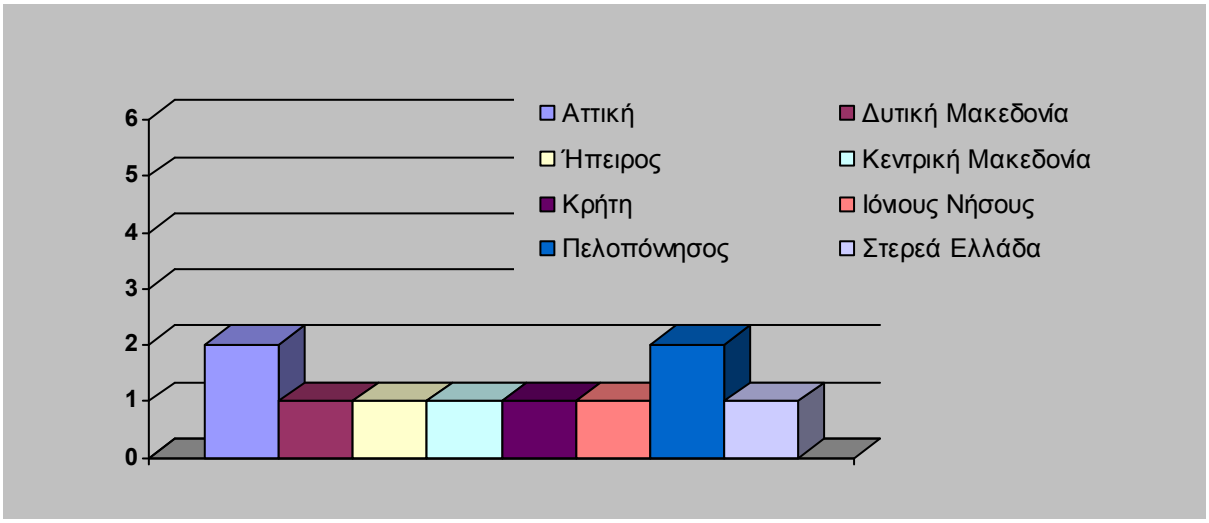
5.3. Αποτελέσματα έρευνας

Το μέγεθος των επιχειρήσεων ήταν 1-20 άτομα κατά 80%, ενώ δύο επιχειρήσεις είχαν πάνω από 20 άτομα προσωπικό.



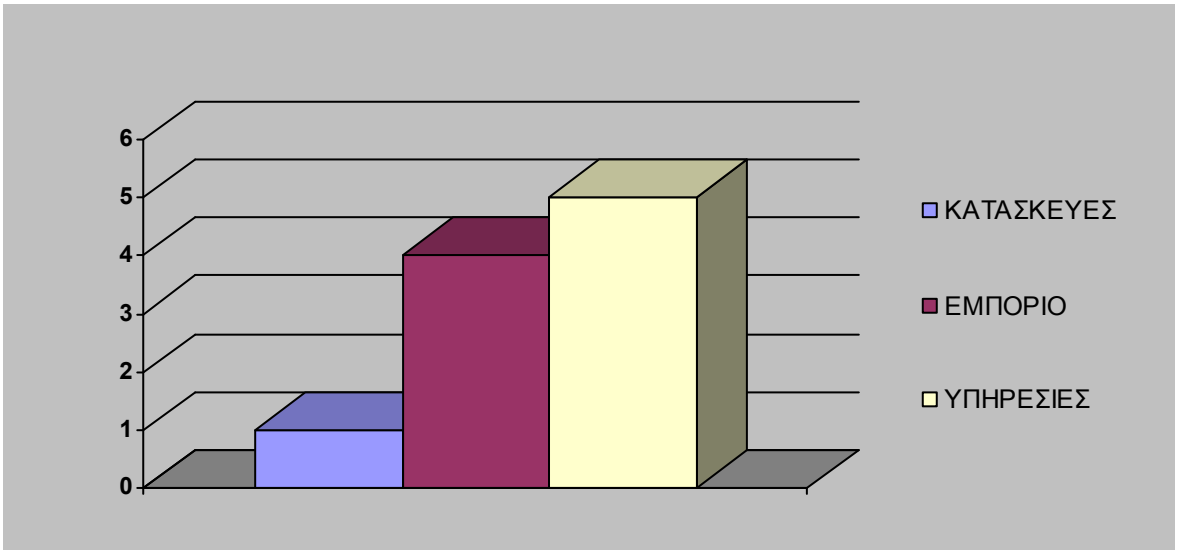
Γράφημα 1 - Μέγεθος επιχείρησης

Το 40% των επιχειρήσεων ανήκαν στην γεωγραφική περιφέρεια της Αττικής και και της Πελοποννήσου, με το υπόλοιπο δείγμα να ισοκαταμερίζεται σε περιοχές από την υπόλοιπη ευρύτερη περιοχή της Ελλάδας.



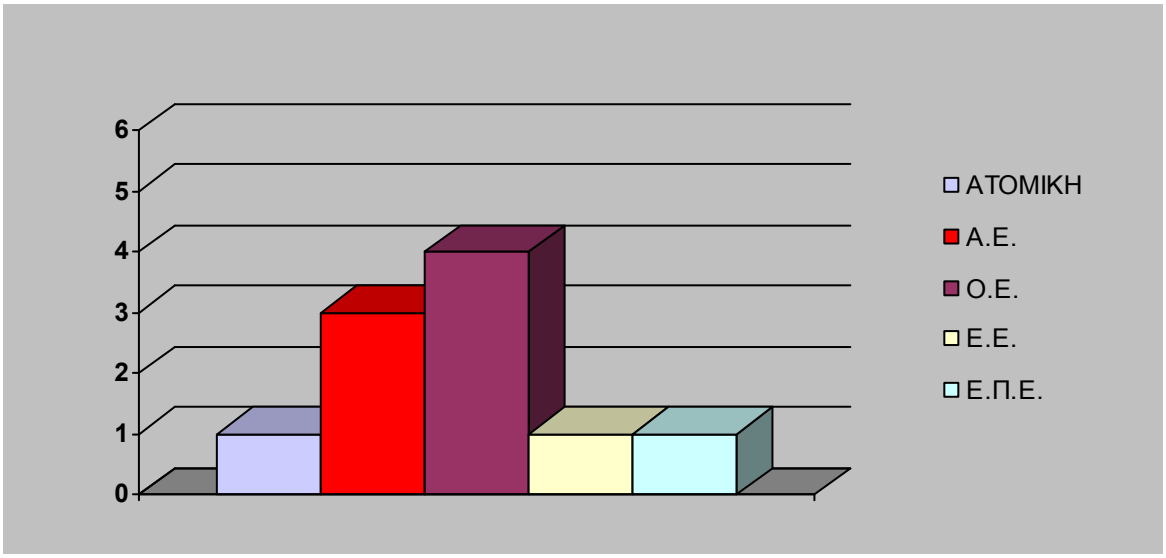
Γράφημα 2 - Περιφέρεια έρευνας

Το 90% των επιχειρήσεων δραστηριοποιείται στον τομέα του εμπορίου και των υπηρεσιών.



