Πανεπιστήμιο Πειραιώς
Τμήμα Πληροφορικής

Διαχείριση Κρίσιμων Πληροφοριακών Υποδομών με τη Χρήση Μεθόδων Ποσοτικοποίησης της Ασφάλειας

Διδακτορική Διατριβή
Εμμανουήλ Δ. Σερρέλη

Πειραιάς 2009

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΙΡΑΙΩΣ

Πανεπιστήμιο Πειραιώς
Τμήμα Πληροφορικής

Διατριβή

Για την απόκτηση Διδακτορικού Διπλώματος
του τμήματος Πληροφορικής

Εμμανουήλ Δ. Σερρέλη

«Διαχείριση Κρίσιμων Πληροφοριακών Υποδομών με την Χρήση Μεθόδων Ποσοτικοποίησης της Ασφάλειας»

Συμβουλευτική Επιτροπή:

Επιβλέπων:

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη:

Βασίλειος Χρυσικόπουλος
Καθηγητής Ιονίου Πανεπιστημίου

Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Εξεταστική Επιτροπή:

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Βασίλειος Χρυσικόπουλος
Καθηγητής Ιονίου Πανεπιστημίου

Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Δημήτριος Γκρίτζαλης
Καθηγητής Οικονομικού Πανεπιστημίου Αθηνών

Δέσποινα Πολέμη
Επίκουρος Καθηγήτρια Πανεπιστημίου Πειραιώς

Εμμανουήλ Μάγκος
Λέκτορας Ιονίου Πανεπιστημίου

Δημήτριος Αποστόλου
Λέκτορας Πανεπιστημίου Πειραιώς

.....
Εμμανουήλ Δ. Σερρέλης
Μηχανικός Η/Υ και Πληροφορικής
Πανεπιστημίου του Λονδίνου
University College London

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διδακτορική διατριβή είναι το αποτέλεσμα ερευνητικής εργασίας που πραγματοποιήθηκε τα τελευταία χρόνια στο Πανεπιστήμιο Πειραιώς. Θα επιθυμούσα να εκφράσω τις ευχαριστίες μου τόσο προς το Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιά για τη δυνατότητα που μου έδωσε να εκπονήσω την παρούσα διατριβή, όσο και όλους όσους συνέβαλαν, με διαφορετικό τρόπο ο καθένας, στην προσπάθεια αυτή.

Θέλω να ευχαριστήσω θερμότατα τον Επιβλέποντα Καθηγητή μου, κ. Νικόλαο Αλεξανδρή, τόσο για την ερευνητική και επιστημονική καθοδήγηση του, όσο για την ειλικρινή αλλά και καθοριστική υποστήριξη του σε όλη τη διάρκεια των ερευνητικών μου δραστηριοτήτων. Είμαι ιδιαίτερα ευγνώμων για την αμέριστη και πολύπλευρη συμπαράστασή του, χωρίς την οποία η έρευνα μου δεν θα ήταν δυνατό να ολοκληρωθεί.

Ευχαριστίες οφείλονται και στον Καθηγητή κ. Χρήστο Δουληγέρη για τις ακαδημαϊκές γνώσεις που μου μετέδωσε αλλά και τις καίριες παρατηρήσεις του στην διατριβή, κατά τη διάρκεια όλων αυτών των ετών, καθώς και στον Καθηγητή κ. Βασίλειο Χρυσικόπουλο για τη συμπαράστασή του και διότι, ως μέλος της τριμελούς μου επιτροπής, συνέβαλε σημαντικά στην ολοκλήρωση αυτής της ερευνητικής μου πορείας.

Επίσης, θα επιθυμούσα να ευχαριστήσω την Επίκουρη Καθηγήτρια κα. Δέσποινα Πολέμη για όλο το ερευνητικό και ενημερωτικό υλικό που μου διέθεσε, για την άψογη συνεργασία σε μια σειρά ερευνητικών προγραμμάτων αλλά και για το συνεχές και ειλικρινές ενδιαφέρον της στην εξέλιξη της ερευνάς μου. Ευχαριστώ πολύ και τον Καθηγητή κ. Mike Burmester για τις ερευνητικές κατευθύνσεις που μου έδωσε στα αρχικά στάδια της ερευνάς μου.

Θα ήθελα ακόμα να ευχαριστήσω θερμά τους κ.κ. Δημήτρη Γκρίτζαλη, Εμμανουήλ Μάγκο και Δημήτριο Αποστόλου για την τιμή που μου έκαναν να είναι μέλη της Εξεταστικής μου Επιτροπής αλλά και τις σημαντικές παρατηρήσεις και προεκτάσεις που έδωσαν στην έρευνά μου.

Ευχαριστώ τους φίλους και συναδέλφους στο Πανεπιστήμιο Πειραιώς και κυρίως τον δρ. Κ. Πατσάκη για όλες τις εποικοδομητικές συζητήσεις που έδωσαν πολλά ερεθίσματα στην έρευνά μου. Ακόμα, ευχαριστώ την Εμπορική Τράπεζα αλλά και τους εκεί συναδέλφους μου για τη δυνατότητα που μου δόθηκε να συνδυάσω την ερευνητική μου δραστηριότητα με την πρακτική εφαρμογή στο αντικείμενο της εργασίας μου αλλά κυρίως για το γεγονός ότι αποτέλεσαν πηγή έμπνευσης – πολλές φορές χωρίς να το συνειδητοποιούν.

Οφείλω ακόμα ένα μεγάλο ευχαριστώ στους γονείς μου για την ηθική και πρακτική υποστήριξή τους, αλλά για τις κατάλληλες συνθήκες που δημιούργησαν έως τώρα για να βρίσκομαι σε αυτή τη ευτυχή θέση, καθώς στους συγγενείς και φίλους που μου συμπαραστάθηκαν. Τέλος, θέλω να

ευχαριστήσω την σύζυγο μου για την υπομονή, την ανοχή και το χαμόγελό της στις μεγάλες απαιτήσεις τόσο της έρευνάς μου, όσο και της τεχνολογικής μου «εμμονής» όλο αυτό το χρονικό διάστημα.

ΠΕΡΙΛΗΨΗ

Η παρούσα διδακτορική διατριβή αφορά στην ανάπτυξη και στην εφαρμογή μεθόδων διαχείρισης κρίσιμων πληροφοριακών υποδομών. Οι μέθοδοι αυτοί αξιολογούνται ως προς το επίπεδο της ασφάλειας που προσφέρουν. Αξιολογώντας τις διάφορες σχετικές προσεγγίσεις μέτρησης και ποσοτικοποίησης της ασφάλειας, το επίπεδο της ασφάλειας αναγνωρίζεται ως ένα μέγεθος που είναι δύσκολο να μετρηθεί αντικειμενικά. Προς αυτήν την κατεύθυνση, ορίζεται ως επιμέρους στόχος η μέτρηση, ποσοτικοποίηση και υπολογισμός της ασφάλειας των πληροφοριακών συστημάτων με αντικειμενικά κριτήρια. Προτείνονται δύο λύσεις μέτρησης, ποσοτικοποίησης και υπολογισμού της ασφάλειας πληροφοριακών συστημάτων βασισμένες σε (διαφορετικά η κάθε μία) αντικειμενικά κριτήρια.

Με βάση τις μεθόδους υπολογισμού της ασφάλειας περιγράφονται οι σχετικοί μέθοδοι αύξησης της ασφάλειας, που είναι και ο κύριος στόχος της διατριβής. Επίσης αναπτύσσονται μεθοδολογίες διαχείρισης και μετασχηματισμού κρίσιμων πληροφοριακών υποδομών με στόχο την βελτιστοποίηση της διαχείρισης των κρίσιμων πληροφοριακών υποδομών και της διαθεσιμότητας των υπηρεσιών και των δεδομένων.

ABSTRACT

This doctoral thesis deals with the development and application of management methods in critical information infrastructures. These methods are evaluated for the level of security they offer. During the evaluation of the various approaches of measurement and quantification of security, it is concluded that security is a notion that is difficult to be measured objectively. To this direction, the measurement, quantification and calculation of security of information systems using objective criteria is set as a secondary objective. Two solutions to measure, quantify and calculate information security, based in unique for each case objective criteria, are proposed.

From the examination and evaluation of the methods of calculation of security several methods to increase security are described. Additionally, two methodologies are also developed, which is the main target of the thesis. These methodologies deal with the management and transformation of critical information infrastructures in order to optimise their function and increase the availability of services and data supported.

ΔΗΜΟΣΙΕΥΣΕΙΣ

Σε αυτές τις δημοσιεύσεις που παρουσιάζονται παρακάτω περιλαμβάνονται εργασίες που έχουν δημοσιευτεί σε διεθνή περιοδικά μετά από πλήρη κρίση, σε διεθνή βιβλία με συλλογές άρθρων, σε διεθνή συνέδρια μετά από πλήρη κρίση. Οι εργασίες αυτές σχετίζονται με την έρευνα που διεξήχθη στο πλαίσιο της παρούσης διατριβής.

Σε διεθνή Περιοδικά μετά από Πλήρη Κρίση

Emmanouil Serrelis**,** Nikolaos Alexandris, **"**How to Achieve and Measure the Benefits of Fault Tolerant Production Infrastructures", Journal On Advances in Networks and Services, Vol. 1, No 1, Year 2008, IARIA Journals, ISSN: 1942-2644

Σε διεθνή Βιβλία με Συλλογές Άρθρων

Emmanouil Serrelis**,** Nikolaos Alexandris, **"**Measuring Network Security", Radio Communications, In-tech edition, Vol. 1, No 1, Year 2009, ISBN: 978-953-7619-X-X, Δεκτό προς δημοσίευση.

Σε διεθνή Συνέδρια μετά από Πλήρη Κρίση

Emmanouil Serrelis, Nikolaos Alexandris, "Disaster Recovery Sites as a Tool of Managing Extreme Attacks," ICISP, pp.20, International Conference on Internet Surveillance and Protection (ICISP'06), 2006, Cap Esterel, Cote d'Azur, France.

Emmanouil Serrelis, Nikolaos Alexandris, "An Empirical Model for Quantifying Security Based on Services," ICCGI, pp.30-36, International Multi-Conference on Computing in the Global Information Technology (ICCGI'07), 2007, Gosier, Guadaloupe, France.

Emmanouil Serrelis, Nikolaos Alexandris, "From High Availability Systems to Fault Tolerant Production Infrastructures", Third International Conference on Networking and Services, IEEE Computer Society, 2007, Athens, Greece.

Emmanouil Serrelis, Nikolaos Alexandris, "Fault Tolerant Production Infrastructures in Practice", IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007, Athens, Greece.

1. Εισαγωγή

1.1. Περιγραφή του ερευνητικού πεδίου

Η ταχεία ανάπτυξη του Διαδικτύου ως μέσο επικοινωνιών και πηγή πληροφοριών, κατά τη διάρκεια των τελευταίων 15 ετών, έχει προκαλέσει πολλούς πρόσθετους προβληματισμούς σε όλες τις επιχειρήσεις και ειδικά σε εκείνες που αναπτύσσουν τις επιχειρηματικές δραστηριότητές τους με τη χρήση του. Δεδομένου ότι ο αριθμός των χρηστών αυξάνεται εκθετικά, ο πιθανός κίνδυνος των κακόβουλων πράξεων αυξάνεται αντίστοιχα. Σε περιπτώσεις όπως εκείνες των τραπεζικών πληροφοριακών συστημάτων, τα χρηματικά ποσά που ανταλλάσσονται είναι σημαντικά μεγαλύτερα από οποιοδήποτε άλλο είδος επιχείρησης, και άρα υπάρχουν περισσότεροι λόγοι ανησυχίας για τους κινδύνους ασφάλειας από το Διαδίκτυο. Οι πιθανοί παράνομοι του Διαδικτύου μπορούν να υπάρξουν ακόμη και μέσα στο δίκτυο της επιχείρησης ή μπορούν να εκμεταλλευτούν άλλα κενά ασφαλείας που δεν είναι άμεσα σχετιζόμενα με τα πληροφοριακά συστήματα.

Παράλληλα, η έλλειψη πολιτικών ασφαλείας, στο επίπεδο του Ανθρώπινου Δυναμικού, μπορεί να υποτιμηθεί ή να παραμεληθεί και δεδομένου ότι τα πληροφοριακά συστήματα είναι ήδη παντού με τη μία μορφή ή την άλλη, υπάρχει μια ανάγκη να βελτιωθούν τόσο οι πολιτικές όσο και τα μέτρα για την ανίχνευση πιθανών αδυναμιών, αναλύοντας και παράγοντας προτάσεις προκειμένου να αναπτύξουν μια ισχυρή, ισορροπημένη και πολύπλευρη ασφάλεια για τα πληροφορικά συστήματα.

Η παρούσα διδακτορική διατριβή ασχολείται με την ανάπτυξη κατάλληλων μέσων και μεθόδων ποσοτικοποίησης, μέτρησης και υπολογισμού της ασφάλειας πληροφοριακών συστημάτων, με βάση τα οποία προτείνει πολιτικές, ενέργειες και μοντέλα που σχετίζονται με την προστασία και την διαχείριση κρίσιμων πληροφοριακών υποδομών, η οποία συνεισφέρει στην αύξηση της συνολικής ασφάλειας των συγκεκριμένων πληροφοριακών συστημάτων.

1.2. Στόχοι της έρευνας

Ο κύριος στόχος της έρευνας είναι η βελτιστοποίηση της ασφάλειας των πληροφοριακών υποδομών και ιδιαιτέρα των κρίσιμων πληροφοριακών υποδομών. Η βελτιστοποίηση αφορά στους τομείς της διαχείρισης των υποδομών αλλά και της ασφάλειας ως γενικότερο θέμα. Επίσης η έρευνα στοχεύει στην ποσοτικοποίηση της ασφάλειας με αντικειμενικά και μη αμφισβητήσιμα κριτήρια.

Ένας επιπλέον στόχος είναι να ισορροπηθούν οι επενδύσεις της ασφάλειας σε κάθε υπηρεσία ώστε να μεγιστοποιηθούν τα κέρδη του οργανισμού.

Γενικότερος στόχος είναι η υποστήριξη ορθολογικών αποφάσεων σχετικά με τις επενδύσεις στον τομέα της ασφάλειας και γενικότερα η σύνδεση των αποτελεσμάτων της ποσοτικοποίησης της ασφάλειας με τις επιχειρηματικές αποφάσεις.

1.3. Κίνητρα

Τα κίνητρα για την επιδίωξη των παραπάνω στόχων είναι πολλά. Πρώτα απ' όλα, το αντικείμενο της διδακτορικής διατριβής αποτελεί ένα ευρύ θέμα το οποίο απολαμβάνει μεγάλου ερευνητικού αλλά και επαγγελματικού ενδιαφέροντος. Το θέμα της ποσοτικοποίησης της ασφάλειας είναι ένα θέμα που αφορά τόσο τον ακαδημαϊκό όσο και τον επαγγελματικό χώρο.

Αυτό συμβαίνει γιατί η ασφάλεια πέρα από τη θεωρητική οπτική της έχει και την πρακτική της πλευρά η οποία μπορεί να μεταφράζεται σε διαφεύγοντα κέρδη ή σε μεγαλύτερες αποδόσεις στις επενδύσεις των εταιριών.

Τέλος, ισχυρό κίνητρο αποτελεί και το γεγονός ότι η ασφάλεια δεν αποτελεί ένα αποκλειστικά τεχνικό θέμα αλλά μπορεί και πρέπει να συνδυάζει αρχές, μεθόδους και γνώσεις από πολλούς άλλους τομείς όπως διοίκηση, νομική, κοινωνιολογία κ.α.

1.4. Μεθοδολογία έρευνας

Τα προβλήματα που επιζητούν λύση στο πλαίσιο της έρευνας είναι πολυσύνθετα και αφορούν την ποσοτικοποίηση και τη διαχείριση αφηρημένων εννοιών όπως η ασφάλεια. Έτσι αναζητήθηκαν τρόποι για τη χρήση και τον συνδυασμό μεγεθών που μπορούν να ποσοτικοποιηθούν με αντικειμενικό τρόπο.

Από την έρευνα προέκυψε ότι οι αφηρημένες έννοιες είναι δύσκολο να ποσοτικοποιηθούν μέσω άμεσης μέτρησης. Αυτός ήταν και ο λόγος που αναπτύχθηκαν μέθοδοι υπολογισμού της ασφάλειας. Η χρήση παραγόντων διαφορετικών από των υπαρχουσών μεθοδολογιών στόχευε στην αντικειμενικότητα της μεθόδου και στην διασφάλιση της συνέπειας των υπολογισμών ανεξαρτήτως του χρόνου υπολογισμού.

Για τη διευκόλυνση του υπολογισμού της ασφάλειας, η έρευνα εστίασε στον υπολογισμό της ασφάλειας σημαντικών επιχειρηματικών υπηρεσιών. Ο συνδυασμός των επιπέδων ασφάλειας των επιμέρους υπηρεσιών ενός οργανισμού παράγει την τιμή της ασφάλειας για ολόκληρο τον οργανισμό.

Σε ο,τι αφορά στην αύξηση και τη διαχείριση της ασφάλειας, εξετάστηκε η εφαρμογή των κλασικών μεθόδων υπολογισμού ως σχετικό εργαλείο διαχείρισης και αναπτύχθηκαν δύο νέες προσεγγίσεις οι οποίες και χρησιμοποιήθηκαν και αυτές ως μέθοδοι βελτιστοποίησης των πληροφοριακών υποδομών και ειδικότερα της ασφάλειάς τους.

1.5. Δομή της διατριβής

Στην εισαγωγή περιγράφονται τα βασικά προβλήματα τα οποία κλήθηκε να επιλύσει η έρευνα ενώ γίνεται έκθεση των στόχων της έρευνας αναφέροντας παράλληλα τα κίνητρα που στήριξαν το ενδιαφέρον για το συγκεκριμένο ερευνητικό πεδίο. Αναλύεται η μεθοδολογία που ακολουθήθηκε κατά τη διάρκεια της έρευνας και αναφέρονται τα οφέλη που προέκυψαν από τα

αποτελέσματα της έρευνας βασικών εννοιών, απαραίτητων για την περιγραφή του προβλήματος.

Στο δεύτερο κεφάλαιο παρουσιάζονται οι σχετικές έννοιες και ορισμοί από τον τομέα της ασφάλειας των πληροφοριακών συστημάτων ενώ περιγράφονται τα γενικά χαρακτηριστικά των πληροφοριακών υποδομών και συστημάτων. Ειδικότερα παρουσιάζονται και αναλύονται οι κατηγορίες των παραγωγικών υποδομών και συστημάτων και τίθενται οι ιδιαιτερότητες των κρίσιμων υποδομών και συστημάτων. Το δεύτερο κεφάλαιο διαπραγματεύεται ακόμα τα στοιχεία που σχετίζονται με τη διαθεσιμότητα των πληροφοριακών υποδομών, όπως η ανοχή σε βλάβες, η εξισορρόπηση φορτίου και οι υποδομές ανάκαμψης μετά από καταστροφή.

Το τρίτο κεφάλαιο, είναι αυτό στο οποίο παρουσιάζονται οι προσεγγίσεις που είναι σχετικές με τον μετασχηματισμό των πληροφοριακών υποδομών. Αναπτύσσεται η Θεωρία Διαχείρισης Αλλαγών και παρουσιάζεται η Βιβλιοθήκη Υποδομής Τεχνολογίας Πληροφοριών. Στη συνέχεια αναπτύσσεται μια κατηγοριοποίηση των μεθοδολογιών μέτρησης της ασφάλειας από τη διεθνή βιβλιογραφία, στις οποίες εντάσσονται και αξιολογούνται οι γνωστές θεωρίες ανάλυσης ευπάθειας, δοκιμών διείσδυσης, υλοποιήσεις αναφοράς, οι βέλτιστες πρακτικές και η διαχείριση κινδύνων. Τέλος, εισάγονται δύο νέες κατηγορίες: αυτή της συνεκτίμησης δομικών στοιχείων της ασφάλειας και εκείνη της συνεκτίμησης παραγόντων έμμεσα σχετιζόμενων με την ασφάλεια.

Στο τέταρτο κεφάλαιο, αναπτύσσονται τα χαρακτηριστικά της μέτρησης της ασφάλειας, οι στόχοι της μέτρησης και οι εναλλακτικές τεχνικές της ποσοτικοποίησης της ασφάλειας. Γίνεται ακόμα μια κριτική σύγκριση μεταξύ της ποσοτικοποίησης και της ποιοτικής ανάλυσης και στοιχειοθετούνται οι απαιτήσεις για κάθε μέθοδο μέτρησης της ασφάλειας. Στη συνέχεια, πραγματοποιείται μια επιχειρηματολογία για τη στροφή προς τον υπολογισμό της ασφάλειας. Με βάση την επιχειρηματολογία αυτή, παρουσιάζονται και αξιολογούνται οι κλασικοί τρόποι υπολογισμού της ασφάλειας και

αναπτύσσονται δύο νέοι, οι οποίοι αποτελούν και μέρος των τελικών αποτελεσμάτων της έρευνας. Το κεφάλαιο ολοκληρώνεται με την παρουσίαση των τεχνικών οπτικοποίησης της ασφάλειας.

Το πέμπτο κεφάλαιο κάνει χρήση των συμπερασμάτων του τέταρτου κεφαλαίου. Αναλύεται η αύξηση της ασφάλειας με τη χρήση τόσο των κλασικών μεθόδων υπολογισμού, όσο και με τις προσεγγίσεις που εισήχθησαν στο τέταρτο κεφάλαιο.

Στο έκτο κεφάλαιο αρχικά αναφέρονται οι μεθοδολογίες διαχείρισης των πληροφοριακών υποδομών. Διερευνάται το πεδίο εφαρμογής των μεθόδων υπολογισμού της ασφάλειας ως εργαλείο βελτιστοποίησης της ασφάλειας των πληροφοριακών υποδομών σε οικονομικό και λειτουργικό επίπεδο. Επίσης, υπολογίζεται και ισορροπείται η αποδοτικότητα των επενδύσεων στην ασφάλεια των πληροφοριακών υποδομών με τα αντίστοιχα οφέλη.

Στο έβδομο κεφάλαιο, παρουσιάζονται τα οφέλη αλλά και οι περιορισμοί των μεθόδων που αναπτύχθηκαν ενώ εξάγονται πρακτικά συμπεράσματα για τις εφαρμογές των μεθόδων.

Τέλος το όγδοο κεφάλαιο, είναι η συνολική ανακεφαλαίωση. Γίνεται σύνοψη των προτάσεων που παρουσιάστηκαν στα επιμέρους κεφάλαια και τονίζεται πως συγκροτούν την πρωτοτυπία της εργασίας. Γίνονται προτάσεις και επισημάνσεις σε επιμέρους θέματα, που χρήζουν περαιτέρω έρευνας.

2. Βασικές έννοιες – Ορισμοί

2.1. Εισαγωγή

Το κεφάλαιο αυτό περιλαμβάνει μια εισαγωγή στη θεωρία, τις έννοιες, τους μηχανισμούς και τις τεχνολογίες οι οποίες αποτελούν τη βάση της έρευνας της διδακτορικής αυτής διατριβής. Ο ακριβής ορισμός των εννοιών που παρουσιάζονται θεωρείται απαραίτητος, τόσο για τη διασύνδεση των γενικών θεμάτων της Πληροφορικής με το κύριο μέρος της έρευνας, όσο και για την επαλήθευση της ακριβούς χρήσης των εννοιών αυτών στο πλαίσιο της συγκεκριμένης διατριβής.

Το κεφάλαιο αυτό περιλαμβάνει τρεις θεματικούς κύκλους. Ο πρώτος θεματικός κύκλος εστιάζει στην Ασφάλεια των Πληροφοριακών Συστημάτων καθώς και στις βασικές έννοιες αυτής.

Ο δεύτερος θεματικός κύκλος αφορά στους κανόνες λειτουργίας και διαχωρισμού των Πληροφοριακών Υποδομών και Συστημάτων. Διαχωρίζονται οι Παραγωγικές Υποδομές από τις υπόλοιπες Υποδομές, ενώ αναγνωρίζονται οι ιδιαιτερότητες των κρίσιμων υποδομών ως προς τα λειτουργικά χαρακτηριστικά και τους αντίστοιχους περιορισμούς αλλά και τις συνεπακόλουθες οικονομικές επιπτώσεις.

Ο τρίτος θεματικός κύκλος περιλαμβάνει τα ειδικότερα θέματα της διαθεσιμότητας των Πληροφοριακών Υποδομών. Στα θέματα αυτά περιλαμβάνονται η ανοχή σε υπολογιστικά λάθη, φυσικές βλάβες και καταστροφές. Παρουσιάζονται επίσης οι τεχνολογίες εξισορρόπησης υπολογιστικού φορτίου και αύξησης της διαθεσιμότητας υπηρεσιών καθώς και οι υποδομές ανάκαμψης από καταστροφή.

2.2. Γενικοί ορισμοί

Η θεματολογία της διατριβής κινείται στο πλαίσιο των πληροφοριακών συστημάτων αλλά και της διαχείρισης πόρων. Κατά συνέπεια χρησιμοποιεί

όρους Πληροφορικής αλλά και Επιχειρησιακής Διοίκησης. Στο κείμενο χρησιμοποιούνται οι ελληνικοί όροι παραθέτοντας όμως και τους αγγλικούς όπου αυτοί θεωρούνται πιο δόκιμοι στην επιστημονική και επαγγελματική πρακτική.

Ο πρώτος ορισμός που θα πρέπει να αναφερθεί αφορά στον όρο «Πληροφοριακό Σύστημα». Κατά το [1] «ένα πληροφοριακό σύστημα (Information System) συνδυάζει την τεχνολογία πληροφορικής (Information Technology) με δεδομένα, διαδικασίες επεξεργασίας δεδομένων και τους ανθρώπους που συλλέγουν και χρησιμοποιούν τα δεδομένα».

Συμπληρωματικά του πληροφοριακού συστήματος, στο πλαίσιο της διατριβής χρησιμοποιείται και ο όρος «Πληροφοριακή Υποδομή» με διαφορετική απόδοση. Κατά το [2] μια Πληροφοριακή Υποδομή «…αποτελείται από 1) το υλικό (hardware), το λογισμικό (software) και τον επικοινωνιακό εξοπλισμό, 2) τους τεχνικούς / μηχανικούς της πληροφορικής και το σχετιζόμενο προσωπικό και 3) την οργάνωση και τις διαδικασίες οι οποίες επηρεάζουν τη χρήση και την επεξεργασία της πληροφορίας. Η Πληροφοριακή Υποδομή παρέχει την τεχνολογική βάση για έναν οργανισμό να διαχειριστεί την πληροφορία του και τα Πληροφοριακά Συστήματά του».

2.3. Ασφάλεια πληροφοριακών συστημάτων

Όπως αναφέρθηκε, τα δομικά στοιχεία ενός Πληροφοριακού Συστήματος είναι το υλικό, το λογισμικό, τα δεδομένα, οι άνθρωποι και οι διαδικασίες. Η Ασφάλεια των Πληροφοριακών Συστημάτων αφορά στην προστασία όλων αυτών των στοιχείων όπως και του Πληροφοριακού Συστήματος ως συνόλου. Στην επιστημονική και επαγγελματική καθημερινότητα, όπως πολύ ορθά αναφέρεται στο [3], ο όρος αυτός δίνει περισσότερη έμφαση στους διάφορους τεχνικούς παράγοντες που σχετίζονται με την ασφάλεια. Η ίδια πηγή διαχωρίζει την ασφάλεια στον έλεγχο και στην προστασία, η οποία με την σειρά της αποτελείται από δύο συνιστώσες: την πρόληψη και τη θεραπεία.

Η ασφάλεια των Πληροφοριακών Συστημάτων περιλαμβάνει τα μέτρα πρόληψης «φθορών» των δομικών τους στοιχείων, μηχανισμούς ανίχνευσης του πότε, πώς και από ποιόν προκλήθηκε φθορά αλλά και τα αντίμετρα αποκατάστασης ή επαναφοράς του Πληροφοριακού Συστήματος στην επιθυμητή λειτουργική κατάσταση.

Από πολλαπλές πηγές, όπως στην [4], λογίζονται ως θεμελιώδεις αρχές της ασφάλειας των Πληροφοριακών Συστημάτων η Ακεραιότητα, η Διαθεσιμότητα και η Εμπιστευτικότητα.

Η αρχή της Εμπιστευτικότητας (Confidentiality) αποσκοπεί στην μη αποκάλυψη ευαίσθητων πληροφοριών σε μη εξουσιοδοτημένα άτομα. Η Εμπιστευτικότητα μπορεί να εκφραστεί ως Ιδιωτικότητα (Privacy), η οποία αφορά συνήθως προσωπικά δεδομένα, ή Μυστικότητα (Secrecy) η οποία αφορά δεδομένα τα οποία συνήθως αφορούν έναν οργανισμό.

Η αρχή της Ακεραιότητας (Integrity) των δεδομένων είναι μια βασική απαίτηση του ιδιοκτήτη (owner) μιας πληροφορίας η οποία αφορά στην προστασία των Πληροφοριακών Συστημάτων από ανεπιθύμητες αλλαγές. Αυτό περιλαμβάνει μια «πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων» [4].

Η Διαθεσιμότητα (Availability) των Πληροφοριακών Συστημάτων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των νομίμων χρηστών όποτε απαιτείται η χρήση τους. Σε αυτή των βασική αρχή εστιάζει την προσοχή της η διατριβή και αναπτύσσεται η απαραίτητη έρευνα.

Ως δευτερεύουσες αρχές της ασφάλειας των Πληροφοριακών Συστημάτων θεωρούνται η μη-Αποποίηση Ευθύνης και η Αυθεντικοποίηση. Η μη-Αποποίηση

Ευθύνης (Non-Repudiation) είναι η εξασφάλιση ότι οι συναλλασσόμενοι (χρήστες και πάροχοι προϊόντων και υπηρεσιών) δεν μπορούν να αρνηθούν ούτε την συμμετοχή τους στην συναλλαγή ούτε το περιεχόμενο αυτής. Η Αυθεντικοποίηση (Authentication) έχει την έννοια της επαλήθευσης ή της πιστοποίησης της ταυτότητας μιας οντότητας (χρήστη ή παρόχου προϊόντων και υπηρεσιών).

2.4. Πληροφοριακές Υποδομές και Συστήματα

Οι σύγχρονες Πληροφοριακές Υποδομές υποστηρίζουν και εξυπηρετούν ουσιαστικά όλες τις διαφορετικές ανθρώπινες δραστηριότητες, από τις πιο απλές μέχρι και τις πιο σύνθετες. Πάνω σε αυτές στηρίζονται υπηρεσίες που σχετίζονται με τις βασικές ανάγκες της σημερινής κοινωνίας, όπως η ύδρευση, η επικοινωνία, οι συναλλαγές και η διατροφή. Η ενότητα αυτή παρουσιάζει τα είδη των Πληροφοριακών Υποδομών που απασχόλησαν την έρευνά μας.

2.4.1. Παραγωγικές υποδομές και συστήματα

Όπως αναφέρθηκε και παραπάνω οι Πληροφοριακές Υποδομές παρέχουν τη τεχνολογική βάση για τους οργανισμούς να διαχειριστούν τις πληροφορίες τους καθώς και τα Πληροφοριακά Συστήματά τους. Στο πλαίσιο της διατριβής, θεωρούμε τέσσερεις μορφές Συστημάτων και Υποδομών. Αυτά είναι τα Παραγωγικά Πληροφοριακά Συστήματα, τα προ-Παραγωγικά Πληροφοριακά Συστήματα, τα Πληροφοριακά Συστήματα Λήψης Αποφάσεων και τα Δοκιμαστικά Πληροφοριακά Συστήματα.

Τα Παραγωγικά Πληροφοριακά Συστήματα (Production IT Systems) και οι αντίστοιχες Υποδομές αφορούν μόνο τα Πληροφοριακά Συστήματα που εξυπηρετούν ανάγκες των πελατών ενός οργανισμού. Βρίσκονται δηλαδή στην «πρώτη γραμμή» του οργανισμού και είναι απαραίτητα για την εξυπηρέτηση των βασικών επιχειρηματικών σκοπών της επιχείρησης ή του οργανισμού. Ενδέχεται να είναι Συστήματα που εξυπηρετούν συναλλαγές με πελάτες και προμηθευτές καθώς και εσωτερικές συναλλαγές στον κάθε οργανισμό.

Τα προ-Παραγωγικά Πληροφοριακά Συστήματα (pre-Production IT Systems) και οι αντίστοιχες Υποδομές αφορούν μόνο τα υπό ανάπτυξη Πληροφοριακά Συστήματα ενός οργανισμού και δεν έχουν ακόμα ενταχθεί στην παραγωγική διαδικασία. Με την ολοκλήρωση της φάσης της ανάπτυξης, τα συστήματα και οι υποδομές αυτές κατατάσσονται στα Παραγωγικά Πληροφοριακά Συστήματα και πλέον εξυπηρετούν τους επιχειρηματικούς σκοπούς του οργανισμού. Παράδειγμα θα μπορούσε να αποτελέσει ένα νέο σύστημα διαχείρισης προσωπικού στο οποίο δεν έχουν ακόμα εισαχθεί τα κατάλληλα δεδομένα.

Τα Πληροφοριακά Συστήματα Λήψης Αποφάσεων (Decision Support Systems) και οι αντίστοιχες Υποδομές αποτελούν μια ειδική κατηγορία και αφορούν τα Πληροφοριακά Συστήματα τα οποία υποστηρίζουν τη διοίκηση ενός οργανισμού από πολλά και διαφορετικά επίπεδα. Τα συστήματα αυτά διαχειρίζονται και επεξεργάζονται πληροφορίες οι οποίες υποβοηθούν την κατανόηση των θέσεων και των επιδόσεων του οργανισμού με σκοπό τη λήψη αποφάσεων βασισμένων σε έγκυρα στοιχεία. Η βασική διαφορά τους με τα Παραγωγικά Πληροφοριακά Συστήματα είναι ότι τα τελευταία είναι απαραίτητα για τη λειτουργία του οργανισμού, ενώ τα Πληροφοριακά Συστήματα Λήψης Αποφάσεων δεν θεωρούνται απαραίτητα.

Θα πρέπει να σημειωθεί ότι υπάρχουν συστήματα και υποδομές οι οποίες έχουν κοινά χαρακτηριστικά και με τα Παραγωγικά Πληροφοριακά Συστήματα και με τα Πληροφοριακά Συστήματα Λήψης Αποφάσεων. Ένα παράδειγμα αυτών μπορεί να είναι ένα Σύστημα Λήψης Αποφάσεων το οποίο υπολογίζει και παρουσιάζει τον πιστωτικό κίνδυνο σε πραγματικό χρόνο. Στο πλαίσιο της διατριβής, αυτού του είδους τα συστήματα κατατάσσονται στα Παραγωγικά Πληροφοριακά Συστήματα.

Τα Δοκιμαστικά Πληροφοριακά Συστήματα (Test IT Systems) και οι αντίστοιχες Υποδομές αφορούν Πληροφοριακά Συστήματα που δεν εξυπηρετούν υπηρεσίες προς τους πελάτες ή το προσωπικό της. Λειτουργούν μόνο για λόγους συντήρησης και δεν θεωρούνται απαραίτητα για τη

λειτουργία μιας επιχείρησης. Ένα παράδειγμα ενός Δοκιμαστικού Πληροφοριακού Συστήματος είναι ένα σύστημα ανάπτυξης νέων εφαρμογών σε ένα χρηματοπιστωτικό οργανισμό. Το σύστημα αυτό είναι παρόμοιο με το αντίστοιχο παραγωγικό, αλλά χρησιμοποιείται μόνο για τις δοκιμές νέων εφαρμογών πριν αυτές ενσωματωθούν στα Παραγωγικά Συστήματα.

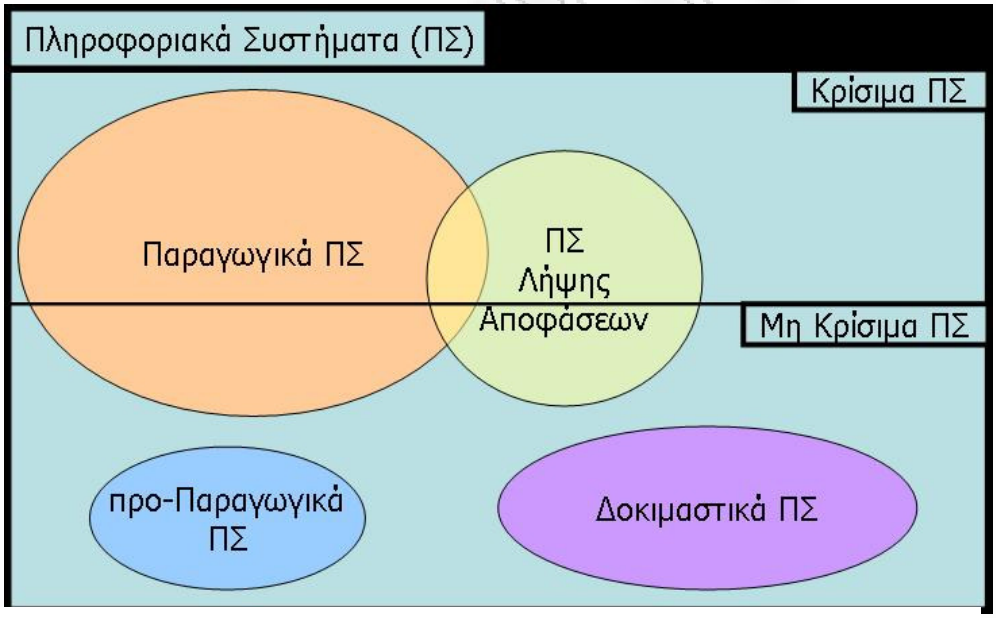
2.4.2. Κρίσιμες υποδομές και συστήματα

Επιπλέον του βασικού διαχωρισμού που αναφέρθηκε παραπάνω, οι Πληροφοριακές Υποδομές μπορούν να διαχωριστούν σε Κρίσιμες και μη Κρίσιμες πληροφοριακές υποδομές. Στην ενότητα αυτή παρουσιάζονται τα λειτουργικά χαρακτηριστικά, οι περιορισμοί αλλά και οι πιθανές επιπτώσεις από τη μη διαθεσιμότητα κρίσιμων υποδομών.

Σύμφωνα με το [5] ως Κρίσιμες Υποδομές (Critical Infrastructures) ορίζονται «οι οργανισμοί και τα δίκτυα πληροφοριών, επικοινωνιών και διανομής τα οποία διασφαλίζουν διαρκή διανομή εκείνων των αγαθών και των υπηρεσιών που είναι απαραίτητα για την εθνική άμυνα, την οικονομία, τη δημόσια υγεία και την ασφάλεια των πολιτών». Εξετάζοντας τις κρίσιμες υποδομές και τα συστήματα από την οπτική ενός συγκεκριμένου οργανισμού, είναι δυνατό να αποδώσουμε τον συγκεκριμένο ορισμό λαμβάνοντας υπόψη τις λειτουργικές ιδιαιτερότητες καθώς και τους επιχειρηματικούς στόχους του οργανισμού.

Στο πλαίσιο ενός οργανισμού, Κρίσιμες Πληροφοριακές Υποδομές και Συστήματα ονομάζονται οι Υποδομές και τα Συστήματα εκείνα που χωρίς την ύπαρξη και τη σωστή λειτουργία τους δεν είναι εφικτή η εκπλήρωση των επιχειρηματικών του στόχων, όπως η παροχή υπηρεσιών και η παραγωγή προϊόντων.

Οι Κρίσιμες Πληροφοριακές Υποδομές και Συστήματα αφορούν αποκλειστικά Παραγωγικές Υποδομές και Συστήματα, μια που εξ ορισμού οι Παραγωγικές Υποδομές είναι απαραίτητες για την εξυπηρέτηση των βασικών επιχειρηματικών σκοπών της επιχείρησης ή του οργανισμού. Μέρος των Πληροφοριακών Συστημάτων Λήψης Αποφάσεων μπορεί να είναι επίσης κρίσιμο για έναν οργανισμό λόγω του γεγονότος ότι ο συγκεκριμένος οργανισμός δεν μπορεί να προσφέρει τις υπηρεσίες ή τα προϊόντα του με τους ποιοτικούς κανόνες ή τους εμπορικούς όρους που ο ίδιος επιθυμεί. Δεν αποτελεί όμως συνηθισμένη πρακτική να χαρακτηρίζονται τα προ-Παραγωγικά και τα Δοκιμαστικά Πληροφοριακά Συστήματα ως κρίσιμα. Το Διάγραμμα 2.1 παρουσιάζει τον διαχωρισμό των συστημάτων όπως αυτός περιγράφεται στην διατριβή.



Διάγραμμα 2.1 – Διαχωρισμός πληροφοριακών συστημάτων

Υπάρχουν διάφορα παραδείγματα τα οποία αναδεικνύουν τα διαφορετικά κριτήρια που χρησιμοποιούνται για να χαρακτηριστούν οι Πληροφοριακές Υποδομές και Συστήματα ως κρίσιμα.

Ένα χαρακτηριστικό παράδειγμα αφορά ένα χρηματοπιστωτικό οργανισμό όπου ένα Πληροφοριακό Σύστημα διαχείρισης κινδύνου μπορεί θεωρητικά να μην είναι απαραίτητο για τη δανειοδότηση ενός πελάτη. Ο οργανισμός όμως

είναι πιθανό να μην αποδέχεται τον συγκεκριμένο χρηματοπιστωτικό κίνδυνο σε οποιαδήποτε συνθήκες. Η **λειτουργική απαίτηση** αυτή χαρακτηρίζει το συγκεκριμένο Σύστημα Λήψης Αποφάσεων ως κρίσιμο. Το κριτήριο κρισιμότητας που αναφέρεται εδώ είναι το επίπεδο αποδοχής ενός χρηματοπιστωτικού κινδύνου.

Σε ένα άλλο παράδειγμα, ενδέχεται κάποια από τα Παραγωγικά Συστήματα να μην επηρεάζουν τόσο πολύ την παροχή των υπηρεσιών ή την παροχή των προϊόντων. Στο παράδειγμα μιας εταιρίας συσκευασίας, η μη διαθεσιμότητα ενός Πληροφοριακού Συστήματος υπεύθυνου για την εκτύπωση χαρτιού διαστάσεων 3x3 μέτρων μπορεί να μην θεωρείται σημαντική, λόγω των χαμηλών εσόδων ως **ποσοστό επί των συνολικών εσόδων**. Το γεγονός αυτό χαρακτηρίζει το συγκεκριμένο Σύστημα ως μη κρίσιμο. Στο συγκεκριμένο παράδειγμα το κριτήριο κρισιμότητας είναι το ποσοστό συνεισφοράς ενός συγκεκριμένου Πληροφοριακού Συστήματος στα συνολικά έσοδα ενός οργανισμού.

Μια άλλη ομάδα περιπτώσεων αφορά τους οργανισμούς που χαρακτηρίζουν ένα πληροφοριακό σύστημα ή υποδομή ως κρίσιμα ή μη κρίσιμα ανάλογα με τη χρονική ανοχή που μπορούν να επιδείξουν σε μια περίπτωση μη διαθεσιμότητάς τους. Ένα χαρακτηριστικό παράδειγμα είναι ένα πληροφοριακό σύστημα διαχείρισης αποθήκης. Εάν υπάρχει μια σημαντική **χρονική ανοχή** (π.χ. 2 εβδομάδες) μη διαθεσιμότητας το σύστημα αυτό θα μπορούσε να χαρακτηριστεί μη κρίσιμο.

