ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
«ΟΡΓΑΝΩΣΗ ΚΑΙ ΔΙΟΙΚΗΣΗ ΔΗΜΟΣΙΩΝ ΥΠΗΡΕΣΙΩΝ, ΟΡΓΑΝΙΣΜΩΝ ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΩΝ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Διοίκηση Ολικής Ποιότητας στην Ασφάλεια Πληροφοριακών Συστημάτων Δημοσίων Οργανισμών και Υπηρεσιών

Τσιφτσίδης Γεώργιος
Α.Μ. ΠΜΣ06038

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ:
Βασιλική Σκίντζη

Τρίπολη, Ιούνιος 2008

Πίνακας περιεχομένων

Κατάλογος σχημάτων

Κατάλογος πινάκων

Περίληψη

Η ασφάλεια είναι κρίσιμος παράγων για την επιτυχία οποιουδήποτε οργανισμού. Οι οργανισμοί και τα πληροφοριακά τους συστήματα συνεχώς αντιμετωπίζουν απειλές της ασφάλειάς τους από ένα μεγάλο εύρος διαφορετικών πηγών, όπως ηλεκτρονική απάτη, βιομηχανική κατασκοπεία, βανδαλισμός, φωτιά ή πλημύρα. Επιπλέον, επιθέσεις με ιούς (viruses), hacking, cracking και επιθέσεις τύπου άρνησης παροχής υπηρεσιών (denial of service) έχουν πλέον γίνει συνήθεις και όλο πιο πολύπλοκες στην αντιμετώπισή τους.

Σαν απάντηση, οι οργανισμοί υιοθετούν νέες πολιτικές ασφάλειας. Είναι σαφές ότι πολλές από αυτές τις πολιτικές ασφάλειας έχουν κόστος όταν κάθε οργανισμός έχει περιορισμένους πόρους που μπορεί να αφιερώσει στην προστασία της ροής των πληροφοριών του. Το κόστος της ασφάλειας μπορεί να είναι χρηματικό (π.χ. η τιμή ενός firewall) ή μη-χρηματικό (π.χ. η απαίτηση από τους υπαλλήλους να χρησιμοποιούν σύνθετους κωδικούς πρόσβασης).

Ο στόχος ενός οργανισμού πρέπει να είναι στο να αναπτύξει την πιο κατάλληλη προσέγγιση στην ασφάλεια (δηλαδή, μια ισορροπία μεταξύ του κόστους και της αποτελεσματικότητας). Αυτό γίνεται περισσότερο περίπλοκο από το γεγονός ότι είναι πιθανό να υπάρχουν διαφορετικές προτεραιότητες μέσα σε ένα οργανισμό.

Επιπρόσθετα όσο οι οργανισμοί εξελίσσονται και επεκτείνονται δημιουργώντας διαρκώς νέες διασυνδέσεις με προμηθευτές, πελάτες, και άλλους οργανισμούς, θα υπάρχει διαρκώς ένα ευρύτερο φάσμα των απαιτήσεων ασφάλειας. Η διαχείριση της ασφάλειας είναι ένα διοικητικό και όχι ένα αμιγώς τεχνικό πρόβλημα.

Υπάρχουν πολλές σημαντικές ομοιότητες μεταξύ των προσπαθειών για Διοίκηση Ολικής Ποιότητας (από το 1950 και μετά) και του αυξανόμενου ενδιαφέροντος για το κόστος και την ποιότητα της ασφάλειας στις επιχειρήσεις σήμερα. Η Διοίκηση Ολικής ποιότητας είναι ένας συνδυασμός εργαλείων ποιότητας και διοίκησης με τα οποία διοίκηση και υπάλληλοι επιφέρουν τη συνεχή βελτίωση των λειτουργιών. Η κουλτούρα της Διοίκησης Ολικής Ποιότητας απαιτεί όλα να γίνονται σωστά από την πρώτη φορά και στη συνέχεια να υπάρχει διαρκής βελτίωση από εκείνο το σημείο.

Κάποια στιγμή θεωρήθηκε ότι έπρεπε να γίνει επιλογή μεταξύ της βελτίωσης της ποιότητας και της μείωσης του κόστους. Η Διοίκηση Ολικής

Ποιότητας έδειξε ότι ήταν δυνατό να βελτιωθεί και η ποιότητα και η αποδοτικότητα δαπανών. Πολλοί άνθρωποι βλέπουν τώρα την ασφάλεια σαν ένα "πρόσθετο" κόστος (όπως κάποτε εξετάστηκε η βελτίωση ποιότητας), αλλά αυτή η άποψη βρίσκεται υπό αμφισβήτηση. Υπάρχουν εκείνοι που θεωρούν ότι μια σαφέστερη κατανόηση της ασφάλειας μπορεί να οδηγήσει όχι μόνο στην αύξηση της ασφάλειας αλλά και το χαμηλότερο κόστος. Ένα σημαντικό πρώτο βήμα στην προσπάθεια για Διοίκηση Ολικής Ποιότητας ήταν ο ακριβής προσδιορισμός του τι σημαίνει ακριβώς "ποιότητα" , ειδικά κάτω από μια πιο ολιστική έννοια. Προκειμένου να σημειωθεί σοβαρή πρόοδος προς τη βελτίωση της ασφάλειας σε επιχειρησιακό επίπεδο, πρέπει να προσδιορίσουμε την έννοια της ποιοτικής επιχειρησιακής ασφάλειας και να αναπτύξουμε αποτελεσματικούς τρόπους αποτίμησης και μέτρησής της.

Αυτή η διπλωματική εργασία εξετάζει το θέμα της χρησιμοποίησης των μοντέλων και των μεθοδολογιών της Διοίκησης Ολικής Ποιότητας προκειμένου να δημιουργηθεί μια αποτελεσματική ασφάλεια Πληροφοριακών Συστημάτων στο Δημόσιο Τομέα.

Executive Summary

Security is crucial for the success of any organization. Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

In response, organizations have adopted new security policies. It is clear that many of these security policies are valuable, however an organization may be limited in how much of its resources it can devote to protecting its flows of information. Security costs can be incurred monetarily (e.g., the price of a new firewall) or non-monetarily (e.g., requiring employees to use convoluted passwords). An organization's goal should be to develop the most appropriate approach to security (i.e., a balance between cost and effectiveness). This is further complicated by the fact that there are likely to be different priorities for the various stakeholders in the organization. Furthermore, as organizations evolve towards becoming extended enterprises, including close ties with suppliers, customers, and other partners, there will be a significant increase in the number of stakeholders and thus a wider range of security requirements. Security administration is a management and not a purely technical issue.

There are many important similarities between the Total Quality Management (TQM) efforts (of the 1950s onward) and the increasing concerns about the cost and quality of security in enterprises today. Total Quality Management is a combination of quality and management tools by which management and employees become involved in the continuous improvement of operations. The culture of TQM demands that organizations do it right first time and continuously improve from there. At one time it was thought that one had to choose between improving quality and lowering cost. TQM showed that it was possible to improve both quality and cost efficiency.

Many people now view security as an "add-on" cost (as improved quality was once considered), but that view is being increasingly challenged. There are those that believe that a clearer understanding of security can lead to not only increased security but also lower costs. An important early step in the TQM effort was to more precisely define what "quality" meant, especially in a more holistic sense. In order to make

serious progress towards improving enterprise level security, we need to define the concept of enterprise "security" and develop effective ways to assess and measure it.

This master thesis deals with the subject of using models and methodologies of Total Quality Management in order to build an effective Information System Security into public sector.

Εισαγωγή

Ο δημόσιος τομέας αντιμετωπίζει την πρόκληση του eGovernment που συνίσταται, στη χρήση τεχνολογιών Πληροφορικής και Επικοινωνιών, σε συνδυασμό με οργανωσιακές αλλαγές και τη δημιουργία νέων δυνατοτήτων, με σκοπό τη βελτίωση της παροχής των δημόσιων υπηρεσιών, στην αύξηση της Συμμετοχικής Δημοκρατίας και στην ενίσχυση της χάραξης της Δημόσιας Πολιτικής. Οι οργανισμοί του δημόσιου δικτυώνονται όλο και περισσότερο καθώς υπάρχει απαίτηση για ανταλλαγή πληροφοριών, οι οποίες γίνονται διαθέσιμες ηλεκτρονικά.

Ταυτόχρονα οι Δημόσιοι Οργανισμοί αυξάνουν διαρκώς την εξάρτησή τους από τα Πληροφοριακά Συστήματα. Αυτό συνδέεται με μια εξαιρετική αύξηση στη χρήση των υπηρεσιών Διαδικτύου, μέσου του οποίου διεξάγεται πλέον ένας σημαντικός αριθμός εργασιών και παροχής δημοσίων υπηρεσιών. Η αυξανόμενη χρήση των Πληροφοριακών Συστημάτων στην αποθήκευση, την επεξεργασία και διανομή των πληροφοριών, καθιστά την ασφάλειά τους περισσότερο σημαντική.

Η ασφάλεια των προσωπικών δεδομένων που αποθηκεύουν και επεξεργάζονται οι δημόσιοι οργανισμοί, είναι ζωτικής σημασίας για τη διατήρηση της δημόσιας εμπιστοσύνης προς τους οργανισμούς. Οι απειλές, από άλλες ξένες κυβερνητικές υπηρεσίες, παράνομους, και δημοσιογράφους, είναι πολυάριθμες. Η διακοπή μιας παρουσίας στο Διαδίκτυο μπορεί να είναι καταστρεπτική για τους επιχειρησιακούς στόχους των οργανισμών και τη δημόσια εικόνα τους. Επίσης η ασφάλεια των πληροφοριών και των δικτύων επικοινωνιών αναγνωρίζεται σαν ένα όλο και περισσότερο ζωτικής σημασίας στοιχείο, για την εξασφάλιση της ευρείας συμμετοχής των πολιτών στην Κοινωνία της Πληροφορίας. Δεδομένου ότι νέα μοντέλα Δημοσιών Οργανισμών και Υπηρεσιών αναπτύσσονται για να εκμεταλλευτούν τις διευκολύνσεις και τις δυνατότητες που παρέχονται από τα νέα μέσα παγκόσμιων επικοινωνιών και πληροφορικής, αυξάνεται ο προβληματισμός αν η ασφάλεια των Πληροφοριακών Συστημάτων και το απόρρητο των επικοινωνιών, μπορεί να εμποδίσει τη πλήρη υιοθέτησή τους. Η ασφάλεια είναι επίσης ουσιαστική στη διατήρηση της εμπιστοσύνης των πολιτών για τη διαρκή χρήση των υπαρχόντων και των μελλοντικών τεχνολογιών. Η κυβέρνηση θέλει να εξασφαλίσει ότι η χώρα είναι ένας ασφαλής τόπος για να είναι on-line. Η καλή ασφάλεια πληροφοριών αντιμετωπίζεται όλο και περισσότερο ως σημαντική για την επιτυχία και τη σταθερότητα της χώρας συνολικά.

Σύμφωνα με την με την εξαμηνιαία έκθεση της Symantec για τις διαδικτυακές απειλές (ISTR, 2007), προκύπτει ότι οι πιο δημοφιλείς στόχοι διεθνώς είναι οι οικονομικές υπηρεσίες, και ακολουθούν οι τηλεπικοινωνίες και ο δημόσιος τομέας.

Για τους λόγους αυτούς οι Δημόσιοι Οργανισμοί και Υπηρεσίες στην Ελλάδα πρέπει να λάβουν τα ανάλογα μέτρα, ώστε να αναπτύξουν και να βελτιώσουν τις άμυνες, που θα τους προσφέρουν υψηλότερη ασφάλεια σε ηλεκτρονικές επιθέσεις εναντίον των υποδομών τους και της υποκλοπής ευαίσθητων προσωπικών δεδομένων.

Όμως η δημιουργία ενός ασφαλούς περιβάλλοντος για τους δημόσιους οργανισμούς δεν είναι απλή υπόθεση. Πρόκειται για μια μεγάλη επένδυση που δεν αφορά μόνο την αγορά των κατάλληλων λογισμικών και υπολογιστών. Ούτε είναι τόσο απλό ώστε να ανατεθεί απλώς σαν έργο *outsourcing* σε ένα εξωτερικό παράγοντα ή ακόμη σε μια ομάδα ανθρώπων μέσα στον οργανισμό. Είναι απολύτως απαραίτητη η επένδυση όχι μόνο σε τεχνολογία, αλλά και στην εκπαίδευση των ανθρώπων και στον εκσυγχρονισμό των διοικητικών δομών. Απαιτείται η χάραξη πολιτικών, η ανάπτυξη στρατηγικών, η σχεδίαση μεθοδολογιών, η υλοποίηση μέτρων ελέγχου, η διαμόρφωση της κατάλληλης κουλτούρας, καθώς και η διαρκής αξιολόγηση και βελτίωση του συνολικού εγχειρήματος. Το πρόβλημα είναι πολύπλευρο και σύνθετο. Οι παράγοντες που πρέπει να ληφθούν υπόψη αποτελούν στη μεγάλη τους πλειοψηφία στοιχεία, που τα τελευταία χρόνια έχουν εμφανιστεί και απασχολήσει τους επιστήμονες – ερευνητές του χώρου, παρόλο που η προσέγγιση της ασφάλειας μέσω της Διοίκησης Ολικής Ποιότητας έχει ελάχιστα διερευνηθεί, μολονότι αρχές της, μέσω της πιστοποίησης κατά ISO 27001:2005, υιοθετούνται ευρέως.

Διαβάζοντας κάποιος τη παρούσα εργασία θα μπορέσει να κατανοήσει βασικά ζητήματα γύρω από την ασφάλεια των Πληροφοριακών Συστημάτων, την Διοίκηση Ολικής Ποιότητας και να εμβαθύνει κυρίως στη διαδικασία εκπόνησης μιας πολιτικής ασφάλειας καθώς και στους παράγοντες που την επηρεάζουν. Πρόκειται για μια εργασία που προσπαθεί να διερευνήσει τη δυνατότητα και τη καταλληλότητα υιοθέτησης των αρχών της Διοίκησης Ολικής Ποιότητας για τη δημιουργία ενός μοντέλου Διαχείρισης Ασφάλειας Ολικής Ποιότητας, που μπορεί να εφαρμοσθεί σε Δημόσιους οργανισμούς και επιχειρήσεις.

Η εργασία στηρίζεται σε μια διεξοδική και σε βάθος έρευνα σε σχετικές πηγές και τη βιβλιογραφία.

Προφανώς αφού μιλάμε για συστήματα δεν θα μπορούσαμε παρά να αρχίζαμε στο πρώτο κεφάλαιο από μια εννοιολογική ανάλυση της συστημικής προσέγγισης και

μια εισαγωγή στα Πληροφοριακά Συστήματα.

Στο δεύτερο κεφάλαιο γίνεται αναφορά στη Διοίκηση Ολικής Ποιότητας, και δεν θα μπορούσε να γίνει διαφορετικά καθώς σκοπός της εργασίας αυτής είναι, να διερευνήσει αν η υιοθέτηση των αρχών της, θα μπορούσε να δώσει λύση στο μεγάλο πρόβλημα της ασφάλειας των Πληροφοριακών Συστημάτων. Έτσι γίνεται αναφορά στα μοντέλα και εργαλεία Διοίκησης Ολικής Ποιότητας, τόσο γιατί προωθείται γενικότερα η εφαρμογή τους με στόχο την ενίσχυση της αποτελεσματικότητας των υπηρεσιών του Δημόσιου τομέα, όσο και γιατί εφαρμόζονται στο προτεινόμενο μοντέλο του Συστήματος Διαχείρισης Ασφάλειας Ολικής Ποιότητας.

Το τρίτο κεφάλαιο ασχολείται με το ζητούμενο της εργασίας, που είναι η ασφάλεια των Πληροφοριακών Συστημάτων. Αφού μιλάμε για ασφάλεια δεν θα μπορούσαμε παρά να αρχίζαμε από μια ανασκόπηση των απειλών – κινδύνων που αντιμετωπίζει ένας Δημόσιος οργανισμός καθώς αντιμετωπίζει εξωτερικές και εσωτερικές απειλές. Αφού γίνουν οι εννοιολογικές αναλύσεις των σχετικών με την ασφάλεια ορισμών, στη συνέχεια παρατίθενται τα μοντέλα ασφάλειας ΠΣ.

Στο βασικότερο τμήμα της εργασίας, το τέταρτο κεφάλαιο, δημιουργείται ένα μεθοδολογικό πλαίσιο για την ένταξη όλων των ζητημάτων δημιουργίας ασφάλειας σε ένα Σύστημα Διαχείρισης Ασφάλειας Ολικής Ποιότητας. Στα πλαίσια αυτά προτείνεται ένα μοντέλο το οποίο στηρίζεται στο σύστημα του ISO/IEC 27001:2005 και στο οποίο εφαρμόζονται οι αρχές της ΔΟΠ και υιοθετούνται έγγραφα και συστάσεις των οργανισμών ΟΟΣΑ και ENISA[1] .

Στο πέμπτο κεφάλαιο γίνεται συνοπτική αναφορά στη Πολιτική Ασφάλειας δηλαδή στο αναγκαίο σύνολο των οδηγιών της διοίκησης για τον "τρόπο" με τον οποίο πρέπει να λειτουργεί ο οργανισμός για να υπάρχει ασφάλεια.

Όμως το πεδίο εφαρμογής των τεχνικών, των μεθοδολογιών και των συστημάτων διαχείρισης της ασφάλειας διαφέρει από οργανισμό σε οργανισμό, και κάθε μέτρο και μηχανισμός ασφάλειας έχει ένα κόστος. Η ανάλυση επικινδυνότητας, στην οποία γίνεται αναφορά στο έκτο κεφάλαιο, απαντά στο ερώτημα της επιλογής αντιμέτρων που θα προσφέρουν προστασία ανάλογη των κινδύνων που απειλούν ένα οργανισμό.

Παράλληλα με τα μέτρα, οι σημερινές επιχειρήσεις και οργανισμοί απαιτείται να έχουν μια κουλτούρα ασφάλειας που να είναι κυρίαρχη στο σύνολο της οργάνωσης, και που να ευθυγραμμίζει τους ανθρώπους και τις πρακτικές με τους στόχους

---

[1]Αντιπροσωπεία της ΕΕ για θέματα ασφάλειας.

ασφάλειας. Έτσι στο έβδομο κεφάλαιο προσεγγίζονται εννοιολογικά η οργανωσιακή κουλτούρα και η κουλτούρα ασφάλειας. Στη συνέχεια αναπτύσσονται πρώτα η προσέγγιση της ENISA αναφορικά με τη δημιουργία μιας κουλτούρας ασφάλειας και στη συνέχεια η αλλαγή κουλτούρας με το μοντέλο της 'Οργάνωσης που Μαθαίνει την Ασφάλεια'.

Σε κάθε Σύστημα Διαχείρισης Ασφάλειας απαιτείται η εκπαίδευση και η ενημέρωση του προσωπικού ώστε να διασφαλιστεί ότι είναι εκπαιδευμένο, εκτελεί τις εργασίες του και συμπεριφέρεται σύμφωνα με τις απαιτήσεις του Συστήματος Διαχείρισης Ασφάλειας. Το ζήτημα της ενημέρωσης ασφάλειας είναι το αντικείμενο του ογδόου, και τελευταίου, κεφαλαίου της εργασίας. Εδώ παρουσιάζεται ένα μοντέλο προγράμματος ενημέρωσης που προέρχεται από την ENISA.

Τέλος στα συμπεράσματα της εργασίας αυτής υποστηρίζεται ότι η εισαγωγή αρχικά ενός Συστήματος Διοίκησης Ποιότητας και στη συνέχεια ενός Συστήματος Διαχείρισης Ασφάλειας Ολικής Ποιότητας, σύμφωνα με το προτεινόμενο μοντέλο της εργασίας, αποτελεί μια αξιόπιστη και εφαρμόσιμη επιλογή η οποία διασφαλίζει το αναγκαίο και ασφαλές περιβάλλον για την αποτελεσματική λειτουργία των οργανισμών στα πλαίσια της Ηλεκτρονικής Διακυβέρνησης γενικότερα.

Κεφάλαιο 1

Συστημική προσέγγιση

1.1. Εισαγωγή

Η επιλογή της συστημικής προσέγγισης για τη μελέτη και ανάλυση του αντικειμένου της διπλωματικής εργασίας θεωρήθηκε απαραίτητη λαμβάνοντας υπόψη τόσο την πολυπλοκότητα που παρουσιάζει το θέμα όσο και την προσπάθεια αποφυγής μιας "μονολιθικής και παράλληλα μηχανιστικής προσέγγισης" (Waldman, 1994:513), η οποία θα αποτελούσε τροχοπέδη για μια ολοκληρωμένη προσέγγιση γύρω από το ζήτημα της ασφάλειας και από την ανάλυση της σχέσης Διοίκηση Ολικής Ποιότητας και ασφάλεια Πληροφοριακών Συστημάτων.

Η μελέτη της ασφάλειας των Πληροφοριακών συστημάτων μέσα από μια φιλοσοφία ποιότητας προϋποθέτει την χρησιμοποίηση μιας προσέγγισης η οποία θα δίνει μια ολοκληρωμένη εικόνα των παραγόντων που επηρεάζουν τη συγκεκριμένη σχέση και αλληλεπιδράσεις και αλληλεξαρτήσεις μεταξύ αυτών των παραγόντων.

Αυτό σημαίνει ότι η ασφάλεια των ΠΣ επηρεάζεται και από "εσωτερικές" μεταβλητές και παράγοντες αλλά και από μεταβλητές του ευρύτερου περιβάλλοντος και φυσικά από ζητήσεις, περιορισμούς, κινδύνους και ευκαιρίες του ίδιου του συστήματος.

1.2. Αρχές της θεωρίας συστημάτων

Η συστημική προσέγγιση αποτελεί έναν νέο τρόπο σκέψης ή οπτική γωνία και μέθοδο μελέτης φαινομένων και οργανισμών. Αυτή στηρίζεται στις αρχές της *γενικής θεωρίας συστημάτων* που αναπτύχθηκε κατά τη δεκαετία του 1950, κυρίως από τους Bertalanffly, Boulding, Rapoport, και Gerard. Η βασική λογική και επιδίωξη συγχρόνως της γενικής θεωρίας των συστημάτων συνίσταται στην ύπαρξη ενός γενικού πλαισίου αρχών το οποίο μπορεί να χρησιμοποιηθεί για την μελέτη και έρευνα όλων των φαινομένων. Έτσι θα μπορούσε να αναπτυχθεί η συνεργασία των διάφορων περιχαρακωμένων επιστημονικών κλάδων και να επιτευχθεί η διεπιστημονική προσέγγιση. Στη θεωρία των οργανώσεων και το μάνατζμεντ γενικότερα, η συστημική προσέγγιση έχει βοηθήσει την αναλυτική και συνθετική

σκέψη και συμβάλει έτσι στην καλύτερη κατανόηση των φαινομένων. (Δ.Μπουραντάς, 2002:31)

Σύστημα ονομάζεται ένα οργανωμένο και ολοκληρωμένο σύνολο από αλληλεξαρτώμενα και αλληλεπιδρώντα συστατικά στοιχεία. Ένα σύστημα έχει *αντικειμενικούς σκοπούς* ή *στόχους* που συχνά είναι δύσκολο να παρατηρηθούν.

Το περιβάλλον ενός συστήματος περιλαμβάνει οτιδήποτε υπάρχει έξω από τον έλεγχο του. Το περιβάλλον καθορίζει κατά κάποιο τρόπο την αποδοτικότητα του συστήματος και κατά συνέπεια, υπάρχει αλληλεπίδραση και αλληλεξάρτηση μεταξύ ενός συστήματος και του περιβάλλοντος μέσα στο οποίο λειτουργεί.

Πόροι είναι όλα τα μέσα που έχει στη διάθεση του το σύστημα για την εκτέλεση των αναγκαίων δραστηριοτήτων κατά τρόπο ώστε να επιτυγχάνονται οι στόχοι του. Σε αντίθεση με το περιβάλλον, οι πόροι είναι εσωτερικοί στο σύστημα και ευρίσκονται υπό τον έλεγχο του. Ένα σύστημα αποτελείται από συστατικά στοιχεία όπως διεργασίες, δραστηριότητες, αποστολές ή τα επιμέρους τμήματα του που αποβλέπουν στην επίτευξη των στόχων του. Για την κατανόηση ενός συστήματος είναι απαραίτητη η ολική θεώρηση του και όχι η θεώρηση των επιμέρους συστατικών του (π.χ. των οργανωτικών του μονάδων).

Η διοίκηση ενός συστήματος αποτελείται από εκείνες τις δραστηριότητες που αποσκοπούν στον προγραμματισμό (planning) και τον έλεγχο (control). Ο προγραμματισμός περιλαμβάνει τον καθορισμό των στόχων του συστήματος, την αξιοποίηση των πόρων του, την κατασκευή ενός προγράμματος για την ανάληψη διαφόρων δραστηριοτήτων και την επιλογή μας στρατηγικής για τις σχέσεις με το περιβάλλον του. Ο έλεγχος αφορά την υλοποίηση των προγραμμάτων που καθορίστηκαν κατά τη διαδικασία του προγραμματισμού. Έτσι, ο έλεγχος συνδέεται με την ροή των πληροφοριών και την παρακολούθηση της αποδοτικότητας του συστήματος για την ανάληψη κάποιας διορθωτικής δράσης (feedback).

Γενικά, κάθε σύστημα δέχεται κάποια εισερχόμενα τα οποία επεξεργάζεται για την παραγωγή κάποιων εξερχόμενων, αποτελείται από έναν αριθμό συστατικών στοιχείων που ονομάζονται υποσυστήματα και υπάρχει και λειτουργεί μέσα σε κάποιο περιβάλλον. Κάθε σύστημα ή υποσύστημα έχει κάποια όρια, τα οποία το διακρίνουν από το περιβάλλον του, και διαθέτει κάποιο μηχανισμό για την παρακολούθηση της αποδοτικότητας του και για την ανάληψη δράσης ελέγχου όπου απαιτείται (Γ.Βασιλακόπουλος Β.Χρυσικόπουλος, 1990:15).

1.3. Ο Οργανισμός ως σύστημα

Κάθε οργανισμός μπορεί να θεωρηθεί ως σύστημα με εισερχόμενα, εξερχόμενα, υποσυστήματα, μηχανισμούς ελέγχου και πόρους. Οι οργανισμοί υπάρχουν και λειτουργούν σε περιβάλλοντα των οποίων η ύπαρξη είναι τόσο γνωστή που θεωρείται συνήθως ως δεδομένη.

Οι οργανισμοί, όπως και όλα τα συστήματα, έχουν κάποια αποστολή ή κάποιο αντικειμενικό σκοπό, αξιοποιούν τους διαθέσιμους από το περιβάλλον πόρους, τους οργανώνουν και επιδιώκουν την επίτευξη του σκοπού αυτού. Κάθε οργανισμός προσθέτει κάποια αξία στα εισερχόμενα επεξεργάζοντάς τα και επιστρέφει τα εξερχόμενα στο περιβάλλον του για να τα ανταλλάξει με στόχο την απόκτηση πόρων. Εάν ο οργανισμός ανταμοίβεται για την προστιθέμενη αξία που παρέχει μπορεί να αποκτήσει περισσότερους πόρους και να συνεχίσει ομαλά την λειτουργία του. Στην αντίθετη περίπτωση, ο οργανισμός πρέπει να χρησιμοποιήσει τις πληροφορίες επανάδρασης για να προβεί στις αναγκαίες αλλαγές και να προσαρμοσθεί ώστε να συνεχίσει να υπάρχει. Δηλαδή, ο οργανισμός πρέπει να διαθέτει σωστή πληροφόρηση για να αντιδρά με επιτυχία στο περιβάλλον μέσα στο οποίο λειτουργεί. (Βασιλακόπουλος, Χρυσικόπουλος, 1990:23)

Σύμφωνα με τη συστημική προσέγγιση, η αλλαγή παίρνει τη μορφή "προσαρμογής" και εμφανίζεται σαν το προϊόν εξωγενών διαφοροποιήσεων και μεταβολών του περιβάλλοντος. Ένας "ζωντανός" οργανισμός θα πρέπει να εκλαμβάνει, να επεξεργάζεται και να απαντά σε ένα συνεχώς μεταβαλλόμενο περιβάλλον και να προσαρμόζεται , επαναπροσδιορίζοντας εσωτερικές οργανωσιακές δομές για τη διασφάλιση της επιβίωσης ή της αποτελεσματικότητας. Η διεξοδική και σε βάθος μελέτη των προσδιοριστικών παραγόντων του συστήματος επικοινωνίας καθώς και των μεθόδων και τεχνικών επικοινωνίας που χρησιμοποιούν οι οργανισμοί για την συλλογή, επεξεργασία και τυποποίηση πληροφοριών από το περιβάλλον για τη λήψη αποφάσεων, προσφέρει τη βάση για την αποτελεσματική μελέτη των επιπτώσεων του περιβάλλοντος στον οργανισμό ως σύνολο.

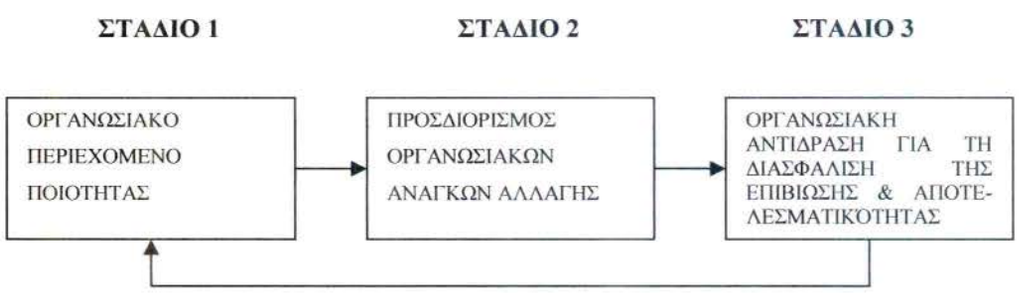
Για την υιοθέτηση της Διοίκησης Ολικής Ποιότητας[2] από ένα οργανισμό και

---

[2]«Μία ολική οργανωσιακή προσέγγιση για την ικανοποίηση των αναγκών και των προσδοκιών των πελατών που εμπλέκει όλους τους προϊσταμένους και υπαλλήλους στην χρήση ποσοτικών μεθόδων προκειμένου να επιτευχθεί συνεχής βελτίωση των διαδικασιών, των προϊόντων και των υπηρεσιών του οργανισμού» ορισμός του Αμερικανικού Ομοσπονδιακού Ινστιτούτου Ποιότητας, 1990 (S. Harrison, 1993:418).

λαμβάνοντας υπόψη ότι τα προβλήματα της ποιότητας πηγάζουν από εξωτερικούς παράγοντες (Benson et. al, 1991:1107), όπως οι απαιτήσεις των πελατών, ο αυξανόμενος ανταγωνισμός, οι νόμοι και οι κανονισμοί του κράτους, τότε η συστημική προσέγγιση είναι απαραίτητη για τη συγκεκριμενοποίηση και κρυσταλοποίηση των θεμελιωδών στηριγμάτων, αρχών και πρακτικών μεθόδων της Διοίκησης Ολικής Ποιότητας. Σύμφωνα με τον Benson ακολουθώντας την συστημική προσέγγιση, η ΔΟΠ μπορεί να χαρακτηρισθεί σαν μια διαδικασία τριών σταδίων (Σχήμα 1). Στο πρώτο στάδιο ο οργανισμός μέσω των στελεχών της αντιλαμβάνεται το οργανωσιακό περιεχόμενο της Διοίκησης Ολικής Ποιότητας το οποίο αποτελείται από εξωτερικές ζητήσεις/πιέσεις για βελτίωση της ποιότητας, από προηγούμενους δείκτες απόδοσης των προσπαθειών βελτίωσης της ποιότητας, την υπάρχουσα πολιτική και στρατηγική οργάνωσης και διοίκησης ποιότητας.

Ακόμη σε αυτό το στάδιο εξετάζονται οι επιδράσεις και οι επιρροές από το εξωτερικό περιβάλλον όπως ανταγωνιστές πιέσεις και εισαγωγή νέων μεθόδων ή συστημάτων διασφάλισης ποιότητας. Στο δεύτερο στάδιο, ανάλογα με το οργανωσιακό περιεχόμενο της ποιότητας, οι απόψεις και τα πιστεύω των στελεχών σχηματίζονται αναφορικά με την ποιότητα. Οι οργανισμοί θα πρέπει να εντοπίσουν τις περιοχές εκείνες οι οποίες χρίζουν επίλυσης και τα μέσα που χρειάζονται καθώς και τους απαραίτητους πόρους για την αντιμετώπισή τους.



Σχήμα 1 . Η Συστημική προσέγγιση της Διοίκησης Ολικής Ποιότητας

Στο τρίτο στάδιο γνωρίζοντας το περιεχόμενο και τις οργανωσιακές ανάγκες για αλλαγή, ο οργανισμός αντιδρά με την εφαρμογή διαφόρων μεθόδων και προσεγγίσεων για την απόκτηση της επιδιωκόμενης ποιότητας. Η ποιότητα σύμφωνα με τους θεωρητικούς δεν είναι μόνο η επίτευξη ποιοτικών προϊόντων ή υπηρεσιών αλλά η εμφύτευση μιας φιλοσοφίας συνεχούς βελτίωσης με σκοπό την ικανοποίηση

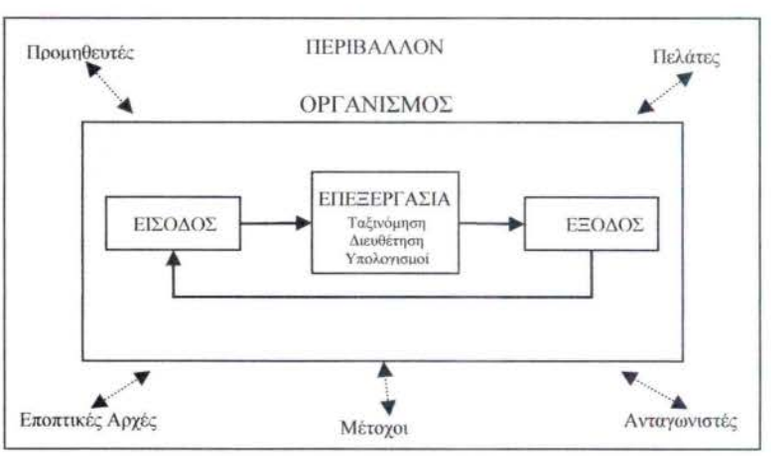
των αναγκών του πελάτη. (Juran, 1998:42-50; Crosby, 1979)

1.4. Πληροφοριακό Σύστημα

Ένα Πληροφοριακό Σύστημα μπορεί να οριστεί τεχνικά (Laudon, 2006:8-9) ως ένα σύνολο αλληλοσχετιζόμενων στοιχείων που λειτουργούν μαζί για τη συλλογή, επεξεργασία, αποθήκευση και διάδοση πληροφοριών ώστε να υποστηρίζουν τη λήψη αποφάσεων, στο συντονισμό, τον έλεγχο, την ανάλυση και την απεικόνιση σε ένα οργανισμό. Ένα πληροφοριακό σύστημα δημιουργεί οικονομική αξία για την επιχείρηση προσφέροντας μια οργανωσιακή και διοικητική λύση, με βάση την τεχνολογία των πληροφοριών, σε μια πρόκληση που τίθεται από το περιβάλλον.

Ένας πληρέστερος ορισμός ενός Πληροφοριακού Συστήματος, στηριζόμενου σε υπολογιστές, είναι αυτός σύμφωνα με τον οποίον: (Κιουντούζης, 2002:320) «*Πληροφοριακό Σύστημα είναι ένα οργανωμένο σύνολο από πέντε στοιχεία (άνθρωποι, λογισμικό, υλικό, διαδικασίες και δεδομένα), τα οποία αλληλεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση πληροφορίας, για την υποστήριξη των ανθρώπινων δραστηριοτήτων, στα πλαίσια του οργανισμού*». Η τεχνική χρήση του όρου σημαίνει λοιπόν ότι το Πληροφοριακό Σύστημα αποτελείται από επιμέρους στοιχεία, που αλληλεπιδρούν, χαρακτηρίζεται από οργάνωση και εξετάζεται ως μία ενιαία ολότητα.

Ένα πληροφοριακό σύστημα περιέχει πληροφορίες για τον οργανισμό και το περιβάλλον του. Τα ΠΣ μετατρέπουν πρωτογενή δεδομένα σε πληροφορίες μέσα από τρεις βασικές δραστηριότητες: είσοδο, επεξεργασία και έξοδο (σχήμα 2).



Σχήμα 2: Οι λειτουργίες ενός πληροφοριακού συστήματος

Η αναπληροφόρηση από την έξοδο επιστρέφει σε κατάλληλους ανθρώπους ή

δραστηριότητες μέσα στον οργανισμό για να αξιολογηθεί και να βελτιωθεί η είσοδος. Παράγοντες του περιβάλλοντος, όπως πελάτες, προμηθευτές, ανταγωνιστές, προμηθευτές, ανταγωνιστές, μέτοχοι, και εποπτικές αρχές αλληλεπιδρούν με τον οργανισμό και τα πληροφοριακά του συστήματα.

Τα ΠΣ στους οργανισμούς είναι αποτέλεσμα της δομής, της κουλτούρας, της πολιτικής, της ροής εργασίας και των πρότυπων διαδικασιών λειτουργίας του οργανισμού. Αποτελούν μηχανισμούς για οργανωσιακή αλλαγή και δημιουργία αξίας, επιτρέποντας να αναδιατυπωθούν αυτά τα στοιχεία του οργανισμού σε νέα επιχειρηματικά μοντέλα. (Laudon, 2006:37)

1.5. Σύγχρονες προσεγγίσεις στα Πληροφοριακά Συστήματα

Οι πολλαπλές θεωρήσεις των πληροφοριακών συστημάτων δείχνουν ότι η μελέτη τους είναι ένα διεπιστημονικό πεδίο. Σε γενικές γραμμές, το πεδίο μπορεί να διαιρεθεί στην τεχνική προσέγγιση και την συμπεριφορική προσέγγιση. (Laudon,2006:19)

Τα πληροφοριακά συστήματα είναι κοινωνικοτεχνικά συστήματα. Αν και απαρτίζονται από μηχανήματα, συσκευές, και απτή φυσική τεχνολογία, χρειάζονται σημαντικές κοινωνικές, οργανωτικές, και διανοητικές επενδύσεις για να λειτουργήσουν όπως πρέπει.

1.5.1. **Τεχνική Προσέγγιση**

Η τεχνική προσέγγιση στα πληροφοριακά συστήματα δίνει έμφαση σε μαθηματικά μοντέλα για τη μελέτη των πληροφοριακών συστημάτων, καθώς και στην υλική τεχνολογία και στις τυπικές δυνατότητες αυτών των συστημάτων. Οι γνωστικοί κλάδοι που συμβάλλουν στην τεχνική *προ*σέγγιση είναι η πληροφορική, η διοίκηση επιχειρήσεων και η επιχειρησιακή έρευνα. Η πληροφορική ασχολείται με την καθιέρωση θεωριών υπολογισιμότητας, μεθόδων υπολογισμού, και μεθόδων αποδοτικής αποθήκευσης και προσπέλασης δεδομένων. Η διοίκηση επιχειρήσεων δίνει έμφαση στην ανάπτυξη μοντέλων λήψης αποφάσεων και στις πρακτικές του μάνατζμεντ. Η επιχειρησιακή έρευνα εστιάζει στις μαθηματικές τεχνικές για τη βελτιστοποίηση επιλεγμένων παραμέτρων των οργανισμών, όπως είναι οι μεταφορές, ο έλεγχος αποθεμάτων, και το κόστος συναλλαγών.

1.5.2. Συμπεριφορική Προσέγγιση

Ένα σημαντικό μέρος του πεδίου των πληροφοριακών συστημάτων αφορά συμπεριφορικά ζητήματα που ανακύπτουν κατά την ανάπτυξη και τη συντήρηση σε βάθος χρόνου των πληροφοριακών συστημάτων. Θέματα όπως η στρατηγική ολοκλήρωση της επιχείρησης, ο σχεδιασμός, η εφαρμογή, η αξιοποίηση, και η διοίκηση δεν μπορούν να διερευνηθούν επαρκώς με τα μοντέλα της τεχνικής προσέγγισης. Άλλοι συμπεριφορικοί γνωστικοί κλάδοι όπως η ψυχολογία και η κοινωνιολογία, συμβάλουν σε σημαντικό βαθμό με τις δικές τους έννοιες και μεθόδους. Η συμπεριφορική προσέγγιση επικεντρώνει το ενδιαφέρον της σε αλλαγές στις στάσεις, στις πολιτικές διοίκησης και οργάνωσης, και στη συμπεριφορά.

Κεφάλαιο 2

Διοίκηση Ολικής Ποιότητος και Συστήματα Διοίκησης Ποιότητος

2.1. Εισαγωγή

Τα τελευταία χρόνια στην Ελλάδα όπως και στην Ευρωπαϊκή Ένωση γίνονται προσπάθειες αναβάθμισης των Υπηρεσιών του Δημόσιου τομέα με στόχο την ενίσχυση της αποτελεσματικότητας και της παραγωγικότητάς τους. Αναμφίβολα η υιοθέτηση και εφαρμογή Μοντέλων Διοίκησης Ολικής Ποιότητας στην Ελληνική Δημόσια Διοίκηση (CAF[3], EFQM[4], ISO 9000), ακολουθώντας τις σχετικές συστάσεις της Ευρωπαϊκής Ένωσης, δίνει τη δυνατότητα να προχωρήσουν σε ακόμη μεγαλύτερο βάθος οι απαραίτητες μεταβολές, ώστε να δημιουργηθεί μια συνεχής και συνεπής ροή υψηλής ποιότητας και αξιοπιστίας των υπηρεσιών.

Η Διοίκηση Ολικής Ποιότητας αποτελεί ένα ολοκληρωμένο σύστημα διοίκησης της ποιότητας σε όλους τους τομείς - λειτουργίες - δραστηριότητες της επιχείρησης – οργανισμού. Βασικό στοιχείο της λογικής της Διοίκησης της Ολικής Ποιότητας είναι ότι η ποιότητα του τελικού προϊόντος ή υπηρεσίας και η εξυπηρέτηση των πελατών δεν μπορεί να υπάρξει, αν δεν υπάρχει ποιότητα σε όλα τα προηγούμενα στάδια των επιχειρησιακών διεργασιών-λειτουργιών.

Στο κεφάλαιο αυτό θα προσεγγίσουμε τη Διοίκηση Ολικής Ποιότητας γιατί στο προτεινόμενο μοντέλο ασφάλειας Πληροφοριακών Συστημάτων έχουν υιοθετηθεί οι αρχές της.

Έτσι αρχικά γίνεται μια εννοιολογική ανάλυση της Διοίκησης Ολικής Ποιότητας, του Συστήματος Διοίκησης ή Διαχείρισης Ποιότητας και αναφορά στις αρχές Ολικής Ποιότητας. Ακολουθούν οι προϋποθέσεις και οι ενέργειες εισαγωγής Διοίκησης Ολικής Ποιότητας, και η απαρίθμηση των διάφορων μοντέλων και εργαλείων της

---

[3]Το CAF ή ΚΠΑ είναι ένα εύκολο στη χρήση του εργαλείο, ώστε να βοηθηθούν οι οργανώσεις του δημοσίου τομέα σε όλη την Ευρώπη να χρησιμοποιήσουν τεχνικές Διοίκησης Ολικής Ποιότητας και να βελτιώσουν την απόδοσή τους. Παρέχει ένα πλαίσιο αυτό-αξιολόγησης που είναι εννοιολογικά παρόμοιο με τα κύρια μοντέλα Διοίκησης Ολικής Ποιότητας, ιδιαιτέρως με το EFQM, αλλά έχει διαμορφωθεί ειδικά για τις οργανώσεις του δημοσίου τομέα, λαμβάνοντας υπόψη τις διαφορές τους. http://www.eipa.eu

[4]Ευρωπαϊκό Ίδρυμα για τη Διοίκηση Ολικής Ποιότητας: Το μοντέλο του EFQM χρησιμοποιείται ως κοινή βάση αξιολόγησης των ευρωπαϊκών επιχειρήσεων για την απονομή βραβείου ποιότητας, αλλά και ως μοντέλο για την αυτό-αξιολόγηση των οργανισμών με στόχο την επίτευξη συνεχούς βελτίωσης. http://www.efqm.org

ΔΟΠ. Επιχειρείται μια προσέγγιση για την εφαρμογή της ΔΟΠ στο δημόσιο τομέα και στη συνέχεια η παράθεση των αναγκαίων Αρχών της ΔΟΠ.

Τέλος αφού γίνει αναφορά στον κύκλο βελτίωσης ποιότητας PDCA ο οποίος χρησιμοποιείται στο προτεινόμενο μοντέλο της εργασίας, το κεφάλαιο κλείνει με μια συνοπτική παρουσίαση του ΚΑΠ (CAF) και του ISO 9000 δεδομένου του ότι, το προτεινόμενο μοντέλο ασφάλειας Πληροφοριακών Συστημάτων προβλέπει πριν την εφαρμογή του, να έχει προηγηθεί η εισαγωγή στον οργανισμό ενός μοντέλου διοίκησης στο οποίο έχουν εφαρμοστεί οι αρχές της ΔΟΠ.

2.2. Διοίκηση Ολικής Ποιότητας

Βάσει ενός ορισμού που δόθηκε το 1992 από μία ομάδα εξειδικευμένων στελεχών: «ΔΟΠ είναι ένα ανθρωποκεντρικό σύστημα διοίκησης που στοχεύει στην συνεχή αύξηση της ικανοποίησης των πελατών με συνεχώς χαμηλότερο κόστος. Η ΔΟΠ είναι μία ολική συστημική προσέγγιση και ένα αναπόσπαστο τμήμα της στρατηγικής σε υψηλό επίπεδο λειτουργεί οριζόντια διαλειτουργικά και διατμηματικά, εμπλέκει όλους τους εργαζόμενους, από το υψηλότερο έως το χαμηλότερο επίπεδο, και εκτείνεται προς τα πίσω και προς τα μπροστά προκειμένου να περιλάβει ολόκληρη την αλυσίδα των προμηθευτών και των πελατών. Η ΔΟΠ τονίζει την ανάγκη για μάθηση και προσαρμογή στη συνεχή αλλαγή ως καθοριστικό παράγοντα της επιτυχίας της οργάνωσης. Η ΔΟΠ περιλαμβάνει συστήματα, μεθόδους και εργαλεία. Τα συστήματα επιτρέπουν την αλλαγή, ενώ η φιλοσοφία παραμένει η ίδια. Η ΔΟΠ εδράζεται σε αξίες που τονίζουν της σημασία της αξίας του ατόμου καθώς και την δύναμη της συλλογικής δράσης». (Evans Lindsay, 1999:118)

2.3. Σύστημα Διοίκησης ή Διαχείρισης Ποιότητας

Η έννοια της Διοίκησης ή Διαχείρισης Ποιότητας (Quality Management) περιλαμβάνει ένα σύνολο οργανωτικών δραστηριοτήτων στα πλαίσια λειτουργίας ενός οργανισμού όπως είναι μια επιχείρηση, μια δημόσια υπηρεσία, μια μονάδα υγείας, κλπ. Πρακτικά, η εισαγωγή των οργανωτικών αυτών δραστηριοτήτων έχει ως απώτερο στόχο να εξασφαλίσει ότι τα προϊόντα και/ή οι υπηρεσίες που προσφέρονται από τον φορέα, θα πληρούν όλες τις υφιστάμενες σχετικές προδιαγραφές ποιότητας,

σε συνεχή βάση και με αξιοπιστία[5]. Το αποτέλεσμα της εισαγωγής των παραπάνω οργανωτικών δραστηριοτήτων στα πλαίσια της λειτουργίας του φορέα είναι η δημιουργία ενός (συνήθως πολύπλοκου) οργανωτικού μηχανισμού που καλύπτει ένα σύνολο επιχειρησιακών διεργασιών και ονομάζεται Σύστημα Διοίκησης Ποιότητας ή Σύστημα Διαχείρισης Ποιότητας (Quality Management System).

Ένα Σύστημα Διοίκησης Ποιότητας μπορεί να ορισθεί ως εξής: Το σύνολο των τυποποιημένων διεργασιών και των χρησιμοποιούμενων πόρων (οργάνωση, ανθρώπινοι πόροι, υποδομές και εξοπλισμός) για την επίτευξη των τιθέμενων στόχων ποιότητας .

Η έννοια της διεργασίας προσδιορίζεται ως εξής: Διεργασία (Process) είναι μια δραστηριότητα που μετασχηματίζει εισερχόμενα δεδομένα (inputs) σε εξερχόμενα αποτελέσματα (outputs). Οι διεργασίες περιλαμβάνουν επιμέρους Διαδικασίες (Procedures) οι οποίες ελέγχουν τις διάφορες λειτουργίες του οργανισμού.

Ο γενικός στόχος του Συστήματος Διοίκησης Ποιότητας είναι η τήρηση και η βελτίωση των προδιαγραφών (χαρακτηριστικών) των προϊόντων ή υπηρεσιών που προσφέρει ο οργανισμός έτσι ώστε να καλύπτονται οι συνεχώς μεταβαλλόμενες απαιτήσεις των πελατών. Ο όρος "πελάτης" χρησιμοποιείται εδώ με την γενική έννοια του χρήστη των προϊόντων ή των υπηρεσιών που προσφέρει ο οργανισμός (δηλαδή ο πελάτης στην περίπτωση μιας επιχείρησης, ο ασθενής στην περίπτωση της μονάδας υγείας, ο πολίτης στην περίπτωση μιας δημόσιας υπηρεσίας, κλπ).

Η Ποιότητα (Quality) ενός προϊόντος ή μιας υπηρεσίας ορίζεται ως το σύνολο των χαρακτηριστικών που καθορίζουν την δυνατότητα του προϊόντος ή της υπηρεσίας να ικανοποιήσει ρητές ή εννοούμενες ανάγκες.

Η τήρηση και βελτίωση των προδιαγραφών του προϊόντος ή της υπηρεσίας σημαίνει ότι θα πρέπει να υλοποιούνται τα εξής:

- Καθορισμός και τήρηση ενός προδιαγεγραμμένου (standard) τρόπου λειτουργίας του οργανισμού
- Έχουν τεθεί στόχοι βελτίωσης λειτουργίας του οργανισμού σύμφωνα με τις απαιτήσεις των χρηστών (πχ της αγοράς στην περίπτωση μιας επιχείρησης), ή στόχοι βελτίωσης που τίθενται από εσωτερικές ανάγκες βελτίωσης της λειτουργίας του οργανισμού.