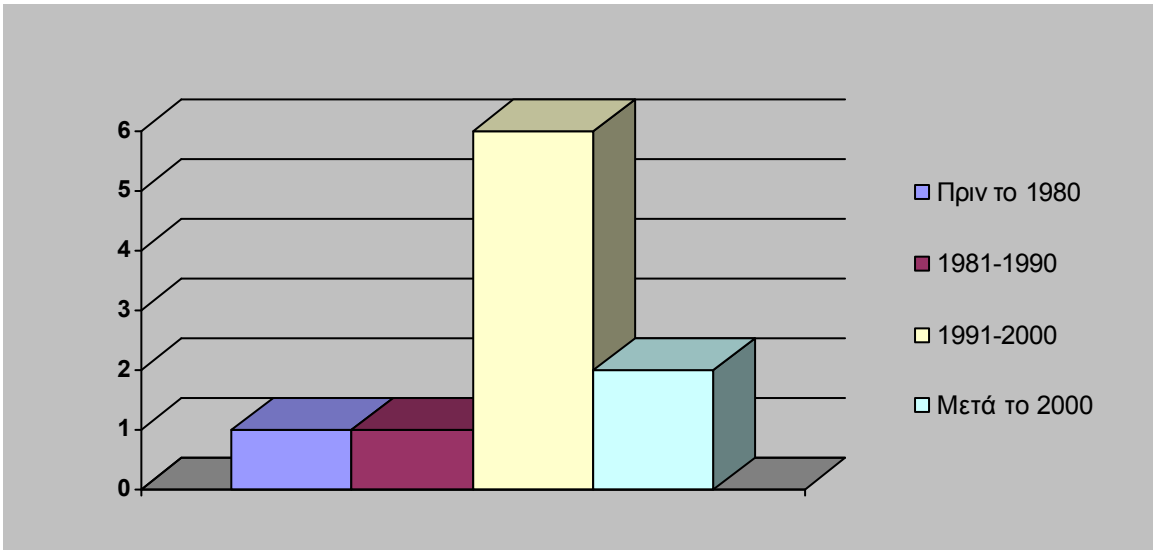
Γράφημα 3 - Κλάδος Επιχείρησης

Η νομική μορφή των επιχειρήσεων ήταν κυρίως ομόρρυθμες (Ο.Ε.) σε ποσοστό 40%, ενώ υπήρξαν τρεις ανώνυμες εταιρείες Α.Ε. (30%), μία ατομική επιχείρηση, μία ετερόρρυθμη (Ε.Ε) και μία Ε.Π.Ε.



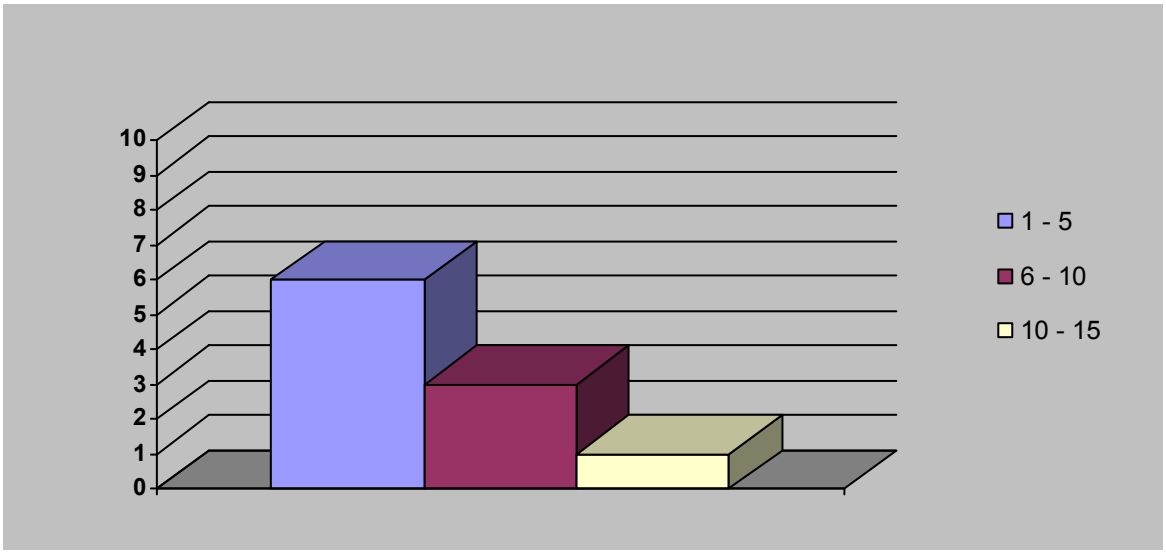
Γράφημα 4 - Νομική μορφή

Το έτος ίδρυσης των επιχειρήσεων αφορούσε κυρίως τη χρονική περίοδο 1991-2000 (60%), ενώ υπήρχε παρουσία εταιρειών από κάθε δεκαετία πριν και μετά από αυτή.



Γράφημα 5 - Έτος Ίδρυσης

Στο σύνολο των επιχειρήσεων το 60% διαθέτουν από 1-5 υπολογιστικά συστήματα, ενώ μόλις το 10% άνω των 10.



Γράφημα 6 – Αριθμός Η/Υ

Όσον αφορά τα ζητήματα ασφάλειας, το επίπεδο ενημέρωσης των χρηστών-εργαζομένων χαρακτηρίζεται μέτριο, ενώ κάτι αντίστοιχο ισχύει συνολικά για τις περισσότερες επιχειρήσεις κι όχι μόνον για τους χρήστες του δικτύου τους.