Ένα άλλο παράδειγμα, αυτό των χρηματοπιστωτικών οργανισμών σε σχέση με τους κανόνες της Επιτροπής της Βασιλείας [6]. Οι κανόνες της «Βασιλείας 2» καθορίζουν το ύψος των εποπτικών κεφαλαίων που πρέπει να έχουν οι τράπεζες για να μπορούν να δανείζουν και να κάνουν άλλες εργασίες. Ο έλεγχος συμμόρφωσης με αυτούς τους κανόνες γίνεται με τη χρήση ειδικών Πληροφοριακών Συστημάτων, μη διαθεσιμότητα και λειτουργία των οποίων επισείει σημαντικές κυρώσεις. Το παράδειγμα αυτό αναδεικνύει πως η

κανονιστική συμμόρφωση μπορεί να αποτελέσει ένα ακόμη κριτήριο κρισιμότητας των Πληροφοριακών Υποδομών και Συστημάτων.

Τα παραπάνω κριτήρια αποτυπώνονται συγκεντρωτικά στον Πίνακα 2.1.

Κριτήρια χαρακτηρισμού των Πληροφοριακών Υποδομών και Συστημάτων ως κρίσιμα	
Βασικό Κριτήριο : Μέγεθος επικινδυνότητας – Κίνδυνος / Ρίσκο	
Λειτουργικές προδιαγραφές	Ποσοστό επί των συνολικών Εσόδων
Χρονική Ανοχή	Κανονιστική Συμμόρφωση

Πίνακας 2.1 – Κριτήρια κρίσιμων υποδομών και συστημάτων

Θα πρέπει να επισημανθεί ότι το ίδιο Πληροφοριακό Σύστημα μπορεί να είναι κρίσιμο για έναν οργανισμό και μη κρίσιμο για ένα άλλο. Στο παράδειγμα με τη διαχείριση της αποθήκης, το συγκεκριμένο πληροφοριακό σύστημα θα μπορούσε να είναι κρίσιμο για μια εταιρία που ειδικεύεται στην αποθήκευση και άρα βασίζει την κύρια επιχειρηματική της δραστηριότητα στο συγκεκριμένο σύστημα.

Είναι επίσης πιθανό, οι Κρίσιμες Πληροφοριακές Υποδομές να αποτελούν Πληροφοριακές Υποδομές που βρίσκονται εκτός του Οργανισμού. Στο παράδειγμα της εταιρίας συσκευασίας, κρίσιμη Πληροφοριακή Υποδομή μπορεί να είναι και η Πληροφοριακή Υποδομή του προμηθευτή πρώτων υλών της εταιρίας.

Το κοινό στοιχείο αυτών των κριτηρίων είναι ότι μπορούν να μεταφραστούν σε ένα βασικό κριτήριο χαρακτηρισμού των Πληροφοριακών Υποδομών και Συστημάτων ως κρίσιμα ή μη κρίσιμα. Το κριτήριο αυτό είναι το μέγεθος της επικινδυνότητας (ή Κίνδυνος ή Ρίσκο - Risk) και σύμφωνα με το [7] περιλαμβάνει «την πιθανότητα βλάβης ή απώλειας και αναφέρεται στην αβεβαιότητα των μελλοντικών γεγονότων και των πιθανών αποτελεσμάτων που θα μπορούσαν να έχουν ένα ανεπιθύμητο αποτέλεσμα σε έναν οργανισμό».

Γενικά, ο κίνδυνος είναι η πιθανότητα ενός ανεπιθύμητου αποτελέσματος σε μια κατάσταση με αβέβαιο αποτέλεσμα. Η διαχείριση του κινδύνου είναι το αντικείμενο της ασφάλειας, το οποίο αποτελεί το γενικότερο αντικείμενο αυτής της διατριβής. Ο κίνδυνος αυξάνεται όσο αυξάνεται η αξία των παγίων για έναν οργανισμό. Εάν θεωρήσουμε ως πάγια τις Πληροφοριακές Υποδομές και τα Πληροφοριακά Συστήματα, τότε η μεγαλύτερη αξία τους συνεπάγεται και μεγαλύτερη κρισιμότητα άρα και μεγαλύτερο κίνδυνο.

Τα παραπάνω εκφράζονται και μαθηματικά από την παρακάτω εξίσωση [8]:

$$R = V \times P \times S$$

όπου : R είναι ο κίνδυνος (Risk)

V είναι η αξία του παγίου (Value of asset)

P είναι η πιθανότητα να συμβεί η απειλή (Probability of occurrence of threat)

S είναι το μέγεθος της έκθεσης του παγίου (ή αδυναμία - vulnerability of the asset to the threat).

Στα παραδείγματα που δόθηκαν παραπάνω η αξία του παγίου, δηλαδή των Πληροφοριακών Συστημάτων και Υποδομών, είναι υψηλή άρα αποτελούν κρίσιμες, για τους αντίστοιχους οργανισμούς, υποδομές.

Υπάρχουν, όμως και παραδείγματα τα οποία δίνουν έμφαση στην **πιθανότητα** να συμβεί μια συγκεκριμένη απειλή, όπως ένα Πληροφοριακό Σύστημα το οποίο χρησιμοποιείται για την εξόρυξη ορυκτών και απειλείται από φυσικές αιτίες – π.χ. υψηλές θερμοκρασίες, σκόνη και υγρασία. Οι συγκεκριμένες απειλές παρουσιάζουν μεγάλη πιθανότητα να συμβούν άρα το μέγεθος της επικινδυνότητας που παρουσιάζει το συγκεκριμένο Πληροφοριακό Σύστημα είναι αυξημένο.

Ανάλογα, στο παράδειγμα ενός Πληροφοριακού Συστήματος που καθοδηγεί ένα διαστημικό όχημα, το μέγεθος της έκθεσής του σε μια απειλή από κομήτη

μεταφράζεται σε ένα σημαντικό μέγεθος της επικινδυνότητας που αντιμετωπίζει το συγκεκριμένο Πληροφοριακό Σύστημα.

Θα πρέπει να παρατηρηθεί ότι πιθανώς τα παραπάνω μεγέθη δεν μπορούν να μετρηθούν με απόλυτη ακρίβεια και αντικειμενικότητα σε όλες τις περιπτώσεις. Για το λόγο αυτό, συχνά ο υπολογισμός του επιπέδου της επικινδυνότητας αναφέρεται ως ***εκτίμηση κινδύνου***. Ο όρος εκτίμηση υπονοεί ότι πιθανώς υπάρχουν υποκειμενικά κριτήρια τα οποία είναι δυνατό να επηρεάζουν τη συγκεκριμένη διαδικασία.

Συμπερασματικά, ο χαρακτηρισμός ενός Πληροφοριακού Συστήματος ή μιας Πληροφοριακής Υποδομής ως κρίσιμου ή μη, πραγματοποιείται με την εκτίμηση του μεγέθους της επικινδυνότητας που παρουσιάζει. Τα Πληροφοριακά Συστήματα και οι Πληροφοριακές Υποδομές που εκτιμάται ότι παρουσιάζουν το μεγαλύτερο μέγεθος επικινδυνότητας είναι και τα κρισιμότερα για ένα οργανισμό και άρα χρήζουν περισσότερης προστασίας από τους υπόλοιπους.

2.5. Διαθεσιμότητα υποδομών ανεκτικών σε λάθη, βλάβες και καταστροφές

Όπως αναφέρθηκε σε προηγούμενη ενότητα υπάρχουν υποδομές και συστήματα οι οποίες παρουσιάζουν υψηλό κίνδυνο και ως εκ τούτου χαρακτηρίζονται κρίσιμες. Για αυτές, λοιπόν, τις υποδομές είναι απαραίτητο να υλοποιούνται οι κατάλληλοι μηχανισμοί, διαδικασίες και τεχνολογίες οι οποίες θα διασφαλίζουν τη διαθεσιμότητα αυτών των υπηρεσιών ακόμα και σε έκτακτες περιπτώσεις ανάγκης, όπου ένα μέρος ή ολόκληρη η υποδομή, είτε έχει επηρεαστεί από κάποιο λάθος, είτε έχει εμφανίσει κάποια βλάβη, είτε ακόμα έχει υποστεί κάποια καταστροφή.

Οι παρακάτω παράγραφοι παρουσιάζουν τις ιδιότητες των μηχανισμών, των διαδικασιών και των τεχνολογιών οι οποίες επηρεάζουν τη διαθεσιμότητα των υποδομών και των συστημάτων.

2.5.1. Διαθεσιμότητα

Όπως αναφέρθηκε και στη σχετική ενότητα, η Διαθεσιμότητα είναι μία από τις θεμελιώδεις αρχές της Ασφάλειας Πληροφοριακών Συστημάτων. Στην ενότητα αυτή παρουσιάζονται οι βασικές προϋποθέσεις και τις τεχνικές που υιοθετούνται στην παροχή υπηρεσιών που βασίζονται σε υποδομές και συστήματα υψηλής διαθεσιμότητας.

Σύμφωνα με το [9], Διαθεσιμότητα είναι το ποσοστό του χρόνου που ***μπορεί*** να χρησιμοποιηθεί μια υπηρεσία, εφαρμογή, σύστημα ή υποδομή για παραγωγική δουλειά σε σχέση με το χρόνο που ***πρέπει*** να είναι λειτουργική. Ο χρόνος για τον οποίο η υπηρεσία, εφαρμογή, σύστημα ή υποδομή θα πρέπει να είναι λειτουργική καλείται Περίοδος Λειτουργίας (Mission Time), η οποία μπορεί να είναι οι τυπικές εργάσιμες ώρες (5 ημέρες ανά εβδομάδα, 8 ώρες ανά ημέρα – 8x5) ή συνεχής λειτουργία (7 ημέρες ανά εβδομάδα, 24 ώρες ανά ημέρα – 24x7).

Ο σημαντικότερος δείκτης είναι αυτός της διαθεσιμότητας μιας επιχειρηματικής υπηρεσίας (Business Service), διότι μια επιχειρηματική υπηρεσία προϋποθέτει όλα τα υπόλοιπα στοιχεία, όπως τα Πληροφοριακά Συστήματα και τις αντίστοιχες Υποδομές ενώ το αντίστροφο δεν ισχύει. Είναι λοιπόν ασφαλές να θεωρηθεί ότι η διαθεσιμότητα των επιχειρηματικών υπηρεσιών έχει την ύψιστη σημασία για έναν οργανισμό, σε σύγκριση με την διαθεσιμότητα οποιουδήποτε άλλου Συστήματος ή Υποδομής – Πληροφοριακής ή μη. Στο πλαίσιο της διατριβής αυτής, τα Πληροφοριακά Συστήματα θεωρούνται ως ο σημαντικότερος κρίκος της αλυσίδας παροχής μιας επιχειρηματικής υπηρεσίας και για αυτό η εξέταση που ακολουθεί εστιάζεται σε αυτά.

Υπάρχουν δύο κύριοι παράγοντες που καθορίζουν την διαθεσιμότητα των Πληροφοριακών Συστημάτων.

Ο πρώτος παράγοντας είναι το χρονικό διάστημα που απαιτείται για την αποκατάσταση της λειτουργίας των συστημάτων από την στιγμή που θα εμφανιστεί η βλάβη.

Κάθε οργανισμός ορίζει ένα μέγιστο χρόνο για να επανέλθει ένα Πληροφοριακό Σύστημα από την στιγμή που προκύψει μια βλάβη. Αυτό το χρονικό διάστημα ονομάζεται Μέγιστος Αποδεκτός Χρόνος Αποκατάστασης (MAXA / Recovery Time Objective – RTO). Εάν ο χρόνος επαναφοράς μετά από μια βλάβη είναι τελικά μεγαλύτερος από τον MAXA τότε θεωρείται ότι ο οργανισμός υφίσταται ανεπανόρθωτη ζημιά.

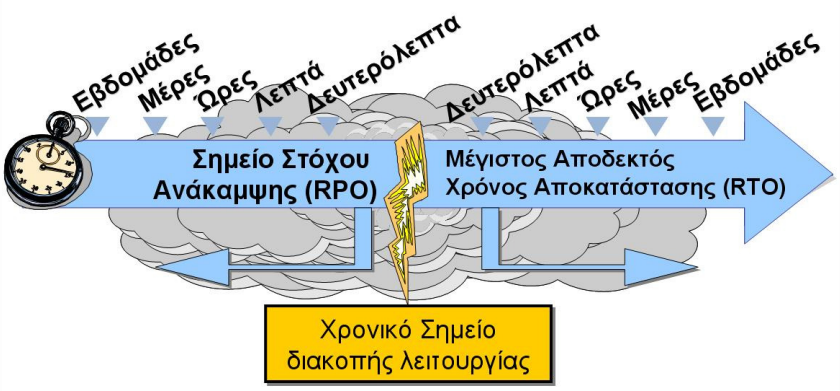
Ο πραγματικός χρόνος επαναφοράς ποικίλει από περίπτωση σε περίπτωση [9]. Εάν, για παράδειγμα, μια εφαρμογή παρουσιάσει βλάβη, η επαναφορά μπορεί να απαιτεί μόνο την επανεκκίνηση της εφαρμογής στο ίδιο σύστημα. Εάν όμως οφείλεται σε ένα άγνωστο σφάλμα του υλικού τότε μπορεί να είναι πολύ πιο χρονοβόρο απαιτώντας πολύ περισσότερες ενέργειες όπως:

- Ειδοποίηση του παρόχου της υπηρεσίας για τη βλάβη
- Αναμονή για την ανταπόκριση του αρμόδιου τεχνικού
- Ακριβής προσδιορισμός των στοιχείων που δυσλειτουργούν
- Αντικατάσταση των δυσλειτουργούντων στοιχείων
- Επανεκκίνηση συστήματος
- Επαναφορά του συστήματος αρχείων
- Επαναφορά της βάσης δεδομένων
- Επανεκκίνηση του λογισμικού που είναι υπεύθυνο για τις δικτυακές επικοινωνίες
- Επανεκκίνηση της εφαρμογής

Ο δεύτερος παράγοντας αναφέρεται στον όγκο των χαμένων πληροφοριών λόγω της βλάβης, το οποίο συνδέεται άμεσα με την παλαιότητα των δεδομένων με τα οποία θα ανακάμψουν τα συστήματα μετά από τη συγκεκριμένη βλάβη.

Όπως και για τον καθορισμό του MAXA, έτσι και σε αυτή την περίπτωση, κάθε οργανισμός ορίζει ένα μέγιστο όγκο χαμένων δεδομένων ο οποίος θεωρείται αποδεκτός κατά την επαναφορά ενός Πληροφοριακού Συστήματος από μια βλάβη. Ο μέγιστος επιτρεπτός όγκος χαμένων δεδομένων ορίζει το Σημείο Στόχου Ανάκαμψης (ΣΣΑ / Recovery Point Objective – RPO) το οποίο εκφράζεται σε μονάδες χρόνου. Αυτό είναι το χρονικό διάστημα πριν από την βλάβη, για το οποίο, όποια πληροφορία δημιουργήθηκε θα χαθεί με την επαναφορά των συστημάτων. Εφόσον τα δεδομένα που θα διατηρηθούν μετά την επαναφορά των συστημάτων είναι από σημείο που προηγείται του ΣΣΑ τότε θεωρείται ότι ο οργανισμός υφίσταται ανεπανόρθωτη ζημιά.

Το Διάγραμμα 2.2 παρουσιάζει τους δύο κύριους παράγοντες της διαθεσιμότητας σε σχέση με ένα τυχαίο γεγονός διακοπής της λειτουργίας των Πληροφοριακών Συστημάτων.



Διάγραμμα 2.2 – Παράγοντες διαθεσιμότητας

Επιπλέον των παραπάνω, υπάρχουν και δύο δευτερεύοντες παράγοντες που καθορίζουν την διαθεσιμότητα των Πληροφοριακών Συστημάτων. Αυτοί είναι η Αξιοπιστία και η Ανακτησιμότητα.

Η Αξιοπιστία (Reliability) των στοιχείων που συνθέτουν τα συστήματα, είναι η συχνότητα με την οποία εμφανίζουν βλάβη. Τα στοιχεία αυτά αποτελούν τα Πληροφοριακά Συστήματα περιλαμβάνουν κατ' ελάχιστο το υλικό (hardware), το λειτουργικό σύστημα (operating system) και το λογισμικό εφαρμογής (application software). Είναι επίσης πιθανό να εξαρτώνται από συσκευές

αποθήκευσης δεδομένων (data storage devices), συσκευές δικτυακής πρόσβασης (network access devices), βάσεις δεδομένων (databases) και διάφορα άλλα συστατικά. Κάθε ένα από αυτά τα στοιχεία έχει τον δικό του χρόνο πριν εμφανίσει μια βλάβη. Αυτό το χρονικό διάστημα ονομάζεται Μέσος Χρόνος Πριν από την εμφάνιση Αστοχίας ή Δυσλειτουργίας (ΜΧΠΑ / Mean Time Before Failure – MTBF) και αποτελεί ένα στατιστικό στοιχείο με βάση το οποίο εκτιμάται η Αξιοπιστία κάθε στοιχείου (ή αυτοτελούς μονάδας) ενός Πληροφοριακού Συστήματος.

Η Ανακτησιμότητα [10] (Recoverability) των στοιχείων που συνθέτουν τα συστήματα, είναι το χρονικό διάστημα το οποίο απαιτείται για την επιδιόρθωση μιας βλάβης. Κάθε ένα από τα στοιχεία (ή αυτοτελείς μονάδες) των Πληροφοριακών Συστημάτων έχει τον δικό του χρόνο επιδιόρθωσης για κάθε βλάβη. Αυτό το χρονικό διάστημα ονομάζεται Μέσος Χρόνος Επιδιόρθωσης (ΜΧΕ / Mean Time To Repair – MTTR) και αποτελεί ένα στατιστικό στοιχείο με βάση το οποίο εκτιμάται η Ανακτησιμότητα κάθε στοιχείου (ή αυτοτελούς μονάδας) ενός Πληροφοριακού Συστήματος.

Παράγοντας Διαθεσιμότητας	**Μετρήσιμο Μέγεθος**	**Μονάδα Μέτρησης**
Κύριοι Παράγοντες		
Το χρονικό διάστημα που απαιτείται για την αποκατάσταση της λειτουργίας των συστημάτων	Μέγιστος Αποδεκτός Χρόνος Αποκατάστασης (Recovery Time Objective)	Δευτερόλεπτα / Λεπτά / Ώρες / Μέρες / Εβδομάδες
Το χρονικό σημείο στο οποίο θα επανέλθουν τα δεδομένα μετά από μια βλάβη	Σημείο Στόχου Ανάκαμψης (Recovery Point Objective)	Δευτερόλεπτα / Λεπτά / Ώρες / Μέρες / Εβδομάδες
Δευτερεύοντες Παράγοντες		
Αξιοπιστία	Μέσος Χρόνος Πριν από την εμφάνιση Αστοχίας ή Δυσλειτουργίας	Ώρες / Μέρες
Ανακτησιμότητα	Μέσος Χρόνος Επιδιόρθωσης	Λεπτά / Ώρες / Μέρες

Πίνακας 2.2 – Παράγοντες απεικόνισης διαθεσιμότητας

Ο Πίνακας 2.2 παρουσιάζει συγκεντρωτικά όλους τους παράγοντες (Κύριους και Δευτερεύοντες) μαζί με τα αντίστοιχα μεγέθη που χρησιμοποιούνται για την απεικόνιση της Διαθεσιμότητας.

Όπως γίνεται κατανοητό η διαθεσιμότητα ενός πληροφοριακού συστήματος και κατ' επέκταση και μιας επιχειρηματικής υπηρεσίας είναι συνάρτηση πολλαπλών παραγόντων. Έτσι, ο χρόνος που απαιτείται για να επανέλθει ένα Πληροφοριακό Σύστημα από τη στιγμή που προκύψει μια βλάβη εξαρτάται τόσο από το ακριβές αίτιο που προκάλεσε τη βλάβη καθώς και από το πλήθος και το είδος των στοιχείων του Πληροφοριακού Συστήματος που επηρεάστηκαν από τη βλάβη.

2.5.2. Υψηλή διαθεσιμότητα

Η αύξηση της διαθεσιμότητας των Πληροφοριακών Συστημάτων υλοποιείται με πολλούς και διαφορετικούς τρόπους, με τον καθένα να χρησιμοποιεί διαφορετικές τεχνικές και τεχνολογίες. Η πιο διαδεδομένη τεχνική ορολογία για να περιγράψει τις τεχνικές αυτές είναι οι τεχνικές Υψηλής Διαθεσιμότητας (High Availability).

Όπως αναφέρεται και στο [11], «οι βασικές έννοιες και οι τεχνικές που χρησιμοποιούνται για να χτίσουν τα υπολογιστικά συστήματα υψηλής διαθεσιμότητας είναι να είναι διαμορφώσιμα, να έχουν υπομονάδες γρήγορης αστοχίας, να έχουν ανεξάρτητες μονάδες αποτυχίας, να υπάρχει πλεονασμός και να είναι επισκευάσιμα». Οι έννοιες και οι τεχνικές αυτές αναφέρονται τόσο στο υλικό και στο λογισμικό, όσο και στην ανοχή των ελαττωματικών διαδικασιών και των ελαττωμάτων που σχετίζονται με τις όποιες παραμέτρους του περιβάλλοντος.

Οι κύριοι χρήστες των συστημάτων υψηλής διαθεσιμότητας (high-availability systems) είναι οι οργανισμοί που σχετίζονται με ελέγχους διεργασιών και παραγωγής καθώς και με εφαρμογές επεξεργασίας. Επιχειρήσεις που σχετίζονται με κρίσιμα αντικείμενα όπως τηλεφωνικά δίκτυα, μεταφορές, υγεία και χρηματικές συναλλαγές δεν έχουν την πολυτέλεια να σταματήσουν τη λειτουργία τους λόγω μιας διακοπής λειτουργίας των Πληροφοριακών τους Συστημάτων.

Σε αυτές τις περιπτώσεις, οι διακοπές λειτουργίας μεταφράζονται άμεσα σε μειωμένη παραγωγικότητα και κέρδη, ενώ εάν οι διακοπές συνεχιστούν μπορεί να οδηγήσουν σε απώλειες χρημάτων, ευκαιριών, ακόμα ανθρώπινων ζωών.

Είναι σημαντικό να εκτιμάται ο βαθμός ετοιμότητας των οργανισμών για αυτές τις περιπτώσεις. Η εκτίμηση αυτή μπορεί να γίνει με τη μέτρηση της διαθεσιμότητας του κάθε Πληροφοριακού Συστήματος. Ο δείκτης της διαθεσιμότητας αποτυπώνεται ως ποσοστό του χρόνου που **είναι** πραγματικά διαθέσιμο για χρήση το κάθε Πληροφοριακό Σύστημα σε σχέση με το χρόνο που θα **έπρεπε** να είναι διαθέσιμο.

Για τα συστήματα τα οποία θα πρέπει να είναι συνεχώς διαθέσιμα, η διαθεσιμότητα εκφράζεται ως ποσοστό διαθεσιμότητας ανά έτος.

Για παράδειγμα, Πληροφοριακά Συστήματα τα οποία αποτυγχάνουν να εξυπηρετήσουν τους χρήστες τους κάθε δύο εβδομάδες και έχουν κατά μέσο όρο δέκα ώρες χρόνο επαναφοράς, υπολογίζεται ότι έχουν διαθεσιμότητα περίπου 90% μέσα σε ένα έτος. Άλλα συστήματα μπορεί να αποτυγχάνουν γύρω στις 40 φορές ετησίως, ενώ κάθε επισκευή διαρκεί περίπου δύο ώρες. Αυτά τα συστήματα έχουν διαθεσιμότητα περίπου 99% ανά έτος. Συστήματα που παρουσιάζουν ανοχές σε κάποια από τα σφάλματα ή βλάβες αποτυγχάνουν μία φορά κάθε λίγα χρόνια και επισκευάζονται μέσα σε μερικές ώρες. Αυτά έχουν διαθεσιμότητα 99,99% ανά έτος.

Τα πιο εξελιγμένα συστήματα υψηλής διαθεσιμότητας που υπάρχουν σήμερα (όπως για παράδειγμα το [18]) απαιτούν τις λιγότερες αποτυχίες και γρηγορότερη επισκευή και επιτυγχάνουν σήμερα επιδόσεις που φτάνουν διαθεσιμότητα 99,999% ανά έτος. Αυτό σημαίνει ότι ο μέσος χρόνος μη διαθεσιμότητας ανά έτος είναι περίπου 5 λεπτά.

Ο Πίνακας 2.3 από το [11] παρουσιάζει την διαθεσιμότητα διαφορετικών συστημάτων.

Τύπος Συστήματος	Περίοδος μη διαθεσιμότητας (min/year)	Διαθεσιμότητα
Χωρίς διαχείριση	50,000	90.0%
Βασική διαχείριση	5,000	99.0%
Καλή διαχείριση	500	99.9%
Με ανοχές σε βλάβες	50	99.99%
Υψηλής διαθεσιμότητας	5	99.999%
Πολύ υψηλής διαθεσιμότητας	0.5	99.9999%
Υπερ-υψηλής διαθεσιμότητας	0.05	99.99999%

Πίνακας 2.3 – Είδη διαθεσιμότητας

2.5.3. Ανοχή σε βλάβες

Μια ειδική τεχνική αύξησης της διαθεσιμότητας είναι η τεχνική Ανοχών σε Σφάλματα (Fault tolerance). Η τεχνική αυτή εμπλουτίζει τα Πληροφοριακά Συστήματα με επιπλέον πόρους που επιτρέπουν σε μια εφαρμογή ή υπηρεσία να ξεπεράσει μια βλάβη ή ένα σφάλμα χωρίς αυτή να διακοπεί [9]. Πολλές από τις λύσεις υψηλής διαθεσιμότητας που υπάρχουν στη σημερινή αγορά στην πραγματικότητα παρέχουν Ανοχή σε Σφάλματα συγκεκριμένων συστατικών στοιχείων (ή υποσυστημάτων) μιας εφαρμογής. Παράδειγμα υλοποίησης της Ανοχής σε Σφάλματα σε συγκεκριμένο υποσύστημα είναι τα αντίγραφα δίσκων (Disk mirroring), όπου δύο δίσκοι περιέχουν δύο πιστά αντίγραφα των δεδομένων. Εάν ένας από τους δίσκους παρουσιάσει βλάβη ή σφάλμα, υπάρχει το άλλο αντίγραφο των δεδομένων το οποίο είναι διαθέσιμο ακαριαία ώστε η εφαρμογή να μπορέσει να συνεχίσει χωρίς καμία διακοπή. Ακόμα και με αυτόν τον μηχανισμό, από την στιγμή που θα εμφανιστεί η βλάβη, το σύστημα (άρα και η εφαρμογή – υπηρεσία) γίνεται ευάλωτο σε βλάβες που είναι δυνατό να προκληθούν στον δίσκο, ο οποίος έχει πλέον το μόνο αντίγραφο των δεδομένων και αποτελεί μοναδικό σημείο αποτυχίας (single point of failure). Θα πρέπει λοιπόν να γίνει όσο πιο γρήγορα γίνεται ένα αντίγραφο του εναπομείναντα δίσκου. Πιθανώς όμως, αυτή η διαδικασία να έχει αρνητικό αντίκτυπο στην αποδοτικότητα του συστήματος, εφόσον απαιτούνται πόροι από το σύστημα που εξυπηρετεί και την ίδια την εφαρμογή.

Μια λύση πλήρως Ανεκτική σε Σφάλματα απαιτεί ότι όλοι οι πόροι στους οποίους βασίζεται η εφαρμογή όπως επίσης και η ίδια η εφαρμογή, δεν αποτελούν μοναδικό σημείο αποτυχίας. Αυτό προϋποθέτει την ύπαρξη ενός ανεξάρτητου υπολογιστικού συστήματος (επεξεργαστή) με αντίγραφό της αντίστοιχης προσωρινής μνήμης (RAM), τα οποία δεν θα ανήκουν στο ίδιο πολυ-επεξεργαστικό σύστημα που εξυπηρετεί την εφαρμογή. Στο ακραίο σενάριο, σύμφωνα με το οποίο σε ένα από τους επεξεργαστές ή στην μνήμη διαπιστώνεται βλάβη, το αντίγραφο της εφαρμογής συνεχίζει να εκτελείται. Άλλου τύπου βλάβες ή σφάλματα απλώς θα απαιτήσουν από την εφαρμογή να χρησιμοποιήσει εναλλακτικούς πόρους, όπως δίσκους, οδηγούς, ελεγκτές ή δικτυακές συνδέσεις. Ως αποτέλεσμα αυτής της δίδυμης αρχιτεκτονικής υλικού και διαδικασιών, οι λύσεις που υποστηρίζουν Ανοχές σε Σφάλματα είναι σημαντικά πιο ακριβές από τις απλές λύσεις υψηλής διαθεσιμότητας. Μια λύση Ανοχών σε Σφάλματα θα μπορούσε να χρησιμοποιηθεί σε μια περίπτωση όπου υπάρχει σχεδόν μηδενική ανοχή σε μη διαθεσιμότητα, όπως ένα σύστημα ελέγχου πτήσεων αεροδρομίου ή ένα σύστημα αγοραπωλησίας μετοχών σε πραγματικό χρόνο (real-time).

Για την αποτίμηση ενός συστήματος με Ανοχές σε Σφάλματα, ειδική προσοχή θα πρέπει να δοθεί στις διαδικασίες επιδιόρθωσης. Όσο ένα σύστημα είναι σε θέση να λειτουργεί κανονικά εν μέσω ενός σφάλματος, για να διασφαλιστεί ότι μια επακόλουθη βλάβη δεν θα προκαλέσει διακοπή και στη λειτουργία του συστήματος, το δυσλειτουργικό υποσύστημα θα πρέπει να αντικατασταθεί άμεσα.

2.5.4. Εξισορρόπηση φορτίου

Επιπλέον των τεχνικών Ανοχής σε Σφάλματα, υπάρχει και η τεχνική Εξισορρόπησης Φορτίου. Η τεχνική αυτή κατανέμει εργασία μεταξύ επεξεργαστών, διαδικασιών, δίσκων ή άλλων πόρων με σκοπό να επιτύχει την βέλτιστη χρησιμοποίηση των διαθέσιμων πόρων και να ελαχιστοποιήσει τον χρόνο εκτέλεσης των εφαρμογών. Παρέχει επίσης τη δυνατότητα να συνδυαστούν εξυπηρετητές (servers) στην παροχή μιας κοινής υπηρεσίας,

ακολουθώντας κοινές διαδικασίες και κανόνες [12]. Η Εξισορρόπηση Φορτίου μπορεί επίσης να χρησιμοποιηθεί και για να αυξήσει τις δυνατότητες μιας ομάδας συστημάτων πέρα από το δυναμικό ενός επιμέρους συστήματος. Συνήθως υλοποιείται με Συσκευές Εξισορρόπησης Φορτίου (Load Balancers) οι οποίοι χρησιμοποιούν ειδικές τεχνικές και μοντέλα καταμερισμού εργασιών.

Η τεχνική Εξισορρόπησης Φορτίου θεωρείται ως συμπληρωματική των τεχνικών Ανοχής σε Σφάλματα, διότι συχνά παρέχει τη δυνατότητα να διατηρούνται τις υπηρεσίες ανεπηρέαστες κατά τη διάρκεια συγκεκριμένου αριθμού αλλεπάλληλων βλαβών [13]. Επίσης, οι παραδοσιακές υλοποιήσεις των τεχνικών Ανοχής σε Σφάλματα συχνά περιλαμβάνουν πανομοιότυπο υλικό και λογισμικό συνδεδεμένο με σύνθετους τρόπους οι οποίοι είναι ανεπτυγμένοι ειδικά για τις συγκεκριμένες εφαρμογές. Το γεγονός αυτό συνεπάγεται υψηλότερο κόστος υλοποίησης και μεγαλύτερους χρόνους αδράνειας, οι οποίοι δεν καθιστούν τέτοιου είδους λύσεις ελκυστικές για βραχυπρόθεσμες επενδύσεις. Η πρόκληση είναι λοιπόν να προσφερθούν λύσεις Ανοχής σε Σφάλματα οι οποίες θα μπορούσαν να συνεισφέρουν σε όλες τις επιχειρησιακές ανάγκες – από τις καθημερινές μέχρι και μια ενδεχόμενη περίπτωση ολοκληρωτικής καταστροφής.

2.5.5. Υποδομές ανάκαμψης μετά από καταστροφή

Τόσο η πρόκληση μιας ελκυστικής επένδυσης αύξησης της διαθεσιμότητας, που αναφέρθηκε στην προηγούμενη παράγραφο, όσο και οι διάφορες σύγχρονες επιταγές κανονιστικής συμμόρφωσης [6] έχουν διαμορφώσει σχετικά πρόσφατα ένα τοπίο όπου τα σενάρια καταστροφής μιας Πληροφοριακής Υποδομής δεν θεωρούνται ως ακραία αλλά αποτελούν πλέον καθημερινή σκέψη των οργανισμών. Στην ενότητα αυτή θα εξεταστούν οι συνθήκες και οι προϋποθέσεις μιας καταστροφής όπως επίσης και οι παράμετροι που επηρεάζουν μια Πληροφοριακή Υποδομή σε μια τέτοια περίπτωση.

Καταστροφή, όπως ορίζεται από τη βιβλιογραφία [14], αποτελεί κάθε γεγονός που μπορεί να προκαλέσει τη διακοπή ή τη σοβαρή δυσλειτουργία των διαδικασιών ενός οργανισμού, πάνω από το ανώτατο ανεκτό χρονικό διάστημα. Το χρονικό διάστημα αυτό καθορίζεται από τον κάθε οργανισμό και σχετίζεται με το είδος των επιχειρηματικών δραστηριοτήτων του, τη γεωγραφική του θέση και διασπορά, την τεχνολογική του υποδομή, αλλά και τις εναλλακτικές λύσεις λειτουργίας που μπορεί να διαθέτει. Είναι επίσης δυνατό, να καθορίζεται από τρίτες οντότητες όπως Οργανισμούς – εκδότες κανονιστικών πλαισίων.

Βασιζόμενος στα πιθανά σενάρια καταστροφών αλλά και τις υποχρεώσεις που απορρέουν από το οικείο ρυθμιστικό και κανονιστικό πλαίσιο, ο κάθε οργανισμός που διαθέτει κρίσιμες υποδομές, σχεδιάζει, διαμορφώνει και συντηρεί ένα Πλάνο Επιχειρησιακής Συνέχειας (Business Continuity Plan). Το πλάνο αυτό είναι απαραίτητο λόγω του μετρήσιμου και μη κόστους που συνεπάγεται η μη λειτουργία κάθε οργανισμού αλλά και των συγκριτικών ωφελειών που μπορεί να προσφέρει έναντι των ανταγωνιστών [15]. Παραδείγματα τόσο του κόστους όσο και των ωφελειών παρουσιάζονται στον Πίνακα 2.4.

Κόστη	**Ωφέλειες**
Μη μετρήσιμα	**Μη μετρήσιμα**
Απώλεια πελατών Απώλεια μεριδίου αγοράς Αντίκτυπο σε επιχειρησιακούς εταίρους Αναγνώριση εσόδων από τρίτους Απώλειες από εκπτώσεις Απώλεια πιστοληπτικής ικανότητας	Εξασφάλιση επιβίωσης της επιχείρησης Λιγότερες ή καθόλου χαμένες πληροφορίες Μικρότερο κόστος ανάκαμψης Μικρός χρόνος μη διαθεσιμότητας Δυνατότητα αποφυγής διαφυγόντων κερδών Διατήρηση σημαντικών πελατών Δυνατότητα αποφυγής επιβολής ποινικών ρητρών Ισχυρό μήνυμα στον ανταγωνισμό Φήμη εταιρείας Προπομπός πιστοποίησης ασφάλειας Προπομπός πιστοποίησης του οικείου κλάδου
Μετρήσιμα	
Απώλεια μετρητών Τιμή μετοχής Εγγυήσεις πληρωμών Κόστη υπερωριών ανάκαμψης Ρήτρες Φορολογικές επιπτώσεις	

Πίνακας 2.4 – Παραδείγματα κόστους και ωφελειών υποδομών

Από τα παραπάνω κόστη γίνεται αντιληπτό ότι η σημασία πρόβλεψης και σχεδιασμού καταστάσεων καταστροφής είναι αρκετά σημαντική ιδιαίτερα για τους οργανισμούς που στηρίζουν την επιχειρηματική τους δραστηριότητα στα Πληροφοριακά Συστήματα και Υποδομές. Λόγω της φύσης, της πιθανής έκτασης αλλά και των επιχειρηματικών συνεπειών των καταστροφών, είθισται [14] να χρησιμοποιείται ο όρος Ανάκαμψη από Καταστροφή (Disaster Recovery) σε αντιδιαστολή με τον όρο Επαναφορά από Βλάβη (ή Σφάλμα). Είναι επίσης αποδεκτό ότι η Επανάκαμψη αφορά άμεσα τις υποδομές και έμμεσα τα συστήματα τα οποία «επαναφέρονται».

Τα τεχνολογικά μέσα, τα οποία αναπτύχθηκαν και χρησιμοποιούνται για την αντιμετώπιση καταστάσεων με τόσο σημαντικές επιπτώσεις, είναι οι Εναλλακτικές Υποδομές (Backup Infrastructures) ή αλλιώς Υποδομές Ανάκαμψης μετά από Καταστροφή (Disaster Recovery Infrastructures). Οι Εναλλακτικές Υποδομές διαφοροποιούνται από τις Παραγωγικές Υποδομές αφού, οι μεν πρώτες ενεργοποιούνται μόνο σε μια περίπτωση καταστροφής, οι δε Παραγωγικές λειτουργούν για την εξυπηρέτηση των καθημερινών αναγκών ενός οργανισμού.

Η αξία των Εναλλακτικών Υποδομών αναγνωρίζεται με τη χρήση των παραγόντων ΜΑΧΑ (RTO) και ΣΣΑ (RPO) οι οποίες αποτυπώνουν τις δυνατότητές τους σε μια περίπτωση καταστροφής. Όσο μικρότερες είναι οι τιμές που έχουν αυτοί οι δύο παράγοντες τόσο λιγότερες είναι οι επιπτώσεις για τον οργανισμό.

Θα πρέπει να σημειωθεί εδώ ότι οι Εναλλακτικές Υποδομές αναγνωρίζονται ως μια μάλλον δαπανηρή λύση [16], η οποία δικαιολογεί την ύπαρξή της μόνο σε περιπτώσεις ακραίας καταστροφής. Το γεγονός αυτό δημιουργεί διάφορες προκλήσεις που σχετίζονται με τη βελτιστοποίηση και την καλύτερη εκμετάλλευση της συγκεκριμένης επένδυσης, θέματα που θα αναπτυχθούν στα επόμενα κεφάλαια.

2.6. Σύνοψη και συμπεράσματα

Στο κεφάλαιο αυτό αναφέρθηκε η βασική θεωρία και οι έννοιες, όπως επίσης και οι μηχανισμοί και οι τεχνολογίες οι οποίες αποτελούν τη βάση της για την ανάπτυξη των επόμενων κεφαλαίων. Ο πρώτος θεματικός κύκλος ανέφερε τις βασικές έννοιες της Ασφάλειας των Πληροφοριακών Συστημάτων που θα χρησιμοποιηθούν στη συνέχεια. Ο δεύτερος θεματικός κύκλος περιέγραψε τους κανόνες λειτουργίας και διαχωρισμού των Πληροφοριακών Υποδομών και Συστημάτων. Τα Παραγωγικά Συστήματα διαχωρίστηκαν από τα υπόλοιπα Συστήματα (δηλαδή τα προ-Παραγωγικά, τα Συστήματα Λήψης Αποφάσεων και αυτά των Δοκιμών) και περιγράφηκαν τα χαρακτηριστικά των κρίσιμων υποδομών. Στον τρίτο και τελευταίο θεματικό κύκλο περιλήφθηκαν τα ειδικότερα θέματα της διαθεσιμότητας των Πληροφοριακών Υποδομών. Τα θέματα αυτά ήταν η ανοχή σε υπολογιστικά λάθη, οι φυσικές βλάβες και καταστροφές, οι τεχνολογίες εξισορρόπησης υπολογιστικού φορτίου και αύξησης της διαθεσιμότητας υπηρεσιών καθώς και οι υποδομές ανάκαμψης από καταστροφή. Τέλος αναγνωρίστηκε η ανάγκη για την εισαγωγή μιας ειδικής κατηγορίας Πληροφοριακών Υποδομών – αυτών των Πληροφοριακών Υποδομών Ανάκαμψης μετά από Καταστροφή.

2.7. Βιβλιογραφία κεφαλαίου

[1] St. R. Gordon, Judith R. Gordon, "Information Systems: A management approach", International Edition, Wiley, 1996, ISBN 0-03-016314-5, σελ.10

[2] St. R. Gordon, Judith R. Gordon, "Information Systems: A management approach", International Edition, Wiley, 1996, ISBN 0-03-016314-5, σελ.434

[3] Γ. Πάγκαλος, Ι. Μαυρίδης, "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων", Εκδόσεις Ανικούλα, 2002, ISBN 960-516-018-8, σελ.16

[4] Γ. Πάγκαλος, Ι. Μαυρίδης, "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων", Εκδόσεις Ανικούλα, 2002, ISBN 960-516-018-8, σελ.18

[5] Δημ. Γκρίτζαλης, "Ασφάλεια Κρίσιμων Υποδομών: Διεθνές Τοπίο και Προοπτικές", ανακτήθηκε: 14/6/09, http://www.adae.gr/adae/docs/imerida/Dimitrios_Gkritzalis.pdf

[6] Bank for International Settlements, "Basel II: Revised international capital framework", ανακτήθηκε: 14/6/09, http://www.bis.org/publ/bcbsca.htm

[7] M. Andress, "Surviving Security, How to Integrate People, Process and Technology", Sams, 2001, ISBN 978-0672324789, σελ.30.

[8] H. F. Tipton και M. Krause, "Information Security Management Handbook", Auerbach Publications, 2007, ISBN 978-1420067088, σελ.277

[9] J. Wright και Ann Katan, "High Availability: A perspective", Gartner Research, 2003, ID Number: DPRO-90193

[10] Αγγλική Ορολογία - Τμήμα Φιλολογίας, Πανεπιστήμιο Πατρών, ανακτήθηκε: 14/6/09, http://users.uoi.gr/gjxydo/lexicon/byletter/lookup.php?text=R

[11] Στ. Βολογιαννίδης, «Διαθεσιμότητα Υπολογιστικών Συστημάτων», ανακτήθηκε: 14/6/09, http://www.teiser.gr/icd/staff/vologian/files/Projects_BP/Διαθεσιμότητα Υπολογιστικών Συστημάτων.ppt

[12] W. Tarreau, «Making applications scalable with Load Balancing», ανακτήθηκε: 14/6/09, http://1wt.eu/articles/2006_lb/index.html

[13] «Highly Available Embedded Computer Platforms Become Reality», White paper, International Engineering Consortium, ανακτήθηκε: 14/6/09, http://www.iec.org/online/tutorials/ha_embed/topic01.html

[14] "Disaster Recovery Planning – Process & Options", Comprehensive Consulting Solutions, Inc.2001, ανακτήθηκε: 14/6/09, www.comp-soln.com/DRP2_whitepaper.pdf

[15] D. Honour, "The business benefits of business continuity", 2007, ανακτήθηκε: 14/6/09, http://www.continuitycentral.com/feature0427.htm

[16] P. Fallara, "Disaster recovery planning", Potentials, IEEE, 2003, Volume: 22, Issue: 5, ISSN: 0278-6648

[17] "Achieving High Availability on Linux for System z with Linux-HA", IBM Redbook, ανακτήθηκε: 14/6/09, http://www.redbooks.ibm.com/redpieces/abstracts/sg247711.html

3. Επισκόπηση σχετικών προσεγγίσεων

3.1. Εισαγωγή

Το κεφάλαιο αυτό περιλαμβάνει μια παρουσίαση και αξιολόγηση των προσεγγίσεων που είναι σχετικές με το αντικείμενο της έρευνας. Υπάρχουν δύο βασικά θέματα τα οποία αποτέλεσαν και το ερευνητικό ερέθισμα της διατριβής αυτής. Αυτά είναι οι μεθοδολογίες μετασχηματισμού των πληροφοριακών υποδομών και οι μεθοδολογίες μέτρησης της ασφάλειας.