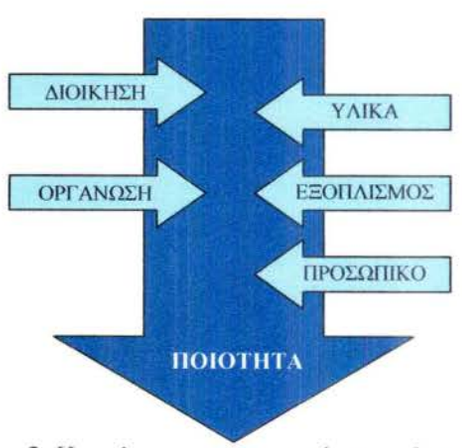
---

[5]Ψηφιακό Κέντρο Έρευνας http://www.vrc.gr

Η Διοίκηση Ποιότητας δεν θα πρέπει να συγχέεται με τις ενέργειες που αφορούν τον έλεγχο της ποιότητας ενός συγκεκριμένου προϊόντος ή μιας υπηρεσίας. Δηλαδή Διοίκηση Ποιότητας δεν σημαίνει ποιοτικός έλεγχος ενός προϊόντος ούτε αφορά την ποιότητα κατασκευής πχ ενός αυτοκινήτου. Η Διοίκηση Ποιότητας είναι πολύ ευρύτερη σαν έννοια και αφορά τον τρόπο οργάνωσης και λειτουργίας της όλης επιχείρησης. Παραδείγματος χάριν, στην περίπτωση που μια επιχείρηση είναι πιστοποιημένη κατά ISO, αυτό σημαίνει ότι είναι πιστοποιημένη η ποιότητα της συνολικής λειτουργίας της επιχείρησης και όχι η ποιότητα των προϊόντων ή των υπηρεσιών που αυτή παρέχει προς τους πελάτες.

Η θέσπιση προδιαγραφών ποιότητας για το τελικό προϊόν ή την υπηρεσία απαιτεί τον καθορισμό όλων των εμπλεκόμενων ενεργειών και των πόρων που χρησιμοποιούνται για την υλοποίηση του προϊόντος. Δηλαδή απαιτεί την κατάρτιση προδιαγραφών για όλα τα στάδια ανάπτυξης του προϊόντος ή της υπηρεσίας. Κατά την έννοια αυτή η ποιότητα ενσωματώνεται στο προϊόν ή την υπηρεσία σταδιακά και σε όλα τα στάδια ανάπτυξης ή παραγωγής. Άρα όλες οι λειτουργίες της επιχείρησης μπορούν να επηρεάσουν την ποιότητα του τελικού προϊόντος ή της υπηρεσίας και ακριβώς γι' αυτόν τον λόγο αυτό απαιτείται η κατάρτιση προδιαγραφών για όλα τα στάδια ανάπτυξης.

Τα παραπάνω αναπαρίστανται γραφικά στο επόμενο σχήμα όπου η Ποιότητα εμφανίζεται ως η συνισταμένη πολλών επιμέρους στοιχείων της λειτουργίας της επιχείρησης και των πόρων που χρησιμοποιούνται για την παραγωγή του προϊόντος ή της υπηρεσίας.



Σχήμα 3: Η ποιότητα ως συνισταμένη επιμέρους στοιχείων
πηγή: Ψηφιακό κέντρο έρευνας

Μια από τις λανθασμένες απόψεις που ίσχυαν παλαιότερα ήταν ότι η ποιότητα είναι κάτι μη μετρήσιμο ή απροσδιόριστο. Σήμερα, σαν αποτέλεσμα των εξελίξεων και της διάδοσης των Αρχών Διοίκησης Ολικής Ποιότητας, είναι πλέον αποδεκτό, ότι η ποιότητα της λειτουργίας ενός φορέα είναι μετρήσιμη και βελτιώσιμη. Η ποιότητα μπορεί να αναλυθεί σε επιμέρους χαρακτηριστικά τα οποία λειτουργούν σαν συνιστώσες και τα οποία ο φορέας μπορεί με συστηματικό και μεθοδικό τρόπο να παρακολουθήσει και να βελτιώσει.

Αυτός είναι και ο λόγος για τον οποίο θα πρέπει να τίθενται στόχοι βελτίωσης της λειτουργίας του φορέα σύμφωνα με τις απαιτήσεις των χρηστών, όπως έχει αναφερθεί.

2.4. Βασικές αρχές της ολικής ποιότητας

Οι βασικές αρχές της ολικής ποιότητας είναι: (Κέφης 2005:42)

- ✓ η δέσμευση της ηγεσίας
- ✓ η έννοια του εσωτερικού και εξωτερικού πελάτη
- ✓ η ικανοποίηση του καταναλωτή
- ✓ η φιλοσοφία των μηδέν λαθών
- ✓ η συνεχής εκπαίδευση
- ✓ η συνεχής βελτίωση.

Η δέσμευση και η συμμετοχή των στελεχών εξαρτάται από τη Γενική Διεύθυνση που δημιουργεί και συντηρεί τα οράματα, θέτει τους στόχους, παρακινεί και επιβραβεύει.

Πελάτης δεν είναι μόνο ο αποδέκτης και χρήστης του τελικού αγαθού ή υπηρεσίας (εξωτερικός πελάτης). Είναι ο οποιοσδήποτε, στον οποίο ένα άτομο παρέχει πληροφορίες, υπηρεσίες ή τα μέσα για να συνεχίσει τη δική του εργασία μέσα στο εσωτερικό περιβάλλον της επιχειρηματικής μονάδας (εσωτερικός πελάτης).

Θεμελιώδης αρχή της Ολικής Ποιότητας είναι η *ικανοποίηση του πελάτη.* Αποτελεί την κινητήρια δύναμη για να πραγματοποιηθεί η μεγάλη αλλαγή στον οργανισμό, στα συστήματα, στις διαδικασίες, στον εξοπλισμό, στα μέσα, στα προϊόντα.

Η φιλοσοφία των μηδέν λαθών προϋποθέτει ότι το ανθρώπινο δυναμικό του οργανισμού είναι άριστα εκπαιδευμένο ώστε να εντοπίζει τα διαφαινόμενα προβλήματα και να προβαίνει στην άμεση επίλυση τους.

Η *εκπαίδευση* είναι το βασικότερο όπλο για την αλλαγή νοοτροπίας στην επιχείρηση

ή στον οργανισμό. Τα εκπαιδευτικά προγράμματα μπορούν να λάβουν χώρα κατά τη διάρκεια του χρόνου εργασίας (on the job training methods) ή εκτός του χρόνου εργασίας (off the job training methods).

Το μάνατζμεντ έχει εστιάσει την προσοχή του σε καινοτομικά *επιτεύγματα* (νέες εφευρέσεις, τεχνολογία, αυτοματισμό). Η ΔΟΠ εστιάζει στην ανεύρεση κερδοφόρων βελτιώσεων εφαρμόζοντας τον κύκλο P - D - C - A (Plan - Do - Check - Act/Σχεδίασε - Εφάρμοσε - Έλεγξε - Ενήργησε) σε κάθε διαδικασία που χρησιμοποιείται για την παραγωγή αγαθών και την παροχή υπηρεσιών (Σχήμα 4).

Ένας οργανισμός πρέπει να διαθέτει *όραμα* (vision). Το όραμα είναι η περιγραφή των ιδανικών και των επιδιώξεων του. Η διατύπωση και η διάδοση του οράματος προς τα στελέχη είναι καθήκον της γενικής διεύθυνσης. Οι ειδικότεροι στόχοι όπως και οι δραστηριότητες για επίτευξη των στόχων διατυπώνονται και συντονίζονται με βάση το όραμα.

Ο λόγος ύπαρξης του οργανισμού ονομάζεται *αποστολή* (mission). Το όραμα και η αποστολή του οργανισμού θέτουν γενικούς στόχους, γι' αυτό χρειάζονται την ύπαρξη *πολιτικής* (politics), που δεικνύει τον τρόπο επίτευξης τους.

2.5. Σύστημα Διοίκησης Ολικής Ποιότητας

Ως σύστημα η Διοίκηση Ολικής Ποιότητας (Δ. Μπουραντάς, 2003:515) αποτελείται από:

- ένα συνολικό πλαίσιο στρατηγικών και πολιτικών που αφορούν την ποιότητα και τις σχέσεις της με τις γενικές στρατηγικές, το όραμα, την αποστολή και τους επιχειρησιακούς στόχους
- συστήματα, διαδικασίες, μεθόδους, τεχνικές και εργαλεία που αφορούν το σχεδιασμό και τη διασφάλιση της ποιότητας παντού (π.χ. ISO, συστήματα πρόληψης λαθών κ.λπ.)
- μια οργανωσιακή κουλτούρα η οποία δίνει έμφαση σε αξίες, πιστεύω και σημασίες που συνδέονται άμεσα με την εξασφάλιση της ποιότητας
- ικανότητες των εργαζομένων να επιτυγχάνουν ποιότητα παντού.

Προκειμένου να επιτευχθεί η μετάβαση από την παραδοσιακή προσέγγιση στη ΔΟΠ απαιτείται επιπλέον η αλλαγή της οργανωσιακής κουλτούρας του οργανισμού, δηλαδή πρέπει να γίνουν τροποποιήσεις στην οργανωσιακή δομή, στο σύστημα

διοίκησης ανθρωπινού δυναμικού, στο σύστημα ελέγχου και διάχυσης της πληροφορίας καθώς και στο στυλ διοίκησης σε όλα τα επίπεδα του οργανισμού, πάντα με την υποστήριξη της ανώτερης ηγεσίας. (Kim et. al., 1995:679)

2.6. Εφαρμογή της διοίκησης ολικής ποιότητας

Η εισαγωγή της Διοίκησης Ολικής Ποιότητας στην Επιχείρηση - Οργανισμό ασφαλώς δεν είναι εύκολη υπόθεση σύμφωνα με τα όσα έχουν προηγηθεί. Καταρχήν πρέπει να υπάρξουν οι κατάλληλες προϋποθέσεις (Μπουραντάς, 2002:516) όπως:

- ✓ η πίστη, η δέσμευση και η συνεχής υποστήριξη από την Ανωτάτη Διοίκηση
- ✓ η μακροπρόθεσμη προσέγγιση με την έννοια ότι η ποιότητα ως κουλτούρα και ικανότητες απαιτεί αρκετό χρόνο για να εδραιωθεί
- ✓ σύνδεση της Διοίκησης της Ολικής Ποιότητας με το όραμα, τις επιχειρησιακές στρατηγικές και τους επιχειρησιακούς στόχους
- ✓ σωστός σχεδιασμός των ενεργειών, των υπευθυνοτήτων, των μέσων και του χρονοπρογράμματος που απαιτούνται για την εφαρμογή της Διοίκησης Ολικής Ποιότητας.

Οι βασικές ενέργειες που απαιτούνται για την εισαγωγή της Διοίκησης της Ολικής Ποιότητας αφορούν τους παρακάτω τομείς: (Μπουραντάς, 2002:516)

- ✓ διαμόρφωση στρατηγικής και σχεδίων εισαγωγής της Διοίκησης Ολικής Ποιότητας
- ✓ διαμόρφωση και εφαρμογή των διαδικασιών, των δομών και της τεχνολογίας που εξασφαλίζουν την επιθυμητή ποιότητα
- ✓ προσαρμογή των συστημάτων αμοιβών και αξιολόγησης της απόδοσης των εργαζομένων στις απαιτήσεις της «ποιότητας»
- ✓ επικοινωνία και συμβολικές πράξεις της Ανώτατης Διοίκησης για τη διαμόρφωση της κατάλληλης κουλτούρας
- ✓ εκπαίδευση των μάνατζερ και των εργαζομένων για την απόκτηση ικανοτήτων και κατάλληλης κουλτούρας
- ✓ εφαρμογή συστήματος παρακολούθησης της εφαρμογής της Διοίκησης Ολικής Ποιότητας και μέτρησης των αποτελεσμάτων της.

2.7. Μοντέλα τεχνικές εργαλεία Διοίκησης Ολικής Ποιότητας

Για την ανάπτυξη και εφαρμογή της Διοίκησης Ολικής Ποιότητας έχουν αναπτυχθεί διάφορες μέθοδοι, τεχνικές και συστήματα όπως:

- Συστήματα Διοίκησης Ποιότητας (ISO)
- Συγκριτική Πρωτοτυποποίηση (Benchmarking)
- Εξισορροπημένη Κάρτα (Balance Scorecard)
- Ανασχεδιασμός Επιχειρησιακών Διαδικασιών (Business Process Reengineering – BPR) Λειτουργική Ανάπτυξη Ποιότητας (Quality Function Deployment – QFD) ή "Σπίτι της Ποιότητας"
- Εξωτερίκευση Διαδικασιών (Outsourcing),

αλλά και υποστηρικτικές τεχνικές και εργαλεία όπως:

- Διάγραμμα Αιτίας - Αποτελέσματος (Cause - Effect Diagram)
- Μοντέλο Μελέτης των Αποτυχιών - Λαθών και Ανάλυση Αποτελεσμάτων (Failure Mode and Effect Analysis)
- Ανάλυση Pareto (Pareto Analysis)
- Διάγραμμα Ροής (Flow Chart) κλπ.

Σημείωση: Ορισμένα από αυτά αναπτύχθηκαν στα πλαίσια εφαρμογής άλλων προσεγγίσεων του μάνατζμεντ.

Επίσης έχουν αναπτυχθεί και προωθητικά βραβεία ποιότητας όπως:

- Μοντέλο Επιχειρηματικής Αριστείας, (EFQM[6])
- το Κοινό πλαίσιο Αξιολόγησης (CAF[7])
- και το Εθνικό Βραβείο Ποιότητας Δημοσίων Υπηρεσιών.

Σημείωση: Τα βραβεία αποτελούν επίσης και μοντέλα Διοίκησης Ολικής Ποιότητας και δίνεται έμφαση στην υιοθέτησή τους, καθώς υποστηρίζονται από την Ευρωπαϊκή Επιτροπή και έχουν υιοθετηθεί και προωθούνται από το επιχειρησιακό πρόγραμμα «Πολιτεία».

---

[6] http://www.efqm.org
[7] http://www.eipa.eu

2.8. Διοίκηση Ολικής Ποιότητας και Δημόσιος Τομέας

Η χρήση των μεθόδων που προαναφέρθηκαν στον τομέα των υπηρεσιών, παρουσιάζει ορισμένες ιδιαιτερότητες και σε κάθε περίπτωση διαφοροποιείται σημαντικά η εφαρμογή της φιλοσοφίας και των εργαλείων της ΔΟΠ στον τομέα αυτό σε σχέση με τον τομέα παραγωγής προϊόντων. Τι εννοούμε όμως με τον όρο «υπηρεσία». Ως υπηρεσία ορίζεται «μία κοινωνική πράξη που συντελείται μέσω της επαφής του πελάτη και του εκπροσώπου του οργανισμού που παρέχει την υπηρεσία». (Evans, Lindsay, 1999:49) Η βασική διαφορά είναι ότι η παραγόμενη υπηρεσία, σε αντίθεση με τα προϊόντα, είναι άυλη. Αυτό σημαίνει ότι ενώ στα προϊόντα υπάρχουν μετρήσιμες παράμετροι με βάση κάποιες προδιαγραφές που τίθενται κάθε φορά, η ποιότητα των υπηρεσιών μπορεί να αξιολογηθεί μόνο βάσει των προσδοκιών του πελάτη, οι οποίες είναι υποκειμενικές και αρκετά συχνά συγκεχυμένες. Έτσι, ενώ στην παραγωγή προϊόντων η χρήση των τεχνικών της ΔΟΠ διαδίδεται ταχύτατα από το 1950 και μετά, στον τομέα των υπηρεσιών αρχίζει να υπάρχει κάποιο ενδιαφέρον από το 1980 (Redman, et.al.,1995:21), ενώ στον τομέα των δημοσίων υπηρεσιών η εξέλιξη αυτή καθυστερεί ακόμη περισσότερο.

Το 1985 γίνονται οι πρώτες προσπάθειες από δημόσιους φορείς του δημοσίου στις ΗΠΑ για την εφαρμογή των αρχών της ΔΟΠ. Το 1990 το Ομοσπονδιακό Ινστιτούτο Ποιότητας δίνει τον εξής ορισμό για τη ΔΟΠ στο δημόσιο τομέα: *«Μία ολική οργανωσιακή προσέγγιση για την ικανοποίηση των αναγκών και των προσδοκιών των πελατών που εμπλέκει όλους τους προϊσταμένους και υπαλλήλους στην χρήση ποσοτικών μεθόδων προκειμένου να επιτευχθεί συνεχής βελτίωση των διαδικασιών, των προϊόντων και των υπηρεσιών του οργανισμού».* (Harrison, Stupak, 1993:418)

Έκτοτε πολλές χώρες επιχειρούν και επιτυγχάνουν σε μικρότερο ή μεγαλύτερο βαθμό την εισαγωγή των αρχών της Διοίκησης Ολικής Ποιότητας στις δημόσιες υπηρεσίες. Οι λόγοι που σταδιακά οδήγησαν προς την κατεύθυνση αυτή ήταν η γενικευμένη διαμαρτυρία για τις συνεχείς αυξήσεις των φόρων, τον υψηλό πληθωρισμό, την έλλειψη ικανοποίησης από την ποιότητα των δημοσίων υπηρεσιών και την οικονομική κακοδιαχείρηση του δημοσίου χρήματος.

Παράλληλα δημιουργήθηκε η ανάγκη για την υιοθέτηση μίας κουλτούρας προσανατολισμένης προς τις πρακτικές του ιδιωτικού τομέα και την εφαρμογή κατάλληλων μέτρων, ώστε να επιτευχθεί η αποτελεσματικότητα η αποδοτικότητα, και η οικονομία (effectiveness, efficiency, economy).

Η ευρωπαϊκή συζήτηση για την ποιότητα στις δημόσιες υπηρεσίες ανάγεται σε μία περίοδο πριν την αλλαγή της χιλιετίας, καθώς ορισμένες ευρωπαϊκές κυβερνήσεις άρχισαν να εφαρμόζουν σειρά μεταρρυθμίσεων στις αρχές της δεκαετίας του 1980 ώστε να εστιαστεί ο δημόσιος τομέας της χώρας τους σε θέματα επιδόσεων, να προσανατολιστεί προς τον πελάτη και να ανταποκρίνεται στον πολίτη. Η έννοια της ποιότητας στην προσπάθεια αυτή ήταν συστατικό στοιχείο, αν και όχι πάντα ξεκάθαρο. Οι περιπτώσεις των «καλύτερων διοικητικών πρακτικών» που παρουσιάστηκαν στο 3ο Συνέδριο Ποιότητας στο Ρόττερνταμ της Ολλανδίας αποδεικνύουν ότι τα παρακάτω μεταρρυθμιστικά προγράμματα εστιάζονται στα κάτωθι:

1. *Προσανατολισμός στις επιδόσεις και τα αποτελέσματα* (π.χ. μέσω συστημάτων δεικτών επιδόσεων, προϋπολογισμών που συνδέονται με την επίδοση, την οικονομικότερη διαχείριση μέσων, τον έλεγχο των λειτουργιών, κτλ) σημαίνει ότι τα διοικητικά στελέχη του δημοσίου τομέα έπρεπε να βρουν καινούρια εργαλεία για να πετύχουν καλύτερα αποτελέσματα μέσα στα όρια των υφισταμένων – συνήθως μειωμένων- προϋπολογισμών.

2. *Βελτίωση του προσανατολισμού προς τον πελάτη / ελάφρυνση της γραφειοκρατίας* (π.χ., μέσω της εκπαίδευσης στην καλύτερη γνώση των αναγκών του πελάτη, των χαρτών δικαιωμάτων των πολιτών, της απλούστευσης των τύπων και των διαδικασιών) σήμαινε ότι οι δημόσιες υπηρεσίες έπρεπε να αντιμετωπίσουν τις αυξανόμενες προσδοκίες των πολιτών. Ωστόσο, εκείνοι που λαμβάνουν τις αποφάσεις στο δημόσιο τομέα, σε αντίθεση με τον ιδιωτικό, πρέπει να είναι σίγουροι ότι διατηρείται η ισορροπία μεταξύ του γενικού δημοσίου συμφέροντος και των ειδικών αναγκών των συγκεκριμένων ομάδων πολιτών. Για το λόγο αυτό, στο δημόσιο τομέα ο «πελάτης» δεν θα γίνει ποτέ ο απόλυτος «βασιλιάς». (Gaster, Squires, 2003:3)

3. *Επίτευξη των ολοκληρωμένων υπηρεσιών,* έτσι ώστε οι πολίτες να μην χρειάζεται να πηγαίνουν σε πολλές διαφορετικές υπηρεσίες για να βρουν τη λύση σε ένα πρόβλημά τους (π.χ., υπηρεσίες μίας στάσης), προσπάθειες ενσωμάτωσης κοινωνικής και υγειονομικής μέριμνας, συνεργασία ιδιωτικού και δημοσίου τομέα.

Για να μπορέσουν να προσαρμοστούν στις νέες απαιτήσεις των σύγχρονων αυτών εκσυγχρονιστικών προγραμμάτων, οι οργανώσεις δημοσίων υπηρεσιών πρέπει να αναπτύξουν νέες ικανότητες και διαδικασίες, οι οποίες με τη σειρά τους συνεπάγονται: (3ο Συνέδριο Ποιότητας)

1. Βελτίωση της ποιότητας του προσωπικού της δημόσιας υπηρεσίας (π.χ., μέσω της ανάπτυξης και της εκπαίδευσης). Είναι αδύνατο να βελτιωθεί ο προσανατολισμός προς τον πελάτη, να εισαχθούν νέα πληροφοριακά και επικοινωνιακά συστήματα ή να εφαρμοσθούν εργαλεία όπως το CAF, το ISO ή το EFQM, χωρίς σημαντική επένδυση στην εκπαίδευση του προσωπικού.

2. Υιοθέτηση εργαλείων ποιότητας που αναπτύχθηκαν για χρήση στον ιδιωτικό τομέα ώστε να γίνουν συμβατά στο δημόσιο (υπάρχουν πολλά στάδια εξέλιξης εδώ, συμπεριλαμβανομένων εκείνων που προέρχονται από τη Διοίκηση Ολικής Ποιότητας, τον Ευρωπαϊκό Οργανισμό για τη Διοίκηση Ποιότητας (EFQM), το Κοινό Πλαίσιο Αξιολόγησης (CAF) και την εξισορροπημένη βαθμολογία (Balanced Scorecard).

3. Μέτρηση της ανάγκης βελτίωσης της ποιότητας, αλλά και των συνεπειών της, μέσω διαφόρων συστημάτων μέτρησης της ικανοποίησης των πολιτών. Οι δημόσιες υπηρεσίες παρουσιάζουν κάποιες ιδιαιτερότητες ως προς την εφαρμογή της ΔΟΠ, με την πιο βασική ότι δεν έχουν σαν στόχο το κέρδος όπως συμβαίνει με τις ιδιωτικές επιχειρήσεις. Από την άλλη οι δημόσιοι οργανισμοί συνήθως δεν έχουν καθορισμένες διαδικασίες και εξαρτώνται κυρίως από τον ανθρώπινο παράγοντα. Αυτό έχει σαν αποτέλεσμα κάθε περίπτωση να αντιμετωπίζεται ως μοναδική με αποτέλεσμα την αύξηση του κόστους. Μία ακόμα ιδιαιτερότητα που αποτελεί μία πρόσθετη δυσκολία στην προσπάθεια εφαρμογής της ΔΟΠ στον Δημόσιο τομέα είναι ότι ο ορισμός του πελάτη στις δημόσιες υπηρεσίες είναι περίπλοκος. Και αυτό γιατί υπάρχει διαχωρισμός μεταξύ του χρήστη της δημόσιας υπηρεσίας και των επωφελούμενων από αυτή. Αυτό σημαίνει ότι υπό ορισμένες συνθήκες η ικανοποίηση του χρήστη δεν συνεπάγεται και ικανοποίηση των συνολικών κοινωνικών αναγκών και ότι οι δημόσιοι οργανισμοί μπορεί να ενδιαφέρονται αποκλειστικά για τις ατομικές ανάγκες των χρηστών των υπηρεσιών τους, αλλά παράλληλα και για τις ανάγκες τις κοινωνίας συνολικά.

Επίσης, όσον αφορά στο ανθρώπινο δυναμικό των δημοσίων υπηρεσιών και ειδικότερα στη χώρα μας πρέπει να ληφθεί υπ' όψιν ότι η εξέλιξη των δημοσίων υπαλλήλων καθορίζεται σύμφωνα με τον Υπαλληλικό Κώδικα, δηλ. από ένα νομοθετικό κείμενο, στο οποίο εμπίπτει το σύνολο των υπαλλήλων όλων των υπηρεσιών του στενού δημόσιου τομέα τουλάχιστον. Η εισαγωγή δε των χρηματικών κινήτρων για την καλή απόδοση ή ως επιβράβευση των υπαλλήλων μπορεί να

εφαρμοσθεί με μεγάλη δυσκολία[8]. Η ποιότητα ωστόσο των υπηρεσιών βασίζεται κυρίως στον ανθρώπινο παράγοντα και έτσι η ύπαρξη κινήτρων στο δημόσιο για καλή απόδοση είναι απαραίτητη. Αυτό σημαίνει ότι πρέπει να βρεθούν τρόποι και μηχανισμοί ενδυνάμωσης του ανθρώπινου παράγοντα στον ελληνικό δημόσιο τομέα προκειμένου να εφαρμοσθεί η Διοίκηση Ολικής Ποιότητας, ενώ παράλληλα θα πρέπει να ενισχύεται στους υπαλλήλους το πνεύμα της κοινωνικής προσφοράς και του δημοσίου καθήκοντος.

Τέλος, όσον αφορά στο ρόλο της ηγεσίας, της οποίας η υποστήριξη είναι πρώτιστης σημασίας προκειμένου να υιοθετηθεί η φιλοσοφία της ΔΟΠ από έναν οργανισμό, στο δημόσιο τομέα παρουσιάζεται το πρόβλημα της ασυνέχειας της διοίκησης. Υπάρχει ωστόσο, και η άποψη ότι μπορούμε να έχουμε εφαρμογή τέτοιων μεθόδων στην Δημόσια Διοίκηση ανεξαρτήτως των αλλαγών στο υψηλότερο επίπεδο της ιεραρχίας, όπου και παρουσιάζονται οι συχνότερες αλλαγές, γιατί συνήθως τέτοιου είδους πρωτοβουλίες στον δημόσιο τομέα δεν ξεκινούν από το υψηλότερο επίπεδο της ιεραρχίας, αλλά από πρωτοβουλίες στελεχών μεσαίου ή ανώτερου επιπέδου και στη συνέχεια διαχέονται προς τα πάνω και προς τα κάτω στην ιεραρχική δομή του οργανισμού. (Sensenbrenner, 1995:90)

2.9. Οι Αρχές Διοίκησης Ολικής Ποιότητας

Οι Αρχές Διοίκησης Ολικής Ποιότητας είναι ένα σύνολο κατευθυντήριων αρχών που αφορούν την εφαρμογή Συστημάτων Διοίκησης Ποιότητας. Οι αρχές αυτές δεν προσδιορίζουν έναν διαφορετικό τύπο Διοίκησης Ποιότητας αλλά είναι ένα σύνολο συστάσεων οι οποίες προτείνονται προς ενσωμάτωση στα Συστήματα Διοίκησης Ποιότητας. Δηλαδή στην ουσία δεν υπάρχει η έννοια "Σύστημα Διοίκησης Ολικής Ποιότητας", απλώς ένα Σύστημα Διοίκησης Ποιότητας μπορεί να εφαρμόζει τις Αρχές Διοίκησης Ολικής Ποιότητας.

Η ενσωμάτωση των Αρχών Διοίκησης Ολικής Ποιότητας στα Συστήματα Διοίκησης Ποιότητας οδηγεί σε συνεκτικά και καλώς οργανωμένα συστήματα για την ικανοποίηση εσωτερικών και εξωτερικών πελατών (χρηστών) ή προμηθευτών μέσω της ολοκλήρωσης (ενοποίησης) του επιχειρησιακού περιβάλλοντος και της συνεχούς

[8]Αυτό γιατί στη χώρα μας εφαρμόζεται το ενιαίο μισθολόγιο (Ν. 3230/2002) για όλους τους δημοσίους υπαλλήλους στο οποίο καθορίζονται ρητά τα επιπλέον επιδόματα ή οι χρηματικές αποζημιώσεις.

βελτίωσης μέσω κύκλων ανάπτυξης, βελτίωσης και συντήρησης, ώστε να ανταποκρίνεται στις απαιτήσεις ενός συνεχώς μεταβαλλόμενου περιβάλλοντος. Επίσης η βελτίωση μπορεί να κριθεί αναγκαία όχι από εξωτερικά αίτια (πχ απαιτήσεις πελατών ή απαιτήσεις της αγοράς), αλλά από εσωτερικές ανάγκες βελτίωσης της λειτουργίας του φορέα.

Οι Αρχές Διοίκησης Ολικής Ποιότητας κατά ISO 9004:2000 συνοψίζονται ως εξής:

- ✓ εστίαση στον πελάτη
- ✓ ηγεσία
- ✓ ενεργός συμμετοχή του προσωπικού
- ✓ προσέγγιση βασισμένη σε διεργασίες
- ✓ συστημική προσέγγιση της διοίκησης
- ✓ συνεχής βελτίωση
- ✓ λήψη αποφάσεων βασισμένη σε αντικειμενικά στοιχεία
- ✓ σχέσεις αμοιβαίου οφέλους με τους προμηθευτές.

2.10. Συνεχής Βελτίωση μέσω Κύκλου Βελτίωσης PDCA

Η συνεχής βελτίωση της λειτουργίας του φορέα επιτυγχάνεται μέσω των κύκλων βελτίωσης. Ένας κύκλος βελτίωσης περιλαμβάνει τα εξής στάδια:

1. προσδιορισμός Στόχων Ποιότητας
2. λειτουργία του φορέα
3. μέτρηση στοιχείων που σχετίζονται με την παρακολούθηση των στόχων ποιότητας
4. αξιολόγηση των μετρήσεων

Στην συνέχεια ο κύκλος επαναλαμβάνεται θέτοντας κατ΄ αρχήν νέες τιμές των Στόχων Ποιότητας για τον επόμενο κύκλο.

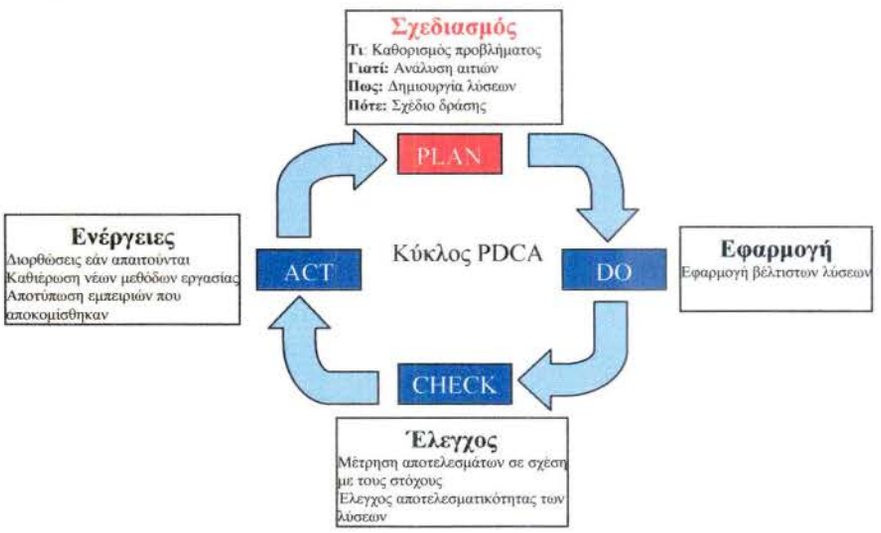
Ένα σημαντικό χαρακτηριστικό των κύκλων βελτίωσης είναι ότι μπορούν να εφαρμοσθούν σε επίπεδο Συστήματος αλλά και σε κατώτερα επίπεδα όπως στο επίπεδο των Διεργασιών ή και στο επίπεδο των επιμέρους Διαδικασιών.

Μια πολύ γνωστή κωδικοποίηση του παραπάνω κύκλου είναι ο λεγόμενος Κύκλος PDCA. Τα στοιχεία PDCA αντιστοιχούν στις αγγλικές λέξεις:

1. **Plan** (αντιστοιχεί στον προσδιορισμό Στόχων Ποιότητας)
2. **Do** (αντιστοιχεί στην λειτουργία του φορέα)

3. **Check** (αντιστοιχεί στην μέτρηση των στοιχείων που σχετίζονται με την παρακολούθηση των Στόχων Ποιότητας) και
4. **Act** (αντιστοιχεί στην αξιολόγηση των μετρήσεων και τον προσδιορισμό νέων τιμών των Στόχων Ποιότητας).

Ο κύκλος PDCA παρουσιάζεται στο σχήμα 4. (Κέφης, 2005:123)



Σχήμα 4: ο κύκλος βελτίωσης PDCA

Ο Κύκλος PDCA μπορεί να εφαρμοσθεί σε επίπεδο Συστήματος αλλά και σε κατώτερα επίπεδα όπως στο επίπεδο των Διεργασιών ή και στο επίπεδο των επιμέρους Διαδικασιών.

Στο επίπεδο Συστήματος η φάση **Act** του Κύκλου PDCA περιλαμβάνει τον προσδιορισμό νέων στόχων. Όταν ο Κύκλος PDCA εφαρμόζεται στα κατώτερα επίπεδα, η φάση **Act** μπορεί να περιλαμβάνει και ευρύτερες διορθωτικές ενέργειες όπως η ανασχεδίαση Διεργασιών ή επιμέρους Διαδικασιών.

Από την παραπάνω περιγραφή προκύπτει ότι ο Κύκλος PDCA και γενικότερα οι κύκλοι βελτίωσης της ποιότητας, αποτελούν κλασικά παραδείγματα συστημάτων με ανάδραση (feedback).

Ο κύκλος PDCA σε επίπεδο Συστήματος, έχει προκαθορισμένη διάρκεια δηλαδή καλύπτει μια σταθερή χρονική περίοδο και οι μετρήσεις των στοιχείων λαμβάνονται στα πλαίσια της χρονικής αυτής περιόδου.

Δεν υπάρχει συγκεκριμένη σύσταση για την ακριβή διάρκεια της χρονικής αυτής περιόδου αλλά στις περισσότερες περιπτώσεις έχει εξάμηνη ή δωδεκάμηνη διάρκεια. Το βασικό ζητούμενο εδώ είναι, να υπάρξει επαρκής χρόνος στα πλαίσια του κύκλου

βελτίωσης, ώστε να λειτουργήσει ο φορέας και να συλλεχθούν επαρκή στοιχεία. Από την άλλη πλευρά η υπερβολική επιμήκυνση της διάρκειας του κύκλου βελτίωσης, μπορεί να οδηγήσει σε καθυστέρηση του απόκρισης του φορέα σε αλλαγές του περιβάλλοντός του, σε απώλεια της ευελιξίας του, σε καθυστέρηση καταγραφής εσωτερικών του προβλημάτων, και άλλες παρόμοιες αρνητικές επιπτώσεις.

Η διάρκεια του κύκλου βελτίωσης καθορίζεται με σαφήνεια στην τεκμηρίωση του Συστήματος Διοίκησης Ποιότητας. Ο φορέας είναι σε θέση να τροποποιεί την διάρκεια του κύκλου βελτίωσης, εφ' όσον υπάρξει τέτοια ανάγκη, μέσω των προβλεπόμενων διαδικασιών τροποποίησης του Συστήματος Διοίκησης Ποιότητας.

2.11. Η σειρά προτύπων ISO 9000[9]

Η σειρά προτύπων ISO 9000 περιλαμβάνει πρότυπα που αφορούν τον σχεδιασμό την ανάπτυξη και την εφαρμογή Συστημάτων Διοίκησης Ποιότητας για οργανισμούς κάθε τύπου και ανεξάρτητα από το είδος του παραγομένου προϊόντος ή των παρεχομένων υπηρεσιών. Τα πρότυπα της σειράς ISO 9000 είναι τα εξής:

- ISO 9000:2000 Quality Management Systems — Fundamentals and Vocabulary (Συστήματα διοίκησης ποιότητας–Βασικές έννοιες και λεξικό όρων).

  Το πρότυπο αυτό ανήκει στην κατηγορία των Κατευθυντήριων Οδηγιών. Εστιάζεται στις βασικές έννοιες και τους ορισμούς της Διοίκησης Ποιότητας. Το πρότυπο αυτό υπερκαλύπτει και αντικαθιστά το προγενέστερο πρότυπο ISO 8402:1994.
- ISO 9001:2000 Quality Management Systems — Requirements (Συστήματα διοίκησης ποιότητας–Απαιτήσεις).

  Το πρότυπο αυτό είναι σήμερα το βασικό πρότυπο Διοίκησης Ποιότητας και περιλαμβάνει τις απαιτήσεις σχετικά με τον σχεδιασμό και εφαρμογή Συστημάτων Διοίκησης Ποιότητας. Το πρότυπο αυτό οριοθετεί νέα δεδομένα στο πεδίο της ολικής ποιότητας καθώς ανοίγει το δρόμο για τη μετατροπή των προτύπων από *Συστήματα Διασφάλισης Ποιότητας* σε *Συστήματα Διοίκησης ή Διαχείρισης της Ποιότητας*. Από όλα τα πρότυπα της σειράς ISO 9000, είναι το μόνο που μπορεί να πιστοποιηθεί.

---

[9] Ψηφιακό Κέντρο Έρευνας

- ISO 9004:2000 Quality Management Systems — Guidelines for Performance Improvements (Συστήματα διοίκησης ποιότητας–Κατευθυντήριες οδηγίες για βελτιώσεις της επίδοσης).

  Το πρότυπο αυτό ανήκει στην κατηγορία των κατευθυντήριων οδηγιών. Περιλαμβάνει οδηγίες και ανάλυση σχετικά με την κάλυψη όλων των απαιτήσεων που θέτει το πρότυπο ISO 9001:2000. Επιπλέον περιλαμβάνει μια σειρά προσεγγίσεων στα θέματα διοίκησης ολικής ποιότητας με έμφαση στην συστημική φύση των μηχανισμών διοίκησης ποιότητας. Το πρότυπο ISO 9004:2000 καλύπτει τα θέματα διοίκησης ποιότητας σε όλη την έκταση της αλυσίδας: Προμηθευτές–Φορέας–Πελάτες. Είναι έντονα εστιασμένο στον στόχο της συνεχούς βελτίωσης της συνολικής επίδοσης και της αποδοτικότητας του φορέα.

Από την προηγηθείσα περιγραφή προκύπτει ότι από τα πρότυπα της σειράς ISO 9000, το βασικό πρότυπο για τον σχεδιασμό και εφαρμογή Συστημάτων Διοίκησης Ποιότητας είναι το πρότυπο ISO 9001:2000, ενώ η πληρέστερη πηγή κατευθυντήριων οδηγιών για την εφαρμογή του ISO 9001:2000, είναι το πρότυπο ISO 9004:2000. Τα δύο αυτά πρότυπα έχουν αναπτυχθεί ώστε να αλληλοσυμπληρώνονται ως ένα συνεκτικό ζεύγος προτύπων για τον σχεδιασμό και την εφαρμογή των Συστημάτων Διοίκησης Ποιότητας. Βέβαια, λόγω της διαφορετικής φύσης τους είναι δυνατόν να χρησιμοποιηθούν και ανεξάρτητα. Είναι σημαντικό να αποσαφηνισθεί ότι το πρότυπο ISO 9001:2000 περιγράφει τις απαιτήσεις που θα πρέπει να πληροί το Σύστημα Διοίκησης Ποιότητας του φορέα, αλλά όχι και τον τρόπο με τον οποίο αυτό θα πραγματοποιηθεί. Επίσης, θα πρέπει να αναφερθεί ότι η πιστοποίηση ενός οργανισμού αφορά την αποδεδειγμένη συμμόρφωσή του με τις απαιτήσεις του προτύπου ISO 9001:2000. Από τα τρία πρότυπα της σειράς ISO 9000, μόνον το ISO 9001:2000 μπορεί να πιστοποιηθεί, επειδή είναι το μόνο που περιλαμβάνει τις απαιτήσεις που θα πρέπει να πληρούνται σχετικά με τον σχεδιασμό και την εφαρμογή ενός Συστήματος Διοίκησης Ποιότητας σε έναν οργανισμό. Δεν υφίσταται πιστοποίηση κατά ISO 9004:2000 επειδή το πρότυπο αυτό περιλαμβάνει κατευθυντήριες οδηγίες και όχι πιστοποιήσιμες απαιτήσεις για το Σύστημα Διοίκησης Ποιότητας του φορέα. Για ανάλογους λόγους δεν υφίσταται πιστοποίηση ούτε κατά ISO 9000:2000.

2.12. Το Κοινό Πλαίσιο Αξιολόγησης[10]

Το Κοινό Πλαίσιο Αξιολόγησης (ΚΠΑ) είναι ένα εργαλείο Διοίκησης Ολικής Ποιότητας που έχει επηρεαστεί από το Πρότυπο Αριστείας του Ευρωπαϊκού Ιδρύματος για τη Διοίκηση Ποιότητας (European Foundation Quality Management - EFQM) και το πρότυπο του Γερμανικού Πανεπιστημίου Διοικητικών Επιστημών Speyer. Σύμφωνα με το ΚΠΑ τα άριστα αποτελέσματα ως προς την οργανωτική απόδοση, τους πελάτες/πολίτες και την κοινωνία εξαρτώνται *από την ηγεσία, τη στρατηγική και τον προγραμματισμό, το ανθρώπινο δυναμικό, τις συνεργασίες και τους πόρους και τις διοικητικές διαδικασίες.* Το ΚΠΑ αποτελεί μια ολιστική ανάλυση της οργανωτικής απόδοσης προσεγγίζοντάς την από διαφορετικές οπτικές ταυτόχρονα.

Το ΚΠΑ είναι το αποτέλεσμα της συνεργασίας των Υπουργών της Ευρωπαϊκής Ένωσης που είναι υπεύθυνοι για τη Δημόσια Διοίκηση. Διαμορφώθηκε από την Ομάδα Καινοτόμων Δημοσίων Υπηρεσιών (Innovative Public Services Group - IPSG), που αποτελείται από εθνικούς εμπειρογνώμονες και συστάθηκε με απόφαση των Γενικών Διευθυντών. Σκοπός της ομάδας αυτής είναι η προώθηση ανταλλαγών και η οργάνωση συνεργασιών στο πεδίο των διοικητικών καινοτομιών και της παροχής δημοσίων υπηρεσιών στους πολίτες των κρατών μελών της Ευρωπαϊκής Ένωσης.

Το ΚΠΑ προσφέρεται ως ένα εύκολο στη χρήση του εργαλείο, ώστε να βοηθηθούν οι οργανώσεις του δημοσίου τομέα σε όλη την Ευρώπη να χρησιμοποιήσουν τεχνικές Διοίκησης Ολικής Ποιότητας και να βελτιώσουν την απόδοσή τους. Παρέχει ένα πλαίσιο αυτό-αξιολόγησης που είναι εννοιολογικά παρόμοιο με τα κύρια μοντέλα Διοίκησης Ολικής Ποιότητας, ιδιαιτέρως με το EFQM, αλλά έχει διαμορφωθεί ειδικά για τις οργανώσεις του δημοσίου τομέα, λαμβάνοντας υπόψη τις διαφορές τους.

Το ΚΠΑ έχει τέσσερις κυρίους σκοπούς:

1. να εισαγάγει στη δημόσια διοίκηση τις αρχές της Διοίκησης Ολικής Ποιότητας και προοδευτικά να την οδηγήσει, μέσω της χρήσης και της κατανόησης της αυτό-αξιολόγησης, από την αλληλουχία των δραστηριοτήτων «Προγραμματισμός-Εκτέλεση» σε έναν ολοκληρωμένο κύκλο ποιότητας

---

[10]Κοινό Πλαίσιο Αξιολόγησης, Υπουργείο Εσωτερικών, Διεύθυνση Ποιότητας και Αποδοτικότητας, 2007.

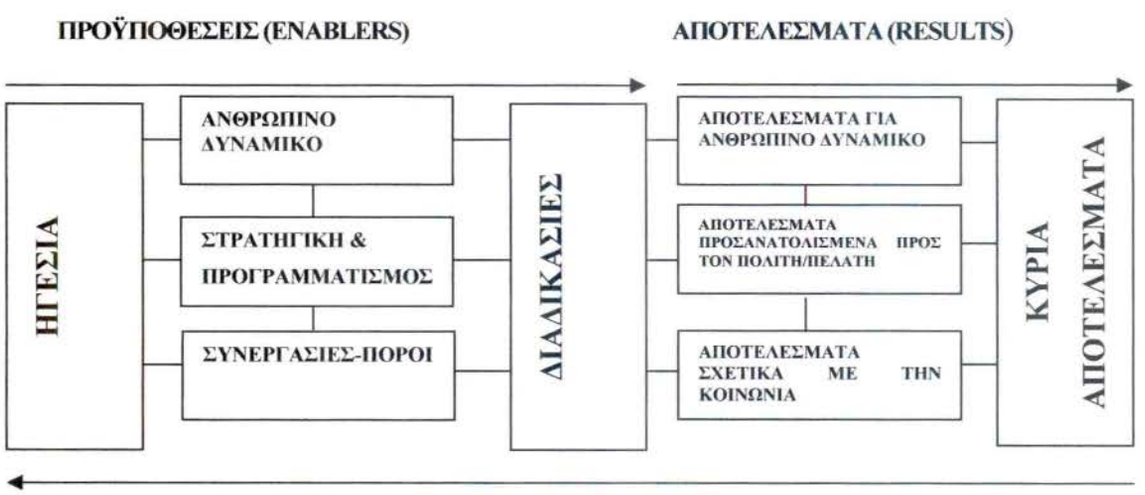
αποτελούμενο από τον Προγραμματισμό, την Εκτέλεση, τον Έλεγχο και την Ανάδραση,

2. να διευκολύνει την αυτό-αξιολόγηση μιας δημόσιας οργάνωσης, ώστε να αποτυπωθεί επαρκώς η υφιστάμενη κατάσταση και να σχεδιαστούν δράσεις βελτίωσης,
3. να αποτελέσει τη «γέφυρα» μεταξύ των διαφορετικών μοντέλων που χρησιμοποιούνται στη διοίκηση ποιότητας,
4. να διευκολύνει τη συγκριτική μάθηση μεταξύ των οργανώσεων του δημοσίου τομέα.

Το ΚΠΑ μπορεί να εφαρμοστεί στο σύνολο των δημοσίων οργανώσεων ανεξάρτητα από επίπεδο λειτουργίας σε εθνικό/ομοσπονδιακό, περιφερειακό και τοπικό επίπεδο. Μπορεί επίσης να χρησιμοποιηθεί σε ένα μεγάλο εύρος συνθηκών όπως π.χ. ως μέρος ενός συστηματικού προγράμματος μεταρρύθμισης ή ως βάση στοχευμένων διοικητικών βελτιώσεων στο δημόσιο τομέα. Σε ορισμένες περιπτώσεις, και ειδικά σε πολύ μεγάλες οργανώσεις, μια αυτό-αξιολόγηση μπορεί επίσης να λάβει χώρα σε έναν τομέα της οργάνωσης π.χ. σε ένα επιλεγμένο τμήμα ή διεύθυνση ή γενική διεύθυνση.

2.13. Δομή του Κοινού Πλαισίου Αξιολόγησης

Η δομή του ΚΠΑ είναι η ακόλουθη:



Σχήμα 5: Το Κοινό Πλαίσιο Αξιολόγησης
Πηγή: Υπουργείο Εσωτερικών, ΚΠΑ 2007:8

Η δομή των εννέα κριτηρίων προσδιορίζει τα κύρια σημεία που πρέπει να ληφθούν υπόψη σε οποιαδήποτε οργανωτική ανάλυση. Τα κριτήρια 1 έως 5 αφορούν τις προϋποθέσεις μιας οργάνωσης. Οι προϋποθέσεις καθορίζουν το τι κάνει η οργάνωση και πώς προσεγγίζει τα έργα που της έχουν ανατεθεί, ώστε να επιτύχει τα επιθυμητά αποτελέσματα. Τα κριτήρια 6 έως 9 αφορούν τα αποτελέσματα που επιτυγχάνει η δημόσια οργάνωση ως προς τους πολίτες/πελάτες, το ανθρώπινο δυναμικό, την κοινωνία και τα βασικά αποτελέσματα μέσω μετρήσεων της ικανοποίησης των πολιτών από τη λειτουργία μιας δημόσιας οργάνωσης. Τα ανωτέρω κριτήρια βασίζονται στη χρησιμοποίηση δεικτών μέτρησης αποτελεσμάτων. Κάθε κριτήριο χωρίζεται σε έναν αριθμό 28 υποκριτηρίων, τα οποία προσδιορίζουν τα κύρια ζητήματα που πρέπει να ληφθούν υπόψη όταν αξιολογείται μια οργάνωση. Το περιεχόμενο κάθε υποκριτηρίου εκφράζεται μέσω παραδειγμάτων που εξηγούν τη φύση του. Κάθε παράδειγμα αφορά και ένα πεδίο ή πτυχή της διοικητικής πραγματικότητας που προσεγγίζεται ώστε να διερευνηθεί εάν αυτή ανταποκρίνεται στις προβλεπόμενες απαιτήσεις από το ΚΠΑ.

2.14. Κύρια Χαρακτηριστικά του Κοινού Πλαισίου Αξιολόγησης

Η χρήση του ΚΠΑ παρέχει στην οργάνωση ένα πλαίσιο αρχών και διαδικασιών, των οποίων η εφαρμογή συμβάλλει στη συνεχή διοικητική βελτίωση. Το ΚΠΑ παρέχει:

- μια αξιολόγηση βασισμένη σε πραγματικά στοιχεία, δηλαδή σε ένα σύνολο κριτηρίων που έχουν γίνει ευρέως αποδεκτά από όλο τον ευρωπαϊκό δημόσιο τομέα,
- ευκαιρίες να αναγνωριστεί η πρόοδος που έχει συντελεστεί και να εντοπιστούν πεδία εξαιρετικών αποδόσεων,
- ένα μέσο διασφάλισης της συνέπειας και της συνέχειας ως προς το τι πρέπει να γίνει για να βελτιωθεί η δημόσια οργάνωση,
- ένα σύνδεσμο μεταξύ των διαφορετικών επιδιωκόμενων αποτελεσμάτων και των υποστηρικτικών πρακτικών ή προϋποθέσεων,
- ένα μέσο για να δημιουργηθεί ενθουσιασμός μεταξύ των υπαλλήλων με τη συμμετοχή τους στη διαδικασία βελτίωσης,
- ευκαιρίες να προωθηθούν και να γίνουν κοινό κτήμα οι καλές διοικητικές πρακτικές ενδο-διοικητικά αλλά και μεταξύ διαφορετικών οργανώσεων,

- ένα μέσο ενσωμάτωσης των διαφόρων πρωτοβουλιών ποιότητας στις καθημερινές επιχειρησιακές λειτουργίες,
- ένα μέσο μέτρησης της προόδου μέσω της περιοδικής αξιολόγησης ανά τακτά χρονικά διαστήματα.