Σχεδόν όλοι οι ερωτηθέντες παραδέχονται ότι έχουν σημειωθεί περιστατικά παραβίασης της ασφάλειας τα οποία μάλιστα στις περισσότερες περιπτώσεις χαρακτηρίζονται ως ιδιαίτερα σημαντικά. Σε όλες τις επιχειρήσεις έχουν ληφθεί μέτρα αντιμετώπισης παρόμοιων περιστατικών, τα οποία βασίζονται κυρίως στην συνεργασία με εξειδικευμένους φορείς (outsourcing) και όχι στην τεχνογνωσία των στελεχών της επιχείρησης, κάτι αναμενόμενο από τη στιγμή που το επίπεδο των εταιρειών σε ζητήματα ασφάλειας χαρακτηρίζεται ως μέτριο.

Μόλις δύο επιχειρήσεις διαθέτουν ειδικό τμήμα πρόληψης και αντιμετώπισης επιθέσεων στο δίκτυό τους. Σχετικά με την πολιτική ασφαλείας, η πλειοψηφία των ερωτηθέντων απάντησε ότι έχει καταρτιστεί από την εταιρεία τους παρόμοιο πλάνο ή τουλάχιστον βρίσκεται σε διαδικασία κατάρτισης.

Μέτρα ασφαλείας

Στην ερώτηση σχετικά με το ποια μέτρα ασφαλείας θεωρούνται αποτελεσματικότερα, η συντριπτική πλειοψηφία των ερωτηθέντων θεωρεί ότι όλα τα αναφερόμενα στο ερωτηματολόγιο μέτρα (firewalls, προγράμματα antivirus, αυστηρή τήρηση των επιπέδων προσβασιμότητας, απομόνωση του εσωτερικού δικτύου) είναι απολύτως απαραίτητα.

Όσον αφορά τους στόχους που πρέπει να έχει η προστασία δεν θεωρούνται όλοι εξίσου σημαντικοί, καθώς οι περισσότεροι απαντούν ότι βασικός στόχος είναι η πρόληψη του φαινομένου deny-of-access και η απρόσκοπτη συνέχιση της λειτουργίας του δικτύου της επιχείρησης.

Ως κυριότεροι λόγοι που συντελούν στην παραβίαση των συστημάτων αναφέρονται η ελλιπής εκπαίδευση των χρηστών και η αδιαφορία τους για θέματα ασφάλειας, κάτι που επιβεβαιώνει το μέτριο επίπεδο ενημέρωσής τους σε ζητήματα ασφάλειας.

Στο θέμα του κινδύνου για την ασφάλεια που προέρχεται από το εσωτερικό της επιχείρησης, οι περισσότεροι από τους ερωτηθέντες δεν το έχουν αντιμετωπίσει καθόλου (60%), ενώ οι υπόλοιποι δηλώνουν ότι έχουν λάβει όλα τα αναγκαία μέτρα για την πρόληψή του (προγράμματα παρακολούθησης της εσωτερικής κίνησης, διαβάθμιση της δυνατότητας πρόσβασης στα δεδομένα, εφαρμογή επίσημης πολιτικής ασφαλείας της εταιρείας).

Σχετικά με τη φυσική ασφάλεια, όλοι οι ερωτηθέντες την θεωρούν απαραίτητη κι έχουν μεριμνήσει για την εξασφάλισή της. Αυτό ίσως οφείλεται στο γεγονός ότι η φυσική ασφάλεια είναι πιο απτή και προσεγγίσιμη από άλλες μορφές ασφάλειας και αποτελεί βασική προϋπόθεση για την ύπαρξη και προστασία του δικτύου.

Το ζήτημα της επιχειρησιακής συνέχειας δεν έχει απασχολήσει τις επιχειρήσεις όσο θα έπρεπε και η πλειοψηφία εξ αυτών δεν έχει εκπονήσει σχέδιο επιχειρησιακής συνέχειας.

Προσωπικά δεδομένα

Όσον αφορά το ζήτημα της προστασίας των προσωπικών δεδομένων οι ερωτηθέντες εμφανίζονται ιδιαίτερα ενημερωμένοι. Πιο συγκεκριμένα, οι περισσότεροι είναι εξοικειωμένοι με τους όρους "Προσωπικά Δεδομένα" και "Προστασία της Ιδιωτικότητας" καθώς επίσης έχουν μελετήσει την υπάρχουσα νομοθεσία στο συγκεκριμένο ζήτημα.

Παρ' όλη όμως την πληροφόρησή τους για το ζήτημα της προστασίας των προσωπικών δεδομένων, στις περισσότερες περιπτώσεις η πληροφόρηση αυτή δεν συνοδεύεται από συγκεκριμένες ενέργειες που θα έπρεπε να γίνουν στο θέμα αυτό (επικοινωνία με την Αρχή προστασίας των προσωπικών δεδομένων, ύπαρξη δήλωσης στην ιστοσελίδα της επιχείρησης σχετικά με την πολιτική προστασίας των προσωπικών δεδομένων που ακολουθείται, χρησιμοποίηση κάποιου μέσου αυτόματης διαπίστωσης της ταυτότητας των χρηστών, τεχνολογίες ενίσχυσης της ιδιωτικότητας).

Αυτή η αδράνεια στη λήψη μέτρων για την προστασία των προσωπικών δεδομένων εξηγείται σε ένα βαθμό από το γεγονός ότι οι περισσότεροι ερωτηθέντες δεν θεωρούν ότι ο φόβος για την αδυναμία προστασίας των προσωπικών δεδομένων αποτελεί ανασταλτικό παράγοντα στην πραγματοποίηση ενδοδικτυακών συναλλαγών, αλλά προβάλλουν ως σημαντικότερη αιτία την έλλειψη εξοικείωσης των καταναλωτών με την τεχνολογία και ειδικότερα με το Internet.

Οικονομικά στοιχεία

Σχετικά με τα ζητήματα οικονομικού κόστους των περιστατικών παραβίασης της ασφάλειας, οι περισσότεροι από τους συμμετέχοντες είτε δεν απάντησαν καθόλου είτε έδωσαν πολύ γενικές απαντήσεις σε αυτή την ενότητα. Η αδυναμία συλλογής στοιχείων για τα οικονομικά ζητήματα οφείλεται σε μία αναμενόμενη άρνηση των ερωτηθέντων να αποκαλύψουν ευαίσθητα οικονομικά στοιχεία της εταιρείας τους.