Στην πρώτη θεματική ενότητα του κεφαλαίου, οι μεθοδολογίες μετασχηματισμού των πληροφοριακών υποδομών που εξετάζονται είναι η Διαχείριση Αλλαγών (Change Management) και η Βιβλιοθήκη Υποδομής Τεχνολογίας Πληροφοριών (Information Technology Infrastructure Library / ITIL). Στις σχετικές παραγράφους αναλύεται τόσο το θεωρητικό υπόβαθρό τους όσο και το είδος της σχέσης τους με τη συγκεκριμένη έρευνα, το οποίο αποτέλεσε και κριτήριο επιλογής τους.

Στη δεύτερη θεματική ενότητα εξετάζονται μια σειρά από μεθοδολογίες μέτρησης της ασφάλειας. Οι βασικότερες μεθοδολογίες παρουσιάζονται ταξινομημένες σε πέντε βασικές κατηγορίες και αξιολογούνται με κριτικό και συνθετικό τρόπο. Εισάγονται επίσης δύο νέες κατηγορίες, οι οποίες περιλαμβάνουν νεότερες και πιο σύνθετες μεθοδολογίες. Η αξιολόγηση του συνόλου των μεθοδολογιών αποτελεί και το εφαλτήριο για τη βελτίωση και προσαρμογή των μεθοδολογιών στις ανάγκες της συγκεκριμένης διατριβής, αναγνωρίζοντας τα θετικά και τα αρνητικά στοιχεία κάθε κατηγορίας.

3.2. Μεθοδολογίες μετασχηματισμού πληροφοριακών υποδομών

Η παράγραφος αυτή παρουσιάζει τις διαφορετικές προσεγγίσεις στα θέματα μετασχηματισμού των πληροφοριακών υποδομών, με έμφαση στη θεωρία Διαχείρισης Αλλαγών αλλά και της μεθοδολογίας ITIL. Οι προσεγγίσεις αυτές εξετάζονται κριτικά ως προς τα πλεονεκτήματά τους αλλά και ως προς τους πιθανούς περιορισμούς τους.

3.2.1. Θεωρία διαχείρισης αλλαγών

«Η θεωρία της διαχείρισης αλλαγών περιγράφει μια δομημένη προσέγγιση μετασχηματισμού ατόμων, ομάδων, οργανισμών και κοινοτήτων οι οποίες μετατρέπουν το στόχο σε μια άλλη επιθυμητή κατάσταση» [1]. Αυτή είναι ακριβώς η περίπτωση, με την οποία έρχεται κανείς αντιμέτωπος όταν επιθυμεί να μετατρέψει μια πληροφοριακή υποδομή σε μια άλλη και ως εκ τούτου θεωρείται πολύ χρήσιμο να παρουσιαστούν τα σημεία εκείνα τα οποία είναι κατάλληλα και εφαρμόσιμα σε τέτοιου είδους καταστάσεις. Υπάρχουν πολλαπλές προσεγγίσεις της θεωρίας της διαχείρισης αλλαγών. Οι πιο δημοφιλείς παρουσιάζονται από τους Martin [2] και Mullins [3]. Το αντικείμενό τους εφαρμόζεται σε πολλά πεδία περιλαμβανομένου και του πεδίου της Πληροφορικής.

Η αλλαγή όπως αναφέρεται τόσο στις συγκεκριμένες πηγές αλλά και στην πλειοψηφία της σχετικής βιβλιογραφίας, αποτελεί μέσο εξέλιξης αλλά και αιτία προβλημάτων. Όπως τονίζεται στο [4], η πρώτη ερώτηση που κάνει κανείς όταν προσπαθεί να λύσει ένα τεχνικό ή διαδικαστικό πρόβλημα είναι να ρωτήσει «τι έχει αλλάξει;». Έχοντας υλοποιήσει μια μεθοδολογία διαχείρισης αλλαγών, κάθε τέτοια ερώτηση είναι πολύ ευκολότερο να απαντηθεί.

Όπως αναφέρθηκε και στον σχετικό ορισμό, η διαχείριση αλλαγών απαιτεί συνδυασμό ανθρώπινων πόρων, τεχνικών μέσων (υλικό και λογισμικό) αλλά και διαδικασιών. Όταν οι αλλαγές πραγματοποιούνται με έναν τυποποιημένο τρόπο, το αποτέλεσμα είναι πολλαπλά θετικό. Επιτυγχάνεται αύξηση της αποδοτικότητας και της παραγωγικότητας του προσωπικού καθώς και μείωση της μη διαθεσιμότητας των σχετιζόμενων συστημάτων και των οικείων υπηρεσιών τους. Κατ' επέκταση υπάρχει και μείωση του Μέσου Χρόνου Επιδιόρθωσης (ΜΧΕ / Mean Time To Repair – MTTR). Η διαχείριση των αλλαγών μπορεί να επηρεάσει θετικά τον τομέα της ασφάλειας, παρέχοντας αξιόπιστα στοιχεία ελέγχου καθώς και αυξημένο έλεγχο εξειδικευμένων αλλαγών, τα οποία και μπορούν να συνεισφέρουν σε μειωμένα κόστη για την Πληροφορική.

Η διαχείριση των αλλαγών είναι ζωτικής σημασίας για τη συντήρηση συστημάτων υψηλής διαθεσιμότητας, τα οποία πιθανώς να πρέπει να ικανοποιούν συγκεκριμένα επίπεδα διαθεσιμότητας των υπηρεσιών τους. Με βάση το σκεπτικό αυτό, οι βέλτιστες πρακτικές που χρησιμοποιούνται από τις εταιρίες εφαρμόζουν όλες τις αλλαγές τους κατά τις φάσεις της ανάπτυξης και των δοκιμών, ούτως ώστε να πραγματοποιούνται αλλαγές σε παραγωγικά συστήματα μόνο σε σπάνιες καταστάσεις έκτακτης ανάγκης. Ιδανικά, οι διαδικασίες των αλλαγών επισημοποιούνται και ενσωματώνουν τους τομείς της ασφάλειας, των δοκιμών και της τεκμηρίωσης. Οι οργανισμοί θα πρέπει ακόμα να εξασφαλίζουν την ύπαρξη των κατάλληλων προληπτικών, διαγνωστικών και επιδιορθωτικών μηχανισμών, ώστε να ικανοποιούνται και οι σχετικές απαιτήσεις νομικών και κανονιστικών πλαισίων, όπως το Sarbanes-Oxley (SOX).

Ο μελετητικός οίκος Forrester αναφέρει χαρακτηριστικά στο [5] ότι «Στον τομέα της Πληροφορικής, η αλλαγή είναι μια μηχανή προόδου, αλλά και μια πηγή αφανισμού... Παρόλο που οι διαδικασίες αλλαγών του λογισμικού είναι μια σχετικά ώριμη διαδικασία, πολλοί οργανισμοί υλοποιούν τις αλλαγές χειροκίνητα, επαφιόμενοι κυρίως στη γνώση και την εμπειρία του τεχνικού προσωπικού. Αυτή η εξειδικευμένη διαδικασία προσεγγίζει τα όριά της, με το σημερινό σύνθετο περιβάλλον, όπου οι κίνδυνοι που κληρονομούνται με τις αλλαγές πολλαπλασιάζονται».

Η αυτοματοποίηση της διαχείρισης των αλλαγών συνεπάγεται και την εφαρμογή μιας αποτελεσματικής διαδικασίας διαχείρισης αλλαγών η οποία συνοψίζεται στα ακόλουθα έξι βήματα:

1. Υποβολή μιας αίτησης για αλλαγή.
2. Αξιολόγηση της αίτησης υπό το πρίσμα των αρνητικών αντίκτυπων και των ωφελειών της αλλαγής. Υπολογισμός των απαιτούμενων πόρων.
3. Αποδοχή της αλλαγής και εξασφάλιση των απαιτούμενων πόρων.

4. Ανάπτυξη και δοκιμή της αλλαγής στο πλαίσιο ενός προ-παραγωγικού περιβάλλοντος.
5. Υλοποίηση της αλλαγής στο Παραγωγικό περιβάλλον
6. Επαλήθευση και αποδοχή της αλλαγής από κάποιον εκτός της ομάδας υλοποίησης του οργανισμού.

Το τελευταίο βήμα (Βήμα 6) είναι το κρίσιμο βήμα το οποίο οι περισσότεροι οργανισμοί συνήθως παραβλέπουν. Για την αποδοτικότερη διαχείριση των αλλαγών, απαιτείται η ολοκλήρωση του συνόλου των παραπάνω βημάτων. Αυτό μπορεί να επιτευχθεί με τη διεξαγωγή μιας τελικής επαλήθευσης, για την ορθότητα της υλοποίησης της αλλαγής που απαιτήθηκε, στο σύνολο των εμπλεκομένων συστημάτων. Για λόγους ασφάλειας μπορεί να ελεγχθεί και κατά πόσο έχουν παραβιαστεί και οι μηχανισμοί ελέγχου των αλλαγών. Χωρίς αυτό το βήμα, η διαδικασία των αλλαγών παραμένει ανοικτή, και είναι αδύνατον να αναγνωριστεί η διαφορά μεταξύ εξουσιοδοτημένων, πετυχημένων αλλαγών και μη εξουσιοδοτημένων (ή μη πετυχημένων) αλλαγών.

Με βάση τα αποτελέσματα που παρουσιάζονται στις παραπάνω μελέτες γίνεται σαφές ότι η μείωση των διακοπών λειτουργίας των υπηρεσιών από ανθρώπινα λάθη με τη χρήση αυτοματοποιημένων διαδικασιών συνεπάγεται μειώσεις στα λειτουργικά έξοδα καθώς και μεγαλύτερη αποδοτικότητα στη λειτουργία της επιχείρησης. Η σημασία αυτού του γεγονότος γίνεται ευκολότερα αντιληπτή εάν αναλογιστεί κανείς ότι τα στοιχεία από το [5] έδειξαν ότι 80% των προϋπολογισμών πληροφορικής των οργανισμών χρησιμοποιείται για τη συντήρηση της τρέχουσας κατάστασης. Με την υλοποίηση εφαρμόσιμων διαδικασιών διαχείρισης των αλλαγών, οι οργανισμοί επιτυγχάνουν τον καλύτερο έλεγχο των Πληροφοριακών Υποδομών άρα και των εξόδων τους. Επιπλέον, με τη γνώση των παραμέτρων της αλλαγής, ο οργανισμός ολοκληρώνει τη διαδικασία των αλλαγών βελτιώνοντας τη διαθεσιμότητα, τη δυνατότητα ελέγχου, ενώ μειώνει τα συνολικά λειτουργικά έξοδα.

Η χρήση της θεωρίας διαχείρισης αλλαγών βρίσκει εφαρμογή στο κεφάλαιο 5 της διατριβής και συγκεκριμένα ως μέθοδος βελτιστοποίησης των Κρίσιμων Πληροφοριακών Υποδομών Ασφάλειας.

3.2.2. Βιβλιοθήκη Υποδομής Τεχνολογίας Πληροφοριών

Το Information Technology Infrastructure Library, το οποίο όπως έχει ήδη αναφερθεί μπορεί να αποδοθεί στα ελληνικά ως Βιβλιοθήκη Υποδομής Τεχνολογίας Πληροφοριών, είναι ευρύτερα γνωστό με το ακρωνύμιο ITIL [6]. Περιγράφεται αναλυτικά σε μια σειρά βιβλίων και εκπαιδευτικών οδηγών τα οποία σκιαγραφούν και εξηγούν, κυρίως από τη διαχειριστική οπτική, τις πρακτικές οι οποίες θεωρούνται οι πιο ευεργετικές για τις υπηρεσίες πληροφορικής. Ο στόχος του ITIL είναι η υιοθέτηση και εφαρμογή υψηλών προτύπων για την αύξηση της αξίας της Πληροφορικής εντός ενός οργανισμού αλλά και την παροχή των καθημερινών εργασιών και υπηρεσιών Πληροφορικής με οικονομικά συμφέροντα τρόπο. Οι διαδικασίες που περιγράφονται από το ITIL είναι ανεξάρτητες από τους προμηθευτές και έχουν κυρίως διδακτικό χαρακτήρα για τα διευθυντικά στελέχη των οργανισμών, περιλαμβάνοντας τις βέλτιστες πρακτικές τόσο για τις καθημερινές εργασίες της πληροφορικής όσο και για τις εργασίες ανάπτυξης νέων υπηρεσιών πληροφορικής.

Θα πρέπει να σημειωθεί ότι το ακρωνύμιο ITIL είναι κατοχυρωμένο, όπως και το σχετικό εκπαιδευτικό υλικό το οποίο υπόκειται στους νόμους πνευματικής ιδιοκτησίας.

Το ITIL έχει μια μακρά ιστορία ανάπτυξης και, ενώ πολλοί επαγγελματίες της πληροφορικής πιστεύουν ότι το ITIL εξελίχθηκε από τα «yellow books» που αποτελούσαν πηγή βέλτιστων πρακτικών και οδηγιών της IBM τη δεκαετία του 1980, έγινε επίσημο πλαίσιο – βιβλιοθήκη των βέλτιστων πρακτικών της Πληροφορικής στα μέσα της δεκαετίας του 1990. Η τελευταία (τρίτη) έκδοση του ITIL έχει γίνει διαθέσιμη από το 2007, με διαρκώς αυξανόμενη αποδοχή από τους επαγγελματίες της Πληροφορικής. Περιλαμβάνει πέντε βασικά

κείμενα: τη Στρατηγική των Υπηρεσιών (Service Strategy), το Σχεδιασμό των Υπηρεσιών (Service Design), τη Μετάπτωση των Υπηρεσιών (Service Transition), τη Λειτουργία των Υπηρεσιών (Service Operation) και τη Συνεχή Βελτίωση των Υπηρεσιών (Continual Service Improvement).

Η πρώτη έκδοση του ITIL περιλάμβανε μια σειρά από βιβλία τα οποία κάλυπταν συγκεκριμένα θέματα της Διαχείρισης Υπηρεσιών Πληροφορικής. Όμως, μετά την πρώτη έκδοση, τα βιβλία της βιβλιοθήκης αυξήθηκαν σε πάνω από τριάντα τόμους. Ο αριθμός αυτός ήταν απαγορευτικός για να διαβαστεί, να αφομοιωθεί και ακόμα περισσότερο να αποκτηθεί, λόγω του κόστους του και έτσι η δεύτερη έκδοση συμπυκνώθηκε.

Η δεύτερη έκδοση του ITIL διατίθεντο σε ομάδες βιβλίων τα οποία είχαν σχέση με οδηγίες διαδικασιών και περιλάμβαναν διαφορετικές οπτικές της Πληροφορικής, συμπεριλαμβανομένων και των εφαρμογών, των υπηρεσιών και της διαχείρισης των υποδομών. Θα πρέπει να σημειωθεί ότι η πιο δημοφιλής ομάδα βιβλίων περιλάμβανε τις υπηρεσίες και ειδικότερα την Υποστήριξη Υπηρεσιών (Service Support) και την Παροχή Υπηρεσιών (Service Delivery).

Υπάρχουν διάφορα πλεονεκτήματα για τους οργανισμούς με τη χρήση του ITIL για πολλές από τις ανάγκες που σχετίζονται με την Πληροφορική. Ένα κύριο πλεονέκτημα είναι ότι μέσω των οδηγιών και των βέλτιστων πρακτικών τα οποία διδάσκονται, ο κάθε οργανισμός μπορεί να εξοικονομήσει ένα σημαντικό ποσό από τον προϋπολογισμό του, εφόσον υλοποιήσει μέρος ή ολόκληρο το ITIL.

Ένα άλλο πλεονέκτημα του ITIL είναι ότι μπορεί να βοηθήσει τις διευθύνσεις πληροφορικής να οργανωθούν με ένα ομοιόμορφο τρόπο που θα τις φέρει πιο κοντά στους επιχειρηματικούς στόχους κάθε οργανισμού. Σε κάθε περίπτωση το ITIL έχει δοκιμαστεί σε οργανισμούς για πάνω από μία δεκαετία και έχει αποδειχτεί ότι μπορεί να είναι ωφέλιμο και αποδοτικό. [6]

Παρόλο που τα πλεονεκτήματα του ITIL είναι σαφώς πιο πολλά από τα μειονεκτήματά του, κρίνεται χρήσιμο να αναφερθούν και κάποια από τα μειονεκτήματά του. Ένα βασικό μειονέκτημά του, είναι το γεγονός ότι το ITIL δεν αποτελεί μια ολοκληρωμένη λύση διαχείρισης Πληροφοριακών Υποδομών και Υπηρεσιών. Υπάρχουν τομείς τους οποίους καλύπτει με άριστο τρόπο, υπάρχουν όμως και τομείς που δεν καλύπτονται εξίσου καλά.

Το συγκεκριμένο χαρακτηριστικό όμως δεν αποτελεί ιδιαίτερο πρόβλημα για την εφαρμογή κάποιων από τις βέλτιστες πρακτικές που προτείνει το ITIL, λόγω της επιλεκτικής εφαρμογής κάποιων από τις προτεινόμενες πρακτικές. Το ITIL βρίσκει εφαρμογή στο κεφάλαιο 5 της διατριβής και συγκεκριμένα ως μέθοδος βελτιστοποίησης των Κρίσιμων Πληροφοριακών Υποδομών Ασφάλειας, με την υιοθέτηση και τον συνδυασμό μεθοδολογιών, εργαλείων, μετρικών (ή αλλιώς μετρήσιμων μεγεθών) και ρόλων. Η υιοθέτηση των μετρικών του ITIL εξυπηρετεί τις ανάγκες της μεθοδολογίας μετασχηματισμού που θα αναφερθεί στο κεφάλαιο 5, παρέχοντας ένα πλαίσιο που είναι οικείο σε κάθε γνώστη του ITIL και κυρίως του τύπου των μετρικών του.

3.3. Μεθοδολογίες μέτρησης της ασφάλειας

3.3.1. Γενικά

Οι περισσότεροι οργανισμοί θεωρούν την Ασφάλεια «πρώτη προτεραιότητα» για τα διευθυντικά στελέχη, ενώ μελέτες όπως η [7] αναδεικνύουν το γεγονός ότι υψηλόβαθμα στελέχη αξιολογούν τη σημαντικότητα της ασφάλειας με 7.5 στα 10. Τα τελευταία χρόνια, ο νόμος των Sarbanes-Oxley αλλά και η εξάπλωση του λειτουργικού συστήματος των Windows προκάλεσαν σημαντική αύξηση των σχετικών δαπανών. Σύμφωνα με στοιχεία του [8], το 2002 ο μέσος προϋπολογισμός των μέσων αμερικάνικων εταιριών για την ασφάλεια ήταν 1,1 εκ. δολάρια. Από τότε, οι προϋπολογισμοί αυξήθηκαν με μέσο ετήσιο ρυθμό αύξησης στο 20% περίπου, αλλά τα περισσότερα χρήματα ξοδεύτηκαν σε προϊόντα και όχι σε διαδικασίες, γεγονός το οποίο αποτελεί λανθασμένη

τακτική μια που η ασφάλεια είναι διαδικασία και όχι προϊόν, σύμφωνα με τον Schneier στο [9]. Η τακτική αυτή οφείλεται στο γεγονός ότι συνήθως οι ερωτήσεις που αφορούν την ασφάλεια, αν και φαινομενικά απλές, δεν είναι καθόλου εύκολο να απαντηθούν. Για παράδειγμα οι παρακάτω ερωτήσεις θα μπορούσαν να αποτελούν εύκολη εργασία εάν απευθυνόντουσαν σε ένα τμήμα πωλήσεων:

- Είναι η ασφάλεια του οργανισμού καλύτερη φέτος;
- Ποιο είναι το κέρδος ή η αξία που κερδίζει ο οργανισμός από τις επενδύσεις στην ασφάλεια;
- Πώς μπορεί ένας οργανισμός να συγκριθεί με έναν άλλο σε ό,τι αφορά την ασφάλεια;

Δεν είναι όμως το ίδιο εύκολο να απαντηθούν όταν απευθύνονται σε κάποιον υπεύθυνο ασφάλειας, διότι η ασφάλεια είναι μια αφηρημένη έννοια, η οποία δεν είναι εύκολο να ποσοτικοποιηθεί. Έτσι, οι απαντήσεις πολλών στελεχών πληροφορικής στα συγκεκριμένα ερωτήματα είναι συνήθως νεφελώδεις.

Οι επιχειρηματικές πιέσεις οδηγούν αναπόφευκτα τους οργανισμούς στην υιοθέτηση καλύτερων μεθόδων για τη μέτρηση της αποτελεσματικότητας των έργων ασφάλειάς τους. Ταυτόχρονα, η έλλειψη επικοινωνίας και ανταλλαγής των σχετικών πληροφοριών αποτρέπει την ισότιμη και ελεύθερη συζήτηση, η οποία θα μπορούσε να διαμορφώσει ένα τυποποιημένο πλαίσιο μεθόδων για τα θέματα της ασφάλειας.

Στον τομέα της μέτρησης της ασφάλειας, οι νέες καινοτόμες εφευρέσεις είναι πολύ περιορισμένες λόγω της αβεβαιότητας και της έλλειψης ενός ουσιαστικού και μετρήσιμου μεγέθους της ασφάλειας. Κατά την παράδοση, όμως, όπου τα μετρήσιμα στοιχεία είναι περιορισμένα ή δεν είναι διαθέσιμα, η συνήθης πρακτική είναι η ανάπτυξη μοντέλων από άλλα ερευνητικά πεδία και η γνωμοδότηση των ειδικών ασφάλειας για τη συμπλήρωση των δεδομένων. Κατά συνέπεια, κάποιο καλώς πληροφορημένο μοντέλο θα μπορούσε να

βοηθήσει στον καθορισμό κάποιων καλών μετρικών, ή τουλάχιστον στον καθορισμό των χαρακτηριστικών αυτών.

Η μοντελοποίηση συνδέεται με τη μέτρηση. Στον κόσμο της ασφάλειας Πληροφοριακών Συστημάτων, οι περισσότεροι παρατηρητές που μιλάνε για «μετρικές ασφάλειας» γενικά τις αντιμετωπίζουν από την οπτική της μοντελοποίησης των απειλών, του κινδύνου και των ζημιών. Λιγότεροι ενδιαφέρονται για την οπτική της μοντελοποίησης και προτιμούν απλώς να μετρήσουν «κάτι». Με τον κίνδυνο της υπερ-απλούστευσης, οι οπαδοί της μοντελοποίησης ασχολούνται κυρίως με ισότητες κινδύνου, προσδοκίες ζημιών, οικονομικά κίνητρα και τα αίτια του κινδύνου. Αντίθετα, οι οπαδοί των μετρήσεων ασχολούνται με εμπειρικά δεδομένα, συσχετισμούς, διαμοιρασμό δεδομένων και την αιτιότητα. Αυτές οι δύο γενικές προσεγγίσεις συγγενεύουν με την παλαιότερη διαίρεση σε θεωρητικούς και εμπειρικούς επιστήμονες.

Στην περίπτωση της ασφάλειας η αλήθεια μπορεί να αποκαλυφθεί με τον συνδυασμό των δύο. Ο Leach υποστηρίζει κάτι τέτοιο στο [10] ισχυριζόμενος ότι υπάρχουν δύο σημεία που θα πρέπει κανείς να λάβει υπόψη του. Αρχικά θα πρέπει να μετρηθεί η απειλή και όχι μόνο τα περιστατικά που αναγνωρίζονται και οι έλεγχοι που εφαρμόζονται, ώστε να υπάρχει και η γνώση των αιτίων εμφάνισης ή μη εμφάνισης των περιστατικών. Δευτερευόντως, απαιτείται ένα μοντέλο για την καλύτερη προβολή και πρόβλεψη των μελλοντικών περιστατικών.

Όπως αναφέρεται και από τον Jaquith [11], ένα καλό μοντέλο μπορεί να τροφοδοτεί τους οργανισμούς με την κατάλληλη αιτιολογία για τη μέτρηση. Παράλληλα, κάποιες μετρήσεις μπορούν να υποδείξουν έμμεσα ποια μοντέλα θα πρέπει να χρησιμοποιηθούν στην ασφάλεια. Είναι επίσης εφικτό να ανανεώνονται και να διορθώνονται τα μοντέλα με κάθε νέα ροή δεδομένων, αντικαθιστώντας ίσως στο μέλλον τελείως την ανάγκη για γνωμοδότηση των ειδικών ασφάλειας με αντικειμενικές μετρήσεις. Μια τέτοια προσέγγιση

επιχειρείται και στο πλαίσιο της διατριβής, βασιζόμενη και εμπνεόμενη από τις ήδη διαθέσιμες μεθόδους για τη μέτρηση της ασφάλειας.

Είναι λοιπόν πολύ χρήσιμο να μελετηθούν και να αξιολογηθούν οι υπάρχουσες προσεγγίσεις για την κατηγοριοποίηση των μεθόδων που ασχολούνται με την Μέτρηση και Μοντελοποίηση της Ασφάλειας, ώστε να μπορούν αυτές να συντεθούν σε μια σειρά νέων μετρικών ή ενός μοντέλου μέτρησης της ασφάλειας. Η βιβλιογραφία που σχετίζεται με τις μεθοδολογίες μέτρησης της ασφάλειας περιλαμβάνει μια σειρά από προσεγγίσεις για τη μέτρηση της ασφάλειας αλλά και την κατηγοριοποίηση των μεθόδων αυτών. Ο τρόπος που επιλέχθηκε για την κατηγοριοποίηση και τον διαχωρισμό των διαφορετικών μεθόδων αναδεικνύει και μια άλλη σημαντική συνεισφορά της διατριβής – αυτή της ανάπτυξης μια συστηματικής κατηγοριοποίησης των μεθόδων Μέτρησης και Μοντελοποίησης της Ασφάλειας. Οι κατηγορίες συνοψίζονται στον Πίνακα 3.5 και παρουσιάζονται στις παρακάτω ενότητες:

Κατηγορίες μεθόδων Μέτρησης και Μοντελοποίησης της Ασφάλειας
Ανάλυση Ευπάθειας
Δοκιμές Διείσδυσης
Σύγκριση με Υλοποιήσεις Αναφοράς
Βέλτιστες Πρακτικές
Διαχείριση Κινδύνων
Συνεκτίμηση των δομικών στοιχείων της ασφάλειας
Συνεκτίμηση παραγόντων έμμεσα σχετιζόμενων με την ασφάλεια

Πίνακας 3.5 – Κατηγορίες μεθόδων μέτρησης ασφάλειας

3.3.2. Ανάλυση Ευπάθειας

Η Ανάλυση Ευπάθειας (Vulnerability analysis) είναι μια διαδικασία η οποία οριοθετεί, προσδιορίζει και ταξινομεί τα κενά ασφάλειας (ευπάθειες) σε ένα υπολογιστικό σύστημα, δίκτυο ή πληροφορική υποδομή. Επιπρόσθετα, μπορεί να προβλέψει την αποτελεσματικότητα των προτεινόμενων αντίμετρων και να αξιολογήσει την πραγματική αποτελεσματικότητα των αντίμετρων αφού αυτά έχουν υλοποιηθεί.

Οι λύσεις που είναι βασισμένες στην Ανάλυση Ευπάθειας όπως οι [12], [13] και [14] συνδέουν το επίπεδο της ασφάλειας ενός πληροφοριακού συστήματος με τον αριθμό των ευπαθειών που σχετίζονται με το δίκτυο του.

Ο McClure στο [15] ορίζει τους κινδύνους ως μια συνάρτηση των απειλών (threats), ευπαθειών (vulnerabilities) και εκθέσεων (exposures) έναντι των αντιμέτρων (countermeasures) που εφαρμόζονται. Επιχειρεί να διαχωρίσει τους κινδύνους σε τρία μέρη, ανάλογα με τη μέθοδο που μπορεί να χρησιμοποιήσει ένας hacker για να εισβάλει σε ένα δίκτυο. Στο πρώτο μέρος οι κίνδυνοι οφείλονται στις αδυναμίες των λειτουργικών συστημάτων ή στην λανθασμένη ρύθμιση τους. Στο δεύτερο μέρος οι κίνδυνοι οφείλονται στη φύση και στα χαρακτηριστικά των δικτυακών στοιχείων ενός συστήματος. Εδώ περιλαμβάνονται τα Firewalls, Switches, Routers αλλά και τα πρωτόκολλα IP, TCP, UDP, OSFP, 802.11. Τέλος, στο τρίτο μέρος, εξετάζονται οι κίνδυνοι που οφείλονται στο λογισμικό, όπως τα Back Doors, Trojans, Viruses αλλά και στις web-based εφαρμογές.

Στην ίδια πηγή αλλά και από άλλους όπως στο [16] γίνεται επίσης ο διαχωρισμός σε τυχαίες επιθέσεις και σε στοχοθετημένες επιθέσεις. Οι τυχαίες επιθέσεις περιλαμβάνουν ιούς, Port Scans, DoS και κατά λάθος επιθέσεις. Οι στοχευμένες επιθέσεις περιλαμβάνουν DDoS, κλοπή πληροφοριών, εισαγωγή κακόβουλου κώδικα, παράνομες πράξεις από έμπιστα πρόσωπα (υπαλλήλους, συμβούλους, συνεταίρους κ.α.), αλλοίωση του περιεχομένου του Web Server και κακόβουλες πράξεις από δυσαρεστημένα πρόσωπα.

Υπάρχει πληθώρα τυποποιημένων εργαλείων τα οποία πραγματοποιούν ανάλυση των ευπαθειών πληροφοριακών συστημάτων αλλά και δικτύων. Αυτά μπορούν να βασίζονται σε κάποιο λογισμικό ή σε εξειδικευμένες συσκευές.

Δυστυχώς οι συσκευές Ανάλυσης Ευπάθειας δεν μπορούν να χρησιμοποιηθούν για να μετρήσουν την ασφάλεια μιας ολόκληρης οργάνωσης επειδή δεν

λαμβάνουν υπόψη πολλούς παράγοντες όπως οι λειτουργικές αδυναμίες και η ασφάλεια προσωπικού. Επιπλέον, τα αποτελέσματα δεν συσχετίζονται καθόλου με τον αριθμό πραγματικών γεγονότων ασφάλειας.

3.3.3. Δοκιμές Διείσδυσης

Μια Δοκιμή Διείσδυσης αποτελεί συνήθως μια μη τυποποιημένη διαδικασία η οποία οργανώνεται με μη περιοδικό τρόπο για την ανίχνευση κενών ασφάλειας σε ένα συγκεκριμένο πληροφοριακό σύστημα ή μια ομάδα συστημάτων. Οι λύσεις που είναι βασισμένες σε Δοκιμές Διείσδυσης (Penetration Testing) όπως οι [17] και [18] ακολουθούν τα ακριβή βήματα των πραγματικών επιτιθεμένων χωρίς όμως να προκαλούν πραγματική ζημία στα πληροφορικά συστήματα. Εντούτοις τα αποτελέσματα, όπως αυτά παρουσιάζονται τελικά, είναι περισσότερο υποκειμενικές εκτιμήσεις από αντικειμενικές μετρήσεις. Επιπλέον, εστιάζουν πάντα στις σχετικές με την τεχνολογία πτυχές της οργάνωσης και παραμελούν άλλους σοβαρούς παράγοντες όπως η λειτουργική και φυσική ασφάλεια. Το αποτέλεσμα είναι η καταγραφή και ο προσδιορισμός των κενών ασφάλειας που υπάρχουν την συγκεκριμένη χρονική στιγμή και δεν εγγυώνται την εγκυρότητά τους για καμιά άλλη χρονική στιγμή.

3.3.4. Σύγκριση με Υλοποιήσεις Αναφοράς

Οι λύσεις που είναι βασισμένες στη Σύγκριση με Υλοποιήσεις Αναφοράς (Baselines) όπως η [19] περιέχουν τους τυποποιημένους ελέγχους ασφαλείας, οι οποίοι ισχύουν στη μεγάλη πλειοψηφία των πληροφοριακών συστημάτων που παρέχουν μια βασική ασφάλεια. Η βάση για την απόφαση εάν η οργάνωση ή η συγκεκριμένη υπηρεσία ικανοποιεί τις απαιτήσεις ασφάλειας είναι βασισμένη στην προσωπική κρίση του ελεγκτή. Τα κύρια ερωτήματα σχετικά με αυτό το είδος προσέγγισης είναι ότι είναι πολύ υποκειμενικό και τείνει να αλλάξει κάθε φορά που αλλάζει ο ελεγκτής. Και πάλι η έκβαση είναι περισσότερο μια εκτίμηση από μια κατάλληλη μέτρηση.

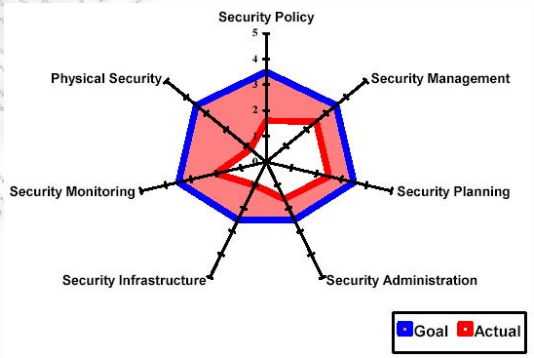
3.3.5. Βέλτιστες Πρακτικές

Οι λύσεις που είναι βασισμένες στις Βέλτιστες Πρακτικές (Best-practice) όπως είναι οι ISO/IEC 17799 [20], BS 7799 [21], [22] και NIST SP 800-33 [23] αναφέρονται σε διάφορες προτάσεις για τα αντίμετρα και τους κατάλληλους ελέγχους για να βελτιώσουν την ασφάλεια των πληροφοριών μιας οργάνωσης. Αν και αυτές οι προσεγγίσεις είναι αρκετά λεπτομερείς και επεξηγηματικές, είναι πιο χρήσιμες κατά την ανάπτυξη των νέων υποδομών και των υπηρεσιών παρά για την αξιολόγηση των πληροφοριακών υποδομών που ήδη βρίσκονται σε λειτουργία. Έως τώρα οι πτυχές του προσδιορισμού της ποσότητας και της μέτρησης της ασφάλειας δεν αποτελούσαν προτεραιότητα στην εφαρμογή των συγκεκριμένων μεθόδων.

Η νεότερη προσέγγιση που βασίζεται σε βέλτιστες πρακτικές είναι αυτή του ITIL v3 που εισαγάγει νέες μεθοδολογίες διαχείρισης της ασφάλεια και για το οποίο υπάρχει ειδική μνεία στο κεφάλαιο 5.

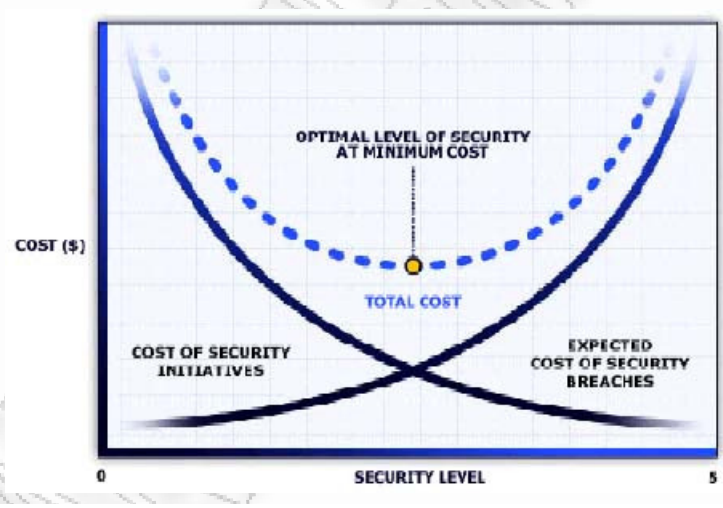
3.3.6. Διαχείριση Κινδύνων

Οι λύσεις που είναι βασισμένες στη Διαχείριση Ρίσκου – Κινδύνου (Risk Management) όπως η [24] αξιολογούν την ασφάλεια με την περιγραφή, την ανάλυση και την αξιολόγηση των συγκεκριμένων σεναρίων. Επιπλέον, δεδομένου ότι η εκτίμηση του κινδύνου είναι βασισμένη στην προσωπική κρίση του ελεγκτή, τέτοιες λύσεις τείνουν να είναι πολύ υποκειμενικές.



Διάγραμμα 3.3 [25] – Πυξίδα ασφάλειας

Μια προσπάθεια ταξινόμησης των κινδύνων έχει γίνει από την εταιρεία Espiria, η οποία και απορροφήθηκε από την Solutionary [25]. Προτείνεται η χρήση μίας «Πυξίδας Ασφαλείας» (Διάγραμμα 3.3), η οποία όχι μόνο παρουσιάζει τους παράγοντες της ασφάλειας ενός συστήματος αλλά τους ποσοτικοποιεί μέσα από μία σειρά από τυποποιημένες ερωτήσεις. Οι παράγοντες αυτοί είναι: Η Πολιτική Ασφάλειας (Security Policy), η Διοίκηση της Ασφάλειας (Security Management), ο Σχεδιασμός της Ασφάλειας (Security Planning), η Διαχείριση της Ασφάλειας (Security Administration), η Υποδομή Ασφάλειας (Security Infrastructure), η Παρακολούθηση της Ασφάλειας (Security Monitoring) και η Φυσική Ασφάλεια (Physical Security). Στη συνέχεια συγκρίνει την παρούσα κατάσταση με την επιθυμητή κατάσταση ασφάλειας και προτείνει τρόπους για τη βελτίωση μέρους ή του συνολικού συστήματος. Σε γενικές γραμμές, συσχετίζει το επίπεδο της ασφάλειας τόσο με το τεχνικό μέρος όσο και με το διαχειριστικό μέρος του συστήματος. Συνδυάζει επίσης το επίπεδο της ασφάλειας και το κόστος για την απόκτηση του. (Διάγραμμα 3.4)



Διάγραμμα 3.4 [25] – Συνδυασμός ασφάλειας και κόστους

Μια άλλη πολύ ενδιαφέρουσα προσπάθεια έχει γίνει από τον Lindgreen στο [26]. Σε αυτή τη μελέτη, το ενδιαφέρον και η κατηγοριοποίηση των κινδύνων εστιάζεται στο διαχειριστικό μέρος με τη συμμετοχή και του ανθρώπινου δυναμικού. Η ασφάλεια των πληροφοριών εκφράζεται ως μέρος της οργανωτικής δομής της επιχείρησης. Έτσι οι κίνδυνοι διαχωρίζονται σε

κινδύνους του προσωπικού, των κεφαλαίων, οικονομικούς και της πληροφορίας. (Πίνακας 3.6 [26])

Resources	Total Enterprise Risk Management			
	Personnel	Assets	Finance	Information
Risk/risk area	* Illness * Turnover * Decreased motivation * Knowledge drain ...	* Fire * Burglary * Theft * Disasters ...	* Currency risks * Interest risks * Payments due * Cash flow risks ...	* Eavesdropping * Illegal modification * Interruptions * Masquerading ...
Measures	* Human resource management ...	* Security * Alarms * Insurance ...	* Treasury * Insurance ...	* Information security * ICT audit ...

Πίνακας 3.6 – Διαχωρισμός κινδύνων

Εκτός από τις λύσεις που σχολιάστηκαν παραπάνω, ο Weiβ προτείνει στο [27] τον συνδυασμό ενιαίων παραγόντων ασφάλειας προκειμένου να υπολογιστεί το επίπεδο ασφάλειας μιας ολόκληρης οργάνωσης. Τέλος, η πιο σχετική εργασία είναι αυτή του ISO 27004 [28] που θα είναι το νέο πρότυπο του ISO στις μετρήσεις ασφαλείας πληροφοριών με σκοπό την καλύτερη διοίκηση της ασφάλειας. Το πρότυπο δεν έχει ακόμα οριστικοποιηθεί και κατά το στάδιο συγγραφής της εργασίας αποτελεί ακόμα σχέδιο εργασίας, που διατίθεται για μελέτη και σχόλια. Σύμφωνα με τον προγραμματισμό του International Organization for Standardization (ISO) και του International Electrotechnical Commission (IEC) που είναι υπεύθυνοι για την ανάπτυξή του, θα δημοσιευθεί εντός του 2009. Το πρότυπο αναμένεται να βοηθήσει τους οργανισμούς στη μέτρηση και στην αποτύπωση της αποτελεσματικότητας των συστημάτων διαχείρισης ασφαλείας πληροφοριών τους, που καλύπτουν και τις δύο διοικητικές διαδικασίες ασφάλειας (που καθορίζονται στο ISO 27001 [29]) και τους ελέγχους (ISO 17799/27002).

3.3.7. Συνεκτίμηση δομικών στοιχείων της ασφάλειας

Εκτός των παραπάνω κατηγοριών υπάρχουν δύο πιο σύνθετες κατηγορίες μέτρησης της ασφάλειας. Η πρώτη αφορά στη συνεκτίμηση των δομικών στοιχείων της ασφάλειας. Τα δομικά στοιχεία της ασφάλειας, όπως περιγράφηκαν στο κεφάλαιο 2 είναι η Ακεραιότητα, η Διαθεσιμότητα και η Εμπιστευτικότητα. Ως συμπληρωματικά στοιχεία της ασφάλειας των

Πληροφοριακών Συστημάτων θεωρούνται η μη-Αποποίηση Ευθύνης και η Αυθεντικοποίηση.

Μια προσπάθεια που εντάσσεται σε αυτή την κατηγορία είναι εκείνη του Knorr στο [30]. Στο πλαίσιο αυτής, προτείνεται μία δομημένη προσέγγιση για την ανάλυση μέτρων ασφαλείας και για την ποσοτικοποίηση της συνολικής ασφάλειας μιας ηλεκτρονικής επιχειρηματικής εφαρμογής (Electronic Business Application). Χρησιμοποιείται ένας πίνακας που αναπαριστά την «συνολική ασφάλεια» και την διαιρεί σε μικρότερα μέρη. Τα μέρη αυτά αντιστοιχούν σε περιοχές, πιθανούς στόχους και μηχανισμούς ασφαλείας της εφαρμογής και συσχετίζονται με τα συμμετέχοντα μέρη μιας ηλεκτρονικής επιχειρηματικής εφαρμογής (πελάτης, έμπορος, μέσο επικοινωνίας). Η διαδικασία αυτή αποσκοπεί στον υπολογισμό ενός «ποσοτικοποιητή» (quantifier) μιας ηλεκτρονικής επιχειρηματικής εφαρμογής, ο οποίος λειτουργεί ως μέσο για την ανάλυση, σχεδιασμό και μέτρο σύγκρισης με παρόμοιες εφαρμογές.

Η συγκεκριμένη εργασία περιορίζεται σε εμπορικές σχέσεις (Business to Consumer – B2C), ενώ για την διεκπεραίωση μιας ασφαλούς ηλεκτρονικής επιχειρηματικής εφαρμογής απαιτείται η συμβολή όλων, ανεξαιρέτως, των συμβαλλόμενων μερών. Αυτό όμως μπορεί να είναι εξαιρετικά δύσκολο λόγω:

α. Συμμετοχής ανομοιογενών συστημάτων

β. Του γεγονότος ότι ένα μέρος δεν μπορεί να επηρεάσει τον τρόπο λειτουργίας και τον δείκτη ασφαλείας ενός άλλου μέρους (τουλάχιστον με νόμιμο τρόπο!)

γ. Του πολύ χαμηλού δείκτη ασφαλείας του μέσου επικοινωνίας (Internet).

Κάθε συμβαλλόμενο μέρος μπορεί να έχει διαφορετικές (πιθανώς αντικρουόμενες) προτεραιότητες όσον αφορά την ασφάλεια κατά τη συναλλαγή. Το γεγονός αυτό είναι ιδιαίτερα σημαντικό καθώς η βαρύτητα των παραγόντων που αναφέρονται στον Πίνακα της Ασφάλειας (Security Matrix)

μπορεί να διαφοροποιείται ανάλογα με την οπτική γωνία (εμπόρου, πελάτη, μέσου μετάδοσης) από την οποία γίνεται η ανάλυση.