2.15. Έννοιες και αξίες του ΚΠΑ

Το ΚΠΑ ως εργαλείο της Διοίκησης Ολικής Ποιότητας θεμελιώνεται στις βασικές έννοιες και αξίες που συνθέτουν τη διοικητική αριστεία, όπως αυτή έχει αποτυπωθεί από το EFQM, και ειδικότερα στον προσανατολισμό στα αποτελέσματα, στην εξυπηρέτηση του πελάτη, στην ηγεσία και στην αξιοπιστία της στοχοθεσίας, στη διοίκηση μέσω διαδικασιών και πραγματικών δεδομένων, στη συμμετοχή του ανθρώπινου δυναμικού, στη συνεχή βελτίωση και καινοτομία, στις αμοιβαία επωφελείς συνεργασίες και στη συλλογική κοινωνική ευθύνη. Το ΚΠΑ βοηθάει στη βελτίωση της απόδοσης των δημοσίων οργανώσεων στη βάση των παραπάνω εννοιών.

Το δημόσιο μάνατζμεντ και η ποιότητα στο δημόσιο τομέα διαφέρουν σε σχέση με τον ιδιωτικό τομέα. Οι βασικές κοινές προϋποθέσεις λειτουργίας της δημόσιας διοίκησης στην ευρωπαϊκή κοινωνικοπολιτική και διοικητική κουλτούρα είναι: η νομιμότητα (δημοκρατική, κοινοβουλευτική), η αρχή του νόμου και η ηθική συμπεριφορά που βασίζεται σε κοινές αξίες και αρχές όπως ο ανοιχτός χαρακτήρας της διοίκησης, η υποχρέωση λογοδοσίας, η συμμετοχή, η ποικιλομορφία, η ισότητα, η κοινωνική δικαιοσύνη, η αλληλεγγύη, η συνεργασία και οι συμπράξεις.

Αν και το ΚΠΑ εστιάζεται κυρίως στην αξιολόγηση της απόδοσης της διοίκησης και στον προσδιορισμό των οργανωτικών της αιτιών, ώστε να καταστήσει δυνατή τη διοικητική βελτίωση, ο τελικός στόχος της εφαρμογής του είναι *η συνεισφορά στην καλή διακυβέρνηση.*

Έτσι, η αξιολόγηση της απόδοσης αφορά τα εξής ζητήματα:

- την ικανότητα ανταπόκρισης στις ανάγκες των πολιτών και τη λογοδοσία,
- την έννομη λειτουργία της και τη δράση της εντός του προβλεπόμενου θεσμικού-κανονιστικού πλαισίου,
- την επικοινωνία με το πολιτικό επίπεδο,
- τη συμμετοχή των μετόχων και την εξισορρόπηση των αναγκών των μετόχων,

- την άριστη παροχή υπηρεσιών,
- την εξοικονόμηση πόρων,
- την επίτευξη των στόχων και
- τη διαχείριση του εκσυγχρονισμού, της καινοτομίας και της αλλαγής.

2.16. Αλληλένδετες λειτουργίες στο πλαίσιο του προτύπου

Η ολιστική προσέγγιση βάσει της Διοίκησης Ολικής Ποιότητας και του ΚΠΑ δεν σημαίνει μόνο ότι οι λειτουργίες της δημόσιας οργάνωσης αξιολογούνται προσεκτικά, αλλά και ότι μετρούνται οι παραγόμενες επιπτώσεις από τη μεταξύ τους αλληλεξάρτηση. Ο διαχωρισμός που θα μπορούσε να γίνει είναι αυτός μεταξύ:

- της σχέσης αιτίου-αποτελέσματος, δηλαδή μεταξύ του αριστερού τμήματος του προτύπου (οι προϋποθέσεις – αιτίες) και του δεξιού τμήματος (τα αποτελέσματα-συνέπειες) και
- της ολιστικής σχέσης μεταξύ των αιτιών (προϋποθέσεων).

Μόνο στο τελευταίο μπορεί να εφαρμοστεί ο ολιστικός χαρακτήρας.

Η αυτό-αξιολόγηση και η βελτίωση των δημοσίων οργανώσεων είναι πολύ δύσκολη χωρίς αξιόπιστη πληροφόρηση για τις διαφορετικές λειτουργίες της δημόσιας οργάνωσης. Το ΚΠΑ ενεργοποιεί τις οργανώσεις του δημοσίου τομέα προκειμένου να συλλέξουν και να χρησιμοποιήσουν πληροφορίες, αλλά πολύ συχνά αυτή η πληροφόρηση δεν είναι διαθέσιμη σε μια πρώτη αυτό-αξιολόγηση. Αυτό συμβαίνει διότι το ΚΠΑ αντιμετωπίζεται συχνά ως μέτρηση που ξεκινά από μηδενική βάση. Υποδεικνύει τις περιοχές εκείνες που είναι βασικές για να ξεκινήσει η μέτρηση. Όσο περισσότερο μια διοίκηση εξελίσσεται προς τη συνεχή βελτίωση τόσο περισσότερο θα συλλέγει και θα διαχειρίζεται την πληροφόρηση με συστηματικό και προοδευτικό τρόπο, εσωτερικά και εξωτερικά.

Κεφάλαιο 3

Πληροφοριακά Συστήματα, Ασφάλεια και Ποιότητα Ασφάλειας

3.1. Εισαγωγή

Η ενίσχυση της αποτελεσματικότητας και της παραγωγικότητας της Διοίκησης και η καλύτερη και ταχύτερη εξυπηρέτηση του πολίτη, είναι στρατηγικοί στόχοι της Διοικητικής Μεταρρύθμισης που βρίσκεται σ' εξέλιξη, οι οποίοι δεν μπορούν να προωθηθούν με επάρκεια χωρίς την εισαγωγή των εφαρμογών της Ηλεκτρονικής Διακυβέρνησης, τη χρήση Πληροφοριακών Συστημάτων και τεχνολογιών επικοινωνιών όπως η ευρυζωνικότητα[11]. Όμως για διάφορους λόγους το περιβάλλον της Ηλεκτρονικής Διακυβέρνησης δεν παρέχει ασφάλεια.

Τα Πληροφοριακά Συστήματα θα πρέπει να προστατεύονται από τις κάθε μορφής απειλές, χωρίς όμως, ταυτόχρονα, η προστασία αυτή να εμποδίζει τη ροή των πληροφοριών. Η ασφάλεια ενός πληροφοριακού συστήματος παρουσιάζει ιδιαιτερότητες και δυσκολίες ως επιστημονικός ερευνητικός χώρος αλλά και ως επιστημονική πρακτική. Ο προσέγγιση στην ασφάλεια των ΠΣ πρέπει επίσης να είναι στο πεδίο της τεχνικής, αλλά και της συμπεριφορικής προσέγγισης.

Στο κεφάλαιο αυτό αρχικά γίνεται μια εννοιολογική προσέγγιση της ασφάλειας των Πληροφοριακών Συστημάτων και αναφορά στο "Σπίτι της Ασφάλειας". Θα αναφερθούν ποιοι είναι οι δικαιούχοι της ασφάλειας και ποιοι οι επίβουλοί της. Ακολουθεί αναφορά στα μοντέλα ασφάλειας. Στο τέλος του κεφαλαίου θα επιχειρηθεί μια προσέγγιση της ασφάλειας κάτω από το πρίσμα της ποιότητας, και τη σχέση της με τη Διοίκηση Ολικής Ποιότητας.

---

[11]Τεχνολογία που παρέχει τη δυνατότητα πρόσβασης και χρήσης διαδραστικών ηλεκτρονικών υπηρεσιών που απαιτούν την ανταλλαγή μεγάλων ποσοτήτων πληροφοριών, φωνής, εικόνας και βίντεο.

3.2. Πληροφοριακά Συστήματα και Ασφάλεια

Κυρίαρχο ρόλο τόσο στις διαδικασίες βελτίωσης ποιότητας προϊόντων και υπηρεσιών όσο και στην λήψη ποιοτικών διοικητικών αποφάσεων παίζουν τα πληροφοριακά συστήματα. Τα πληροφοριακά συστήματα αποτελούν το θεμέλιο των νέων, βασισμένων στις γνώσεις, προϊόντων και υπηρεσιών στις οικονομίες της γνώσης και βοηθούν τους οργανισμούς να διαχειριστούν τους γνωστικούς πόρους τους. Τα πληροφοριακά συστήματα δίνουν στους οργανισμούς τη δυνατότητα να υιοθετούν πιο επίπεδες, περισσότερο αποκεντρωμένες δομές, με ευέλικτες διευθετήσεις μεταξύ εργαζομένων και στελεχών και με ευκολία συντονισμού με άλλους οργανισμούς από μεγάλη απόσταση. Οι οργανισμοί μπορούν να γίνουν περισσότερο ανταγωνιστικοί και αποτελεσματικοί μετασχηματιζόμενοι σε ψηφιακούς, όπου όλες σχεδόν οι βασικές επιχειρησιακές διεργασίες και οι σχέσεις με τους πελάτες, τους προμηθευτές και τους εργαζομένους υποβοηθούνται ψηφιακά. Το πληροφοριακό σύστημα είναι τμήμα μιας σειράς δραστηριοτήτων προστιθέμενης αξίας για τη συγκέντρωση, το μετασχηματισμό και τη διάδοση πληροφοριών τις οποίες μπορούν να χρησιμοποιήσουν τα διευθυντικά στελέχη για να βελτιώσουν τη λήψη αποφάσεων.

Όσο όμως αυξάνει η σημαντικότητα του ρόλου των πληροφοριακών συστημάτων στη λειτουργία των οργανισμών, τόσο αυξάνει και η εξάρτηση από τον ασφαλή και ομαλό τρόπο λειτουργία τους. Καθώς τα δεδομένα βρίσκονται σε ηλεκτρονική μορφή και πολλές διαδικασίες είναι αόρατες λόγω αυτοματισμού, τα πληροφοριακά συστήματα σε υπολογιστή είναι ευαίσθητα σε καταστροφή, κακή χρήση, σφάλματα, απάτες, και βλάβες υλικού ή λογισμικού. Τα συστήματα που λειτουργούν σε δίκτυο και αυτά που χρησιμοποιούν το Internet είναι ιδιαίτερα τρωτά, επειδή τα δεδομένα και τα αρχεία τους μπορούν να προσπελαστούν αμέσως και άμεσα από τερματικά υπολογιστών ή από πολλά σημεία του δικτύου. Χάκερ μπορούν να διεισδύσουν σε εταιρικά δίκτυα, να προσπελάσουν τους πόρους του δικτύου, και να προκαλέσουν σοβαρές διαταραχές στα συστήματα, αναστατώνοντας τη ροή των πληροφοριών. Κακόβουλο λογισμικό (malicious codes) μπορεί να εισαχθεί και να εξαπλωθεί ανεξέλεγκτα από σύστημα σε σύστημα, και να καταστρέψει προγράμματα, δεδομένα ακόμη και συστήματα. Επιπρόσθετα όσο οι οργανισμοί εξελίσσονται και επεκτείνονται δημιουργώντας διαρκώς νέες διασυνδέσεις με προμηθευτές, πελάτες, άλλους οργανισμούς και συνεργάτες, θα υπάρχει ένα διαρκώς ευρυνόμενο φάσμα απαιτήσεων ασφάλειας. Η ασφάλεια συνεπώς αποτελεί έναν κρίσιμο παράγοντα για

την επιτυχία οποιουδήποτε οργανισμού.

3.3. Ασφάλεια Πληροφοριακού συστήματος

Είναι γεγονός ότι στη διεθνή επιστημονική βιβλιογραφία δεν υπάρχει ορισμός της ασφάλειας Πληροφοριακού Συστήματος στον οποίο όλοι να συμφωνούν. Ένας ορισμός που περιγράφει, το περιεχόμενο του όρου (Κιουντούζης, 1995:320) είναι: «*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*».

Ο παραπάνω ορισμός παρέχει το πλεονέκτημα της άμεσης αναφοράς στα ακόλουθα βασικά στοιχεία:

- ✓ έμφαση όχι μόνο στο Πληροφοριακό Σύστημα ως ολότητα αλλά και σε όλα τα επιμέρους στοιχεία του
- ✓ η προστασία αφορά κάθε είδους απειλή (τυχαία ή σκόπιμη)
- ✓ η ασφάλεια Πληροφοριακού Συστήματος συνδέεται άμεσα τόσο με τις τεχνικές, διαδικασίες και διοικητικά μέτρα όσο και με τις αντιλήψεις, αρχές και παραδοχές
- ✓ το πλαίσιο αυτό χαρακτηρίζεται από οργάνωση.

Η ασφάλεια των πληροφοριακών συστημάτων (Πάγκαλος, Μαυρίδης, 2002:16) σχετίζεται με:

1. *Πρόληψη (prevention):* Την λήψη δηλαδή μέτρων για να προληφθούν φθορές των συστατικών ενός πληροφοριακού συστήματος.
2. *Ανίχνευση (detection):* Την λήψη μέτρων για την ανίχνευση του πότε, πως και από ποιον προκλήθηκε φθορά σε ένα συστατικό ενός πληροφοριακού συστήματος.
3. *Αντίδραση (reaction):* Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός πληροφοριακού συστήματος.

3.4. Η Ασφάλεια ως Απαίτηση Δικαιούχων

Τα ΠΣ έχουν βασικό ρόλο στη λειτουργία των δημόσιων οργανισμών στα πλαίσια της Ηλεκτρονικής Διακυβέρνησης. Από την αποτελεσματική και την ασφαλή λειτουργία τους θα εξαρτηθεί η πραγματοποίηση της μετάβασης και η λειτουργία στις νέες συνθήκες διακυβέρνησης. Συνεπώς είναι πολλοί αυτοί που έχουν άμεσο συμφέρον, άρα και δικαίωμα απαίτησης, για την ύπαρξη μέτρων ασφάλειας στο Πληροφοριακό Σύστημα. Ενδεικτικά αυτοί, που έχουν δικαίωμα απαίτησης στο να υπάρχουν μηχανισμοί και μέτρα ασφάλειας, είναι:

1. Η διοίκηση του οργανισμού. Με δεδομένο το ρόλο του Πληροφοριακού Συστήματος και τη σημασία των πληροφοριακών πόρων, σε συνδυασμό με την υψηλή οικονομική δαπάνη και τη σπουδαιότητα που απαιτεί η απρόσκοπτη λειτουργία του συστήματος, είναι εύλογο να ενδιαφέρεται η διοίκηση για το επίπεδο ασφάλειάς του.
2. Ιδιοκτήτες και Διαχειριστές δεδομένων και διεργασιών, αφού τυχόν μειωμένα μέτρα ασφαλείας καθιστούν το σύστημα ευπαθές και ευάλωτο στις πάσης φύσεως απειλές από τρίτους.
3. Οι εμπλεκόμενοι στην ανάπτυξη του Πληροφοριακού Συστήματος. Οι υπεύθυνοι λειτουργίας του Πληροφοριακού Συστήματος. Στην κατηγορία αυτή ανήκουν όλοι όσοι εμπλέκονται στη καλή λειτουργία του υπολογιστικού και τεχνολογικού εξοπλισμού.
4. Οι καταναλωτές των τελικών προϊόντων και υπηρεσιών. Οι απλοί πελάτες και πολίτες, που χρησιμοποιούν το ΠΣ για τη λήψη μιας υπηρεσίας ή την πραγματοποίηση μιας ενέργειάς του.
5. Η πολιτεία παίζει σημαντικό ρόλο στη διαμόρφωση των μέτρων ασφάλειας, με το να θέτει πλαίσια και κανόνες που πρέπει να τηρούνται. Η βαρύτητα των ποινικών αδικημάτων που μπορούν να διαπραχθούν από την παράνομη συλλογή, αρχειοθέτηση, χρήση, μετάδοση και επεξεργασία πληροφοριών, αναγκάζει την πολιτεία να θεσπίσει Ανεξάρτητες Διοικητικές Αρχές εντεταλμένες να ελέγχουν την ασφάλεια κάθε πληροφοριακού συστήματος.
6. Τέλος μια αποτυχία στην αντιμετώπιση μιας δικτυακής επίθεσης σε ένα Δημόσιο Οργανισμό πέρα από την πιθανή απώλεια ευαίσθητων δημόσιων ή ιδιωτικών δεδομένων από τα αρχεία του οργανισμού, θα προκαλέσει μεγάλο πλήγμα στη

δημόσια εικόνα και την αξιοπιστία τόσο του οργανισμού όσο και του ίδιου του κράτους.

Είναι φανερό, ότι στο όλο θέμα εμπλέκονται αρκετοί παράγοντες όπως, επίσης και πολλοί ενδιαφερόμενοι. Είναι φυσικό κάθε ένας από αυτούς να προσδοκά διαφορετικά πράγματα. Για παράδειγμα, η διοίκηση είναι εύλογο να δίνει μεγάλη σημασία στο οικονομικό κόστος και στον πιθανό ανασχεδιασμό δραστηριοτήτων, που συνεπάγεται η εφαρμογή των μέτρων ασφαλείας. Επιθυμεί επίσης την ύπαρξη αιτιολόγησης για το ύψος κάθε δαπάνης και πρότασης ανασχεδιασμού. Οι τελικοί χρήστες και η πολιτεία δίνουν έμφαση κυρίως στην πληρότητα ικανοποίησης των απαιτήσεων ασφάλειας (π.χ. διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα, κ.ά.), αγνοώντας το κόστος. Οι διαχειριστές διεργασιών και οι υπεύθυνοι λειτουργίας ενδιαφέρονται, παράλληλα, όπως τα αντίμετρα που προτείνονται να ταιριάζουν με τα οργανωσιακά χαρακτηριστικά και την κουλτούρα του οργανισμού, ώστε να μην απαιτούνται πολλές αλλαγές στη δομή και στον τρόπο λειτουργίας της επιχείρησης. Τέλος, οι υπεύθυνοι ανάπτυξης του πληροφοριακού συστήματος καθώς και οι ειδικοί ασφάλειας ενδιαφέρονται για μια σειρά από παράγοντες, όπως, το επιστημολογικό/ οντολογικό πλαίσιο της κάθε προσέγγισης, το εύρος εφαρμογής, την ασύμμετρη ή όχι έμφαση στα στοιχεία του πληροφοριακού συστήματος, το ρόλο του αναλυτή και των χρηστών, το δυναμικό ή στατικό χαρακτήρα κάθε πρότασης, το πρόσφορο της υιοθέτησης της κ.ά.

3.5. Επίβουλοι του συστήματος

Οι επιθέσεις κατά του συστήματος, αν ταξινομηθούν με βάση το σκοπό τους, δίνουν τις εξής πέντε κατηγορίες:

1. *Εισαγωγή ή μετατροπή* δεδομένων χωρίς εξουσιοδότηση ή καταστροφή δεδομένων ή προγραμμάτων ενός πληροφοριακού συστήματος.
2. *Αλλοίωση ή μείωση* της αξιοπιστίας των δεδομένων του Πληροφοριακού Συστήματος.
3. *Παρεμπόδιση* της ομαλής λειτουργίας του.
4. *Χωρίς άδεια εισβολή* και αφαίρεση στοιχείων.
5. *Παραβίαση* των αποκλειστικών δικαιωμάτων του δημιουργού, του κατόχου, δεδομένων, προγραμμάτων και γενικά πληροφοριακού υλικού.

Στις παραπάνω κατηγορίες θα πρέπει να προστεθεί η επίθεση με ιομορφικό λογισμικό. Ποίοι είναι όμως αυτοί, που απειλούν το Πληροφοριακό Σύστημα; Είναι ενδιαφέρον ότι σε πρόσφατη έρευνα (2003), που έγινε στις Η.Π.Α., διαπιστώθηκε ότι το 55% των παραβιάσεων έγινε από υπαλλήλους του οργανισμού, 38% από hackers και το 8% από ανταγωνιστές. Το ότι ή κυριότερη απειλή προέρχεται από μέσα από τον οργανισμό το δείχνουν και οι ετήσιες εκθέσεις του Computer Security Institute (2003 CSI/FBI Computer Crime and Security Survey) των τελευταίων χρόνων. Εργολάβοι, συνεταίροι, σύμβουλοι, δυσαρεστημένο προσωπικό, υπάλληλοι (εν ενεργεία και πρώην) που θέλουν να εκδικηθούν τη διοίκηση για τις αποφάσεις της και τέλος, χρήστες με λανθασμένη αντίληψη για τα δικαιώματα και τα προνόμια τους, είναι μερικές από τις αιτίες που προκαλούν αυτού του είδους τις ενέργειες. (Ε.Κιουντούζης, 2004:322)

3.6. Θεμελιώδεις έννοιες

Είναι γενικά αποδεκτό σήμερα (Πάγκαλος, Μαυρίδης 2002:18) ότι η έννοια της ασφάλειας των πληροφοριακών συστημάτων (information system security) συνδέεται στενά με τρεις βασικές έννοιες:

- *Εμπιστευτικότητα (Confidentiality),* σημαίνει πρόληψη μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Άλλες εκφάνσεις της εμπιστευτικότητας είναι:
    - Η ιδιωτικότητα (privacy): προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα.
    - Η μυστικότητα (secrecy): προστασία των δεδομένων που ανήκουν σε έναν οργανισμό.
- *Ακεραιότητα (Integrity),* σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.
- *Διαθεσιμότητα (Availability),* ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος (ΠΣ) όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα.

Η ασφάλεια πληροφοριών επιτυγχάνεται με την υλοποίηση των κατάλληλων μηχανισμών ελέγχου, οι οποίοι μπορεί να είναι πολιτικές, πρακτικές, διαδικασίες,

οργανωτικές δομές και λειτουργίες λογισμικού. Αυτοί οι μηχανισμοί ελέγχου είναι απαραίτητοι προκειμένου να διασφαλιστεί ότι ικανοποιούνται οι απαιτήσεις ασφάλειας του οργανισμού.

3.7. The House of Security

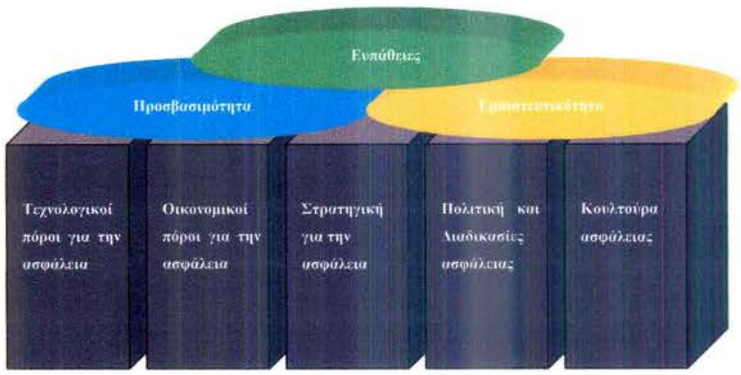
Στο MIT Sloan School of Management έγινε μια προσπάθεια για τον ακριβή προσδιορισμό του τι σημαίνει ακριβώς " ποιότητα ασφάλειας" , ειδικά κάτω από μια πιο ολιστική έννοια.

Έτσι μέσω λεπτομερούς βιβλιογραφικής επισκόπησης, αναζητήσεων στο Web, και διάφορων ερευνών, ερευνητές προσδιόρισαν περίπου 300 ζητήματα ασφάλειας (security issues). Αυτά τα ζητήματα ασφάλειας βρέθηκαν να ομαδοποιούνται πρώτιστα σε οκτώ ομαδικούς μετα-σχηματισμούς (meta-groupings) ή υποδομές (constructs), ως εξής: (Madnick, Siegel, 2006)

- Η καλή ασφάλεια (good security) παρέχει τη δυνατότητα πρόσβασης (accessibility) σε δεδομένα και δίκτυα σε αρμόδιους (appropriate) χρήστες προστατεύοντας ταυτόχρονα την εμπιστευτικότητα (confidentiality) των δεδομένων και ελαχιστοποιώντας τις ευπάθειες (vulnerabilities) που μπορεί να χρησιμοποιηθούν από επιθέσεις και απειλές (attacks and threats).
- Η ορθή πρακτική ασφάλειας (good security practice) υπερβαίνει τις τεχνικές IT λύσεις. Οδηγείται από μια Στρατηγική της επιχείρησης (business strategy) με τις σχετικές Πολιτικές Ασφάλειας και Διαδικασίες (security policies and procedures) και εφαρμόζεται σε μια Κουλτούρα Ασφάλειας (culture of security). Αυτές οι πρακτικές υποστηρίζονται από IT Πόρους (IT resources) και Οικονομικούς Πόρους (financial resources) που αφιερώνονται στην ασφάλεια. Αυτές οι οκτώ υποδομές διαμορφώνουν το σπίτι της ασφάλειας *House of Security*[12] , όπως φαίνεται στο σχήμα 6.

---

[12]Ο όρος αποτελεί παράφραση του όρου " House of Quality" ή Quality Function Deployment QFD που είναι μέθοδος ανάπτυξης ποιότητας και αποτελεί τρόπο ολοκληρωμένης ικανοποίησης των επιθυμητών στόχων ποιότητας σε κάθε τμήμα και διαδικασία μιας επιχείρησης (Δερβιτσιώτης, 2005:353).



Σχήμα 6: Οι Οκτώ Υποδομές οργανωμένες σαν το Σπίτι της Ασφάλειας. Πηγή MIT

Οι πρώτες τρεις δομές, παροχή δυνατότητας πρόσβασης, προστασία της εμπιστευτικότητας, και ελαχιστοποίηση των αδυναμιών, είναι οι στόχοι της ασφάλειας πληροφοριών, και είναι έτσι οι εξαρτημένες μεταβλητές. Αυτές είναι:

1. *Ευπάθεια (Vulnerability)*: Δυνατότητα ώστε τα δεδομένα και τα δίκτυα να αλλοιωθούν (tampered) , να υποστούν επίθεση (attacked), ή να καταστραφούν (destroyed).
2. *Δυνατότητα πρόσβασης (Accessibility)*: Διαθεσιμότητα των δεδομένων και των δικτύων στους αρμόδιους χρήστες.
3. *Εμπιστευτικότητα (Confidentiality)*: Προστασία των εμπιστευτικών (confidential) εταιρικών δεδομένων και η μυστικότητα (privacy) των ατομικών δεδομένων.

Οι επόμενες πέντε υποδομές περιλαμβάνουν τις πρακτικές ασφάλειας (security practices) που συμβάλλουν ιδιαίτερα στην ασφάλεια των πληροφοριών, και έτσι θεωρούνται ανεξάρτητες μεταβλητές. Αυτές ορίζονται κατωτέρω:

1. *Πόροι τεχνολογίας πληροφοριών (IT) για την ασφάλεια*: Πόροι IT για την υποστήριξη των πρακτικών ασφάλειας δεδομένων και δικτύων.
2. *Οικονομικοί πόροι για την ασφάλεια*: Οικονομικοί πόροι για την υποστήριξη των πρακτικών ασφάλειας δεδομένων και δικτύων.

3. *Επιχειρησιακή Στρατηγική για την ασφάλεια*: Στρατηγική ορισμού κατεύθυνσης και ατζέντας για τις πρακτικές ασφάλειας δεδομένων και δικτύων.
4. *Πολιτική ασφάλειας και διαδικασίες*: Δηλωμένοι (stated) κανόνες και διαδικασίες ασφάλειας δεδομένων και δικτύων.
5. *Κουλτούρα ασφάλειας*: Υποστηρικτικό περιβάλλον για την εφαρμογή των πρακτικών ασφάλειας δεδομένων και δικτύων.

3.8. Μοντέλα Ασφάλειας Πληροφοριακών Συστημάτων

Τα μοντέλα αυτά χρησιμοποιούνται ως βάση για τη δημιουργία των μηχανισμών και των μέτρων προστασίας. Υπάρχουν δύο μεγάλες κατηγορίες προσεγγίσεων (Ε. Κιουντούζης, 2004:323-331) στο θέμα της ασφάλειας πληροφοριακών συστημάτων: αυτές που στηρίζονται σε βέλτιστες πρακτικές, και αυτές που προέρχονται από ερευνητικές προσπάθειες.

3.8.1. **Προσεγγίσεις με βάση βέλτιστες πρακτικές**

Στην κατηγορία αυτή ανήκουν οι προσεγγίσεις εκείνες, που στηριζόμενες στη συσσωρευμένη γνώση των ειδικών της ασφάλειας, προσπαθούν να αντιμετωπίσουν το θέμα, σχεδόν πάντα με κανονιστικό τρόπο, δηλαδή με λεπτομερείς διατάξεις. Τα πλέον γνωστά μοντέλα της κατηγορίας αυτής είναι:

(α) Το μοντέλο του καταλόγου

(β) Το μοντέλο του κιβωτισμού

(γ) Το μοντέλο του πίνακα

(δ) Τα πρότυπα ασφάλειας

(ε) Η ανάλυση και διαχείριση κινδύνων

Α. Το μοντέλο του καταλόγου (checklists) στηρίζεται σε έναν κατάλογο από παράγοντες ή θέματα που θεωρούνται (από ειδικούς σε θέματα ασφαλείας) σημαντικά, χωρίς να παίζει ρόλο η διάταξη ή σχέση μεταξύ των παραγόντων. Έτσι, με βάση τις απαντήσεις σε εκατοντάδες ερωτήσεις προσδιορίζονται είτε οι ενέργειες που πρέπει να γίνουν (action based checklists) ώστε το σύστημα να θεωρείται ασφαλές (Wood, 1987), είτε οι απειλές (threat based checklist) και τα σημεία ελέγχου (Ward, 1986) .

Β. Το μοντέλο του κιβωτισμού είναι μια σειρά από διαδοχικούς ομόκεντρους κύκλους, οι οποίοι, εξεταζόμενοι από τα μέσα προς τα έξω, εμφανίζονται να προστατεύουν τα δεδομένα, τον υπολογιστή, την υπολογιστική υποδομή, τον οργανισμό, το υπάρχον νομικό πλαίσιο και, τέλος, ο εξωτερικός κύκλος, το κοινωνικό πλαίσιο.

Γ. Το μοντέλο του πίνακα (matrix) στην ουσία εστιάζεται στην ασφάλεια της πληροφορίας (data). Το μεγάλο πλεονέκτημα του είναι ότι επιτρέπει την απεικόνιση θεμάτων ασφάλειας πληροφοριών ταυτόχρονα με την μορφή ενός πίνακα με τρεις διαφορετικές διαστάσεις.

- Στην πρώτη διάσταση να απεικονίζονται τα βασικά χαρακτηριστικά για να θεωρείται ένα σύστημα ασφαλές: εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.
- Στη δεύτερη διάσταση να απεικονίζονται τρεις καταστάσεις στις οποίες βρίσκεται η πληροφορία μέσα στο σύστημα: μεταβίβαση, αποθήκευση και επεξεργασία.
- Στην τρίτη διάσταση να απεικονίζονται τα μέτρα ασφάλειας ταξινομημένα σε τρεις μεγάλες κατηγορίες: τεχνολογία, πολιτική και εκπαίδευση προσωπικού.

Δ. Τα πρότυπα ασφάλειας (security standards) έκαναν την εμφάνιση τους τις δύο τελευταίες δεκαετίες (π.χ. ITSEC, IBAG, ISO, Common Criteria, COBIT, NIST's κ.λπ.). Υιοθετούν την ίδια προσέγγιση με το μοντέλο του καταλόγου (κανονιστική αξιοποίηση της συσσωρευμένης γνώσης των ειδικών) αλλά χωρίς να απαιτούν την άμεση απάντηση πληθώρας ερωτήσεων, καθορίζουν απαιτήσεις ασφάλειας γενικής χρήσης και ανά κατηγορία προστατευόμενου αγαθού.

Ε. Η ανάλυση και διαχείριση κινδύνων γίνεται σε δύο διαδοχικές φάσεις, κάθε μια από τις οποίες υποδιαιρείται σε μια σειρά από βήματα. Η ανάλυση επικινδυνότητας (risk analysis) απαντά στο ερώτημα της επιλογής αντιμέτρων, που θα προσφέρουν προστασία ανάλογη των κινδύνων που απειλούν το Π.Σ. Η διαχείριση κινδύνων σχετίζεται με την υλοποίηση, εγκατάσταση, εφαρμογή και εποπτεία λειτουργίας των αντιμέτρων. Όλες οι προτάσεις για ανάλυση επικινδυνότητας μπορούν να θεωρηθούν ως τεχνοκρατικές, αφού βασίζονται στη στατιστική θεωρία αποφάσεων και χρησιμοποιούνται ως τεχνικές ποσοτικοποίησης άυλων χαρακτηριστικών ενός συστήματος, όπως της πιθανότητας μη εξουσιοδοτημένης προσπέλασης, η οποία στη συνέχεια μετατρέπεται σε μεγέθη κόστους. Η μόνη τεχνική που κάπως

διαφοροποιείται είναι η Security By Analysis[13] (SBA), η οποία αναπτύχθηκε στη Σουηδία στη δεκαετία του '70 και στηρίζεται σε ομάδες χρηστών που προτείνουν και αναλύουν σενάρια πιθανών απειλών και μπορεί να θεωρηθεί ως ανθρωποκεντρική. Αναφορά γίνεται στο σχετικό κεφάλαιο.

3.8.2. Προσεγγίσεις με βάση Ερευνητικές Προσπάθειες

Οι σημαντικές ερευνητικές προσπάθειες των τελευταίων ετών είναι:

3.8.2.1. *Μοντελοποίηση υπευθυνοτήτων*

Σύμφωνα με αυτήν μια πολιτική ασφάλειας του οργανισμού (πρέπει να) περιγράφει το ποιος είναι υπεύθυνος σε ποιον, τον κατάλογο των υποχρεώσεων, το πως εκπληρώνεται κάθε μια υποχρέωση, την κατάσταση των πραγμάτων για τα οποία ισχύει υπευθυνότητα, κ.τ.λ. Δηλαδή, διατύπωση της *'need to know'* αρχής. Έτσι μέσα στον οργανισμό δημιουργείται ένα δίκτυο υπευθυνοτήτων (responsibilities) όπου εμπλέκονται υποχρεώσεις, δραστηριότητες, ρόλοι, δικαιώματα, δυνατότητες, υπευθυνότητες, πόροι και, φυσικά, άνθρωποι. Διάρρηξη του δικτύου αυτού είναι ενδεχόμενο να έχει επιπτώσεις σε αυτό που καλούμε ασφάλεια του πληροφοριακού συστήματος.

3.8.2.2. *Μοντέλα επαλλήλων στρωμάτων*

Το μοντέλο του κιβωτισμού δέχθηκε ισχυρή κριτική γιατί, μεταξύ των άλλων, η φωλιασμένη μορφή προστασίας που παρέχει, έκανε πολλούς να πιστεύουν ότι τέλεια ασφάλεια μπορεί να επιτευχθεί από καλή εφαρμογή των μέτρων και των μηχανισμών που αντιστοιχούν και σε ένα μόνο κύκλο. Έτσι ο Stewart Kowalski (1991) στο Security by Consensus μοντέλο του προσπαθεί να αμβλύνει την αυστηρή κανονιστική προσέγγιση του μοντέλου του κιβωτισμού εισάγοντας και την κοινωνική διάσταση. Συγκεκριμένα το μοντέλο του αποτελείται από τρία μέρη:

1. Μία διαστρωμάτωση από πέντε επίπεδα: το κοινωνικό-ηθικό, το νομικό, το επίπεδο διαχείρισης, το λειτουργικό επίπεδο, το τεχνικό επίπεδο.
2. Μία συλλογή από κοινωνικούς και τεχνικούς μηχανισμούς ελέγχου, μια αλυσίδα από ελέγχους, η οποία διαδοχικά συνδέει όλα τα επίπεδα.

---

[13]http://www.thesbamethod.com

3. Μία τεχνική ονοματοδοσίας (labeling technique), όπου σε κάθε επίπεδο ορίζεται το συντακτικό (syntax) και η σημασιολογία του (semantics) και η σημασιολογία του ενός επιπέδου γίνεται προσπάθεια να συνδεθεί με τη συντακτική δομή του επόμενου επιπέδου.

3.8.2.3. *Ενσωμάτωση ασφάλειας κατά την ανάπτυξη*

Σχεδόν όλες οι προσπάθειες που έχουμε περιγράψει μέχρι τώρα, ανεξάρτητα αν στηρίζονται σε βέλτιστες πρακτικές ή σε ερευνητική δραστηριότητα, θεωρούν την ασφάλεια ως ένα ξεχωριστό χαρακτηριστικό που θα πρέπει να προστεθεί στα γνωρίσματα του πληροφοριακού συστήματος. Το φαινόμενο αυτό θα το ονομάσουμε φαινόμενο δυϊσμού. Μια κατηγορία ερευνητών, στην προσπάθεια τους να απομακρυνθεί από το δυϊσμό, εισηγήθηκε όπως η ασφάλεια ενσωματώνεται σ' ένα σύστημα κατά τις φάσεις ανάπτυξης του πληροφοριακού συστήματος. Για παράδειγμα, ο Baskerville (1993) εισηγείται το σχεδιασμό μηχανισμών ελέγχου σε λογικό επίπεδο, στο στάδιο ανάπτυξης δηλαδή, όπου εξετάζουμε λύσεις ανεξάρτητα της φυσικής υλοποίησης. Συγκεκριμένα προτείνει όπως παράλληλα με τη δομημένη ανάλυση και σχεδίαση, γίνει χρήση τεχνικών που εισάγουν την ασφάλεια, όπως για παράδειγμα «διαγράμματα ροής δεδομένων με ασφάλεια» (data flow diagram with security).

Η δεύτερη προσπάθεια προς την ίδια κατεύθυνση αφορά τη σύνδεση της SSADM (Structured Systems Analysis and Design Method), μιας μεθόδου ανάπτυξης που θεωρείται πρότυπη στην Αγγλία, με τη μέθοδο ανάλυσης και διαχείρισης επικινδυνότητας CRAMM, που επίσης είναι πρότυπο στην ίδια χώρα.

Τέλος, προκειμένου να δοθεί ίση βαρύτητα στις ανθρώπινες και τεχνολογικές ανάγκες, οι Warren και Batten (2002), με το ίδιο σκεπτικό (εμπλουτισμός υπαρχόντων μεθοδολογιών ανάπτυξης Π.Σ.), τροποποιούν κατάλληλα τη μεθοδολογία ETHICS (Mumford, 1985:97) ώστε να περιλάβουν και τα χαρακτηριστικά ασφαλείας.

3.8.2.4. *Συστημικές προσεγγίσεις*

Στην κατηγορία αυτή ανήκουν οι μεθοδολογίες που προσπαθούν να αποφύγουν το φαινόμενο του δυϊσμού κάνοντας χρήση της συστημικής οπτικής, εξετάζοντας δηλαδή, το αντικείμενο ολιστικά. Δύο ερευνητικές προσπάθειες ανήκουν στην κατηγορία αυτή, η Ιδεατή Μεθοδολογία και η προσέγγιση του Βιώσιμου Συστήματος.

Η Ιδεατή Μεθοδολογία (Virtual Methodology) για την ασφάλεια ενός πληροφοριακού

συστήματος προτάθηκε από την Jean Hitchings (1995) και λαμβάνει υπόψη της τόσο τα τεχνικά, όσο και τα οργανωσιακά θέματα. Στηρίζεται στη μεταφορά της συστημικότητας από το φυσικό κόσμο, δηλαδή το αντικείμενο παρατήρησης (οργανισμό), στη μεθοδολογία. Για το λόγο αυτό, η Ιδεατή Μεθοδολογία αποτελείται από φάσεις σε αλληλεπίδραση, οι οποίες δεν είναι απαραίτητο να εκτελεσθούν σειριακά, η μία μετά την άλλη.

Ίσως περισσότερο ορθόδοξη, από συστημικής πλευράς, είναι η οπτική του Βιώσιμου Συστήματος (Viable System) που εισηγούνται οι Karyda et.al. (2001). Εδώ οι ερευνητές εισηγούνται την απομάκρυνση από την «κλασική» θεώρηση της ασφάλειας, όπου κυριαρχούν τα τρία χαρακτηριστικά - εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και αντί αυτών προτείνουν τον όρο *«βιωσιμότητα»* του συστήματος.

Βασικοί παράγοντες επιτυχίας στην υλοποίηση της ασφάλειας[14]

Η εμπειρία δείχνει ότι οι ακόλουθοι παράγοντες έχουν ιδιαίτερη σημασία στην υλοποίηση της ασφάλειας πληροφοριών μέσα σε έναν οργανισμό:

- Πολιτική ασφάλειας, στόχοι και δραστηριότητες που αντικατοπτρίζουν τους στόχους του οργανισμού.
- Εφαρμογή διαδικασιών ασφάλειας με τρόπο συμβατό με την κουλτούρα του οργανισμού.
- Ενεργή υποστήριξη από τη διοίκηση του οργανισμού.
- Κατανόηση των απαιτήσεων ασφάλειας, της αποτίμησης κινδύνων και της διαχείρισης τους.
- Κατανόηση από όλο το προσωπικό του οργανισμού της αναγκαιότητας ύπαρξης και λειτουργίας μέτρων ασφάλειας.
- Γνώση της πολιτικής ασφάλειας από όλο το προσωπικό και τους εξωτερικούς συνεργάτες.
- Ενημέρωση και εκπαίδευση προσωπικού.
- Ένα κατανοητό και ισορροπημένο σύστημα μέτρησης που να μπορεί να αξιολογήσει την απόδοση του συστήματος ασφάλειας των πληροφοριών και να προτείνει πιθανές βελτιώσεις.

---

[14]ISO/IEC 17799:2005

3.9. Ποιότητα Ασφάλειας Πληροφοριακών Συστημάτων

Σύμφωνα με την επικρατούσα προσέγγιση, πρέπει πάντα να βρίσκεται μια ισορροπία μεταξύ της ποιότητας ασφάλειας που απαιτεί ο οργανισμός και του κόστους που μπορεί να αντέξει. Σε πολλές περιπτώσεις, υπάρχει μια άμεση σχέση μεταξύ του επιπέδου ποιότητας (ή της ανοχής για τις παραβιάσεις) και του κόστους του προγράμματος ασφάλειας. Επομένως, εάν υπάρχει περιορισμός στον προϋπολογισμό τότε θα πρέπει να ρυθμιστεί το πεδίο εφαρμογής της ασφάλειας ή της ποιότητάς της. Ευνόητο είναι, σύμφωνα με αυτήν την άποψη, να αποκτηθεί η υψηλότερη ποιότητα ασφάλειας που μπορεί να αντέξει οικονομικά ο οργανισμός, αναγνωρίζοντας ότι καμία λύση ασφάλειας δεν είναι πάντα απολύτως τέλεια.

Από την άλλη πλευρά υπάρχει η άποψη ότι, μια σαφέστερη κατανόηση της ασφάλειας μπορεί να οδηγήσει όχι μόνο στην αύξησή της, αλλά και στο χαμηλότερο κόστος. Υπάρχουν πολλές σημαντικές ομοιότητες μεταξύ των προσπαθειών για Διοίκηση Ολικής Ποιότητας και του αυξανόμενου ενδιαφέροντος για το κόστος και την ποιότητα της ασφάλειας στους οργανισμούς και τις επιχειρήσεις σήμερα. Στο παρελθόν, θεωρήθηκε ότι έπρεπε να γίνει επιλογή μεταξύ της βελτίωσης της ποιότητας και της μείωσης του κόστους. Η ΔΟΠ έδειξε ότι ήταν δυνατό να βελτιωθεί και η ποιότητα και η αποδοτικότητα δαπανών (cost efficiency). Υπάρχει η άποψη που βλέπει τώρα την ασφάλεια σαν ένα "πρόσθετο" κόστος (όπως κάποτε εξετάστηκε η βελτίωση ποιότητας), αλλά αυτή η άποψη αμφισβητείται (Madnick, Siegel, 2006).

Ένα σημαντικό πρώτο βήμα στην προσπάθεια για ΔΟΠ ήταν ο ακριβής προσδιορισμός του τι σημαίνει ακριβώς "ποιότητα", ειδικά κάτω από μια πιο ολιστική έννοια. Προκειμένου να σημειωθεί σοβαρή πρόοδος προς τη βελτίωση της ασφάλειας σε επιχειρησιακό επίπεδο, πρέπει να προσδιοριστεί η έννοια της επιχειρησιακής ασφάλειας (enterprise security) ολιστικά, και να αναπτυχθούν αποτελεσματικοί τρόποι αξιολόγησης και μέτρησής της.

Στις περισσότερες σύγχρονες επιχειρήσεις και οργανισμούς τα πληροφοριακά συστήματα καταλαμβάνουν ένα κεντρικό και ουσιαστικό μέρος των επιχειρησιακών λειτουργιών. Πολλοί δε από αυτούς εξαρτούνται ολοκληρωτικά από αυτά για να λειτουργήσουν και να επιβιώσουν. Η επιτυχής λειτουργία σε πολλούς οργανισμούς εξαρτάται από το πόσο καλά μπορούν να χρησιμοποιήσουν προσωπικό και πληροφορίες στο να προσφέρουν τις υπηρεσίες και προϊόντα με τρόπο

αποτελεσματικό και αποδοτικό. Λόγω αυτής της εξάρτησης, ο αυξανόμενος αριθμός των περιστατικών παραβίασης (violation) της ασφάλειας[15] των ΠΣ λόγω της "κακής" ποιότητας της ασφάλειας, αντιπροσωπεύουν μια σημαντική απειλή για τις επιχειρήσεις και τους οργανισμούς και συνεπώς για την οικονομία και την κοινωνία της χώρας συνολικά.

Κάθε παραβίαση (violation) ασφάλειας[16] ή απώλεια (loss) του ΠΣ έχει επίπτωση[17] (impact) στον οργανισμό που ακόμη μπορεί να οδηγήσει στην πλήρη διακοπή της λειτουργίας του. Αυτός ο κίνδυνος είναι ζήτημα ζωτικής σημασίας που πρέπει να αντιμετωπισθεί. Η διαθεσιμότητα, η αξιοπιστία, η ακεραιότητα και η εμπιστευτικότητα των ΠΣ είναι τα θεμελιώδη "ποιοτικά κριτήρια" οποιουδήποτε ΠΣ. Αυτά τα ποιοτικά κριτήρια καθορίζονται σύμφωνα με τις επιχειρησιακές ανάγκες και την αποδοχή, καθώς ο όρος ποιότητα ερμηνεύεται με βάση την προσωπική άποψη και κουλτούρα και μπορεί να εφαρμοστεί σε κάθε κοινωνικό τομέα συμπεριλαμβανομένων των Πληροφοριακών Συστημάτων και της ασφάλειας αυτών. (M. Devargas,1995:2)

Όταν εξετάζουμε την ασφάλεια ενός Πληροφοριακού Συστήματος, ουσιαστικά εξετάζουμε την ποιότητα των σχετικών διαδικασιών. Παραδείγματος χάριν, από τη ποιότητα της εκτέλεσης της διαδικασίας αξιολόγησης επικινδυνότητας (risk assessment) θα εξαρτηθεί στο πόσο καλά θα είναι προστατευμένο το ΠΣ.

Η ποιότητα και η ασφάλεια έχουν πολλά κοινά γνωρίσματα . Όπως ακριβώς με την ποιότητα, η ασφάλεια είναι δύσκολο να ποσοτικοποιηθεί ή να αναγνωρισθεί, επειδή το μέτρο της επιτυχίας της είναι η απουσία αποτυχίας. Η προσδοκία από ένα σύστημα ασφάλειας είναι η μηδενική αποτυχία και όχι η κατά 98 τις εκατό επιτυχία.

Βασική αρχή της ΔΟΠ είναι ότι: η λογική της ποιότητας δεν δέχεται ότι τα «λάθη» είναι ανθρώπινα αλλά στηρίζεται στην αρχή «χωρίς κανένα σφάλμα» ή «κάντο σωστά από την πρώτη στιγμή» (Μπουραντάς, 2002:516). Αυτή η αρχή εφαρμόζεται τόσο στην παραγωγή υπηρεσιών όσο και προϊόντων. Σύμφωνα με αυτή ο καθένας έχει τον έλεγχο της ποιότητας της δικής του εργασίας αλλά ταυτόχρονα εξαρτάται από την ποιότητα εργασίας των άλλων σε μια αλυσίδα ποιότητας.

Αυτή η αρχή αφορά άμεσα και είναι απαραίτητη στην ασφάλεια των Πληροφοριακών

---

[15]Παραβίαση: Γεγονός κατά το οποίο περιορίσθηκαν κάποιες από τις αυθεντικότητα, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, εγκυρότητα (Δ.Γκρίτζαλης, 2004)

[16]Παραβίαση: Γεγονός κατά το οποίο περιορίσθηκαν κάποιες από τις αυθεντικότητα, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, εγκυρότητα (Δ.Γκρίτζαλης, 2004)

[17]Επίπτωση: Απώλεια μιας αξίας, η αύξηση του κόστους ή άλλη ζημιά που μπορεί να προκύψει ως συνέπεια μιας παραβίασης

Συστημάτων καθώς αναφέρεται στην πρόληψη των Απειλών και των Αδυναμιών[18]. Οι Απειλές και οι Αδυναμίες μπορεί να είναι σκόπιμες ή τυχαίες, ανθρώπινες ή όχι. Οι σκόπιμες Απειλές προέρχονται από ανθρώπους, αλλά οι Απειλές και οι Αδυναμίες που προέρχονται από ανθρώπους δεν είναι όλες σκόπιμες (Γκρίτζαλης, 2004:28). Πολλές από αυτές προέρχονται από την έλλειψη κατανόησης των όρων ασφάλειας, την κακή ποιότητα λογισμικού, την έλλειψη κατάλληλων διαδικασιών και πρακτικών εργασίας, τους ανεπαρκείς ελέγχους και ακόμη ανεπαρκείς διαδικασίες αποκατάστασης καταστροφής (disaster recovery). Τα περισσότερα από αυτά τα προβλήματα μπορούν να αποφευχθούν εάν υπάρξει η κατάλληλη φροντίδα και προσοχή. Η ανάπτυξη της φιλοσοφίας «χωρίς κανένα σφάλμα» ή «κάντο σωστά από την πρώτη στιγμή», η ατομική ευθύνη για ποιότητα ασφάλειας και οι διαδικασίες ποιότητας μπορούν θα ελαχιστοποιήσουν το επίπεδο της απειλής. Όλα αυτά είναι προβλήματα διοίκησης τα οποία έχει σαν στόχο να επιλύει η Διοίκηση Ολικής Ποιότητας.