Σε κάποιες περιπτώσεις οι ερωτηθέντες εξέφρασαν αδυναμία να απαντήσουν σε ερωτήσεις οικονομικής φύσεως γιατί δεν τους έχει απασχολήσει σοβαρά το ζήτημα. Παρότι θεωρούν ότι πολλά περιστατικά παραβίασης της ασφάλειας έχουν σημαντικές οικονομικές συνέπειες για την επιχείρησή τους, βασική τους προτεραιότητα παραμένει η αποκατάσταση της λειτουργίας των συστημάτων τους και όχι τόσο η αποτίμηση του περιστατικού σε οικονομικό κόστος.

Ένα από σημαντικότερα αποτελέσματα της έρευνας είναι ότι στην ερώτηση σχετικά με την ύπαρξη συγκεκριμένης μεθόδου κοστολόγησης των περιστατικών το σύνολο των ερωτηθέντων απαντά αρνητικά. Αυτό δείχνει με τον πλέον χαρακτηριστικό τρόπο την αδυναμία των επιχειρήσεων να συγκεκριμενοποιήσουν τα διαφορετικά κόστη που μπορούν να προκύψουν από ένα περιστατικό παραβίασης της ασφάλειας.

ΚΕΦΑΛΑΙΟ 6

ΣΥΜΠΕΡΑΣΜΑΤΑ

Πόσο ασφαλείς μπορούμε να είμαστε τελικά; Αυτό είναι το μεγάλο ζητούμενο. Μπορούμε να είμαστε ασφαλείς σε ικανοποιητικό βαθμό, προφανώς. Η πολιτική ασφάλειας είναι το πρώτο σκαλοπάτι που πρέπει να ανέβει κάποιος αν θέλει να "χτίσει" ένα ασφαλές δίκτυο. Η ανάλυση ρίσκου και η αποτίμηση κινδύνων είναι διαδικασίες απαραίτητες, που πλέον διευκολύνονται σημαντικά από την ύπαρξη των σχετικών λογισμικών. Ακόμη και στην περίπτωση ενός διαχειριστή ο οποίος δεν έχει εξαιρετικά υψηλό επίπεδο γνώσεων, το κατάλληλο εργαλείο μπορεί να κάνει σημαντικές υποδείξεις που θα δώσουν τις κατευθύνσεις για ένα σημαντικό επίπεδο ασφάλειας.

Η έννοια της ασφάλειας είναι μια έννοια συνδεδεμένη ούτως ή άλλως στενά με την ανθρώπινη φύση: θέλουμε να νιώθουμε ασφαλής, το επιζητούμε και το ίδιο επιθυμούμε για οτιδήποτε έχουμε δημιουργήσει. Το δίκτυο μιας επιχείρησης είναι σήμερα οι πνεύμονές της, αυτό που της δίνει την επικοινωνία με τον έξω κόσμο. Η οικονομία και η στρατηγική μιας επιχείρησης είναι πλέον ταυτισμένη με το δίκτυό της: εφημερίδες, ξενοδοχεία, κατασκευαστικές εταιρίες, νοσοκομεία, υπουργεία, αλλά και μικρότερης κλίμακας επαγγελματικοί χώροι, όπως δικηγορικά γραφεία και κτηματομεσιτικά γραφεία, δεν μπορούν πια να φανταστούν την λειτουργία τους χωρίς Internet και γενικότερα χωρίς δικτύωση μεταξύ των εργαζομένων. Είναι ζήτημα ουσίας λοιπόν το δίκτυο αυτό να λειτουργεί σωστά, ελλοχεύοντας τους ελάχιστους δυνατούς κινδύνους για τα δεδομένα και του ανθρώπους του.

Το να προβλεφθούν οι κίνδυνοι σε οποιαδήποτε ενέργεια της ζωής μας είναι σχεδόν αδύνατο, από την άποψη ότι οι πιθανοί συνδυασμοί ενεργειών που δύνανται να προκαλέσουν πρόβλημα είναι αμέτρητοι. Η κύρια δυσκολία όμως σε μια επιτυχημένη διαδικασία ανάλυσης ρίσκου δεν είναι αυτή. Η κύρια δυσκολία είναι ίδια η ανθρώπινη φύση που κρύβει εκπλήξεις, ευχάριστες ή – στην προκειμένη περίπτωση – δυσάρεστες.

Από μια άποψη λοιπόν, η πολιτική ασφάλειας είναι ο "ψυχολόγος" του πληροφοριακού συστήματος. Λαμβάνοντας υπόψη την εξάρτηση του από τον παράγοντα άνθρωπο, η πολιτική ασφάλειας καλείται να προβλέψει πιθανές ενέργειες και αντιδράσεις κάποιου, πράγμα εξαιρετικά πολύπλοκο εξαιτίας της ίδιας της πολυπλοκότητας των ανθρώπων.

Το σκαλοπάτι που οδηγεί σε μια σωστή πολιτική ασφάλειας είναι η ανάλυση ρίσκου και η εκτίμηση κινδύνων στο δικτυακό περιβάλλον. Κανείς δεν αμφιβάλλει ότι αυτή η διαδικασία μπορεί να γίνει χειροκίνητα. Ένα δυνατό ανθρώπινο μυαλό μπορεί να προβλέψει τα πάντα, ή σχεδόν τα πάντα. Σήμερα όμως το κατάλληλο λογισμικό είναι σύμμαχος και από αυτόν τον κανόνα δεν εξαιρείται ο παραπάνω τομέας.

Ιδιαίτερα σημαντικό στοχείο αποτελεί το γεγονός να υπάρχει συνδετικός κρίκος μεταξύ διαχειριστή και προσωπικού. Το προσωπικό μιας επιχείρησης γνωρίζει τα πάντα σχετικά με το αντικείμενο εργασίας του, αλλά πιθανόν να μην έχει την παραμικρή ιδέα από ασφαλείς ασύρματες συνδέσεις υπολογιστών. Είναι ζήτημα ουσίας, να έχει πρόσβαση σε αυτές τις πληροφορίες. Ο καλύτερος τρόπος να πραγματοποιηθεί αυτό, είναι μια καλογραμμένη πολιτική ασφάλειας. Η ύπαρξη ενός γραπτού κειμένου δεν είναι χρήσιμη μόνο στον διαχειριστή. Είναι χρήσιμη κυρίως σε όλους όσους εμπλέκονται στην διοίκηση μιας επιχείρησης και πιθανόν χρηματοδοτούν το δίκτυο. Η απλή γλώσσα είναι κατανοητή σε όλους.