Ο Πίνακας 3.7 (όπως αυτός παρουσιάζεται στην δημοσίευση [30]) παρουσιάζει πιθανές απειλές διαχωρισμένες στα 4 επιλεγμένα δομικά στοιχεία (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Υπευθυνότητα) καθώς και στα συμβαλλόμενα μέρη. Με βάση την παραπάνω διάκριση των απειλών προτείνονται και διάφοροι τρόποι αντιμετώπισής τους. Οι τρόποι αυτοί κατηγοριοποιούνται σύμφωνα με το συμβαλλόμενο μέρος (πελάτης, έμπορος, μέσο μετάδοσης). Η ποσοτικοποίηση γίνεται με τη χρήση ενός πίνακα που περιέχει καταχωρήσεις οι οποίες είναι πραγματικοί αριθμοί. Οι αριθμοί αντιπροσωπεύουν το μέγεθος της προσπάθειας που έχει γίνει για την εφαρμογή των παραπάνω μέτρων ασφαλείας. Μεγαλύτερη τιμή στις καταχωρήσεις αντιστοιχεί σε μεγαλύτερο επίπεδο ασφάλειας.

Threats	Confidentiality	Integrity	Availability	Accountability
Customer	cookies	malware (e.g. tro-jan horses)	malware (e.g. tro-jan horses)	repudiation
Merchant	data protection problems	hacking attacks	hacking attacks	repudiation
Trans-mission	eavesdropping	sequence number guessing	denial-of-service attacks, worms	spoofing attacks

Measures	Confidentiality	Integrity	Availability	Accountability
Customer	configuration, awareness	malware scanning	malware scanning	client certificates
Merchant	access control	IDS, security tests	IDS, security tests	server certificates
Trans-mission	encryption (SSL, ESP)	SSL	'redundant network design'	AH

Πίνακας 3.7 – Διαχωρισμός απειλών

Ο ποσοτικοποιητής υπολογίζεται με την πρόσθεση των επιμέρους δεικτών επιπέδων ασφάλειας για κάθε ένα από τα παραπάνω στοιχεία του Πίνακα 3.7. Οι δείκτες θα πρέπει να είναι σταθμισμένοι ανάλογα με την επιμέρους επίδρασή τους στην συγκεκριμένη εφαρμογή). Εναλλακτικά μπορεί να υπολογισθεί ως γινόμενο των επιμέρους δεικτών επιπέδων ασφάλειας (και πάλι όμως πολλαπλασιαζόμενα με το την επιμέρους επίδρασή τους στη συγκεκριμένη εφαρμογή).

Το πρόβλημα δεν εστιάζεται τόσο στον υπολογισμό του ποσοτικοποιητή όσο στην εκτίμηση των επιμέρους δεικτών επιπέδων ασφάλειας. Αυτή γίνεται με ένα μάλλον αυθαίρετο τρόπο, βασιζόμενη στην εμπειρία και στο ένστικτο του εκτιμητή. Στην ουσία, αυτή η μέθοδος χρησιμοποιεί τον ποσοτικοποιητή ως ποσοστό των υλοποιηθέντων μέτρων σε σχέση με τα απαραίτητα μέτρα ασφάλειας. Με τον υπολογισμό του, ο ποσοτικοποιητής μπορεί να χρησιμοποιηθεί:

α. Για την ανάλυση της ασφάλειας της εφαρμογής (όσο μεγαλύτερη η τιμή του ποσοτικοποιητή, τόσο καλύτερο επίπεδο ασφάλειας παρέχεται).

β. Για τη σύγκριση με παρόμοια συστήματα (ο μεγαλύτερος δείκτης παρέχει ασφαλέστερες υπηρεσίες). Στην περίπτωση αυτή θα πρέπει να διασφαλιστεί ότι τα συστήματα είναι συγκρίσιμα μεταξύ τους. Ακόμα, θα πρέπει η εκτίμηση των επιμέρους δεικτών επιπέδων ασφάλειας που αναφέρθηκαν παραπάνω να γίνει με παρόμοιο τρόπο. Τέλος η διαδικασία διαχωρισμού των απειλών πρέπει να είναι επίσης παρόμοια.

γ. Για τον σχεδιασμό της ασφάλειας της εφαρμογής (κατά τη διάρκεια της διαδικασίας ανάπτυξης).

Μια άλλη προσπάθεια που συνδυάζει τεχνικές από πολλές από τις παραπάνω προσεγγίσεις και εντάσσεται στην κατηγορία συνεκτίμησης των δομικών στοιχείων της ασφάλειας είναι αυτή που περιγράφεται στο κεφάλαιο 4 της διατριβής. Όπως παρουσιάζεται και αναλυτικότερα εκεί, η συγκεκριμένη προσπάθεια εστιάζει στο γεγονός ότι οι οργανισμοί δεν χρησιμοποιούν ομοιόμορφες μεθόδους μέτρησης για όλες τις υπηρεσίες της Πληροφορικής. Επιπλέον, οι όποιες επιλεχθείσες μέθοδοι αλλά και τα μετρήσιμα μεγέθη, δεν είναι πλήρως αντικειμενικά, γεγονός που αποτυπώνεται και στην αξιολόγηση των μεθόδων των παραπάνω παραγράφων.

Η συγκεκριμένη έρευνα πρότεινε μια διαφορετική προσέγγιση για την ποσοτικοποίηση της ασφάλειας συγκεκριμένων υπηρεσιών αλλά και της

συνολικής ασφάλειας ενός οργανισμού. Αυτό επιτυγχάνεται με την ανάλυση της ασφάλειας κάθε υπηρεσίας σε πέντε (5) βασικές συνιστώσες οι οποίες είναι δυνατόν να μετρηθούν με αντικειμενικό τρόπο. Οι συνιστώσες αυτές είναι τα δομικά στοιχεία που αναφέρθηκαν στο κεφάλαιο 2. Για τη μέτρηση των στοιχείων αυτών, δημιουργούνται μια σειρά αντικειμενικών ερωτήσεων οι οποίες αποτυπώνουν κάθε στοιχείο ξεχωριστά. Η συνολική ασφάλεια μιας υπηρεσίας είναι ο σταθμισμένος μέσος όρος των στοιχείων αυτών, με βάση τη σημασία που δίνεται σε κάθε στοιχείο ανά υπηρεσία.

Για τον υπολογισμό της συνολικής ασφάλειας ενός οργανισμού, χρησιμοποιούνται οι τιμές της ασφάλειας κάθε υπηρεσίας, ανάλογα με τη σημασία που έχουν αυτές στον οργανισμό. Έτσι η τιμή της συνολικής ασφάλειας του οργανισμού προκύπτει από τον σταθμισμένο μέσο όρο των υπηρεσιών με βάση την αξία της κάθε υπηρεσίας στον οργανισμό.

Στόχος της παραπάνω προσέγγισης ήταν να παρουσιάσει μια αντικειμενική εικόνα του επιπέδου της ασφάλειας τόσο για τις προσφερόμενες υπηρεσίες ενός οργανισμού όσο και για τον επίπεδο της συνολικής ασφάλειας.

3.3.8. Συνεκτίμηση παραγόντων έμμεσα σχετιζόμενων με την ασφάλεια

Η δεύτερη πιο σύνθετη κατηγορία μέτρησης της ασφάλειας, αφορά στη συνεκτίμηση παραγόντων. Οι προσεγγίσεις αυτού του τύπου, αν και περιορισμένες, μπορούν να ομαδοποιηθούν με το σκεπτικό ότι μετρούν ή υπολογίζουν στοιχεία τα οποία δεν είναι άμεσα σχετιζόμενα με την ασφάλεια. Ερευνούν τη σχέση μεταξύ μεγεθών τα οποία είναι εύκολα και αντικειμενικά μετρήσιμα και της ασφάλειας υπηρεσιών.

Χαρακτηριστικό παράδειγμα αυτής της κατηγορίας είναι η προσέγγιση που παρουσιάζεται στο [31], όπου εξετάζεται το οικονομικό αντίκτυπο των περιστατικών ασφάλειας. Το οικονομικό αντίκτυπο μεταφράζεται σε μείωση της τιμής των μετοχών του οργανισμού, ως αποτέλεσμα της αρνητικής

εικόνας που δημιουργείται στο επενδυτικό κοινό. Έτσι η τιμή των μετοχών αποτελεί ένα μέγεθος με το οποίο μπορεί έμμεσα να αξιολογηθεί το επίπεδο της ασφάλειας ενός οργανισμού.

Η προσέγγιση αυτή αποτέλεσε τη βάση για την αντίστοιχη παράγραφο του κεφαλαίου 4, το οποίο και στοχεύει στην ανάπτυξη μιας μεθοδολογίας για την αντικειμενική μέτρηση της ασφάλειας με τη χρήση στοιχείων που σχετίζονται έμμεσα ή άμεσα με την ασφάλεια.

3.4. Σύνοψη και συμπεράσματα

Το κεφάλαιο 3 παρουσιάζει μια επισκόπηση της βιβλιογραφίας η οποία είναι σχετική με το αντικείμενο της διατριβής και αποτελεί τη βάση για τα επόμενα κεφάλαια. Η βιβλιογραφία αφορά στις μεθοδολογίες μετασχηματισμού των Πληροφοριακών Υποδομών καθώς και στις προσεγγίσεις για τη Μέτρηση και Μοντελοποίηση της Ασφάλειας.

Οι μεθοδολογίες μετασχηματισμού των πληροφοριακών υποδομών βασίζονται στην κλασική θεωρία Διαχείρισης Αλλαγών αλλά και στη νεότερη και περισσότερο προσανατολισμένη στις Υπηρεσίες Πληροφορικής, Βιβλιοθήκη Υποδομής Τεχνολογίας Πληροφοριών.

Οι πιο πολλές από τις προσεγγίσεις για την Μέτρηση και Μοντελοποίηση της Ασφάλειας, δίνουν έμφαση σε διαφορετικές οπτικές της Ασφάλειας αντί να πραγματοποιούν αντικειμενικές μετρήσεις. Υπάρχουν πολύ λίγες προσεγγίσεις οι οποίες εστιάζουν στην παροχή των μέσων της μέτρησης της ασφάλειας.

3.5. Βιβλιογραφία κεφαλαίου

[1] "Change Management", Wikipedia, ανακτήθηκε: 14/6/09, http://en.wikipedia.org/wiki/Change_management

[2] J. Martin, "Organisational Behaviour", Thomson Business Press, 1998, ISBN 1-86152-180-4, σελ. 575-600

[3] L. J. Mullins, "Management and Organisational Behaviour", 5th Edition, Pitman Publishing, 1999, ISBN 0-273-63552-2, σελ. 821-830

[4] "Change Management: Five basic principles, and how to apply them", ανακτήθηκε: 14/6/09, http://www.teamtechnology.co.uk/changemanagement.html

[5] J. P. Garbani, "Best Practices For Infrastructure Change Management: Regain Control Of Runaway IT Infrastructures", Forrester Research, ανακτήθηκε: 14/6/09, http://www.forrester.com/Research/Document/Excerpt/0,7211,34048,00.html

[6] ITIL Homepage, ανακτήθηκε: 14/6/09, http://www.itil-officialsite.com/home/home.asp

[7] M. Gerencser and D. Aguirre, "Security Concerns Prominent on CEO Agenda," strategy + business magazine, Τεύχος Φεβρουαρίου 2002, ανακτήθηκε: 14/6/09, http://www.strategy-business.com/press/enews/article/?ptag-ps=&art=254087&pg=0

[8] A. Carey, "Worldwide Information Security Services Forecast, 2001–2006," IDC report no. 26899, Απρίλιος 2002

[9] B. Schneier, "Secrets & Lies, Digital Security in a Networked World", John Wiley & Sons, 2000, ISBN 0-471-25311-1

[10] John Leach, securitymetrics.org mailing list message, "Modelers v measurers (was: Risk metrics)", Ιανουάριος, 2006.

[11] A. Jaquith, "Security Metrics: Replacing Fear, Uncertainty, and Doubt", Addison-Wesley Professional, 2007, ISBN 978-0321349989, σελ. 9-15

[12] Microsoft Baseline Security Analyzer, Microsoft Corporation, ανακτήθηκε: 14/6/09, www.microsoft.com/technet/security/tools/mbsahome.mspx

[13] The center for internet security (cisecurity), ανακτήθηκε: 14/6/09, http://www.cisecurity.com/

[14] Nessus, ανακτήθηκε: 14/6/09, http://www.nessus.org/nessus/

[15] St. McClure, "Hacking Exposed 4th Edition: Network Security Secrets And Solutions", McGraw-Hill Osborne Media, 2005, ISBN 978-0072260816.

[16] «RedSiren», Western Independent Bankers, 2002 Annual Conference, ανακτήθηκε: 14/6/09, http://www.wib.org/conferences__education/past_programs/2005__earlier/2002_annual_conference/handouts/redsiren.pdf

[17] D. A. Shinberg, "A Management Guide to Penetration Testing", SANS Institute, Reading Room, 2003.

[18] "Penetration Testing Guide", Corsaire Limited, 2004, ανακτήθηκε: 14/6/09, http://www.penetration-testing.com/

[19] IT Baseline Protection Manual, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2004.

[20] ISO/IEC. Information technology – Security techniques – Code of practice for information security management (final draft). ISO, 2008.

[21] Information Security Management. Specification for Information Security Management Systems (BS 7799-2). British Standard Institute, London, 1999.

[22] Information Security Management. Code of Practice for Information Security Management. (BS 7799-1). British Standard Institute, London, 1999.

[23] R. Ross, St. Katzke, Ar. Johnson, M. Swanson, G. Stoneburner, G. Rogers, και An. Lee. "Recommended Security Controls for Federal Information Systems" (Final public draft; NIST SP 800-53). National Institute of Standards and Technology Gaithersburg, 2005.

[24] G. Stoneburner, Al. Goguen, και Al. Feringa. "Risk Management Guide for Information Technology Systems" (NIST SP 800-30). National Institute of Standards and Technology, Gaithersburg, 2002.

[25] Solutionary managed security service provider, ανακτήθηκε: 14/6/09, http://www.solutionary.com/

[26] Ed. R. Lindgreen, J. Acohen, H. de Boer, G. Uit de Bosch, C. van Rinsum: "Building on Solid Foundations: An Information Security Case Study", IEEE IFIP Conference Proceedings; Vol. 200. Σελ. 57-72

[27] S. Weiβ, Ol. Weissmann, F. Dressler. A comprehensive and Comparative Metric for Information Security. Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis 2005 (ICTSM2005), Dallas, TX, USA, November 2005, pp. 1-10.

[28] ISO/IEC 27004 Information technology — Information security management (draft), ανακτήθηκε: 14/6/09, http://www.iso27001security.com/html/27004.html

[29] ISO 27001 Security Management Standard, ανακτήθηκε: 14/6/09, http://www.27001-online.com/

[30] K. Knorr; S. Rohrig. "Security of Electronic Business Applications: Structure and Quantification", 2000, Towards the E-Society: First IFIP Conference on E-Commerce, E-Business, and E-Government.

[31] K. Campbell, L. A. Gordon, M. P. Loeb and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," Journal of Computer Security, Vol. 11 (2003), pp. 431-448.

4. Μέτρηση της ασφάλειας

4.1. Εισαγωγή

Η διάσημη ρήση του Λόρδου Κέλβιν με την οποία υποστήριξε ότι «Δεν μπορείς να βελτιώσεις ότι δεν μπορείς να μετρήσεις» αποτελεί το βασικό κίνητρο του κεφαλαίου αυτού. Η σημερινή εποχή της πληροφορίας έχει δώσει νέες ερμηνείες στη συγκεκριμένη ρήση, εκφράζοντας την ανάγκη της μέτρησης αφηρημένων εννοιών όπως η ασφάλεια των Πληροφοριακών Συστημάτων. Στο ίδιο πνεύμα, πολλαπλές πηγές που εκτείνονται από την ακαδημαϊκή έρευνα ως τον βιομηχανικό σχεδιασμό, όπως οι [1], [2] και [3], τονίζουν τη σημασία της μέτρησης της ασφάλειας εντός των Πληροφοριακών Υποδομών.

Το κεφάλαιο αυτό παρέχει τις απαιτούμενες πληροφορίες αλλά και τα κατάλληλα εργαλεία για τη μέτρηση της ασφάλειας τόσο των Πληροφοριακών Υποδομών όσο και των υπηρεσιών που βασίζονται σε Πληροφοριακές Υποδομές. Σκοπός των μεθοδολογιών που αναπτύσσονται εδώ είναι να αποτελέσουν ένα καλύτερο μέσο διαχείρισης των Πληροφοριακών Υποδομών και ειδικότερα, των Κρίσιμων Πληροφοριακών Υποδομών Ασφάλειας, το οποίο αποτελεί και το κύριο αντικείμενο της διατριβής.

Το παρόν κεφάλαιο διαχωρίζεται σε τέσσερα επιμέρους μέρη.

Το πρώτο περιγράφει και αναλύει τις βασικές απαιτήσεις κάθε μεθοδολογίας για τη μέτρηση της ασφάλειας.

Το δεύτερο μέρος αναφέρεται σε συγκεκριμένες μεθοδολογίες μέτρησης της ασφάλειας, όπως αυτές παρουσιάστηκαν στο κεφάλαιο 3 και παρουσιάζει τα όρια τους. Τα όρια αυτά σχετίζονται με οικονομικούς, φυσικούς, τεχνικούς, λειτουργικούς, οργανωτικούς ή διαδικαστικούς περιορισμούς.

Το τρίτο μέρος του κεφαλαίου αναλύεται η πρόταση δύο διαφορετικών προσεγγίσεων μέτρησης της ασφάλειας, οι οποίες επιχειρούν να ξεπεράσουν

κάποιο από τα όρια των μεθοδολογιών που παρουσιάστηκαν στο κεφάλαιο 3. Η πρώτη επιχειρεί να υπολογίσει την ασφάλεια με τον συνδυασμό των δομικών στοιχείων της ασφάλειας, ενώ η δεύτερη προσεγγίζει την ασφάλεια ως μέγεθος έμμεσα σχετιζόμενο με κάποιους εύκολα μετρήσιμους παράγοντες.

Το τέταρτο και τελευταίο μέρος του κεφαλαίου αφορά την οπτικοποίηση της ασφάλειας, τομέας που αποτελεί αναπόσπαστο κομμάτι κάθε προσπάθειας εκτίμησης, μέτρησης ή υπολογισμού της ασφάλειας. Στην παράγραφο αυτή συγκεντρώνονται οι βέλτιστες πρακτικές για την αποδοτικότερη παρουσίαση του επιπέδου της ασφάλειας ενός οργανισμού.

4.2. Ποσοτικοποίηση και μέτρηση της ασφάλειας

4.2.1. Μέτρηση της ασφάλειας

Αδιαμφισβήτητα, η σημασία της επιστημονικής μέτρησης είναι πολύ μεγάλη. Όπως και στις παλαιότερες φυσικές επιστήμες, έτσι και στην επιστήμη της Πληροφορικής και ειδικότερα στον τομέα της ασφάλειας των Πληροφοριακών Συστημάτων, οι επιστημονικές μετρήσεις μπορούν να συμβάλουν καθοριστικά στη διατύπωση και επαλήθευση θεωριών. Για την καλύτερη κατανόηση και εκμετάλλευση των αποτελεσμάτων των μετρήσεων κρίνεται σκόπιμο να οριστεί η μέτρηση από την οπτική της ασφάλειας των Πληροφοριακών Συστημάτων.

Σύμφωνα με το αμερικανικό λεξικό του Πρίνστον ο γενικός ορισμός της μέτρησης (measurement) είναι «η διαδικασία του προσδιορισμού μιας ιδιότητας (ή φαινόμενου) με έναν αριθμό, με τη χρήση κάποιου ή κάποιων προκαθορισμένων κανόνων» [4]. Άμεσα σχετιζόμενη με τη μέτρηση είναι η έννοια του μετρικού συστήματος (metric) το οποίο σύμφωνα με το ίδιο λεξικό είναι «μια σειρά πρότυπων μεγεθών τα οποία διευκολύνουν την ποσοτικοποίηση κάποιων συγκεκριμένων χαρακτηριστικών» [5].

Εστιάζοντας στο επιστημονικό πεδίο της Πληροφορικής το [6] διαχωρίζει μεταξύ μετρικών συστημάτων τα οποία χρησιμοποιούνται για την ποσοτικοποίηση αξιών, δηλαδή ως έλεγχος της καλής λειτουργίας και εκείνων που χρησιμοποιούνται για τη μέτρηση της αποδοτικότητας. Η μέτρηση της ασφάλειας είναι ένα θέμα το οποίο κατατάσσεται στην πρώτη κατηγορία, δηλαδή ως ποσοτικοποίηση μιας αξίας.

Παρόλο που η ασφάλεια των Πληροφοριακών Συστημάτων αποτελεί μια πάγια απαίτηση εξακολουθεί να είναι μια αφηρημένη έννοια. Όπως κάθε αφηρημένη έννοια, έτσι και η ασφάλεια χαρακτηρίζεται από μια ασάφεια στην υλοποίηση και στη μέτρησή της. Αυτό γιατί, δεν είναι δυνατό να προσδιοριστεί εύκολα ένας αριθμός ο οποίος, σύμφωνα τον πρώτο ορισμό της μέτρησης, να αποδοθεί στην ασφάλεια και να εκφράσει την κατάστασή της. Η δυσκολία μέτρησης της ασφάλειας, οδηγεί λοιπόν στην αναζήτηση των κατάλληλων μεθόδων που θα μπορέσουν να καθορίσουν τόσο τα κατάλληλα μεγέθη όσο και τους κανόνες μέτρησης.

Οι σχετικές προσεγγίσεις που παρουσιάστηκαν και αξιολογήθηκαν στο Κεφάλαιο 3 δίνουν έμφαση σε διαφορετικές οπτικές της Ασφάλειας αντί να πραγματοποιούν αντικειμενικές μετρήσεις οι οποίες να μπορούν στη συνέχεια να χρησιμοποιηθούν για τη βελτιστοποίηση της λειτουργίας των Πληροφοριακών Συστημάτων.

4.2.2. Στόχοι της μέτρησης της ασφάλειας

Η σημερινή εποχή είναι μια εποχή της μοντελοποίησης συστημάτων και της μέτρησης μεγεθών. Τα μοντέλα και οι μετρήσεις καθορίζονται συνήθως σύμφωνα με τις δυνατότητες που έχουν να αποτυπώσουν αποτελέσματα τα οποία μπορούν να μειώσουν την αβεβαιότητα του μέλλοντος. Μειώνοντας την αβεβαιότητα γίνεται ευκολότερο να παρθούν λογικά δικαιολογημένες αποφάσεις που βασίζονται σε στοιχεία και κατά συνέπεια να μειώνεται ο κίνδυνος κάθε ενέργειας που σχετίζεται με κάποιο μοντέλο.

Δυστυχώς η ασφάλεια είναι ένα από τα λιγοστά πεδία που σχετίζονται με τη διαχείριση πόρων, το οποίο δεν απολαμβάνει τα οφέλη ούτε μιας καλοδιατυπωμένης σειράς τεχνικών μέτρησης ούτε ενός εξειδικευμένου μοντέλου υπολογισμού της ολικής ασφάλειας μιας υπηρεσίας ή ενός οργανισμού. Αντίθετα, σε άλλα πεδία όπως η Λογιστική υπάρχουν μετρήσιμα μεγέθη όπως τα «συνολικά κέρδη ανά έτος» και τα «συνολικά έξοδα ανά εξάμηνο», τα οποία και βοηθούν τα στελέχη να κατανοήσουν πόσο αποδοτικά δραστηριοποιούνται οι οργανισμοί τους.

Τα κέρδη από τη μέτρηση και κατ' επέκταση τη διαχείριση της ασφάλειας μπορούν να κατηγοριοποιηθούν ως εξής:

- **Διευκόλυνση της επιχειρηματικής στρατηγικής**: Η ασφάλεια των Πληροφορικών Συστημάτων είναι ζωτικής σημασίας για τη δημιουργία και την υποστήριξη της εμπιστοσύνης μεταξύ των οργανισμών, των συνεργατών, των πελατών και των υπαλλήλων τους. Αυτό σημαίνει ότι απαιτείται μια ισχυρή ευθυγράμμιση μεταξύ των επιχειρηματικών και τεχνολογικών στρατηγικών με τις στρατηγικές ασφάλειας.

- **Υποστήριξη των καθημερινών επιχειρηματικών δραστηριοτήτων**: Όσο η αξία της πληροφορίας αυξάνεται τόσο γίνεται και πιο ορατή ως στόχος ενδεχόμενης κλοπής, απάτης και επίθεσης. Ακόμα και ακούσια και συμπτωματικά γεγονότα τα οποία καθιστούν τα Πληροφορικά Συστήματα μη διαθέσιμα μπορούν να καταστήσουν και τις αντίστοιχες επιχειρηματικές δραστηριότητες ανέφικτες.

- **Διαχείριση κινδύνου**: Η βελτίωση της διαχείρισης του κινδύνου μπορεί να συνεισφέρει όχι μόνο στη στήριξη αποφάσεων αλλά και στην αξιοποίηση επιχειρηματικών ευκαιριών.

- **Μείωση περιττών εξόδων**: Μια ανεπαρκής αντίληψη της ασφάλειας μπορεί να οδηγήσει σε αντιοικονομική λειτουργία τόσο των πληροφοριακών υποδομών όσο και των επιχειρηματικών δραστηριοτήτων, αλλά και σε εν δυνάμει έξοδα προβολής και προστασίας των επιχειρηματικών προϊόντων και υπηρεσιών.

- **Αντιμετώπιση νομικών υποχρεώσεων**: Οι παραβιάσεις της ασφάλειας δημιουργούν μια σειρά δικαστικών κινδύνων και πιθανώς και υποχρεώσεων.

- **Αντιμετώπιση κανονιστικών υποχρεώσεων**: Η ανάγκη για ισχυρές διαδικασίες διαχείρισης κινδύνου αποτελούν και κανονιστική υποχρέωση όπου ο πιστωτικός έλεγχος περιλαμβάνει και τον κίνδυνο που αφορά και τα Πληροφοριακά Συστήματα.

Μια τυποποιημένη προσέγγιση μέτρησης της ασφάλειας αναζητά τη λειτουργία του οργανισμού χωρίς τον φόβο της αβεβαιότητας και της αμφιβολίας σε ένα πλαίσιο όπου η πιθανότητα του κινδύνου θα μπορεί να ποσοτικοποιηθεί, το εύρος της πιθανής ζημιάς θα μπορεί να εκτιμηθεί, η απόδοση των μηχανισμών θα μπορεί να αποτυπωθεί και το κόστος των ελεγκτικών μηχανισμών ασφάλειας θα μπορεί να αξιολογηθεί σύμφωνα με την αποτελεσματικότητα τους.

4.2.3. Ποσοτικοποίηση της ασφάλειας

Από τα παραπάνω γίνεται αντιληπτό ότι δεν είναι εφικτό να μετρηθεί ένα αφηρημένο μέγεθος, όπως η ασφάλεια, χωρίς προηγουμένως να ποσοτικοποιηθεί κάποιο μέγεθος. Είναι λοιπόν απαραίτητο να οριστεί σαφώς το πλαίσιο που αφορά στην ποσοτικοποίηση μεγεθών.

Σύμφωνα με το [7] η ποσοτικοποίηση «...στα μαθηματικά και στις εμπειρικές επιστήμες, αναφέρεται στις ανθρώπινες δραστηριότητες της καταμέτρησης και

μέτρησης οι οποίες αποτυπώνουν τις παρατηρήσεις και εμπειρίες που πραγματοποιούνται με φυσικά μέσα με κάποια ομάδα αριθμών.»

Αντίστοιχα στον τομέα της ασφάλειας των Πληροφοριακών Συστημάτων, η ποσοτικοποίηση αποσκοπεί στην αποτύπωση του επιπέδου της ασφάλειας μετατρέποντας τις παρατηρήσεις και εμπειρίες που πραγματοποιούνται με φυσικά μέσα σε κάποιο αριθμητικό μέγεθος. Εφόσον η ασφάλεια είναι μια αφηρημένη έννοια, οι παραπάνω παρατηρήσεις θα πρέπει να αφορούν κάποια άλλα μεγέθη που σχετίζονται με την ασφάλεια είτε άμεσα είτε έμμεσα.

4.2.4. Σύγκριση Ποσοτικοποίησης και Ποιοτικής ανάλυσης

Ανατρέχοντας στις τεχνικές που σχετίζονται με τη μέτρηση αφηρημένων εννοιών, θεωρείται σημαντικό να αξιολογηθεί και η προσέγγιση της Ποιοτικής Ανάλυσης όπως αυτή περιγράφεται στο [8].

Η Ποιοτική Ανάλυση έχει τα παρακάτω χαρακτηριστικά, τα οποία και τη διαφοροποιούν από την Ποσοτική Ανάλυση (Ποσοτικοποίηση):

1. Ασχολείται κυρίως με τις διαδικασίες και λιγότερο με τα αποτελέσματα ή τα παράγωγα αυτών των διαδικασιών.
2. Ασχολείται κυρίως με προτιμήσεις, εμπειρίες και δομές.
3. Συλλέγει κυρίως πρωτογενή δεδομένα τα οποία είναι ευάλωτα σε υποκειμενικές κρίσεις και αντιλήψεις.
4. Απαιτεί άμεση παρατήρηση και καταγραφή συμπεριφορών καθώς και άμεση επαφή με το περιβάλλον αξιολόγησης.
5. Είναι περιγραφική – αφαιρετική – «αναλογική».
6. Είναι ενδεικτική γιατί περιλαμβάνει αρχές, υποθέσεις και θεωρίες βασισμένες μόνο στις συγκεκριμένες μετρήσεις.

Ο πίνακας 4.8 από το [9] παρουσιάζει όλα μια σύγκριση των δύο μεθόδων.

Ποσοτικοποίηση	Ποιοτική Ανάλυση
Παραδοχές • Τα κοινωνικά γεγονότα έχουν μια αντικειμενική φύση • Η μέθοδος οδηγεί στο αποτέλεσμα • Οι μεταβλητές μπορούν να αναγνωριστούν και οι σχέσεις τους να μετρηθούν • «Εξωτερική» οπτική	**Παραδοχές** • Τα κοινωνικά γεγονότα έχουν μια υποκειμενική φύση • Το αποτέλεσμα οδηγεί στην μέθοδο • Οι μεταβλητές είναι περίπλοκες, ασαφείς και δύσκολα μετρήσιμες • «Εσωτερική» οπτική
Σκοπός • Γενίκευση • Πρόβλεψη • Αιτιώδεις εξηγήσεις	**Σκοπός** • Συνύφανση των δεδομένων • Απόδοση • Κατανόηση των διαφορετικών οπτικών
Προσέγγιση • Αρχίζει με υποθέσεις και θεωρίες • Μεθόδευση και έλεγχος • Χρησιμοποιεί τυποποιημένα εργαλεία • Πειραματισμός • Συμπερασματικός • Ανάλυση των δομικών στοιχείων • Αναζήτα πρότυπα • Μειώνει τα δεδομένα σε αριθμητικούς δείκτες • Χρησιμοποιεί αφηρημένη γλώσσα	**Προσέγγιση** • Ολοκληρώνεται με υποθέσεις και θεωρίες • Ανάδειξη και απεικόνιση • Ο ερευνητής αποτελεί μέρος της ανάλυσης • Φυσιοκρατικός • Επαγωγικός • Αναζητά δομές • Αναζήτα πλουραλισμό των μεθόδων • Κάνει ελάχιστη χρήση αριθμητικών δεικτών • Χρησιμοποιεί περιγραφική γλώσσα
Ο ρόλος του ερευνητή • Ουδέτερος και αμερόληπτος • Αντικειμενική απεικόνιση	**Ο ρόλος του ερευνητή** • Προσωπική εμπλοκή και πιθανή μεροληψία • Φίλα προσκείμενη κατανόηση των μεγεθών

Πίνακας 4.8 – Σύγκριση ποσοτικής και ποιοτικής ανάλυσης

Έχοντας αξιολογήσει τα χαρακτηριστικά και των δύο μεθόδων, θεωρείται ότι παρόλο που και οι δύο προσεγγίσεις έχουν τα αρνητικά και τα θετικά τους, η ασφάλεια μπορεί να αξιολογηθεί και να αποτυπωθεί και με τις δύο μεθόδους. Όμως η υποκειμενική φύση της Ποιοτικής Ανάλυσης είναι δυνατό να οδηγήσει

σε διαφορετικά αποτελέσματα δύο αξιολογητές της ασφάλειας ενός οργανισμού ή μιας υπηρεσίας ακολουθώντας την ίδια μεθοδολογία. Το γεγονός αυτό θεωρείται πολύ σημαντικό στο πλαίσιο της διατριβής και κατά συνέπεια οι μεθοδολογίες που προτείνονται βασίζονται στην Ποσοτικοποίηση.

4.2.5. Απαιτήσεις για τις μεθόδους μέτρησης της ασφάλειας

Έχοντας περιγράψει όλα τα γενικά στοιχεία των μεθόδων μέτρησης, η συγκεκριμένη παράγραφος συνδυάζει τα παραπάνω και εστιάζει στις εξειδικευμένες απαιτήσεις των μεθοδολογιών μέτρησης της ασφάλειας. Η υλοποίηση των απαιτήσεων αυτών είναι απαραίτητη για να καταστήσει τη διαδικασία της ποσοτικοποίησης της ασφάλειας αξιοποιήσιμη.

Μια αρχική απαίτηση είναι η διευκόλυνση της διορατικότητας των ανώτατων στελεχών ενός οργανισμού στον τομέα της ασφάλειας. Η κάθε μεθοδολογία μέτρησης θα πρέπει δηλαδή πρωτίστως να αποσκοπεί στην παράθεση των στοιχείων εκείνων που θα σκιαγραφούν πλήρως τόσο την παρούσα κατάσταση όσο και τη μελλοντική τάση από την οπτική της ασφάλειας. Επιπροσθέτως η ανάλυση των απαιτήσεων θα πρέπει να:

- Βοηθά έναν αναλυτή να διαγνώσει τα θέματα που σχετίζονται με την ασφάλεια και να αξιολογήσει την απόδοση των μηχανισμών και διαδικασιών της ασφάλειας που έχουν ήδη υλοποιηθεί.

- Ποσοτικοποιεί συγκεκριμένα χαρακτηριστικά και παραμέτρους της ασφάλειας

- Διευκολύνει τη διερεύνηση «πριν και μετά» και υποθετικών σεναρίων.

- Εστιάζει το ενδιαφέρον των μετρήσεων στα αίτια, τα μέσα και τα αποτελέσματα παρά στις μεθοδολογίες από όπου αποκόμισε τα σχετικά πορίσματα.

Σύμφωνα με το [10], κάθε μεθοδολογία μέτρησης της ασφάλειας θα πρέπει να έχει τα χαρακτηριστικά του Πίνακα 4.9 και αναλύονται παρακάτω:

Χαρακτηριστικά Μεθόδων Μέτρησης Ασφάλειας
Συνέπεια
Χαμηλού κόστους συλλογή των δεδομένων
Αναπαράσταση ως ποσοστό ή ως αριθμός
Χρήση τουλάχιστον μιας μονάδας μέτρησης
Σχέση με το ευρύτερο πλαίσιο
Βαρύτητα στη συνολική εκτίμηση
Επαναληψημότητα
Συγκρισιμότητα

Πίνακας 4.9 – Χαρακτηριστικά μεθόδων μέτρησης ασφάλειας

Συνέπεια

Οι μεθοδολογίες μέτρησης παρέχουν αξιοπιστία όταν μπορούν να υπολογισθούν με έναν συνεπή τρόπο. Διαφορετικοί άνθρωποι πρέπει να είναι σε θέση να εφαρμόσουν τη μέθοδο στο ίδιο σύνολο δεδομένων και να καταλήξουν σε ισοδύναμες απαντήσεις. Η συνθήκη που απαιτείται για να επαληθεύσει το παραπάνω εκφράζεται ως εξής: «Δύο διαφορετικά άτομα στα οποία υποβληθεί η ίδια ερώτηση δίνουν την ίδια απάντηση σχετικά με τη μέτρηση κάποιου μεγέθους;». Οι μετρήσεις αυτές θα πρέπει να διαφοροποιηθούν από τις μετρήσεις που εξαρτώνται από τις υποκειμενικές κρίσεις των ερευνητών οι οποίες αναφέρονται ως κατατάξεις ή διαβαθμίσεις.

Μια μεθοδολογία μέτρησης μπορεί να εξασφαλίσει τη συνέπειά της με την καταγραφή των επιμέρους βημάτων της μέτρησης με έναν τρόπο που θα είναι διαφανής και σαφής προς τον άνθρωπο που θα κληθεί να μετρήσει. Θα πρέπει δηλαδή η κάθε μεθοδολογία μέτρησης να εξηγεί το «πως» εφαρμόζεται το κάθε βήμα της μέτρησης και το «γιατί» εφαρμόζεται με το συγκεκριμένο τρόπο.

Ένας ιδιαίτερα αποδοτικός τρόπος διατήρησης της συνέπειας είναι χρήση ερωτήσεων μερικής αγνοίας, δηλαδή ερωτήσεων που μπορούν να απαντηθούν με ένα «ναι» ή ένα «όχι». Ένας άλλος τρόπος είναι η χρήση

αυτοματοποιημένων διαδικασιών, οι οποίες ακολουθούν κάθε φορά την ίδια διαδικασία μέτρησης χωρίς αποκλίσεις.

Χαμηλού κόστους συλλογή των δεδομένων

Κάθε μεθοδολογία μέτρησης χρειάζεται χρόνο για να υπολογίσει τα αποτελέσματα. Όλες οι μεθοδολογίες μέτρησης ξεκινούν με ακατέργαστα δεδομένα και στη συνέχεια, ακολουθώντας το εκάστοτε μοντέλο, τα μετατρέπουν σε χρήσιμες πληροφορίες. Άρα, αρχικά, κάποιος ή κάτι πρέπει να συλλέξει τα δεδομένα από μια κατάλληλη πηγή, να τα μετασχηματίσει στην επιθυμητή μορφή, και τελικά να υπολογίσει και να μορφοποιήσει τα αποτελέσματα.

Στο πλαίσιο μιας αποδοτικής μεθοδολογίας μέτρησης, αυτά τα βήματα μετατροπής και μορφοποίησης θα πρέπει να συγκεντρώνονται με τη χρήση μιας ενιαίας και γρήγορης διαδικασίας. Εάν η διαδικασία μέτρησης είναι ανεπαρκής, η μέθοδος συγκέντρωσης των δεδομένων μπορεί να κοστίσει στον οργανισμό χρόνο και χρήμα τα οποία θα μπορούσαν να δαπανηθούν στην ανάλυση των αποτελεσμάτων.

Το υψηλό κόστος μιας μεθοδολογίας μέτρησης μπορεί να οφείλεται σε μια σειρά από παράγοντες όπως η συχνότητα των μετρήσεων, η πολυπλοκότητα της διαδικασίας και η μη αυτοματοποίησή της.

Είναι λοιπόν λογικό για ένα μοντέλο μέτρησης να κάνει και προτάσεις επί των βέλτιστων υποψηφίων πηγών δεδομένων, υπό το πρίσμα της οικονομίας χρόνου και χρήματος.

Αναπαράσταση ως ποσοστό ή ως αριθμός

Όλες οι μετρήσεις θα πρέπει να εκφράζονται ως απόλυτος αριθμός ή ποσοστό, το οποίο θα αναπαριστά κάτι που μετρά μια ποσότητα μεγέθους. Όπως αναφέρθηκε και προηγουμένως, οι διαβαθμίσεις όπως «υψηλό, μεσαίο, χαμηλό» ή «1, 2, 3» (από μια τριτοβάθμια κλίμακα) αναπαριστούν σχετικές

βαθμολογίες αλλά δεν μετράνε κάποιο μέγεθος, οπότε και δεν μπορούν να χρησιμοποιηθούν σε ένα μοντέλο μέτρησης. Έτσι, με τη φράση "εκφράζεται σε αριθμό," εννοείται ο πληθικός αριθμός, ο οποίος υποδηλώνει το πλήθος των στοιχείων του συνόλου και όχι ο αριθμός που δηλώνει την σειρά των στοιχείων του συνόλου.

Έτσι, οι μεθοδολογίες μέτρησης που δεν εκφράζονται ως αριθμοί δεν είναι κατάλληλες για τη μέτρηση της ασφάλειας. Οι ενδείξεις του τύπου "φωτεινός σηματοδότης" με τις τρεις ενδείξεις κόκκινο, κίτρινο, πράσινο δεν αποτελούν κάποιου τύπου μέτρηση αφού δεν περιλαμβάνουν κάποια αριθμητική κλίμακα.

Θα πρέπει να σημειωθεί ότι τα χρώματα του φωτεινού σηματοδότη μπορούν να χρησιμοποιηθούν ως απεικόνιση ή παρουσίαση της τρέχουσας κατάστασης αλλά σε αφαιρετικό επίπεδο συμπληρώνοντας τα απαραίτητα αριθμητικά δεδομένα. Περαιτέρω πληροφορίες σχετικά με την απεικόνιση της ασφάλειας περιλαμβάνονται στο κεφάλαιο 4.5.3 το οποίο αναφέρει τους κανόνες οπτικοποίησης των αποτελεσμάτων μέτρησης της ασφάλειας.

Χρήση τουλάχιστον μιας μονάδας μέτρησης

Άλλη μια βασική απαίτηση ενός μοντέλου μέτρησης της ασφάλειας είναι ότι όλες οι σχετιζόμενες μετρήσεις θα πρέπει να περιλαμβάνουν επίσης μια σχετική μονάδα μέτρησης, η οποία θα χαρακτηρίζει τα μεγέθη που μετρούνται. Για παράδειγμα, η μέτρηση «αριθμός των φυσικών εισβολών στο κτήριο της πληροφορικής» χρησιμοποιεί ως μονάδα μέτρησης τις εισβολές. Με τη χρήση των μονάδων μέτρησης, ο ερευνητής γνωρίζει πως να εκφράζει με τον ίδιο τρόπο παρόμοιες μετρήσεις.

Σε κάποιες περιπτώσεις είναι καλύτερο να χρησιμοποιούνται περισσότερες από μία μονάδα μέτρησης με σκοπό τη διευκόλυνση της σύγκρισης διαφορετικών εφαρμογών. Στο παραπάνω παράδειγμα η γενικότερη μονάδα μέτρησης μπορεί να αποδοθεί και ως «αριθμός ατόμων που αποπειράθηκαν να εισβάλουν στο κτίριο της πληροφορικής», η οποία είναι και μια άλλη μονάδα

μέτρησης. Η χρήση αυτής της μονάδας μπορεί να είναι καταλληλότερη για τη σύγκριση με ένα άλλο μετρήσιμο μέγεθος, αυτό του «συνολικού αριθμού ατόμων που εισέρχονται στο κτίριο της πληροφορικής».

Σχέση με το ευρύτερο πλαίσιο

Μία άλλη απαίτηση για τις καλές μεθοδολογίες μέτρησης είναι ότι σημαίνουν κάτι για τα πρόσωπα που τις εξετάζουν. Αποκαλύπτουν θέματα της υπό εξέταση υποδομής ή υπηρεσίας βελτιώνοντας ή επιδεικνύοντας την αξία των ανθρώπων και των διαδικασιών για τον οργανισμό. Παρόλο που η σχέση δεν αποτελεί κύρια απαίτηση για μια καλή μέτρηση, βοηθά στη διατήρηση των αποτελεσμάτων των μετρήσεων εντός του πλαισίου ενδιαφέροντος του οργανισμού και την καθιστά περισσότερο αξιοποιήσιμη. Αυτό ωφελεί τους τελικούς αποδέκτες (συνήθως τα ανώτατα στελέχη ενός οργανισμού) να κατανοήσουν και να αποφασίσουν με ορθολογιστικό τρόπο βασιζόμενοι σε αποτελέσματα σχετικών μετρήσεων.