Όπως για την Διοίκηση Ολικής Ποιότητας ο ανθρώπινος παράγοντας είναι συνιστώσα ποιοτικής και αναπτυξιακής διαδικασίας (Κέφης, 2005:78), έτσι και για την ασφάλεια, η οποία αντιμετωπίζει διαρκώς νέες προκλήσεις λόγω της συνεχούς εξέλιξης των νέων τεχνολογιών, απαιτείται σημαντική αναβάθμιση του ανθρώπινου δυναμικού. Απαιτείται ο επαναπροσδιορισμός του ρόλου των εργαζομένων, και οι συμμετοχικές διαδικασίες αποτελούν τη συνιστώσα για τη διαρκή αναβάθμιση και τη βελτίωση των διαδικασιών ασφάλειας. Η διατήρηση της ασφάλειας στους οργανισμούς και τις επιχειρήσεις σήμερα επικεντρώνεται στο να ελαχιστοποιηθούν όσο το δυνατό οι εσωτερικές απειλές και η αμέλεια, και να αντιμετωπισθούν οι επιθέσεις από το εξωτερικό του οργανισμού.

Σε μια έρευνα του 2006 για τα μέλη του Ιδρύματος Ασφάλειας Υπολογιστών Computer Security Institute (CSI), που πραγματοποιήθηκε από κοινού από CSI και το U.S. Federal Bureau of Investigation, το 30 τοις εκατό των μεγάλων επιχειρήσεων που αποκρίθηκαν στην έρευνα είπαν ότι οι απειλές από το εσωτερικό των οργανισμών τους ήταν η αιτία τουλάχιστον του 50 τοις εκατό των απωλειών τους λόγω ρηγμάτων[19] ασφάλειας (security breaches) το 2005.

Ομοίως, στο περιοδικό CSO Magazine/Cisco μια ψηφοφορία μεταξύ των chief

---

[18] Αδυναμία: Χαρακτηριστικό ενός πληροφοριακού συστήματος που μπορεί να επιτρέψει να συμβεί μια παραβίαση.
[19] Ρήγμα Ασφάλειας: Μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση ή απόκρυψη πληροφοριών

security officers (CSOs), περίπου το 59 τοις εκατό ανάφερε τα λάθη των υπαλλήλων σαν την υπαριθμό ένα απειλή, ενώ το 37 τοις εκατό ανέφερε τη δολιοφθορά των υπαλλήλων ή των συνεργατών ως την υπαριθμό ένα απειλή (CISCO,2007).

Από όσα προαναφέρθηκαν γίνεται σαφές ότι ο δρόμος για τη Ποιοτική Ασφάλεια περνά μέσα από την επίτευξη της ποιότητας στο ανθρώπινο δυναμικό της επιχείρησης ή του οργανισμού. Για να συμβεί κάτι τέτοιο είναι απαραίτητη η επικοινωνία, η ομαδική εργασία, η συμμετοχή των εργαζομένων στη λήψη των αποφάσεων (για θέματα κυρίως μικρότερης σημασίας), η εκπαίδευση-κατάρτιση και η παροχή κινήτρων. Οι εργαζόμενοι πρέπει να γίνουν κοινωνοί των θεμάτων που έχουν σχέση με το «ποιοτικό ζήτημα της ασφάλειας» προκειμένου να αποφευχθούν φαινόμενα ελλιπούς καθοδήγησης, σύγχυσης, λαθών, αμελειών, απώλειας ενδιαφέροντος και εντέλει δημιουργίας Παραβιάσεων Ασφάλειας. Οι άνθρωποι χρειάζονται ενθάρρυνση ώστε να ελέγχουν και να βελτιώνουν τις διαδικασίες ασφαλείας στις οποίες εμπλέκονται και σχετίζονται με τη σφαίρα των ευθυνών τους. Ο ανθρώπινος παράγοντας αποτελεί ένα ιδιαίτερα υψηλής αξίας στοιχείο που επηρεάζει τη βιωσιμότητα του οργανισμού και για το λόγο αυτόν πρέπει να προσεχθεί ιδιαίτερα.

Η ασφάλεια, επομένως, είναι και διοικητικό πρόβλημα και όχι αποκλειστικά ένα πρόβλημα τεχνολογίας (Devargas, 1995:66)! Η έλλειψη καθοδήγησης και δέσμευσης εκ μέρους της διοίκησης θα δημιουργήσει ένα κλίμα αβεβαιότητας που οδηγεί σε ανεπαρκή και ακατάλληλα μέτρα ασφάλειας.

Συνεπώς αφού η ποιότητα ασφάλειας είναι και διοικητικό πρόβλημα που για την επίλυσή του προϋποθέτει ποιότητα και συμμετοχή του ανθρώπινου δυναμικού του οργανισμού, η εφαρμογή των αρχών της Διοίκησης Ολικής Ποιότητας στον οργανισμό είναι απαραίτητη.

Κεφάλαιο 4

Μοντέλο Συστήματος Διαχείρισης Ασφάλειας Ολικής Ποιότητας ΠΣ

4.1. Εισαγωγή

Στο κεφάλαιο αυτό, στα πλαίσια της συστημικής αλλά και ποιοτικής προσέγγισης της ασφάλειας, αναπτύσσεται ένα μοντέλο με το όνομα Σύστημα Διαχείρισης Ασφάλειας Ολικής Ποιότητας (Total Security Quality Managemet System TSQMS) το οποίο ουσιαστικά στηρίζεται στο πρότυπο ISO/IEC 27001:2005 και που απαιτεί ένα περιβάλλον λειτουργίας στο οποίο εφαρμόζονται οι αρχές της Διοίκησης Ολικής Ποιότητας. Το προτεινόμενο μοντέλο έχει δυνατότητα εφαρμογής του σε κάθε είδους Δημόσιο Οργανισμό και Υπηρεσία, αφού περιλαμβάνει, με πληρότητα, βασικούς κανόνες ακολουθητέας πρακτικής για επίτευξη αποτελεσματικής διαχείρισης της ασφάλειας Πληροφοριακών Συστημάτων.

Στα πλαίσια αυτά αφού γίνει μια αναφορά στους λόγους αναγκαιότητας και στα οφέλη ενός Συστήματος Διαχείρισης Ασφάλειας, στη συνέχεια αναπτύσσεται το μοντέλο TSQMS.

4.2. Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

Η πληροφορία που παράγει ή διαχειρίζεται ένας οργανισμός κατά την λειτουργία του, είναι ένα αντικείμενο ζωτικής σημασίας. Αυτό ισχύει σε μικρότερο ή μεγαλύτερο βαθμό για όλους τους οργανισμούς ανεξάρτητα από το είδος, το μέγεθος, και τον επιχειρησιακό κλάδο στον οποίο δραστηριοποιείται ο κάθε οργανισμός. Για τον λόγο αυτό, είναι ιδιαίτερα σημαντικό θέμα, η προστασία της πληροφορίας του οργανισμού. Η πληροφορία εδώ νοείται με την πλέον γενική της έννοια και μπορεί να διατίθεται σε διάφορες μορφές όπως, έντυπη ή χειρόγραφη σε χαρτί, σε ηλεκτρονική μορφή, αποθηκευμένη σε συστήματα υπολογιστών ή διακινούμενη σε δίκτυα κάθε είδους, μέσω ηλεκτρονικού ταχυδρομείου ή άλλων υπηρεσιών. Επίσης η πληροφορία μπορεί να επιδεικνύεται σε παρουσιάσεις με διαφάνειες ή films, ή ακόμη να παράγεται σε προφορική μορφή κατά την διάρκεια συζητήσεων.

Στον σημερινό ιδιαίτερα ανταγωνιστικό χώρο των επιχειρήσεων (αλλά και των οργανισμών κάθε τύπου), η πληροφορία είναι ένα επαπειλούμενο αντικείμενο και οι

απειλές μπορούν να προέρχονται από πολλές πηγές. Οι απειλές αυτές μπορούν να είναι εσωτερικές ή εξωτερικές. Μπορούν να είναι συμπτωματικές ή να προέρχονται από ηθελημένη κακή πρόθεση πρόκλησης ζημιών στον οργανισμό.

Ιδιαίτερα μετά τις εξελίξεις των τεχνολογιών πληροφορικής και επικοινωνιών και την ευρεία ανάπτυξη και χρήση εταιρικών δικτύων και εφαρμογών όπως το ηλεκτρονικό ταχυδρομείο, οι συναλλαγές μέσω του διαδικτύου, κλπ, οι απειλές κατά της πληροφορίας ενός οργανισμού, έχουν πολλαπλασιασθεί. Υπάρχει λοιπόν η ανάγκη για κάθε οργανισμό να προστατέψει την ζωτική του πληροφορία, καθώς και την πληροφορία που αφορά τους πελάτες του, αναπτύσσοντας την κατάλληλη Πολιτική Ασφάλειας Πληροφοριών και λαμβάνοντας όλα τα απαραίτητα μέτρα για την υλοποίησή της. Για τον σκοπό αυτό απαιτείται η ανάπτυξη και ενσωμάτωση στην λειτουργία του οργανισμού, ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System–ISMS) είναι μια συνολική και συστηματική προσέγγιση του οργανισμού στην διαχείριση της ευαίσθητης πληροφορίας του και των κινδύνων που την απειλούν, έτσι ώστε η πληροφορία να παραμένει ασφαλής.

Ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών είναι ένα σύστημα διοίκησης που επιδρά στο σύνολο του οργανισμού και περιλαμβάνει το προσωπικό, τις διαδικασίες και στα Πληροφοριακά Συστήματα του οργανισμού. Επίσης, ένα τέτοιο σύστημα μπορεί να ενσωματωθεί σε οργανισμούς κάθε είδους, μεγέθους, ή επιχειρησιακού κλάδου. Από την άποψη αυτή, ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών εμφανίζει αρκετές ομοιότητες με ένα Σύστημα Διοίκησης Ποιότητας. Σε πολλές περιπτώσεις ένας οργανισμός αναπτύσσει ταυτόχρονα και συνδυασμένα, το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών μαζί με το Σύστημα Διοίκησης Ποιότητας.

4.3. Η αναγκαιότητα του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

Όπως δηλώνουν εμπειρογνώμονες ασφάλειας αλλά και επιβεβαιώνουν οι στατιστικές (ENISA, 2006):

- οι διαχειριστές ασφάλειας ΠΣ αφιερώνουν περίπου μόνο το 1/3 του χρόνου τους στην εξέταση των τεχνικών πτυχών της ασφάλειας. Τα υπόλοιπα 2/3 αναλώνονται στην ανάπτυξη πολιτικών και διαδικασιών, στην εκτέλεση

αναθεωρήσεων της ασφάλειας, στην διεξαγωγή αναλύσεων επικινδυνότητας, στην εξέταση των σχεδίων συνέχισης λειτουργίας και στην προώθηση της ενημέρωσης για την ασφάλεια

- η ασφάλεια εξαρτάται περισσότερο από τους ανθρώπους παρά από την τεχνολογία
- οι υπάλληλοι του οργανισμού αποτελούν μια πολύ μεγαλύτερη απειλή για την ασφάλεια πληροφοριών απ'ό,τι οι ξένοι
- η ασφάλεια είναι όπως μια αλυσίδα. Είναι τόσο ισχυρή όσο ο πιο αδύνατος κρίκος της
- ο βαθμός ασφάλειας εξαρτάται από τρεις παράγοντες: τον κίνδυνο που ο οργανισμός είναι πρόθυμος να αναλάβει, τη λειτουργικότητα του συστήματος και το κόστος που είναι διατεθειμένος να πληρώσει
- η ασφάλεια δεν είναι μια κατάσταση ή ένα στιγμιότυπο αλλά μια διαρκής διαδικασία.

Αυτά τα γεγονότα οδηγούν αναπόφευκτα στο συμπέρασμα ότι:

Η διαχείριση ασφάλειας είναι ένα ζήτημα διοίκησης και ΟΧΙ ένα καθαρώς τεχνικό ζήτημα.

Οι ωφέλειες για έναν οργανισμό από την εισαγωγή ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών είναι σημαντικές και πολλαπλές. Ενδεικτικά αναφέρονται οι εξής ωφέλειες από την εφαρμογή ενός τέτοιου συστήματος:

- ✓ Αξιοπιστία, εμπιστευτικότητα και δημιουργία εμπιστοσύνης από την πλευρά των πελατών ως αποτέλεσμα της ασφάλειας της πληροφορίας που αφορά τους πελάτες.
- ✓ Εξοικονόμηση κόστους λόγω της μείωσης των κινδύνων απώλειας πληροφοριών ή κοινοποίησης εμπιστευτικής πληροφορίας σε τρίτους. Το κόστος της παραβίασης της ασφάλειας πληροφοριών με οποιονδήποτε τρόπο, μπορεί να είναι σημαντικό. Η εφαρμογή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών δίνει σημαντική αξία στον οργανισμό και έχει ιδιαίτερα θετικές επιπτώσεις στην στάση των επενδυτών ή των μετόχων και του κοινού.
- ✓ Συμμόρφωση με το κανονιστικό πλαίσιο περί χειρισμού δεδομένων. Η εφαρμογή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών αντιμετωπίζει με συστηματικό τρόπο όλα τα θέματα συμμόρφωσης με την σχετική νομοθεσία.

- ✓ Διασφάλιση και επίδειξη δέσμευσης σε όλα τα επίπεδα του οργανισμού.

4.4. Οφέλη ενός ISMS σύμφωνα με το ISO 27001

Συνοπτικά τα οφέλη για έναν οργανισμό από την υιοθέτηση ενός Συστήματος Διοίκησης Ασφάλειας Πληροφοριών είναι σημαντικά και πολλαπλά. Ενδεικτικά αναφέρονται τα εξής:

- ✓ αποδεικνύει τη συμμόρφωση με τις απαιτήσεις του προτύπου ISO/IEC 27001:2005.
- ✓ παροχή διαβεβαίωσης στους διευθυντές και στα ενδιαφερόμενα μέρη ότι η επιχείρηση συμμορφώνεται με την υπάρχουσα νομοθεσία.
- ✓ βελτιώνει την αξιοπιστία και ενισχύει την εμπιστοσύνη πελατών.
- ✓ αποδεικνύει τη δέσμευση της ανώτερης διοίκησης για την ασφάλεια των πληροφοριών ενός οργανισμού.
- ✓ δέσμευση του προσωπικού και βελτίωση της κουλτούρας ασφάλειας των πληροφοριών στην εργασία.
- ✓ παρέχει την ευκαιρία για τη συνεχή βελτίωση μέσω των συστηματικών επιθεωρήσεων.
- ✓ εξασφάλιση της αποτελεσματικής ολοκλήρωσης των θεμάτων διαχείρισης της ασφάλειας των πληροφοριών με άλλα διαχειριστικά συστήματα (π.χ. ISO 9001:2000).
- ✓ μείωση του κόστους – από άμεσα κόστη π.χ. κλοπή φορητού υπολογιστή, και από έμμεσα κόστη π.χ. φήμη, νομικές απώλειες.
- ✓ παροχή ανταγωνιστικού πλεονεκτήματος και αναβάθμιση της εικόνας του Οργανισμού

Για την ανάπτυξη και εφαρμογή Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών, υπάρχουν δύο αλληλοσυμπληρούμενα πρότυπα:

- Οι απαιτήσεις που πρέπει να πληρούνται από ένα σύστημα διαχείρισης ασφάλειας παρέχονται από τα πρότυπα ISO/IEC 27001:2005 "Information Security Management Systems – Requirements" και BS 7799-2:2002
- Οι κατευθυντήριες οδηγίες για το πώς θα μπορούσαν να καλυφθούν αυτές οι απαιτήσεις περιέχονται στα πρότυπα ISO/IEC 17799:2005 "Code of practice for information security management" και BS 7799-1:2002.

Υπάρχει μια σειρά από πρότυπα που μπορούν να βοηθήσουν σε κάθε ένα τα επιμέρους στάδια της δημιουργίας του συστήματος (π.χ. ISO 13335, ISO 12207, ISO 18045, ISO 15408 κ.α.)

4.5. Σύστημα Διαχείρισης Ασφάλειας Ολικής Ποιότητας TSQMS[20]

Για την ανάπτυξη (establishing), την εφαρμογή (implementing), την λειτουργία (operating), τον έλεγχο (monitoring), την αναθεώρηση (reviewing), τη διατήρηση (maintaining) και τη βελτίωση (improving) ενός Συστήματος Διαχείρισης Ασφάλειας Ολικής Ποιότητας ΠΣ (TSQMS), μπορεί να εφαρμοσθεί ένα μοντέλο όπως αυτό που προβλέπεται στο ISO/IEC 27001:2005. Η υιοθέτηση ενός TSQMS πρέπει να είναι μια στρατηγική απόφαση για ένα οργανισμό. Ο σχεδιασμός και η εφαρμογή ενός TSQMS επηρεάζονται από τις ανάγκες, τους στόχους, τις απαιτήσεις ασφάλειας, τις διαδικασίες που χρησιμοποιούνται, το μέγεθος και τη δομή του οργανισμού. Η εφαρμογή ενός TSQMS θα επιφέρει αλλαγές στον οργανισμό και στα συστήματα υποστήριξής του. Το TSQMS θα διαμορφωθεί σύμφωνα με τις ανάγκες της οργανισμού.

Υιοθετείται η προσέγγιση της διεργασίας για την ανάπτυξη, την εφαρμογή, τη λειτουργία, τον έλεγχο, την αναθεώρηση, τη συντήρηση και τη βελτίωση του TSQMS ενός οργανισμού. Ένας οργανισμός πρέπει να προσδιορίσει και να διαχειρισθεί πολλές δραστηριότητες προκειμένου να λειτουργήσει αποτελεσματικά. Οποιαδήποτε δραστηριότητα που διαχειρίζεται και χρησιμοποιεί πόρους προκειμένου να μετασχηματιστούν οι εισροές σε εκροές, μπορεί να θεωρηθεί ως μια διεργασία. Συχνά η εκροή από μια διεργασία διαμορφώνει άμεσα την εισροή σε μια επόμενη διεργασία. Η εφαρμογή ενός συστήματος από διεργασίες μέσα σε ένα οργανισμό, μαζί με τον προσδιορισμό, τις αλληλεπιδράσεις αυτών των διεργασιών, και τη διαχείρισή τους, αναφέρονται ως "προσέγγιση διεργασίας".

Η προσέγγιση διεργασίας για τη διαχείριση ασφάλειας πληροφοριών υπογραμμίζει τη σημασία:

a) της κατανόησης των απαιτήσεων ασφάλειας πληροφοριών ενός οργανισμού και της ανάγκης για τη καθιέρωση της πολιτικής και των στόχων για την ασφάλεια πληροφοριών

---

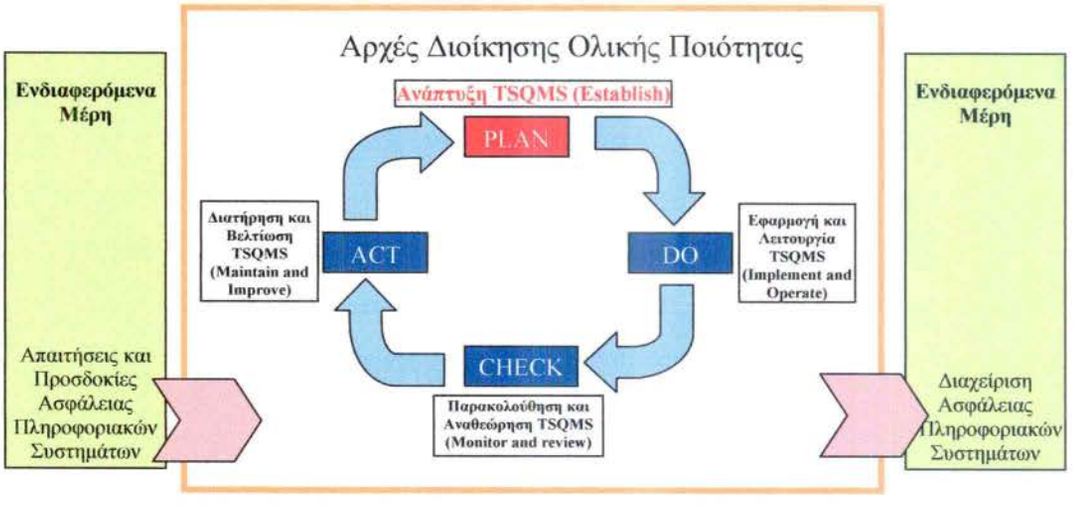
[20] Το κείμενο στο μεγαλύτερο μέρος του προέρχεται από το ISO/IEC 27001:2005

b) την εφαρμογή και τη λειτουργία ελέγχων για τη διαχείριση των κινδύνων ασφάλειας πληροφοριών στα πλαίσια των γενικών επιχειρησιακών κινδύνων του οργανισμού

c) τον έλεγχο και την αναθεώρηση της απόδοσης και της αποτελεσματικότητας του TSQMS και

d) τη συνεχή βελτίωση βασισμένη στην αντικειμενική μέτρηση.

Το μοντέλο "Plan-Do-Check-Act" (PDCA), εφαρμόζεται σε όλες τις διεργασίες του TSQMS. Όμως το TSQMS απαιτεί την ύπαρξη ενός περιβάλλοντος λειτουργίας στο οποίο εφαρμόζονται οι αρχές της Διοίκησης Ολικής Ποιότητας. Δηλαδή απαιτείται πριν αναπτυχθεί ένα σύστημα TSQMS να έχει εφαρμοσθεί με επιτυχία στον οργανισμό ένα μοντέλο Διοίκησης Ολικής Ποιότητας. Αυτό μπορεί να είναι είτε το EFQM, είτε το σχεδιασμένο για Δημόσιους Οργανισμούς CAF, είτε το ISO 9000. Το σχήμα 7 επεξηγεί πώς ένα TSQMS λειτουργώντας σε ένα περιβάλλον Διοίκησης Ολικής Ποιότητας, παίρνει ως εισροές τις απαιτήσεις ασφάλειας των Πληροφοριακών Συστημάτων και τις προσδοκίες των ενδιαφερόμενων μερών, και μέσω των απαραίτητων ενεργειών και διεργασιών παράγει σαν εκροή την ασφάλεια των Πληροφοριακών Συστημάτων που ικανοποιεί αυτές τις απαιτήσεις και προσδοκίες.
Αυτό το μοντέλο πρότυπο παρέχει ένα ισχυρό πεδίο για την εφαρμογή των αρχών και των οδηγιών για τη διαχείριση της αποτίμησης επικινδυνότητας, το σχεδιασμό και την εφαρμογή της ασφάλειας, τη διαχείριση και την επαναξιολόγηση της ασφάλειας.



Σχήμα 7: Μοντέλο Διαχείρισης Ολικής Ποιότητας Ασφάλειας TSQMS

4.6. Διαφορές του TSQMS από το ISMS του ISO

Η φιλοσοφία του ISO στηρίζεται στη χρήση προδιαγραφών που διέπουν μέρος ή το σύνολο των διεργασιών που λαμβάνουν χώρα στον οργανισμό αυτόν. Ο καθορισμός των προδιαγραφών και η συμμόρφωση με αυτές επιτυγχάνεται με την βοήθεια ενός λιγότερο ή περισσότερο γραφειοκρατικού συστήματος σύμφωνα με τις οδηγίες του προτύπου (διαδικασίες, έντυπα καταγραφής και οδηγίες εργασίας), καθώς και από εσωτερικούς και κυρίως εξωτερικούς ελέγχους. Η γραφειοκρατική δομή του ISO δίνει τη δυνατότητα στην υφιστάμενη γραφειοκρατία των Δημόσιων Οργανισμών να ενσωματωθεί, να λειτουργήσει και να βοηθήσει την υπόθεση της ποιότητας αντί να την καταπνίγει.

Ένα ΣΔΠ όπως το ISO προσφέρει στον οργανισμό έναν οδηγό για την καθημερινή λειτουργία του σύμφωνα με τις προδιαγραφές και τους όρους που αυτός θέτει, αλλά πάντα σε απόλυτη συμβατότητα με τους περιορισμούς του προτύπου. Αυτό όμως πιθανότατα στραγγαλίζει και περιορίζει τον οργανισμό και το ανθρώπινο δυναμικό του οργανισμού αναφορικά με θέματα ευελιξίας, πρωτοβουλιών και καινοτομίας στην αντιμετώπιση των κινδύνων, καθώς οι κίνδυνοι διαρκώς μεταβάλλονται και συνεχώς νέοι εμφανίζονται. Το ISO έχει υιοθετήσει κάποιες από τις αρχές της ΔΟΠ αλλά στη συνέχεια αφήνεται στην ευχέρεια του οργανισμού αν και ποιες άλλες θα υιοθετήσει στις επιμέρους διεργασίες και διαδικασίες. Για παράδειγμα δεν απαιτείται η αλλαγή στη συμπεριφορά, στον τρόπο αντιμετώπισης και στις εργασιακές πρακτικές, όταν η προσωπική συνεισφορά του κάθε εργαζόμενου συμβάλλει στην αλλαγή της νοοτροπίας και της οργανωτικής κουλτούρας. Δεν προσεγγίζεται το κρίσιμο ζήτημα της κουλτούρας ασφάλειας. Δεν απαιτείται από τη διοίκηση να αναλάβει προσωπικά την ηγεσία της προσπάθειας για ασφάλεια και να παρέχει καθοδήγηση δίνοντας πρώτη το παράδειγμα. Αντιμετωπίζει συμβατικά τους εργαζόμενους όταν ο καθένας από αυτούς είναι ένας κρίκος στην αλυσίδα της ασφάλειας, ο οποίος θα πρέπει να είναι συνειδητοποιημένος και να νοιώθει υπεύθυνος για αυτό που κάνει και που δεν διστάζει να επισημαίνει τα προβλήματα τους συστήματος, παίρνοντας ακόμη και πρωτοβουλίες αντιμετώπισής τους. Στη δε κρίσιμη διεργασία εκπαίδευση-ενημέρωση αυτή δεν αντιμετωπίζεται σαν επένδυση αλλά μάλλον σαν απαραίτητη δαπάνη.

Εκείνο που διαφοροποιεί την ποιότητα ασφάλειας από την ποιότητα υπηρεσιών ή προϊόντων είναι ότι ακόμη και το λάθος ή αμέλεια ενός ανθρώπου, μπορεί να έχει

καταστροφικές επιπτώσεις στα δεδομένα, στη λειτουργία και στη φήμη του οργανισμού[21].

Έτσι το μοντέλο TSQMS υιοθετεί απόλυτα το σχετικό μοντέλο του ISO για τα πλεονεκτήματά του, αλλά ταυτόχρονα υιοθετεί τις αρχές της Διοίκησης Ολικής Ποιότητας σε όλες τις διεργασίες με σημαντικότερη αυτή της αποτίμησης επικινδυνότητας. Ιδιαίτερα δίνεται έμφαση στην κουλτούρα ασφάλειας και στην εκπαίδευση-ενημέρωση του προσωπικού, στηριζόμενο σε έγγραφα και συστάσεις του Ευρωπαϊκού Οργανισμού ΟΟΣΑ[22] και της ENISA[23].

Επίσης το μοντέλο TSQMS απαιτεί πριν την εφαρμογή του, να έχει προηγηθεί η ανάπτυξη ενός περιβάλλοντος αρχών ΔΟΠ με την εφαρμογή ενός μοντέλου όπως το ΚΠΑ (CAF), δεδομένου του ότι είναι μάλλον αδύνατο να αναπτυχθεί μια κουλτούρα ασφάλειας, χωρίς να προϋπάρχει μια κουλτούρα ποιότητας στον οργανισμό ή να αναπτυχθεί ένα Σύστημα Διαχείρισης Ασφάλειας Ολικής Ποιότητας χωρίς να προϋπάρχει σε λειτουργία ένα Σύστημα Διοίκησης Ολικής Ποιότητας.

---

[21] Ανώνυμος (25-3-2008), 'Χάθηκαν προσωπικά δεδομένα 2.500 Αμερικανών' και 'Διαρροές σε 19 φορείς', ΚΟΣΜΟΣ kathimerini.gr

[22] Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (OECD)

[23] Η ENISA είναι μια αντιπροσωπεία της Ευρωπαϊκής Ένωσης που δημιουργήθηκε για να προωθήσει τη λειτουργικότητα της εσωτερικής αγοράς, συμβουλεύοντας και βοηθώντας τα κράτη μέλη, τους οργανισμούς και τις επιχειρήσεις της ΕΕ στο πώς να εξασφαλίσουν ένα υψηλό και αποτελεσματικό επίπεδο ασφάλειας δικτύων και πληροφοριών.

4.7. Ανάπτυξη και διαχείριση του TSQMS (Establishing Managing)

Ανάπτυξη της πολιτικής, των στόχων, των διεργασιών και των διαδικασιών διαχείρισης της επικινδυνότητας και βελτίωσης της ασφάλειας πληροφοριών για την παραγωγή αποτελεσμάτων σύμφωνα με τις γενικές πολιτικές και τους στόχους ενός οργανισμού.

4.7.1. **Σχεδιασμός (Plan)**

4.7.1.1. *Ανάπτυξη του TSQMS (Establish)*

Για την ανάπτυξη του TSQMS ο οργανισμός πρέπει να ακολουθήσει τα ακόλουθα βήματα.

a) Καθορισμός του πεδίου εφαρμογής (scope) και τα όρια του TSQMS σε αντιστοιχία με τα χαρακτηριστικά του οργανισμού, της θέσης του, των στοιχείων (assets) και της τεχνολογίας του, συμπεριλαμβανομένων των λεπτομερειών και της αιτιολόγησης για τις οποιεσδήποτε εξαιρέσεις από το πεδίο εφαρμογής.

b) Καθορισμός μιας Πολιτικής Ασφάλειας TSQMS σε αντιστοιχία με τα χαρακτηριστικά του οργανισμού, της θέσης του, των στοιχείων και της τεχνολογίας του που: (βλ. κεφ.5)

   1. περιλαμβάνει ένα πλαίσιο για τους τιθεμένους στόχους και που καθιερώνει ένα γενικό προσανατολισμό και τις αρχές δράσης αναφορικά με την ασφάλεια πληροφοριών
   2. λαμβάνει υπόψη τις επιχειρησιακές, τις νομικές ή ρυθμιστικές απαιτήσεις, και τις συμβατικές υποχρεώσεις ασφάλειας
   3. ευθυγραμμίζεται με το στρατηγικό risk management του οργανισμού στο γενικότερο πλαίσιο του οποίου θα γίνει η ανάπτυξη και διατήρηση του TSQMS
   4. καθιερώνει τα κριτήρια σε σχέση με τα οποία θα αξιολογηθεί ο κίνδυνος (4.7.1.1.c)) και
   5. έχει εγκριθεί από τη διοίκηση.

c) Καθορισμός της προσέγγισης για την αποτίμηση επικινδυνότητας (risk assessment) του οργανισμού (βλ. κεφ. 6).

Η μεθοδολογία αποτίμησης επικινδυνότητας που θα επιλεγεί θα πρέπει να εξασφαλίσει ότι οι αποτιμήσεις επικινδυνότητας θα παράγουν αποτελέσματα που μπορούν να είναι συγκρίσιμα και αναπαραγωγίσιμα .

ΣΗΜΕΙΩΣΗ: Υπάρχουν διάφορες μεθοδολογίες για την αποτίμηση επικινδυνότητας όπως για παράδειγμα αυτές που αναφέρονται σε έγγραφο της ENISA[24] (2006) "Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools". Επίσης παράδειγμα μεθοδολογίας αποτίμησης επικινδυνότητας υπάρχει στο ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Techniques for the management of IT Security.*

d) Προσδιορισμός των κινδύνων.
   1) Προσδιορισμός των στοιχείων (assets) στο πεδίο εφαρμογής του TSQMS, και των ιδιοκτητών αυτών των στοιχείων.
   2) Προσδιορισμός των απειλών γι αυτά τα στοιχεία.
   3) Προσδιορισμός των ευπαθειών που μπορούν να χρησιμοποιηθούν από τις απειλές.
   4) Προσδιορισμός των επιπτώσεων από την απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας που μπορούν να υπάρξουν για αυτά τα στοιχεία.

e) Ανάλυση και αξιολόγηση των κινδύνων.
   1) Αποτίμηση των επιχειρησιακών επιπτώσεων επάνω στον οργανισμό που μπορεί να προκύψουν από αποτυχίες ασφάλειας (security failures), λαμβάνοντας υπόψη τις συνέπειες από την απώλεια της εμπιστευτικότητας, της ακεραιότητας ή διαθεσιμότητας των στοιχείων.

---

[24] Η ENISA είναι μια αντιπροσωπεία της Ευρωπαϊκής Ένωσης που δημιουργήθηκε για να προωθήσει τη λειτουργικότητα της εσωτερικής αγοράς, συμβουλεύοντας και βοηθώντας τα κράτη μέλη, τους οργανισμούς και τις επιχειρήσεις της ΕΕ στο πώς να εξασφαλίσουν ένα υψηλό και αποτελεσματικό επίπεδο ασφάλειας δικτύων και πληροφοριών.

2) Αποτίμηση της ρεαλιστικής πιθανότητας να συμβούν αποτυχίες ασφάλειας, λαμβάνοντας υπόψη τις επικρατούσες απειλές και ευπάθειες, τις επιπτώσεις που συνδέονται με αυτά τα στοιχεία, καθώς και τα μέτρα ελέγχου που ήδη βρίσκονται σε εφαρμογή.
3) Εκτίμηση του επιπέδου των κινδύνων.
4) Καθορισμός για το εάν οι κίνδυνοι είναι αποδεκτοί ή απαιτούν αντιμετώπιση, χρησιμοποιώντας τα κριτήρια για την αποδοχή των κινδύνων που έχουν καθιερωθεί στο (βλ. 4.7.1.1.c)2)).

f) Προσδιορισμός και αξιολόγηση των επιλογών για την αντιμετώπιση των κινδύνων.

Πιθανές ενέργειες περιλαμβάνουν:

1) την εφαρμογή των κατάλληλων μέτρων ελέγχου (controls)
2) εσκεμμένη και αντικειμενική αποδοχή κινδύνων, που ικανοποιούν σαφώς τις πολιτικές του οργανισμού και τα κριτήρια αποδοχής κινδύνων (βλ. 4.7.1.1.c)2))
3) αποφυγή των κινδύνων, και
4) μεταφορά των σχετικών επιχειρησιακών κινδύνων σε άλλα συμβαλλόμενα μέρη, π.χ. ασφαλιστές, προμηθευτές.

g) Επιλογή των στόχων και των μέτρων ελέγχου για την αντιμετώπιση των κινδύνων.

Οι στόχοι και τα μέτρα ελέγχου πρέπει να επιλέγονται και να εφαρμόζονται, ώστε να καλύπτουν τις απαιτήσεις που προσδιορίζονται από τις διαδικασίες αποτίμησης και αντιμετώπισης επικινδυνότητας. Αυτή η επιλογή θα πρέπει να λάβει υπόψη τα κριτήρια για την αποδοχή των κινδύνων (βλ. 4.7.1.1.c)2)) καθώς επίσης και των νομικών, ρυθμιστικών και συμβατικών απαιτήσεων.

Στόχοι και τα μέτρα ελέγχου μπορεί να επιλεχθούν από το παράρτημα Α του προτύπου ISO/IEC 27001:2005, σαν μέρος αυτής της διαδικασίας και εφόσον είναι κατάλληλοι να καλύψουν προσδιορισμένες απαιτήσεις. Διαφορετικά πρέπει να επιλεχθούν άλλοι πρόσθετοι από άλλες πηγές.

ΣΗΜΕΙΩΣΗ: Το παράρτημα Α στο ISO 27001:2005 περιέχει έναν περιεκτικό κατάλογο στόχων και μέτρων ελέγχου ο οποίος μπορεί να χρησιμοποιηθεί σαν αφετηρία διασφαλίζοντας ότι δεν αγνοήθηκε κάποιο σημαντικό μέτρο ελέγχου κατά τη διαδικασία.

h) Λήψη της έγκρισης από τη διοίκηση σχετικά με τους προτεινόμενους παραμένοντες (χωρίς μέτρα ελέγχου) κινδύνους.

i) Λήψη της έγκρισης από τη διοίκηση για να εφαρμοστεί και να λειτουργήσει το TSQMS.

j) Προετοιμασία της έκθεσης εφαρμοσιμότητας (Statement of Applicability).

Μια έκθεση εφαρμοσιμότητας πρέπει να περιλαμβάνει τα εξής:

1) τους στόχους και τα μέτρα ελέγχου που επιλέχθηκαν (βλ. 4.7.1.1.g)) και τους λόγους για την επιλογή τους
2) τους στόχοι και τα μέτρα ελέγχου που ήδη εφαρμόζονται (βλ. 4.7.1.1.e)2)) και
3) τους στόχους και μέτρα ελέγχου του παραρτήματος Α που έχουν αποκλεισθεί και η αιτιολόγηση για τον αποκλεισμό τους.

ΣΗΜΕΙΩΣΗ: Η έκθεση εφαρμοσιμότητας παρέχει μια περίληψη των αποφάσεων σχετικά με την αντιμετώπιση του κινδύνου. Η αιτιολόγηση των αποκλεισμών εξασφαλίζει μέσω της διασταύρωσης, ότι κανένα μέτρο ελέγχου δεν έχει παραλειφθεί ακούσια.

4.7.2. **Εφαρμογή (DO)**

4.7.2.1. *Εφαρμογή και Λειτουργία TSQMS (Implement Operate)*

Εφαρμογή και λειτουργία της πολιτικής TSQMS, των μέτρων ελέγχου, των διεργασιών και των διαδικασιών.

Η οργανισμός πρέπει να κάνει τα ακόλουθα.

a) Να διατυπώσει ένα σχέδιο αντιμετώπισης κινδύνου που να προσδιορίζει την κατάλληλη διοικητική δράση, τους πόρους, τις ευθύνες και τις προτεραιότητες για τη διαχείριση των κινδύνων ασφάλειας πληροφοριών. (βλ. 4.9.).

b) Να εφαρμόσει το σχέδιο αντιμετώπισης κινδύνου προκειμένου να επιτευχθούν οι προσδιορισμένοι στόχοι ελέγχου, το οποίο περιλαμβάνει την εκτίμηση της χρηματοδότησης και την κατανομή των ρόλων και των ευθυνών.

c) Να εφαρμόσει τα μέτρα ελέγχου που επιλέχθηκαν (βλ. 4.7.1.1.g)) για να επιτύχει τους στόχους ελέγχου.

d) Να καθορίσει πώς θα μετρήσει την αποτελεσματικότητα των επιλεγμένων μέτρων ή της ομάδας μέτρων ελέγχου και να διευκρινίζει πώς αυτές οι μετρήσεις

πρόκειται να χρησιμοποιηθούν στο να αποτιμήσουν την αποτελεσματικότητα του μέτρου ώστε να παραγάγουν συγκρίσιμα και αναπαραγωγίσιμα αποτελέσματα (βλ. 4.7.3.1.c)).

ΣΗΜΕΙΩΣΗ: Η μέτρηση της αποτελεσματικότητας των μέτρων ελέγχου επιτρέπει στους διευθυντές και στο προσωπικό να προσδιορίσουν το πόσο καλά τα μέτρα ελέγχου επιτυγχάνουν στους στόχους ελέγχου για τους οποίους σχεδιάστηκαν.

e) Να δημιουργήσει την κατάλληλη κουλτούρα ασφάλειας στον οργανισμό (βλ. 4.9.2.2).
f) Να εφαρμόσει τα προγράμματα εκπαίδευσης και ενημέρωσης (βλ. 4.9.2.3).
g) Να διαχειριστεί τη λειτουργία του TSQMS.
h) Να διαχειριστεί τους πόρους για το TSQMS (βλ. 4.9.2).
i) Να εφαρμόσει διαδικασίες και άλλα μέτρα ελέγχου που να είναι ικανά ανιχνεύουν γρήγορα και να αντιμετωπίζουν τα συμβάντα ασφάλειας (βλ. 4.7.3.1.α)).

4.7.3. **Έλεγχος (Check)**

4.7.3.1. *Παρακολούθηση και Αναθεώρηση TSQMS (Monitor Review)*

Αποτίμηση και, όπου είναι δυνατό, μέτρηση της απόδοσης της διεργασίας σε σχέση με την πολιτική TSQMS, των στόχων και τη πρακτική εμπειρία και αναφορά των αποτελεσμάτων στη διοίκηση για αναθεώρηση.

Η οργανισμός πρέπει να κάνει τα ακόλουθα.

a) Να εκτελεί διαδικασίες γενικής παρακολούθησης (monitoring), επισκόπησης και άλλους ελέγχους ώστε:
   1) να ανιχνεύει αμέσως τα λάθη στα αποτελέσματα της επεξεργασίας
   2) να προσδιορίζει αμέσως τις απόπειρες και τις επιτυχείς παραβιάσεις και τα συμβάντα ασφάλειας
   3) να επιτρέπει στη διαχείριση να προσδιορίζει εάν οι δράσεις ασφάλειας που ανατίθενται σε ανθρώπους ή που εφαρμόζονται με τεχνολογικά μέσα εκτελούνται όπως θα έπρεπε
   4) να βοηθά στην ανίχνευση των συμβάντων ασφάλειας και με αυτόν τον τρόπο να αποτρέπει τα συμβάντα ασφάλειας με την χρήση δεικτών και

5) να προσδιορίζει εάν οι ενέργειες που έγιναν για να αντιμετωπίσουν μια παραβίαση της ασφάλειας ήταν αποτελεσματικές.

b) Να εκτελεί τις συνήθεις αναθεωρήσεις αποτελεσματικότητας του TSQMS (συμπεριλαμβανομένης της εκπλήρωσης της πολιτικής και των στόχων, και της αναθεώρησης των μέτρων ελέγχου ασφάλειας) λαμβάνοντας υπόψη τα αποτελέσματα των επιθεωρήσεων (audits) ασφάλειας, των συμβάντων, των αποτελεσμάτων από τις μετρήσεις αποτελεσματικότητας, των προτάσεων και της ανατροφοδότησης (feedback) από όλα τα ενδιαφερόμενα συμβαλλόμενα μέρη.

c) Να μετρά την αποτελεσματικότητα των μέτρων ελέγχου για να ελέγχει εάν οι απαιτήσεις ασφάλειας έχουν καλυφθεί.

d) Να αναθεωρεί τις αποτιμήσεις επικινδυνότητας σε προγραμματισμένα χρονικά διαστήματα και να αναθεωρεί τους υπολειπόμενους κινδύνους και τα προσδιορισμένα αποδεκτά επίπεδα κινδύνου, λαμβάνοντας υπόψη τις αλλαγές:

1) στην οργάνωση
2) στη τεχνολογία
3) σε προσδιορισμένες απειλές
4) στην αποτελεσματικότητα των εφαρμοσμένων μέτρων ελέγχου ασφάλειας και
5) σε εξωτερικά γεγονότα, όπως οι αλλαγές στο νομικό ή στο ρυθμιστικό περιβάλλον, αλλαγή στις συμβατικές υποχρεώσεις, και κοινωνικές αλλαγές.

e) Την εκτέλεση εσωτερικών επιθεωρήσεων (audits) του TSQMS σε προγραμματισμένα χρονικά διαστήματα (βλ. 4.10).

ΣΗΜΕΙΩΣΗ: Οι εσωτερικές επιθεωρήσεις, διεξάγονται είτε από τον ίδιο τον οργανισμό για εσωτερικούς λόγους ή εξ' ονόματός του από εξωτερικό παράγοντα.

f) Ανάληψη διαχειριστικής αναθεώρησης του TSQMS σε κανονική βάση για να διασφαλισθεί ότι το πεδίο εφαρμογής παραμένει επαρκές και ότι έχουν προσδιορισθεί οι βελτιώσεις στη διεργασία TSQMS (βλ. 4.11.1).

g) Αναβάθμιση σχεδίων ασφάλειας για να λάβουν υπόψη τα ευρήματα της παρακολούθησης και της επισκόπισης των δραστηριοτήτων.

h) Καταγραφή ενεργειών και γεγονότων που θα μπορούσαν να ασκήσουν επίδραση στην αποτελεσματικότητα ή στην απόδοση του TSQMS. (βλ. 4.8.3).

4.7.4. **Ενέργειες (Act)**

4.7.4.1. *Διατήρηση και Βελτίωση TSQMS (Maintain Improve)*

Λήψη διορθωτικών και προληπτικών μέτρων, βασισμένων στα αποτελέσματα του εσωτερικού ελέγχου του TSQMS ή της διαχειριστικής αναθεώρησης ή άλλων σχετικών πληροφοριών, για να επιτευχθεί η συνεχής βελτίωση του TSQMS.

Ο οργανισμός πρέπει να εκτελεί σε τακτική βάση τα ακόλουθα.

a) να εφαρμόζει τις προσδιορισμένες βελτιώσεις στο TSQMS.
b) να λαμβάνει κατάλληλα διορθωτικά και προληπτικά μέτρα σύμφωνα με 4.12.2. και 4.12.3. να εφαρμόζει τα μαθήματα από τα παθήματα ασφάλειας που προέρχονται από την εμπειρία άλλων οργανισμών αλλά και των δικών του.
c) να διαβιβάζει τις ενέργειες και τις βελτιώσεις σε όλα τα ενδιαφερόμενα μέρη σε ένα επίπεδο λεπτομέρειας κατάλληλο των περιστάσεων και όπως έχει συμφωνηθεί σχετικά.
d) να διασφαλίζει ότι οι βελτιώσεις επιτυγχάνουν τους στόχους για τους οποίους προορίζονται.

4.8. Απαιτήσεις τεκμηρίωσης

4.8.1. **Γενικά**

Η τεκμηρίωση πρέπει να περιλαμβάνει τα έγγραφα των αποφάσεων της διοίκησης, διασφαλίζοντας ότι οι ενέργειες ακολουθούν τις αποφάσεις της διοίκησης και τις πολιτικές. Είναι σημαντικό να είναι σε θέση να καταδείξει τη σχέση των επιλεγμένων μέτρων ελέγχου με τα αποτελέσματα των διαδικασιών αποτίμησης και αντιμετώπισης του κινδύνου και στη συνέχεια σε σχέση με την πολιτική και τους στόχους του TSQMS.

Η τεκμηρίωση TSQMS πρέπει να περιλαμβάνει:

a) καταγραμμένες δηλώσεις της πολιτικής και των στόχων του TSQMS (βλ. 4.7.1.1.b))
b) το πεδίο εφαρμογής του TSQMS (βλ. 4.7.1.1.a))
c) τις διαδικασίες και τα μέτρα έλεγχου υποστήριξης του TSQMS
d) μια περιγραφή της μεθοδολογίας αποτίμηση του κινδύνου (βλ. 4.7.1.1.c))
e) την έκθεση αποτίμησης του κινδύνου (βλ. 4.7.1.1.c) μέχρι (βλ. 4.7.1.1.g))

f) το σχέδιο αντιμετώπισης κινδύνου (βλ. τις 4.7.2.1.b))

g) οι καταγραμμένες διαδικασίες απαιτούνται από τον οργανισμό ώστε να εξασφαλίσει τον αποτελεσματικό σχεδιασμό, την υλοποίηση και τον έλεγχο των διαδικασιών ασφάλειας πληροφοριών και του πώς θα μετρήσει την αποτελεσματικότητα των μέτρων ελέγχου (βλ. τις 4.7.3.1.c))

h) τα αρχεία που απαιτούνται από το ISO (βλ. τις 4.8.3) και

i) την έκθεση εφαρμοσιμότητας.

4.8.2. Έλεγχος των εγγράφων

Τα έγγραφα που απαιτούνται από το TSQMS πρέπει να προστατεύονται και να ελέγχονται. Πρέπει να δημιουργηθεί μια καταγραμμένη διαδικασία για να καθορίσει τις διοικητικές ενέργειες που απαιτούνται για:

a) την έγκριση των εγγράφων ως προς την επάρκεια πριν την έκδοση

b) την αναθεώρηση και αναβάθμιση των εγγράφων

c) να εξασφαλίσει ότι προσδιορίζονται οι αλλαγές και η ισχύουσα αναθεώρηση

d) να εξασφαλίσει ότι οι σχετικές εκδόσεις των εγγράφων εφαρμογής είναι διαθέσιμες για χρήση

e) να εξασφαλίσει ότι τα έγγραφα παραμένουν ευανάγνωστα και κατανοητά

f) να εξασφαλίσει ότι τα έγγραφα είναι διαθέσιμα σε εκείνους που τα χρειάζονται, και μεταφέρονται, αποθηκεύονται και αποσύρονται σύμφωνα με τις σχετικές για την ταξινόμησή τους διαδικασίες

g) να εξασφαλίσει ότι προσδιορίζονται τα έγγραφα εξωτερικής προέλευσης

h) να εξασφαλίσει ότι η διανομή των εγγράφων είναι ελεγχόμενη

i) να αποτρέπει την κατά λάθος χρήση ξεπερασμένων εγγράφων και

j) εφαρμόσει τον κατάλληλο προσδιορισμό για αυτά που διατηρούνται για οποιοδήποτε σκοπό.

4.8.3. Έλεγχος των αρχείων

Τα αρχεία να αναπτύσσονται και να διατηρούνται για να παρέχουν τα στοιχεία της συμμόρφωσης στις απαιτήσεις και την αποτελεσματική λειτουργία του TSQMS. Αυτά θα πρέπει να προστατεύονται και να ελέγχονται. Το TSQMS θα πρέπει να λαμβάνει υπόψη οποιεσδήποτε σχετικές νομικές ή ρυθμιστικές απαιτήσεις και συμβατικές υποχρεώσεις. Τα αρχεία πρέπει να παραμείνουν ευανάγνωστα, κατανοητά και ανακτήσιμα. Οι έλεγχοι που απαιτούνται για τον προσδιορισμό, την

αποθήκευση, την προστασία, την ανάκτηση, το χρόνο διατήρησης και τη διάθεση των αρχείων να είναι τεκμηριωμένοι και να εφαρμόζονται.