Συμπερασματικά, η ασφάλεια και η διαχείριση ενός δικτύου υπολογιστών είναι πάρα πολύ δύσκολες υποθέσεις. Το ζήτημα της καλής λειτουργίας ενός δικτύου όμως, ενώ εξαρτάται σε μεγάλο βαθμό από την ασφάλεια, δεν εναπόκειται μόνο σε αυτή. Η διαχείριση είναι μία ακόμη λέξη κλειδί και δεν είναι υπερβολή να πούμε ότι από ένα γενικότερο πλαίσιο σωστής διαχείρισης ξεκινά ένα καλά δομημένο, χωρίς προβλήματα και απώλειες, δίκτυο.

Η κατανομή των ρόλων είναι ένα κομμάτι στο οποίο μπορεί να υπάρξει πλούσιο πεδίο για μελλοντική επέκταση. Οργανισμοί και επιχειρήσεις έχουν υποστεί καταστροφικά λάθη εξαιτίας λανθασμένων επιλογών στο κρίσιμο αυτό ζήτημα. Είναι λάθος να στηρίζεται όλο το σύστημα ασφαλείας σε έναν άνθρωπο και η κατανομή των ρόλων πρέπει να προβλέπεται απαραιτήτως στον σχεδιασμό.

Συμπερασματικά, οι μηχανισμοί και οι τεχνικές από μόνα τους δεν συνιστούν μέτρα ασφαλείας. Αυτά πρέπει να λειτουργούν κάτω από ένα μοντέλο ασφάλειας.

Είναι επίσης γεγονός ότι στις επιχειρήσεις αυτό που έχει σημασία στο τέλος της ημέρας είναι το κόστος. Θα μπορούσαν λοιπόν να προστεθούν κάποια σειρά ερωτήσεων, μέσα από τις οποίες στην τελική αναφορά θα προκύπτει κάποιο συμπέρασμα για το οικονομικό κόστος που θα υπάρξει από μια ενδεχόμενη παραβίαση ασφάλειας. Αυτό είναι ένα επιχείρημα που πείθει τους περισσότερους διοικητικούς στην λήψη των αναγκαίων μέτρων.

Η προσθήκη νέων κατηγοριών και ερωτήσεων ή τροποποίηση αυτών που υπάρχουν ήδη, προκειμένου να επιτευχθεί καλύτερη συλλογή δεδομένων για το διαχειριζόμενο δίκτυο, λόγω του ότι υπάρχει πάντα το ενδεχόμενο να εμφανιστούν νέες και καλύτερες τεχνολογίες, θα αποτελούσε ένα καλό πεδίο για μελλοντική βελτίωση.

Και μην ξεχνάμε!

Απειλές υπάρχουν πάντα!

Απαιτείται συνεχής και δυναμική ασφάλεια!

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Κιουντούζης Ε., 2003. *Ασφάλεια Πληροφοριακών Συστημάτων: Προσεγγίσεις Ασφάλειας Πληροφοριακών Συστημάτων*, *Prashant* Krishnamurthy, Εκδόσεις Μπένου, Αθήνα

[2] Garfinkel S., Spafford G., 1996, *Practical Unix & Internet Security*, O' Reilly & Associates, 2nd edition

[3] Gheswick R. W., Bellovin M. S., 1994, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley

[4] Κομνηνός Θ., Σπυράκης Π., 2002, *Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων: Αναχαιτίστε τους εισβολείς*, Ελληνικά Γράμματα, Αθήνα

[5] Αλεξανδρής Ν., Κιουντούζης Ε., 1995, *Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα*, Ελληνική Εταιρεία Επιστημόνων ηλεκτρονικών Υπολογιστών & Πληροφορικής

[6] Πάγκαλος Γ., Μαυρίδης Ι., 2002, *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων: Πολιτικές και Μοντέλα Ασφάλειας ΠΣ*, Εκδόσεις Ανίκουλα, Θεσσαλονίκη

[7] Tanenbaum A., 2000, *Δίκτυα Υπολογιστών*, Εκδόσεις Παπασωτηρίου, Αθήνα

[8] Strebe M., 2004, *Newtork Security Foundations*, Sybex

[9] Κοκολάκης Σ., 2000, *Ασφάλεια Πληροφοριακών Συστημάτων: Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας ΠΣ*, Οικονομικό Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής, Αθήνα

[10] Gollmann D., 1999, *Computer Security*, John Wiley & Sons

[11]] Strebe M., 2005, *Ασφάλεια Δικτύων – Εισαγωγή στη Σύγχρονη Τεχνολογία*, Εκδόσεις Γκιούρδας Μ., Αθήνα

[12] Denning J. P., 1990, *Computer Under Attack: Intruders, Worms and Viruses*, Addison-Wesley

[13] Steven L., 1984, *Hackers: Heroes of the Computer Revolution*, Anchor Publishing

[14] Steriling B., 1993, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Bantam Books, Reprint edition

[15] Scambray J., Kurtz S. G., *Hacking Exposed: Network Security Secrets & Solutions*, 2nd edition

[16] Ζορκάδης Β., Σιουγλέ Ε., Σχέδιο ασφάλειας και σχέδιο έκτακτης ανάγκης, www.dpa.gr (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)

[17] Shoniregun A. C., 2007, *Impacts and Risk Assessment of Technology for Internet Security – Enabled Information Small-Medium Enterprises*

[18] ENISA, 2007, *Πακέτο Πληροφοριών για Μικρομεσαίες Επιχειρήσεις (MME)*, Τεχνικό τμήμα ENISA

[19] OCTAVE, 2005, *The OCTAVE (SM) Method Implementation Guide Version 2.0*

[20] ENISA, 2006, *Risk Management: Implementation principles and inventories for Risk Management / Risk Assessment methods and tools*, ENISA

Ηλεκτρονικές Πηγές

www.wikipedia.org

www.riskworld.net

www.encyclopedia.com

www.enisa.europa.eu/

www.webopedia.com

www.ey.com/security

www.dpa.gr

www.go-online.gr/ebusiness/specials

www.ote/gr/efta

www.information-security-policies-and-standrards.com

http://en.wikipedia.org

http://searchsecurity.techtarget.com/tip

http://sme.cordis.lu/home/

http://europa/eu/int/information_society/

www.pirotexnimata.gr

www.zitros.gr

www.goutos.com

www.polymorpho.gr

www.spitiko.com.gr

www.theocar.com

petikasfruits.eu

www.diesi.gr

www.greeksilver.gr

www.apollonion-hotel.gr

ΠΑΡΑΡΤΗΜΑ

ΠΑΡΑΡΤΗΜΑ Α. Ερωτηματολόγιο

Α. ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ

1. Ποιο είναι το μέγεθος της επιχείρησής σας;