Ως παράδειγμα μπορεί να αναφερθεί η χρήση μιας μέτρησης όπως "ο μέσος όρος των επιθέσεων" για έναν ολόκληρο οργανισμό. Η μέτρηση αυτή μπορεί να έχει όλα τα παραπάνω χαρακτηριστικά (συνέπεια, αριθμητική τιμή κ.λπ) αλλά επί της ουσίας δεν βοηθά κανέναν να κάνει καλύτερα τη δουλειά του. Εάν αυτή η μέτρηση διαφοροποιηθεί και συνδεθεί με τις επιχειρηματικές υπηρεσίες που προσφέρει, όπως οι διακομιστές ηλεκτρονικού εμπορίου, θα αποτελέσει πολύ σημαντικότερο εργαλείο για τη λήψη αποφάσεων που θα αφορούν συγκεκριμένους τομείς, όπως η προστασία συγκεκριμένων διακομιστών αλλά και η φυσική προστασία του προσωπικού.

Επιπλέον των παραπάνω απαιτήσεων μπορούν να δοθούν ακόμα τρεις συμπληρωματικές απαιτήσεις για τις μεθοδολογίες μέτρησης οι οποίες βοηθούν στην ολοκληρωμένη περιγραφή της ασφάλειας ενός οργανισμού. Οι συγκεκριμένες απαιτήσεις είναι πιθανό να καλύπτονται εν μέρει από τις προηγούμενες αλλά ουσιαστικά αποτελούν ανεξάρτητες απαιτήσεις.

Βαρύτητα στην συνολική εκτίμηση

Η εκτίμηση της ασφάλειας ενός μεμονωμένου παράγοντα που επηρεάζει την ασφάλεια είναι αδιαμφισβήτητα χρήσιμη. Παρόλα αυτά, ένα επίσης σημαντικό θέμα είναι η επίδραση αυτών των μεμονωμένων εκτιμήσεων ασφάλειας σ' ολόκληρο οργανισμό.

Το χαρακτηριστικό αυτό σχετίζεται με το προηγούμενο («Σχέση με το ευρύτερο πλαίσιο») λόγω της σχετικότητας που υποδηλώνεται μεταξύ των μετρήσιμων μεγεθών και της συνολικότερης ασφάλειας του οργανισμού. Διαφέρει όμως στο γεγονός ότι η απαίτηση της συνολικής εκτίμησης περιλαμβάνει τον τρόπο και το μέγεθος με το οποίο μια συγκεκριμένη μέτρηση επηρεάζει την ασφάλεια και τη λειτουργία του οργανισμού.

Για παράδειγμα, η μέτρηση «αριθμών διακοπών ρεύματος» είναι συγκεκριμένη και σχετική με την ασφάλεια. Ο τρόπος όμως με τον οποίο αυτή επηρεάζει την λειτουργία του οργανισμού μπορεί να αποτελέσει και τη βαρύτητα του συγκεκριμένου μεγέθους. Έτσι, στην περίπτωση που δεν υπάρχει τρόπος να αντιμετωπιστεί μια διακοπή ρεύματος (π.χ. γεννήτρια) η βαρύτητα της μέτρησης αυτής σε σχέση με τη συνολική εκτίμηση της ασφάλειας θα πρέπει να είναι πολύ μεγάλη.

Θα πρέπει να διευκρινιστεί ότι η απαίτηση της συνολικής εκτίμησης μπορεί να θεωρηθεί και επέκταση των μετρήσεων, μια που πιθανώς να απαιτεί και κάποιας μορφής υπολογισμό. Περισσότερα για τον υπολογισμό της ασφάλειας και πως αυτός σχετίζεται με τις μετρήσεις αναφέρονται στο Κεφαλαίο 4.3.

Επαναληψημότητα

Η απαίτηση της επαναληψημότητας περιλαμβάνει τη μέτρηση των ίδιων μεγεθών με την εφαρμογή των ίδιων μεθόδων σε διαφορετικές χρονικές στιγμές. Η επανάληψη αυτή στοχεύει τόσο στην επαλήθευση προηγουμένων στοιχείων όσο και στη παρατήρηση και καταγραφή της εξέλιξης του συγκεκριμένου μεγέθους.

Έτσι, η επανάληψη αυτή δεν θα πρέπει να αποτελεί μέτρηση από έναν μόνο άνθρωπο αλλά να επαληθεύεται και από τις μετρήσεις διαφορετικών ανθρώπων.

Σε ότι αφορά την εξέλιξη των μεγεθών που μετρούνται, οι μετρήσεις θα πρέπει να γίνονται είτε περιοδικά, για την ανίχνευση απροσδόκητων μεταβολών είτε αμέσως μετά από κάποια γνωστή αλλαγή η οποία πιθανώς να έχει επηρεάσει την ασφάλεια.

Ειδικότερα, οι μετρήσεις θα πρέπει να υπολογίζονται με συχνότητα ανάλογη με το ρυθμό αλλαγής της διαδικασίας. Οι μεθοδολογίες με δειγματοληψίες ανά σύντομα χρονικά διαστήματα βοηθούν τους οργανισμούς να αναλύσουν την αποτελεσματικότητα της ασφάλειας σε συγκεκριμένα χρονικά διαστήματα και να είναι σε θέση να αντιδράσουν έγκαιρα σε κάθε νέο περιστατικό ασφάλειας. Φυσικά, σε μια απόφαση για το αν μια μέτρηση θα πρέπει να υπολογίζεται συχνά, θα πρέπει να λαμβάνεται υπόψη και το κόστος μέτρησης σε χρόνο και χρήμα. Εναλλακτικά μπορούν να πραγματοποιούνται και μετρήσεις πριν και μετά από κάθε αλλαγή.

Συγκρισιμότητα

Είναι πολύ σημαντικό, επίσης, να μετράμε και να παρατηρούμε τη βελτίωση ή την επιδείνωση της ασφάλειας με την πάροδο του χρόνου. Για το λόγο αυτό, τα αποτελέσματα των μετρήσεων θα πρέπει να μπορούν να είναι συγκρίσιμα με αντίστοιχα αποτελέσματα άλλων οργανισμών και διαφορετικών καταστάσεων ώστε να μπορούν να αντιπαραβάλλονται.

Όπως αναφέρθηκε και παραπάνω, ένας τρόπος είναι η χρήση κοινών μεγεθών και μονάδων μέτρησης. Επιπροσθέτως, είναι δυνατή η πραγματοποίηση μετρήσεων στα ίδια χρονικά σημεία ή χρονικά σημεία με κοινά χαρακτηριστικά, π.χ. μέτρηση του αριθμού των ληστειών την τελευταία και την πρώτη ημέρα κάθε μήνα.

4.3. Από τις μετρήσεις στον υπολογισμό της ασφάλειας

Όπως ορίζει το λεξικό του Webster στο [11] ο υπολογισμός είναι «μια σχεδιασμένη διαδικασία μετατροπής ενός ή περισσοτέρων μεγεθών σε ένα ή περισσότερα αποτελέσματα». Ο όρος υπολογισμός χρησιμοποιείται σε πλήθος επιστημών, από τον σαφώς προσδιορισμένο αριθμητικό υπολογισμό έως τον υπολογισμό αφηρημένων εννοιών ο οποίος πραγματοποιείται με τη χρήση ειδικών αλγορίθμων και τον κατάλληλο συνδυασμό παραγόντων.

Ένας άλλος, εναλλακτικός τρόπος υπολογισμού μεγεθών είναι και η στατιστική ανάλυση, π.χ. ο υπολογισμός των πιθανών αποτελεσμάτων ενός εκλογικού αποτελέσματος.

Σε κάθε περίπτωση ο υπολογισμός ενός μεγέθους ενδείκνυται σε περιπτώσεις όπου δεν είναι εφικτή η άμεση μέτρησή του ή η καταγραφή του μεγέθους. Αυτές οι περιπτώσεις περιλαμβάνουν κατά βάση αφηρημένες έννοιες οι οποίες δεν είναι ευθέως μετρήσιμες, με χαρακτηριστικό παράδειγμα αυτό της ασφάλειας.

Ο υπολογισμός της ασφάλειας διαφοροποιείται από τη μέτρηση της ασφάλειας. Ενώ η μέτρηση βασίζεται στη λήψη και αποτύπωση πρωτογενών μεγεθών, ο υπολογισμός χρησιμοποιεί τα πρωτογενή μεγέθη με συνδυαστικό τρόπο ώστε να παράγει ένα αποτέλεσμα το οποίο και αποτυπώνει την ασφάλεια.

Κρίνεται ότι λόγω της αφηρημένης φύσης της ασφάλειας των πληροφοριακών συστημάτων, μια απευθείας μέτρηση δεν θα έχει πραγματικά και αξιοποιήσιμα αποτελέσματα, μια που θα βασίζεται στις παραδοχές μεθόδων που αναφέρθηκαν στο κεφάλαιο 3.3. Ο υπολογισμός όμως της ασφάλειας μπορεί να είναι αποδοτικότερος απαλείφοντας αυτό το μειονέκτημα χρησιμοποιώντας μετρήσιμα μεγέθη.

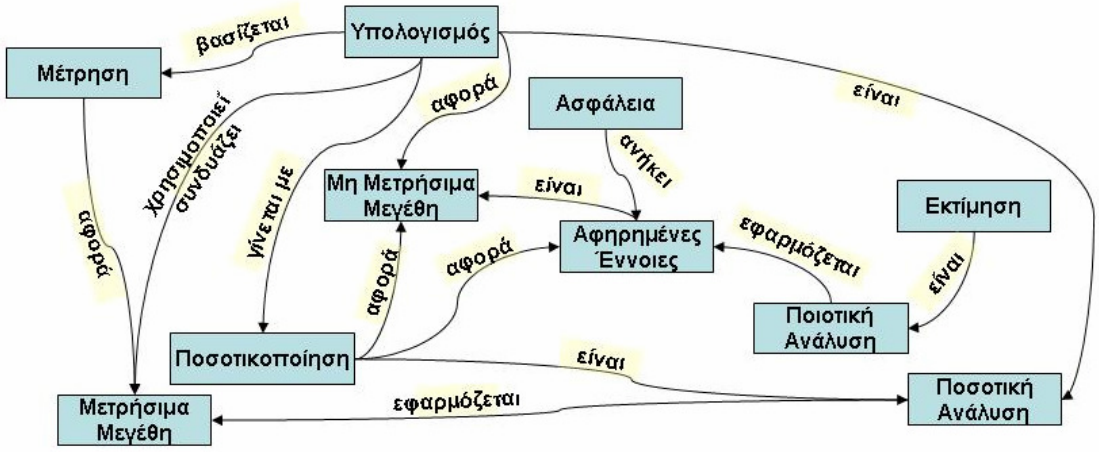
Υπάρχουν διάφορες μέθοδοι για τον υπολογισμό της ασφάλειας. Αυτές μπορούν να εξαρτώνται από τις κρίσεις και εκτιμήσεις των ερευνητών και να αποδίδονται ως κατατάξεις ή διαβαθμίσεις. Μια δεύτερη κατηγορία μεθόδων μπορεί να βασίζεται σε στατιστικές μεθόδους, οι οποίες να καταλήγουν σε μια εκτίμηση του επιπέδου της ασφάλειας. Άλλες μέθοδοι μπορούν να συνδυάζουν τη μέτρηση μεγεθών, με τον συνυπολογισμό των οποίων να προκύπτει η τιμή της ασφάλειας.

Η βέλτιστη μέθοδος υπολογισμού της ασφάλειας διαφοροποιείται ανάλογα με τις ανάγκες του κάθε οργανισμού, υπηρεσίας, υποδομής ή συστήματος. Σε κάθε περίπτωση, όμως θα πρέπει να επιλέγεται με μια διαδικασία η οποία θα βασίζεται σε σαφώς ορισμένα μεγέθη τα οποία θα έχουν επίσης σαφώς καθορισμένες σχέσεις μεταξύ τους.

Θα πρέπει ακόμα να διευκρινιστεί ότι οι μέθοδοι υπολογισμού και οι μέθοδοι μέτρησης της ασφάλειας δεν αποτελούν εναλλακτικές λύσεις μεταξύ τους, αλλά συμπληρωματικές. Δεν νοείται ακριβής μέτρηση της ασφάλειας, λόγω της αφηρημένης φύσης που την χαρακτηρίζει, αλλά και ο υπολογισμός της ασφάλειας δεν μπορεί να είναι αξιόπιστος εάν δεν βασίζεται σε μετρήσιμα μεγέθη. Κατά συνέπεια ο ερευνητής της ασφάλειας θα πρέπει να χρησιμοποιεί μεθοδολογίες μέτρησης από τις οποίες θα προκύπτουν μετρήσιμα μεγέθη. Από τον συνδυασμό των μεγεθών αυτών θα προκύπτει και το επιθυμητό μέγεθος της ασφάλειας.

Στο πλαίσιο της έρευνας και με στόχο την καλύτερη απεικόνιση των σχέσεων μεταξύ των εννοιών που αναφέρθηκαν παραπάνω, δημιουργήσαμε το Διάγραμμα 4.5 (σελ.81). Το συγκεκριμένο διάγραμμα αποτελεί μια προσαρμοσμένη έκδοση του Σημασιολογικού Μοντέλου Δεδομένων (Semantic Data Model) όπως αυτό περιγράφεται από τον Sommerville στο [12]. Χρησιμοποιεί μικρά παραλληλόγραμμα τα οποία απεικονίζουν τις έννοιες και βέλη τα οποία χαρακτηρίζουν το είδος της σχέσης μεταξύ δύο εννοιών. Η σχέση μεταξύ δύο εννοιών μπορεί να είναι μόνο μια και δεν γίνεται χρήση των

σχέσεων κληρονομικότητας του πρωτότυπου Σημασιολογικού Μοντέλου Δεδομένων.



Διάγραμμα 4.5 – Σχέσεις εννοιών ασφάλειας

Με τη χρήση του συγκεκριμένου διαγράμματος γίνεται ευκολότερα αντιληπτό ότι ο υπολογισμός της ασφάλειας γίνεται με δύο τρόπους. Είτε με τη ποσοτικοποίηση μη μετρήσιμων μεγεθών και αφηρημένων εννοιών, όπως είναι η ασφάλεια, είτε με τη χρήση των μεγεθών που μετρούνται με τις σχετικές μεθοδολογίες μέτρησης της ασφάλειας. Οι τελευταίες αφορούν μετρήσιμα μεγέθη και εφαρμόζονται ως ένα είδος ποσοτικής ανάλυσης. Επίσης, το επίπεδο της ασφάλειας μπορεί να προκύψει ως εκτίμηση των ερευνητών η οποία εφαρμόζεται ως ένα είδος ποιοτικής ανάλυσης.

4.4. Μέθοδοι υπολογισμού

Έχοντας περιγράψει τους λόγους για τους οποίους η προσέγγιση του υπολογισμού ενδείκνυται για τη ποσοτικοποίηση της ασφάλειας περισσότερο από την προσπάθεια μέτρησης αυτής, αλλά και όλο το υπόβαθρο των μεθοδολογιών μέτρησης της ασφάλειας είναι πλέον εφικτό να αναλυθούν οι τρόποι υπολογισμού της ασφάλειας. Στο πλαίσιο αυτό παρουσιάζονται δύο κλασικοί τρόποι υπολογισμού της ασφάλειας και προτείνονται δύο εναλλακτικοί οι οποίοι προέκυψαν από την έρευνα.

4.4.1. Κλασικοί τρόποι υπολογισμού

Οι μεθοδολογίες υπολογισμού της ασφάλειας που παρουσιάζονται εδώ είναι η Διαχείριση των Κινδύνων και η Ανάλυση των Κενών Ασφάλειας. Αμφότερες οι μεθοδολογίες αναφέρθηκαν στο Κεφάλαιο 3 είτε άμεσα (Διαχείριση Κινδύνων στο κεφάλαιο 3.3.6) είτε έμμεσα (Ανάλυση των Κενών Ασφάλειας στο κεφάλαιο 3.3.4 ως «Σύγκριση με Υλοποιήσεις Αναφοράς»). Παρόλο που στο Κεφάλαιο 3 κατατάχθηκαν ως μεθοδολογίες μέτρησης της ασφάλειας, λόγω των βημάτων που ακολουθούνται κατά τη χρήση τους, μπορούν να υπαχθούν και ως μέθοδοι υπολογισμού της ασφάλειας. Η παρούσα έρευνα παρουσιάζει και αναλύει στις παραγράφους που ακολουθούν τον υπολογιστικό χαρακτήρα των δύο μεθόδων.

Διαχείριση Κινδύνων

Ο πρώτος τρόπος υπολογισμού της ασφάλειας πραγματοποιείται με τη χρήση των μεθόδων υπολογισμού Διαχείρισης Κινδύνων. Η στενή σχέση της Διαχείρισης Κινδύνων με την ασφάλεια τονίζεται με τη χρήση του ορισμού της ασφάλειας όπως αυτός ορίζεται από τον Tipton στο [13]. Εκεί αναφέρεται ότι η ασφάλεια είναι ουσιαστικά η διαδικασία της διαχείρισης των κινδύνων.

Όμως, η έννοια της διαχείρισης κινδύνων είναι ευρύτερη από αυτήν που χρησιμοποιείται στο πλαίσιο της επιστήμης της πληροφορικής. Η κύρια διαφοροποίηση που υπάρχει σχετίζεται με τους στόχους που αφορούν οι κίνδυνοι στην πληροφορική και στο ευρύτερο πλαίσιο. Όπως αναφέρεται και στον ιστότοπο του προγράμματος «Δικτυωθείτε» στο [14], «Η Ασφάλεια Πληροφοριών αποκρούει τις απειλές εναντίον του πληροφοριακού και υπολογιστικού κεφαλαίου, ενώ η Διαχείριση Επιχειρηματικού Κινδύνου αφορά στην πρόληψη οικονομικών και γενικότερα εσωτερικών κρίσεων, οι οποίες μάλιστα αντικατοπτρίζονται στους συνεργάτες και το προσωπικό της επιχείρησης, γι' αυτό και επηρεάζουν παράγοντες όπως η οικονομική ασφάλεια, η νομική και εμπορική αξιοπιστία (η καλή φήμη της επιχείρησης, τόσο προς τους καταναλωτές όσο και προς άλλες επιχειρήσεις), κ.λπ.»

Έτσι, ενώ η ασφάλεια εστιάζει στην προστασία και την ακεραιότητα των πληροφοριακών πόρων, η Διαχείριση Επιχειρηματικού Κινδύνου αφορά σε γενικότερα ζητήματα, τα οποία επηρεάζουν άμεσα τη βιωσιμότητα ενός οργανισμού. Άρα, η Ασφάλεια των Πληροφοριακών Συστημάτων μπορεί να θεωρηθεί μια υποκατηγορία της Διαχείρισης Κρίσεων.

Κατά τον Olzak στο [15] η Διαχείριση Κινδύνων είναι «η μέθοδος η οποία χρησιμοποιείται συχνότερα ως ο δρόμος για την επίτευξη λογικών και κατάλληλων δαπανών για τη διαχείριση των μηχανισμών ασφάλειας». Εντούτοις, φαίνεται να υπάρχει αμφισβήτηση μεταξύ των επαγγελματιών ασφάλειας που υποστηρίζουν ότι αυτή είναι η κατάλληλη προσέγγιση και εκείνων που πιστεύουν ότι η διαχείριση του κινδύνου είναι ατελής ως μεθοδολογία, λόγω του υποκειμενικού χαρακτήρα της.

Υπάρχουν αρκετά πλεονεκτήματα σε αυτή τη μέθοδο υπολογισμού. Χρησιμοποιείται ευρέως, πολλές φορές και με δογματική ευλάβεια, ως το βασικό μέγεθος μέτρησης της ασφάλειας. Η εκτίμηση του κινδύνου πραγματοποιείται με τη χρήση συγκεκριμένων τύπων, οι οποίοι αποκαλύπτουν διαφορετικές πτυχές των κινδύνων. Στο κεφάλαιο 2.4.2 αναφέρθηκε ο πιο διαδεδομένος τύπος για τον κίνδυνο:

$$R = V \times P \times S$$

όπου : R είναι ο κίνδυνος
V είναι η αξία του παγίου
P είναι η πιθανότητα να συμβεί η απειλή
S είναι το μέγεθος της έκθεσης του παγίου

Από αυτόν το τύπο, προκύπτει ότι η διαχείριση των κινδύνων συμβάλλει στη λήψη αποφάσεων σχετικά με το πόσο «ρίσκο» μπορεί ένας οργανισμός να δεχθεί, βασιζόμενος στη πιθανότητα ότι μπορεί να συμβεί ένα ανεπιθύμητο γεγονός αλλά και την επιχειρηματική επίδραση που θα έχει από αυτό το γεγονός. Με τη χρήση αυτής της μεθόδου, μπορούν να εγκατασταθούν οι

κατάλληλοι μηχανισμοί οι οποίοι θα διασφαλίζουν μια οικονομικά λογική προστασία των επιχειρηματικών δραστηριοτήτων. Όπως είναι προφανές η κάλυψη όλων των πιθανών κινδύνων δεν αποτελεί μια συνετή προσέγγιση από οικονομικής πλευράς, συνεπώς η εφαρμογή της μεθόδου αυτής θα πρέπει να ισορροπεί μεταξύ της κάλυψης των κινδύνων αλλά και των ουσιαστικών κερδών.

Ένα άλλο θετικό της μεθόδου αυτής είναι ότι ακολουθεί τον τρόπο με τον οποίο λαμβάνονται οι επιχειρηματικές αποφάσεις, επιτρέποντας στους υπεύθυνους ασφάλειας να «μιλήσουν» τη γλώσσα των ανώτατων στελεχών που εστιάζουν στις επιχειρηματικές και λογιστικές πλευρές του οργανισμού. Ακόμα και για τους ίδιους τους υπεύθυνους ασφάλειας είναι ιδιαίτερα χρήσιμο να γνωρίζουν ποιοι κίνδυνοι αποτελούν τις προτεραιότητές τους με βάση τις επιχειρηματικές ανάγκες.

Εκτός όμως από τα πλεονεκτήματα, υπάρχουν και αρκετά μειονεκτήματα σε αυτή τη μέθοδο υπολογισμού. Η χρήση του συγκεκριμένου τύπου διασφαλίζει μεν τη συνέπεια στον τρόπο υπολογισμού, αποκαλύπτει όμως και τον υποκειμενικό της χαρακτήρα με την εισαγωγή του υποκειμενικού μεγέθους της πιθανότητας.

Όπως υποστηρίζεται και από τον Parker στο [16], πολλές φορές τα στελέχη ενός οργανισμού προτιμούν να αποδέχονται τους κινδύνους ασφάλειας, εάν η κάλυψή τους απαιτεί προσωπικό το οποίο θα μπορούσε να απασχοληθεί με την επίτευξη ενός επιχειρηματικού στόχου. Επίσης, η μεθοδολογία της διαχείρισης κινδύνων βασίζεται στην προστασία από κάτι που δεν έχει συμβεί ακόμα. Το γεγονός αυτό κάνει δύσκολο την ποσοτικοποίηση των επιχειρηματικών επιπτώσεων για κάποια περιστατικά ασφάλειας τα οποία είτε δεν έχουν συμβεί ποτέ είτε συμβαίνουν πολύ σπάνια.

Επί της ουσίας η μείωση των κινδύνων βασίζεται σε υποκειμενικές εκτιμήσεις και δεν μπορεί να αποτελέσει αξιόπιστη και αξιοποιήσιμη μέθοδο υπολογισμού

της ασφάλειας. Όπως αναφέρει ο Parker στο [16], ο κίνδυνος δεν είναι υπολογίσιμος, επειδή η συχνότητα και οι επιδράσεις των μελλοντικών περιστατικών είναι εξαρτώμενες από άγνωστες και συνεχώς μεταβλητές παραμέτρους. Οι παράμετροι αυτοί μπορεί να είναι η ύπαρξη επιτιθέμενων με άγνωστες ικανότητες, γνώσεις, πόρους, δικαιώματα πρόσβασης, κίνητρα και στόχους, οι οποίοι μπορεί να ενεργούν από άγνωστες φυσικές θέσεις σε τυχαία χρονικά σημεία. Επιπλέον, η διαρκώς μεταβαλλόμενη φύση των απειλών επηρεάζει και τη διάρκεια της ισχύος των αποτελεσμάτων της μεθόδου. Πολλές φορές αυτή η δυναμική φύση των απειλών καθιστά πρακτικά αδύνατη την εκτίμηση τόσο της πιθανότητας να συμβούν όσο και των αντίστοιχων οικονομικών επιδράσεων.

Συμπερασματικά, η μέθοδος της διαχείρισης των κινδύνων, δεν είναι δυνατόν να είναι ακριβής, όπως ακριβής δεν μπορεί να είναι και η εκτίμηση των οικονομικών απωλειών από ένα περιστατικό ασφάλειας ή η εκτίμηση της πιθανότητας να συμβεί το συγκεκριμένο περιστατικό. Σε κάθε περίπτωση, η διαχείριση των κινδύνων δεν μπορεί να θεωρηθεί πάντα αξιόπιστη και συνεπής ως προς τα αποτελέσματά της.

Ανάλυση κενών ασφάλειας

Ο δεύτερος τρόπος υπολογισμού της ασφάλειας πραγματοποιείται με τη χρήση των μεθόδων Ανάλυσης των Κενών Ασφάλειας (Gap Analysis). Η ανάλυση των κενών ασφάλειας είναι ουσιαστικά ο προσδιορισμός των κενών και των αδυναμιών που σχετίζονται με τις πολιτικές, τις διαδικασίες, τις πληροφοριακές υποδομές, τις επιχειρηματικές υπηρεσίες, τις εφαρμογές και τα πληροφοριακά συστήματα υπό την οπτική της ασφάλειας.

Υπάρχει μια πληθώρα προσεγγίσεων για αυτόν τον προσδιορισμό, αλλά μπορούν να περιγραφούν όλες με ένα γενικό τρόπο. Η διαδικασία ξεκινά με κάποιον αναλυτή, ο οποίος καταγράφει και αναλύει τα παραπάνω στοιχεία (πολιτικές, υποδομές κ.λπ.) και τα συγκρίνει με κάποιο ή κάποια κείμενα αναφοράς. Τα κείμενα αυτά μπορούν να είναι διεθνή πρότυπα, εθνική ή

διεθνής νομοθεσία, βέλτιστες πρακτικές, κανονιστικά και ρυθμιστικά πλαίσια, εσωτερικοί κανονισμοί και πολιτικές, παρατηρήσεις της εσωτερικής επιθεώρησης κ.α. Παραδείγματα τέτοιων κειμένων είναι:

- BS7799 / ISO17799: Αποτελούν πρότυπα που σχετίζονται με την ασφάλεια πληροφοριακών συστημάτων. Το πρότυπο αρχικά ξεκίνησε από το Ηνωμένο Βασίλειο ως BS 7799 και αναπτύχθηκε από το Βρετανικό Ίδρυμα Προτύπων. Αργότερα, μετατράπηκε στο διεθνές πρότυπο ISO IEC 17799.
- ISO 27000 series: Διεθνές πρότυπο για την ασφάλεια της πληροφορίας το οποίο αντικατέστησε το ISO 17799.
- TCSEC (Trusted Computer System Evaluation Criteria): Πρότυπο για την εκτίμηση της αποδοτικότητας των μηχανισμών ασφάλειας τα οποία είναι ενσωματωμένα σε αυτοματοποιημένα συστήματα επεξεργασίας δεδομένων.
- ITIL (Information Technology Infrastructure Library): Συλλογή βέλτιστων πρακτικών (αναφέρθηκε στο Κεφάλαιο 3.2.1)
- Basel II: Ευρωπαϊκοί κανόνες κεφαλαιακής επάρκειας για χρηματοπιστωτικούς οργανισμούς.
- PCI: Πρότυπο ασφάλειας το οποίο περιγράφει τις τεχνικές και λειτουργικές απαιτήσεις και προδιαγραφές που διασφαλίζουν την προστασία των προσωπικών δεδομένων και ιδιαίτερα των δεδομένων που αφορούν σε παροχή οικονομικών υπηρεσιών.
- Sarbanes-Oxley Act: Αποτελεί μια από τις σημαντικότερες αμερικάνικες νομοθεσίες σχετικά με τις εταιρικές διαδικασίες, τα οικονομικά στοιχεία και τα δημόσια λογιστικά.
- HIPAA (Health Insurance Portability and Accountability Act): Αποτελεί μια ομαδοποίηση των αμερικάνικων κανονισμών, που αφορούν την καταπολέμηση της σπατάλης, της απάτης και της κατάχρησης σε φορείς παροχής υγειονομικής περίθαλψης και ασφάλισης υγείας.
- COPPA (Children's Online Privacy Protection Act): Αμερικάνικος νόμος περί προστασίας του απορρήτου των παιδιών στο Internet.

Στις περιπτώσεις όπου ο αναλυτής διαπιστώνει κάποια διαφορά μεταξύ των στοιχείων που έχουν υλοποιηθεί και των κειμένων που χρησιμοποίησε, αυτή καταγράφεται ως κενό ασφάλειας. Όταν η διαδικασία ολοκληρωθεί το μέγεθος της ασφάλειας μπορεί να υπολογιστεί ως το ποσοστό των κενών επί των συνολικών κανόνων του κειμένου ή των κειμένων αναφοράς. Όσο μεγαλύτερο είναι το ποσοστό αυτό, τόσο μεγαλύτερο είναι και το μέγεθος της ασφάλειας. Για τα όποια κενά μεταξύ των κειμένων αναφοράς και της πραγματικής υλοποίησης θα πρέπει να παρθούν κάποια μέτρα τα οποία θα καλύψουν αυτά τα κενά.

Πρέπει να σημειωθεί ότι οι τύποι των συγκρίσεων είναι δύο: Ο πρώτος αφορά τη σύγκριση μεταξύ μιας εξωτερικής πηγής (προτύπου, νομοθεσίας κ.λπ.) και των πολιτικών και διαδικασιών ενός οργανισμού. Η σύγκριση αυτή συνήθως γίνεται από κάποιον πιστοποιημένο αναλυτή στο αντίστοιχο πρότυπο (π.χ. ISO 27000), μπορεί να οδηγήσει στην αλλαγή των πολιτικών ασφάλειας ενός οργανισμού ενώ είναι πολύ πιθανό να επηρεάζει και την τεχνική υλοποίηση (υποδομές, συστήματα κ.λπ.) εντός του οργανισμού.

Ο δεύτερος τύπος σύγκρισης αποτελεί μια εσωτερική διαδικασία ενός οργανισμού, αφορά τη σύγκριση μεταξύ της τεχνικής υλοποίησης (εφαρμογές, υποδομές, συστήματα, κ.λπ.) εντός του οργανισμού και μιας εταιρικής πολιτικής ασφάλειας ενώ πραγματοποιείται συνήθως από κάποιο εξειδικευμένο εσωτερικό ελεγκτή. Τα όποια κενά καταγραφούν οδηγούν συνήθως σε αλλαγές που αφορούν μόνο στην τεχνική υλοποίηση και παραμετροποίηση των συστημάτων εντός του οργανισμού.

Γίνεται εύκολα αντιληπτό ότι παρουσιάζεται αυξημένη δυσκολία στην κάλυψη των κενών του πρώτου τύπου σύγκρισης σε σύγκριση με τον δεύτερο λόγω των αυξημένων απαιτήσεων για αλλαγές τόσο σε επίπεδο πολιτικών όσο και σε επίπεδο υλοποίησης.

Η αξιολόγηση της συγκεκριμένης διαδικασίας ως μεθοδολογία υπολογισμού της ασφάλειας, παρουσιάζει μια σειρά από θετικά αλλά και αρνητικά στοιχεία. Αντίθετα με τη μέθοδο Διαχείρισης των Κινδύνων, η προσέγγιση της Ανάλυσης των Κενών Ασφάλειας, επηρεάζεται λιγότερο από τις υποκειμενικές εκτιμήσεις των αναλυτών. Η υποκειμενικότητα της συγκεκριμένης μεθόδου είναι σαφώς μικρότερη λόγω της χρήσεων τυποποιημένων ερωτήσεων, οι οποίες προκύπτουν από τις απαιτήσεις των κειμένων αναφοράς. Στους αναλυτές εναπόκειται η σωστή απόδοση των απαιτήσεων των κειμένων αναφοράς σε ερωτήσεις μερικής άγνοιας με απαντήσεις οι οποίες θα επιδεικνύουν συνέπεια, δηλαδή δεν θα αλλάζουν ανάλογα με το άτομο που συμμετέχει στη διαδικασία.

Είναι ακόμα πιθανό να υπάρχει δυσκολία στη σύγκριση όλων των στοιχείων και παραγόντων μιας τεχνικής υλοποίησης και των αντιστοίχων κειμένων αναφοράς, λόγω του μεγέθους, της πολυπλοκότητας και των διαθέσιμων πόρων (χρόνος, χρήμα και προσωπικό) που μπορεί να εμφανίζει ο κάθε οργανισμός.

Ένα επιπλέον, και ίσως το πιο σημαντικό, σημείο για τη δυσκολία χρήσης της μεθόδου Ανάλυσης των Κενών Ασφάλειας ως μεθοδολογία υπολογισμού της ασφάλειας είναι το γεγονός ότι δεν λαμβάνεται υπόψη η προτεραιότητα που έχει κάθε κενό ασφάλειας για τον οργανισμό. Αυτό σημαίνει ότι ένα κενό ασφάλειας το οποίο καταγράφεται από την παραπάνω διαδικασία δεν αξιολογείται ως προς το μέγεθος της επίδρασης του στις επιχειρηματικές δραστηριότητες του οργανισμού. Με αυτόν τον τρόπο, ο αναλυτής δεν μπορεί να επισημάνει ποιες θα πρέπει να είναι οι προτεραιότητες μεταξύ των κενών που θα πρέπει να καλύψει ο οργανισμός.

4.4.2. Εναλλακτικοί τρόποι υπολογισμού

Οι εναλλακτικοί τρόποι υπολογισμού της ασφάλειας που αναφέρονται σε αυτή τη παράγραφο αποτελούν προσπάθειες κάλυψης των κενών και των αδυναμιών των παραπάνω προσεγγίσεων. Παρουσιάζονται δύο τρόποι

υπολογισμού οι οποίοι αποτελούν ένα μέρος των αποτελεσμάτων της έρευνας για την ποσοτικοποίηση, μέτρηση και τον υπολογισμό της ασφάλειας. Ο πρώτος τρόπος επιχειρεί να υπολογίσει την ασφάλεια με τον συνδυασμό των δομικών στοιχείων της ασφάλειας, ενώ ο δεύτερος προσεγγίζει την ασφάλεια ως μέγεθος το οποίο υπολογίζεται με τον συνδυασμό κάποιων εύκολα μετρήσιμων παραγόντων οι οποίοι σχετίζονται έμμεσα με την ασφάλεια.

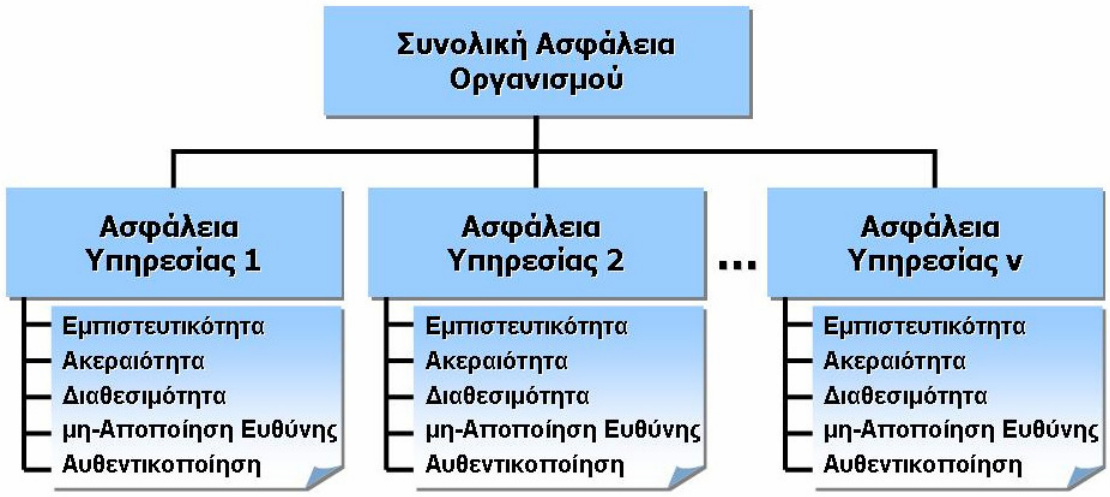
4.4.2.1. Υπολογισμός με τον συνδυασμό των δομικών στοιχείων της ασφάλειας

Η πρώτη προσέγγιση υπολογισμού της ασφάλειας που προέκυψε από την έρευνα, αντιμετωπίζει την ασφάλεια ως ένα υπολογίσιμο μέγεθος το οποίο μπορεί να προκύψει με τον συνδυασμό μετρήσιμων μεγεθών.

Η βασική αρχή του μοντέλου υπολογισμού βασίζεται στον υπολογισμό της ασφάλειας των υπηρεσιών ενός οργανισμού, θεωρώντας ότι η διοίκηση ενός οργανισμού ωφελείται περισσότερο από τη γνώση του επιπέδου της ασφάλειας των επιμέρους προσφερομένων υπηρεσιών και λιγότερο από την απομονωμένη οπτική που δίνεται από τον υπολογισμό της ασφάλειας ολόκληρου του οργανισμό. Η προσέγγιση αυτή ενισχύεται εάν κανείς αναλογιστεί την ανάλογη περίπτωση με τον υπολογισμό της Απόδοσης Μιας Επένδυσης (Return On Investment / ROI). Και στη περίπτωση αυτή έχει πολύ μεγαλύτερη αξία να είναι γνωστή η ROI των επιμέρους υπηρεσιών παρά η απόδοση της επένδυσης ολόκληρου του οργανισμού. Θα πρέπει να τονιστεί ότι με τον όρο «υπηρεσία» εννοείται μια επιχειρηματική υπηρεσία, όπως η υπηρεσία του ηλεκτρονικού ταχυδρομείου και η ηλεκτρονική τραπεζική (αμφότερα παραδείγματα από ένα τραπεζικό οργανισμό) και όχι καθαυτές οι τεχνολογικές υπηρεσίες. Άλλα παραδείγματα των υπηρεσιών των οποίων η ασφάλεια υπολογίζεται είναι η υπηρεσία ασφάλειας ενός κτηρίου αλλά και οι καταθέσεις σε μια τράπεζα.

Η συγκεκριμένη προσέγγιση βασίζεται, επίσης, στην παραδοχή ότι οι αφηρημένες έννοιες μπορούν να υπολογιστούν έμμεσα με τον συνδυασμό των

παραγόντων που τις αποτελούν. Η αφηρημένη έννοια της υγείας χρησιμοποιεί κάποια από τα συμπτώματα όπως η πίεση, η θερμοκρασία και ο σφυγμός για να υπολογιστεί το επίπεδό της. Αντίστοιχα, ο υπολογισμός της ασφάλειας μπορεί να πραγματοποιηθεί έμμεσα με τον συνδυασμό των παραγόντων που την αποτελούν. Αυτοί οι παράγοντες αποτελούν τα δομικά στοιχεία της ασφάλειας και προκύπτουν από τον ορισμό της ασφάλειας που δόθηκε στο Κεφάλαιο 2. Εκεί διακρίνονται τα πέντε δομικά στοιχεία της ασφάλειας: η Ακεραιότητα, η Διαθεσιμότητα, η Εμπιστευτικότητα, η μη-Αποποίηση της Ευθύνης και η Αυθεντικοποίηση, τα οποία αποτελούν και τα μεγέθη που θα πρέπει να ποσοτικοποιηθούν ή να μετρηθούν άμεσα. Η ποσοτικοποίηση των δομικών στοιχείων πραγματοποιείται με τρόπο που στοχεύει στην αντικειμενικότητα των αποτελεσμάτων, προσπαθώντας να καταστήσει την όλη διαδικασία συνεπή με τις απαιτήσεις των μεθοδολογιών μέτρησης της ασφάλειας όπως αυτές αναλύθηκαν στο Κεφάλαιο 4.2.5. Το αποτέλεσμα της ποσοτικοποίησης, καταλήγει στα μεγέθη των επιμέρους στοιχείων τα οποία και συνθέτονται για τον υπολογισμό της ασφάλειας της κάθε υπηρεσίας. Με την ολοκλήρωση του υπολογισμού κάθε επιμέρους υπηρεσίας, είναι εφικτός και ο υπολογισμός της συνολικής ασφάλειας του οργανισμού. Το διάγραμμα 4.6 παρουσιάζει μια απεικόνιση της ιεραρχίας που ακολουθείται από την συγκεκριμένη μεθοδολογία για τον υπολογισμό της ασφάλειας.



Διάγραμμα 4.6 – Ιεραρχία μεθοδολογίας υπολογισμού ασφάλειας

Ουσιαστικά, αναγνωρίζοντας ότι ο υπολογισμός της ασφάλειας ενός οργανισμού είναι ένα σύνθετο πρόβλημα, η ανάλυση του σε ευκολότερα επιμέρους προβλήματα μπορεί να συνεισφέρει και να απλοποιήσει τη λύση του. Ως επιμέρους προβλήματα ορίζονται ο υπολογισμός της ασφάλειας των επιμέρους υπηρεσιών. Όπως όμως αναφέρθηκε, ακόμα και το πρόβλημα της μέτρησης της ασφάλειας μιας μόνο υπηρεσίας εξακολουθεί να είναι ένα σύνθετο πρόβλημα, διότι ο βασικός ισχυρισμός ότι η ασφάλεια δεν μπορεί να μετρηθεί άμεσα ισχύει και σε αυτή τη περίπτωση. Συνεπώς, γίνεται προσπάθεια να απλοποιήσουμε και αυτό το σύνθετο πρόβλημα περαιτέρω, με τη χρήση των δομικών στοιχείων τα οποία μπορούν να μετρηθούν ευκολότερα, με πιο άμεσο και αντικειμενικό τρόπο.

Η μέθοδος αυτή δίνει έμφαση στην απαίτηση της συνέπειας και της αντικειμενικότητας, όπως αυτή αναφέρθηκε στο Κεφάλαιο 4.2.5. Για να διασφαλιστεί η αντικειμενική φύση των μετρήσεων, η μέθοδος χρησιμοποιεί ιστορικά στοιχεία τα οποία μπορούν να αντληθούν με την υποβολή συγκεκριμένου τύπου ερωτήσεων σχετικών με την ασφάλεια των υπηρεσιών. Αυτές οι ερωτήσεις θα πρέπει να στοχεύουν να έχουν μονοσήμαντες απαντήσεις.

Ένα παράδειγμα μιας τέτοιας ερώτησης μπορεί να είναι: «Ποιος είναι ο συνολικός αριθμός Υ των προσπαθειών παραβίασης της εμπιστευτικότητας για την υπηρεσία του ηλεκτρονικού ταχυδρομείου;». Ένα άλλο σχετικό παράδειγμα είναι: «Ποιος είναι ο συνολικός αριθμός Χ των **αποτυχημένων** προσπαθειών παραβίασης της εμπιστευτικότητας για την υπηρεσία του ηλεκτρονικού ταχυδρομείου;». Και στα δύο παραδείγματα προκύπτει ένας ακέραιος αριθμός με μια μονάδα μέτρησης (αριθμός των προσπαθειών) ο οποίος σχετίζεται με την εμπιστευτικότητα (ένα από τα δομικά στοιχεία της ασφάλειας), το οποίο είναι ένας από τους παράγοντες της ασφάλειας του ηλεκτρονικού ταχυδρομείου (δηλ. συγκεκριμένης υπηρεσίας).

Μπορούν να τεθούν πολλοί τύποι παρόμοιων ερωτήσεων, η επιλογή των οποίων είναι στην ευχέρεια του χρήστη της μεθοδολογίας. Αυτή η πληθώρα επιλογών οφείλεται στη διαφορετικότητα των υπηρεσιών και της δομής κάθε οργανισμού από τους άλλους. Σε κάθε περίπτωση, η εφαρμογή της μεθόδου απαιτεί την υποβολή μονοσήμαντων ερωτήσεων οι οποίες θα έχουν αποκλειστικά αντικειμενικές απαντήσεις.