Πρέπει να διατηρούνται αρχεία για τις διεργασίες ανάπτυξης και διαχείρισης του TSQMS και για όλα τα σημαντικά συμβάντα ασφάλειας

4.9. Ευθύνη της Διοίκησης

4.9.1. **Δέσμευση της Διοίκησης**

Η διοίκηση πρέπει να παρέχει στοιχεία για τη δέσμευσή της ως προς την ανάπτυξη, την εφαρμογή, την λειτουργία, τον έλεγχο, την αναθεώρηση, τη διατήρηση και τη βελτίωση του TSQMS μέσω της:

a) καθιέρωσης μιας πολιτικής TSQMS
b) εξασφάλισης ότι αναπτύσσονται οι στόχοι και τα σχέδια του TSQMS
c) καθιέρωσης των ρόλων και των ευθυνών για την ασφάλεια πληροφοριών
d) μετάδοσης στον οργανισμό της σημασίας της επίτευξης των στόχων της ασφάλειας πληροφοριών, στην συμμόρφωση με τη πολιτική ασφάλειας πληροφοριών, των ευθυνών βάσει του νόμου και της ανάγκης για συνεχή βελτίωση, παρέχοντας καθοδήγηση και δίνοντας το παράδειγμα, διαμορφώνοντας την κατάλληλη κουλτούρα ασφάλειας.
e) παροχής ικανοποιητικών πόρων για την ανάπτυξη, την εφαρμογή, την λειτουργία, τον έλεγχο, την αναθεώρηση, τη διατήρηση και τη βελτίωση του TSQMS. (βλ. τις 4.9.2.1.)
f) απόφασης για τα κριτήρια αποδοχής των κινδύνων και των αποδεκτών επιπέδων κινδύνου
g) με την εξασφάλιση ότι θα διεξάγονται οι εσωτερικές επιθεωρήσεις του TSQMS. (βλ. 4.10) και
h) με τη διεξαγωγή διοικητικών επισκοπήσεων του TSQMS. (βλ. 4.11).

4.9.2. **Διαχείριση Πόρων**

4.9.2.1. *Παροχή πόρων*

Ο οργανισμός πρέπει να καθορίσει και να παράσχει τους πόρους που απαιτούνται για: για την ανάπτυξη, την εφαρμογή, την λειτουργία, τον έλεγχο, την αναθεώρηση, τη διατήρηση και τη βελτίωση του TSQMS

a) την διασφάλιση ότι οι διαδικασίες ασφάλειας πληροφοριών υποστηρίζουν τις επιχειρησιακές απαιτήσεις
b) τον προσδιορισμό και την αντιμετώπιση των νομικών και ρυθμιστικών απαιτήσεων και τις συμβατικών υποχρεώσεων ασφάλειας
c) τη διατήρηση επαρκούς ασφάλειας με τη σωστή εφαρμογή όλων των αναγκαίων μέτρων ελέγχου
d) να διεξαγάγει αναθεωρήσεις όταν χρειάζεται και για να αντιδρά κατάλληλα στα αποτελέσματα αυτών των αναθεωρήσεων και
e) όπου απαιτείται, να βελτιώνει την αποτελεσματικότητα του TSQMS.

4.9.2.2. *Κουλτούρα ασφάλειας*

Ο οργανισμός απαιτείται να έχει μια κουλτούρα ασφάλειας που να είναι κυρίαρχη στο σύνολο της οργάνωσης, και που να ευθυγραμμίζει τους ανθρώπους και τις πρακτικές με τους στόχους ασφάλειας (βλ. κεφ. 7)

4.9.2.3. *Εκπαίδευση, ενημέρωση και ικανότητες*

Ο οργανισμός πρέπει να εξασφαλίσει ότι όλο το προσωπικό στο οποίο ανατίθενται καθήκοντα που καθορίζονται στο TSQMS είναι ικανό να εκτελέσει την αποστολή του μέσω:

a) του καθορισμού των απαραίτητων ικανοτήτων για το προσωπικό που εκτελεί εργασίες που επηρεάζουν το TSQMS
b) την παροχή εκπαίδευσης ή λαμβάνοντας άλλα μέτρα (π.χ. προσλαμβάνοντας ειδικό προσωπικό) που ικανοποιεί αυτές οι ανάγκες
c) Δημιουργία προγράμματος ενημέρωσης ασφάλειας σαν μια διαρκή επαναληπτική διαδικασία (βλ. κεφ. 8)
d) αξιολογώντας την αποτελεσματικότητα των δράσεων που γίνονται και
e) διατηρώντας αρχεία της εκπαίδευσης, της ενημέρωσης, των δεξιοτήτων, της εμπειρίας και των προσόντων (βλ. 4.8.3).

Ο οργανισμός πρέπει επίσης θα εξασφαλίσει ότι όλο το σχετικό προσωπικό είναι ενήμερο της σχετικότητας και της σπουδαιότητας των δραστηριοτήτων τους για την ασφάλεια των πληροφοριών και πώς να συμβάλλει στην επίτευξη των στόχων του TSQMS.

4.10. Εσωτερικές επιθεωρήσεις (audits)

Ο οργανισμός πρέπει να διεξάγει εσωτερικές επιθεωρήσεις του TSQMS σε προγραμματισμένα διαστήματα για να προσδιορίσει εάν οι στόχοι, τα μέτρα ελέγχου, οι διεργασίες και οι διαδικασίες του TSQMS:

a) είναι προσαρμοσμένα στις απαιτήσεις της σχετικής νομοθεσίας, των κανονισμών αλλά και των απαιτήσεων π.χ. του ISO
b) είναι προσαρμοσμένα στις προσδιορισμένες απαιτήσεις ασφάλειας
c) εφαρμόζονται αποτελεσματικά και διατηρούνται και
d) εκτελούνται όπως αναμένεται.

Ένα πρόγραμμα εσωτερικής επιθεώρησης πρέπει να προγραμματιστεί, λαμβάνοντας υπόψη τη κατάσταση και τη σημαντικότητα των διαδικασιών και των περιοχών που επιθεωρούνται, καθώς επίσης και τα αποτελέσματα των προηγούμενων επιθεωρήσεων. Πρέπει να καθορίζονται τα κριτήρια, το πεδίο, η συχνότητα και οι μέθοδοι της επιθεώρησης. Η επιλογή των επιθεωρητών και η εκτέλεση των επιθεωρήσεων πρέπει να εξασφαλίζουν την αντικειμενικότητα και την αμεροληψία της διαδικασίας επιθεώρησης. Οι επιθεωρητές δεν θα επιθεωρήσουν τη δική τους εργασία.

Οι ευθύνες και οι απαιτήσεις για τον σχεδιασμό και τη διεξαγωγή επιθεωρήσεων, για την υποβολή εκθέσεων των αποτελεσμάτων και για τη διατήρηση των αρχείων (βλ. 4.8.3.) πρέπει να καθορίζονται με μια τεκμηριωμένη διαδικασία.

Η αρμόδια διοίκηση της οποίας η περιοχή επιθεωρείται πρέπει να διασφαλίσει ότι οι ενέργειες θα εκτελούνται χωρίς αδικαιολόγητη καθυστέρηση που έχουν σκοπό να εξαλείψουν τις ανιχνεύσιμες μη συμμορφώσεις και τις αιτίες τους. Να ακολουθούν δραστηριότητες που να περιλαμβάνουν την επαλήθευση των ενεργειών που έγιναν λαμβάνονται και την υποβολή έκθεσης επί των αποτελεσμάτων επαλήθευσης. (βλ. 4.12.).

Σημείωση: Το ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing,* μπορεί να παρέχει χρήσιμες οδηγίες για την πραγματοποίηση των εσωτερικών επιθεωρήσεων TSQMS.

4.11. Αναθεώρηση του TSQMS από τη Διαχείριση

4.11.1. **Γενικά**

Η Διαχείριση πρέπει να προβαίνει σε αναθεώρηση του TSQMS του οργανισμού σε προγραμματισμένα διαστήματα (τουλάχιστον μία φορά το χρόνο) για να εξασφαλίσει τη διαρκή καταλληλότητα, την επάρκεια και την αποτελεσματικότητά του. Αυτή η αναθεώρηση πρέπει να περιλαμβάνει και ευκαιριακές αποτιμήσεις για τη βελτίωση και την ανάγκη για αλλαγές στο TSQMS, συμπεριλαμβανομένων των στόχων ασφάλειας και της πολιτικής ασφάλειας των πληροφοριών. Τα αποτελέσματα των αναθεωρήσεων πρέπει να τεκμηριώνονται επαρκώς και τα σχετικά αρχεία να διατηρούνται. (βλ. 4.8.3.).

4.11.2. **Εισροές της αναθεώρησης**

Οι εισροές στη διεργασία αναθεώρησης πρέπει να περιλαμβάνουν:

a) τα αποτελέσματα των επιθεωρήσεων του TSQMS και των αναθεωρήσεων
b) την ανατροφοδότηση από τα ενδιαφερόμενα συμβαλλόμενα μέρη
c) τεχνικές, προϊόντα ή διαδικασίες, οι οποίες θα μπορούσαν να χρησιμοποιηθούν στον οργανισμό για να βελτιώσουν την απόδοση και την αποτελεσματικότητα του TSQMS
d) κατάσταση των προληπτικών και διορθωτικών ενεργειών
e) ευπάθειες ή απειλές που δεν αντιμετωπίσθηκαν επαρκώς από την προηγούμενη αποτίμηση του κινδύνου
f) τα αποτελέσματα από τις μετρήσεις αποτελεσματικότητας
g) τις ενέργειες που ακολούθησαν τις προηγούμενες διαχειριστικές αναθεωρήσεις
h) οποιεσδήποτε αλλαγές που θα μπορούσαν να έχουν επιπτώσεις στο TSQMS; και
i) συστάσεις για βελτίωση.

4.11.3. **Εκροές αναθεώρησης**

Οι εκροές από τη διεργασία διαχειριστικής αναθεώρησης πρέπει να περιλαμβάνουν οποιεσδήποτε αποφάσεις και ενέργειες σχετικές με τα ακόλουθα.

a) Βελτίωση της αποτελεσματικότητας του TSQMS.

b) Αναβάθμιση του σχεδίου αποτίμησης και αντιμετώπισης του κινδύνου.

c) Τροποποίηση των διαδικασιών και των ελέγχων που επηρεάζουν την ασφάλεια πληροφοριών, σαν αναγκαία, για να ανταποκριθούν σε εσωτερικά ή εξωτερικά γεγονότα που μπορεί να έχουν επίπτωση στο TSQMS, συμπεριλαμβανομένων αλλαγών σε:

1) επιχειρησιακές απαιτήσεις
2) απαιτήσεις ασφάλειας
3) επιχειρησιακές διεργασίες που επηρεάζουν τις υπάρχουσες επιχειρησιακές απαιτήσεις
4) ρυθμιστικές ή νομικές απαιτήσεις
5) συμβατικές υποχρεώσεις και
6) στα επίπεδα επικινδυνότητας ή/και στα κριτήρια για την αποδοχή της επικινδυνότητας
7) ανάγκες για πόρους
8) βελτίωση στη μέθοδο μέτρησης της αποτελεσματικότητας των ελέγχων.

4.12. Βελτίωση του TSQMS

4.12.1. **Διαρκής βελτίωση**

Ο οργανισμός πρέπει να βελτιώνει διαρκώς την αποτελεσματικότητα του TSQMS μέσω της χρήσης της πολιτικής ασφάλειας, των στόχων ασφάλειας, των αποτελεσμάτων των επιθεωρήσεων, της ανάλυσης των συμβάντων που έχουν καταγραφεί από την παρακολούθηση, από τις διορθωτικές και προληπτικές ενέργειες και τη διαχειριστική αναθεώρηση. (βλ. 4.11.).

4.12.2. **Διορθωτικές ενέργειες**

Ο οργανισμός πρέπει να λάβει μέτρα ώστε να εξαλείψει τις αιτίες των μη συμμορφώσεων με τις απαιτήσεις του TSQMS προκειμένου να αποτραπεί η επανάληψη τους. Μια τεκμηριωμένη διαδικασία για τις διορθωτικές ενέργειες πρέπει να καθορίζει τις απαιτήσεις για:

a) τον προσδιορισμό των μη συμμορφώσεων
b) τον καθορισμό των αιτιών των μη συμμορφώσεων

c) την αξιολόγηση της ανάγκης για ενέργειες που θα εξασφαλίζουν ότι δεν θα ξαναεμφανιστούν μη συμμορφώσεις
d) τον προσδιορισμό και την εφαρμογή των απαιτούμενων διορθωτικών ενεργειών
e) τη καταγραφή των αποτελεσμάτων των διορθωτικών ενεργειών (βλ. τις 4.8.3) και
f) την αναθεώρηση των διορθωτικών ενεργειών που λαμβάνονται.

4.12.3. **Προληπτικές ενέργειες**

Ο οργανισμός πρέπει να καθορίσει τις πράξεις για την εξάλειψη των αιτιών των πιθανών μη συμμορφώσεων με τις απαιτήσεις ISMS προκειμένου να αποτραπεί η επανεμφάνισή τους. Οι προληπτικές ενέργειες που λαμβάνονται πρέπει να είναι σχετικές και κατάλληλες με τις επιπτώσεις των πιθανών προβλημάτων. Η τεκμηριωμένη διαδικασία για τις προληπτικές ενέργειες θα πρέπει να καθορίζει τις απαιτήσεις για:

a) προσδιορισμός των πιθανών μη συμμορφώσεων και των αιτιών τους
b) αξιολόγηση της ανάγκης για ενέργειες αποτροπής της εμφάνισης των μη συμμορφώσεων
c) προσδιορισμός και εφαρμογή των απαιτούμενων προληπτικών ενεργειών καθοριστικός
d) καταγραφή των αποτελεσμάτων των ενεργειών (βλ. τις 4.8.3); και
e) αναθεώρηση των προληπτικών ενεργειών μέτρων που έχουν παρθεί.

Η οργανισμός πρέπει να προσδιορίσει τους μεταβαλλόμενους κινδύνους και να προσδιορίσει τις απαιτήσεις για προληπτικές ενέργειες που εστιάζονται ακριβώς σε αυτούς τους μεταβαλλόμενους κινδύνους.

Η προτεραιότητα των προληπτικών ενεργειών θα καθοριστεί με βάση τα αποτελέσματα της αποτίμησης επικινδυνότητας.

ΣΗΜΕΙΩΣΗ: Οι προληπτικές ενέργειες για να αποτραπούν οι μη συμμορφώσεις είναι συχνά οικονομικά πιο αποδοτικές από τις διορθωτικές ενέργειες.

Κεφάλαιο 5

Πολιτική Ασφάλειας (Security Policy)

5.1. Εισαγωγή

Γενικά, στο πλαίσιο της λειτουργίας ενός οργανισμού, μια *πολιτική* αποτελεί το σύνολο των οδηγιών της διοίκησης για τον "τρόπο" με τον οποίο πρέπει να λειτουργεί ο οργανισμός. Περιλαμβάνει δηλαδή γενικές προτάσεις — δηλώσεις (high-level statements) που έχουν στόχο να καθοδηγήσουν τη λήψη αποφάσεων σχετικά με τα τρέχοντα και μελλοντικά ζητήματα που αντιμετωπίζουν τα μέλη του οργανισμού. Πολλές φορές στον όρο 'πολιτική' αποδίδεται η έννοια των γενικευμένων απαιτήσεων, στις οποίες θα πρέπει να ανταποκρίνεται η δράση και οι επιλογές των ανθρώπων τους οποίους αφορά η πολιτική. (Καρύδα, 2004:377)
Στο κεφαλαίο αυτό γίνεται αναφορά στην Πολιτική Ασφάλειας των Πληροφοριακών Συστημάτων, δεδομένου του ότι η δημιουργία μιας πολιτικής ασφάλειας αποτελεί βασικό στάδιο στην ανάπτυξη ενός συστήματος ασφάλειας Πληροφοριακών Συστημάτων.

5.2. Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων

Η Πολιτική Ασφάλειας των Πληροφοριακών Συστημάτων, αν και μπορεί να διαφέρει σημαντικά από οργανισμό σε οργανισμό, περιλαμβάνει γενικά το σκοπό και τους στόχους της ασφάλειας, οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν την προστασία των πληροφοριακών συστημάτων του οργανισμού. Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην πολιτική ασφάλειας υλοποιούνται με την εφαρμογή των μέτρων προστασίας για την ασφάλεια των πληροφοριακών συστημάτων. Η πολιτική ασφάλειας διατυπώνεται σε ένα έγγραφο, το οποίο θα πρέπει να γνωρίζουν και να ακολουθούν όλα τα μέλη του οργανισμού, στις δραστηριότητες τους που έχουν σχέση με τα πληροφοριακά συστήματα που καλύπτει η πολιτική. Στην πολιτική ασφάλειας, δηλαδή, καθορίζονται οι στόχοι της ασφάλειας, καθώς και ο τρόπος με τον οποίο οι στόχοι αυτοί θα υλοποιηθούν. Βασικό συστατικό στοιχείο, επομένως, κάθε πολιτικής ασφάλειας πληροφοριακών συστημάτων είναι η περιγραφή των κανόνων και των διαδικασιών που πρέπει να

ακολουθούνται για την προστασία των πληροφοριακών συστημάτων, καθώς και ο καθορισμός των συγκεκριμένων ρόλων και αρμοδιοτήτων που απαιτούνται για την υλοποίηση της πολιτικής ασφάλειας.

Η εφαρμογή μιας πολιτικής ασφάλειας σε έναν οργανισμό έχει δεσμευτικό χαρακτήρα για όλα τα μέλη του οργανισμού. Αυτό σημαίνει ότι η τήρηση των διαδικασιών και οδηγιών που προβλέπει η πολιτική ασφάλειας, και η εφαρμογή των μέτρων ασφάλειας που προδιαγράφονται σε αυτήν, είναι υποχρεωτική για όλους τους χρήστες των πληροφοριακών συστημάτων.

Οι πολιτικές ασφάλειας δηλώνουν τους στόχους για την ασφάλεια των πληροφοριακών συστημάτων και τα γενικά μέσα για την επίτευξη τους, ενώ οι οδηγίες (guidelines), που περιλαμβάνονται στην πολιτική ασφάλειας, αποσκοπούν στη δημιουργία του κατάλληλου πλαισίου για την επίτευξη των στόχων της πολιτικής ασφάλειας. Οι διαδικασίες (procedures) δίνουν συγκεκριμένες κατευθύνσεις για την υλοποίηση και εφαρμογή των οδηγιών της πολιτικής (ISO 13335).

Τέλος, μια Πολιτική Ασφάλειας συνοδεύεται από ένα σύνολο μέτρων προστασίας (security measures, security controls), ή αντιμέτρων (countermeasures) ή μέτρων ασφάλειας (security measures, security controls) όπως αλλιώς λέγονται, η εφαρμογή των οποίων παρέχει στα πληροφοριακά συστήματα το επίπεδο ασφάλειας που προσδιορίζεται στην πολιτική ασφάλειας.

Μια πολιτική ασφαλείας πρέπει να περιλαμβάνει τα ακόλουθα στοιχεία[25]:

- ✓ Στοιχεία (Assets): πρόκειται για τις οντότητες (πχ υλικό, λογισμικό, πληροφορίες, θέσεις κλειδιά του οργανισμού κλπ) του πληροφοριακού συστήματος που έχουν αξία και πρέπει να προστατευθούν
- ✓ Ρόλους και αρμοδιότητες (Roles and Responsibilities): πρόκειται για τους ρόλους και τις υπευθυνότητες, αρμοδιότητες, καθήκοντα, ευθύνες του κάθε ρόλου για θέματα που αφορούν το πληροφοριακό σύστημα και την ασφάλειά του
- ✓ Στόχους (Security policy objectives): πρόκειται για το στόχο (ή τους στόχους) ασφαλείας που καθορίζει συνοπτικά την εστίαση της πολιτικής και θέτει περιορισμούς

[25] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

- ✓ Πεδίο εφαρμογής της πολιτικής ασφαλείας (Scope of Security Policy): πρόκειται για την εμβέλεια, την έκταση και το χώρο που αφορά η πολιτική ασφαλείας
- ✓ Οδηγίες, κατευθυντήριες γραμμές (Guidelines)
- ✓ Κουλτούρα, άλλες πολιτικές, νομοθεσία (Culture, legislation, other policies): πρόκειται για το σύνολο των πεποιθήσεων, αξιών, αρχών, πολιτικών, κωδίκων δεοντολογίας, νόμων που συνθέτουν την κουλτούρα του οργανισμού και του περιβάλλοντος αυτού και ανατροφοδοτούν τους μηχανισμούς του μέσω μιας διαδικασίας συνεχούς εκμάθησης
- ✓ Υλοποίηση και εφαρμογή της πολιτικής ασφαλείας - Ενημέρωση και συμμόρφωση (Implementation and application of the security policy - Awareness, enforcement, breach): πρόκειται για το οργανωτικό πλαίσιο ρόλων, αρμοδιοτήτων, κανονισμών, επιτροπών για την υλοποίηση και εφαρμογή της πολιτικής ασφαλείας, για την ενημέρωση του προσωπικού σχετικά με την συμμόρφωση και τις ενέργειες που λαμβάνονται στην περίπτωση παραβίασής της πολιτικής ασφαλείας
- ✓ Επισκόπηση και αναθεώρηση της πολιτικής (Review and audit): πρόκειται για την τακτική επισκόπηση και αναθεώρηση της πολιτικής σύμφωνα με τις εκάστοτε συνθήκες ώστε να είναι επίκαιρη και να καλύπτει το σύνολο των δομικών στοιχείων του πληροφοριακού συστήματος και των διαδικασιών διαχείρισης

Τα βασικά χαρακτηριστικά της πολιτικής ασφαλείας πρέπει να είναι τα παρακάτω:

- ✓ Απαιτεί συμμόρφωση από το προσωπικό του οργανισμού. Το έγγραφο της πολιτικής θα πρέπει να είναι στη διάθεση όλου του προσωπικού
- ✓ Εκφράζει γενικότερες απόψεις ή αρχές του οργανισμού
- ✓ Είναι σαφής ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της και εφαρμόσιμη από άποψη κόστους
- ✓ Είναι γενικεύσιμη ώστε η εφαρμογή της να είναι επεκτάσιμη σε μελλοντικά συστήματα που ενδεχομένως ενταχθούν στο πληροφοριακό σύστημα του οργανισμού
- ✓ 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 στα εξής :

- Στην οργανωτική δομή και στην κουλτούρα του οργανισμού
- Στις απαιτήσεις ασφαλείας
- Στις τεχνολογικές εξελίξεις

Κεφάλαιο 6

Ανάλυση Κινδύνων

6.1. Εισαγωγή

Η ανάλυση κινδύνων ασφάλειας ενός πληροφοριακού συστήματος είναι μια διεργασία που έχει σκοπό να προσδιορίσει τον βαθμό ασφάλειας του Πληροφοριακού Συστήματος και να παρθεί μια ορθολογιστική απόφαση για το πώς η ασφάλεια του συστήματος μπορεί και πρέπει να βελτιωθεί. Επίσης απαντά στη προσπάθεια αιτιολόγησης των μέτρων ασφάλειας και ιδιαίτερα εκείνων που είναι διοικητικού και οργανωτικού χαρακτήρα, δεδομένης της αντίληψης ότι το ζήτημα της ασφάλειας είναι αποκλειστικά ένα "τεχνικό ζήτημα". Όλα αυτά είναι απαραίτητα στην διαδικασία ένταξης συστημάτων ασφάλειας στο πλαίσιο λειτουργίας ενός οργανισμού, ζήτημα το οποίο δεν θα πρέπει να θεωρηθεί εύκολη υπόθεση, γεγονός που εξηγεί σε μεγάλο βαθμό και το χαμηλό επίπεδο ασφάλειας που παρουσιάζουν τα Πληροφοριακά Συστήματα των σύγχρονων οργανισμών.

Το κεφάλαιο αυτό ξεκινά με την εννοιολογική προσέγγιση της ανάλυσης και διαχείρισης της επικινδυνότητας, συνεχίζει με τη μεθοδολογία τους, και την επιλογή των μέτρων ελέγχου επικινδυνότητας. Ολοκληρώνεται με την παρουσίαση της μεθόδου SBA (Security By Analysis) η οποία εφαρμόζει τις αρχές της Διοίκησης Ολικής Ποιότητας.

6.2. Ανάλυση και Διαχείριση Επικινδυνότητας ΠΣ

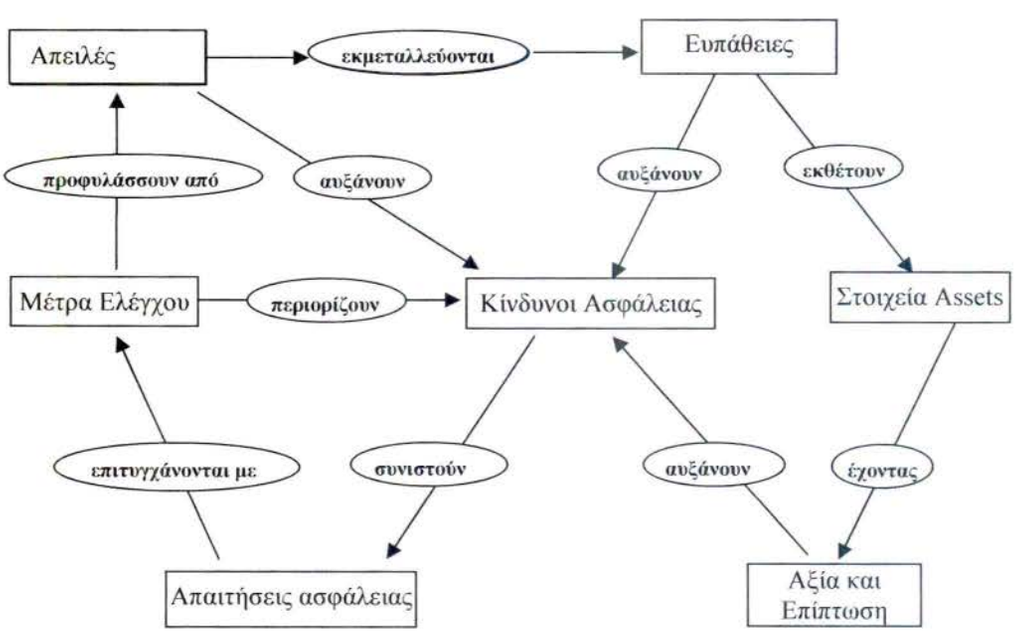
Η ανάλυση επικινδυνότητας (risk analysis) απαντά στο ερώτημα της επιλογής αντιμέτρων που θα προσφέρουν προστασία *ανάλογη* των κινδύνων που απειλούν το ΠΣ. Η ανάλυση επικινδυνότητας αναστρέφει το μοντέλο της *αξιολόγησης επενδύσεων*, όπου μία επένδυση θεωρείται συμφέρουσα αν το κόστος της (σε σταθερές τιμές) υπολείπεται του γινομένου του αναμενόμενου κέρδους επί την πιθανότητα επίτευξης του κέρδους[26]. Εδώ, η *επικινδυνότητα* (Ε) ορίζεται ως το

[26]Η αξιολόγηση μιας επένδυσης είναι μία αρκετά πιο σύνθετη διαδικασία, όπου λαμβάνονται υπόψη πολλά περισσότερα κριτήρια.

γινόμενο της *πιθανότητας* (Π) πραγματοποίησης ενός επεισοδίου ασφάλειας (security incident) επί το *κόστος* (Κ) που θα επιφέρει το επεισόδιο ασφάλειας, ήτοι: Ε = Π x Κ. (Κοκολάκης,2004:337-341).

Αναλυτικότερα, η πιθανότητα πραγματοποίησης ενός επεισοδίου εκτιμάται ως συνάρτηση της πιθανότητας εμφάνισης μίας *απειλής* (threat) και της σχετικής *ευπάθειας* (αδυναμία, αλωσιμότητα, vulnerability) του συστήματος που δύναται να επιτρέψει στην απειλή να πραγματοποιηθεί. Αντίστοιχα, το κόστος από την πραγματοποίηση ενός επεισοδίου εκτιμάται με βάση την *επίπτωση* (impact) πάνω στον οργανισμό, που θα έχει η ζημιά που θα προκληθεί στα *περιουσιακά στοιχεία (στοιχεία,* assets) του ΠΣ (Σχήμα 8). Έτσι, τελικά, η επικινδυνότητα εκτιμάται ως συνάρτηση τριών παραγόντων: (α) της αξίας των *στοιχείων* (assets), που προκύπτει από την αντίστοιχη επίπτωση της ζημιάς που θα υποστούν, (β) της σοβαρότητας των *απειλών* (threats) και (γ) του επιπέδου της *ευπάθειας* (vulnerability) του ΠΣ.

Το μοντέλο αυτό δίνει τη δυνατότητα αποτίμησης της επικινδυνότητας σε χρηματικούς όρους, έτσι ώστε να συγκριθεί με το κόστος των σχετικών αντιμέτρων. Συχνότερα, όμως, η αποτίμηση γίνεται σε απλή αριθμητική κλίμακα, καθώς οι επιπτώσεις από την απώλεια ορισμένων στοιχείων (π.χ. απώλεια ανθρώπινης ζωής) είναι δύσκολο να αποτιμηθούν οικονομικά.



Σχήμα 8: Σχέσεις Απειλών Ευπαθειών και Κινδύνων Ασφάλειας.
πηγή: ISO/IEC TR 13335 part 1:16

ανάλυση της επικινδυνότητας αποτελεί προϋπόθεση για τη μετέπειτα διαχείρισης της, που είναι και ο αντικειμενικός στόχος της όλης προσπάθειας. Ο όρος *διαχείριση επικινδυνότητας* αναφέρεται στον έλεγχο της επικινδυνότητας, ώστε να παραμένει σε αποδεκτά επίπεδα. Η επικινδυνότητα μπορεί να μειωθεί, με την εφαρμογή αντιμέτρων, να μεταβιβαστεί, π.χ. με ασφάλιση, ή να αναληφθεί δηλαδή να αποδεχθούμε ότι είμαστε διατεθειμένοι να υποστούμε τις επιπτώσεις αν συμβεί ένα επεισόδιο.

6.3. Η μεθοδολογία της ανάλυσης και διαχείρισης επικινδυνότητας

Με τον όρο *μεθοδολογία* εννοούμε ένα οργανωμένο σύνολο αρχών και κανόνων, το οποίο καθοδηγεί τη δράση ένα συγκεκριμένο γνωστικό χώρο. Μεθοδολογία είναι ο *λόγος περί της μεθόδου.* Προδιαγράφει, δηλαδή, τις μεθόδους που μπορούν να χρησιμοποιηθούν σ' ένα γνωστικό χώρο, εκφράζοντας με αυτόν τον τρόπο μία συγκεκριμένη άποψη (φιλοσοφική, επιστημολογική, βιωματική). Η μεθοδολογία "υλοποιείται" με ένα σύνολο *μεθόδων, τεχνικών* και *εργαλείων.*

Η μεθοδολογία της *ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ* υιοθετεί τις βασικές αρχές και το επιστημολογικό υπόβαθρο της στατιστικής επιστήμης και των πιθανοτήτων και κυρίως του κλάδου που αναφέρεται συνήθως ως στατιστική Bayes (Bayesian Statistics), από το όνομα του μαθηματικού Thomas Bayes (1702-1761) που διατύπωσε το ομώνυμο θεώρημα

Η στατιστική κατά Bayes θεμελιώνει την άποψη ότι η πιθανότητα να συμβεί ένα γεγονός στο μέλλον αποτελεί μετρήσιμο μέγεθος. Η πιθανότητα αυτή μπορεί να προσδιοριστεί, αν αναλυθούν οι παράγοντες από τους οποίους εξαρτάται. Μπορούμε, για παράδειγμα, να υπολογίσουμε την πιθανότητα να κλαπούν τα απόρρητα δεδομένα που διατηρούμε στον υπολογιστή μας, ως συνάρτηση της πιθανότητας ένας επίδοξος εισβολέας να προσπαθήσει να "παρεισφρήσει" στον υπολογιστή μας και της πιθανότητας να το επιτύχει. Στη γλώσσα της ανάλυσης επικινδυνότητας, η πρώτη πιθανότητα μας δίνει το μέγεθος της απειλής και η δεύτερη το μέγεθος της ευπάθειας του συστήματος μας.

Έτσι, η ανάλυση επικινδυνότητας αποτιμά την πιθανότητα να συμβεί ένα συμβάν ασφάλειας (security incident), αναλύοντας και αποτιμώντας τους παράγοντες που συνδέονται με την πραγματοποίηση του, δηλ. την απειλή και την ευπάθεια. Έπειτα, συνδυάζει την πιθανότητα αυτή με την επίπτωση που προκύπτει από την

πραγματοποίηση του επεισοδίου, για να υπολογίσει την επικινδυνότητα του συστήματος.

Η μεθοδολογία δεν περιγράφει συγκεκριμένες μεθόδους για την ανάλυση και αποτίμηση της επικινδυνότητας. Προσδιορίζει, όμως, ορισμένα στάδια που θα πρέπει να ακολουθηθούν. Σύμφωνα με το Διεθνή Οργανισμό Τυποποίησης (ISO — International Organization for Standardization[27]) τα στάδια αυτά είναι:

- Προσδιορισμός και αποτίμηση των στοιχείων (assets).
- Εκτίμηση της απειλής.
- Εκτίμηση της ευπάθειας.
- Εκτίμηση των υφιστάμενων μέσων προστασίας.
- Υπολογισμός της επικινδυνότητας.

Τα στάδια που περιγράφει το ISO αποτελούν ένα γενικό πλαίσιο. Μπορούν να εξειδικευθούν, να συγχωνευθούν, να αντιστραφεί η σειρά τους κ.λπ., όμως κάθε μέθοδος ανάλυσης επικινδυνότητας θα πρέπει να τα συμπεριλάβει σε κάποια μορφή.

Με τον υπολογισμό της επικινδυνότητας ολοκληρώνεται η ανάλυση επικινδυνότητας. Το ζητούμενο, όμως, είναι ο περιορισμός της επικινδυνότητας εντός αποδεκτών ορίων. Αυτό είναι το αντικείμενο της *διαχείρισης επικινδυνότητας*. Η διαχείριση της επικινδυνότητας περιλαμβάνει τα εξής στάδια:

- Επιλογή αντιμέτρων (countermeasures, safeguards).
- Καθορισμός πολιτικής ασφάλειας.
- Σύνταξη σχεδίου ασφάλειας.
- Εφαρμογή και παρακολούθηση του σχεδίου ασφάλειας.

Το Σχέδιο Ασφάλειας αποτελεί το βασικό εργαλείο για τη διαχείριση της επικινδυνότητας και περιλαμβάνει (α) την πολιτική ασφάλειας, (β) τα αντίμετρα και (γ) τη στρατηγική εφαρμογής του σχεδίου.

Στόχος, λοιπόν, της όλης προσπάθειας είναι ο περιορισμός της επικινδυνότητας. Το συναγόμενο ερώτημα είναι: Σε ποιο βαθμό θα πρέπει να περιορίσουμε την επικινδυνότητα; Μπορούμε να τη μηδενίσουμε;

Μηδενική επικινδυνότητα έχουμε είτε όταν η αξία των στοιχείων του συστήματος (στοιχεία, assets) είναι ίση με το μηδέν, είτε όταν η πιθανότητα πραγματοποίησης ενός επεισοδίου ασφάλειας είναι ίση με το μηδέν. Αν κατά την ανάλυση

---

[27]ISO/IEC/JTC1 13335 Information Technology – Security Techniques – Guidelines for Management of IT Security (GMITS), 1996

επικινδυνότητας εντοπίσουμε ότι κάποια στοιχεία του συστήματος μας έχουν ελάχιστη ή μηδενική αξία, τότε δεν θα τα συμπεριλάβουμε στη διαχείριση επικινδυνότητας, καθώς η λήψη μέτρων προστασίας αυτών των στοιχείων στερείται νοήματος.

Επίσης, είναι πιθανόν να έχουμε στοιχεία με σημαντική αξία και να λάβουμε την απόφαση να μειώσουμε ή να μηδενίσουμε την αξία τους. Για παράδειγμα, αν τηρούμε ευαίσθητα προσωπικά δεδομένα και το κόστος προστασίας τους είναι πολύ υψηλό, τότε είναι πιθανόν να αποφασίσουμε ότι δεν συμφέρει να διατηρούμε τέτοια δεδομένα και να διακόψουμε τη συλλογή τους. Σε μια άλλη περίπτωση, είναι πιθανόν να θεωρήσουμε ότι το κόστος προστασίας του εξοπλισμού μας είναι εξαιρετικά υψηλό και να αποφασίσουμε τη διακοπή της χρήσης ιδιόκτητου εξοπλισμού και την αγορά υπηρεσιών πληροφορικής από τρίτους (outsourcing).

Όσον αφορά το δεύτερο σκέλος, δηλαδή την πιθανότητα να συμβεί ένα συμβάν ασφάλειας, ο μηδενισμός της πιθανότητας αυτής (δηλ. η επίτευξη απόλυτης ασφάλειας) δεν είναι εφικτός για τους εξής λόγους:

- Οι απειλές, που αντιμετωπίζει ένα ανοικτό σύστημα που λειτουργεί σε ένα δυναμικό περιβάλλον, όπως είναι τα σύγχρονα ΠΣ, είναι δυναμικές (δηλαδή χαρακτηρίζονται από συνεχή μεταβλητότητα) και οι αιτίες που τις προκαλούν είναι εξαιρετικά σύνθετες.
- Η ανθρώπινη συμπεριφορά, η οποία είναι δύσκολο να προβλεφθεί και να μοντελοποιηθεί, παίζει ιδιαίτερα σημαντικό ρόλο στην ασφάλεια των ΠΣ.
- Οι πόροι που διαθέτει ένας οργανισμός ή μία επιχείρηση είναι πεπερασμένοι.

Όπως φαίνεται από σχετικές έρευνες (Kiountouzis et.al.), η ανάπτυξη τεχνικών και μέτρων ασφάλειας δεν επαρκεί, καθώς το αδύνατο σημείο κάθε ΠΣ παραμένει ο άνθρωπος (χρήστης, χειριστής, σχεδιαστής, κ.λπ.). Συνεπώς, η ανάπτυξη ασφαλών ΠΣ θα πρέπει να δίνει βαρύτητα εξίσου στον τεχνικό παράγοντα όσο και στους ανθρώπους.

Παράλληλα, οι απειλές που αντιμετωπίζει ένα ΠΣ χαρακτηρίζονται από ποικιλία, συμπλοκότητα και συνεχή μεταβλητότητα. Για παράδειγμα, υπάρχουν φυσικές απειλές (πχ. πυρκαγιά, σεισμός, κ.λπ.), απειλές μη-εξουσιοδοτημένης πρόσβασης (πχ. hacking), τεχνικές βλάβες, λάθος χειρισμοί κ.λπ. Καθώς το τεχνολογικό και κοινωνικό περιβάλλον εξελίσσεται διαρκώς και με ταχύ ρυθμό, έτσι και οι απειλές μεταβάλλονται και εξελίσσονται.

Τέλος, το κόστος των μέτρων προστασίας δεν μπορεί να αγνοηθεί. Το κόστος αυτό δεν αφορά μόνο στην προμήθεια και εγκατάσταση μέτρων και εργαλείων προστασίας. Συμπεριλαμβάνει το κόστος από τη χρήση πολύτιμων ανθρώπινων πόρων, το κόστος για εκπαίδευση και ενημέρωση των χρηστών, καθώς και για τη διεκπεραίωση εργασιών και διαδικασιών που αφορούν την ασφάλεια.

Κατά συνέπεια, εφόσον ο μηδενισμός της επικινδυνότητας δεν είναι εφικτός, το ενδιαφέρον εστιάζεται στον περιορισμό της επικινδυνότητας σε αποδεκτά επίπεδα. Η απόφαση αυτή δεν είναι ποτέ μονοσήμαντη, αλλά εξαρτάται αφενός από το κόστος και αφετέρου από την αποτελεσματικότητα των μέτρων προστασίας που απαιτούνται για τη μείωση της επικινδυνότητας.

Όταν η λήψη μέτρων για τη μείωση της επικινδυνότητας δεν κρίνεται συμφέρουσα, τότε υπάρχουν άλλες δύο εναλλακτικές επιλογές: η μεταβίβαση της επικινδυνότητας και η αποδοχή της επικινδυνότητας. Στην πρώτη περίπτωση η επικινδυνότητα μεταβιβάζεται σε τρίτους, συνήθως με την καταβολή του αντίστοιχου τιμήματος. Χαρακτηριστική περίπτωση μεταβίβασης επικινδυνότητας αποτελεί η ασφάλιση, όπου η επικινδυνότητα μεταβιβάζεται στην ασφαλιστική εταιρεία, στην οποία καταβάλλεται το αντίστοιχο αντίτιμο.

Η δεύτερη επιλογή αφορά στην αποδοχή της επικινδυνότητας. Σε αυτήν την περίπτωση ο οργανισμός αποδέχεται συνειδητά τις επιπτώσεις που ενδέχεται να υποστεί εάν συμβεί μία παραβίαση της ασφάλειας του ΠΣ. Επιλέγει, όμως, να μην υλοποιήσει τα μέτρα προστασίας που απαιτούνται για να μειωθεί η σχετική επικινδυνότητα. Υπάρχουν αρκετές περιπτώσεις που συνειδητά επιλέγεται η αποδοχή της επικινδυνότητας, όπως, για παράδειγμα, περιπτώσεις όπου τα μέτρα προστασίας αντιβαίνουν στην πολιτική και την κουλτούρα του οργανισμού.

6.4. Επιλογή μέτρων ελέγχου επικινδυνότητας (controls)[28]

Εφόσον καθοριστούν οι απαιτήσεις ασφάλειας, μπορεί να γίνει η επιλογή των κατάλληλων μέτρων ελέγχου και προστασίας, τα οποία θα μειώσουν τον κίνδυνο σε αποδεκτά επίπεδα. Τα απαραίτητα μέτρα μπορούν να επιλεγούν από οποιοδήποτε σύνολο είναι κατάλληλο για τον οργανισμό. Υπάρχουν πολλοί διαφορετικοί τρόποι για τη διαχείριση κινδύνων. Πρέπει όμως να ληφθεί υπόψη ότι δεν είναι όλα τα μέσα

[28]ISO/IEC 17799:2005

το ίδιο κατάλληλα ή το ίδιο πρακτικά για όλους τους οργανισμούς.

Τα μέτρα ελέγχου (controls) θα πρέπει να επιλεγούν με κριτήριο το κόστος υλοποίησής τους σε σχέση με τους κινδύνους που καλούνται να αντιμετωπίσουν και το κόστος των πιθανών επιπτώσεων των τελευταίων στον οργανισμό. Επίσης, θα πρέπει να συμπεριληφθούν και ποιοτικοί παράγοντες, όπως η απώλεια φήμης για τον οργανισμό. Ένας αριθμός μέτρων ελέγχου και προστασίας θεωρούνται θεμελιώδεις και αποτελούν τη βάση για την ασφάλεια πληροφοριών. Βασίζονται είτε σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική στην ασφάλεια.

Μέτρα ελέγχου απαραίτητα σε έναν οργανισμό και που βασίζονται στη νομοθεσία είναι:

- Διαφύλαξη των προσωπικών δεδομένων
- Διαφύλαξη των δεδομένων του οργανισμού
- Δικαιώματα πνευματικής ιδιοκτησίας

Μέτρα ελέγχου που έχουν καθιερωθεί ως κοινή πρακτική είναι:

- Πολιτική ασφάλειας
- Καταμερισμός καθηκόντων σχετικών με την ασφάλεια
- Ενημέρωση και εκπαίδευση ασφάλειας
- Διαχείριση στη σωστή χρήση των εφαρμογών
- Διαχείριση δημοσιευμένων τεχνικών ευπαθειών (π.χ. patches)
- Διαχείριση της επιχειρησιακής συνέχειας
- Διαχείριση συμβάντων ασφάλειας και βελτίωση

Τα προαναφερθέντα μέτρα ελέγχου μπορούν να χρησιμοποιηθούν σχεδόν σε κάθε οργανισμό. Ένα ολοκληρωμένο σύνολο μέτρων ελέγχου παρουσιάζονται σαν απαιτήσεις στο πρότυπο ISO/IEC 17799:2005.

Πρέπει να σημειωθεί ότι αν και όλα τα μέτρα σε αυτά τα πρότυπα είναι σημαντικά και θα πρέπει να εξετάζεται η υιοθέτησή τους, αυτό θα πρέπει να γίνεται σε σχέση με τους συγκεκριμένους κινδύνους που αντιμετωπίζει ο οργανισμός. Ως εκ τούτου, αν και η ανωτέρω προσέγγιση θεωρείται καλή αφετηρία, δεν αντικαθιστά την επιλογή των μέτρων ελέγχου που προκύπτουν από μια αποτίμηση επικινδυνότητας.

6.5. Μέθοδοι Ανάλυσης και Διαχείρισης Επικινδυνότητας ΠΣ

Έχουν αναπτυχθεί ένα μεγάλο πλήθος μεθόδων ανάλυσης και διαχείρισης επικινδυνότητας οι κυριότερες των οποίων περιγράφονται στο έγγραφο της ENISA[29], και πολλές από τις οποίες υποστηρίζονται από εργαλεία λογισμικού.
Στα πλαίσια της προσέγγισης της ασφάλειας μέσω των αρχών της Διοίκησης Ολικής Ποιότητας που ακολουθείται στην παρούσα εργασία, θα γίνει σύντομη αναφορά στη μέθοδο SBA (Security By Analysis).

6.5.1. **Security By Analysis (SBA)**[30]

Η SBA (Security By Analysis) αναπτύχθηκε στη Σουηδία στις αρχές της δεκαετίας του '80. Αν και είναι ελάχιστα γνωστή εκτός της Σκανδιναβικής χερσονήσου, αποτελεί την πλέον δημοφιλή και ευρέως εφαρμοζόμενη μέθοδο ανάλυσης επικινδυνότητας στη Σουηδία. Η SBA θα πρέπει να θεωρείται λιγότερο ως αυστηρή μέθοδος και περισσότερο ως μία ανθρωποκεντρική οπτική απέναντι στο ζήτημα της ανάλυσης επικινδυνότητας.
Η SBA βασίζεται στη διαπίστωση ότι οι άνθρωποι που συμμετέχουν στην καθημερινή λειτουργία του συστήματος, ανεξάρτητα από το ρόλο και τη θέση τους στην ιεραρχία, είναι αυτοί που έχουν τις περισσότερες πιθανότητες να εντοπίσουν τα προβλήματα ασφάλειας και να προτείνουν λύσεις. Τα είκοσι έτη επιτυχημένης εφαρμογής της μεθόδου ενισχύουν την παραπάνω θέση και καταδεικνύουν ότι η ανθρωποκεντρική ανάλυση επικινδυνότητας αποτελεί μία ρεαλιστική και αποτελεσματική προσέγγιση.
Η SBA αποτελείται στην πραγματικότητα από ένα σύνολο μεθόδων, που ακολουθούν την ίδια φιλοσοφία και λειτουργούν συμπληρωματικά. Οι κυριότερες από αυτές είναι η SBA Check και η SBA Scenario. Και οι δύο μέθοδοι υποστηρίζονται από ειδικό λογισμικό, που διευκολύνει σημαντικά την εφαρμογή τους.
Η SBA Check χρησιμοποιείται για την ταχεία αποτίμηση του επιπέδου ασφάλειας ενός πληροφοριακού συστήματος. Αποτελείται κατά βάση από μία σειρά ερωτηματολογίων, που εστιάζουν, κυρίως, στη διαχείριση της ασφάλειας του

---

[29]ENISA (2006) "Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools".

[30] Κοκολάκης, 2004:343

συστήματος, έχοντας ως σημείο αναφοράς το πρότυπο ISO/DEC 17799 και ακολουθώντας το κλασικό μοντέλο του καταλόγου (checklist model). Σύμφωνα με το μοντέλο του καταλόγου η ασφάλεια ενός συστήματος ελέγχεται με βάση έναν κατάλογο από ενδεικνυόμενες ενέργειες και μέτρα προστασίας (checklist), που βρίσκουν εφαρμογή σε ένα μεγάλο εύρος διαφορετικών συστημάτων. Η SBA Check είναι ιδιαίτερα εύκολη στην εφαρμογή της και υποστηρίζεται από ειδικό λογισμικό.

Η SBA Scenario αποτελεί τον πυρήνα της SBA και χρησιμοποιείται για την ποσοτική (quantitative) ανάλυση της επικινδυνότητας ενός πληροφοριακού συστήματος. Η εφαρμογή της υποστηρίζεται από ειδικό λογισμικό, το οποίο καλύπτει όλα τα στάδια της μεθόδου, εκτός από τη δημιουργική φάση της επινόησης πιθανών σεναρίων παραβίασης της ασφάλειας του ΠΣ. Ανάλογα με το μέγεθος του πληροφοριακού συστήματος παρέχονται οι εξής τρεις επιλογές:

1) Main analysis: Πλήρης ανάλυση με στόχο τον προσδιορισμό της πιθανότητας πραγματοποίησης ενός επεισοδίου ασφάλειας και την εκτίμηση του κόστους με αναλυτικές αριθμητικές μεθόδους.
2) Ten analysis: Ταχεία ανάλυση με την πιθανότητα και το κόστος να προσδιορίζονται στην κλίμακα 1-10.
3) Risk window: Συνοπτική ανάλυση βασισμένη σε μία ποιοτική κλίμακα τεσσάρων βαθμίδων.

Η SBA Scenario περιλαμβάνει τα εξής τέσσερα στάδια:

1. Προετοιμασία (Preparation).
2. Σενάρια (Scenarios).
3. Σύνοψη (Overview).
4. Σχέδιο Δράσης (Action Plan).

6.5.1.1. *Προετοιμασία (Στάδιο 1ο)*

Στο στάδιο της προετοιμασίας συγκροτούνται οι ομάδες ανάλυσης και διδάσκεται η SBA. Βασικό στοιχείο της φιλοσοφίας της μεθόδου είναι η συμμετοχή εργαζομένων από διάφορες θέσεις και βαθμίδες. Οι ίδιοι οι εργαζόμενοι στο σύστημα είναι υπεύθυνοι για την επιτυχία του έργου της ανάλυσης επικινδυνότητας, ενώ ο ρόλος του ειδικού της ασφάλειας περιορίζεται στη διδασκαλία της μεθόδου και στο συντονισμό των εργασιών της ομάδας. Με στόχο την επίτευξη μεγαλύτερης αποτελεσματικότητας συνήθως συγκροτούνται περισσότερες από μία ομάδες.