☐ 1-5 άτομα ☐ 6-10 άτομα ☐ 11-20 άτομα ☐ >20 άτομα

2. Σε ποια γεωγραφική περιφέρεια ανήκει η επιχείρησή σας;

☐ Ανατ. Μακεδονία - Θράκη
☐ Αττική
☐ Βόρειο Αιγαίο
☐ Δυτική Ελλάδα
☐ Δυτική Μακεδονία
☐ Ήπειρο
☐ Θεσσαλία
☐ Ιόνιους Νήσους
☐ Κεντρική Μακεδονία
☐ Κρήτη
☐ Νότιο Αιγαίο
☐ Πελοπόννησο
☐ Στερεά Ελλάδα

3. Σε ποιο κλάδο δραστηριοποιείται η επιχείρησή σας;

☐ Εμπόριο
☐ Κατασκευές
☐ Υπηρεσίες
☐ Μεταποίηση
☐ Άλλο

4. Ποια είναι η νομική μορφή της επιχείρησή σας;

☐ Ατομική
☐ Ομόρρυθμη
☐ Εταιρεία Περιορισμένης Ευθύνης (Ε.Π.Ε.)
☐ Ανώνυμη (Α.Ε.)
☐ Άλλο

5. Ποιο έτος ιδρύθηκε η επιχείρησή σας;

☐ Πριν το 1980 ☐ 1981-1990 ☐ 1991-2000 ☐ Μετά το 2000

6. Πόσα υπολογιστικά συστήματα διαθέτει η επιχείρησή σας;

☐ 1- 5 Η/Υ ☐ 6- 10 Η/Υ ☐ 10 – 15 Η/Υ ☐ >20 Η/Υ

7. Ποιες υπηρεσίες Ι.Τ. περιλαμβάνει η επιχείρισή σας;

☐ Web Server

☐ Mail Server

☐ File Server

☐ Print Server

☐ Database

☐ Web Integration

☐ E-Commerce

8. Πως θα χαρακτηρίζατε το επίπεδο ενημέρωσης του προσωπικού σχετικά με θέματα ασφάλειας δικτύου;

☐ Πολύ Καλό

☐ Καλό

☐ Μέτριο

☐ Καμία ενημέρωση

9. Έχουν παρατηρηθεί περιστατικά παραβίασης ασφαλείας στην επιχείρησή σας;

☐ Όχι, δεν έχει παρατηρηθεί κανένα περιστατικό

☐ Ναι, έχουν παρατηρηθεί τέτοια περιστατικά

☐ Δεν απαντώ

10. Αν έχουν παρατηρηθεί περιστατικά παραβίασης ασφαλείας, πόσο σημαντικά ήταν;

☐ Αρκετά σημαντικά

☐ Ιδιαίτερα δύσκολα περιστατικά

☐ Ασήμαντα

11. Έχετε λάβει μέτρα προστασίας-πρόληψης τέτοιων περιστατικών;

☐ Ναι

☐ Όχι

☐ Δεν Απαντώ

12. Αν υπάρχουν μέτρα προστασίας-πρόληψης, που βασίζονται κυρίως αυτά;

- ☐ Στην τεχνογνωσία των στελεχών της επιχείρησης
- ☐ Σε εξειδικευμένους συνεργαζόμενους φορείς (outsourcing)
- ☐ Άλλες μεθόδους _____ _____
- ☐ Δεν Απαντώ

13. Διαθέτει η επιχείρησή σας τμήμα πρόληψης και αντιμετώπισης τέτοιων επιθέσεων;

☐ Ναι ☐ Όχι

14. Υπάρχει Πολιτική Ασφαλείας ειδικά σχεδιασμένη για την ανάγκες της επιχείρησής σας;

☐ Ναι ☐ Όχι

Β. ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

15. Ποια μέτρα προστασίας θεωρείτε πιο αποτελεσματικά;

- ☐ Προγράμματα Antivirus
- ☐ Firewalls
- ☐ Αυστηρή τήρηση επιπέδων προσβασιμότητας
- ☐ Απομόνωση εσωτερικού δικτύου
- ☐ Άλλο _____ _____

16. Που θεωρείτε ότι πρέπει κυρίως να στοχεύουν τα μέτρα προστασίας;

- ☐ Προστασία των δεδομένων της επιχείρησης
- ☐ Προστασία των προσωπικών δεδομένων των πελατών
- ☐ Διατήρηση της αξιοπιστίας του δικτύου (deny-of-access)
- ☐ Λογισμικό και εφαρμογές

17. Σε περίπτωση παραβίασης της ασφάλειας της επιχείρησής σας, σε ποιες ενέργειες θα προβείτε, σχετικά με την ενημέρωση τρίτων;

- ☐ Επίλυση προβλήματος εσωτερικά χωρίς περαιτέρω δημοσιοποίησή του
- ☐ Αναφορά στις αρμόδιες αστυνομικές και δικαστικές αρχές
- ☐ Δημοσιοποίηση σε οργανισμούς-φορείς που ασχολούνται με την ασφάλεια

18. Ποιοι θεωρείτε ότι είναι οι κυριότεροι λόγοι που συντελούν στην παραβίαση των συστημάτων μιας επιχείρησης;

- ☐ Ελλιπής εκπαίδευση των χρηστών σε θέματα ασφαλείας
- ☐ Αδιαφορία των χρηστών για τήρηση κανόνων ασφαλείας
- ☐ Ελλιπής μέτρα προστασίας του δικτύου
- ☐ Άλλοι λόγοι

19. Έχετε λάβει μέτρα πρόληψης και αντιμετώπισης των εσωτερικών κινδύνων;

☐ Ναι ☐ Όχι ☐ Δεν γνωρίζω/Δεν απαντώ

20. Αν ναι, ποια μέτρα είναι αυτά;

- ☐ Διαβάθμιση της δυνατότητας πρόσβασης στα δεδομένα
- ☐ Προγράμματα παρακολούθησης της κίνησης στο εσωτερικό δίκτυο
- ☐ Εφαρμογή πολιτικής ασφαλείας που εκτελείται από εξειδικευμένο προσωπικό
- ☐ Άλλα μέτρα