Οι πηγές των απαντήσεων μπορούν επίσης να διαφέρουν από οργανισμό σε οργανισμό. Ακόμα και έτσι όμως, υπάρχει μια σειρά από πηγές αντικειμενικών απαντήσεων, οι οποίες συναντώνται σε πολλούς οργανισμούς. Αυτοί μπορεί να είναι οι ελεγκτές δικτυακής κίνησης όπως είναι οι μηχανισμοί ανίχνευσης εισβολών, οι κάμερες ασφάλειας ενός κτηρίου, οι φύλακες εισόδου, τα στατιστικά των εξυπηρετητών ή, για το παραπάνω παράδειγμα του ηλεκτρονικού ταχυδρομείου, το σύστημα φιλτραρίσματος των ηλεκτρονικών μηνυμάτων.

Ο αναλυτής – χρήστης της μεθόδου αυτής θα πρέπει να θυμάται ότι αυτές οι ερωτήσεις είναι πολύ σημαντικές, αφιερώνοντας σημαντικό χρόνο για την προετοιμασία τους. Μια χρήσιμη οδηγία για τη διευκόλυνση της όλης διαδικασίας είναι ο διαχωρισμός πιθανών υπό-υπηρεσιών για τις οποίες ο καθορισμός των σχετικών ερωτήσεων μπορεί να πραγματοποιηθεί ευκολότερα.

Συμπληρωματικά των παραπάνω, θεωρείται χρήσιμο να δημιουργηθεί μια μέθοδος για την ανεύρεση και τον προσδιορισμό όλων των υπηρεσιών που προσφέρονται από τον οργανισμό. Ένας τρόπος να γίνει αυτό είναι η ξεχωριστή εξέταση των τμημάτων του οργανισμού. Η παροχή μιας υπηρεσίας μπορεί να πραγματοποιείται αποκλειστικά από ένα τμήμα του οργανισμού, είναι όμως δυνατό να απαιτείται η συμμετοχή πολλαπλών τμημάτων τα οποία έχουν διαφορετικές λειτουργίες. Στην περίπτωση αυτή κάθε υπηρεσία που καταγράφεται θα πρέπει να αντιπαραβάλλεται με κάθε προηγούμενη που πιθανώς να έχει αναφερθεί και από κάποιο άλλο τμήμα.

Ένα άλλο σημαντικό ζήτημα είναι ότι κάθε δομικό στοιχείο μπορεί να θεωρηθεί το ίδιο σημαντικό για την ασφάλεια της υπηρεσίας, ή μπορεί να αποφασιστεί ότι κάποιες υπηρεσίες επηρεάζονται περισσότερο από κάποιο στοιχείο και λιγότερο από κάποια άλλα. Στη δεύτερη περίπτωση θα πρέπει οι απαντήσεις να σταθμιστούν ως προς τη σημαντικότητά τους και τον βαθμό επηρεασμού της υπηρεσίας.

Με τη συγκέντρωση όλων των ερωτήσεων και των αντιστοίχων απαντήσεων, είναι πλέον δυνατό να υπολογιστεί το μέγεθος της ασφάλειας για κάθε υπηρεσία. Αυτό γίνεται με τη χρήση των ερωτήσεων ανά ζεύγη, όπως στο προηγούμενο παράδειγμα του ηλεκτρονικού ταχυδρομείου. Από τον λόγο των Χ προς Υ προκύπτει ένα ποσοστό. Ο σταθμισμένος μέσος όρος των ποσοστών κάθε δομικού στοιχείου αποτελεί και το επίπεδο της ασφάλειας της συγκεκριμένης υπηρεσίας.

Για την καλύτερη κατανόηση της μεθοδολογίας παρατίθεται και ένα υποθετικό παράδειγμα ενός μεγάλου οργανισμού με δέκα χιλιάδες υπαλλήλους για το οποίο εξετάζεται το επίπεδο της ασφάλειας της υπηρεσίας διαχείρισης ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (anti-spam) του ηλεκτρονικού ταχυδρομείου. Η συγκεκριμένη υπηρεσία παρέχεται από το Τμήμα Πληροφορικής σε όλους τους υπαλλήλους του οργανισμού.

Για τον υπολογισμό της ασφάλειας θα πρέπει να υποβληθούν ερωτήσεις που να σχετίζονται με το anti-spam και οι απαντήσεις να μην επιδέχονται αμφισβήτηση. Δύο τέτοιες ερωτήσεις μπορεί να είναι:

- Α. Ποιος είναι ο αριθμός όλων των spam emails που εντόπισε ο μηχανισμός anti-spam του οργανισμού εντός του τελευταίου έτους;

και

- Β. Ποιος είναι ο αριθμός των spam emails που δεν εντόπισε ο μηχανισμός anti-spam του οργανισμού και τελικά παραδόθηκαν στους υπαλλήλους;

Η ερώτηση Α μπορεί να απαντηθεί από τους διαχειριστές της υπηρεσίας ενώ η ερώτηση Β μπορεί να απαντηθεί με ένα ερωτηματολόγιο που θα στοχεύει στους τελικούς χρήστες – υπαλλήλους. Σημειώνεται ότι οι δύο ερωτήσεις θα πρέπει να εστιάσουν σε κάθε ένα από τα πέντε δομικά στοιχεία της ασφάλειας. Έτσι το ερώτημα Α μετατρέπεται στα εξής:

- Α1. Ποιος είναι ο αριθμός όλων των spam emails που εντόπισε ο μηχανισμός anti-spam του οργανισμού εντός του τελευταίου έτους και αποτέλεσαν απειλή για την Αυθεντικοποίηση;

- Α2. Ποιος είναι ο αριθμός όλων των spam emails που εντόπισε ο μηχανισμός anti-spam του οργανισμού εντός του τελευταίου έτους και αποτέλεσαν απειλή για τη μη-Αποποίηση της Ευθύνης;

- Α3. Ποιος είναι ο αριθμός όλων των spam emails που εντόπισε ο μηχανισμός anti-spam του οργανισμού εντός του τελευταίου έτους και αποτέλεσαν απειλή για την Εμπιστευτικότητα;

- Α4. Ποιος είναι ο αριθμός όλων των spam emails που εντόπισε ο μηχανισμός anti-spam του οργανισμού εντός του τελευταίου έτους και αποτέλεσαν απειλή για την Ακεραιότητα;

- Α5. Ποιος είναι ο αριθμός όλων των spam emails που εντόπισε ο μηχανισμός anti-spam του οργανισμού εντός του τελευταίου έτους και αποτέλεσαν απειλή για τη Διαθεσιμότητα;

Με παρόμοιο τρόπο υποβλήθηκε στους χρήστες και το ερώτημα Β για κάθε ένα από τα δομικά στοιχεία της ασφάλειας:

- Β1. Ποιος είναι ο αριθμός των spam emails που δεν εντόπισε ο μηχανισμός anti-spam του οργανισμού, παραδόθηκαν στους υπαλλήλους και αποτέλεσαν απειλή για την Αυθεντικοποίηση;

- B2. Ποιος είναι ο αριθμός των spam emails που δεν εντόπισε ο μηχανισμός anti-spam του οργανισμού, παραδόθηκαν στους υπαλλήλους και αποτέλεσαν απειλή για τη μη-Αποποίηση της Ευθύνης;

- B3. Ποιος είναι ο αριθμός των spam emails που δεν εντόπισε ο μηχανισμός anti-spam του οργανισμού, παραδόθηκαν στους υπαλλήλους και αποτέλεσαν απειλή για την Εμπιστευτικότητα;

- B4. Ποιος είναι ο αριθμός των spam emails που δεν εντόπισε ο μηχανισμός anti-spam του οργανισμού, παραδόθηκαν στους υπαλλήλους και αποτέλεσαν απειλή για την Ακεραιότητα;

- B5. Ποιος είναι ο αριθμός των spam emails που δεν εντόπισε ο μηχανισμός anti-spam του οργανισμού, παραδόθηκαν στους υπαλλήλους και αποτέλεσαν απειλή για τη Διαθεσιμότητα;

Τα πρωτογενή δεδομένα είναι οι απαντήσεις που ελήφθησαν και αναπαρίστανται ως ποσοστά:

$$\text{Δομικό στοιχείο } x = \frac{\text{Αριθμός spam που εντοπίσθηκαν και αποτελούν απειλή } x}{\text{Συνολικός αριθμός spam που αποτελούν απειλή } x}$$

Όπου x είναι κάθε ένα από τα δομικά στοιχεία της ασφάλειας (Ακεραιότητα, Διαθεσιμότητα, Εμπιστευτικότητα, μη-Αποποίηση Ευθύνης και Αυθεντικοποίηση). Ο «Αριθμός spam που εντοπίσθηκαν και αποτελούν απειλή x» είναι ο αριθμός που προκύπτει για κάθε μια από τις απαντήσεις Ax, ενώ ο «Συνολικός αριθμός spam που αποτελούν απειλή x» είναι το άθροισμα των spam που είτε εντοπίστηκαν είτε όχι αποτελούν απειλή. Ο τελευταίος αριθμός προκύπτει από το άθροισμα των απαντήσεων Ax και Bx.

Τα υποθετικά αποτελέσματα του παραδείγματος παρουσιάζονται στον Πίνακα 4.10:

Ερωτήσεις	Απαντήσεις
A. Spam emails που εντοπίστηκαν	**2.007.500**
A1.Αυθεντικοποίηση	854.255
A2.Μη-Αποποίηση Ευθύνης	64.069
A3.Εμπιστευτικότητα	384.415
A4.Ακεραιότητα	234.920
A5.Διαθεσιμότητα	469.840
B. Spam emails που δεν εντοπίστηκαν	**126.402**
A1.Αυθεντικοποίηση	42.713
A2.Μη-Αποποίηση Ευθύνης	5
A3.Εμπιστευτικότητα	41.463
A4.Ακεραιότητα	21.356
A5.Διαθεσιμότητα	20.865
A+B. Συνολικά spam emails	**2.133.902**
A1+B1.Αυθεντικοποίηση	896.968
A2+B2.Μη-Αποποίηση Ευθύνης	64.074
A3+B3.Εμπιστευτικότητα	425.878
A4+B4.Ακεραιότητα	256.277
A5+B5.Διαθεσιμότητα	490.705

Πίνακας 4.10 – Αποτελέσματα παραδείγματος υπολογισμού ασφάλειας (α)

Με την ολοκλήρωση αυτής της διαδικασίας, η μεθοδολογία είναι σε θέση όχι μόνο να αποτυπώσει το μέγεθος της ασφάλειας αλλά να συγκρίνει το τρέχον μέγεθος με τον στόχο – επιθυμητό επίπεδο ασφάλειας που πιθανώς να έχει τεθεί, για κάθε παράγοντα x. Ο στόχος αυτός συνήθως αποτελεί απόφαση κάποιου υψηλόβαθμου στελέχους – ιδιοκτήτη των υπηρεσιών και των πληροφοριών που ανταλλάσσονται.

Το επιθυμητό επίπεδο ασφάλειας πρέπει να αποτελεί ένα ρεαλιστικό στόχο λαμβάνοντας υπόψη ότι ένας απόλυτος στόχος απαιτεί και μια σημαντική οικονομική επένδυση.

Στο σημείο αυτό θα πρέπει επίσης να αποφασιστεί εάν για τη συγκεκριμένη υπηρεσία κάθε παράγοντας x επηρεάζει το ίδιο. Εάν αυτό δεν ισχύει θα πρέπει

να υπολογιστεί το σταθμισμένο ποσοστό – στόχος για κάθε x. Αυτό γίνεται με τον παρακάτω τύπο:

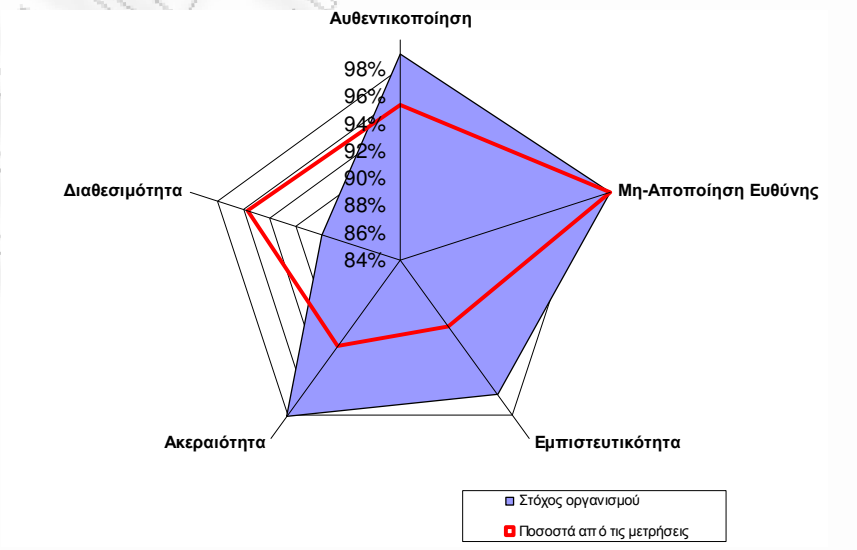
$$\text{Σταθμισμένος στόχος για το x} = \frac{\text{Στόχος όπως ορίστηκε από τον οργανισμό για το x}}{\text{Άθροισμα στόχων για όλους τους παράγοντες}}$$

Στη συνέχεια σταθμίζεται η μέτρηση για κάθε δομικό στοιχείο x, η οποία είναι το γινόμενο της πραγματικής απάντησης (μέτρησης) με το σταθμισμένο στόχο. Η τελική τιμή της ασφάλειας είναι το άθροισμα των σταθμισμένων μετρήσεων όλων των δομικών στοιχείων. Τα αποτελέσματα του παραδείγματος παρουσιάζονται στον Πίνακα 4.11.

Δομικό Στοιχείο Ασφάλειας	Στόχος οργανισμού	Ποσοστά από τις μετρήσεις (απαντήσεις)	Σταθμισμένος στόχος	Σταθμισμένη μέτρηση
Αυθεντικοποίηση	99%	95%	20%	**20%**
Μη-Αποποίηση Ευθύνης	100%	100%	21%	**21%**
Εμπιστευτικότητα	96%	90%	20%	**18%**
Ακεραιότητα	98%	92%	20%	**19%**
Διαθεσιμότητα	90%	96%	19%	**18%**
	Ασφάλεια Υπηρεσίας anti-spam			**95%**

Πίνακας 4.11 – Αποτελέσματα παραδείγματος υπολογισμού ασφάλειας (β)

Για την καλύτερη αναπαράσταση των αποτελεσμάτων, τα αριθμητικά αποτελέσματα παρουσιάζονται στο διάγραμμα 4.7 – τύπου ραντάρ.



Διάγραμμα 4.7 – Αποτελέσματα παραδείγματος υπολογισμού ασφάλειας (γ)

Στο διάγραμμα αυτό υπάρχουν 5 άξονες και ο καθένας αναπαριστά το ποσοστό καθενός από τους πέντε παράγοντες. Το διάγραμμα παρουσιάζει με ένα πολύ γρήγορο τρόπο τόσο την τρέχουσα κατάσταση όσο και το επιθυμητό επίπεδο στόχο για τη συγκεκριμένη υπηρεσία. Η έντονη γραμμή αναπαριστά το τρέχον επίπεδο ασφάλειας για την υπηρεσία του anti-spam και η γραμμοσκιασμένη περιοχή τον αντίστοιχο στόχο του οργανισμού.

Παρατηρώντας το διάγραμμα μπορεί εύκολα να βγει το συμπέρασμα ότι η τρέχουσα κατάσταση είναι πολύ κοντά στην επιθυμητή για όλους τους παράγοντες. Μολαταύτα, υπάρχουν κάποιες αποκλίσεις κυρίως στα στοιχεία της ακεραιότητας και της εμπιστευτικότητας, τα οποία χρήζουν της προσοχής του οργανισμού. Αντίθετα ο παράγοντας της διαθεσιμότητας βρίσκεται σε καλύτερο σημείο από το επιθυμητό και δεν απαιτείται κάποια περαιτέρω επένδυση. Η συνολική ασφάλεια για την υπηρεσία υπολογίστηκε στο 95%, βασισμένη σε πραγματικά στοιχεία και αντικειμενικές μετρήσεις.

Έχοντας ολοκληρώσει τους υπολογισμούς της ασφάλειας για κάθε υπηρεσία είναι πλέον εφικτό να υπολογιστεί και το επίπεδο της ασφάλειας για το σύνολο του οργανισμού. Η βασική παραδοχή για αυτό είναι ότι όλες οι εξεταζόμενες υπηρεσίες δεν έχουν την ίδια επίδραση στη συνολική ασφάλεια. Για την κάλυψη αυτού του χαρακτηριστικού η μεθοδολογία προτείνει η συνολική ασφάλεια του οργανισμού να είναι ο σταθμισμένος μέσος όρος των επιπέδων ασφάλειας της κάθε υπηρεσίας.

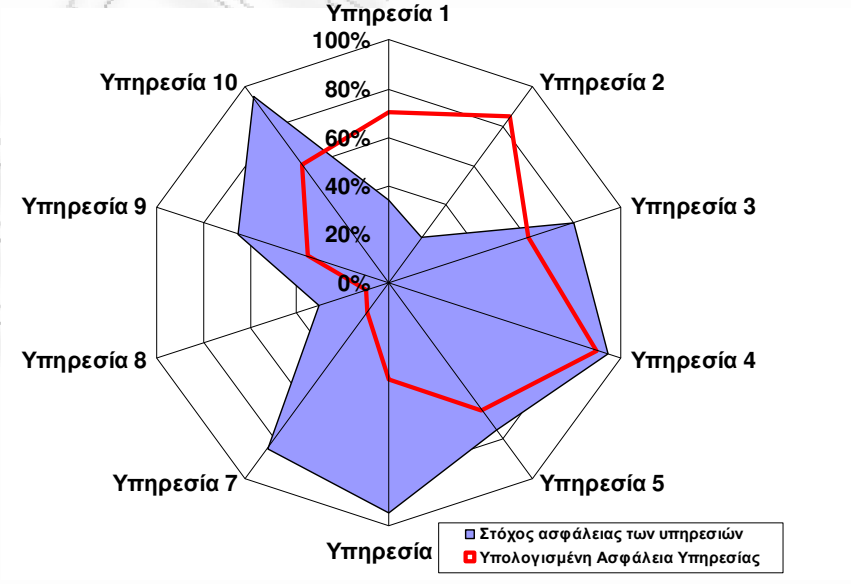
Η στάθμιση πραγματοποιείται ανάλογα με την σημαντικότητα της κάθε υπηρεσίας, η οποία μπορεί να προκύψει από τα κέρδη που επιφέρει αυτή στον οργανισμό ή η εν γένει αξία της, όπως αυτή αξιολογείται από τα υψηλά διοικητικά στελέχη. Για λόγους οικονομίας χρόνου η μεθοδολογία επιτρέπει τη χρήση των 10 ή 20 σημαντικότερων υπηρεσιών αντί για το σύνολο αυτών.

Ο πίνακας 4.12 παρουσιάζει την επέκταση του προηγούμενου παραδείγματος.

Υπηρεσίες	Αξία υπηρεσίας στον οργανισμό	Στόχος ασφάλειας των υπηρεσιών	Υπολογισμένη Ασφάλεια Υπηρεσίας	Σταθμισμένος στόχος ασφάλειας	Σταθμισμένη ασφάλεια
Υπηρεσία 1	2%	34%	70%	0,68%	**1,40%**
Υπηρεσία 2	3%	23%	85%	0,69%	**2,55%**
Υπηρεσία 3	10%	80%	60%	8,00%	**6,00%**
Υπηρεσία 4	12%	95%	90%	11,40%	**10,80%**
Υπηρεσία 5	13%	75%	65%	9,75%	**8,45%**
Υπηρεσία 6	23%	95%	40%	21,85%	**9,20%**
Υπηρεσία 7	12%	85%	15%	10,20%	**1,80%**
Υπηρεσία 8	4%	30%	10%	1,20%	**0,40%**
Υπηρεσία 9	9%	65%	35%	5,85%	**3,15%**
Υπηρεσία 10	12%	95%	60%	11,40%	**7,20%**
		Συνολική Ασφάλεια Οργανισμού		**81,02%**	**50,95%**

Πίνακας 4.12 – Αποτελέσματα παραδείγματος υπολογισμού ασφάλειας (δ)

Η στήλη «Στόχος ασφάλειας των υπηρεσιών» εκφράζει το επιθυμητό επίπεδο ασφάλειας για κάθε υπηρεσία, ενώ η στήλη «Υπολογισμένη Ασφάλεια Υπηρεσίας» είναι το αποτέλεσμα των υπολογισμών που αφορούσαν στην ασφάλεια των υπηρεσιών. Το άθροισμα της στήλης «Σταθμισμένος στόχος ασφάλειας» εκφράζει το επιθυμητό επίπεδο της συνολικής ασφάλειας του οργανισμού. Τα παραπάνω στοιχεία παρουσιάζονται εποπτικά στο διάγραμμα 4.8.



Διάγραμμα 4.8 – Αποτελέσματα παραδείγματος υπολογισμού ασφάλειας (ε)

Όπως μπορεί να φανεί, υπάρχει μια σημαντική διαφορά γύρω στο 30% μεταξύ του επιθυμητού επιπέδου ασφάλειας που είναι περίπου 81% για όλο τον οργανισμό και το τρέχον επίπεδο που βρίσκεται κοντά στο 51%.

Επίσης υπάρχουν κάποιες υπηρεσίες, όπως οι 1 και 2, οι οποίες απολαμβάνουν ένα επίπεδο ασφάλειας, πολύ μεγαλύτερο από το επιθυμητό. Αντίθετα άλλες υπηρεσίες, όπως οι 6, 7, 8, 9 και 10 βρίσκονται πίσω από τον οροθετημένο στόχο της ασφάλειας που έχει τεθεί από τον οργανισμό. Αυτού του είδους οι παρατηρήσεις μπορούν να βοηθήσουν στην καλύτερη λήψη αποφάσεων και επενδύσεων. Στο συγκεκριμένο παράδειγμα, ο οργανισμός θα πρέπει να εστιάσει από τις υπηρεσίες 1 και 2 στις υπηρεσίες 6 έως 10, χωρίς όμως να αμελήσει τις υπηρεσίες 3 έως 5. Η αλλαγή στην εστίαση μπορεί να συνεπάγεται μια διαφορετική κατανομή των πόρων (χρηματικών και ανθρώπινων) προς τις υπηρεσίες που τους χρειάζονται περισσότερο.

4.4.2.2. Υπολογισμός με παράγοντες έμμεσα σχετιζόμενους με την ασφάλεια

Στο πλαίσιο της παρούσας έρευνας, δημιουργήθηκε και μια δεύτερη προσέγγιση υπολογισμού της ασφάλειας, η οποία αντιμετωπίζει την ασφάλεια ως μέγεθος το οποίο υπολογίζεται με τον συνδυασμό κάποιων εύκολα μετρήσιμων παραγόντων. Οι παράγοντες αυτοί σχετίζονται έμμεσα με την ασφάλεια και μάλιστα, όπως και στην πρώτη προσέγγιση, με το επίπεδο ασφάλειας μιας συγκεκριμένης επιχειρηματικής υπηρεσίας.

Η προσέγγιση αυτή έχει ως βασική αρχή ότι οι αφηρημένες έννοιες μπορούν να υπολογιστούν με τον συνδυασμό παραγόντων που σχετίζονται έμμεσα με αυτές. Παράλληλα επιδιώκει την πραγμάτωση των παρακάτω γενικών απαιτήσεων:

- Αντιμετώπιση της ασφάλειας ως παράγοντα που δραστηριοποιείται εντός του περιβάλλοντος παραγωγής και όχι ως ένα παράλληλο ζήτημα με ελάχιστο ή καθόλου επιχειρησιακό ενδιαφέρον.
- Χρήση και συνδυασμό μεγεθών που μπορούν να μετρηθούν ή να ποσοτικοποιηθούν με αντικειμενικό τρόπο.

- Σύνδεση των αποτελεσμάτων του υπολογισμού της ασφάλειας με τις επιχειρηματικές αποφάσεις.

Για την εφαρμογή της συγκεκριμένης μεθοδολογίας υπολογισμού της ασφάλειας, θα πρέπει να προσδιοριστούν οι πηγές των πρωτογενών δεδομένων τα οποία θα συνδυαστούν για τον υπολογισμό της ασφάλειας. Η συγκεκριμένη μεθοδολογία θεωρεί ότι η τιμή της ασφάλειας μπορεί να προκύψει από το συνδυασμό κάποιων από τους παράγοντες που σχετίζονται με την ασφάλεια. Οι παράγοντες που επιλέχθηκαν είναι πέντε και αφορούν όλοι τους κάποιο επιχειρηματικό, λειτουργικό ή εμπορικό μέγεθος. Για λόγους συντομίας οι παραπάνω παράγοντες αναφέρονται ως CARLS από τα αρχικά των παραγόντων στην αγγλική γλώσσα. Αυτοί είναι:

- Συμμόρφωση (Compliance): Εκφράζει το ποσοστό της συμμόρφωσης με το νομικό και κανονιστικό πλαίσιο που είναι οικείο στην υπηρεσία.
- Διαθεσιμότητα (Availability): Εκφράζει το ποσοστό της διαθεσιμότητας της υπηρεσίας όπως αυτή ορίστηκε στο κεφάλαιο 2.
- Απόδοση (Return): Εκφράζει το μέγεθος των κερδών που προκύπτει από την συγκεκριμένη υπηρεσία.
- Παθητικό (Liabilities): Εκφράζει το μέγεθος των οικονομικών απωλειών λόγω της παροχής της υπηρεσίας.
- Δείκτης μετοχής (Stock price): Εκφράζει την τιμή της μετοχής της εταιρίας.

Όλοι οι παράγοντες αποτελούν ουσιαστικά διαφορετικές πτυχές των επιχειρηματικών υπηρεσιών και πρέπει να είναι διαθέσιμοι για να συντεθούν σε μια τιμή που αντιπροσωπεύει το επίπεδο ασφάλειας κάθε μιας από τις υπηρεσίες. Οι παράγοντες έχουν δύο βασικά πλεονεκτήματα, οι οποίοι είναι οι κύριοι λόγοι για την επιλογή τους σε αυτό το μοντέλο.

Το πρώτο πλεονέκτημα είναι το γεγονός ότι ήδη, όλοι οι παράγοντες μετρούνται για λόγους επιχειρησιακής αξιολόγησης. Αυτό σημαίνει ότι δεν χρειάζεται καμία πρόσθετη προσπάθεια για να συγκεντρώσει τις πληροφορίες

που απαιτούνται. Το δεύτερο πλεονέκτημα είναι το γεγονός ότι κάθε παράγοντας αντιπροσωπεύει αντικειμενική εικόνα για τον οργανισμό, της οποίας η ισχύς δεν μπορεί να αμφισβητηθεί.

Η μέτρηση και παρακολούθηση όλων αυτών των παραγόντων θεωρείται απαραίτητη για την ανάπτυξη, τη βιωσιμότητα και την ορθή λειτουργία κάθε οργανισμού. Είναι εξαιρετικά σύνηθες, στη συντριπτική πλειοψηφία των οργανισμών, να παρακολουθούνται και να καταγράφονται όλοι οι παραπάνω παράγοντες για όλο τον οργανισμό. Σε πολλές ακόμα περιπτώσεις οι παράγοντες αυτοί καταγράφονται για κάθε υπηρεσία ξεχωριστά. Το γεγονός αυτό κάνει την συλλογή των στοιχείων αυτών μια απλή και εύκολα πραγματοποιήσιμη διαδικασία. Επιπλέον, οι παράγοντες CARLS έχουν πολύ περισσότερο νόημα για τους ανθρώπους που βρίσκονται σε μη τεχνικές θέσεις και η νοοτροπία τους είναι προσανατολισμένη στις επιχειρησιακές ανάγκες των οργανισμών τους. Σε σύγκριση με την προηγούμενη προσέγγιση αυτό αποτελεί πλεονέκτημα διότι έτσι διευκολύνεται η κατανόηση αλλά και η χρηστικότητα του μεγέθους της ασφάλειας το οποίο βασίζεται σε οικείες έννοιες και όχι σε τεχνικούς όρους όπως «ακεραιότητα» και «εμπιστευτικότητα».

Ο επιδιωκόμενος στόχος παραμένει ο υπολογισμός της τιμής της ασφάλειας μιας συγκεκριμένης υπηρεσίας. Αυτός πραγματοποιείται με τον προσδιορισμό, την ποσοτικοποίηση και το συνδυασμό των παραγόντων που μπορούν να μετρηθούν εύκολα και που σχετίζονται έμμεσα με την ασφάλεια. Η τιμή αυτή απεικονίζει το επίπεδο ασφάλειας μιας συγκεκριμένης υπηρεσίας. Στις επόμενες παραγράφους παρουσιάζονται τα επιχειρήματα υπέρ της επιλογής των συγκεκριμένων παραγόντων αναφέροντας γιατί οι παράγοντες CARLS θεωρούνται κατάλληλοι για τον υπολογισμό της ασφάλειας.

Έχοντας, ολοκληρώσει την επιχειρηματολογία υπέρ της επιλογής των συγκεκριμένων παραγόντων, ακολουθεί μια ανάλυση για κάθε έναν από αυτούς.

Συμμόρφωση: Ο αντίκτυπος της μη συμμόρφωσης είναι προφανής. Όμως πολλοί οργανισμοί επιλέγουν να λειτουργήσουν χωρίς τις απαραίτητες διαδικασίες συμμόρφωσης με το νομικό και το κανονιστικό πλαίσιο. Πολλές φορές δεν αποτελούν κίνητρο ούτε οι ρυθμιστικές και ποινικές κυρώσεις της ελλιπούς ή αναποτελεσματικής συμμόρφωσης. Η μη συμμόρφωση μπορεί να έχει αντίκτυπο στη ρευστότητα, η οποία μπορεί να έχει περεταίρω επιπτώσεις στη δυνατότητά του οργανισμού να επενδύσει τα απαραίτητα κεφάλαια για την ανάπτυξή του.

Οι επιπτώσεις όμως που σχετίζονται με την ασφάλεια είναι εμφανέστερες και μεγαλύτερες. Εφόσον οι ρυθμιστικές, νομικές και κανονιστικές αρχές έχουν ως σκοπό την προστασία των πελατών, των οργανισμών αλλά και τους κράτους, το επίπεδο της ασφάλειας αναπόφευκτα επηρεάζεται με την ελλιπή υλοποίηση ή ενασχόληση με τη συμμόρφωση.

Υπάρχει φυσικά και ένα σημαντικό κόστος που σχετίζεται με την προσπάθεια συμμόρφωσης, το οποίο θα πρέπει να λαμβάνεται υπόψη. Κατά συνέπεια, η πιο δύσκολη πτυχή της συμμόρφωσης είναι να γνωρίζει ο οργανισμός όλα που πρέπει να κάνει, αλλά κυρίως πότε και πώς. Η συνεχής συμμόρφωση απαιτεί μια πάγια επένδυση – για τους ίδιους λόγους που σε μια αρχική προσπάθεια συμμόρφωσης η όλη διαδικασία έγινε γνωστή στο κοινό. Έτσι, η εικόνα που προσέλκυσε πελάτες και επενδυτές κατά την πρώτη αυτή προσπάθεια θα εξακολουθήσει να υφίσταται όσο η προσπάθεια συμμόρφωσης συνεχίζει να πραγματοποιείται και να δημοσιοποιείται.

Διαθεσιμότητα: Εκφράζεται ως ποσοστό χρόνου διαθεσιμότητας σε ένα έτος. Τόσο οι κυβερνητικές οργανώσεις όσο και οι επιχειρήσεις όλων των μεγεθών είναι υποχρεωμένες να δημιουργήσουν και να υλοποιήσουν αναλυτικά σχέδια επιχειρηματικής και λειτουργικής συνέχειας. Παράλληλα, οι περισσότερες οργανώσεις συνειδητοποιούν ότι πρέπει να προστατεύουν τα δεδομένα και τα συστήματά τους από απρόβλεπτες διακοπές ή και απώλειες που

μεταφράζονται σε διαφεύγοντα κέρδη αλλά και απώλεια κύρους και πελατών. Το γεγονός αυτό καθιστά τη διαθεσιμότητα όχι μόνο μια τεχνική απαίτηση αλλά και μια επιχειρηματική ανάγκη. Μεγαλύτερη διαθεσιμότητα συνεπάγεται και μεγαλύτερο επίπεδο ασφάλειας.

Απόδοση: Εκφράζεται ως χρηματικό ποσό. Στο σύγχρονο οικονομικό και εμπορικό σύστημα ο στόχος των μετόχων ενός οργανισμού ή μιας επιχείρησης είναι να αυξήσει τον πλούτο της. Η κερδοφορία είναι λοιπόν ένας μέγιστος παράγοντας ενδιαφέροντος για κάθε επιχειρηματική δραστηριότητα. Οι πιθανοί πιστωτές ανησυχούν για το πώς η επιχείρηση χρησιμοποιεί τους πόρους της, εάν ο τρόπος χρήσης τους είναι επικερδής, έτσι ώστε να μπορεί να πληρώσει τόσο τον τόκο όσο και το κεφάλαιο του πιθανού χρέους της. Παράλληλα, οι ιδιοκτήτες ανησυχούν εάν η επιχείρηση είναι κερδοφόρα έτσι ώστε η τιμή της μετοχής να αυξηθεί. Οι διευθυντές της επιχείρησης επιθυμούν να επιδείξουν την ικανότητά τους στη διαχείριση της επένδυσης των ιδιοκτητών και στη παραγωγή κερδών. Έτσι, οι απαιτήσεις μιας καλής απόδοσης διαδίδεται σε όλο το προσωπικό και ισχύει για όλες τις υπηρεσίες. Ένας βασικός λόγος ο οποίος συνεισφέρει στην κερδοφορία είναι η σωστή και ασφαλής παροχή των επιχειρηματικών υπηρεσιών. Όταν λοιπόν μια υπηρεσία εμφανίζει μια σημαντική απόδοση αυτό μπορεί να είναι μια καλή ένδειξη ότι η συγκεκριμένη υπηρεσία είναι και ασφαλής.

Παθητικό: Εκφράζεται ως χρηματικό ποσό. Οι περισσότερες επιχειρήσεις σχετικές οι οποίες σχετίζονται με το χρηματοπιστωτικό τομέα θα συμφωνούσαν ότι η διαχείριση των οικονομικών επισφαλειών είναι μια από τις πιο βασικές δαπάνες τους. Για αυτή την αιτία, οι επιχειρήσεις προϋπολογίζουν σε ετήσια βάση σχετικά κονδύλια για την κάλυψη οικονομικών απωλειών. Οι απώλειες αυτές κατανέμονται ανάλογα στις προσφερόμενες υπηρεσίες. Όπως και με την απόδοση, έτσι και το παθητικό σχετίζεται με το επίπεδο της ασφάλειας μιας υπηρεσίας. Σε αυτή την περίπτωση υψηλό παθητικό αποτελεί ένδειξη για χαμηλού επιπέδου ασφάλειας.

Δείκτης μετοχής: Εκφράζεται ως χρηματικό ποσό. Με τη χρήση του δείκτη της μετοχής μιας επιχείρησης και ειδικότερα αξιοποιώντας τις διαφοροποιήσεις στην τιμή της είναι δυνατόν να εξεταστούν οι οικονομικές επιπτώσεις εισβολών ασφάλειας. Η μελέτη του Gordon στο [18] κατέδειξε ότι μια αρνητική χρηματιστηριακή αντίδραση που θα επηρεάσει την τιμή της μετοχής αποτελεί συνάρτηση των περιστατικών της ασφάλειας. Αναφέρεται ότι το οικονομικό κόστος των δημοσιοποιημένων εισβολών αποτυπώνεται και μάλιστα με άμεσο τρόπο στις τιμές των μετοχών των εταιριών που υπέστησαν την εισβολή ή που σχετίζονται με την εταιρία που υπέστη την εισβολή.

Η επιλογή των παραπάνω παραγόντων ικανοποιεί τις δύο από τις τρεις βασικές απαιτήσεις που είχαν τεθεί στο πλαίσιο της τρέχουσας προσέγγισης υπολογισμού της ασφάλειας, δηλαδή την αντιμετώπιση της ασφάλειας ως παράγοντα που δραστηριοποιείται εντός του περιβάλλοντος παραγωγής καθώς και τη χρήση και το συνδυασμό μεγεθών που μπορούν να μετρηθούν ή να ποσοτικοποιηθούν με αντικειμενικό τρόπο.

Με τη σύνθεση των παραπάνω παραγόντων είναι εφικτός ο υπολογισμός μιας τιμής που θα απεικονίζει το επίπεδο της ασφάλειας μιας υπηρεσίας. Για τη μαθηματική έκφραση αυτού του υπολογισμού με ένα συγκεκριμένο τύπο, έχουν γίνει διάφορες παραδοχές.

Αρχικά, εισάγεται η έννοια του Επιπέδου – Στόχος για κάθε ένα από τους παραπάνω παράγοντες. Ο στόχος καθορίζεται από τα διευθυντικά στελέχη του οργανισμού, οι οποίοι είναι και «ιδιοκτήτες» των υπηρεσιών, άρα και υπεύθυνοι για τους λειτουργικούς περιορισμούς κάθε υπηρεσίας, όπως η ασφάλεια. Στο πλαίσιο αυτό καθορίζεται το Επίπεδο – Στόχος για τη συμμόρφωση, τη διαθεσιμότητα, την απόδοση, το παθητικό και την τιμή της μετοχής. Ο στόχος για τη συμμόρφωση μπορεί να είναι η ολική συμμόρφωση με ένα πρότυπο του οικείου κλάδου, ή με μια νομοθετική διάταξη ή ακόμα με ένα διεθνές πρότυπο. Παρόμοια, ο στόχος για τη διαθεσιμότητα θα πρέπει να

καθοριστεί λαμβάνοντας υπόψη τις επιχειρηματικές ανάγκες για κάθε υπηρεσία.

Το τρέχον επίπεδο της συμμόρφωσης αναπαρίσταται με ένα «Ναι» ή ένα «Όχι», για την απλοποίηση του μοντέλου. Μια μελλοντική επέκταση του μοντέλου μπορεί να είναι η μετατροπή του συγκεκριμένου δείκτη σε ποσοστό, το οποίο θα υποδηλώνει ότι η υπηρεσία καλύπτει μέρος των απαιτήσεων συμμόρφωσης.

Σε μαθηματικό επίπεδο, η τιμή της ασφάλειας της υπηρεσία μπορεί να εκφραστεί ως συνάρτηση των παραγόντων οι οποίες είναι οι μεταβλητές της συνάρτησης με τη χρήση του ακόλουθου τύπου:

$$Sec_S = \frac{C}{C_T} \times \frac{A}{A_T} \times \frac{R-L}{R_T} \times \frac{S}{S_T}$$

Όπου:

- Sec_s : Το τρέχον επίπεδο ασφάλειας μιας συγκεκριμένης υπηρεσίας s
- C : Το τρέχον επίπεδο συμμόρφωσης το οποίο παίρνει τιμές 0 ή 1
- C_T : Το Επίπεδο – Στόχος της συμμόρφωσης το οποίο παίρνει τιμές 0 ή 1
- A : Το τρέχον επίπεδο διαθεσιμότητας το οποίο παίρνει τιμές από 0 έως 1
- A_T : Το Επίπεδο – Στόχος της διαθεσιμότητας το οποίο παίρνει τιμές από 0 έως 1
- R : Η τρέχουσα απόδοση της υπηρεσίας (σε νόμισμα)
- L : Το τρέχον παθητικό της υπηρεσίας (σε νόμισμα)
- R_T : Το Επίπεδο – Στόχος της απόδοσης της υπηρεσίας (σε νόμισμα)
- S : Η τρέχουσα τιμή της μετοχής της εταιρίας (σε νόμισμα)
- S_T : Το Επίπεδο – Στόχος της τιμής της μετοχής της εταιρίας (σε νόμισμα)

Έχοντας εκφράσει την ασφάλεια με τη χρήση του παραπάνω τύπου, επιδιώκεται η σωστή χρήση των αποτελεσμάτων και μάλιστα με χρηματοοικονομικά κριτήρια. Ο νέος στόχος είναι να ισορροπήσουν οι επενδύσεις της ασφάλειας σε κάθε υπηρεσία ώστε να μεγιστοποιηθούν τα κέρδη του οργανισμού, τα οποία εκφράζονται ως ROI της συγκεκριμένης υπηρεσίας. Αυτό επιτυγχάνεται με τον παρακάτω τύπο:

$$\max ROI(Sec_1, Sec_2, ..., Sec_n)$$

υπό τον όρο

$$\sum_{i=1}^{n} (R_i - I_i - L_i) > 0$$

Όπου:

Sec_n : Το τρέχον επίπεδο ασφάλειας της υπηρεσίας n

R_i : Η τρέχουσα απόδοση της υπηρεσίας i

I_i : Οι συνολικές επενδύσεις στην υπηρεσία i (μέρος της οποίας είναι οι επενδύσεις και τα λειτουργικά έξοδα της ασφάλειας για αυτή την υπηρεσία)

L_i : Το τρέχον παθητικό της υπηρεσίας i

Με τον παραπάνω τύπο επιτυγχάνεται και ο τελευταίος στόχος, δηλαδή η σύνδεση των αποτελεσμάτων του υπολογισμού της ασφάλειας με τις επιχειρηματικές αποφάσεις, που είχε τεθεί στο πλαίσιο αυτής της προσέγγισης.

4.4.3. Οπτικοποίηση της ασφάλειας

Στο πλαίσιο της μέτρησης και του υπολογισμού της ασφάλειας, κρίθηκε σκόπιμο να γίνει ειδική μνεία και στην οπτικοποίηση των μετρήσεων της ασφάλειας, κυρίως ως μέσο καλύτερης διαχείρισης και κατανόησης των μετρήσεων, άρα και ως εργαλείο αύξησης της ασφάλειας.

Η συνήθης πρακτική για την απεικόνιση των θεμάτων που σχετίζονται με την ασφάλεια περιλαμβάνει δύο μορφές:

- Απλά ραβδοδιαγράμματα (bar charts) και πιτοδιαγράμματα (pie charts) τα οποία παρουσιάζουν δείγματα από ένα απλοϊκό μέγεθος όπως είναι ο αριθμός των ευπαθειών όπως αυτός διαπιστώθηκε από ένα αυτοματοποιημένο σύστημα, ή τον αριθμό των ανεπιθύμητων μηνυμάτων στο ηλεκτρονικό ταχυδρομείο (spam emails) όπως αυτός καταγράφηκε από ένα σύστημα φιλτραρίσματος των emails.
- Δείκτες του τύπου «φανάρια κυκλοφορίας» τα οποία υποδηλώνουν τον κίνδυνο με τα κλασικά τρία χρώματα (κόκκινο, κίτρινο, πράσινο) για το αντικείμενο ή τον τομέα υπό εξέταση.

Υπάρχουν όμως προβλήματα και με τις δύο προσεγγίσεις. Τα διαγράμματα τείνουν να είναι αντιπαραγωγικά, καταλαμβάνοντας αρκετό χώρο συγκριτικά με τον αριθμό των δεδομένων που παρουσιάζουν. Επιπρόσθετα, τείνουν να περιλαμβάνουν μόνο ένα μέγεθος ή εύρος δεδομένων αντί για να παραθέτουν μια σειρά από σχετιζόμενα μεγέθη. Τα φανάρια-δείκτες είναι ακόμα χειρότερα επειδή απλοποιούν την πληροφορία περισσότερο από όσο πρέπει. Αυτό έχει ως συνέπεια να επισκιάζουν τις τυχόν διακυμάνσεις, διαφοροποιήσεις και τις λεπτομέρειες οι οποίες τελικά οδηγούν σε ορθολογικές αποφάσεις.