Επίσης, ιδιαίτερη έμφαση αποδίδεται στην οργάνωση του τρόπου εργασίας της κάθε

ομάδας. Σε αυτό το στάδιο ρυθμίζονται ζητήματα, όπως το χρονοδιάγραμμα του έργου, ο προσδιορισμός του αντικειμένου της ανάλυσης (σύστημα, υποσύστημα κ.λπ.), ο καθορισμός της έκτασης (οριοθέτηση) της ανάλυσης, ο καθορισμός του ρόλου που θα αναλάβει το κάθε μέλος της ομάδας, η διαμόρφωση κοινής αντίληψης για το σκοπό του έργου κ.λπ.

6.5.1.2. *Σενάριο (Στάδιο 2ο)*

Στο δεύτερο στάδιο εντοπίζονται, καταγράφονται και αναλύονται τα πιθανά σενάρια επεισοδίων ασφάλειας (events). Πρόκειται για τη δημιουργική φάση της μεθόδου, όπου το κάθε μέλος της ομάδας εργασίας θα πρέπει να αναλάβει πρωτοβουλία και να προτείνει σενάρια, τα οποία θα αξιολογηθούν και θα αναλυθούν με τη βοήθεια των υπολοίπων μελών της ομάδας. Ακολούθως, για κάθε ένα σενάριο διεξάγεται ανάλυση επικινδυνότητας και διαχείριση επικινδυνότητας.

Ανάλυση επικινδυνότητας

Αρχικά, το κάθε σενάριο περιγράφεται αναλυτικά και καταγράφονται όλα τα διαθέσιμα στοιχεία που αφορούν το σενάριο, όπως τα γεγονότα που δύναται να οδηγήσουν στην πραγματοποίηση του σεναρίου κ.λπ. Επίσης, εκτιμάται η πιθανότητα το σενάριο να γίνει πραγματικότητα.

Ακολούθως οι πιθανές συνέπειες από την πραγματοποίηση του σεναρίου προσδιορίζονται και αναλύονται, ώστε να εκτιμηθεί η σοβαρότητα τους και να προσδιοριστεί ποσοτικά το κόστος που αναμένεται να προκύψει.

Διαχείριση επικινδυνότητας

Η διαχείριση της επικινδυνότητας γίνεται σε δύο φάσεις. Αρχικά, προσδιορίζονται οι αδυναμίες του συστήματος που συνδέονται με το σενάριο και δύναται να επιτρέψουν την πραγματοποίηση του. Στη δεύτερη φάση επιλέγονται συγκεκριμένα μέτρα προστασίας. Η αποτελεσματικότητα του κάθε μέτρου αξιολογείται και αντιπαραβάλλεται με το κόστος υλοποίησης.

6.5.1.3. *Σύνοψη (Στάδιο 3ο)*

Στόχος αυτού του σταδίου είναι ο προσδιορισμός των προτεραιοτήτων υλοποίησης των μέτρων προστασίας. Οι προτεραιότητες καθορίζονται με βάση τους εξής δύο παράγοντες:

- το κόστος που ενδέχεται να προκύψει από τη ζημία που θα προκληθεί, εάν δεν υλοποιηθεί το προτεινόμενο μέτρο προστασίας και συμβούν τα γεγονότα που προβλέπει το σχετικό σενάριο και
- τη μείωση της επικινδυνότητας που επιτυγχάνεται με την υλοποίηση του μέτρου προστασίας.

6.5.1.4. *Σχέδιο δράσης (Στάδιο 4ο)*

Στο τελευταίο στάδιο καταρτίζεται ένα συνολικό σχέδιο δράσης για την ασφάλεια του πληροφοριακού συστήματος και καθορίζονται οι υπεύθυνοι για την υλοποίηση των μέτρων προστασίας.

6.5.2. **Πλεονεκτήματα και μειονεκτήματα**

Η SBA διακρίνεται για τον ανθρωποκεντρικό και συμμετοχικό της χαρακτήρα. Δίνει ιδιαίτερη βαρύτητα στη συμμετοχή των ανθρώπων που η εργασία τους σχετίζεται με το πληροφοριακό σύστημα και ενθαρρύνει τη δημιουργικότητα και τη φαντασία τους. Τα βασικότερα πλεονεκτήματα της μεθόδου είναι τα εξής:

- Υιοθετεί μία ολιστική προσέγγιση του ζητήματος της ασφάλειας, εξετάζοντας το πληροφοριακό σύστημα ως ενιαίο σύνολο και μελετώντας το από όλες τις πλευρές.
- Η ανάλυση γίνεται από τους ίδιους τους ανθρώπους που χρησιμοποιούν καθημερινά το σύστημα, γεγονός που ενισχύει την αποτελεσματικότητα της μεθόδου και κυρίως εξασφαλίζει σε μεγάλο βαθμό την αποδοχή και εφαρμογή του σχεδίου ασφάλειας που προκύπτει ως αποτέλεσμα της εφαρμογής της μεθόδου.
- Είναι αρκετά απλή, κατανοητή και από μη-ειδικούς και μπορεί να υλοποιηθεί με μικρό, σχετικά, κόστος.
- Υποστηρίζεται από ειδικό λογισμικό, το οποίο είναι απλό και εύχρηστο.

Τα κυριότερα μειονεκτήματα της μεθόδου είναι τα εξής:

- Στηρίζεται σε μεγάλο βαθμό στις ικανότητες, τη φαντασία και τη διάθεση για συνεισφορά των εργαζομένων.

- Δεν συνοδεύεται από βιβλιοθήκες μέτρων προστασίας. Η επινόηση και ο-σχεδιασμός των μέτρων προστασίας επαφίεται στις ομάδες εργασίας.
- Προϋποθέτει την ανάπτυξη ανθρωποκεντρικής και συμμετοχικής κουλτούρας. Αυτός είναι, ίσως, ο κυριότερος λόγος που η εφαρμογή της μεθόδου δεν έχει επεκταθεί ιδιαίτερα εκτός των Σκανδιναβικών χωρών. Όμως στα πλαίσια της υιοθέτησης ενός Συστήματος Διαχείρισης Ασφάλειας TSQMS που εφαρμόζεται σε ένα περιβάλλον Διοίκησης Ολικής Ποιότητας, η μέθοδος αυτή είναι ιδανική καθώς ικανοποιεί απόλυτα τις αρχές και τις αξίες της ΔΟΠ που τονίζουν της σημασία της αξίας του ατόμου καθώς και την δύναμη της συλλογικής δράσης» (Evans, Lindsay, 1999:118).

Κεφάλαιο 7

Κουλτούρα Ασφάλειας

7.1. Εισαγωγή

Από δημοσιεύματα του τύπου[31] αλλά και σχετικές έρευνες[32] αποδεικνύεται ότι παρά την ύπαρξη μοντέλων, μεθοδολογιών, και συστημάτων για την ασφάλεια των Πληροφοριακών Συστημάτων, οι επιθέσεις και τα συμβάντα ασφάλειας συνεχίζουν να υφίστανται και ακόμη να αυξάνονται σε παγκόσμιο επίπεδο.

Στη προσπάθεια διερεύνησης και εξέτασης αυτού του ζητήματος υπό το πρίσμα της ποιότητας, στο κεφάλαιο αυτό η εργασία προσεγγίζει το ζήτημα της κουλτούρας ασφάλειας, η οποία ενώ συμπεριλαμβάνεται στους βασικούς παράγοντες που διαμορφώνουν την ασφάλεια των Πληροφοριακών Συστημάτων (MIT, 'σπίτι της ασφάλειας') φαίνεται ότι δεν συγκεντρώνει την κατάλληλη προσοχή στη διαχείρισή της .

Στο κεφάλαιο αυτό αφού παρουσιασθεί μια έρευνα του MIT που έγινε το 2006 και έδειξε ότι πραγματικά υπάρχουν χάσματα (gaps[22]) αντίληψης σε διάφορα ζητήματα ασφάλειας με κυριότερο στην κουλτούρα ασφάλειας, στη συνέχεια προχωρά στην ανάλυση της κουλτούρας. Στο πλαίσια αυτά επιχειρείται μια προσέγγιση στο ζήτημα της κουλτούρας ασφάλειας κάτω από το πρίσμα της Διοίκησης Ολικής Ποιότητας. Μετά τον ορισμό της οργανωσιακής κουλτούρας και αναφορά στο σχηματισμό της, αναλύεται η κουλτούρα ασφάλειας και οι τρόποι μέτρησής της. Στη συνέχεια αναπτύσσεται η προσέγγιση της ENISA αναφορικά με τη δημιουργία της κουλτούρας ασφάλειας, καθώς ικανοποιεί τις σχετικές αρχές της ΔΟΠ. Ακολουθεί αναφορά στην αλλαγή κουλτούρας και στο μοντέλο της 'Οργάνωσης που Μαθαίνει την Ασφάλεια' το οποίο μπορεί να χρησιμοποιηθεί για την αλλαγή της κουλτούρας ασφάλειας σε ένα οργανισμό.

---

[31] Άγνωστος (2007). Νέα γκάφα διαρροής προσωπικών δεδομένων στη Βρετανία Στοιχεία για 3 εκατ. άτομα. http://www.pathfinder.gr 18/12/07.

[32] 1) CSI 'The 12th Annual Computer Crime and Security Survey 2007', http://www.gocsi.com
2) Symantec, " Internet Security Threat Report.Volume XII Sept 17", 2007

7.2. Έρευνα του MIT για τις αντιλήψεις στην ασφάλεια

Το 2006, το Massachusetts Institute of Technology (Madnick,2006) πραγματοποίησε την πρώτη φάση μιας μελέτης 1259 ατόμων από έξι επιχειρήσεις διαφορετικού τομέα δραστηριότητας, με ερωτήσεις σχετικές με την προσωπική αξιολόγηση (person's assessment) ως προς την ετοιμότητα του οργανισμού για την καταπολέμηση συγκεκριμένου τύπου κινδύνου ασφάλειας (security risk) και πως αντιλαμβάνονται τη σπουδαιότητα (importance) αυτού του κινδύνου.

Η μελέτη εφάρμοσε μεθοδολογία Διοίκησης Ολικής Ποιότητας. Στους συμμετέχοντες περιελήφθησαν ανώτεροι διοικητικοί υπάλληλοι, διευθυντές IT, διάφορες κατηγορίες υπαλλήλων, συνεργάτες, πελάτες και προμηθευτές. Κάθε συμμετέχων κλήθηκε να απαντήσει σε ερωτήσεις τόσο για τον οργανισμό όσο και για τους συνεργάτες και τους προμηθευτές. Η μελέτη επιδίωξε να προσδιορίσει πώς οι αντιλήψεις διαμορφώνουν τις αποφάσεις σχετικές με τον τύπο των λύσεων ασφάλειας που αποκτώνται από τους οργανισμούς και πώς τα άτομα μέσα και έξω από ένα οργανισμό αντιλαμβάνονται την ετοιμότητα ασφάλειας. Είχε σαν σκοπό επίσης να αποκαλύψει οποιεσδήποτε διαφορές αντίληψης μεταξύ των διαφορετικών ρόλων (παραδείγματος χάριν, ενδιάμεσου επιπέδου διευθυντές σε σύγκριση με την ανώτερη διοίκηση) μέσα σε κάθε επιχείρηση.

Η κλίμακα αξιολόγησης κυμάνθηκε από 1 (η κατάσταση ασφάλειας είναι χαμηλού επιπέδου) ως 7 (η κατάσταση ασφάλειας είναι σε άριστο επίπεδο). Η κλίμακα σπουδαιότητας κυμάνθηκε από 1 (η κατάσταση ασφάλειας αντιμετωπίζεται ως μη σημαντική) ως 7 (αντιμετωπίζεται ως πολύ σημαντική).

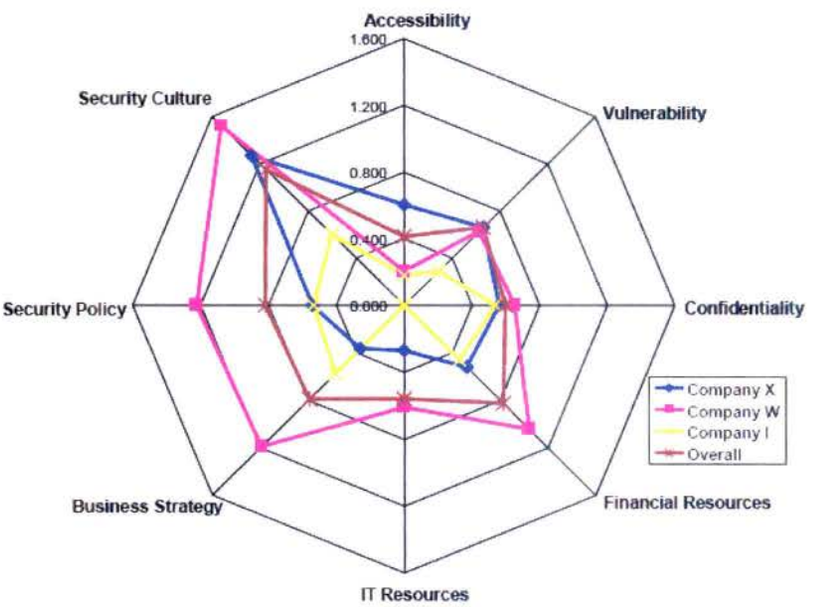
Τα αποτελέσματα της μελέτης παρουσίασαν σημαντικά χάσματα (gap analysis[33]) μεταξύ των απαντήσεων των συμμετεχόντων αναφορικά με τη σπουδαιότητα των οκτώ υποδομών του "σπιτιού της ασφάλειας" (σχήμα 6), και της αξιολόγησής τους ως προς την τρέχουσα ετοιμότητα του οργανισμού τους σε αυτούς τους τομείς. Οι οκτώ υποδομές ασφάλειας περιλαμβάνουν την κουλτούρα ασφάλειας, τη δυνατότητα πρόσβασης, την ευπάθεια, την εμπιστευτικότητα, τους οικονομικούς πόρους, τους πόρους IT, την επιχειρησιακή στρατηγική, και την πολιτική ασφάλειας. Η ενημέρωση

---

[33]Gap analysis: Ανάλυση χάσματος είναι η μελέτη των διαφορών μεταξύ δυο διαφορετικών καταστάσεων ή μοντέλων , (π.χ. μεταξύ του που είμαστε τώρα, και του που θα έπρεπε να είμαστε) και συχνά για τον καθορισμό του πως θα πάμε από τη μία κατάσταση, σε μια νέα κατάσταση.

(awareness) για ορθές πρακτικές ασφάλειας ήταν πολύ μικρότερη από αυτήν που οι συμμετέχοντες είχαν την αντίληψη ότι απαιτείτο. Το μεγαλύτερο χάσμα (σχήμα 9) ήταν μεταξύ της αντίληψης της σημαντικότητας της κουλτούρας ασφάλειας και της αξιολόγησής της στις επιχειρήσεις που ερευνήθηκαν. Άλλα συμπεράσματα από τη μελέτη περιλαμβάνουν τη συνειδητοποίηση ότι οι οργανισμοί εστιάζουν στην δική τους ασφάλεια αγνοώντας την ασφάλεια των συνεργατών, των προμηθευτών, και των πελατών. Ότι άνθρωποι σε διαφορετικά επίπεδα μέσα σε ένα οργανισμό δεν είναι ισοδύναμα ενημερωμένοι σχετικά με τα εργαλεία ασφάλειας και τις καλύτερες πρακτικές και ότι οι ανώτεροι υπάλληλοι έχουν ισχυρή αντίληψη ως προς την σπουδαιότητα της ανάγκης να βελτιωθεί ο τρέχων τρόπος αντιμετώπισης του ζητήματος της ασφάλειας.

Η μελέτη του MIT αποκάλυψε ότι τέτοια χάσματα είναι διαδεδομένα (σχήμα 9).



Σχήμα 9: Αποτελέσματα έρευνας MIT 2006. Gap analysis μεταξύ Σπουδαιότητας και Αξιολόγησης για τις 8 υποδομές του σπιτιού της ασφάλειας. Πηγή http://ebusiness.mit.edu

Αυτό που αποδεικνύεται, μεταξύ των άλλων, από την έρευνα του MIT είναι ότι οι οργανισμοί κατά κανόνα δεν δίνουν τη κατάλληλη βαρύτητα για τη διαμόρφωση της

αναγκαίας κουλτούρας ασφάλειας και τη παροχή της κατάλληλης ενημέρωσης που πρέπει να έχει το προσωπικό, παραβλέποντας τη σημαντικότητά τους στη συνολική ασφάλεια.

7.3. Οργανωσιακή κουλτούρα

Η δημιουργία μιας οργανωσιακής κουλτούρας ολικής ποιότητας είναι μια από τις μεγαλύτερες προκλήσεις ενός προγράμματος Διοίκησης Ολικής Ποιότητας. Η ίδια η επιβίωση μιας οργάνωσης μπορεί να εξαρτηθεί από το πώς θα προσαρμόσει την κουλτούρα της σε ένα επιχειρηματικό περιβάλλον όπου οι αλλαγές είναι καταιγιστικές καθώς επίσης και στις νέες απαιτήσεις των πελατών της (J. Bank, 2000:140). Η έννοια της κουλτούρας προέρχεται από την πολιτισμική ανθρωπολογία και είναι αρκετά δύσκολη να ορισθεί. Ο πιο πλήρης ορισμός είναι αυτός του E. Schein (1985): «Κουλτούρα είναι ένα δομημένο σύνολο από βασικές παραδοχές, που έχουν ανακαλυφθεί - εφευρεθεί ή αναπτυχθεί από μια δεδομένη ομάδα καθώς αυτή μαθαίνει να αντιμετωπίζει προβλήματα εξωτερικής προσαρμογής ή εσωτερικής ολοκλήρωσης - οι οποίες έχουν αποδώσει ικανοποιητικά στο παρελθόν ώστε να θεωρούνται ότι ισχύουν γενικά και επομένως μπορούν να διδαχθούν σε νέα μέλη ως ο σωστός τρόπος αντίληψης, σκέψης, αίσθησης σχετικά με τα προβλήματα αυτά».

Κατά τον E. Schein η κουλτούρα είναι ένα αποτέλεσμα μάθησης μέσα από ομαδική εμπειρία και έχει σημασία μόνο αναφορικά με την ομάδα αυτή. Εμπεριέχεται, δηλαδή, στην έννοια το «γίγνεσθαι» εκτός από το «είναι». Μια οργάνωση είναι μια κουλτούρα - ή έχει μια κουλτούρα - όμως από την άλλη μεριά δημιουργεί, παράγει αυτήν την κουλτούρα (Berger & Luckmann). Υπάρχει μια διαλεκτική σχέση «αιτίου - αιτιατού» μεταξύ ανθρώπινων σχέσεων και κουλτούρας ή ακόμα μεταξύ οργανισμού και κουλτούρας (Thevenet & Schein).

Συνθέτοντας τους προηγούμενους ορισμούς, η κουλτούρα θα μπορούσε να ορισθεί ως ένα σύστημα κοινών (shared - μοιρασμένων) αξιών, πιστεύω, βασικών παραδοχών, σημασιών, άτυπων κανόνων, το οποίο ως κοινό νοητικό πλαίσιο αναφοράς (συλλογικός νοητικός προγραμματισμός - programmation collective de l' esprit humain-Hofstede) συνδέει τους ανθρώπους προσδιορίζοντας το πώς σκέφτονται και συμπεριφέρονται, τι κάνουν, πώς το κάνουν, γιατί το κάνουν (Μπουραντάς, 2002:544).

7.4. Σχηματισμός της κουλτούρας

Η κουλτούρα μιας ομάδας ή μιας οργάνωσης είναι αποτέλεσμα εξελικτικής πορείας, μάθησης και απασχόλησε τους ερευνητές. Ο Kilman αναφέρει ότι «η κουλτούρα διαμορφώνεται κάπως γρήγορα, με βάση την αποστολή, τις ρυθμίσεις, και τις απαιτήσεις γύρω από την έννοια «επιτυχία», υψηλή ποιότητα, αποδοτικότητα, εξυπηρέτηση πελάτη, αξιοπιστία προϊόντων, καινοτομίες, σκληρή δουλειά...». Και αλλού αναφέρει ο ίδιος: «Η κουλτούρα δεσμεύει τη φαντασία και την ενέργεια των ανθρώπων. Τα συστήματα αμοιβών, οι πολιτικές, οι διαδικασίες που διαμορφώνονται δείχνουν ποια είδη συμπεριφοράς και ποιες στάσεις είναι απαραίτητες για την επιτυχία...». Ο Selznick μιλάει για τις διαδικασίες «ενσωμάτωσης» αξιών σε οργανωτικές δομές μέσα από προσδιορισμό της αποστολής, τα προγράμματα, τον τρόπο επιλογής και αξιολόγησης, ενώ από το χώρο των ομάδων οι M. Sheriff, Asch, Blake and Mouton περιγράφουν τον τρόπο σχηματισμού νορμών της ομάδας. Ιδιαίτερα «η αρχή της αυτοκίνησης» (The autokinetic principle) του πρώτου περιγράφει και εξηγεί τον εξελικτικό τρόπο σχηματισμού της κουλτούρας, ως ενός συνόλου νορμών. Μετεγενέστερα, οι Blake & Mouton εξηγούν το σχηματισμό κουλτούρας (κλίματος ή climate όπως την ονομάζουν) σαν αλληλεπίδραση μεταξύ της οργάνωσης και των ατόμων. Ο E. Schein υπογραμμίζει ότι υπάρχουν διάφορες εξηγήσεις γύρω από το σχηματισμό της κουλτούρας και συνοψίζει τρία ρεύματα στη θεωρία που συμβάλλουν το καθένα από τη σκοπιά του στην εξήγηση του πως σχηματίζεται μια κουλτούρα. Πρόκειται για την ψυχοδυναμική θεωρία (δυναμική ομάδων), τη θεωρία της ηγετικής συμπεριφοράς και τη θεωρία μάθησης. Ο Bosche και η Lemaitre αναφέρουν μια ενδιαφέρουσα απογραφή εξωτερικών δεικτών της κουλτούρας και ο Kilman εξηγεί ότι ενώ στην αρχή η κουλτούρα δομείται γύρω από «κρίσιμα περιστατικά», μετά αποκτά ταυτότητα μόνη της και εμφανίζεται σαν μια χωριστή μεταβλητή / γνώρισμα της οργάνωσης. (Μπουραντάς, 2002:547)

Σύμφωνα με τον Kilmann το χάσμα κουλτούρας ή όπως το αποκαλεί «χάσμα κλίματος» είναι μια απόκλιση ανάμεσα στην ιδανική κουλτούρα και την πραγματική. Σύμφωνα με τον ίδιο συγγραφέα αυτό το χάσμα υπάρχει όταν η «κοινωνική ενέργεια» που δημιουργεί η κοινή κουλτούρα «πιέζει τα μέλη» να κινηθούν με πρότυπα συμπεριφοράς τα οποία έχουν ενδεχομένως ξεπεραστεί ή είναι ακατάλληλα (Kilman). Επίσης από τους Harris, Cronel και Handy έχει υποστηριχθεί η ύπαρξη χάσματος κουλτούρας οφειλόμενο σε διαφορά αντίληψης μεταξύ των μελών μιας

οργάνωσης. Αναμφισβήτητα, χάσμα κουλτούρας δημιουργείται επίσης όταν οι υποκουλτούρες των διάφορων τμημάτων, ομάδων κ.λπ. της ίδιας οργάνωσης διαφέρουν μεταξύ τους λίγο ή πολύ. (Schein, Handy)

7.5. Κουλτούρα ασφάλειας

Η κουλτούρα ασφάλειας αποτελεί μια από τις υποδομές στο 'Σπίτι της ασφάλειας' (MIT,2006) καθώς διαμορφώνει το κατάλληλο υποστηρικτικό περιβάλλον που είναι απαραίτητο για την εφαρμογή των πρακτικών ασφάλειας Πληροφοριακών Συστημάτων. Οι σημερινές επιχειρήσεις και οργανισμοί απαιτείται να έχουν μια κουλτούρα ασφάλειας που να είναι κυρίαρχη στο σύνολο της οργάνωσης, και που να ευθυγραμμίζει τους ανθρώπους και τις πρακτικές με τους στόχους ασφάλειας.

Με τον όρο κουλτούρα ασφάλειας, εννοούμε ότι οι χρήστες των πληροφοριακών συστημάτων αποκτούν κοινή αντίληψη και γνώση για την ανάγκη προστασίας και τους στόχους ασφάλειας. Δημιουργούνται έτσι κοινές πρακτικές και πεποιθήσεις που αφορούν στην ανάγκη και τους τρόπους προστασίας των πληροφοριακών συστημάτων και αναπτύσσεται κουλτούρα ασφάλειας. (Καρύδα, 2004:382)

Η κουλτούρα ασφάλειας μιας οργάνωσης, επίσης, μπορεί να ορισθεί ως οι κοινές πεποιθήσεις και στάσεις των εργαζόμενων ως προς τους στόχους και τις πρακτικές ασφάλειας. Εάν, παραδείγματος χάριν, οι περισσότεροι υπάλληλοι τείνουν να αντιστέκονται και να παρακάμπτουν τις πολιτικές ασφάλειας, τότε η κουλτούρα ασφάλειας είναι φτωχή. Ενώ εάν οι περισσότεροι εργαζόμενοι υιοθετούν τις πολιτικές ασφάλειας και τις βλέπουν σαν ένα αναπόσπαστο τμήμα της εργασίας τους, τότε η κουλτούρα ασφάλειας είναι εποικοδομητική. (K.Knapp T.Marshall, 2007:56)

Η έννοια της δημιουργίας και της καλλιέργειας της κουλτούρας ασφάλειας μέσα σε κάθε οργανισμό —όπου οι υπάλληλοι έχουν υιοθετήσει το σύνολο των βασικών αρχών της ασφάλειας, λαμβάνουν διαρκώς κατάρτιση επάνω στις καλύτερες πρακτικές ασφάλειας, και αναλαμβάνουν την ευθύνη των ενεργειών τους —έχει γίνει δημοφιλής και τυγχάνει ευρείας υποστήριξης. (CISCO, 2007)

Η σημασία που έχει η κουλτούρα ασφάλειας σε έναν οργανισμό φαίνεται στα ακόλουθα: Μια πολιτική ασφάλειας, όσο πλήρης και λεπτομερειακή και αν είναι, δε μπορεί ποτέ να καλύψει το σύνολο των απαιτήσεων για την ασφάλεια των πληροφοριακών συστημάτων, αφενός διότι η τεχνολογία αναπτύσσεται με γοργούς ρυθμούς, αφετέρου διότι οι λειτουργίες των περισσότερων οργανισμών δεν είναι

στατικές, αλλά αλλάζουν σε συνάρτηση με το περιβάλλον, που είναι δυναμικό και επίσης μεταβάλλεται με γρήγορους ρυθμούς. Συνεπώς, είναι αναμενόμενο οι χρήστες των πληροφοριακών συστημάτων να αντιμετωπίζουν καταστάσεις ή νέες απειλές κατά των πληροφοριακών συστημάτων που δεν έχουν προβλεφθεί, και για τις οποίες δεν υπάρχει σαφής καθοδήγηση από το έγγραφο στο οποίο περιγράφεται η πολιτική ασφάλειας. Στις περιπτώσεις αυτές, οι χρήστες των πληροφοριακών συστημάτων θα πρέπει να έχουν μια γενικότερη γνώση και να συμμερίζονται τους στόχους της πολιτικής ασφάλειας, ώστε να είναι σε θέση να δράσουν με τρόπο που θα συντελεί στην προστασία των πληροφοριακών συστημάτων. Επομένως, η κουλτούρα ασφάλειας συμβάλλει στην αποτελεσματικότερη αντιμετώπιση των απειλών κατά των πληροφοριακών συστημάτων.

Όλες οι προφυλάξεις ασφάλειας, τελικά εξαρτώνται από το ίδιο τον χρήστη για την επιβολή τους. Είναι σημαντικό η προσπάθεια για περισσότερη ασφάλεια να μην πέσει στην «παγίδα της τεχνολογίας» ώστε να απαιτεί διαρκώς περισσότερη IT τεχνολογία. Αυτή η κατάσταση εμφανίζεται όταν δίνεται υπερβολική έμφαση επάνω στην ίδια την τεχνολογία, χωρίς να δίνεται μεγάλη προσοχή για τις επιπτώσεις στον ανθρώπινο παράγοντα. Παραδείγματος χάριν, πώς αποδέχονται οι χρήστες τους μηχανισμούς ελέγχου πρόσβασης; Εάν οι χρήστες πρόκειται να τους παρακάμψουν επειδή τους θεωρούν ενοχλητικούς, τότε προφανώς οι μηχανισμοί αυτοί χάνουν την αποτελεσματικότητά τους.

Η κουλτούρα μπορεί να επηρεαστεί από προγράμματα εκπαίδευσης και ενημέρωσης. Ένα καλό επιμορφωτικό πρόγραμμα θα βοηθήσει να χτιστεί μια κουλτούρα ευνοϊκή στην ασφαλειοκεντρική σκέψη μεταξύ των υπαλλήλων.

Η διοίκηση μπορεί να βοηθήσει στο να χτιστεί μια κουλτούρα φιλική στην ασφάλεια μέσω του παραδείγματός της. Εάν η διοίκηση εφαρμόσει καλές πρακτικές ασφάλειας τότε θα ακολουθήσουν και οι υπάλληλοι. Το ίδιο θα συμβεί και στην αντίθετη περίπτωση.

Επομένως σε κάθε περίπτωση θα πρέπει να είναι γνωστές οι συνέπειες της πλημμελούς ασφάλειας των ΠΣ, και αυτή η γνωστοποίηση θα πρέπει να καθοδηγεί στον εντοπισμό των απειλών (threat)[34] και στη συνέχεια στη λήψη προληπτικών μέτρων[35] (preventive measures) για την αποφυγή μιας παραβίασης η μιας

---

[34] Απειλή: Ότι μπορεί να περιορίσει την ασφάλεια ενός ΠΣ

[35] Προληπτικό μέτρο: Μέτρο που αποσκοπεί στην πρόληψη μιας απειλής συγκεκριμένου τύπου.

καταστροφής. Εντούτοις, μόνο τα προληπτικά μέτρα δεν είναι από μόνα τους αρκετά αν δεν συνοδεύονται από την συνεργασία και τη δέσμευση του κάθε εργαζόμενου αναφορικά με την ασφάλεια. Η αντίληψη της ασφάλειας επηρεάζεται άμεσα από την ύπαρξη της κατάλληλης οργανωσιακής κουλτούρας μέσα στην οποία έχει ενσωματωθεί η ασφάλεια. Μια από τις πρωταρχικές επιρροές της (όπως και με τη ΔΟΠ) προέρχεται από την ανάγκη διασφάλισης απέναντι στο ενδεχόμενο της αποτυχίας. Επομένως έχουμε ένα ζήτημα συνειδητοποίησης της ευθύνης του καθενός ως προς την ασφάλεια. Αυτή η συνειδητοποίηση θα δημιουργήσει αναπόφευκτα την κατάλληλη αυτοδέσμευση στο να εφαρμόζονται και να ακολουθούνται οι πολιτικές και οι διαδικασίες ασφάλειας, οδηγώντας έτσι είτε στην εξάλειψη, είτε στη μείωση του μεγέθους επίπτωσης από μια παραβίαση.

7.6. Μέτρηση και αποτίμηση μιας αποτελεσματικής κουλτούρας ασφάλειας

Η δημιουργία προγραμμάτων ενημέρωσης ασφάλειας και η καθιέρωση των καλύτερων πρακτικών για την ενίσχυση της ασφάλειας είναι τα λογικά στοιχεία δράσης, αλλά πρέπει να συνοδεύονται από τη δημιουργία των κατάλληλων δεικτών για την μέτρηση της αποτελεσματικότητας μιας τέτοιας προσπάθειας στο σύνολο της επιχείρησης. Μια προσπάθεια για μια καλή κουλτούρα ασφάλειας περιλαμβάνει ανθρώπους, διαδικασίες, και τεχνολογία. Περιλαμβάνει εργαζόμενους και συνεργάτες σε όλα τα επίπεδα, σε θετικά βήματα για την διασφάλιση των στοιχείων και των δεδομένων. Πρέπει να μετρούνται οι ποιοτικές πλευρές της κουλτούρας ασφάλειας, συμπεριλαμβανομένης της ενημέρωσης επάνω στις πολιτικές ασφάλειας και των διαδικασιών, μαζί με τις ποσοτικές μετρήσεις από τις τεχνολογίες ασφάλειας, όπως ο αριθμός των επιγραμμής (online) προσπαθειών παρείσφρησης, διοχέτευση ιών, και προσπαθειών phishing.

Η συνειδητοποίηση και η συμμόρφωση με τις καλύτερες πρακτικές ασφάλειας στο σύνολο της οργάνωσης μπορούν να μετρηθούν με δείκτες, ακριβώς όπως οι δείκτες των τεχνολογιών ασφάλειας μετρούν για το χρόνο λειτουργίας και διακοπής (uptime/downtime), τις προσπάθειες παρείσφρησης (intrusion attempts), το επικίνδυνο λογισμικό (malware), και τις ευπάθειες (vulnerabilities). Όμως ο προσδιορισμός των δεικτών για τη μέτρηση της αποτελεσματικότητας της κουλτούρας ασφάλειας απαιτεί μια εξέταση επάνω στη δυναμική της οργάνωσης και

την εστίαση στη συμπεριφοριστική (behavioral) διάσταση της ασφάλειας.

Μια μελέτη στη Νορβηγία διαπίστωσε ότι η μέτρηση αυτής της συνειδητοποίησης μπορεί να βελτιώσει τις καλύτερες πρακτικές ασφάλειας μέσα στους οργανισμούς, που οδηγούν σε λιγότερα συμβάντα ασφάλειας (security incidents) λόγω απροσεξίας (carelessness) ή παραμέλησης (neglect). Οι υπάλληλοι πήραν μεγαλύτερη ευθύνη για την ασφάλεια των φυσικών και πληροφοριακών στοιχείων σε ένα τέτοιο περιβάλλον και ανέλαβαν έναν πιο ενεργό ρόλο στην ανακάλυψη και την αναφορά των συμβάντων).

Η ανάπτυξη σύνθετων δεικτών μέτρησης ασφάλειας που είναι απλές και κατανοητές και συνδέονται σαφώς με την επιχείρηση, ταξινομήθηκε σαν πρωταρχική απαίτηση μεταξύ των security leaders στο Fortune 500 firms, σύμφωνα με μια έκθεση του 2006 που δημοσιεύθηκε από Center for Digital Strategies στο Tuck School of Business at Dartmouth και στο Institute for Information Infrastructure Protection. (CISCO, 2007)

Η δημιουργία των δεικτών μέτρησης της κουλτούρας ασφάλειας δεν είναι τόσο απλή ώστε να υπάρχει μια που να ταιριάζει σε κάθε περίπτωση. Κάθε οργανισμός είναι μοναδικός, και οι δείκτες μέτρησης συμπεριφοράς πρέπει να προσαρμοστούν προσεκτικά για να συλλάβουν τη σχετική συμπεριφορά σχετικά με την ασφάλεια και τις διαδικασίες.

Η τελική επιτυχία μιας κουλτούρας ασφάλειας προέρχεται όχι από τη μέτρηση της ενημέρωσης και της συμμόρφωσης, αλλά από τα στοιχεία που παρουσιάζουν λιγότερα σοβαρά συμβάντα ασφάλειας, χαμηλότερα ποσοστά παραμέλησης ή απροσεξίας μεταξύ των υπαλλήλων, των συνεργατών, και των προμηθευτών και πιο αυστηρότεροι έλεγχοι στα δεδομένα και τα στοιχεία, με συνέπεια χαμηλότερα ποσοστά κλοπών και απωλειών, υψηλότερα ποσοστά ανακάλυψης συμβάντων ασφάλειας, υποβολής εκθέσεων, και μετριασμού των αντίκτυπου από συμβάντα ασφάλειας, ο καλύτερος χειρισμός συμβάντων και η ενεργός συμμετοχή από τους ενδιαφερόμενους για την βελτίωση της ασφάλειας σε όλο τον οργανισμό.

7.7. Αρχές για τη δημιουργία κουλτούρας ασφάλειας

Στις 25 Ιουλίου 2002 ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (OECD) υιοθέτησε το κείμενο «*OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*» ως σύστασή του.

Στο κείμενο αυτό αναφέρονται τα εξής:

Η χρήση των ΠΣ και των δικτύων και ολόκληρο το ΙΤ περιβάλλον έχουν αλλάξει εντυπωσιακά από το 1992 όταν αρχικά ο OECD υπέβαλε τις *οδηγίες για την ασφάλεια των ΠΣ*. Αυτές οι συνεχόμενες αλλαγές προσφέρουν σημαντικά πλεονεκτήματα αλλά και απαιτούν να δοθεί μεγαλύτερη έμφαση στην ασφάλεια εκ μέρους των κυβερνήσεων, των επιχειρήσεων, των άλλων οργανισμών και των μεμονωμένων χρηστών που αναπτύσσουν, κατέχουν, παρέχουν, διαχειρίζονται υπηρεσίες και χρησιμοποιούν ΠΣ και δίκτυα ("συμμετέχοντες").

Οι υπολογιστές που εξελίσσονται διαρκώς σε ισχυρότερα συστήματα, οι συγκλίνουσες τεχνολογίες και η διαδεδομένη χρήση του Διαδικτύου έχουν αντικαταστήσει τα κλειστά και αυτόνομα συστήματα και δίκτυα. Σήμερα, οι χρήστες διασυνδέονται όλο και περισσότερο σε υπερεθνικά δίκτυα. Επιπλέον, το Διαδίκτυο υποστηρίζει κρίσιμες υποδομές όπως η ενέργεια, οι μεταφορές και οικονομία, και παίζει σημαντικό ρόλο στο πως επιχειρήσεις εκτελούν τις εργασίες τους, στο πώς οι κυβερνήσεις παρέχουν τις υπηρεσίες στους πολίτες και τις επιχειρήσεις, και πώς ιδιώτες επικοινωνούν και ανταλλάσσουν πληροφορίες. Η φύση και ο τύπος των τεχνολογιών των επικοινωνιών και των υποδομών των πληροφοριών έχουν επίσης αλλάξει σημαντικά. Ο αριθμός και η φύση των συσκευών πρόσβασης έχουν πολλαπλασιαστεί και περιλαμβάνουν σταθερές, ασύρματες και κινητές συσκευές με ένα μεγάλο ποσοστό να έχουν πρόσβαση σε διαρκή σύνδεση. Συνεπώς, έχουν αυξηθεί σημαντικά η φύση, ο όγκος και η ευαισθησία των πληροφοριών που ανταλλάσσονται.

Σαν αποτέλεσμα της αυξανόμενης διασυνδεσιμότητας, τα ΠΣ και τα δίκτυα εκτίθενται τώρα σε έναν αυξανόμενο αριθμό και μια ευρυνόμενη ποικιλία απειλών και ευπαθειών. Αυτό αναδεικνύει νέα ζητήματα για την ασφάλεια. Για τους λόγους αυτούς, οι οδηγίες ισχύουν για όλους τους συμμετέχοντες στη νέα κοινωνία της πληροφορίας και προτείνουν την ανάγκη για μια μεγαλύτερη συνειδητοποίηση και κατανόηση των ζητημάτων ασφάλειας και την ανάγκη να αναπτυχθεί μια κουλτούρα ασφάλειας.

7.7.1. **Προς μια κουλτούρα ασφάλειας**

Αυτές οι οδηγίες αποκρίνονται στις απαιτήσεις ενός διαρκώς μεταβαλλόμενου περιβάλλοντος ασφάλειας, με την προώθηση της ανάπτυξης μιας κουλτούρας ασφάλειας – δηλαδή της εστίασης στην ασφάλεια κατά την ανάπτυξη των ΠΣ και των δικτύων και την υιοθέτηση νέων τρόπων σκέψης και συμπεριφοράς στην χρήση

και την αλληλεπίδραση με τα ΠΣ και τα δίκτυα. Οι οδηγίες επισημαίνουν την ανάγκη να μην εξετάζεται εκ των υστέρων η ασφάλεια στον σχεδιασμό και στη χρήση των δικτύων και των συστημάτων. Οι συμμετέχοντες γίνονται όλο και περισσότερο εξαρτώμενοι από τα ΠΣ, τα δίκτυα και τις σχετικές υπηρεσίες, τα οποία πρέπει να είναι αξιόπιστα και ασφαλή. Μόνο μια προσέγγιση που λαμβάνει υπόψη τα συμφέροντα όλων των συμμετεχόντων, τη φύση των συστημάτων, των δικτύων και σχετικών υπηρεσιών, μπορεί να παρέχει αποτελεσματική ασφάλεια.

Κάθε συμμετέχων είναι σημαντικός παράγοντας για τη διασφάλιση της ασφάλειας. Οι συμμετέχοντες, ανάλογα με τον ρόλο τους, πρέπει να γνωρίζουν τους σχετικούς κινδύνους ασφάλειας και τα προληπτικά μέτρα, να αναλαμβάνουν τις ευθύνες τους και να λαμβάνουν μέτρα προς ενίσχυση της ασφάλειας των ΠΣ και δικτύων.

Για τη διαμόρφωση μιας κουλτούρας ασφάλειας εκτός από την ευρεία συμμετοχή απαιτείται η συμμετοχή της ηγεσίας, που πρέπει να οδηγεί σε μια υψηλή προτεραιότητα στον σχεδιασμό και τη διαχείριση της ασφάλειας, καθώς επίσης και στην κατανόηση της ανάγκης για την ασφάλεια μεταξύ όλων των εμπλεκόμενων. Τα ζητήματα ασφάλειας πρέπει να είναι θέματα άμεσου ενδιαφέροντος και ευθύνης σε όλα τα επίπεδα των κυβερνήσεων, των επιχειρήσεων και για όλους τους εμπλεκόμενους. Αυτές οι οδηγίες αποτελούν την αφετηρία για τη δημιουργία μιας κουλτούρας ασφάλειας στο σύνολο της κοινωνίας. Αυτό θα επιτρέψει να λαμβάνεται υπόψη ο παράγοντας ασφάλεια στο σχεδιασμό και τη χρήση όλων των ΠΣ και δικτύων. Αυτές προτείνουν όπως όλοι οι συμμετέχοντες πρέπει να υιοθετούν και να προάγουν μια κουλτούρα ασφάλειας στον τρόπο που σκέπτονται, προσεγγίζουν και ενεργούν με τα ΠΣ και δίκτυα.

7.7.2. **Στόχοι**

Αυτές οι οδηγίες στοχεύουν:

- Να προωθήσουν μια κουλτούρα ασφάλειας μεταξύ όλων των συμμετεχόντων ως μέσο προστασίας των ΠΣ και των δικτύων.
- Να βελτιώσουν την ενημέρωση σχετικά με τους κινδύνους των ΠΣ και των δικτύων, τις πολιτικές, τις πρακτικές, τα μέτρα και τις διαθέσιμες διαδικασίες για την αντιμετώπιση αυτών των κινδύνων, και την απαίτηση για την υιοθέτηση και την εφαρμογή τους.
- Να ενθαρρύνουν τη μεγαλύτερη εμπιστευτικότητα μεταξύ όλων των συμμετεχόντων στα ΠΣ και τα δίκτυα και στον τρόπο με τον οποίο αυτά

παρέχονται και χρησιμοποιούνται.

- Να δημιουργήσουν ένα γενικό πλαίσιο αναφοράς που θα βοηθήσει τους συμμετέχοντες να κατανοήσουν τα ζητήματα ασφάλειας και του σεβασμού των ηθικών αξιών στην ανάπτυξη και την εφαρμογή κατάλληλων πολιτικών, πρακτικών, μέτρων και διαδικασιών για την ασφάλεια των ΠΣ και των δικτύων.
- Να προωθήσουν την κατάλληλη συνεργασία και αλληλοπληροφόρηση, μεταξύ όλων των εμπλεκομένων στην ανάπτυξη και την εφαρμογή των πολιτικών ασφάλειας, τις πρακτικές, των μέτρων και των διαδικασιών.
- Να προωθήσουν την αντιμετώπιση της ασφάλειας ως σημαντικού στόχου μεταξύ όλων των εμπλεκομένων που συμμετέχουν στην ανάπτυξη ή την εφαρμογή των προτύπων.

7.7.3. **Αρχές**

Οι ακόλουθες εννέα αρχές είναι συμπληρωματικές μεταξύ τους και πρέπει να εξετάζονται μαζί. Αφορούν όλους τους συμμετέχοντες σε όλα τα επίπεδα. Σύμφωνα με αυτές τις οδηγίες, οι ευθύνες των συμμετεχόντων ποικίλλουν ανάλογα με τον ρόλο τους. Η ενημέρωση, η εκπαίδευση, και η αλληλοπληροφόρηση μπορεί να οδηγήσει στην κατανόηση και την υιοθέτηση των καλύτερων πρακτικών ασφάλειας. Οι προσπάθειες ενίσχυσης της ασφάλειας των ΠΣ και δικτύων πρέπει να είναι σύμφωνες με τις αξίες μιας δημοκρατικής κοινωνίας, ιδιαίτερα στην ανάγκη για μια ανοικτή και ελεύθερη ροή των πληροφοριών και σεβασμό στην ιδιωτικότητα των ατόμων[36].

7.7.3.1. *Ενημέρωση (Awareness)*

Οι συμμετέχοντες πρέπει να είναι ενήμεροι της ανάγκης για την ασφάλεια των ΠΣ και των δικτύων και για το τι μπορούν να κάνουν για να ενισχύσουν την ασφάλεια.

Η ενημέρωση σχετικά με τους κινδύνους και τα διαθέσιμα μέτρα προστασίας είναι η πρώτη γραμμή υπεράσπισης για την ασφάλεια των ΠΣ και των δικτύων. Τα ΠΣ και τα δίκτυα μπορούν να απειληθούν ταυτόχρονα και από εσωτερικούς και εξωτερικούς κινδύνους. Οι συμμετέχοντες πρέπει να κατανοήσουν ότι οι αποτυχία των μέτρων

---

[36]εκτός από αυτές τις οδηγίες ασφάλειας, ο ΟΟΣΑ έχει αναπτύξει συμπληρωματικές συστάσεις σχετικά με οδηγίες αναφορικά με άλλα ζητήματα σημαντικά για την παγκόσμια κοινωνία των πληροφοριών. Αφορούν τη μυστικότητα (the 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*) και τη κρυπτογραφία (the 1997 *OECD Guidelines for Cryptography Policy*). Αυτές οι οδηγίες ασφάλειας πρέπει να εξετάζονται από κοινού.

ασφάλειας μπορεί να βλάψει σημαντικά τα συστήματα και τα δίκτυα που βρίσκονται υπό τον έλεγχό τους. Πρέπει επίσης να γνωρίζουν την πιθανότητα πρόκληση ζημιών σε άλλους σαν συνεπεία της αλληλοσύνδεσης και της αλληλεξάρτησης μέσω του διαδικτύου. Οι συμμετέχοντες πρέπει να γνωρίζουν τη διαμόρφωση, τις διαθέσιμες αναβαθμίσεις (updates) για το σύστημά τους, τη θέση του μέσα στα δίκτυα, τις ορθές πρακτικές που μπορούν να εφαρμόσουν για να ενισχύσουν την ασφάλεια, και τις απαιτήσεις των άλλων εμπλεκόμενων.

7.7.3.2. *Ευθύνη (Responsibility)*

Όλοι οι συμμετέχοντες είναι υπεύθυνοι για την ασφάλεια των ΠΣ και των δικτύων.

Οι συμμετέχοντες εξαρτώνται από τα διασυνδεμένα ΠΣ και δίκτυα και πρέπει να συνειδητοποιήσουν την ευθύνη τους για την ασφάλεια τους. Η ευθύνη πρέπει να είναι ανάλογη με τον ρόλο του καθενός. Οι συμμετέχοντες πρέπει να ανασκοπούν τις πολιτικές, τις πρακτικές, τα μέτρα, και τις διαδικασίες τους τακτικά και να αξιολογούν εάν αυτά είναι κατάλληλα για το περιβάλλον τους. Εκείνοι που αναπτύσσουν, σχεδιάζουν και παρέχουν προϊόντα και υπηρεσίες πρέπει να δρομολογούν την ασφάλεια συστημάτων και δικτύων και να διανέμουν τις κατάλληλες πληροφορίες συμπεριλαμβανομένων των αναβαθμίσεων κατά τρόπο έγκαιρο έτσι ώστε οι χρήστες να είναι περισσότερο ικανοί να κατανοήσουν τη λειτουργική ασφάλεια των προϊόντων και των υπηρεσιών και τις ευθύνες τους σχετικά με την ασφάλεια.

7.7.3.3. *Αντίδραση (Response)*

Οι συμμετέχοντες πρέπει να ενεργούν κατά τρόπο έγκαιρο και συνεργατικό για να εμποδίσουν (prevent), να ανιχνεύσουν (detect) και να αντιδράσουν (respond) σε συμβάντα ασφάλειας.

Αναγνωρίζοντας την αλληλοσύνδεση των ΠΣ και των δικτύων και τη δυνατότητα για γρήγορη και ευρεία διασπορά ζημίας, οι συμμετέχοντες πρέπει να ενεργήσουν κατά τρόπο έγκαιρο και συνεργατικό για να εξετάσουν τα συμβάντα ασφάλειας. Πρέπει να μοιραστούν τις πληροφορίες για τις απειλές και τις ευπάθειες, ανάλογα με την περίπτωση, και να εφαρμόσουν τις διαδικασίες για γρήγορη και αποτελεσματική συνεργασία για να αποτρέψουν, να ανιχνεύσουν και να αντιδράσουν στα συμβάντα ασφάλειας. Όπου επιτρέπεται, μπορεί να απαιτείται η διασυνοριακή διανομή πληροφοριών και συνεργασία.

7.7.3.4. *Ηθική (Ethics)*

Οι συμμετέχοντες πρέπει να σέβονται τα νόμιμα συμφέροντα (legitimate interests) των άλλων.

Λαμβάνοντας υπόψη τη διεισδυτικότητα των ΠΣ και των δικτύων στις κοινωνίες μας, οι συμμετέχοντες πρέπει να συνειδητοποιήσουν ότι η δράση ή η απραξία τους μπορεί να βλάψει άλλους. Η ηθική συμπεριφορά είναι επομένως κρίσιμη και οι συμμετέχοντες πρέπει να προσπαθήσουν να αναπτύξουν και να υιοθετήσουν τις καλύτερες πρακτικές και να προωθήσουν μια συμπεριφορά που αναγνωρίζει τις ανάγκες ασφάλειας και σέβεται τα νόμιμα συμφέροντα των άλλων.