21. Πόσο σημαντική θεωρείτε την τήρηση αντιγράφων ασφαλείας (backup) των δεδομένων σας;

☐ Απαραίτητη ☐ Αρκετά σημαντική ☐ Όχι και τόσο σημαντική

22. Είστε εξοικειωμένοι με τους όρους Διαθεσιμότητα, Εμπιστευτικότητα και Ακεραιότητα;

- ☐ Ναι, είμαι πλήρως εξοικειωμένος
- ☐ Δεν τους έχω κατανοήσει πλήρως, αλλά τους γνωρίζω
- ☐ Δεν τους έχω κατανοήσει

23. Είστε εξοικειωμένοι με τον όρο «Επιχειρηματική Συνέχεια»; Αν ναι, πως αντιμετωπίζετε το ζήτημα αυτό; Έχετε καταρτίσει Σχέδιο Επιχειρησιακής Συνέχειας;

_____

_____

_____

_____

24. Γνωρίζετε τι περιλαμβάνει ο όρος «Φυσική Ασφάλεια»;

☐ Ναι ☐ Όχι

25. Πόσο σημαντική θεωρείτε ότι είναι και τι μέτρα λαμβάνετε για την εξασφάλισή της;

_____

_____

_____

Γ. ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

26. Είστε εξοικειωμένοι με τους όρους «Προσωπικά Δεδομένα» και «Προστασία της Ιδιωτικότητας»;

☐ Πολύ ☐ Αρκετά ☐ Καθόλου

27. Έχετε γνώση της υπάρχουσας νομοθεσίας σχετικά με τους παραπάνω όρους;

☐ Ναι ☐ Όχι ☐ Γνωρίζω ότι υπάρχει, αλλά όχι λεπτομέρειες

28. Στην ιστοσελίδα σας, περιέχεται δήλωση σχετικά με την Πολιτική Προστασίας Προσωπικών Δεδομένων που ακολουθείτε;

☐ Ναι ☐ Όχι ☐ Όχι, αλλά πρόκειται να γίνει

29. Χρησιμοποιείτε κάποιο μέσο αυτόματης διαπίστωσης της ταυτότητας των χρηστών που επισκέπτονται το site σας (π.χ. cookies ή άλλες συναφείς τεχνικές επιλογές);

☐ Ναι ☐ Όχι ☐ Δεν απαντώ

30. Πιστεύετε ότι ο φόβος αδυναμίας προστασίας των προσωπικών δεδομένων, αποτρέπει τους καταναλωτές στο να προβούν σε ενδοδικτυακές συναλλαγές;

☐ Ναι, πιστεύω ότι είναι ο σημαντικότερος παράγοντας

☐ Όχι, υπάρχουν κυρίως άλλοι λόγοι
_____
_____

☐ Δεν γνωρίζω

31. Έχετε επενδύσει σε τεχνολογίες ενίσχυσης της ιδιωτικότητας;

☐ Ναι ☐ Όχι

32. Πόσο σημαντικές τις θεωρείτε για την απόκτηση της εμπιστοσύνης των πελατών;

_____
_____
_____

Δ. ΟΙΚΟΝΟΜΙΚΑ ΣΤΟΙΧΕΙΑ

33. Πιστεύετε ότι η «Νέα Οικονομία» που δημιουργείται με τη χρήση των νέων τεχνολογιών, θα οδηγήσει σε άμεση ανάγκη ανάπτυξης και λήψης σημαντικών μέτρων ασφαλείας;

- ☐ Ναι, άμεσα
- ☐ Ναι, αλλά όχι άμεσα
- ☐ Όχι, εξαρτάται από τις ανάγκες της κάθε επιχείρησης
- ☐ Δεν απαντώ

34. Πόσο πιστεύετε ότι επηρεάζει την επιχείρισή σας σε οικονομικό επίπεδο ένα περιστατικό παραβίασης της ασφάλειάς της;

☐ Πολύ ☐ Αρκετά ☐ Όχι ιδιαίτερα

35. Ποια θεωρείτε τη σημαντικότερη οικονομική επίπτωση από μια επίθεση στο δίκτυο της επιχείρησης;

- ☐ Κόστος αντιμετώπισης της επίθεσης (recovery cost)
- ☐ Απώλεια εσόδων λόγω διακοπής συναλλαγών-πωλήσεων (διαφυγόντα κέρδη)
- ☐ Μείωση γοήτρου και φήμης της επιχείρησης (αντίκτυπος σε μελλοντικές συναλλαγές-πωλήσεις)
- ☐ Άλλη επίπτωση

36. Τι επιπτώσεις θεωρείτε ότι θα έχει σε άλλους οργανισμούς/υπηρεσίες με τις οποίες συνδέεστε, μια ενδεχόμενη επίθεση στο δίκτυό σας;

- ☐ Ανάλογα προβλήματα στο δίκτυό τους
- ☐ Πρόκληση οικονομικών ζημιών λόγω ελλιπούς συνεργασίας
- ☐ Καμία επίπτωση. Υπάρχουν δικλείδες ασφαλείας που απομονώνουν τυχόν προβλήματα δικτύου εντός της επιχείρησης

37. Ποια θα ήταν η αντίδραση της επιχείρησής σας, σε ανάλογη περίπτωση;

- ☐ Διακοπή συνεργασίας, χωρίς δημοσιοποίηση του θέματος
- ☐ Απαίτηση αποζημιώσεων για πιθανές βλάβες
- ☐ Δημοσιοποίηση του θέματος και χαρακτηρισμός της εταιρείας ως αναξιόπιστης και επικίνδυνης
- ☐ Καμιά ενέργεια

38. Διαθέτει η επιχείρησή σας τη δυνατότητα να υπολογίζει το κόστος μιας ενδεχόμενης (πετυχημένης) επίθεσης στο δίκτυό της;

☐ Ναι ☐ Όχι

39. Ποια κριτήρια χρησιμοποιεί για την κοστολόγησή της;

_____
_____
_____
_____

40. Πόσο προσωπικό του τμήματος IT απασχολείται στον τομέα της ασφάλειας; Αν δεν υπάρχει προσωπικό που να απασχολείται αποκλειστικά στον τομέα της ασφάλειας, ποιο είναι το πλήθος των ανθρωπο-ωρών που δαπανώνται για θέματα ασφαλείας από προσωπικό άλλων τομέων;

_____
_____
_____
_____

Σας ευχαριστούμε πολύ για τη συνεργασία σας!