Η οπτικοποίηση της ασφάλειας, παρουσιάζει πολλά κοινά με την οπτικοποίηση άλλων αφηρημένων εννοιών, και κατά συνέπεια χρησιμοποιεί πολλές από τις κοινές αρχές της οπτικοποίησης. Όπως αναφέρει ο Jaquith στο [17], οι βασικές αρχές της οπτικοποίησης της ασφάλειας είναι οι εξής έξι:

1. Η έμφαση θα πρέπει να είναι στα δεδομένα και όχι στο σχέδιο, ενώ ο αναλυτής δεν θα πρέπει να υποκύπτει στον πειρασμό της χρήσης έντονων φόντων και διακοσμητικών, τα οποία αποσπούν την προσοχή από την πραγματική πληροφορία.
2. Η χρήση τρισδιάστατων αντικειμένων δεν προσφέρει κάποια επιπλέον πληροφορία. Τα τρισδιάστατα αντικείμενα αποσπούν την προσοχή από τις πληροφορίες.

3. Τα πρότυπα των διαγραμμάτων που αφορά στην ασφάλεια θα πρέπει να επιλέγονται και να διαμορφώνονται ανάλογα με τις ανάγκες των υπό παρουσίαση μεγεθών και πληροφοριών.
4. Το κάθε διάγραμμα θα πρέπει να έχει τον ελάχιστο αριθμό στοιχείων. Τα περιττά στοιχεία μπορεί να είναι το πλέγμα, οι σκιές, τα πλαίσια, οι ετικέτες και γενικά οτιδήποτε δεν παρέχει κάποια πληροφορία.
5. Τα χρώματα θα πρέπει να είναι όσο το δυνατόν πιο απλά. Η χρήση μονοχρωματικών διαγραμμάτων είναι η ιδανική λύση γιατί μια ασπρόμαυρη εκτύπωση δεν αφαιρεί καμιά από τις πληροφορίες του διαγράμματος.
6. Οι τίτλοι και οι ετικέτες θα πρέπει να είναι όσο πιο σαφείς και απλοί γίνεται. Ο τίτλος θα πρέπει να είναι εύκολα κατανοητός, οι μονάδες μέτρησης διαθέσιμες για κάθε μέγεθος, τα γράμματα καθαρά και ευδιάκριτα και η πηγή (ή οι πηγές) των δεδομένων να αναφέρονται. Επίσης θα πρέπει να αποφεύγονται οι κάθε τύπου συντομογραφίες.

Οι τύποι των διαθεσίμων απεικονιστικών μεθόδων περιλαμβάνουν μια σειρά από διαγράμματα, το καθένα με τα πλεονεκτήματα και τα μειονεκτήματά του. Η επιλογή του καθενός εξαρτάται από τη φύση των δεδομένων και του μηνύματος – στόχου. Κάποια από αυτά είναι:

1. Τα συσσωρευμένα ραβδοδιαγράμματα (Stacked bar charts), τα οποία παρουσιάζουν τη συνεισφορά κάθε σειράς δεδομένων επί του απόλυτου συνόλου ανά συγκεκριμένα χρονικά διαστήματα.
2. Τα διαγράμματα – καταρράκτες (Waterfall charts), τα οποία παρουσιάζουν πως πολλαπλές κατηγορίες συγκεντρώνονται για να σχηματίσουν ένα γενικό σύνολο σε μια συγκεκριμένη χρονική στιγμή.
3. Τα διαγράμματα χρονολογικών σειρών (Time series charts), τα οποία παρουσιάζουν πως μια ή περισσότερες σειρές μεταβάλλονται σε μια συγκεκριμένη χρονική περίοδο, π.χ. σε 1 ώρα, 1 μήνα, 1 τρίμηνο ή 1 έτος.

4. Τα διαγράμματα χρονολογικών σειρών με δείκτη (Indexed time series charts), τα οποία εκφράζουν κάθε σημείο ως πολλαπλάσιο της αρχικής τιμής του.
5. Τα διαγράμματα χρονολογικών σειρών με τεταρτημόρια (Quartile time series charts), τα οποία σχεδιάζουν τις τιμές ανά τεταρτημόριο για μια σειρά δεδομένων σε ένα συγκεκριμένο χρονικό διάστημα.
6. Τα διαγράμματα διπλών μεταβλητών (Bivariate charts), τα οποία δείχνουν πως δύο μεταβλητές συμπεριφέρονται συγκριτικά μεταξύ τους.
7. Οι πολλαπλοί μικρο-πίνακες (Small multiples), οι οποίοι σχεδιάζουν παρόμοια μικρά διαγράμματα στον ίδιο πίνακα, επιτρέποντας τη γρήγορη επισκόπηση και την αναζήτηση τάσεων, ομοιοτήτων και διαφορών.
8. Οι πολλαπλοί μικρο-πίνακες με τεταρτημόρια (Quartile-plot small multiples), οι οποίοι συνδυάζουν τη συγκριτική δύναμη των πολλαπλών μικρο-πινάκων με την ευκολία των τερτατημορίων.
9. Οι πίνακες δυο-επί-δυο (Two-by-two matrices), τα οποία επεκτείνουν τα διαγράμματα διπλών μεταβλητών ομαδοποιώντας τα αποτελέσματα σε τεταρτημόρια.
10. Τα διαγράμματα μοιρασμένων περιόδων (Period-share charts), στα οποία διακρίνονται τα σημεία βελτίωσης και επιδείνωσης σε δύο συνεχόμενες χρονικές περιόδους.
11. Τα διαγράμματα Παρέτο (Pareto charts), τα οποία παρουσιάζουν ταξινομημένα δεδομένα με τη μορφή ράβδων. Στο δευτερεύοντα άξονα, χρησιμοποιείται μια γραμμή η οποία εκφράζει το συνολικό άθροισμα της κάθε τιμής ως ποσοστό τοις εκατό.
12. Οι πίνακες (Tables), οι οποίοι δείχνουν τα δεδομένα με διάταξη πλέγματος.
13. Οι δενδροειδείς χάρτες (Treemaps), οι οποίοι δείχνουν τις ιεραρχικές σχέσεις σε ομάδες δεδομένων ως σειρές επαναλαμβανόμενων παραλληλόγραμμων.

Οπτικά παραδείγματα των παραπάνω απεικονιστικών μεθόδων βρίσκονται στο Παράρτημα Α : «Παραδείγματα οπτικοποίησης της ασφάλειας».

Η οπτικοποίηση της ασφάλειας θεωρείται αναγκαία για κάθε τομέα που παράγει ή χρησιμοποιεί δεδομένα που σχετίζονται με την ασφάλεια και επιθυμεί να:

- Ερευνήσει και να ανακαλύψει τα δεδομένα, είτε για τα αναλύσει είτε για να τα χρησιμοποιήσει ως υποστηρικτικά στοιχεία και αποδείξεις σε περιπτώσεις όπου έχει τελεστεί κάποιο αδίκημα.
- Κάνει γνωστές πληροφορίες σε έναν οργανισμό ή ελεγκτικό φορέα.
- Αποκτήσει επίγνωση της τρέχουσας κατάστασης και του επιπέδου της ασφάλειας.
- Βελτιώσει τη διαδικασία λήψης των αποφάσεων που σχετίζονται με την ασφάλεια.

Κάθε περίπτωση από αυτές συνδέεται άμεσα τόσο με τον υπολογισμό της ασφάλειας όπως αυτός περιγράφηκε στο Κεφάλαιο 4.4 αλλά και με την αύξηση της ασφάλειας όπως αυτή περιγράφηκε στο Κεφάλαιο 4.5.

4.5. Σύνοψη και συμπεράσματα

Το ερώτημα που αναλύθηκε στο κεφάλαιο 4 είναι πως μπορεί να εφαρμοστούν οι αρχές των αρχών μέτρησης ώστε να επιτευχθεί η μέτρηση της ασφάλειας των επιχειρηματικών υπηρεσιών. Τα κίνητρα που υποστηρίζουν το ερώτημα αυτό εστιάζονται στην ορθή αιτιολόγηση των εξόδων και των επενδύσεων που σχετίζονται με την ασφάλεια. Έτσι, παρόλο που η διαχείριση της ασφάλειας είναι κατανοητή σε τεχνικό και οργανωτικό επίπεδο είναι συχνά δύσκολο να οριστεί μια ποσοτικοποιημένη «έκδοση» της ασφάλειας που θα ήταν περισσότερο κατανοητή σε επιχειρησιακό επίπεδο.

Στο κεφάλαιο αυτό πραγματοποιείται μια κριτική αξιολόγηση και κατηγοριοποίηση των απαιτήσεων των μεθόδων μέτρησης και υπολογισμού της ασφάλειας με βάση την οποία αναγνωρίζονται οι περιορισμοί των

προσεγγίσεων που υπάρχουν και αναπτύσσονται δυο νέες εναλλακτικές προσεγγίσεις οι οποίες επιχειρούν την ποσοτικοποίηση της ασφάλειας με τη χρήση των δομικών στοιχείων της ασφάλειας στη πρώτη προσέγγιση και παραγόντων που σχετίζονται έμμεσα με την ασφάλεια στη δεύτερη προσέγγιση.

Η βασική αρχή που ακολουθήθηκε είναι ότι το βάρος της έρευνας θα πρέπει να μετατοπιστεί από την μέτρηση στον υπολογισμό της ασφάλειας. Άλλες βασικές αρχές ήταν:

- η αντιμετώπιση της ασφάλειας ως παράγοντα που δραστηριοποιείται εντός του περιβάλλοντος παραγωγής,
- η χρήση και ο συνδυασμός μεγεθών που μπορούν να μετρηθούν ή να ποσοτικοποιηθούν με αντικειμενικό τρόπο και
- η σύνδεση των αποτελεσμάτων του υπολογισμού της ασφάλειας με τις επιχειρηματικές αποφάσεις.

Το κεφάλαιο ολοκληρώθηκε με την ανάλυση τεχνικών οπτικοποίησης, διαδικασία η οποία συνδέεται άμεσα τόσο με τον υπολογισμό της ασφάλειας αλλά και με την αύξηση της ασφάλειας του κεφαλαίου 5.

4.6. Βιβλιογραφία κεφαλαίου

[1] J. Danahy, "The Need for Metrics and Measurement in Application Security", OWASP Metrics and Measurement Standards, 2004

[2] D. Fisher, "Experts call for better measurement of security", Blog, ανακτήθηκε: 14/6/09, http://www.threatpost.com/blogs/experts-call-better-measurement-security

[3] W. Sonnenreich, J. Albanese και B. Stout, "Return On Security Investment (ROSI) – A Practical Quantitative Model", Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006

[4] WordNet lexical database of English v.3.0, Αναζήτηση του "measurement", ανακτήθηκε: 14/6/09, http://wordnetweb.princeton.edu/perl/webwn?s=measurement

[5] WordNet lexical database of English v.3.0, Αναζήτηση του "metric", ανακτήθηκε: 14/6/09, http://wordnetweb.princeton.edu/perl/webwn?s=metric

[6] B.Maizlitsh και R. Handler, "IT Portfolio Management: Step by Step", John Wiley & Sons, 2005, ISBN: 978-0-471-64984-7, σελ. 53.

[7] «Quantification», Wikipedia, ανακτήθηκε: 14/6/09, http://en.wikipedia.org/wiki/Quantification

[8] W. Zikmund, "Business Research Methods", Chapter 7, Dryden Press, 2000, ISBN 0-03-025817-0, , σελ. 101-120

[9] Qualitative Analysis, ανακτήθηκε: 14/6/09, http://www.gifted.uconn.edu/siegle/research/Qualitative/qualquan.htm

[10] An. Jaquith, "Metrics Are Nifty", Yankee Group, ανακτήθηκε: 14/6/09, www.securitymetrics.org/content/Wiki.jsp?page=Metricon1.0Keynote

[11] Merriam-Webster Dictionary, Αναζήτηση του "calculation", ανακτήθηκε: 14/6/09, http://www.merriam-webster.com/dictionary/calculation

[12] I. Sommerville, "Software Engineering", Fifth Edition, Addison-Westley, 1996, ISBN: 978-0201427653, σελ. 103-106

[13] H. Tipton, M. Krause, "Information Security Management Handbook", Sixth edition, Auerbach Publications, ISBN 978-1420067088, σελ.301

[14] Αποτίμηση επιχειρηματικού κινδύνου, Πρόγραμμα «Δικτυωθείτε», ανακτήθηκε: 14/6/09, http://www.go-online.gr/ebusiness/specials/article.html?article_id=984#t1_2

[15] T. Olzak, «The Pros and Cons of Security Risk Management», Tech Republic, ανακτήθηκε: 14/6/09, http://blogs.techrepublic.com.com/security/?p=180

[16] D. Parker, "Risks of risk-based security", Communications of the ACM, Volume 50, Issue 3 (March 2007).

[17] A. Jaquith, "Security Metrics: Replacing Fear, Uncertainty, and Doubt", Addison-Wesley Professional, 2007, ISBN 978-0321349989, σελ. 161

[18] K. Campbell, L. A. Gordon, M. P. Loeb and L. Zhou "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", 2003, Journal of Computer Security 11, σελ. 431–448

5. Αύξηση της ασφάλειας

5.1. Εισαγωγή

Με βάση τις μεθοδολογίες που παρουσιάστηκαν και προτάθηκαν στα τρία προηγούμενα κεφάλαια, σε αυτό το κεφάλαιο περιγράφονται οι σχετικές μέθοδοι αύξησης της ασφάλειας ενός Πληροφοριακού Συστήματος. Στη συνέχεια αναπτύσσονται δύο νέοι μέθοδοι που διακρίνονται στις μεθόδους που βασίζονται στη χρήση των κλασικών μεθόδων μέτρησης και υπολογισμού και στις μεθόδους που βασίζονται στη χρήση εναλλακτικών μεθόδων υπολογισμού που προτάθηκαν στο προηγούμενο κεφάλαιο. Κάθε νέα προτεινόμενη μέθοδος αξιολογείται ως προς την καταλληλότητά της, ενώ προβάλλονται τα οφέλη και τα μειονεκτήματά της.

5.2. Αύξηση με τη χρήση κλασικών μεθόδων μέτρησης και υπολογισμού

Μια χαρακτηριστική παρομοίωση των προσπαθειών αύξησης της ασφάλειας εκφράζεται από την Address στο [1] η οποία αναφέρει ότι η κάθε προσπάθεια αύξησης του επιπέδου της ασφάλειας σε ένα οργανισμό μοιάζει με ένα τρίποδο. Όπως κάθε πόδι σε ένα τρίποδο είναι απαραίτητο για τη διατήρηση της ισορροπίας έτσι και η αύξηση της ασφάλειας θα πρέπει να περιλαμβάνει και το ανθρώπινο δυναμικό και τις κατάλληλες διαδικασίες αλλά και την απαραίτητη τεχνολογία για να διατηρηθεί ισορροπημένη και αποδοτική.

Στο πλαίσιο της διατριβής, οι μέθοδοι αύξησης της ασφάλειας θεωρείται ότι μπορούν να εφαρμοστούν σε δύο κατηγορίες περιπτώσεων.

Η πρώτη από αυτές τις περιπτώσεις αφορά τις έκτακτες ανάγκες. Ως έκτακτη ανάγκη ορίζεται στο [2] «μιας τέτοιας έκτακτης έκτασης καταστροφή στο σύστημα πληροφορικής που ουσιαστικά είναι αδύνατη η άμεση επαναλειτουργία του».

Η δεύτερη κατηγορία περιπτώσεων αφορά τις καθημερινές διεργασίες ενός οργανισμού.

Και στις δύο κατηγορίες οι επιμέρους τομείς που θα πρέπει να καλυφθούν απεικονίζονται στο Διάγραμμα 5.9.

Διάγραμμα 5.9 – Τομείς της ασφάλειας

Οι τομείς της ασφάλειας ομαδοποιούνται σε τέσσερις βασικές ομάδες. Αυτές είναι: οι τομείς που σχετίζονται με την τεχνολογία, οι τομείς που σχετίζονται με τις διαδικασίες, οι τομείς που σχετίζονται με την φυσική ασφάλεια και οι τομείς που αφορούν το ανθρώπινο δυναμικό.

Οι τομείς που σχετίζονται με την τεχνολογία αφορούν την ασφάλεια των συστημάτων (διακομιστές, σταθμοί εργασίας κ.λπ.), την ασφάλεια δικτύου (δρομολογητές, πολυπλέκτες κ.λπ.), τις απομακρυσμένες προσβάσεις χρηστών του οργανισμού, τις προσβάσεις τρίτων προσώπων (συνεργατών, πελατών κ.λπ.) και την ασφάλεια των εφαρμογών και γενικότερα του λογισμικού.

Επιπλέον, οι τομείς που σχετίζονται με τις διαδικασίες αφορούν την παρακολούθηση των γεγονότων ασφάλειας, την επεξεργασία των γεγονότων αυτών, την προστασία των πληροφοριών και την επιχειρηματική συνέχεια μετά από καταστροφή.

Ακόμα, οι τομείς που σχετίζονται με τη φυσική ασφάλεια αφορούν την ασφάλεια των κτιρίων ενός οργανισμού, την ασφάλεια των εγκαταστάσεων αλλά και τη διασφάλιση των εγγράφων του οργανισμού.

Αντίστοιχα, οι τομείς που σχετίζονται με το ανθρώπινο δυναμικό καλύπτουν τους τομείς της εκπαίδευσης στον τομέα της ασφάλειας, τις δοκιμές ετοιμότητας και τους ελέγχους του ιστορικού των υπαλλήλων.

Θα πρέπει να σημειωθεί ότι λόγω της αυξημένης πολυπλοκότητας των οργανισμών, οι παραπάνω τομείς μπορούν να αυξηθούν σημαντικά σε αριθμό. Έτσι οι τομείς που αναφέρονται στο Διάγραμμα 5.9 δεν εξαντλούν σε καμία περίπτωση τους τομείς που επηρεάζουν την αύξηση της ασφάλειας ενός οργανισμού. Αποτελούν όμως κοινό τόπο για την πλειονότητα των οργανισμών και το σημείο εκκίνησης για κάθε προσπάθεια αύξησης της ασφάλειας.

Οι τομείς αυτοί αποτελούν κοινό τόπο και για τις μεθόδους και τις τεχνικές μέτρησης της ασφάλειας που αναφέρθηκαν στο κεφάλαιο 3.3 οι οποίες μπορούν να επεκταθούν και να χρησιμοποιηθούν για την αύξηση της ασφάλειας. Ο Πίνακας 5.13 αναφέρει τις αντίστοιχες μεθόδους αύξησης της ασφάλειας.

Κατηγορίες μεθόδων αύξησης της Ασφάλειας
Κάλυψη Ευπαθειών
Ευθυγράμμιση με Υλοποιήσεις Αναφοράς, Βέλτιστες Πρακτικές και Πρότυπα
Διαχείριση Κινδύνων

Πίνακας 5.13 – Κατηγορίες μεθόδων αύξησης της ασφάλειας

5.2.1. Κάλυψη Ευπαθειών

Η πρώτη μέθοδος αύξησης της ασφάλειας μπορεί να βασιστεί στα αποτελέσματα των μεθοδολογιών Ανάλυσης Ευπαθειών και Δοκιμών Διείσδυσης. Η μέθοδος περιγράφει τους τρόπους κάλυψης των τυχόν

ευπαθειών οι οποίες είναι πιθανό να προκύψουν είτε μέσα από μια διαδικασία καταγραφής και ανάλυσης των ευπαθειών είτε με μια σειρά δοκιμών που θα αποσκοπούν στη διείσδυση στα συστήματα και τις υποδομές του οργανισμού.

Μια μεθοδολογία διαχείρισης και κάλυψης των ευπαθειών παρέχει ένα συνεχές πλαίσιο σύνδεσης των στόχων της ασφάλειας με την υλοποίηση, και έτσι προάγεται η συνεχής βελτίωση. Τα οφέλη της ασφάλειας μπορούν να αποκτήσουν μια περισσότερο απτή περιγραφή, μια που τα αποτελέσματα της διαδικασίας μπορούν να ποσοτικοποιηθούν. Η τυποποιημένη εφαρμογή της μεθόδου επιτρέπει επίσης τη διανομή των σχετικών εμπειριών καθώς και την ενθάρρυνση της συμμετοχής διαφορετικών επιπέδων του οργανισμού.

Τα αποτελέσματα των δοκιμών θα πρέπει να περιλαμβάνουν λύσεις για την μείωση ή την εξαφάνιση των ευπαθειών. Το γεγονός αυτό διαφοροποιεί μια τυποποιημένη δοκιμή διείσδυσης από ένα απλό έλεγχο ασφάλειας. Οι σημαντικές ευπάθειες που διαπιστώθηκαν θα πρέπει να αντιμετωπιστούν κατά προτεραιότητα ενώ θα πρέπει να δημιουργηθεί και ένα πλάνο αντιμετώπισης των ευπαθειών. Με την ίδια ή παρόμοια διαδικασία θα πρέπει να δοκιμάζονται όλα τα διαφορετικά τμήματα του οργανισμού. Οι λύσεις που θα επιλεχθούν και θα υλοποιηθούν θα είναι εξαρτώμενες από τις ευπάθειες που ανιχνεύτηκαν, τις απώλειες του οργανισμού εφόσον κάποιος ή κάτι ενεργοποιήσει την ευπάθεια καθώς και το κόστος και την αποδοτικότητα των διαθέσιμων λύσεων.

Μια πιθανή ενέργεια σε ένα οργανισμό μπορεί είναι η απαίτηση κάθε νέο σύστημα που θα διατεθεί σε κοινό να δοκιμάζεται και να ελέγχεται ως προς τις ευπάθειές του. Μια άλλη ενέργεια μπορεί να είναι η κεντρική διαχείριση και δρομολόγηση όλης της ηλεκτρονικής αλληλογραφίας για ένα οργανισμό, ακόμα και αν ο αποστολέας και ο παραλήπτης ανήκουν στον ίδιο οργανισμό.

Σε κάποιες περιπτώσεις αρκεί απλώς η εφαρμογή πολιτικών ασφάλειας που ήδη υπάρχουν για την αντιμετώπιση συγκεκριμένων ευπαθειών. Στο

παράδειγμα της ασφάλειας των σταθμών εργασίας, το λογισμικό απομακρυσμένης διαχείρισης μπορεί να απαγορεύεται ήδη για έναν οργανισμό. Σε άλλες περιπτώσεις απαιτούνται άλλου τύπου ενέργειες όπως η εγκατάσταση της νεότερης έκδοσης μιας εφαρμογής.

Σε κάθε περίπτωση όμως το τελικό κείμενο με αποτελέσματα θα πρέπει να φυλάσσεται αυστηρά. Εάν οι πληροφορίες που περιέχονται εκεί τεθούν στη διάθεση κακόβουλων τρίτων, κάποιος κακόβουλος χρήστης ή επιτιθέμενος θα μπορούσε να εκμεταλλευτεί τις ευπάθειες αυτές πριν ακόμα αυτές αντιμετωπιστούν.

Θα πρέπει ακόμα να τονιστεί ότι μια δοκιμή διείσδυσης είναι απλά μια «εικόνα» των συστημάτων και των δικτύων σε ένα πολύ συγκεκριμένο χρονικό σημείο. Η δοκιμή εκτελείται μόνο στις ευπάθειες που είναι γνωστές από τη συγκεκριμένη έκδοση των εργαλείων που χρησιμοποιεί ο αναλυτής. Η διαδικασία ελέγχου των εφαρμογών, των συστημάτων και της δικτυακής ασφάλειας είναι συνεχής επειδή οι προσθήκες και οι αλλαγές όλων αυτών των παραγόντων είναι συνεχείς. Το γεγονός αυτό επηρεάζει κάθε φορά τα αποτελέσματα του ελέγχου και των δοκιμών.

Άλλα μειονεκτήματα περιλαμβάνουν τη δυσκολία που υπάρχει στην αναζήτηση και τον εντοπισμό ευπαθειών σε συστήματα που χρησιμοποιούν διαφορετικές τεχνολογίες και αρχιτεκτονικές, όπως π.χ. Windows και Mainframe.

Επιπλέον μπορεί να υπάρχουν θέματα ενεργοποίησης ψευδών συναγερμών είτε λόγω της επαναλαμβανόμενης φύσης των δοκιμών είτε λόγω της επιθετικότητας των δοκιμών. Υπάρχουν δοκιμές όπως η Επίθεση Άρνησης Εξυπηρέτησης (Denial of Service), η οποία δεν είναι πάντα εύκολο να δοκιμαστεί διότι μια τέτοια δοκιμή απέχει πολύ λίγο από μια πραγματική επίθεση. Σε πιο ακραίες καταστάσεις, οι επαναλαμβανόμενες δοκιμές μπορεί να προκαλέσουν την αδράνεια των συστημάτων ασφάλειας σε μια πραγματική επίθεση με παρόμοια χαρακτηριστικά.

Υπάρχουν ακόμα θέματα, παραβίασης προσωπικών δεδομένων αλλά και της ιδιωτικότητας των επικοινωνιών, τα οποία πρέπει να λαμβάνονται υπόψη όταν εφαρμόζεται η συγκεκριμένη μέθοδος.

5.2.2. Ευθυγράμμιση με Υλοποιήσεις Αναφοράς, Βέλτιστες Πρακτικές και Πρότυπα

Η δεύτερη μέθοδος αύξησης της ασφάλειας μπορεί να βασιστεί στα αποτελέσματα των μεθόδων σύγκρισης με υλοποιήσεις αναφοράς αλλά και της εφαρμογής βέλτιστων πρακτικών και προτύπων. Η μέθοδος περιγράφει τους τρόπους αύξησης της ασφάλειας με την υιοθέτηση και υλοποίηση υλοποιήσεων αναφοράς, σχετικών βέλτιστων πρακτικών αλλά και σχετικών προτύπων.

Ο πιο σχετικός όρος σε αυτή τη μέθοδο αύξησης της ασφάλειας είναι το «Κανονιστικό Πλαίσιο Ασφάλειας Πληροφοριών». Με αυτό τον όρο αναφέρονται οι απαιτήσεις της ασφάλειας που έχει τέσσερις κύριες πηγές. Αυτές είναι οι Νόμοι, οι Κανονισμοί, τα Πρότυπα και οι Βέλτιστες Πρακτικές.

Η νομοθεσία για την ασφάλεια μπορεί να διαφέρει από χώρα σε χώρα, χωρίς όμως να αποκλείονται και κοινές απαιτήσεις από διαφορετικές χώρες (κυρίως της Ευρωπαϊκής Ένωσης). Οι κανονισμοί που ισχύουν για ένα επιχειρηματικό τομέα ή κλάδο επιβάλλονται από θεσμοθετημένους εποπτικούς φορείς, όπως για παράδειγμα η Επιτροπή Τραπεζικής Εποπτείας (Βασιλεία) ή οι Κεντρικές Τράπεζες. Τα πρότυπα που εκδίδονται από διεθνείς ή εθνικούς οργανισμούς και συνήθως απευθύνονται σε περισσότερους από έναν επιχειρηματικούς κλάδους, όπως για παράδειγμα το ISO 27001, το BS 7799 και το ISO 15000. Επίσης, οι Βέλτιστες Πρακτικές και οι Υλοποιήσεις Αναφοράς εκδίδονται από αναγνωρισμένους φορείς και έχουν ως στόχο την δημιουργία πρακτικών που μπορούν να βοηθήσουν κάθε οργανισμό.

Η νομοθεσία αλλά και οι κανονισμοί έχουν συνήθως υποχρεωτικό χαρακτήρα και η μη συμμόρφωση με αυτά πιθανώς επισείει νομικές και διοικητικές κυρώσεις. Αντίθετα τα πρότυπα και οι πρακτικές έχουν συνήθως προαιρετικό χαρακτήρα. Όλα όμως τα παραπάνω έχουν ως αποτέλεσμα την αύξηση της ασφάλειας μέρους ή όλου του οργανισμού.

Βέβαια, οι κανονιστικές απαιτήσεις συνεπάγονται και κάποιες επιπτώσεις στην πληροφοριακή υποδομή ενός οργανισμού. Οι επιπτώσεις μπορούν να επηρεάσουν τόσο τη γενική πληροφοριακή υποδομή όσο και τις εξειδικευμένες υποδομές ασφάλειας. Στο πλαίσιο της γενικής πληροφοριακής υποδομής όλοι σχεδόν οι κανονισμοί απαιτούν την αποτελεσματική παρακολούθηση και διαχείριση των πληροφοριακών υποδομών αλλά και την εξασφαλισμένη αποθήκευση των κρίσιμων πληροφοριών.

Σε ότι αφορά τις εξειδικευμένες υποδομές ασφάλειας συμπεριλαμβάνονται οι τεχνολογίες που μπορούν να βοηθήσουν στην προστασία των κρίσιμων συστημάτων και ευαίσθητων δεδομένων. Κάποιες χαρακτηριστικές απαιτήσεις από διάφορους κανονισμούς περιλαμβάνουν την υλοποίηση τεχνολογιών προστασίας των κρίσιμων συστημάτων από απειλές που προέρχονται από το δίκτυο, τα λειτουργικά συστήματα, τις εφαρμογές κ.α. Άλλη μια απαίτηση είναι οι κατάλληλοι έλεγχοι πρόσβασης των χρηστών σε κάθε κρίσιμο πόρο του οργανισμού. Επίσης, οι οργανισμοί, στο πλαίσιο της συμμόρφωσης με το κανονιστικό πλαίσιο, θα πρέπει να αναπτύξουν υποδομές που επιτρέπουν την αποτελεσματική παρακολούθηση, ανίχνευση, αξιολόγηση και αντιμετώπιση των περιστατικών ασφάλειας.

Όμως, θα πρέπει να υπογραμμιστεί η διαφορά μεταξύ Ασφάλειας και Συμμόρφωσης. Είναι βασική αρχή ότι η συμμόρφωση δε συνεπάγεται και ασφάλεια. Αυτό συμβαίνει διότι οι περισσότεροι κανονισμοί εστιάζουν στην προστασία συγκεκριμένων δεδομένων, συστημάτων, υπηρεσιών και δεν αντιμετωπίζουν την ασφάλεια ως ευρύτερο θέμα. Αλλά και το αντίστροφο δεν ισχύει: Η ασφάλεια δε συνεπάγεται συμμόρφωση, μια που οι κανονισμοί είναι

πολύ δυναμικοί και απαιτούν ειδικού τύπου επενδύσεις ακόμα και από οργανισμούς που είναι πολύ ευαισθητοποιημένοι στα θέματα της ασφάλειας.

5.2.3. Διαχείριση Κινδύνων

Η Διαχείριση κινδύνων αποτελεί μια από τις δημοφιλέστερες προσεγγίσεις τόσο για την ποσοτικοποίηση της ασφάλειας όσο και για την αύξησή της. Επιτυγχάνεται με την ανάπτυξη ενός αναλυτικού πλάνου το οποίο αφού πραγματοποιήσει την επιλογή των καταλλήλων μηχανισμών ελέγχου και αντίμετρων για κάθε κίνδυνο, τα υποβάλλει για έγκριση στα κατάλληλα διοικητικά στελέχη.

Το πλάνο διαχείρισης κινδύνου θα πρέπει να προτείνει εφαρμόσιμους και αποδοτικούς μηχανισμούς ελέγχου για τη διαχείριση των κινδύνων. Με τη συμπλήρωση της εκτίμησης του κινδύνου, σχηματίζεται μια ομάδα αντιμετώπισης του κινδύνου, η οποία τεκμηριώνει τις αποφάσεις με τις οποίες οι κίνδυνοι αντιμετωπίζονται. Η αντιμετώπιση των κινδύνων συχνά συνεπάγεται αποκλειστικά την επιλογή των αντίμετρων, τα οποία υποδεικνύονται από κάποιο σχετικό πρότυπο.

Μια άλλη συμπληρωματική προσέγγιση μπορεί να είναι η αγορά μιας ασφαλιστικής κάλυψης, η οποία θα αναλάβει την κάλυψη συγκεκριμένων κινδύνων. Έτσι ο οργανισμός είναι σε θέση να διαχειριστεί τους κινδύνους που επιλέγει εκείνος.

Σε κάθε περίπτωση τα αρχικά πλάνα διαχείρισης αλλά και τα αποτελέσματα της ανάλυσης των κινδύνων είναι συνήθως ατελή και κατά συνέπεια απαιτούν περιοδική αναθεώρηση. Οι δύο βασικοί λόγοι για αυτό είναι η επαναξιολόγηση της καταλληλότητας και της αποδοτικότητας των αντιμέτρων αλλά και η επανεκτίμηση των επιπέδων κινδύνου στον οργανισμό.

Εάν οι κίνδυνοι έχουν εκτιμηθεί και ιεραρχηθεί με λανθασμένο τρόπο τότε είναι πιθανό να αφιερωθούν πόροι και να γίνουν περιττά έξοδα για κινδύνους

που δεν είναι τόσο πιθανοί να συμβούν. Αντίστοιχα, κίνδυνοι με μεγαλύτερη πιθανότητα και επιπτώσεις μπορεί να μην τύχουν της απαραίτητης προσοχής. Το ενδεχόμενο αυτό είναι αρκετά πιθανό διότι η Διαχείριση κινδύνων βασίζεται κυρίως στην υποκειμενική κρίση του αναλυτή – αξιολογητή.

Ένας σημαντικός λόγος για τον οποίο η Διαχείριση κινδύνων χαρακτηρίζεται ως πολυέξοδη είναι η γραφειοκρατική διαδικασία που ακολουθεί, τόσο κατά τη διάρκεια της διαμόρφωσης του πλάνου όσο και κατά τη διάρκεια της τεκμηρίωσης των αποτελεσμάτων της μεθόδου αυτής.

5.3. Αύξηση με τη χρήση εναλλακτικών μεθόδων υπολογισμού

Εναλλακτικά των παραπάνω προσεγγίσεων προτείνονται δύο νέες μεθοδολογίες που μπορούν να βοηθήσουν στην αύξηση της ασφάλειας και βασίζονται στις μεθοδολογίες υπολογισμού της ασφάλειας των παραγράφων 4.4.2.1 και 4.4.2.2. Οι μεθοδολογίες, των οποίων η περιγραφή και η ανάλυση αποτέλεσε και μέρος της καινοτομίας της διατριβής, μπορούν να επεκταθούν και συμπεριλάβουν τα απαραίτητα βήματα για την αύξηση της ασφάλειας.

Το αποτέλεσμα του υπολογισμού της ασφάλειας με βάση τα επιμέρους δομικά στοιχεία της ασφάλειας μπορεί να οδηγήσει σε μια επέκταση της συγκεκριμένης μεθόδου περιλαμβάνοντας και τα στοιχεία εκείνα που μπορούν να βοηθήσουν στην αύξηση της ασφάλειας. Έτσι, η αρχή ότι η ασφάλεια μπορεί να υπολογιστεί με το συνδυασμό των δομικών στοιχείων της ασφάλειας, επεκτείνεται με τον ισχυρισμό ότι η αύξηση σε οποιοδήποτε από τα δομικά στοιχεία συνεπάγεται και αύξηση στην συνολική ασφάλεια μιας υπηρεσίας.

Χρησιμοποιώντας το παράδειγμα του κεφαλαίου 4 για την υπηρεσία του ηλεκτρονικού ταχυδρομείου, γίνεται εύκολα αντιληπτό ότι η χρήση ενός νέου μηχανισμού anti-spam, που μπορεί να αυξήσει τον αριθμό των spam emails που εντοπίζονται από το μηχανισμό αυξάνει και τη συνολική ασφάλεια.

Εάν για παράδειγμα, τα μεγέθη των δομικών στοιχείων του πίνακα 4.11 αλλάξουν στα μεγέθη που φαίνονται στον πίνακα 5.14 τότε όπως φαίνεται και στον πίνακα 5.15 η ασφάλεια αυξάνεται κατά 2%, δηλαδή από 95% σε 97% και βρίσκεται πολύ πιο κοντά στους στόχους του οργανισμού.

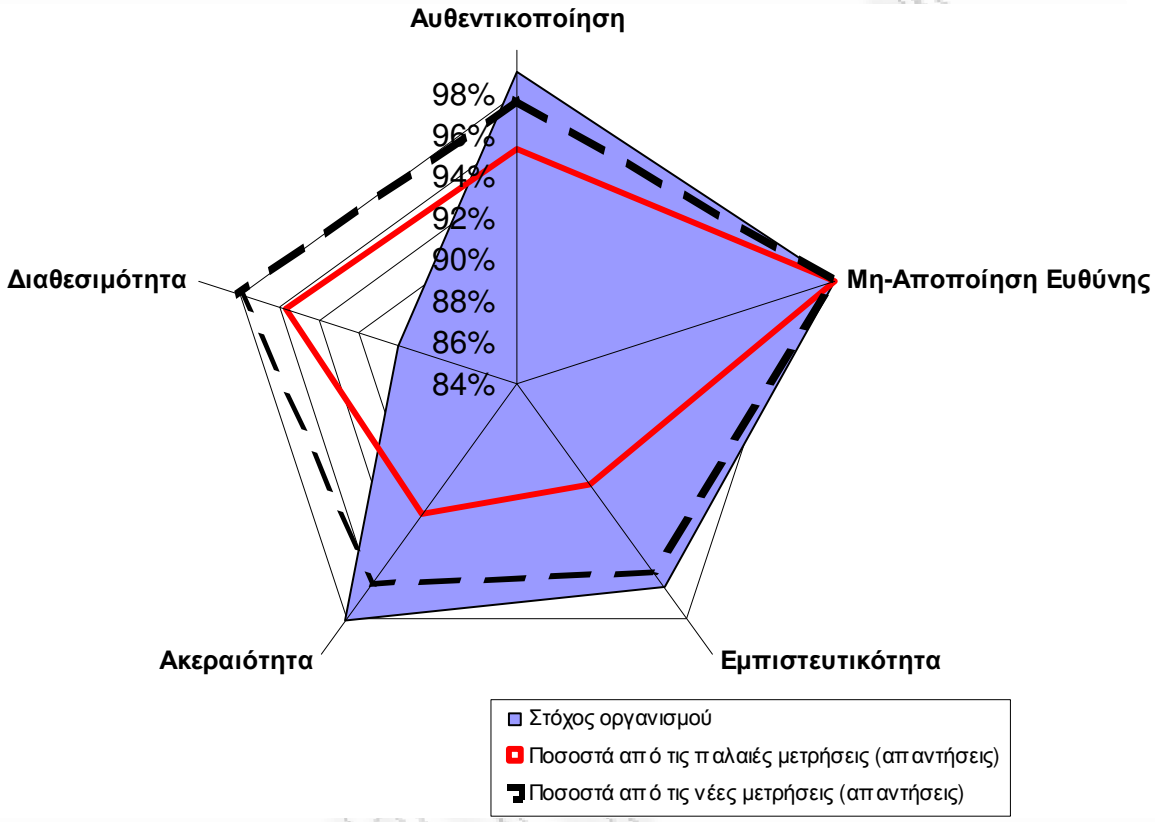
Ερωτήσεις	Απαντήσεις
A. Spam emails που εντοπίστηκαν	**2.070.701**
A1.Αυθεντικοποίηση	875.612
A2.Μη-Αποποίηση Ευθύνης	64.072
A3.Εμπιστευτικότητα	405.146
A4.Ακεραιότητα	245.598
A5.Διαθεσιμότητα	480.273
B. Spam emails που δεν εντοπίστηκαν	**63.201**
A1.Αυθεντικοποίηση	21.356
A2.Μη-Αποποίηση Ευθύνης	3
A3.Εμπιστευτικότητα	20.732
A4.Ακεραιότητα	10.678
A5.Διαθεσιμότητα	10.433
A+B. Συνολικά spam emails	**2.133.902**
A1+B1.Αυθεντικοποίηση	896.968
A2+B2.Μη-Αποποίηση Ευθύνης	64.074
A3+B3.Εμπιστευτικότητα	425.878
A4+B4.Ακεραιότητα	256.277
A5+B5.Διαθεσιμότητα	490.705

Πίνακας 5.14 – Αποτελέσματα παραδείγματος αύξησης ασφάλειας (α)

Δομικό Στοιχείο Ασφάλειας	Στόχος οργανισμού	Ποσοστά από τις παλαιές μετρήσεις (απαντήσεις)	Σταθμισμένος στόχος	Σταθμισμένη μέτρηση
Αυθεντικοποίηση	99%	98%	20%	**20%**
Μη-Αποποίηση Ευθύνης	100%	100%	21%	**21%**
Εμπιστευτικότητα	96%	95%	20%	**19%**
Ακεραιότητα	98%	96%	20%	**19%**
Διαθεσιμότητα	90%	98%	19%	**18%**
		Ασφάλεια Υπηρεσίας		**97%**

Πίνακας 5.15 – Αποτελέσματα παραδείγματος αύξησης ασφάλειας (β)

Η συγκριτική απεικόνιση των δύο μετρήσεων (πριν και μετά την χρήση του νέου μηχανισμού anti-spam) απεικονίζονται στο Διάγραμμα 5.10.



Διάγραμμα 5.10 – Αποτελέσματα παραδείγματος αύξησης ασφάλειας (γ)

Το πλεονέκτημα αυτής της μεθόδου είναι ότι επιτρέπει την άμεση σύγκριση της προηγούμενης κατάστασης της ασφάλειας με την κατάσταση που προκύπτει με τις αλλαγές.

Θα πρέπει να σημειωθεί εδώ ότι οι αλλαγές που θα προκαλέσουν την αύξηση της ασφάλειας δεν είναι ίδιες για κάθε οργανισμό, πληροφοριακό σύστημα ή υπηρεσία. Μπορούν όμως να αναφερθούν μια σειρά από επιμέρους εργασίες με την εκτέλεση των οποίων μπορούν να ωφεληθούν όλοι οι οργανισμοί.

Οι εργασίες αυτές συγκεντρώθηκαν και αποτυπώνονται στον Πίνακα 5.16.

Εργασίες αύξησης της Ασφάλειας
Παρακολούθηση και έλεγχος υπηρεσιών
Έλεγχος διαδικασιών ασφάλειας
Έλεγχοι εγκατάστασης νέων συστημάτων
Περιοδικοί έλεγχοι συστημάτων
Δειγματοληπτικοί έλεγχοι συστημάτων
Έλεγχοι σημαντικών αρχείων και βάσεων δεδομένων
Έλεγχοι αλλαγών δικαιωμάτων χρηστών
Εγκατάσταση ενημερώσεων και διορθώσεων λογισμικού
Συντήρηση και ανανέωση πολιτικών και διαδικασιών ασφάλειας
Αξιολόγηση νέων προϊόντων ασφάλειας (υλικό και λογισμικό)
Σχεδιασμός και υλοποίηση κατατμήσεων των υποδομών και των δικτύων
Τεχνολογική ενημέρωση
Συνεχής εκπαίδευση και ευαισθητοποίηση στην ασφάλεια
Διερεύνηση, συντονισμός και παρακολούθηση περιστατικών ασφάλειας

Πίνακας 5.16 – Ενέργειες αύξησης της ασφάλειας

Οι εργασίες αυτές αποτελούν τη βάση για τις ενέργειες που θα πρέπει να εκτελέσει ένας οργανισμός για να αυξήσει την ασφάλεια των συστημάτων, των υποδομών και των υπηρεσιών του.

Η δεύτερη εναλλακτική προσέγγιση για την αύξηση της ασφάλειας βασίζεται στη μέθοδο που περιγράφεται στο κεφάλαιο 4.4.2.2. και υπολογίζει την ασφάλεια ως μια συνάρτηση έμμεσα σχετιζόμενων παραγόντων όπως η συμμόρφωση σε νομοθεσία, κανονιστικά πλαίσια και πρότυπα, η διαθεσιμότητα των επιχειρηματικών υπηρεσιών, η απόδοση μιας συγκεκριμένης υπηρεσίας, το παθητικό (απώλειες) λόγω της παροχής της υπηρεσίας και το δείκτη της μετοχής της εταιρίας.

Η συσχέτιση αυτής της μεθόδου με την αύξηση της ασφάλειας είναι έμμεση. Η αύξηση της ασφάλειας υπολογίζεται με βάση τους παράγοντες CARLS, όπου μια αλλαγή σε κάποιον από τους τομείς της ασφάλειας θα επηρεάσει και κάποιον από αυτούς τους παράγοντες.