7.7.3.5. *Δημοκρατία (Democracy)*

Η ασφάλεια των ΠΣ και των δικτύων πρέπει να είναι συμβατή με τις βασικές αξίες μιας δημοκρατικής κοινωνίας.

Η ασφάλεια πρέπει να εφαρμόζεται κατά τρόπο σύμφωνο με τις αξίες που αναγνωρίζονται από τις δημοκρατικές κοινωνίες συμπεριλαμβανομένων, της ελευθερίας στην ανταλλαγή σκέψεων και ιδεών, της ελεύθερης ροής των πληροφοριών, της εμπιστευτικότητας των πληροφοριών και της επικοινωνίας, της κατάλληλης προστασίας των προσωπικών πληροφοριών, της ειλικρίνειας και της διαφάνειας.

7.7.3.6. *Αποτίμηση επικινδυνότητας (Risk assessment)*

Οι συμμετέχοντες πρέπει να διεξάγουν αποτιμήσεις επικινδυνότητας.

Η αποτίμηση επικινδυνότητας προσδιορίζει τις απειλές και τις ευπάθειες και πρέπει να γίνεται σε ευρεία βάση για να καλύπτει τους βασικούς εσωτερικούς και εξωτερικούς παράγοντες, όπως η τεχνολογία, τους φυσικούς και τους ανθρώπινους παράγοντες, τις πολιτικές και τις υπηρεσίες τρίτων με επιπτώσεις στην ασφάλεια. Η αποτίμηση επικινδυνότητας θα επιτρέψει τον προσδιορισμό του αποδεκτού επιπέδου του κινδύνου και θα βοηθήσει στην επιλογή των κατάλληλων μέτρων ελέγχου για τη διαχείριση της επικινδυνότητας, που είναι πιθανό να προκαλέσει ζημιά στα ΠΣ και τα δίκτυα, λαμβάνοντας ταυτόχρονα υπόψη τη φύση και τη σημασία των πληροφοριών που πρέπει να προστατεύονται. Λόγω της αυξανόμενης διασυνδεσιμότητας των ΠΣ, η αποτίμηση επικινδυνότητας πρέπει να περιλαμβάνει την αξιολόγηση της πιθανής ζημιάς που μπορεί να προέλθει από άλλα ή που μπορεί να προκληθεί σε άλλα ΠΣ.

7.7.3.7. *Σχεδιασμός και εφαρμογή ασφάλειας (Design Implementation)*

Οι συμμετέχοντες πρέπει να ενσωματώσουν την ασφάλεια ως συστατικό στοιχείο των ΠΣ και των δικτύων.

Τα συστήματα, τα δίκτυα και οι πολιτικές πρέπει να σχεδιαστούν, να εφαρμοστούν και να συντονιστούν κατάλληλα ώστε να βελτιστοποιήσουν την ασφάλεια. Μια σημαντική, αλλά όχι αποκλειστική, εστίαση αυτής της προσπάθειας είναι ο σχεδιασμός και η υιοθέτηση των κατάλληλων μέτρων και λύσεων προστασίας για την αποφυγή ή την ελαχιστοποίηση της πιθανής ζημιάς από προσδιορισμένες απειλές και ευπάθειες. Τεχνικά και μη τεχνικά μέτρα και λύσεις προστασίας απαιτείται να είναι ανάλογα με την αξία των πληροφοριών στα ΠΣ και τα δίκτυα. Η ασφάλεια πρέπει να είναι ένα συστατικό στοιχείο όλων των προϊόντων, των υπηρεσιών, των συστημάτων και των δικτύων, και αναπόσπαστο τμήμα του σχεδιασμού και της αρχιτεκτονικής των συστημάτων. Για τους τελικούς χρήστες, ο σχεδιασμός και η εφαρμογή ασφάλειας συνίστανται κατά ένα μεγάλο μέρος στην επιλογή και τη διαμόρφωση προϊόντων και υπηρεσιών για το σύστημά τους.

7.7.3.8. *Διαχείριση ασφάλειας (Security management)*

Οι συμμετέχοντες πρέπει να υιοθετήσουν μια ολοκληρωμένη προσέγγιση στη διαχείριση ασφάλειας.

Η διαχείριση ασφάλειας πρέπει να βασίζεται στην αποτίμηση επικινδυνότητας και πρέπει να είναι δυναμική, καλύπτοντας όλα τα επίπεδα δραστηριοτήτων των συμμετεχόντων και όλες τις πτυχές των χειρισμών τους. Πρέπει να περιλαμβάνει την πρόβλεψη για αντίδραση σε μελλοντικές απειλές και να εξετάζει την πρόληψη, την ανίχνευση και την αντίδραση σε συμβάντα ασφάλειας, την αποκατάσταση συστημάτων, την διαρκή συντήρηση, την αναθεώρηση και την επιθεώρηση. Οι πολιτικές ασφάλειας των ΠΣ και δικτύων, οι πρακτικές, τα μέτρα και οι διαδικασίες πρέπει να συντονιστούν και να ενσωματωθούν για να δημιουργήσουν ένα ολοκληρωμένο σύστημα ασφάλειας. Οι απαιτήσεις της διαχείρισης ασφάλειας εξαρτώνται από το επίπεδο εμπλοκής, το ρόλο του συμμετέχοντος, τον εμπεριεχόμενο κίνδυνο και τις απαιτήσεις του συστήματος.

7.7.3.9. *Επαναξιολόγηση (Reassessment)*

Οι συμμετέχοντες πρέπει να αναθεωρούν και να επαναξιολογούν την ασφάλεια των ΠΣ

και των δικτύων, και να πραγματοποιούν τις κατάλληλες τροποποιήσεις στις πολιτικές, τις πρακτικές, τα μέτρα και τις διαδικασίες ασφάλειας.

Νέες και μεταβαλλόμενες απειλές και ευπάθειες ανακαλύπτονται συνεχώς. Οι συμμετέχοντες διαρκώς πρέπει να αναθεωρούν, να επαναξιολογούν και να τροποποιούν όλες τις πτυχές της ασφάλειας σε συνάρτηση με τους εξελισσόμενους κινδύνους.

7.8. Αλλαγή κουλτούρας

Η αποτελεσματικότητα ενός προγράμματος ασφάλειας εξαρτάται τελικά από τη συμπεριφορά των ανθρώπων. Η συμπεριφορά, με τη σειρά της, εξαρτάται από το τι ξέρουν οι άνθρωποι, το πώς αισθάνονται, και τι τους υπαγορεύουν τα ένστικτά τους να κάνουν. Μολονότι ένα επιμορφωτικό πρόγραμμα ενημέρωσης μπορεί να μεταδώσει γνώσεις ασφάλειας ΠΣ, σπανίως επιδρά στα συναισθήματα των ανθρώπων σχετικά με την ευθύνη τους ως προς την ασφάλεια ή τα βαθύτερα ένστικτα τους ως προς την ασφάλεια. (S. Stahl, 2007:565)

Το αποτέλεσμα είναι συχνά ένα χάσμα μεταξύ των απαιτήσεων της πολιτικής ασφάλειας και της συμπεριφοράς των ανθρώπων. Ο ρόλος της κουλτούρας είναι να κλείσει αυτό το χάσμα. Είναι ευθύνη της διοίκησης να παρθούν τα κατάλληλα μέτρα που απαιτούνται για να αλλαχτεί ο τρόπος με τον οποίο η οργάνωση αντιλαμβάνεται, σκέφτεται, και αισθάνεται σε σχέση με τα προβλήματα ασφάλειας ΠΣ και να ενσωματωθεί η κουλτούρα ασφάλειας στην οργανωσιακή κουλτούρα.

Για την αλλαγή της κουλτούρας δεν υπάρχει συνταγή ή στερεότυπη μεθοδολογία. Αντίθετα, η διαδικασία, οι ρόλοι, οι μέθοδοι και τα εργαλεία της αλλαγής της κουλτούρας πρέπει να είναι εξειδικευμένα για την κάθε περίπτωση που συνήθως είναι μοναδική. (Μπουραντάς, 2002:570)

Βασικά της προσέγγισης αλλαγής της κουλτούρας πρέπει να είναι:

- *Συστημική προσέγγιση:* Η κουλτούρα αποτελεί μια ολότητα αποτελούμενη από επιμέρους στοιχεία. Συνεπώς η αλλαγή της απαιτεί τη σύλληψη και τη διαχείριση τόσο της ολότητας (big picture) όσο και των επιμέρους στοιχείων αυτής.
- *Συμμετοχική προσέγγιση:* Κουλτούρα σημαίνει κοινές ενστερνισμένες από όλους αξίες, πιστεύω, σημασίες, πεποιθήσεις κ.λπ. Συνεπώς, η συμμετοχή όσο το δυνατόν μεγαλύτερου αριθμού στελεχών και εργαζομένων είναι απαραίτητη.

4. *Διαμόρφωση των νέων στοιχείων:* Σύμφωνα με το «χάσμα κουλτούρας» διαμορφώνονται τα νέα στοιχεία αυτής όπως όραμα, αξίες αρχές, πιστεύω κ.λπ. Σημαντικό ζήτημα εδώ είναι ο προσδιορισμός των νέων ρόλων, συμπεριφορών, ικανοτήτων και πρακτικών που συνεπάγονται τα νέα στοιχεία της κουλτούρας.
5. *Σχέδιο αλλαγής:* Στο σχέδιο αλλαγής, πρώτον, προσδιορίζονται και προγραμματίζεται οι ενέργειες, οι μέθοδοι τα μέσα κ.λπ. για την επικοινωνία, την διάδοση, την αποδοχή και την ενστέρνιση των νέων στοιχείων της κουλτούρας από όλους τους εργαζομένους. Δεύτερον, προσδιορίζεται και προγραμματίζονται η υλοποίηση των αλλαγών στις δομές, στα συστήματα (κυρίως στα συστήματα Διοίκησης Ανθρώπινων Πόρων) που πρέπει να γίνουν ώστε να προσαρμοσθούν στις απαιτήσεις της νέας κουλτούρας. Ασφαλώς κατά το σχεδιασμό των αλλαγών λαμβάνονται υπόψη οι αντιστάσεις σε αυτές και προσδιορίζονται οι ρόλοι που πρέπει να παιχθούν για την υλοποίηση τους.
6. *Υλοποίηση σχεδίων αλλαγής:* Τα σχέδια αλλαγών υλοποιούνται.
7. *Παρακολούθηση - αξιολόγηση αποτελεσμάτων:* Η υλοποίηση των αλλαγών παρακολουθούνται, αντιμετωπίζονται προβλήματα ή αποκλίσεις, ελέγχονται τα αποτελέσματα και γίνονται πιθανές διορθώσεις.

Η δημιουργία μιας κουλτούρας που αντιλαμβάνεται, σκέφτεται, και αισθάνεται σωστά όσον αφορά τα προβλήματα ασφάλειας ΠΣ, μπορεί να συμβεί μόνο βαθμιαία καθώς θα εξελίσσεται σε μια οργάνωση που μαθαίνει (learning organization) την ασφάλεια. (S. Stahl, 2007:558)

7.9. Οργάνωση που μαθαίνει την ασφάλεια

Σύμφωνα με τον ορισμό του Peter Senge (1990) που θεωρείται ένας από τους πρωτεργάτες της Μαθησιακής Οργάνωσης, καθώς και άλλων γνωστών συγγραφέων, η Μαθησιακή Οργάνωση είναι εκείνη η οργάνωση που μέσω της συνειδητής και σκόπιμης χρήσης των μαθησιακών διαδικασιών σε ατομικό, ομαδικό και οργανωσιακό επίπεδο, της συνεχούς αξιοποίησης της εμπειρίας και του συνεχούς πειραματισμού μαθαίνει διαρκώς, δημιουργεί νέα κοινή γνώση, αναπτύσσει νέα νοητικά μοντέλα ώστε να επιτύχει την προσαρμογή της στο περιβάλλον και την προσαρμογή του περιβάλλοντος σε αυτήν και έτσι διαρκώς να εξασφαλίζει το μέλλον που επιθυμεί. Αξίζει να τονιστεί ότι η Μαθησιακή Οργάνωση ως έννοια και πρακτική

συμπεριλαμβάνει την Ολική Ποιότητα. (Δ. Μπουραντάς, 2002:478)

Ένας οργανισμός που μαθαίνει την ασφάλεια (συμφώνα με τον ορισμό που δίνει ο D.Garvin (1993:78) για learning organization), είναι ένας οργανισμός που έχει τη δυνατότητα να δημιουργεί, να αποκτά, και να μεταφέρει τη γνώση για την ασφάλεια και που τροποποιεί τη συμπεριφορά του ώστε να αντανακλά τη νέα γνώση και ιδέες. Στο έργο Fifth Discipline, ο Peter Senge, προσδιόρισε πέντε βασικές αρχές που είναι προϋποθέσεις για τη δημιουργία ενός οργανισμού που μαθαίνει. Αυτές είναι:

1. Προσωπική κυριαρχία (Personal Mastery)

Οι άνθρωποι που χαρακτηρίζονται από υψηλό επίπεδο «προσωπικής κυριαρχίας» συνειδητοποιούν το ποιοι είναι, που θέλουν και πώς να πάνε, τις συνέπειες των πράξεων, των συναισθημάτων και των αποτελεσμάτων τους. Επίσης διακρίνονται από ένα αίσθημα αποστολής, αυτογνωσία και διάθεση για συνεχή ανάπτυξη, πράγματα που αποτελούν το θεμέλιο της μάθησης.

Η εφαρμογή αυτής της αρχής δημιουργεί ένα περιβάλλον όπου οι άνθρωποι δεν φοβούνται να αναγνωρίσουν την ανεπάρκεια των γνώσεών τους σχετικά με την ασφάλεια, που τους βοηθά να γνωρίσουν τους σημαντικούς κινδύνους που μπορεί προξενήσει η συμπεριφορά τους στην ασφάλεια, και να κατανοήσουν με σαφήνεια τις ευθύνες που έχουν ως προς την ασφάλεια. Αυτό μπορεί να οδηγήσει σε μια κουλτούρα ασφάλειας όπου υπάρχει συνειδητοποίηση σχετικά με τους κινδύνους που υπάρχουν και του τι πρέπει να κάνουν όλοι ώστε να αντιμετωπισθούν αυτοί οι κίνδυνοι.

2. Νοητικά πρότυπα (Mental Models)

Τα νοητικά μοντέλα συνίστανται σε υποθέσεις, παραδοχές, γενικεύσεις, σημασίες, εικόνες κ.λπ. οι οποίες προσδιορίζουν το πώς αντιλαμβανόμαστε και κατανοούμε τον κόσμο ή την πραγματικότητα, το πώς σκεφτόμαστε και ενεργούμε.

Αυτή η αρχή παρέχει στους ανθρώπους τα απαραίτητα νοητικά εργαλεία απαραίτητα για την κατανόηση της ασφάλειας των ΠΣ, έτσι ώστε οι αρχές της να εφαρμόζονται σε κάθε περίπτωση όπου οι άνθρωποι μπορούν να βάλουν τα ΠΣ σε κίνδυνο.

3. Κοινό όραμα (Shared Vision)

Το κοινό όραμα ενεργοποιεί - κινητοποιεί τους ανθρώπους για συνεχή βελτίωση και πρόοδο. Η διάθεση για μάθηση και μάλιστα για οργανωσιακή μάθηση δεν μπορεί να υπάρχει αν δεν έχει νόημα. Αυτό το νόημα το δημιουργεί το κοινό όραμα το οποίο θα εκφράζει το προσωπικό όραμα, τις προσωπικές και συλλογικές προσδοκίες, επιθυμίες και όνειρα.

Αυτή η αρχή επιτρέπει τη σύνδεση της ασφάλειας των ΠΣ με την ίδια την επιτυχία ή την αποτυχία της οργάνωσης, και βοηθά τους ανθρώπους να καταλάβουν, παραδείγματος χάριν, πώς μια παραβίαση ασφάλειας θα μπορούσε να προκαλέσει ανεπανόρθωτη βλάβη στον οργανισμό αλλά και στους ίδιους. Αυξάνοντας την ανησυχία των υπαλλήλων σχετικά με την κλοπή ταυτότητας (identity theft) δίνεται η δυνατότητα να συνδεθεί η ασφάλεια με την ηθική του κανόνα: τα προσωπικά δεδομένα του καθενός είναι σε κίνδυνο. Πρέπει να προφυλάσσουμε τα προσωπικά δεδομένα των άλλων όπως εμείς θέλουμε να στηριζόμαστε στους άλλους για να προστατεύουν τα δικά μας.

4. Ομαδική εκμάθηση (Team Learning)

Η σπουδαιότητα της ομαδικής μάθησης προκύπτει από τις σημαντικές συνέργειες που μπορούν να επιτύχουν τα άτομα όταν μαθαίνουν ομαδικά. Ομαδική μάθηση είναι η ικανότητα να αναπτύσουμε «συλλογική εξυπνάδα», «ομαδική νοημοσύνη» και κοινές γνώσεις. Ομαδική μάθηση σημαίνει διάλογος, συμμετοχή όλων στη δημιουργία και μοίρασμα της γνώσης, χτίσιμο της γνώσης του ενός πάνω στη γνώση του άλλου, κατανόηση των νοητικών μοντέλων των άλλων και δημιουργία κοινών νοητικών μοντέλων.

Αυτή η αρχή μπορεί να βοηθήσει τους ανθρώπους να καταλάβουν τους λόγους πίσω από όλους τους κανόνες ασφάλειας. Γενικά στους ανθρώπους δεν αρέσει να ακολουθούν κανόνες, αλλά αναπτύσσουν συμπεριφορά υιοθέτησής τους όταν ανακαλύψουν την αναγκαιότητά τους για τους εαυτούς τους. Παράλληλα δημιουργεί συνθήκες αλληλοεκπαίδευσης μεταξύ των υπαλλήλων και να τους παρακινεί ώστε το θέμα της ασφάλειας να αποτελεί κοινό αντικείμενο ενδιαφέροντος και συζήτησης μεταξύ τους.

5. Συστημική σκέψη (Systems Thinking)

Η συστημική σκέψη αποτελεί βασική αρχή μάθησης αφού μετατρέπει και αυξάνει την ικανότητα:

- ✓ να αντιλαμβανόμαστε και να κατανοούμε το όλο και όχι μόνο τα μέρη
- ✓ να κατανοούμε, να αναλύουμε και να συνθέτουμε αλληλοσυσχετίσεις, αλληλεξαρτήσεις και αλληλεπιδράσεις μεταξύ των μερών που συνιστούν την ολότητα
- ✓ να προσδιορίζουμε και να κατανοούμε βαθιές αιτίες και συμπτώματα και τις σχέσεις μεταξύ τους
- ✓ να χρησιμοποιούμε μια κοινή γλώσσα και ένα κοινό εργαλείο για την κατανόηση, ανάλυση και σύνθεση πολύπλοκων φαινομένων.

Η συστημική σκέψη δίνει τη δυνατότητα να κατανοηθούν πλήρως οι σχέσεις αιτίας και αποτελέσματος (cause-and-effect relationships) που υπάρχουν μεταξύ των γεγονότων, και ότι κάθε τι που κάνουμε μπορεί ταυτόχρονα να είναι και αίτιο και αποτέλεσμα. Επάνω στην κουλτούρα επιδρούν πάρα πολλές δυνάμεις και ένας τεράστιος αριθμός αιτιών και αποτελεσμάτων επιδρούν επάνω στην εξέλιξη της. Αυτή η αρχή επιτρέπει να αναπτυχθεί μια στρατηγική για την ασφάλεια των ΠΣ που θα ευθυγραμμίζει την αλλαγή κουλτούρας ασφάλειας με αυτές τις δυνάμεις.

7.10. Πρακτικές και εργαλεία οργανωσιακής μάθησης

Προκειμένου οι επιχειρήσεις να αναπτύξουν την οργανωσιακή μάθηση και να τείνουν προς τις «μαθησιακές οργανώσεις» εφαρμόζουν πρακτικές και εργαλεία. Οι κύριες πρακτικές για την ανάπτυξη της οργανωσιακής μάθησης αφορούν συνήθως τους παρακάτω τομείς (Δ. Μπουραντάς, 2002:482):

Κουλτούρα μάθησης: έμφαση στην αξία της συνεχούς μάθησης, βελτίωσης, ανάπτυξης και καινοτομίας, στον πειραματισμό, στην κατανόηση των λαθών και αποτυχιών, στην ανάληψη κινδύνου και στο διάλογο.

Οργανωτικές δομές: ευέλικτες, οριζόντιες και αποκεντρωμένες δομές που διευκολύνουν τη συμμετοχή, την ανταλλαγή και διάχυση της γνώσης.

Διαδικασίες λήψης αποφάσεων: ολοκληρωμένα συστήματα πληροφοριών, συστήματα που διευκολύνουν τη διάχυση, την ανταλλαγή και τη μεταφορά της γνώσης.

Διατμηματικές ομάδες: Ομάδες από διαφορετικές λειτουργίες ή οργανωτικές μονάδες, ανεπτυγμένοι μηχανισμοί οριζόντιας συνεργασίας και ολοκλήρωσης.

Εκπαίδευση/ Ανάπτυξη: Σχεδιασμένες, μακροπρόθεσμες εκπαιδευτικές και αναπτυξιακές ενέργειες «στη δουλειά και έξω από τη δουλειά», διαδικασίες μάθησης από την εμπειρία (επιτυχίες, αποτυχίες), διαδικασίες ανταλλαγής εμπειριών και «μοιράσματος» της γνώσης μεταξύ ατόμων, ομάδων, οργανωτικών μονάδων.

Συστήματα διοίκησης ανθρώπινων πόρων: εκτεταμένη χρήση εργαλείων μάθησης, σύστημα αμοιβών, αξιολόγησης, ανάθεσης υπευθυνοτήτων που ενθαρρύνουν, δημιουργούν κίνητρα και υποστηρίζουν τη μάθηση.

7.10.1. **Εργαλεία οργανωσιακής μάθησης**

Για την υποστήριξη της οργανωσιακής μάθησης έχει αναπτυχθεί ένας μεγάλος ορισμός μεθόδων - εργαλείων που έχουν αρχίσει να χρησιμοποιούνται στις «πρωτοπόρες» επιχειρήσεις. Μερικά από αυτά είναι:

Εργαλεία πρώτης γενιάς

- Συστήματα προτάσεων εργαζομένων
- Benchmarking
- Κύκλοι ποιότητας
- Επανασχεδιασμός Επιχειρησιακών διαδικασιών
- Έρευνες ικανοποίησης εργαζομένων
- Έρευνες ικανοποίησης πελατών
- Διαγνωστικές μελέτες, αναπληροφόρηση (feed back) και συμβουλευτικές παρεμβάσεις από εξωτερικούς συμβούλους
- Εργαστηριακά εκπαιδευτικά προγράμματα (σεμινάρια)

Εργαλεία δεύτερης γενιάς

- Διάλογος (διαδικασία κοινής σκέψης, χτίσιμο της γνώσης του ενός πάνω στη γνώση του άλλου)
- Συστήματα διοίκησης της γνώσης (knowledge Management)
- Σενάρια (περιγραφή εναλλακτικών και επιθυμητών εικόνων για το μέλλον, υποθέσεις «what - if)
- Μάθηση από την πράξη (Action learning, μάθηση από την αντιμετώπιση πραγματικών προβλημάτων)

- Εργαστήρια αυτογνωσίας, αλλαγής των νοητικών χαρτών
- Εργαστήρια - συσκέψεις στρατηγικής ανάλυσης, σχεδιασμού και βελτιωτικών αλλαγών
- Καθοδήγηση και συμβουλευτική (coaching, mentoring)
- Προσομειώσεις - πάγια (simuworlds, microworeds)
- Appreciative inquiry (μάθηση μέσω της ανάλυσης σε βάθος των εμπειριών, της συνειδητοποίησης των θετικών δυνάμεων και του επιθυμητού μέλλοντος).

Κεφάλαιο 8

Εκπαίδευση και Ενημέρωση Ασφάλειας

8.1. Εισαγωγή

Σε κάθε Σύστημα Διαχείρισης Ασφάλειας απαιτείται η εκπαίδευση και η ενημέρωση του προσωπικού ώστε να διασφαλιστεί ότι το προσωπικό είναι εκπαιδευμένο και εκτελεί τις εργασίες του και συμπεριφέρεται σύμφωνα με τις απαιτήσεις του Συστήματος Διαχείρισης Ασφάλειας ΠΣ. Όμως οι οργανισμοί, όπως αποδεικνύεται και από μια έρευνα της ENISA[37], για την οποία θα γίνει αναφορά στη συνέχεια, αντιμετωπίζουν την εκπαίδευση σαν κόστος, και συνεπώς θεωρούν ότι αυτή θα πρέπει να περιορίζεται στα απολύτως απαραίτητα.

Αντίθετα η διοίκηση που υιοθετεί της αρχές της Διοίκησης Ολικής Ποιότητας, θεωρεί την εκπαίδευση σαν επένδυση και θεωρεί τις δαπάνες για την εκπαίδευση όλων, ως την καλύτερη επένδυση για την αναβάθμιση των ικανοτήτων του ανθρώπινου δυναμικού της.

Στο κεφάλαιο αυτό αφού γίνει μια εννοιολογική προσέγγιση στην εκπαίδευση ποιότητας, και στα βήματα του κύκλου της εκπαίδευσης στην ποιότητα, αναλύεται η ενημέρωση ασφάλειας. Αφού παρουσιασθεί το μοντέλο ενός προγράμματος ενημέρωσης, στη συνέχεια και με βάση μια έρευνα της ENISA προσεγγίζονται οι τρόποι βελτίωσης της ενημέρωσης, και της μέτρησης της αποτελεσματικότητας των προγραμμάτων ενημέρωσης. Το κεφάλαιο τελειώνει με ένα παράδειγμα ενός ισορροπημένου συνόλου βασικών δεικτών απόδοσης.

8.2. Εκπαίδευση ποιότητας

Μια από τις βασικές αρχές της ολικής ποιότητας είναι η συνεχής εκπαίδευση, η οποία είναι το βασικότερο όπλο για την αλλαγή νοοτροπίας στον οργανισμό. Η εκπαίδευση του ανθρώπινου δυναμικού έχει σαν πρωταρχικό στόχο, να βοηθήσει την εφαρμογή της Διοίκησης Ποιότητας και ν'αναπτύξει τις γνώσεις και τις ικανότητες του κάθε

---

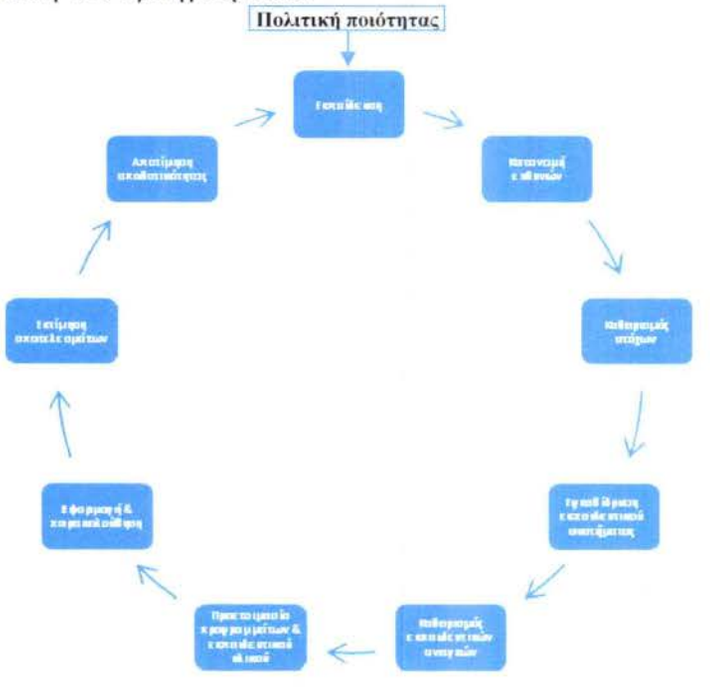
[37]Η ENISA είναι μια αντιπροσωπεία της Ευρωπαϊκής Ένωσης που δημιουργήθηκε για να προωθήσει τη λειτουργικότητα της εσωτερικής αγοράς, συμβουλεύοντας και βοηθώντας τα κράτη μέλη, τους οργανισμούς και τις επιχειρήσεις της ΕΕ στο πώς να εξασφαλίσουν ένα υψηλό και αποτελεσματικό επίπεδο ασφάλειας δικτύων και πληροφοριών.

εργαζόμενου.

Σύμφωνα με την Ιαπωνική άποψη, η εκπαίδευση είναι ο σημαντικότερος παράγοντας στη Διοίκηση Ποιότητας, γιατί λειτουργεί σαν "κλειδί" υποκίνησης για την εφαρμογή της διαρκούς βελτίωσης. Στις σημερινές συνθήκες της κοινωνικής και οικονομικής παγκοσμιοποίησης η ενημέρωση, η πληροφόρηση και η εκπαίδευση θεωρούνται τα τρία βασικά συστατικά στοιχεία της επιβίωσης των ατόμων και κατ' επέκταση των οργανισμών. Οι επιχειρήσεις και οι οργανισμοί απαιτούν από τους εργαζομένους ένα ευρύ φάσμα ικανοτήτων. Για να γίνει αυτό πραγματικότητα πρέπει να σχεδιαστεί ένα εκπαιδευτικό πρόγραμμα το οποίο θα δίνει θεμελιωμένες απαντήσεις σε πέντε καίρια ερωτήματα (Κέφης, 2005:81):

— Ποιο είδος εκπαίδευσης χρειαζόμαστε;
— Ποιοι είναι υποψήφιοι για εκπαίδευση;
— Πώς θα διεξαχθεί η διαδικασία της εκπαίδευσης;
— Πώς θα αξιολογηθεί η αποδοτικότητα του εκπαιδευτικού προγράμματος;
— Πώς θα βελτιωθεί η εκπαιδευτική διαδικασία;

Στο Διάγραμμα 3 απεικονίζονται τα βήματα που ακολουθούνται ώστε να εφαρμοστεί ένα επιτυχημένο εκπαιδευτικό πρόγραμμα. Τα βήματα αυτά συνδέονται μεταξύ τους, αποτελούν μια αλληλουχία κάθε τμήμα της οποίας απαιτεί για την πραγμάτωση του την ολοκλήρωση του προηγούμενου.



Σχήμα 10: Ο κύκλος της εκπαίδευσης στην ποιότητα.
Πηγή: Oakland J.S., *Total Quality Management,* 2nd Edition, Butterworth-Heinemann Ltd, Oxford, 1995

8.2.1. Ενημέρωση (awareness) Ασφαλείας

Υπάρχουν διάφορες προσεγγίσεις ως προς τον ορισμό της ενημέρωσης (awareness) ασφάλειας πληροφοριών. Μία που είναι σύμφωνη με το μοντέλο που ανέπτυξε το U.S. National Institute of Standards and Technology (NIST, 1998) με το έγγραφο SP800-16 "IT Security Training Requirements", και που αντιμετωπίζει την ενημέρωση σαν πρόγραμμα που προηγείται του προγράμματος εκπαίδευσης και στο οποίο παρέχονται οι βασικές έννοιες της ασφάλειας σαν αρχική κατάρτιση, που θα βοηθήσει τους υπαλλήλους στο να παρακολουθήσουν τα εξειδικευμένα και λεπτομερή εκπαιδευτικά μαθήματα θα τους προσφερθούν στη συνέχεια. Ο βασικότερος στόχος αυτού του προγράμματος είναι να προκαλέσει το ενδιαφέρον σε θέματα ασφάλειας πληροφοριών. Μετά από την ενημέρωση, όλοι οι υπάλληλοι πρέπει να λάβουν την συγκεκριμένη, για τη θέση τους, εκπαίδευση στα βασικά της ασφάλειας. (S.D.Hanche, 2007:547)

Η ENISA έχει προσεγγίσει την ενημέρωση ασφάλειας σύμφωνα με τον ορισμό του Information Security Forum (ISF), μιας από τις κύριες παγκόσμιες ανεξάρτητες αρχές στην ασφάλεια πληροφοριών, ο οποίος είναι:

«Ενημέρωση ασφάλειας πληροφοριών είναι μια διαρκής διαδικασία μάθησης που είναι σημαντική για τους παραλήπτες, και παράγει μετρήσιμα οφέλη για τον οργανισμό από τη μόνιμη αλλαγή στη συμπεριφορά».

Σύμφωνα με αυτή τη προσέγγιση, η ενημέρωση ασφάλειας πληροφοριών είναι σημαντικό συστατικό στην ορθή πρακτική για την ασφάλεια. Διάφορα διεθνή πρότυπα αναφέρονται σε αυτή ως προϋπόθεση:

- ISO 27001
- COBIT
- Payment Card Industries – Data Security Standard και
- ISO 9001:2000.

Το πρόγραμμα ενημέρωσης ασφάλειας πρέπει να είναι ένα βασικό στοιχείο στο σχέδιο ασφάλειας ΠΣ κάθε οργανισμού. Εκτός από τα λειτουργικά και τα τεχνικά αντίμετρα που απαιτούνται για να προστατευτεί το σύστημα, η ενημέρωση πρέπει να αποτελεί ουσιαστικό στοιχείο.

Διάφορες στατιστικές έρευνες σχετικά με την ασφάλεια, δείχνουν ότι ένας μεγάλος αριθμός απειλών προέρχεται από το εσωτερικό των οργανισμών. (M. Keeney et. al, 2005) Αυτό σημαίνει ότι οι υπάλληλοι ενός οργανισμού μπορεί είτε σκόπιμα είτε τυχαία, να επιτρέψουν να συμβεί κάποιας μορφής ζημιά στο σύστημα. Σε αυτό

περιλαμβάνονται η χρήση παράνομων αντίγραφων λογισμικού, το κατέβασμα λογισμικού από το Διαδίκτυο, η δημιουργία αδύναμων κωδικών πρόσβασης, ή την έλλειψη προστασίας των κωδικών πρόσβασής τους από τους άλλους. Κατά συνέπεια, οι υπάλληλοι πρέπει να είναι ενήμεροι των κανόνων "καλής συμπεριφοράς" προς τα ΠΣ και πώς να ασκήσουν τις καλές πρακτικές ασφάλειας υπολογιστών.

Οι υπάλληλοι, και ειδικά οι τελικοί χρήστες των ΠΣ, συνήθως δεν γνωρίζουν τις συνέπειες που προκαλούνται από ορισμένες ενέργειες τους στην ασφάλεια. Για τους περισσότερους υπαλλήλους, το ΠΣ είναι ένα εργαλείο που τους βοηθά στην εκτέλεση των εργασιών τους γρηγορότερα και αποτελεσματικότερα, ενώ η ασφάλεια αντιμετωπίζεται μάλλον σαν εμπόδιο, παρά σαν αναγκαιότητα. Κατά συνέπεια, είναι επιτακτικό για κάθε οργανισμό να παρέχει στους υπαλλήλους πληροφορίες σχετικές με την ασφάλεια των ΠΣ, που επισημαίνουν τις απειλές αλλά και τις επιπτώσεις από τη μη ενεργό συμμετοχή τους στην προστασία των ΠΣ. Σε πολλές χώρες, όπως στις ΗΠΑ (νόμος περί ασφάλειας υπολογιστών του 1987), απαιτείται από όλες τις δημόσιες υπηρεσίες η παροχή των σχετικών πληροφοριών ενημέρωσης ασφάλειας σε όλους τους τελικούς χρήστες των ΠΣ.(Hansche, 2007:541) Ανάλογη αύξηση της εστίασης στην ασφάλεια υπάρχει από ρυθμιστικούς οργανισμούς μέσα στα κράτη μέλη της ΕΕ.

Οι υπάλληλοι είναι ένας από τους σημαντικότερους παράγοντες στην διασφάλιση των ΠΣ και των πληροφοριών που επεξεργάζονται. Σε πολλές περιπτώσεις, τα συμβάντα ασφάλειας ΠΣ είναι αποτέλεσμα απροσεξίας και άγνοιας των διαδικασιών και των πολιτικών ασφάλειας ΠΣ. Επομένως, οι ενημερωμένοι και εκπαιδευμένοι υπάλληλοι είναι ένας κρίσιμος παράγοντας στην αποτελεσματική λειτουργία και την προστασία του ΠΣ. Εάν οι υπάλληλοι είναι ενήμεροι των ζητημάτων ασφάλειας, μπορούν να είναι η πρώτη γραμμή άμυνας στην πρόληψη και την έγκαιρη ανίχνευση των προβλημάτων. Επιπλέον, εάν ο καθένας δείχνει ενδιαφέρον και εστιάζει στην ασφάλεια, τότε η προστασία των στοιχείων και των πληροφοριών μπορεί να είναι πολύ ευκολότερη και αποδοτικότερη.

Για να προστατευτούν η εμπιστευτικότητα, η ακεραιότητα, και η διαθεσιμότητα των πληροφοριών, οι οργανισμοί πρέπει να διασφαλίσουν ότι όλα τα εμπλεκόμενα άτομα έχουν κατανοήσει τις ευθύνες τους. Για να το επιτύχουν, οι υπάλληλοι πρέπει να ενημερωθούν επαρκώς για τις πολιτικές και τις απαραίτητες διαδικασίες για τη προστασία των ΠΣ. Υπό αυτήν τη μορφή, όλοι οι τελικοί χρήστες του ΠΣ πρέπει να καταλάβουν τα βασικά της ασφάλειας του ΠΣ και να είναι σε θέση να αποκτήσουν τις

κατάλληλες συνήθειες που ενισχύουν την ασφάλεια, στο καθημερινό περιβάλλον εργασίας τους.

Έτσι αφού αποκτηθεί η απαραίτητη δέσμευση και υποστήριξη από την ανώτερη διοίκηση, και αφού γίνει η κατανομή των σχετικών ευθυνών πρέπει να καθοριστεί σαφώς ο στόχος του προγράμματος συνειδητοποίησης ασφάλειας. Μόλις καθιερωθεί ο στόχος, πρέπει να αποφασιστεί το περιεχόμενο, συμπεριλαμβανομένης της επιλογής του συστήματος εφαρμογής του προγράμματος. Κατά τη διάρκεια αυτής της διαδικασίας, βασικοί παράγοντες που εξετάζονται είναι το πώς θα υπερνικηθούν τα εμπόδια και πως θα αντιμετωπισθούν οι αντιστάσεις. Το τελευταίο στάδιο είναι η αποτίμηση της αποδοτικότητας του προγράμματος.

Συνολικά η αποτελεσματικότερη προσέγγιση σε ένα προγράμματα ενημέρωσης ασφάλειας είναι η διαρκής επαναληπτική διαδικασία, όπως αυτή παρουσιάζεται κατωτέρω (ENISA, 2007):

Σχήμα 11: Επαναληπτική διαδικασία ενημέρωσης ασφαλείας

8.2.1.1. *Σχεδιασμός (PLAN)*

Εισροές: (inputs)

Πολιτική ασφάλειας πληροφοριών, στρατηγική, επιχειρησιακή περίπτωση (business case), αποτίμηση επικινδυνότητας, προϋπολογισμός στόχοι και σκοποί, απαιτήσεις νομοθεσίας/συμμόρφωσης.

Παράγοντες επιτυχίας:

Υποστήριξη διοίκησης, συμμετοχή ολόκληρου του οργανισμού, ενδιαφέρον των

χρηστών, επάρκεια πόρων και χρόνου, κατάλληλη κουλτούρα.

8.2.1.2. *Υλοποίηση (IMPLEMENT)*

Τεχνικές: (techniques)

Κατάρτιση πρόσωπο με πρόσωπο, εισαγωγική κατάρτιση, πολιτική, ιστότοποι ενδοδικτύου, εκπαίδευση μέσω υπολογιστή (CTBs), τεστ και κουίζ.

Παράγοντες επιτυχίας:

Σχετικότητα του υλικού, ευκολία της πρόσβασης και τη χρήση, υποχρεωτική συμμετοχή πέρα από την εθελοντική, εκπαίδευση που στοχεύει σε συγκεκριμένους κινδύνους, ουσιαστική εμπλοκή της διοίκησης.

8.2.1.3. *Αναθεώρηση (REVIEW)*

Τύποι:

Συμβάντα ασφάλειας/βασικές αιτίες πρόκλησης, αποτελέσματα ελέγχων, επιθεώρηση του οργανισμού, τεστ συμπεριφοράς χρηστών, αριθμός προσωπικού που ολοκληρώνει την κατάρτιση.

Παράγοντες επιτυχίας:

Γνώση του αντικειμένου μέτρησης, σχετικότητα της μέτρησης, κανονική και έγκαιρη αξιολόγηση.

8.2.2. **Προσεγγίσεις για τη βελτίωση της ενημέρωσης ασφάλειας**

Η δημιουργία ενός πλαισίου εργασίας για την ενημέρωση ασφάλειας πληροφοριών ξεκινά από την επίσημη πολιτική ασφάλειας. Χωρίς "κανονιστικό" περίγραμμα που να καλύπτει τη χρήση των συστημάτων και των πληροφοριών, και που να επιβάλλει την καλή συμπεριφορά, είναι πολύ δύσκολο να επιτύχει το πρόγραμμα.

Τα πρότυπα καλής πρακτικής (good practice standards) δίνουν ισχυρή έμφαση στην κατοχή μιας πολιτικής ασφάλειας για όλο το εύρος της οργανισμού. Παραδείγματος χάριν, το ISO 27001 προτείνει τους οργανισμούς να υλοποιούν προγράμματα ενημέρωσης και εκπαίδευσης. Μια από τις απαιτήσεις του ISO είναι ότι η διοίκηση έχει διασφαλίσει την εφαρμογή των πολιτικών ασφαλείας εκ μέρους των

εργαζομένων. Για να το επιτύχουν αυτό, οι οργανισμοί, πρέπει να παρέχουν την κατάλληλη κατάρτιση ενημέρωσης και να αναπροσαρμόζουν κανονικά τις οργανωσιακές πολιτικές και διαδικασίες, σχετικά με τις λειτουργίες εργασίας όλων των υπαλλήλων της οργανισμού και, όπου υπάρχουν, των επί σύμβαση και των τρίτων χρηστών.

Παρόμοια, πολλά πρότυπα προτείνουν ή απαιτούν, ότι η κατάρτιση ενημέρωσης των χρηστών πρέπει να περιλαμβάνεται στη πολιτική ασφάλειας ενός οργανισμού. Ένα βασικό στοιχείο οποιασδήποτε πολιτικής ασφάλειας και ενημέρωσης ασφάλειας είναι η ανάλυση απειλών και κινδύνων που αντιμετωπίζει ο οργανισμός. Αυτή η ανάλυση πρέπει να οδηγεί στις περιοχές που πρέπει να καλύψει η πολιτική και η εκπαίδευση.

Κάθε οργανισμός αντιμετωπίζει μεταβαλλόμενα περιβάλλοντα, απειλές και κινδύνους. Για να είναι αποτελεσματικές, οποιεσδήποτε πρωτοβουλίες ενημέρωσης πρέπει να υποστηρίζονται από την ανώτερη διοίκηση. Εάν η ανώτερη διοίκηση δεν αντιμετωπίζει την ενημέρωση ως σημαντική, είναι απίθανο η εκπαίδευση να είναι επιτυχής.

Τα περισσότερα πρότυπα συστήνουν την υιοθέτηση μιας τυποποιημένης προσέγγισης στην ενημέρωση ασφάλειας πληροφοριών. Ένας κατάλληλος κύκλος περιλαμβάνει τρία ενισχυτικά στοιχεία (ENISA, 2007):

1. Ανάλυση απαιτήσεων (Requirements analysis): Είναι αναγκαίο για τη διοίκηση να προσδιοριστεί ποια θέματα πρέπει να κατανοήσει το προσωπικό. Οι χρήστες πρέπει να ενημερωθούν για τα τμήματα της πολιτικής ασφάλειας που είναι σχετικά με τις λειτουργίες της εργασίας τους. Πολλά πρότυπα προτείνουν θέματα που πρέπει να εξετάζονται, όπως είναι το spyware, οι ιοί, οι ισχυροί κωδικοί πρόσβασης κλπ.
2. Κατάρτιση προσαρμοσμένη στο ρόλο (Training tailored to role): Οι υπάλληλοι (συμπεριλαμβανομένων των εργαζόμενων επί σύμβαση), πρέπει να λάβουν την κατάλληλη κατάρτιση, η οποία συνδέεται με το ρόλο τους. Πρέπει επίσης να ενημερώνονται σχετικά με τις αλλαγές στις πολιτικές ασφάλειας και τις διαδικασίες. Επίσης απαιτείται να υπάρχει εκπαίδευση στο πως μπορεί το προσωπικό να εφαρμόσει την ασφάλεια στις καθημερινές διαδικασίες τους.
3. Διαρκής αναθεώρηση (Ongoing review): Το περιεχόμενο του προγράμματος ενημέρωσης πρέπει να αναθεωρείται περιοδικά. Η αποτελεσματικότητα του προγράμματος ενημέρωσης που προορίζεται για συγκεκριμένους συμμετέχοντες πρέπει να αναθεωρείται τακτικά. Οποιεσδήποτε κατάλληλες αλλαγές στην

πρωτότυπη πολιτική ασφάλειας πρέπει να απεικονίζονται στα αντίστοιχα επιμορφωτικά προγράμματα ενημέρωσης ασφάλειας πληροφοριών.

Η ύπαρξη ενός εγκεκριμένου προϋπολογισμού είναι ζωτικής σημασίας για την επίτευξη ενός προγράμματος αποτελεσματικής ενημέρωσης, δεδομένου του ότι απαιτεί χρόνο από το προσωπικό και χρήματα για να δημιουργήσει τα κατάλληλα υλικά. Αυτό το πρόγραμμα αποτελεί μια επένδυση για το μέλλον της επιχείρησης και πρέπει να έχει έγκριση από την ανώτερη διοίκηση.

Παρά την υψηλή προτεραιότητα που δίνεται στην ασφάλεια, πολλοί συμμετέχοντες το βρίσκουν δύσκολο να δικαιολογήσουν τη σημαντικότητα των εξόδων στα προγράμματα ενημέρωσης. Στην έρευνα της ENISA[38] διαπιστώθηκε ότι μόνο το ένα τρίτο των συμμετεχόντων δημιουργεί μια επίσημη επιχειρησιακή περίπτωση (formal business case) για να δικαιολογήσει αυτές τις δαπάνες.

Από αυτούς, μόνο οι μισοί προσπαθούν να μετρήσουν ποσοτικά τα οφέλη που επιτυγχάνουν τα προγράμματα ενημέρωσης, και πολύ λίγες τα αξιολογούν σαν απόδοση μιας επένδυσης (ROI). Το 15% των συμμετεχόντων αποτιμούν τα οφέλη από τα προγράμματά τους ακόμα κι αν δεν προετοιμάζουν μια επίσημη επιχειρησιακή περίπτωση.

Οι περισσότεροι συμμετέχοντες αντιμετωπίζουν την κατάρτιση ενημέρωσης ασφάλειας σαν κάτι που πρέπει να κάνουν, δηλ. σαν απαίτηση στην οποία πρέπει να συμμορφωθούν. Υπό αυτήν τη μορφή, ο προϋπολογισμός τους αντιμετωπίζεται ως γενικά έξοδα παρά σαν μια επένδυση. Αυτό είναι ενδιαφέρον, δεδομένου ότι οι κανονισμοί στα περισσότερα κράτη μέλη της ΕΕ δεν απαιτούν τη συγκεκριμένη κατάρτιση ασφάλειας πληροφοριών. Φαίνεται ότι οι νόμοι προστασίας των δεδομένων της ΕΕ οδηγούν μια αύξηση στην κατάρτιση ενημέρωσης.

Μόλις καθοριστεί ο στόχος ενός προγράμματος ενημέρωσης ασφάλειας πληροφοριών, το επόμενο βήμα είναι να συνταχτεί ένα σχέδιο επικοινωνίας. Αυτό

---

[38] Η έρευνα διεξήχθη το χρονικό διάστημα Μαΐου-Ιουλίου του 2007 χρησιμοποιώντας ένα δομημένο ερωτηματολόγιο. Κλήθηκαν να συμμετάσχουν αρμόδιοι για την ασφάλεια πληροφοριών σε ευρωπαϊκές κυβερνητικές υπηρεσίες και επιχειρήσεις. Ανταποκρίθηκαν 67 οργανισμοί από εννέα διαφορετικές ευρωπαϊκές χώρες. Το μέγεθος των οργανισμών ποίκιλε, από λιγότερο από 50 σε περισσότερο από 10.000 άτομα προσωπικό. Αυτή η έκθεση, δίνει μια ένδειξη στο τι κάνουν οι οργανισμοί της Ευρώπης για να μετρήσουν και να βελτιώσουν την ενημέρωση ασφάλειας πληροφοριών.

συνεπάγεται ανάλυση του ακροατηρίου και εντοπισμός των πλέον κατάλληλων τεχνικών που μπορούν να χρησιμοποιηθούν.

Υπάρχει ένα ευρύ φάσμα διαθέσιμων τεχνικών βελτίωσης της ενημέρωσης. Στην έρευνα της ENISA διαπιστώθηκε ότι οι περισσότεροι συμμετέχοντες χρησιμοποιούν πολλαπλές τεχνικές. Οι επιχειρήσεις που δίνουν χαμηλή προτεραιότητα στην ασφάλεια πληροφοριών λαμβάνουν τα λιγότερα μέτρα ενημέρωσης του προσωπικού.

Υπάρχουν ορισμένες βασικές αρχές τις οποίες κάθε οργάνωση πρέπει να υιοθετήσει. Σχεδόν κάθε συμμετέχων στην έρευνα, έχει καθορίσει τις πολιτικές ασφάλειάς τους, είτε στο εγχειρίδιο προσωπικού τους είτε σε μια χωριστή πολιτική ασφάλειας. Το 85% των συμμετεχόντων έχουν δημιουργήσει ένα ιστότοπο ενδοδικτύου (Intranet site) στον οποίο παρέχονται οδηγίες στο προσωπικό επάνω στα θέματα ασφάλειας πληροφοριών. Αυτές οι τεχνικές έχουν το χαμηλότερο κόστος και έτσι δεν υπάρχει κανένας λόγος να μην χρησιμοποιούνται.