Επωνυμία Επιχείρησης _____

Ονοματεπώνυμο _____

Διεύθυνση _____

Τηλέφωνο _____

e-mail _____

Οι πληροφορίες που μας προσφέρετε θα παραμένουν αυστηρώς εμπιστευτικές και θα χρησιμοποιηθούν μόνο για το σκοπό της μελέτης μας.

ΠΑΡΑΡΤΗΜΑ Β. Κατάλογος Επιχειρήσεων

ΕΠΩΝΥΜΙΑ ΕΠΙΧΕΙΡΗΣΗΣ	ΔΙΑΚΡΙΤΙΚΟΣ ΤΙΤΛΟΣ	ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΔΙΕΥΘΥΝΣΗ	E-MAIL	ΙΣΤΟΣΕΛΙΔΑ
ΚΑΝΕΛΛΟΠΟΥΛΟΣ Γ. ΚΑΙ ΣΙΑ Ο.Ε.	KANELLOPOULOS FIREWORKS	ΕΡΓΟΣΤΑΣΙΟ ΠΥΡΟΤΕΧΝΗΜΑΤΩΝ	ΖΕΥΓΟΛΑΤΕΙΟ ΚΟΡΙΝΘΙΑΣ	info@pirotexnimata.gr	www.pirotexnimata.gr
ΖΗΤΡΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ Ε.Π.Ε.	ΕΚΔΟΣΕΙΣ ΖΗΤΡΟΣ	ΕΚΔΟΤΙΚΟΣ ΟΙΚΟΣ	ΠΛΑΤΩΝΟΣ 2 ΘΕΣΣΑΛΟΝΙΚΗ	info@zitros.gr	www.zitros.gr
Ε.Δ. ΓΟΥΤΟΣ Α.Ε.	GOUTOS REAL ESTATE	ΚΤΗΜΑΤΟΜΕΣΙΤΙΚΗ ΚΑΤΑΣΚΕΥΑΣΤΙΚΗ ΕΤΑΙΡΙΑ	ΑΚΑΜΗΔΙΑΣ 81 ΑΘΗΝΑ	info@goutos.com	www.goutos.com
ΠΑΠΑΔΗΜΗΤΡΙΟΥ ΧΑΡΑΛΑΜΠΟΣ Δ.	ΠΟΛΥΜΟΡΦΟ	ΕΡΓΑΣΤΗΡΙ ΚΟΡΝΙΖΑΣ	ΚΑΚΑΡΑ ΜΙΧΑΗΛ 23 & ΑΓΓΕΛΑΤΟΥ 13 ΧΑΛΚΙΔΑ	polymorpho@gmail.com	www.polymorpho.gr
Γ. & Δ. ΑΛΥΓΙΖΑΚΗΣ & ΣΙΑ Ο.Ε.	ΤΟ ΣΠΙΤΙΚΟ	ΕΡΓΑΣΤΗΡΙΟ ΑΡΤΟΖΑΧΑΡΟΠΛΑΣΤΙΚΗΣ	ΒΙΟ. ΠΑ. ΧΑΝΙΩΝ ΣΟΥΔΑ	info@spitiko.com.gr	www.spitiko.com.gr
ΘΕΟΔΩΡΟΠΟΥΛΟΣ ΘΕΜΙΣΤΟΚΛΗΣ Ε.Ε.	AVANCE RENT A CAR AVANCE TRAVEL	ΜΙΣΘΩΣΕΙΣ ΑΥΤΟΚΙΝΗΤΩΝ	4Ο ΧΛΜ. Ε.Ο. ΝΑΥΠΑΚΤΟΥ ΑΝΤΙΡΙΟΥ ΝΑΥΠΑΚΤΟΣ	info@theocar.com	www.theocar.com

ΕΠΩΝΥΜΙΑ ΕΠΙΧΕΙΡΗΣΗΣ	ΔΙΑΚΡΙΤΙΚΟΣ ΤΙΤΛΟΣ	ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΔΙΕΥΘΥΝΣΗ	E-MAIL	ΙΣΤΟΣΕΛΙΔΑ
ΧΡΗΣΤΟΣ ΠΕΤΙΚΑΣ ΚΑΙ ΤΕΑ ΠΕΤΙΚΑ Ο.Ε.	PETIKAS IMPORT & EXPORT	ΟΠΩΡΟΚΗΠΕΥΤΙΚΑ ΣΥΣΚΕΥΑΣΙΑ ΚΑΙ ΤΥΠΟΠΟΙΗΣΗ	ΑΓ. ΜΑΡΙΝΑ ΗΜΑΘΙΑΣ ΒΕΡΟΙΑ	info@petikasfruits.eu petikas@petikasfruits.gr	petikasfruits.eu
ΡΑΔΙΟΦΩΝΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ	ΔΙΕΣΗ FM Α.Ε.	ΡΑΔΙΟΦΩΝΙΚΟΣ ΥΠΗΡΕΣΙΕΣ-ΣΤΑΘΜΟΙ	ΒΙΛΤΑΝΙΩΤΗ 36 ΚΗΦΙΣΙΑ	diesi@diesi.gr	www.diesi.gr
ΣΤΕΦΟΣ Θ. & ΣΙΑ Ο.Ε.	ΜΑΙΑΝΔΡΟΤΕΧΝΙΚΗ	ΚΑΤΑΣΚΕΥΗ ΧΕΙΡΟΠΟΙΗΤΩΝ ΚΟΣΜΗΜΑΤΩΝ	Σ. ΣΙΑΠΚΑ 9 ΕΛΕΟΥΣΑ ΙΩΑΝΝΙΝΩΝ	info@greeksilver.gr	www.greeksilver.gr
ΞΕΝΟΔΟΧΕΙΑΚΕΣ ΤΟΥΡΙΣΤΙΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΠΑΛΛΙΚΗΣ ΚΕΦΑΛΛΟΝΙΑΣ Α.Ε.	APOLLONION RESORT AND SPA	ΞΕΝΟΔΟΧΕΙΑΚΗ ΚΑΙ ΤΟΥΡΙΣΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ	ΛΗΞΟΥΡΙ ΚΕΦΑΛΛΗΝΙΑΣ	info@apollonion-hotel.gr	www.apollonion-hotel.gr