Εντούτοις, πολλοί συμμετέχοντες θεωρούν ότι οι πολιτικές, τα εγχειρίδια και οι οδηγίες από μόνες τους δεν αποτελούν ένα αποτελεσματικό τρόπο βελτίωσης της ενημέρωσης. Δεν είναι ρεαλιστικό να αναμένεται ότι το προσωπικό θα διαβάζει και θα απορροφά όλες τις πληροφορίες με τις οποίες βομβαρδίζεται. Αυτές οι τεχνικές παίζουν έναν χρήσιμο ρόλο στην υποστήριξη και ενίσχυση άλλων δραστηριοτήτων ενημέρωσης. Αλλά από μόνες τους δεν είναι αποτελεσματικοί τρόποι για να αλλαχτεί η συμπεριφορά προσωπικού. Οι συμμετέχοντες βρίσκουν την εκπαίδευση σε αίθουσα να είναι η αποτελεσματικότερη τεχνική για να αλλάξει ο τρόπος συμπεριφοράς των ανθρώπων. Το 72% περιλαμβάνουν τα μηνύματα ασφάλειας στην εισαγωγική κατάρτιση του νέου προσωπικού. Αυτός ο τρόπος απευθύνεται στους ανθρώπους υψηλού κινδύνου (νέοι υπάλληλοι) και έχει σχετικά χαμηλότερο κόστος, δεδομένου του ότι οι πτυχές ασφάλειας μπορούν να ενσωματωθούν σε υπάρχουσες διαδικασίες εκπαίδευσης.

Ενώ η κατάρτιση σε αίθουσα θεωρείται ιδιαίτερα αποτελεσματική, σχετικά λίγοι συμμετέχοντες παρέχουν διαρκή κατάρτιση ενημέρωσης για το υπάρχον προσωπικό. Αυτό θα μπορούσε να οφείλεται στο σχετικό κόστος αυτών των προγραμμάτων. Ο χρόνος είναι πολύτιμο προϊόν για τους πολυάσχολους ανθρώπους ενός οργανισμού. Είναι πολύ δύσκολο να βρεθεί χρόνος ώστε να καλυφθούν οι ανάγκες της εκπαίδευσης. Τα αποτελεσματικότερα προγράμματα ενημέρωσης φαίνεται να είναι εκείνα που στοχεύουν ώστε τα περιορισμένου προϋπολογισμού προγράμματα κατάρτισης σε αίθουσα, να απευθύνονται στις ομάδες υψηλότερου κινδύνου. Η

γενική κατάρτιση σε αίθουσες εμφανίζεται να μην είναι οικονομικώς αποδοτική.

Αντ'αυτού, οι μισοί από τους συμμετέχοντες στην έρευνα χρησιμοποιούν εκπαίδευση μέσω υπολογιστή (CBT), και τα δύο τρίτα την επιβάλλουν σε όλο το προσωπικό. Ενώ υπάρχει ένα κόστος επένδυσης για τη δημιουργία ενός προγράμματος CBT, μόλις αυτό τρέξει, προσφέρει διαρκή κατάρτιση σε έναν μεγάλο πληθυσμό υπαρχόντων χρηστών με πολύ χαμηλές δαπάνες παράδοσης.

Η συνέπεια στην παράδοσης μέσω CBT είναι συνήθως καλύτερη απ'ό,τι τα μεγάλα επιμορφωτικά προγράμματα σε αίθουσα. Η δημιουργία των τεστ μέσω του CBT επιτρέπει επίσης και τη μέτρηση για το πόσο καλά έχουν απορροφήσει την κατάρτιση οι παραλήπτες.

Μέρος της υλοποίησης ενός αποτελεσματικού προγράμματος είναι να στοχεύουν τα σωστά μηνύματα τους σωστούς ανθρώπους. Αυτό απαιτεί την κατανόηση για τα τρέχοντα ζητήματα ασφάλειας πληροφοριών που αφορούν την κάθε ομάδα εργαζομένων αλλά και του βαθμού στον οποίο τα γνωρίζουν.

Στην έρευνα διαπιστώθηκε, ότι μόνο το 36% των συμμετεχόντων έχουν κάποιο επίσημο μηχανισμό για αυτό. Αυτό συμβαίνει συχνότερα στις οικονομικές υπηρεσίες. Πολλοί οικονομικοί φορείς παροχής υπηρεσιών έχουν διαπιστώσει ότι είναι δυνατό να ξοδευτούν μεγάλα ποσά χρημάτων σε άνευ διακρίσεως δραστηριότητες ενημέρωσης χωρίς να έχει ασκηθεί μεγάλη επίδραση στο γενικό προφίλ της διαχείρισης κινδύνου. Χρησιμοποιούν τώρα έναν συνδυασμό μιας γενικής κάλυψης των βασικών αρχών και μιας στοχευόμενης πρόσθετης δραστηριότητας στους τομείς μέγιστου κινδύνου.

Οι εκστρατείες αφισών, τα διαφημιστικά υλικά (όπως τα στυλό) και το γενικό ηλεκτρονικό ταχυδρομείο χρησιμοποιούνται από έναν σημαντικό αριθμό συμμετεχόντων. Πολλοί δήλωσαν ότι είχαν χρησιμοποιήσει αυτές τις τεχνικές στο παρελθόν αλλά τώρα τις έχουν εγκαταλείψει ή δεν τις χρησιμοποιούν πολύ. Έχουν σχετικά σύντομη διάρκεια επίδρασης και μπορεί να έχουν μεγάλο κόστος στη διανομή τους.

Υπάρχει επίσης ένα όριο στο πόσες πληροφορίες μπορούν να μεταβιβάσουν στον αναγνώστη, καθώς πολλοί άνθρωποι απλώς τα αγνοούν εντελώς.

Ο ένας στους πέντε συμμετέχοντες χρησιμοποιεί έρευνες και κουίζ για να προκαλέσει το ενδιαφέρον και να βελτιώσει την ενημέρωση. Από εκείνους που τα έχουν δοκιμάσει στο παρελθόν, οι περισσότεροι τα βρήκαν αποτελεσματικά. Η κατάλληλη χρήση διάφορων κινήτρων μπορεί να επιτύχει την υψηλή αποδοχή και

μπορεί να κάνει πραγματικά τους ανθρώπους να σκέπτονται για τις συμπεριφορές τους.

Η υλοποίηση ενός πετυχημένου προγράμματος ενημέρωσης ασφάλειας μπορεί να είναι ένας δύσκολος στόχος. Μπορούν να υπάρξουν μερικά μεγάλα ή φαινομενικά αξεπέραστα εμπόδια. Αυτό που είναι περισσότερο αποτελεσματικό μακροπρόθεσμα είναι η ικανότητα να εντοπισθούν οι οποιοιδήποτε ιδιαίτεροι περιορισμοί, όπως η έλλειψη ενδιαφέροντος από την ανώτερη διοίκηση ή μια κουλτούρα αντίστασης μέσα στον οργανισμό. Η αναγνώριση των πιθανών εμποδίων εκ των προτέρων θα επιτρέψει την εφαρμογή σχεδίων ώστε να υπερνικηθούν αυτά τα εμπόδια.

8.2.3. Μέτρηση της αποτελεσματικότητας των προγραμμάτων ενημέρωσης

Η ενημέρωση ασφάλειας πληροφοριών αφορά τις συμπεριφορές των ανθρώπων. Αυτές είναι πάντα δύσκολο να μετρηθούν, έτσι αυτό αποτελεί μια πρόκληση για τους περισσότερους οργανισμούς.

Οι διάφοροι οργανισμοί υιοθετούν διαφορετικές μεθόδους αξιολόγησης της αποτελεσματικότητας των δραστηριοτήτων ενημέρωσης ασφάλειας πληροφοριών. Αυτές περιλαμβάνουν και ποσοτικές και ποιοτικές προσεγγίσεις. Γενικά, υπάρχουν τέσσερις κύριες προσεγγίσεις, κάθε μια με διαφορετικούς δείκτες απόδοσης (ENISA, 2007):

1. Βελτίωση διαδικασίας (Process improvement)

Αυτή η προσέγγιση αξιολογεί την αποτελεσματικότητα του προγράμματος εξετάζοντας τις δραστηριότητές του. Με άλλα λόγια, αυτοί οι δείκτες είναι σχετικοί με την προσπάθεια που γίνεται στο πρόγραμμα. Δεν μετρούν άμεσα εάν το τελικό αποτέλεσμα έχει βελτιώσει την ασφάλεια.

Πιθανοί δείκτες απόδοσης περιλαμβάνουν:

- Τον βαθμό στον οποίο αναπτύσσονται οι οδηγίες ασφάλειας. Παραδείγματος χάριν, οι άνθρωποι μπορούν να αξιολογήσουν το πόσο καλά αντιμετωπίζουν οι οδηγίες ασφάλειας τους σημαντικότερους κινδύνους ή τις τεχνολογικές πλατφόρμες;

- Το βαθμό διάδοσης της καθοδήγησης. Τυπικοί δείκτες είναι ο αριθμός των φυλλαδίων που διανέμονται, ο αριθμός των επισκεπτών στον ιστότοπο του ενδοδικτύου, ή ο αριθμός του προσωπικού που λαμβάνει την κατάρτιση ενημέρωσης.
- Η αποδοτικότητα της διαδικασίας ενημέρωσης. Μέτρο είναι το κόστος παράδοσης, π.χ. κόστος (σε χρόνο και χρήμα) ανά άτομο που εκπαιδεύεται.
- Η σχετικότητα του υλικού ενημέρωσης. Ένα απλό μέτρο είναι εδώ η συχνότητα με την οποία γίνεται ενημέρωση του υλικού.
- Η αποτελεσματικότητα της εφαρμογής των οδηγιών ασφάλειας. Ένας τρόπος μέτρησης είναι οι έρευνες που ρωτούν το προσωπικό εάν γνωρίζει τις οδηγίες ασφάλειας και εάν ξέρουν ποιες διαδικασίες πρέπει να ακολουθούν.

Το πλεονέκτημα των δεικτών βελτίωσης διαδικασίας είναι ότι είναι εύκολο να καθοριστούν και να γίνει η συλλογή τους.

Το μειονέκτημα είναι ότι παρέχουν μόνο έμμεση αναφορά για το εάν το πρόγραμμα καθιστά τον οργανισμό περισσότερο ασφαλή.

2. Αντίσταση σε επίθεση (Attack resistance)

Αυτή η προσέγγιση εστιάζει στη μέτρηση στο πόσο ανθεκτικό είναι το προσωπικό σε μια πιθανή επίθεση. Οι πιθανοί δείκτες επίδοσης περιλαμβάνουν:

- Τον βαθμό στον οποίο το προσωπικό αναγνωρίζει τις επιθέσεις. Αυτό κανονικά περιλαμβάνει τη διενέργεια συγκεκριμένων ερωτήσεων σε δημοσκοπήσεις του προσωπικού, με κουίζ ή τεστ βασισμένα σε υπολογιστή.
- Το βαθμό στον οποίο το προσωπικό πέφτει θύμα των επιθέσεων. Εδώ είναι χρήσιμη η μίμηση επιθέσεων, όπως η αποστολή ηλεκτρονικού ταχυδρομείου που περιέχει εκτελέσιμο κώδικα (executables), ή τηλεφωνήματα στο προσωπικό και προσπάθεια απόσπασης πληροφοριών σχετικών με τους κωδικούς πρόσβασής τους (κοινωνική μηχανική).

Το πλεονέκτημα των δεικτών αντίστασης σε επίθεση, είναι ότι παρέχουν κάποια άμεσα στοιχεία της πραγματικής κατάστασης της ενημερότητας του προσωπικού. Τείνουν να είναι καλοί για τον εντυπωσιασμό της ανώτερης διοίκησης στην ανάγκη για δημιουργία επενδύσεων στην ενημέρωση ασφάλειας.

Το κύριο μειονέκτημα είναι ότι υπάρχουν ενδεχομένως πολλά σενάρια επίθεσης. Οποιοδήποτε μεμονωμένος δείκτης είναι συγκεκριμένος για το σενάριο που εξετάζει. Επίσης η δημιουργία της προσομοίωσης των επιθέσεων μπορεί να είναι σχετικά

ακριβή διαδικασία. Μια βασισμένη στο κίνδυνο (risk-based) προσέγγιση μπορεί να βοηθήσει στο να υπερνικηθούν αυτά τα ζητήματα.

3. Αποδοτικότητα και αποτελεσματικότητα (Efficiency and effectiveness)

Αυτή η προσέγγιση εστιάζει στην πραγματική εμπειρία από τα συμβάντα ασφάλειας μέσα στον οργανισμό. Πιθανοί δείκτες απόδοσης περιλαμβάνουν:

- Η έκταση των συμβάντων ασφάλειας που προκύπτουν εξαιτίας ανθρώπινης συμπεριφοράς. Οι χαρακτηριστικοί δείκτες περιλαμβάνουν τον αριθμό και το κόστος αυτών των συμβάντων. Μερικοί οργανισμοί εξετάζουν επίσης το ποσοστό των συμβάντων ασφάλειας που προκύπτουν εξαιτίας της ανθρώπινης συμπεριφοράς.
- Η διάρκεια του χρόνου διακοπής (downtime) που προκλήθηκε εξαιτίας ανθρώπινης συμπεριφοράς. Αυτό ενδιαφέρει άμεσα σε τομείς όπου η διαθεσιμότητα των συστημάτων είναι κρίσιμη.
- Ο βαθμός στον οποίο η ανθρώπινη συμπεριφορά προκάλεσε τα σοβαρότερα συμβάντα ασφάλειας. Η ανάλυση της βασικής αιτίας που προκάλεσε αυτά τα συμβάντα, παρέχει αυτά τα δεδομένα. Η μέτρηση έπειτα εκφράζεται κανονικά ως ποσοστό του συνολικού αριθμού των σοβαρών γεγονότων.

Το πλεονέκτημα αυτών των δεικτών είναι διπλό: πρώτον, τα δεδομένα μπορούν να συλλεχθούν μέσω της γενικής παρακολούθησης (monitoring) των συμβάντων ασφαλείας την οποία εκτελούν οι περισσότερες ομάδες ασφάλειας πληροφοριών και δεύτερον, αυτές οι στατιστικές συνήθως παρουσιάζουν μεγάλο ενδιαφέρον για την ανώτερη διοίκηση.

Το μειονέκτημα είναι ότι δεν δίνουν απαραιτήτως την αληθινή διάσταση της ενημέρωσης ασφάλειας. Δεν είναι μόνο η ενημέρωση ασφάλειας που καθορίζει πότε εμφανίζονται τα συμβάντα. Ο βαθμός με τον οποίο εμφανίζονται οι επιθέσεις είναι ο κύριος παράγοντας. Μακροπρόθεσμα, η τάση μπορεί να είναι ένας καλός δείκτης της ενημέρωσης. Στην πράξη, εντούτοις, οι άνθρωποι λαμβάνουν συχνά μέτρα βασισμένα σε μεμονωμένα συμβάντα και αυτό μπορεί να μην είναι η αποτελεσματικότερη προσέγγιση.

Εσωτερική προστασία (Internal Protections)

Αυτή η κατηγορία ενδιαφέρεται για το πόσο καλά ένα άτομο προστατεύεται από πιθανές απειλές. Με άλλα λόγια, το άτομο έχει τη κατάλληλη ενημέρωση που οδηγεί

σε ασφαλή συμπεριφορά;

Οι πιθανοί δείκτες απόδοσης περιλαμβάνουν:

- Το βαθμό στον οποίο τα άτομα ενσωματώνουν την ασφάλεια στην ανάπτυξη και την απόκτηση των συστημάτων. Αυτό μπορεί να μετρηθεί με την αναθεώρηση ενός δείγματος των επιχειρησιακών περιπτώσεων και των προδιαγραφών απαιτήσεων.
- Ο βαθμός στον οποίο τα άτομα προστατεύουν τα αρχεία δεδομένων τους. Τα εργαλεία ανίχνευσης (scanning tools) μπορούν να χρησιμοποιηθούν για να δημιουργήσουν μια εικόνα της κατάστασης.
- Ο βαθμός στον οποίο τα άτομα έχουν επιτρέψει στα συστήματά τους να μολυνθούν από ιούς ή άλλο κακόβουλο λογισμικό. Τα σχετικά στατιστικά στοιχεία μπορούν ληφθούν από antivirus δραστηριότητες.
- Ο βαθμός στον οποίο τα άτομα έχουν επιτρέψει στα συστήματά τους να μολυνθούν από ακατάλληλο υλικό (π.χ. πορνογραφικό) ή αναρμόδιο (π.χ. πειρατικό) λογισμικό. Υπάρχουν συγκεκριμένα εργαλεία ανίχνευσης που μπορούν να το μετρήσουν αυτό γρήγορα.

Το πλεονέκτημα αυτών των μέτρων είναι ότι παρέχουν άμεσα στοιχεία σχετικά με τη συμπεριφορά του προσωπικού. Αξιολογούν εάν η ενημέρωση καθιστά τον οργανισμό ασφαλέστερο και αποφεύγουν τις υποθέσεις ή τα συμπεράσματα. Επιπλέον, οι συνήθεις έλεγχοι (από τους εσωτερικούς ή εξωτερικούς ελεγκτές) μπορούν να παρέχουν τη σχετική ανατροφοδότηση, αποτελεσματικά και δωρεάν.

Το μειονέκτημα είναι ότι οποιοσδήποτε μεμονωμένος δείκτης είναι συγκεκριμένος για τη συμπεριφορά που μετρά. Συχνά, ένα πρόγραμμα ενημέρωσης στοχεύει να αλλάξει πολλές συμπεριφορές. Αυτό μπορεί να έχει επίδραση σε πολλούς δείκτες. Κάθε ένας από αυτούς, στη συνέχεια, μπορεί να απαιτήσει επένδυση σε εργαλεία ή σε ελέγχους ανίχνευσης. Μια βασισμένη στον κίνδυνο (risk-based), ή περιστροφική προσέγγιση μπορεί να βοηθήσει στη μείωση της δαπάνης.

Οι περισσότεροι οργανισμοί χρησιμοποιούν έναν συνδυασμό και από τις τέσσερις προσεγγίσεις. Ο συνδυασμός διαφορετικών δεικτών μπορεί να βοηθήσει στη δημιουργία ισορροπημένης κάρτας (balanced scorecard[39]). Οι αποφάσεις βασίζονται στη γενική εικόνα, παρά σε οποιονδήποτε συγκεκριμένο δείκτη.

---

[39]Μεθοδολογία ολοκληρωμένης στοχοθεσίας και μέτρησης των επιδόσεων ενός οργανισμού. Αυτή συνίσταται σε ένα ευρύ εννοιολογικό πλαίσιο και σε ένα αριθμό αντίστοιχων δεικτών που καλύπτουν τους κρίσιμους παράγοντες της αποτελεσματικότητας. (Μπουραντάς, 2002:533)

Οι συμμετέχοντες στην έρευνα της ENISA χρησιμοποιούν μια ευρεία ποικιλία διαφορετικών μεθόδων για να μετρήσουν την αποτελεσματικότητα των πρωτοβουλιών ενημέρωσης ασφάλειας πληροφοριών τους.

Τα μέτρα της εσωτερικής προστασίας είναι γενικώς τα δημοφιλέστερα. Τα δύο τρίτα των συμμετεχόντων χρησιμοποιούν τις πολιτικές των παραβιάσεων που επισημαίνονται στις αναφορές των εσωτερικών ή εξωτερικών ελέγχων σαν δείκτες. Οι έλεγχοι μπορούν να αναληφθούν από μέλη εσωτερικών ομάδων ή μπορούν να είναι ως αποτέλεσμα εξωτερικών ελέγχων από τρίτους. Η αντικειμενική και συστηματική προσέγγιση των ελεγκτών κάνει αυτές τις εκθέσεις αξιόπιστες πηγές πληροφοριών. Επιπλέον, σχεδόν ένα τρίτο των συμμετεχόντων χρησιμοποιεί τα αποτελέσματα των ελέγχων σαν δείκτη για την αξιολόγηση του προγράμματος ενημέρωσης τους.

Όμως μερικοί πιθανοί δείκτες (όπως το ποσοστό των συστημάτων που κατασκευάζονται εξαρχής με προδιαγραφές ασφάλειας) χρησιμοποιούνται ελάχιστα. Τα μέτρα αποδοτικότητας και αποτελεσματικότητας είναι τα επόμενα δημοφιλέστερα. Πολλοί συμμετέχοντες χρησιμοποιούν την εμπειρία τους από συμβάντα ασφάλειας. Οι πιο κοινοί δείκτες είναι ο αριθμός των συμβάντων που προκαλούνται εξαιτίας της ανθρώπινης συμπεριφοράς και από την ανάλυση των βασικών αιτιών που προκαλούν αυτά τα συμβάντα. Περισσότερο από τους μισούς συμμετέχοντες χρησιμοποιούν κάποιον από αυτούς. Το ένα τρίτο εξετάζει επίσης το ποσοστό των συμβάντων που προκαλούνται εξαιτίας της ανθρώπινης συμπεριφοράς. Λίγοι συμμετέχοντες παρακολουθούν το κόστος των συμβάντων, αλλά πολλοί από αυτούς τα θεωρούν σαν έναν από τους βασικότερους δείκτες τους.

Μια σημαντική μερίδα συμμετεχόντων χρησιμοποιεί κάποια μορφή δεικτών αντίστασης επίθεσης. Ένα τρίτο περιλαμβάνει ερωτήσεις σχετικά με την ενημέρωση ασφάλειας στις έρευνες προσωπικού. Στη συνέχεια μετρούν τα επίπεδα ενημέρωσης πριν και μετά από τις πρωτοβουλίες που πραγματοποιούνται.

Εντούτοις, μερικοί συμμετέχοντες δίνουν έμφαση σε ζητήματα σχετικά με την πολυπλοκότητα της συλλογής και της επεξεργασίας αυτών των δεδομένων. Ένα τέταρτο όλων των συμμετεχόντων πραγματοποιεί δοκιμές για να ελέγξει εάν το προσωπικό συμπεριφέρεται με το σωστό τρόπο, όταν παρουσιάζεται μια πιθανή απειλή.

Παρά την ευκολία με την οποία μπορούν να συλλεχθούν οι δείκτες βελτίωσης διαδικασίας, ο αριθμός των συμμετεχόντων που τους χρησιμοποιούν είναι χαμηλός.

Ιδανικά, οι συμμετέχοντες θα επιθυμούσαν να είναι σε θέση να μετρήσουν τις πραγματικές αλλαγές στις συμπεριφορές προσωπικού ως αποτέλεσμα των δραστηριοτήτων ενημέρωσης. Κατά συνέπεια, σχετικά λίγοι συμμετέχοντες βρίσκουν χρήσιμους τους δείκτες (π.χ. τον αριθμό επισκεπτών στον ιστότοπο του ενδοδικτύου ή τον αριθμό των διανεμημένων φυλλαδίων). Οι περισσότερο χρησιμοποιούμενοι δείκτες αυτού του τύπου είναι, ο αριθμός προσωπικού που λαμβάνει την κατάρτιση και η ανατροφοδότηση από το προσωπικό ως προς την ποιότητα του προγράμματος. Κατά προσέγγιση το ένα τρίτο των συμμετεχόντων χρησιμοποίησε έναν από αυτούς τους δείκτες.

Υπάρχει μικρή συναίνεση μεταξύ των συμμετεχόντων για τα αποτελεσματικότερα μέτρα. Αυτό είναι σαφώς μια περιοχή εξέλιξης για ορθή πρακτική.

Ακόμη και οι δημοφιλέστεροι δείκτες κρίνονται ανεπαρκείς από μερικούς οργανισμούς. Παραδείγματος χάριν, πολλοί συμμετέχοντες έχουν εγκαταλείψει τις σχετικές με τα συμβάντα ασφάλειας στατιστικές σαν δείκτη ενημέρωσης ασφάλειας. Ένας λόγος είναι ότι υπάρχουν πολλοί άλλοι παράγοντες που συντελούν για τη δημιουργία του αριθμού των συμβάντων ασφάλειας. Ένας άλλος είναι ότι ο αριθμός των συμβάντων είναι πολύ μικρός και ως εκ τούτου είναι δύσκολη στατιστικά η ανάλυση τάσης.

Συνολικά, υπήρξε μια καλή συσχέτιση μεταξύ των δεικτών που τονίστηκαν ως αποτελεσματικότεροι και των δεικτών που βρέθηκαν να είναι δημοφιλείς και χρησιμοποιούνται σε πραγματική βάση από όλους τους συμμετέχοντες. Γενικά η αποκτηθείσα εμπειρία όλων των προηγούμενων ετών ως προς το τι είναι τελικά λειτουργικό, βρίσκει εφαρμογή στο σήμερα, αλλά οι οργανισμοί συνεχίζουν να βελτιώνουν την προσέγγισή τους, καθώς υπάρχουν πολλά που μαθαίνονται διαρκώς.

Γενικά τα αποτελέσματα δεν παρουσίασαν σημαντικές διαφορές σε σχέση με το τομέα δραστηριοποίησης των συμμετεχόντων. Αυτό δείχνει ότι η αποτελεσματικότητα είναι γενικά παντού η ίδια. Αν και ένα ιδιαίτερο στοιχείο ήταν ότι οι οργανισμοί οικονομικών υπηρεσιών είναι λιγότερο πιθανό να χρησιμοποιήσουν τους δείκτες που αφορούν το κόστος των συμβάντων ασφάλειας, σε σχέση με τους κυβερνητικούς, τους εμπορικούς, τους τηλεπικοινωνιακούς και άλλους οργανισμούς. Πολλοί συμμετέχοντες έχουν αντιμετωπίσει τα προβλήματα του παρελθόντος, δρομολογώντας αποτελεσματικά μέτρα. Είναι σημαντικό ότι οποιαδήποτε μέθοδο χρησιμοποιεί ένας οργανισμός, για να παράγει και να μετρήσει τους δείκτες ενημέρωσης, αντιμετωπίζει τα ίδια κοινά ζητήματα. Οι κύριες ανησυχίες που

προκαλούνται στους συμμετέχοντες στη μελέτη της ENISA περιλαμβάνει:

- *Ζητήματα ποιότητας και συγκρισιμότητας (Quality and comparability issues).* Ένα ιδιαίτερο ζήτημα είναι σχετικό με τις δημοσκοπήσεις (surveys) προσωπικού, καθώς ο τρόπος διατύπωσης των ερωτήσεων, και του εξαναγκασμού συμμετοχής στην έρευνα μπορεί να έχει επιπτώσεις στις απαντήσεις που δίνονται. Συχνά το προσωπικό λέει στις δημοσκοπήσεις οτιδήποτε νομίζει ότι θέλει να ακούσει η διοίκηση, και όχι απαραιτήτως ότι σκέφτεται πραγματικά. Οι επιστροφές συμμόρφωσης από την ανώτερη διοίκηση (π.χ. αυτοαξιολογήσεις), μπορεί να είναι επίσης παραπλανητικές, καθώς οι άνθρωποι που υπογράφουν τις επιστροφές συχνά δεν γνωρίζουν τις λεπτομέρειες των διαδικασιών τους και έτσι αναφέρουν ότι λέγεται από τις ομάδες τους.
- *Σχετικότητα (Relevance).* Είναι σημαντικό να μην ληφθεί λανθασμένο συμπέρασμα από τους δείκτες. Παραδείγματος χάριν, μια αύξηση στα ποσοστά μόλυνσης από ιούς μπορεί να δείξει ένα πρόβλημα με τη ενημέρωση του προσωπικού, αλλά θα μπορούσε εξίσου να είναι ένα ζήτημα που αφορά το λογισμικό των antivirus προγραμμάτων. Μια άνοδος στα συμβάντα ασφάλειας θα μπορούσε να δείξει ένα πρόβλημα με την ενημέρωση (περισσότερες πραγματικές παραβιάσεις), ή βελτίωση στην ενημέρωση (περισσότερες αναφορές των ίδιων παραβιάσεων). Ο αριθμός φυλλαδίων ή του ηλεκτρονικού ταχυδρομείου που στέλνονται δεν σημαίνει απαραιτήτως ότι ο καθένας τα έχει διαβάσει. Η χρησιμοποίηση ενός συνόλου δεικτών επιτρέπει τη δημιουργία μιας ευκρινέστερης εικόνας.
- *Διαθεσιμότητα των συγκεκριμένων δεικτών (Availability of specific indicators).* Μερικοί δείκτες είναι πάρα πολύ δύσκολο να μετρηθούν αποτελεσματικά. Ενώ σε γενικές γραμμές, πολλοί συμμετέχοντες αντιμετωπίζουν την απόδοση της επένδυσης (ROI) σαν μια λογική προσέγγιση, είναι πολύ δύσκολο από τα περισσότερα ευρήματα να ποσοτικοποιηθούν τα οφέλη της καλύτερης ενημέρωσης προσωπικού. Σε ένα μη εμπορικό περιβάλλον (όπου δεν υπάρχουν πωλήσεις) είναι δύσκολο να υπολογισθεί το κόστος των παραβιάσεων ασφάλειας.
- *Επεξεργασία (Processing).* Μόλις συλλεχθούν τα δεδομένα πρέπει να υποβληθούν σε επεξεργασία ώστε να μετατραπούν σε σημαντικές πληροφορίες. Μπορεί να απαιτείται να γίνει διαμόρφωση των πληροφοριών ώστε να αφαιρεθούν ύποπτα αποτελέσματα (παραδείγματος χάριν, εάν υπάρχει ένα πρόβλημα με ένα συγκεκριμένο εκπαιδευτικό πρόγραμμα). Τα δεδομένα μπορεί να πρέπει να

σταθμιστούν για να απεικονίσουν καλύτερα το γενικό προφίλ του προσωπικού του οργανισμού. Ένας γενικός κανόνας λέει ότι όσο λιγότερη επεξεργασία γίνεται, τόσο καλύτερα. Μερικοί συμμετέχοντες, παραδείγματος χάριν, έχουν εγκαταλείψει τη χρησιμοποίηση της σύγκρισης των στοιχείων των ερευνών πριν και μετά λόγω της πολυπλοκότητας της επεξεργασίας που απαιτείται.

Τελικά, φαίνεται ότι υπάρχουν πολλοί λόγοι για τους οποίους μεμονωμένοι δείκτες μπορεί να είναι χρήσιμοι. Μερικοί δείκτες χρησιμοποιούνται επειδή παρέχουν διορατικότητα προς τις πραγματικές συμπεριφορές (π.χ. ανιχνεύσεις ή δοκιμές). Άλλοι υιοθετούνται επειδή έχουν απήχηση στην ανώτερη διοίκηση που υποστηρίζουν τα ενημερωτικά προγράμματα (π.χ. κόστος των συμβάντων). Άλλοι επειδή είναι εύκολοι στο να μετρηθούν (π.χ. αποτελέσματα των ελέγχων).

Κάθε οργανισμός πρέπει να βρει τη σωστή ισορροπία γιατί δεν υπάρχει καμία λύση που να ταιριάζει για όλους. Η προσέγγιση γενικά πρέπει να είναι απλή ώστε να κρατηθεί σε οικονομικά αποδοτικό επίπεδο. Γίνεται μεγάλη προσπάθεια σχετικά με τη ποσοτικοποίηση της ενημέρωσης ασφάλειας, εντούτοις, υπό τον όρο ότι αποφεύγονται τα απλά λάθη, ένα ισορροπημένο σύνολο δεικτών μπορεί να παρέχει μια πραγματική διορατικότητα ως προς την αποτελεσματικότητα των προγραμμάτων ενημέρωσης. Μόνο με αυτήν την διορατικότητα οι οργανισμοί είναι ικανοί να αλλάξουν τα προγράμματά τους, από μια δραστηριότητα συμμόρφωσης σε μια που ωφελεί πραγματικά τις λειτουργίες τους.

Ένα παράδειγμα ενός ισορροπημένου συνόλου βασικών δεικτών απόδοσης παρέχεται στον ακόλουθο πίνακα. (ENISA,2007) Αυτό συνδυάζει τους πέντε δημοφιλέστερους δείκτες που χρησιμοποιούνται από τους συμμετέχοντες σε ένα γενικό πίνακα ενημέρωσης ασφάλειας.

Πίνακας βασικών δεικτών απόδοσης ενημέρωσης

Δείκτες	Σημεία εξέτασης
Αριθμός συμβάντων ασφάλειας λόγω της ανθρώπινης συμπεριφοράς.	Μπορεί να παρουσιάσει τις τάσεις και τις αποκλίσεις στη συμπεριφορά. Μπορεί να βοηθήσει στην κατανόηση των βασικών αιτιών και στον υπολογισμό του κόστους για τον οργανισμό. Μπορεί να μην έχουν γίνει πολλά συμβάντα ώστε να βγουν στατιστικώς σημαντικά αποτελέσματα. Μπορεί να υπάρχουν και άλλοι παράγοντες που να συντελούν στη δημιουργία των συμβάντων.
Ευρήματα ελέγχων.	Γενικά οι έλεγχοι γίνονται από ανεξάρτητους εμπειρογνώμονες που παρέχουν βεβαίωση τρίτου επάνω στις συμπεριφορές. Μπορεί να υπάρξουν σημαντικοί τομείς της ενημέρωσης που δεν επισκοπούνται.
Αποτελέσματα από δημοσκοπήσεις (surveys) προσωπικού.	Εάν χρησιμοποιείται πριν και μετά από τη κάθε κατάρτιση, μπορεί να χρησιμοποιηθεί για να μετρήσει την αποτελεσματικότητα των εκστρατειών ενημέρωσης. Εάν υπάρχουν πολλά δεδομένα, μπορούν να παρέχουν στατιστικά συμπεράσματα επάνω στις συμπεριφορές του προσωπικού. Ανάγκη να στοχεύει στην επαλήθευση των βασικών μηνυμάτων. Πρέπει να σχεδιάζεται προσεκτικά δεδομένου ότι το προσωπικό μπορεί να αποκριθεί με "αναμενόμενες" απαντήσεις και με μη αληθινές συμπεριφορές.
Τεστ για το εάν το προσωπικό ακολουθεί σωστές διαδικασίες.	Πολύ καλός τρόπος για τη μέτρηση των πραγματικών συμπεριφορών και μπορεί να δώσει έμφαση στις αλλαγές μετά από την εκπαίδευση. Πρέπει να σχεδιασθεί και να πραγματοποιηθεί προσεκτικά γιατί θα μπορούσε να παραβιάσει τους νόμους περί προσωπικών και άλλων δεδομένων. Χρειάζεται ένα αρκετά μεγάλο δείγμα για να είναι τα αποτελέσματα στατιστικώς σημαντικά.
Αριθμός του προσωπικού που ολοκλήρωσε την εκπαίδευση.	Ανάγκη να αποφασιστεί ποιος συνδυασμός εκπαίδευσης σε αίθουσα και κατάρτιση βασισμένης σε υπολογιστή θα χρησιμοποιηθεί. Πρέπει να εξετασθεί ποια θα είναι η υποχρεωτική εκπαίδευση. Πρέπει να μπορεί να προσαρμόζεται σε διαφορετικές περιοχές ή περιφέρειες. Μπορεί να απαιτεί τακτικές και ενδεχομένως δαπανηρές αναπροσαρμογές.

Πίνακας 1: Βασικοί δείκτες μέτρησης απόδοσης ενημέρωσης
πηγή: ENISA http://www.enisa.europa.eu

Συμπεράσματα

Συνοψίζοντας, στη σημερινή εποχή της διεθνούς διαδικτύωσης και της ηλεκτρονικής διακυβέρνησης, η ασφάλεια αποτελεί μείζον θέμα για κάθε οργανισμό. Είναι πλέον καθημερινό φαινόμενο τα συμβάντα ασφάλειας τα οποία βάζουν σε κίνδυνο τα Πληροφοριακά Συστήματα, τη λειτουργία και τη φήμη των οργανισμών.

Η υιοθέτησή των αρχών της Διοίκησης Ολικής Ποιότητας μέσω ενός συστήματος Διαχείρισης Ασφαλείας μπορεί να επιλύσει τα ζητήματα ποιότητας ασφάλειας των Πληροφοριακών Συστημάτων, όπως επέλυσε το ζήτημα της ποιότητας στον τομέα των προϊόντων και των υπηρεσιών. Στα πλαίσια της έρευνας για την εργασία εντοπίστηκαν πληθώρα σχετικών συστάσεων από επίσημους και αρμόδιους φορείς και οργανισμούς.

Γενικότερα η Διοίκηση Ολικής Ποιότητας είναι ένα δοκιμασμένο ανθρωποκεντρικό σύστημα διοίκησης για το οποίο έχουν μελετηθεί όλες οι αδυναμίες και οι δυσκολίες εφαρμογής του και κατά συνέπεια έχουν δοθεί και συνεχίζουν να δίνονται λύσεις σε κάθε είδους σχετικά προβλήματα, ενώ παράλληλα έχουν αναπτυχθεί υποστηρικτικές μέθοδοι εργαλεία και τεχνικές. Δεν είναι τυχαίο ότι σε πολλές περιπτώσεις διάφοροι οργανισμοί στην Ευρώπη αναπτύσσουν ταυτόχρονα και συνδυασμένα, το Σύστημα Διοίκησης Ποιότητας (ISO 9001:2000) μαζί με το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISO 27001:2005), ενώ σε άλλους, αφού προηγουμένως έχουν χρησιμοποιήσει μοντέλα-εργαλεία Ολικής Ποιότητας όπως το CAF και το EFQM.

Συμπερασματικά στην εργασία αυτή υποστηρίζεται ότι η ανάπτυξη ενός Συστήματος Διαχείρισης Ασφάλειας, με την παράλληλη διαμόρφωση μιας αναγκαίας κουλτούρας ασφάλειας, κάτω από ένα συνεχές πρόγραμμα ενημέρωσης, σε ένα περιβάλλον Διοίκησης Ολικής Ποιότητας, παρέχει τα εχέγγυα για μια αποτελεσματική ασφάλεια Πληροφοριακών Συστημάτων.

Βιβλιογραφία

[1] Symantec (2007). Internet Security Threat Report.Volume XII Sept 17, 2007 http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=threatreport

[2] Δ. Μπουραντάς, (2002), Μάνατζμεντ, Εκδόσεις Γ.Μπένου, Αθήνα 2002

[3] Γ.Βασιλακόπουλος Β.Χρυσικόπουλος (1990), Πληροφοριακά συστήματα Διοίκησης Ανάλυση Σχεδιασμός, Εκδόσεις Σταμούλης Πειραιάς.

[4] S. Harrison, R. Stupak (1993), "Total Quality Management: The organizational equivalent of truth in public administration theory and practice", Public Administration Quarterly. Winter 1993.

[5] J. Juran and F. Gryna (1998), Juran's Quality Control Handbook, McGraw Hill.

[6] P.B. Crosby (1979), Quality is free. The art of making quality certain, NY, New American Library

[7] G. Benson, J. Saraph and R. Schroeder (1991). The effects of Organizational Context on Quality Management: An empirical investication. Management Science, Vol 37, No 9.

[8] Laudon and J.P.Laudon (2006). Πληροφοριακά Συστήματα Διοίκησης, Διοίκηση της ψηφιακής επιχείρησης. Εκδόσεις Κλειδάριθμος.

[9] Ε. Κιουντούζης (2004).Προσεγγίσεις Ασφαλείας Πληροφοριακών Συστημάτων. στο Σ. Κάτσικας, Δ.Γκρίτζαλης, Σ. Γκρίτζαλης. Ασφάλεια Πληροφοριακών Συστημάτων. Αθήνα, Εκδόσεις Νέων Τεχνολογιών

[10] J. Evans. W. Lindsay (1999), "The management and control of quality", South Western College Publishing, Cincinnati, Ohio.

[11] Β. Κέφης (2005), Διοίκηση Ολικής Ποιότητας: Θεωρία και Πρότυπα, Εκδόσεις Κριτική Αθήνα.

[12] P. Kim, W. Pindur, K. Reynolds (1995), "Creating a new organizational culture: The key to total management in the public sector", International Journal of Public Administration, 18(4).

[13] Tom Redman, Brian Mathews, Adrian Wilkinson, Ed Snape (1995). "Quality management in services: is the public sector keeping pace?". International Journal of Public Sector Management Vol. 8, No. 7.

[14] Gaster, L. and Squires (2003), A. Providing Quality in the Public Sector, A practical approach to improving public services, Maidenhead and Philadelphia, Open University Press.

[15] Sensenbrenner (1995), "The fourth revolution in government change", Journal for quality and participation, Vol. 18, issue 7. 1995

[16] Γ. Πάγκαλος, Ι. Μαυρίδης (2002). Ασφάλεια Πληροφοριακών Συστημάτων και δικτύων. Εκδόσεις Ανικούλα Θεσσαλονίκη 2002.

[17] Κοκολάκης Σ. (2004). Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας ΠΣ. στο Σ. Κάτσικας, Δ.Γκρίτζαλης, Σ. Γκρίτζαλης (2004). Ασφάλεια Πληροφοριακών Συστημάτων. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

[18] Stuart E. Madnick and Michael Siegel (2006) ,Enterprise Security Perception and the "House of Security", Sloan School of Management Massachusetts Institute of Technology Cambridge, 2006.

[19] Wood C.C., Bank W.W., Guarro S.B., Garcia A.A., Hample V.E. and Santorio H.P. (1978), *Computer Security: A Comprehensive Controls Checklist,* John Wiley and Sons.

[20] Ward G.M. and Harris J.D., Managing Computer Risk: A Guide for the Policymaker, 1986, New York, John Wiley and Sons.
[21] Mumford, E., Defining Systems Requirements to meet Business Needs: a Case study example, *The Computer Journal,* Vol.28, No.2, pp. 97-104, 1985.
[22] M. Devargas, (1995), The Total quality management approach to IT security, Blackwell Oxford 1995.
[23] Δ.Γκρίτζαλης (2004). Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση. στο Σ. Κάτσικας, Δ.Γκρίτζαλης, Σ. Γκρίτζαλης (2004). Ασφάλεια Πληροφοριακών Συστημάτων. Αθήνα: Εκδόσεις Νέων Τεχνολογιών
[24] Καρύδα Μ. (2004). Πολιτικές Ασφάλειας ΠΣ. στο Σ. Κάτσικας, Δ.Γκρίτζαλης, Σ. Γκρίτζαλης (2004). Ασφάλεια Πληροφοριακών Συστημάτων. Αθήνα: Εκδόσεις Νέων Τεχνολογιών
[25] Kiountouzis E.A. and Kokolakis S.A. " An analyst's view of information systems security", in Information systems security: Facing the information society of the 21 century, Katsikas S.K and Gritzalis D. (eds), Chapman & Hall, London, 1996
[26] J. Bank (2000), Μάνατζμεντ Ολικής Ποιότητας, Β. Γκιούρδας Εκδοτική Αθήνα.
[27] CISCO, (2007), Measuring and Evaluating an Effective Security Culture, CISCO Systems White Paper, USA.
(http://www.cisco.com/web/about/security/cspo/docs/measuring_effective.pdf)
[28] Stuart Madnick and Michael Siegel (2006), Towards total Security Quality Management (TSQM), Cisco Systems, Projects August 01 2006 (http://digital.mit.edu/research/projects.html).
[29] Wee Horng Ang, Yang W. Lee, Stuart E. Madnick ,Dinsha Mistree, Michael Siegel, Diane M. Strong, Richard Y. Wang Chrisy Yao (2006), House of Security:Locale, Roles and Resources for Ensuring Information Security, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA 02142
[30] Κοινό Πλαίσιο Αξιολόγησης, Υπουργείο Εσωτερικών, Διεύθυνση Ποιότητας και Αποδοτικότητας, 2007
[31] Christopher Pollitt, Geert Bouckaert, Elke Loffler, «Το ταξίδι της ποιότητας στον ευρωπαϊκό Δημόσιο Τομέα. Από το εκεί στο εδώ και μετά πού», Πρακτικά 3ο Συνεδρίου Ποιότητας για τη Δημόσια Διοίκηση στην Ευρωπαϊκή Ένωση, Ρότερνταμ, Ολλανδία
[32] ISO/IEC/JTC1 13335 Information Technology – Security Techniques – Guidelines for Management of IT Security (GMITS), 1996
[33] Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα (2003), Σχέδιο ασφάλειας και σχέδιο έκτακτης ανάγκης, http://www.dpa.gr
[34] OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002
[35] ENISA (2006) , Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, Technical Department of ENISA Section Risk Management, June 2006
[36] ENISA (2007), European Network and information Security Agency, Current practice and measurement of success, July 2007, (http://www.enisa.europa.eu)
[37] NIST (1998), Document SP800-16 "IT Security Training Requirements:

A Role- and Performance-Based Model"
(http://csrc.nist.gov/publications/PubsSPs.html)

[38] Martin J. (1973), Security, Accuracy and Privacy in Computer Systems, Prentice Hall.

[39] Mc Cumber J. (1991), Information Systems Security: A comprehensive Model, in Proceedings of the Nth National Computer Security Conference, October 1991, National Computer Security.

[40] Κατσίκας Σ. (1995), Διαχείριση Κινδύνων, στο Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αλεξανδρής Ν., Κιουντούζης Ε., και Τραπεζάνογλου Β., (Επιμ.), 1995, Αθήνα, Εκδόσεις Ε.Π.Υ.

[41] Backhouse, J. and Dhillon, G. (1996), Structures of Responsibility and Security of Information Systems, European Journal of Information Systems, Vol.5, p. 2-9.

[42] Strens R. and Dobson J. (1992-93), How Responsibility Modeling Leeds to Security Requirements, in New Security Paradigms Worhhop 1992-1993, IEEE, Computer Society Press.

[43] Kowalski St.(1991), Creating Confidence through Consensus, in *Information* Security, Lindsay D.T. and Price W.L. (Editors), pp. 259-269, Elsevier Science Publications.

[44] Γκρίτζαλης Δ. (1994), Ασφάλεια Πληροφοριακών Συστημάτων σε Περιβάλλοντα Υψηλής Ευπάθειας, Διδακτορική διατριβή, Πανεπιστήμιο Αιγαίου, Τμήμα Μαθηματικών, Σάμος 1994.

[45] Baskerville R. (1993), Information Systems Security Design Methods: Implications for Information Systems Development, *ACM Computing Surveys,* Vol.19, No.2, pp. 185-194.

[46] Warren, M.J. and Batten L.M. (2002), Security Management: An Information System Setting, in the *Proceedings of the ACISP 2002 Conference,* Batten, L. & Seberry, J. (Editors) pp. 257-270, Springer- Verlag.

[47] Hitchings J. (1995), Achieving an Integrated Design: the way forward for Information Security, in Information Security-the Next Decade, Ellof, J. and von Solms, S. (Editors) pp. 369-383, Chapman & Hall.

[48] Karyda, M., Kokolakis, S. and Kiountouzis, E. (2001), Redefining Information System Security: Viable Information Systems, in *Trusted Information: The new decade challenge,* Dupuy, M., Paradinas, P. (Editors), pp. 453-467, 2001, Kluwer Academic Publishers.

[49] Tryfonas, T., Kiountouzis, E. and Polymenakou, A. (2001), Embedding Security Practices in contemporary Information Systems Development Approaches, Information Management & Computer Security, Vol. 9, No.4, pp.183-197.

[50] Κοκολάκης Σπ. (2000), Ανάπτυξη και Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων: Εννοιολογικό Πλαίσιο, Μεθοδολογίες και Εργαλεία, Διδακτορική Διατριβή, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών.

[51] Malone, Thomas W (1997),"Is Empowerment Just a Fad? Control Decision Making and IT" Sloan Management Review.

[52] H.F. Tipton – M.K. Krause, (2007). Information Security Management Handbook, Auerback Publications Taylor & Francis Group Boka Raton New York

[53] K.Knapp T.Marshall (2007), Top Management Support Essential for Effective Information, στο SecurityInformation Security Management Handbook,

Auerback Publications Taylor & Francis Group Boka Raton New York
[54] Κ. Δερβιτσιώτης (2005), Διοίκηση Ολικής Ποιότητας, Έκδοση Οικονομική βιβλιοθήκη, 2005.
[55] J. Evans. W. Lindsay (1999), "The management and control of quality", South — Western College Publishing, Cincinnati, Ohio, σελ. 10-16.
[56] A. Wright, "Public Service Quality: Lessons not learned, Total Quality Management" Vol.8. No5. 1997 σελ. 314
[57] Deming W. E.(1986) , Out of the crisis, Institute of Technology - Center of Advanced Engineering Study, Cambridge, MA, 1986.
[58] Δ. Γκρίτζαλης (1995), Εννοιολογική Θεμελίωση, στο Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αλεξανδρής Ν., Κιουντούζης Ε., και Τραπεζάνογλου Β., (Επιμ.), 1995, Αθήνα, Εκδόσεις Ε.Π.Υ.
[59] S. Snedaker,(2006), Syngress IT Security Project Management Handbook, Syngress Publishing Jun 2006
[60] Susan D. Hansche (2007), Making Security Awareness Happen, στο Information Security Management Handbook, Auerback Publications Taylor & Francis Group Boka Raton New York
[61] Stan Stahl (2007), Beyond Information Security Awareness Training: It Is Time To Change the Culture, στο Information Security Management Handbook, Auerback Publications Taylor & Francis Group Boka Raton New York.
[62] Waldman, Michael (1994).Systematic Errors and the Theory of Natural Selection. American Economic Review 84 (No. 3, June 1994): 482-497
[63] M. Keeney, D. Cappelli E. Kowalski A. Moore T. Shimeall (2005), Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, CERT program, http://www.cert.org/insider_threat/insidercross.html
[64] Garvin D. (1993). Building a learning organization. Harvard Business Rev.,71, 4
[65] Senge, P. (1990). The Fifth Discipline, Doubleday Currency, New York
[66] Jeffrey Davis (2007), Overview of an IT Corporate Security Organization στο Information Security Management Handbook, Auerback Publications Taylor & Francis Group Boka Raton New York
[67] Christopher A. Pilewski, Bonnie A. Goins (2007), Creating a Secure Architecture στο Information Security Management Handbook, Auerback Publications Taylor & Francis Group Boka Raton New York

Βιβλιογραφία

Ψηφιακού Κέντρου Έρευνας (2003), Διαχείριση Ποιότητας, (http://www.vrc.gr:8080/roadmaps/roadmaps/quality/page.html?page_id=2002)

[1] ISO 8402:1994 Quality management and quality assurance, Vocabulary, ISO, 1994.
[2] ISO 9000:2000 Quality Management Systems, Fundamentals and Vocabulary, ISO, 2000.
[3] ISO 9001:2000 Quality Management Systems, Requirements, ISO, 2000.
[4] ISO 9004:2000 Quality Management Systems, Guidelines for Performance Improvements, ISO, 2000.
[5] Marsh, J. (1993), "The Quality Toolkit: An A-Z of Tools and Techniques", IFS Ltd., Bedford UK.
[6] Randall, R.C. (1995), "Randall's Practical Guide to ISO 9000: Implementation, Registration, and Beyond", Addison-Wesley.
[7] Επίσημος δικτυακός τόπος του οργανισμού ISO (International Organisation for Standardisation)