Εάν για παράδειγμα οργανισμός συμμορφωθεί με ένα υποχρεωτικό κανονιστικό πλαίσιο το οποίο δεν καλυπτόταν ως σήμερα, τότε η τιμή του C (Compliance) γίνεται 1 και το L (Liabilities) μειώνεται λόγω της παύσης των πιθανών προστίμων ή ρητρών από τη μη συμμόρφωση. Είναι ακόμα πιθανό, λόγω της πιθανής δημοσιοποίησης της ενέργειας αυτής να ανέβει και η τιμή της μετοχής S.

Κατά συνέπεια από τον τύπο που εισάχθηκε στο πλαίσιο της συγκεκριμένης μεθόδου, προκύπτει ότι το τρέχον επίπεδο ασφάλειας Sec μιας συγκεκριμένης υπηρεσίας s θα αυξηθεί.

Από τα παραπάνω συμπεραίνουμε ότι και η πρώτη αλλά και η δεύτερη εναλλακτική προσέγγιση για τον υπολογισμό μπορούν να επεκταθούν και να βοηθήσουν στον υπολογισμό της αύξησης της ασφάλειας. Σε ότι, όμως αφορά την παροχή κατευθύνσεων στους οργανισμούς για την αύξηση της ασφάλειας, μόνο η πρώτη εναλλακτική προσέγγιση παρέχει τη βάση για τις ενέργειες που θα πρέπει να εκτελέσει ένας οργανισμός για να αυξήσει την ασφάλεια των συστημάτων, των υποδομών και των υπηρεσιών του.

5.4. Σύνοψη και συμπεράσματα

Το πέμπτο κεφάλαιο περιλαμβάνει την περιγραφή και την ανάλυση των μεθόδων αύξησης της ασφάλειας ενός Πληροφοριακού Συστήματος. Αυτές διακρίνονται στις μεθόδους που βασίζονται στη χρήση των κλασικών μεθόδων μέτρησης και υπολογισμού και στις μεθόδους που βασίζονται στη χρήση εναλλακτικών μεθόδων υπολογισμού που προτάθηκαν, δηλαδή εκείνης που βασίζει τον υπολογισμό της ασφάλειας στο συνδυασμό των δομικών στοιχείων της ασφάλειας και εκείνης που βασίζεται στην μέθοδο υπολογισμού της ασφάλειας ως συνάρτηση έμμεσα σχετιζόμενων παραγόντων. Όλες οι μέθοδοι αξιολογούνται ως προς την καταλληλότητά τους, αντιπαραβάλλοντας τα οφέλη και τα μειονεκτήματά τους.

Το ερευνητικό ενδιαφέρον του κεφαλαίου εστιάζεται στην πρώτη αλλά και στη δεύτερη εναλλακτική προσέγγιση για τον υπολογισμό της ασφάλειας οι οποίες μπορούν να βοηθήσουν και στην αύξηση της ασφάλειας. Επιπλέον η πρώτη εναλλακτική προσέγγιση παρέχει οδηγίες σχετικά με τις ενέργειες που θα πρέπει να εκτελέσει ένας οργανισμός για να αυξήσει την ασφάλεια των συστημάτων, των υποδομών και των υπηρεσιών του.

5.5. Βιβλιογραφία κεφαλαίου

[1] Mandy Address, "Surviving Security, How to integrate people, process and technology", Sams Publishing, 2002, ISBN 0-672-32129-7, σελ.434

[2] Γ. Πάγκαλος και Ι. Μαυρίδης, "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων", Εκδόσεις Ανικούλα, 2002, ISBN 960-516-018-8, σελ. 265

6. Διαχείριση Ασφάλειας Κρίσιμων Πληροφοριακών Υποδομών

6.1. Εισαγωγή

Ένα ειδικότερο θέμα της αύξησης της ασφάλειας είναι η βελτιστοποίηση της διαχείρισης της ασφάλειας των κρίσιμων πληροφοριακών υποδομών.

Στο παρόν κεφάλαιο αναλύονται οι τρέχουσες μεθοδολογίες διαχείρισης της ασφάλειας των Πληροφοριακών Υποδομών και προτείνονται τρόποι για την τροποποίηση ή προσαρμοσμένη υιοθέτησή τους στη διαχείριση των κρίσιμων πληροφοριακών υποδομών. Επιπλέον, με τη χρήση των μεθόδων υπολογισμού της ασφάλειας που προτάθηκαν στο κεφάλαιο 4 αλλά και των μεθοδολογιών που αναφέρθηκαν στο κεφάλαιο 2, προτείνονται και αναλύονται δύο εξελιγμένες μεθοδολογίες που βελτιστοποιούν τη διαχείριση της ασφάλειας των κρίσιμων πληροφοριακών υποδομών, τόσο από οικονομικής άποψης όσο και από λειτουργικής άποψης.

6.2. Μεθοδολογίες διαχείρισης ασφάλειας κρίσιμων πληροφοριακών υποδομών

Όπως αναφέρθηκε και στο κεφάλαιο 2, οι πληροφοριακές υποδομές παρέχουν τη τεχνολογική βάση για τους οργανισμούς να διαχειριστούν τις πληροφορίες τους καθώς και τα Πληροφοριακά Συστήματά τους. Η βασική διαφορά τους με τις Κρίσιμες Πληροφοριακές Υποδομές και Συστήματα είναι ότι τα τελευταία είναι εκείνα που χωρίς την ύπαρξη και τη σωστή λειτουργία τους δεν είναι εφικτή η εκπλήρωση των επιχειρηματικών στόχων του οργανισμού, όπως η παροχή υπηρεσιών και η παραγωγή προϊόντων.

Η διαχείριση της ασφάλειας των κρίσιμων πληροφοριακών συστημάτων συχνά συνδέεται με τις ενέργειες που αφορούν την επιχειρηματική συνέχεια. Η επιχειρηματική συνέχεια αναφέρεται σε όλα τα οργανωτικά και τεχνικά μέτρα, καθώς και στα μέτρα με τα οποία εξασφαλίζεται το αναγκαίο και κατάλληλο ανθρώπινο δυναμικό, έτσι ώστε μετά την εκδήλωση μιας έκτακτης ανάγκης να διασφαλίζεται η συνέχιση των κύριων επιχειρησιακών λειτουργιών και

υπηρεσιών. Όμως, οι πιο συνηθισμένες ενέργειες που σχετίζονται με την διαχείριση της ασφάλειας επικεντρώνονται στις καθημερινές λειτουργίες των οργανισμών.

Έτσι, για τη διαχείριση των πληροφοριακών υποδομών και συστημάτων έχουν αναπτυχθεί μια σειρά από μεθοδολογίες και θεωρίες που εστιάζουν σε διαφορετικούς τομείς της ασφάλειας τόσο σε περιπτώσεις έκτακτης ανάγκης όσο και κατά τις καθημερινές εργασίες. Καθεμία από τις μεθοδολογίες έχει τα δικά της χαρακτηριστικά καθώς και κάποια ιδιαίτερα μειονεκτήματα και πλεονεκτήματα.

Το συγκεκριμένο κεφάλαιο περιλαμβάνει τους τρόπους με τους οποίους οι θεωρίες και μεθοδολογίες διαχείρισης της ασφάλειας των Πληροφοριακών Υποδομών μπορούν να εφαρμοστούν και στις Κρίσιμες Πληροφοριακές Υποδομές. Επιπλέον τι είδους αλλαγές απαιτούνται για τη διαχείριση της ασφάλειας αυτής της ευαίσθητης κατηγορίας πληροφοριακών υποδομών, αλλά και πως αυτές μπορούν να προσαρμοστούν ώστε να διασφαλίζουν τη διαθεσιμότητα και την ορθή λειτουργία των κρίσιμων πληροφοριακών υποδομών.

Μερικές από τις πιο κοντινές μεθοδολογίες για τη διαχείριση των κρίσιμων πληροφοριακών υποδομών είναι οι ITIL (όπως αναλύθηκε στο κεφάλαιο 3.2.2), το μοντέλο Εξοικείωσης, Πρόβλεψης και Ικανότητας (ΕΠΙ) [1] αλλά και οι ερευνητικές προσπάθειες της Pommerening στο [2], των Pye και Warren στο [3] και των Warren και Leitch στο [4].

Η Pommerening στο [2] ορίζει τις παραμέτρους οι οποίες θα πρέπει να λαμβάνονται υπόψη για την προστασία των κρίσιμων υποδομών. Αυτές διαχωρίζονται στα δικτυακά χαρακτηριστικά καθώς και στην κοινωνικό-οικονομική οπτική του θέματος.

Οι Pye και Warren στο [3] δημιούργησαν ένα μοντέλο περιγραφής κρίσιμων συστημάτων το οποίο περιλαμβάνει τα χαρακτηριστικά των συστημάτων, τις σχέσεις μεταξύ τους καθώς και τη στατική ή δυναμική τους συμπεριφορά σε σχέση με το περιβάλλον τους.

Οι Warren και Leitch στο [4] περιγράφουν τα θέματα ασφάλειας τα οποία αφορούν τα κρίσιμα πληροφοριακά συστήματα σε σχέση με τα συστήματα παραγωγής και κυρίως το μοντέλο διαχείρισης της Εφοδιαστικής Αλυσίδας (Supply Chain Management). Τα θέματα αυτά μπορούν να επεκταθούν στο σύνολο των κρίσιμων πληροφοριακών συστημάτων.

Το μοντέλο ΕΠΙ όπως αυτό περιγράφεται από τον Health στο [1], είναι ένα σύνθετο μέτρο για την αποτελεσματικότητα της αντιμετώπισης των κινδύνων άρα και της διαχείρισης της ασφάλειας. Εκεί υποστηρίζεται ότι υπάρχουν τρεις βασικές μεταβλητές που οδηγούν σε καλή ή κακή διαχείριση της ασφάλειας. Αυτές είναι ο βαθμός εξοικείωσης των ατόμων του οργανισμού με την κάθε πιθανή κατάσταση ασφάλειας, ο βαθμός προβλεψιμότητας των πιθανών κινδύνων καθώς και οι το πλήθος και το είδος των ικανοτήτων που έχουν τα άτομα που διαχειρίζονται την ασφάλεια σε έναν οργανισμό.

Εάν το μέγεθος και των τριών μεταβλητών είναι μεγάλο τότε και ο βαθμός ετοιμότητας του οργανισμού για τα τυχόν περιστατικά ασφάλειας είναι επίσης μεγάλος. Η κάθε μια από αυτές τις μεταβλητές είναι αλληλοσυνδεδεμένη, αλληλεπιδρά με τις άλλες και όλες μαζί εξαρτώνται από την εμπειρία των ατόμων που θα εμπλακούν , όπως επίσης και από τον προγραμματισμό και την ικανότητα ανταλλαγής πληροφοριών για τους διαφορετικούς πιθανούς κινδύνους.

Το συγκεκριμένο μοντέλο ετοιμότητας, αν και ο Health το αναφέρει μόνο ως μοντέλο για την αντιμετώπιση κρίσεων, μπορεί να είναι χρήσιμο και για τη διαχείριση της ασφάλειας υποδομών και συστημάτων που δεν αντιμετωπίζουν απαραίτητα κάποια κρίση. Το τελικό του αποτέλεσμα είναι η αύξηση της

εμπειρίας για την αντιμετώπιση των καταστάσεων που αφορούν όλους τους κινδύνους, δημιουργώντας έτσι τη βάση για μια αποτελεσματικότερη διαχείριση της ασφάλειας μέσα σε έναν οργανισμό.

Επιπλέον των παραπάνω ο Health στο [1], προτείνει και την υιοθέτηση συγκεκριμένων δομών για τη διαχείριση κρίσεων, οι οποίες μπορούν να θεωρηθούν κατάλληλες και για την διαχείριση των ευρύτερων θεμάτων της ασφάλειας. Στο πλαίσιο αυτό διακρίνονται δύο είδη διαχείρισης: το σύστημα διοίκησης ενός περιστατικού ασφάλειας και το πρότυπο σύστημα διαχείρισης εκτάκτων αναγκών. Πλεονέκτημα και των δύο συστημάτων θεωρείται ότι έχουν δοκιμαστεί σε ένα μεγάλο φάσμα κρίσιμων καταστάσεων.

Οι αδυναμίες των δομών αυτών είναι ότι τα συγκεκριμένα συστήματα έχουν, πρώτο, σχεδιαστεί και λειτουργούν από οργανισμούς με ισχυρές απόψεις για την ηγεσία και τον έλεγχο. Δεύτερο, έχουν σχεδιαστεί εστιάζοντας σε μεγάλες φυσικές καταστροφές ενώ είναι λιγότερο εξοικειωμένες με την αντιμετώπιση μεγαλύτερων πεδίων στρατηγικής ή μη φυσικών καταστάσεων. Τρίτο, έχουν σχεδιαστεί περισσότερο για την εφαρμογή επιμέρους τακτικής αντί για τη διαμόρφωση στρατηγικής σε υψηλό επίπεδο.

Λόγω των παραπάνω περιορισμών, τέτοιου είδους δομές, αν και αποτελούν συνήθεις πρακτικές των οργανισμών δεν ανταποκρίνονται στον βαθμό που θα έπρεπε στη διαχείριση της ασφάλειας.

Μια άλλη και πλέον πολύ διαδεδομένη μεθοδολογία διαχείρισης της ασφάλειας ενός οργανισμού είναι εκείνη του ITIL v3. Όπως αναφέρθηκε στο κεφάλαιο 3.2.2 το ITIL σκιαγραφεί και εξηγεί, κυρίως από τη διαχειριστική οπτική, τις πρακτικές οι οποίες θεωρούνται οι πιο ευεργετικές για την παροχή υπηρεσιών πληροφορικής. Σημαντικό μέρος του ITIL αφορά και τη διαχείριση των πληροφορικών υποδομών από την οπτική της ασφαλείας.

Στο πλαίσιο του ITIL, δίνεται έμφαση στις συμβολαιοποιημένες συμφωνίες (Service Level Agreements / SLAs) μεταξύ ενός οργανισμού και ενός παρόχου, που καθορίζουν με τι είδους υπηρεσίες και σε ποιο επίπεδο θα προμηθεύει ο πάροχος τον οργανισμό, κατά τη διάρκεια μιας συνεργασίας. Μέρος των SLAs είναι και οι απαιτήσεις της ασφάλειας οι οποίες, κατά το ITIL, προκύπτουν από την ανάλυση των κινδύνων και τις σχετικές αποφάσεις των αρμοδίων διοικητικών στελεχών. Έτσι η διαχείριση της ασφάλειας των υποδομών ενός οργανισμού κατά ITIL στοχεύει στην εξασφάλιση της τυποποίησης της διαχείρισης αυτής.

Η αυξανόμενη πολυπλοκότητα των πληροφοριακών υποδομών συνεπάγεται και μια ενοποιημένη προσέγγιση για τη διαχείρισή τους. Το ITIL καθορίζει ότι η ασφάλεια των υποδομών (κρίσιμων και μη) αντιμετωπίζεται με ένα ομοιόμορφο τρόπο, διαθέτοντας συνδέσμους και με άλλες διαδικασίες του, οι οποίες αναλαμβάνουν μέρος των διαδικασιών της ασφάλειας.

Η διαχείριση της ασφάλειας περιλαμβάνει, κατά το ITIL, δύο στόχους. Ο πρώτος είναι η ικανοποίηση των απαιτήσεων ασφάλειας τόσο των SLAs όσο και άλλων τρίτων απαιτήσεων όπως νομοθεσία, συμβόλαια και πολιτικές ασφάλειας. Ο δεύτερος στόχος είναι η παροχή ενός βασικού επιπέδου ασφάλειας, ανεξάρτητα από τις όποιες απαιτήσεις του πρώτου στόχου ώστε να εξασφαλίζεται η αδιάλειπτη λειτουργία του οργανισμού.

Βοηθά επίσης στην απλοποίηση της διαχείρισης των συμβολαιοποιημένων συμφωνιών ασφαλείας (Information Security Service Level Management), μια που είναι δυσκολότερο για έναν οργανισμό να διαχειριστεί ένα μεγάλο αριθμό SLAs από το να διαχειριστεί ένα μικρό αριθμό.

Επιπλέον, η βιβλιοθήκη του ITIL καθορίζει μια σειρά από ενέργειες οι οποίες απαιτούνται για την υλοποίησή των διαδικασιών διαχείρισης της ασφάλειας. Αυτές είναι ο σχεδιασμός που σχετίζεται με τα SLAs, η υλοποίηση της ασφάλειας, τόσο για τις τεχνολογικές υποδομές όσο για το ανθρώπινο

δυναμικό και τις σχετικές διαδικασίες. Μια άλλη ομάδα ενεργειών είναι η εκτίμηση και η αξιολόγηση των ελέγχων ασφάλειας καθώς και των αντίστοιχων μετρήσεων. Επιπλέον η κατά ITIL διαχείριση της ασφάλειας περιλαμβάνει την συντήρηση όλων των παραπάνω αλλά και την σχετική αναφορά των αποτελεσμάτων της διαχείρισης της ασφάλειας στα αρμόδια διοικητικά στελέχη.

Στα μειονεκτήματα της προσέγγισης του ITIL για τη διαχείριση της ασφάλειας περιλαμβάνεται το γεγονός ότι δεν λαμβάνει υπόψη τις διαφορετικές υποχρεώσεις των οργανισμών λόγω κανονιστικών και ρυθμιστικών πλαισίων αλλά και τις τυχόν απαιτήσεις που συνεπάγεται μια πιστοποίηση με τα πρότυπα ασφάλειας. Μάλιστα, ο δυναμικός χαρακτήρας που έχουν αυτές οι υποχρεώσεις καθιστά το ITIL μακριά από οποιαδήποτε αλλαγή στις διαδικασίες διαχείρισης της ασφάλειας.

6.3. Βελτιστοποίηση διαχείρισης ασφάλειας κρίσιμων πληροφοριακών υποδομών

Έχοντας περιγράψει τις αδυναμίες των παραδοσιακών μεθόδων διαχείρισης της ασφάλειας των κρίσιμων πληροφοριακών υποδομών αναζητήθηκαν νέοι τρόποι για τη βελτίωσή τόσο για τη διαχείριση της ασφάλειας όσο και για την χρήση των πληροφοριακών υποδομών. Προς την κατεύθυνση αυτή προτείνονται δύο μέθοδοι μετασχηματισμού κρίσιμων πληροφοριακών υποδομών.

Η πρώτη μέθοδος προτείνει τη χρήση των Εναλλακτικών Μηχανογραφικών Κέντρων θέτοντας ως στόχο την αντιμετώπιση Ακραίων Επιθέσεων. Η δεύτερη μέθοδος προτείνει τον μετασχηματισμό των κρίσιμων υποδομών και των εφεδρικών αυτών σε Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα.

6.3.1. Χρήση Εναλλακτικών Μηχανογραφικών Κέντρων για την αντιμετώπιση Ακραίων Επιθέσεων

Η συγκεκριμένη μέθοδος προτείνει τη χρήση των Υπερκείμενων Δικτύων (Overlay Networks) ως εργαλεία για την αντιμετώπιση των επιπτώσεων ακραίων επιθέσεων. Επίσης προτείνει την επέκταση της χρήσης των διαδεδομένων Εναλλακτικών Μηχανογραφικών Κέντρων ως Υπερκείμενα Δίκτυα. Οι επιμέρους στόχοι της μεθόδου είναι η ενεργοποίηση των πληροφοριακών υποδομών με τέτοιο τρόπο ώστε να μπορούν να ανταπεξέλθουν σε σοβαρές δικτυακές ή άλλες επιθέσεις όπως οι επιθέσεις Άρνησης Εξυπηρέτησης (Denial of Service / DoS), οι κατανεμημένες επιθέσεις Άρνησης Εξυπηρέτησης (Distributed Denial of Service / DDoS) αλλά και οι Επιθέσεις εκ των Ένω (Insider Attacks).

6.3.1.1. Η φύση των ακραίων επιθέσεων

Υπάρχουν πολλά είδη επιθέσεων που μπορούν να θεωρηθούν «ακραίες επιθέσεις». Τα κοινά τους χαρακτηριστικά είναι:

Ο επιτιθέμενος έχει απεριόριστους πόρους στην διάθεσή του. Ο επιτιθέμενος θεωρείται ότι είναι ένα άτομο (ή μια ομάδα ατόμων), το οποίο είναι αποφασισμένο να πετύχει το στόχο του. Κατά συνέπεια, δεν υπάρχει όριο στο πλήθος των πόρων που μπορεί να αφιερώσει για την επίθεση στις πληροφοριακές υποδομές του οργανισμού – στόχος. Σε αυτή την περίπτωση οι πόροι μπορεί να είναι χρήματα, υπολογιστική ισχύς ή πρόσβαση. Παραδείγματα αυτής της περίπτωσης μπορεί να είναι οι κυβερνο-πειρατές, οι ανταγωνιστές που δραστηριοποιούνται στην ίδια αγορά με τον εταιρία – στόχο ή ένας κακόβουλος υπάλληλος που έχει σημαντική πρόσβαση και πόρους από τον ίδιο τον οργανισμό.

Οι επιθέσεις στοχεύουν σε κρίσιμες υποδομές. Ο επιτιθέμενος δεν απασχολείται με υποδομές μικρής σημασίας. Το κύριο ενδιαφέρον του είναι να προκαλέσει προβλήματα επηρεάζοντας κρίσιμες υποδομές άρα και κρίσιμες

υπηρεσίες. Παραδείγματα τέτοιων υποδομών είναι τα κεντρικά τραπεζικά συστήματα (Mainframe) και τα συστήματα ελέγχου νομιμοποίησης χρημάτων από παράνομες συναλλαγές (anti-laundering).

Οι επιθέσεις μπορούν να προκαλέσουν τεράστιες ζημιές. Το αποτέλεσμα των, σχετικά σπάνιων, ακραίων επιθέσεων είναι ένα σημαντικότατο ζήτημα στη διαχείριση κινδύνων, λόγω του εύρους και του μεγέθους των ζημιών που μπορούν να προκαλέσουν. Θα πρέπει να τονιστεί όμως ότι η αξιολόγηση μιας επίθεσης ως μιας πιθανής επίθεσης με μέγιστη ζημιά μπορεί να διαφέρει από οργανισμό σε οργανισμό. Για παράδειγμα, η απόκτηση πρόσβασης σε ένα διακομιστή μπορεί να είναι καταστροφική για μια τράπεζα (ιδίως εάν επηρεάζει συναλλαγές) αλλά δεν αποτελεί ιδιαίτερα σημαντικό γεγονός για έναν οργανισμό που έχει στατικό περιεχόμενο στους διακομιστές του. Ο τελευταίος οργανισμός μπορεί να θεωρεί μέγιστη ζημιά την διαγραφή όλων των περιεχομένων ενός εξυπηρετητή αρχείων (file server).

6.3.1.2. Παραδείγματα ακραίων επιθέσεων

Στην προηγουμένη παράγραφο προσδιορίστηκαν τα κύρια χαρακτηριστικά των ακραίων επιθέσεων αναφέροντας και κάποια σχετικά παραδείγματα. Εντούτοις, η μεθοδολογία που προτείνεται λαμβάνει υπόψη δύο συγκεκριμένους τύπους ακραίων επιθέσεων, οι οποίοι και αποτελούν τα παραδείγματα για την εφαρμογή της.

Επιθέσεις Άρνησης Εξυπηρέτησης

Ο στόχος μιας επίθεσης DoS είναι να δεσμευτούν εντελώς οι πόροι ενός κεντρικού υπολογιστή, ο οποίος αποτρέπει τους νόμιμους χρήστες από την πρόσβαση της υπηρεσίας. Μια επιτυχής επίθεση DOS επιτυγχάνει δύο στόχους: εξουδετέρωση του συστήματος - στόχου και απόκρυψη της ταυτότητας του επιτιθεμένου.

Για να εξουδετερώσει το θύμα, ο επιτιθέμενος βασίζεται στην αρχή ότι η μικρή κατανάλωση των πόρων στη δική του πλευρά προκαλεί την πολύ μεγαλύτερη

κατανάλωση των πόρων στην πλευρά του θύματος. Για παράδειγμα, ένα μικρό TCP πακέτο που παράγεται από τον επιτιθέμενο αναγκάζει το σύστημα – στόχος να αφιερώσει ένα κομμάτι της μνήμης του για μια χρονική περίοδο T. Ενώ ο επιτιθέμενος μπορεί να παραγάγει έναν μεγάλο αριθμό πακέτων κατά τη διάρκεια του T, η μνήμη του συστήματος στην πλευρά του θύματος υπερχειλίζει, γεγονός που παραπέμπει στις μεθόδους επίθεσης SYN flooding και connection table overflow ([5], [6], [7]).

Κατανεμημένες Επιθέσεις Άρνησης Εξυπηρέτησης

Για να αποκρύψουν την ταυτότητα του επιτιθεμένου, χρησιμοποιούνται συχνά παραποιημένες IP διευθύνσεις προέλευσης στα πακέτα που στέλνονται από τον επιτιθέμενο. Σε μια DDoS, πολλαπλά κακόβουλα συστήματα εξαπολύουν μια συντονισμένη επίθεση ενάντια σε ένα θύμα, γεγονός που αυξάνει τους διαθεσίμους πόρους για την επίθεση, κάνοντας παράλληλα δυσκολότερη την ταυτοποίηση του επιτιθεμένου. Ο Moore στο [8] κατέδειξε ότι οι επιθέσεις DOS είναι πολύ διαδεδομένες στο διαδίκτυο. Με τη χρησιμοποίηση μιας νέας τεχνικής ελέγχου κυκλοφορίας, την «ανάλυση οπισθοδιασποράς» (backscatter analysis), παρατήρησε 12.805 επιθέσεις σε πάνω από 5.000 μοναδικά συστήματα του διαδικτύου τα οποία ήταν κατανεμημένα σε περισσότερους από 2.000 οργανισμούς κατά τη διάρκεια μιας περιόδου τριών εβδομάδων.

Βυζαντινές Επιθέσεις

Πολλές ευπάθειες στα πρωτόκολλα δικτύων (συμπεριλαμβανομένων και των ασύρματων πρωτοκόλλων δρομολόγησης) προκαλούνται από την έλλειψη μηχανισμών ακεραιότητας και αυθεντικοποίησης μηνυμάτων, η οποία επιτρέπει σε έναν επιτιθέμενο να αλλάξει ή να πλαστογραφήσει τα πακέτα. Σχετική έρευνα για την ασφάλεια των ασύρματων πρωτοκόλλων δρομολόγησης έχει καταγραφεί στα [9], [10], [11] και [12] ενώ για την ασφάλεια των ενσύρματων πρωτοκόλλων δρομολόγησης έχει καταγραφεί στα [13], [14] και [15]. Έτσι, η αυθεντικοποίηση και η ακεραιότητα είναι απαραίτητες για την προστασία ενός πρωτοκόλλου δικτύων, δεδομένου ότι εξασφαλίζουν ότι ένα πακέτο παρήχθη από έναν αυθεντικοποιημένο κόμβο και

δεν έχει πλαστογραφηθεί. Ωστόσο, οι μηχανισμοί αυτοί δεν παρέχουν οποιαδήποτε εγγύηση για τη νομιμότητα των ενεργειών που λαμβάνονται από τους επικυρωμένους κόμβους.

Οι επιθέσεις όπου ο αντίπαλος έχει το ολικό έλεγχο του μηχανισμού αυθεντικοποίησης και μπορεί να εκτελέσει αυθαίρετες εντολές με σκοπό να αναστατώσει το σύστημα αναφέρονται ως βυζαντινές επιθέσεις.

Αν και πολλές Βυζαντινές Επιθέσεις μοιράζονται ορισμένα χαρακτηριστικά γνωρίσματα με το «εγωιστικό» πρόβλημα κόμβων ("selfish" node problem) [16] (π.χ. μην διαβιβάζοντας τα πακέτα στοιχείων άλλων), οι προθέσεις των κόμβων κάτω από αυτά τα δύο μοντέλα συμπεριφοράς είναι διαφορετικές. Ο στόχος ενός εγωιστικού κόμβου είναι να συγκεντρωθούν τα οφέλη από το δίκτυο που συμμετέχει, χωρίς όμως να χρειάζεται να διατεθούν οι πόροι του. Αντίθετα, ο στόχος ενός βυζαντινού κόμβου είναι να διαταραχθεί η επικοινωνία άλλων κόμβων στο δίκτυο, αδιαφορώντας για την κατανάλωση των πόρων του. Υπάρχουν πολλών ειδών Βυζαντινές Επιθέσεις ανάλογα με την προσέγγιση που ακολουθείται κατά την επίθεση:

Επίθεση μαύρων οπών (Black Hole Attack): Ένα βασικό είδος βυζαντινής επίθεσης είναι η επίθεση μαύρων τρυπών όπου ο επιτιθέμενος σταματά την προώθηση δικτυακών πακέτων, αλλά συμμετέχει στο πρωτόκολλο δρομολόγησης.

Επίθεση έντονης πλημμύρας (Flood Rushing Attack): Μια επίθεση τέτοιου είδους εκμεταλλεύεται την τεχνική αντιμετώπισης πλημμυρών που χρησιμοποιείται από πολλά πρωτόκολλα δρομολόγησης.

Βυζαντινή επίθεση Σκουληκότρυπας (Byzantine Wormhole Attack): Εάν περισσότεροι από ένας κόμβοι τεθούν υπό τον έλεγχο του επιτιθέμενου, είναι λογικό να υποτεθεί ότι αυτοί οι κόμβοι μπορούν να αλληλεπιδράσουν προκειμένου να αποκομιστούν πρόσθετα πλεονεκτήματα.

Βυζαντινή Επίθεση Σκουληκότρυπας Υπερκειμένων Δικτύων (Byzantine Overlay Network Wormhole Attack): Μια γενικότερη παραλλαγή της προηγούμενης επίθεσης εμφανίζεται όταν συμβιβάζονται διάφοροι κόμβοι τεθούν υπό τον έλεγχο του επιτιθέμενου και διαμορφώνουν ένα Υπερκείμενο Δίκτυο.

6.3.1.3. Οι βάσεις της προσέγγισης

Προκειμένου να παρουσιαστεί μια λύση στα ανωτέρω ζητήματα, χρησιμοποιήθηκαν οι αρχές των Υπερκείμενων Δικτύων.

Ένα Ευπροσάρμοστο Υπερκείμενο Δίκτυο (Resilient Overlay Network / RON) είναι μια αρχιτεκτονική που επιτρέπει στις κατανεμημένες εφαρμογές Διαδικτύου να ανιχνεύουν και να επανακάμπτουν από τις διακοπές λειτουργίας των δρομολογητών τους καθώς και τις περιόδους χαμηλής αποδοτικότητας μέσα σε λίγα δευτερόλεπτα, βελτιώνοντας τα σημερινά πρωτόκολλα δρομολόγησης ευρείας περιοχής (Wide Area Routing Protocols) τα οποία είναι αρκετά πιο χρονοβόρα στην επανάκαμψή τους. Ένα RON είναι ένα υπερκείμενο επίπεδο εφαρμογών πάνω από το υπάρχον υπόστρωμα δρομολόγησης Διαδικτύου. Οι κόμβοι RON παρακολουθούν τη λειτουργία και την ποιότητα των δρομολογήσεων μεταξύ τους, και χρησιμοποιούν αυτές τις πληροφορίες για να αποφασίσουν εάν θα δρομολογήσουν τα πακέτα άμεσα μέσω του Διαδικτύου ή μέσω άλλων κόμβων RON, βελτιώνοντας το επίπεδο της ασφάλειας.

Η βασική αρχή των Υπερκείμενων Δικτύων είναι ότι θα πρέπει να παρέχει δρομολόγηση με τα ίδια χαρακτηριστικά απόδοσης όπως τα φυσικά δίκτυα.

Ο Keromytis στο [17] έχει υποστηρίξει ότι τα Υπερκείμενα Δίκτυα μπορούν να χρησιμοποιηθούν και κατά των ακραίων επιθέσεων. Σε αυτές τις προσπάθειες τα δίκτυα αυτά αντιμετωπίζονται κυρίως ως ασύρματα δίκτυα που έχουν το πλεονέκτημα της φορητότητας (mobility). Η φορητότητα μπορεί επίσης να

μεταφραστεί στη δυνατότητα «να κρυφτεί» η πληροφορική υποδομή, γεγονός που μπορεί να είναι ιδιαίτερα ενδιαφέρουσα για μια σειρά περιπτώσεων όπως π.χ. για στρατιωτικούς σκοπούς.

Εντούτοις αυτές οι λύσεις τείνουν να είναι αρκετά ακριβές, δεδομένου ότι απαιτούν την ανάπτυξη των νέων πληροφοριακών υποδομών, οι οποίες πιθανότατα θα υπο-χρησιμοποιούνται. Η πιθανότητα αυτή είναι ανάλογη της χαμηλής πιθανότητας εμφάνισης ακραίων επιθέσεων.

6.3.1.4. Ανάλυση της προσέγγισης

Οι οργανισμοί και ειδικά οι χρηματοπιστωτικοί οργανισμοί επενδύουν σε ετήσια βάση σημαντικά ποσά στις λύσεις Ανάκαμψης από Καταστροφή στοχεύοντας κυρίως στην αντιμετώπιση φυσικών ή πολύ μεγάλης κλίμακας καταστροφών, οι οποίες όμως σπάνια συμβαίνουν. Αυτές οι εναλλακτικές υποδομές τείνουν να είναι σε μια κατάσταση μόνιμης αναμονής αναμένοντας μια μεγάλη καταστροφή.

Η παρούσα προσέγγιση βασίζεται στην άποψη ότι η χρήση των τεχνικών που σχετίζονται με τα υπερκείμενα δίκτυα μπορεί να είναι αποδοτικότερη σε οικονομικούς όρους με το συνδυασμό τέτοιων υποδομών Ανάκαμψης από Καταστροφή. Η κύρια διαφορά μεταξύ των προηγούμενων λύσεων και του προτεινόμενου είναι ότι το υπερκείμενο δίκτυο μπορεί να είναι ένα υπάρχον δίκτυο (ή σύνολο συστημάτων) και όχι κάποια δικτυακή υποδομή η οποία θα πρέπει να αναπτυχθεί εξ αρχής. Το υπάρχον αυτό δίκτυο ή υποδομή προτείνεται να είναι η υποδομή Ανάκαμψης από Καταστροφή η οποία αποτελεί κοινή πρακτική των περισσοτέρων μεγάλων οργανισμών.

Η χρήση μιας υποδομής Ανάκαμψης από Καταστροφή ως ενσύρματο ή ασύρματο υπερκείμενο δίκτυο πρέπει να ικανοποιεί όσο το δυνατόν περισσότερες από τις ακόλουθες απαιτήσεις:

α. Οι δύο υποδομές δικτύου, η Κύρια και η Εναλλακτική, πρέπει να κατατέμνονται σε διακριτές ζώνες και να επιτρέπουν τη απομονωμένη

λειτουργία της ζώνης η οποία δέχεται την επίθεση. Ειδική φροντίδα θα πρέπει να ληφθεί για τον αριθμό ζωνών που θα υλοποιηθεί. Ένας μεγάλος αριθμός ζωνών αυξάνει την πολυπλοκότητα της διαχείρισης και της συντήρησης, ενώ ένας μικρός αριθμός ζωνών αυξάνει τον αριθμό των εμπλεκομένων συστημάτων άρα και του χρόνου απόκρισης σε μια επίθεση. Επομένως, είναι απαραίτητη μια ισορροπία μεταξύ της πολυπλοκότητας και της διακριτότητας (granularity) της υποδομής. Ο Πίνακας 6.17 παρουσιάζει μερικά από τα Τμήματα δικτύων (Ζώνες) που μπορούν να εξεταστούν κατά την κατάτμηση δικτύων.

#	Ζώνη Δικτύου	Συστήματα και Υπηρεσίες
1	Δίκτυο Σύνδεσης με το Διαδίκτυο	IDS, Εξωτερικά Firewalls, Proxy Servers, Mail Gateways
2	Δίκτυο Χρηστών	Χρήστες Laptops, η-κιόσκια, Χρήστες Desktop, IDS, Εσωτερικά Firewalls
3	Δίκτυο Τηλεφωνικών Επικοινωνιών	IDS, Remote Access Servers, Terminal Server, Dial-in devices
4	Δίκτυο Πρόσβασης μέσω VPN	Κατάληξη VPN, IDS
5	Δίκτυο Διαχείρισης	Firewalls Διαχείρισης, Διαχείριση IDS, Διαχείριση Δικτύου
6	Ασύρματο Δίκτυο	Wireless Access Points, IDS, Χρήστες μέσω ασύρματου δικτύου
7	Δίκτυο παροχής η-υπηρεσιών	IDS, Εξωτερικά DNS, Secure FTP, Διακομιστές, Εξυπηρετητές Εφαρμογών, Firewall
8	Κεντρικό Δίκτυο	IDS, Υπηρεσίες Εσωτερικού Δικτύου, Υπηρεσίες Καταλόγου, Βάσεις Δεδομένων, Εξυπηρετητές Αρχείων/ Εκτυπώσεων
9	Δίκτυο Ευρείας περιοχής	Υπηρεσίες Συνεργατών, IDS, δρομολογητές ευρείας περιοχής, Συνδέσεις με συνεργάτες / προμηθευτές / υποκαταστήματα / θυγατρικές

Πίνακας 6.17 – Τμήματα δικτύου

β. Το δίκτυο του Κύριου Μηχανογραφικού Κέντρου θα πρέπει να έχει εγκαταστήσει κατάλληλα Συστήματα Ανίχνευσης Επιθέσεων (Intrusion Prevention Systems / IDS), προκειμένου να παρακολουθεί, να επισημαίνει και να ενεργοποιεί το υπερκείμενο δίκτυο στις καταστάσεις ακραίων επιθέσεων.

γ. Και οι δύο υποδομές, η Κύρια και η Εναλλακτική, πρέπει να κάνουν εκτενή χρήση μηχανισμών αντιγραφής (replication) και πλεονασμού (redundancy) που θα επιτρέπουν την προστασία των δεδομένων. Μια σειρά από μεθοδολογίες λήψης εφεδρικών αντιγράφων αλλά και πραγματοποίησης διπλών αντιγράφων στην Εναλλακτική υποδομή θα πρέπει να σχεδιαστεί ώστε να διασφαλίζει πάντα την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, ακόμα και όταν είναι το δίκτυο της Κύριας Υποδομής αντιμετωπίζει κάποια επίθεση.

δ. Οι δύο υποδομές θα πρέπει να χρησιμοποιούν διαφορετικές πλατφόρμες και τεχνολογίες για τη λειτουργία τους. Η πληροφορική υποδομή θα πρέπει να εφαρμοστεί χρησιμοποιώντας διαφορετικά εργαλεία και τις τεχνικές εφαρμογής, ώστε οποιαδήποτε επιτυχής επίθεση στο Κύριο Κέντρο να χρειάζεται μια διαφορετική προσέγγιση για το υπερκείμενο δίκτυο. Σε κάθε περίπτωση, η συνολική λειτουργικότητα του Εναλλακτικού Κέντρου θα πρέπει αντιστοιχεί με τη λειτουργικότητα της Κύριου Κέντρου.

ε. Η υποδομή Ανάκαμψης από Καταστροφή θα πρέπει να υλοποιηθεί με διαφορετικές διευθύνσεις IP για κάθε ένα από τα συστήματά της.

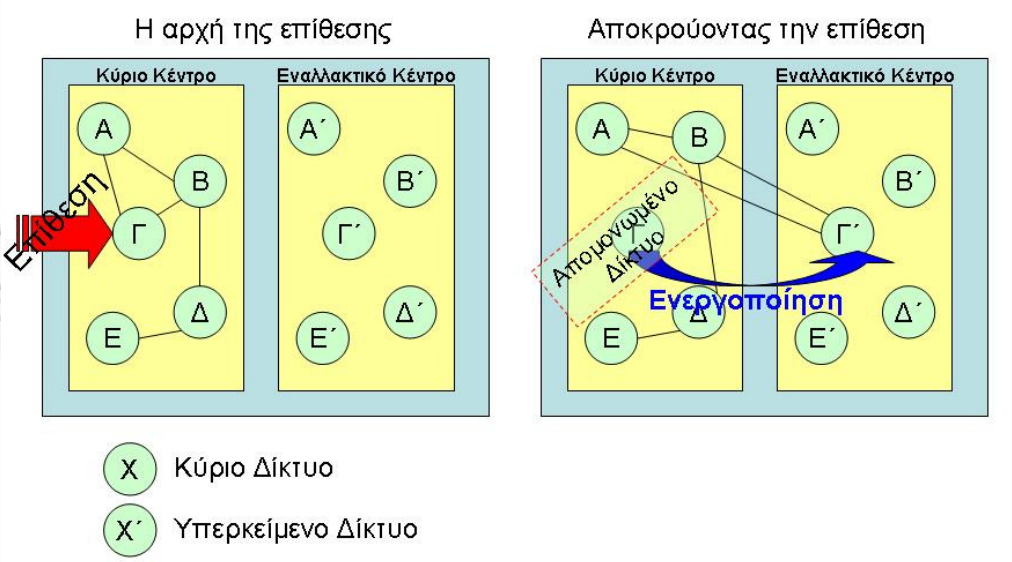
στ. Η υποδομή Ανάκαμψης από Καταστροφή θα πρέπει να χρησιμοποιεί διαφορετικά δίκτυα πρόσβασης. Αυτό συνεπάγεται ότι πρέπει να χρησιμοποιηθεί ένα διαφορετικό εύρος «δημόσιων» διευθύνσεων IP έτσι ώστε οποιοσδήποτε πιθανός εισβολέας δεν θα μπορεί να δρομολογήσει αυτόματα τις προσπάθειες επίθεσης στο υπερκείμενο δίκτυο. Για αυτό τον σκοπό, οι χρόνοι ενημέρωσης των εξυπηρετητών ονοματοδοσίας (Domain Name Servers / DNS) θα πρέπει να είναι πιο μικροί από αυτούς που δίνονται εξ ορισμού. Εντούτοις πρέπει να τονιστεί ότι οι πάρα πολύ μικροί χρόνοι ενημέρωσης μπορεί να προκαλέσουν κύματα συχνών αιτημάτων στους DNS,

υπερφορτώνοντάς τους και δημιουργώντας έτσι έναν πιθανό στόχο για επιθέσεις DoS και DDoS.

Αν και μερικές από τις παραπάνω απαιτήσεις μπορούν να μην ισχύουν σε όλες τις υποδομές, όσο περισσότερες απαιτήσεις ικανοποιούνται, τόσο περισσότερα είδη ακραίων επιθέσεων μπορούν να αποκρουσθούν.

Ο μηχανισμός αντιμετώπισης ακραίων επιθέσεων θα πρέπει να είναι έτοιμος να αντιμετωπίσει τις επιθέσεις DDoS, με την ενεργοποίηση του αντίστοιχου υπερκειμένου δικτύου. Σε αυτήν την περίπτωση οι κύριες συσκευές ή τα συστήματα δικτύων, τα οποία δέχονται επίθεση, δεν θα είναι πλέον ενεργά και οποιαδήποτε παραβίαση της ασφαλείας σχετίζεται με αυτά δεν θα έχει καμιά επίδραση στο υπόλοιπο δίκτυο αλλά και στην παροχή των υπηρεσιών. Μπορεί ακόμα να πραγματοποιηθεί μια επιβεβαίωση από κάποιον διαχειριστή πριν από την ενεργοποίηση του υπερκειμένου δικτύου, γεγονός που πιθανώς θα αύξανε το χρόνο απόκρισης σε μια επίθεση, αλλά επίσης θα μείωνε και τον αριθμό των ενεργειών που αναφέρονται σε ψευδείς επιθέσεις.

Το Διάγραμμα 6.11 απεικονίζει τη γενική διαδικασία αντιμετώπισης επιθέσεων DoS και DDoS.



Διάγραμμα 6.11 – Διαδικασία αντιμετώπισης ακραίων επιθέσεων DDoS

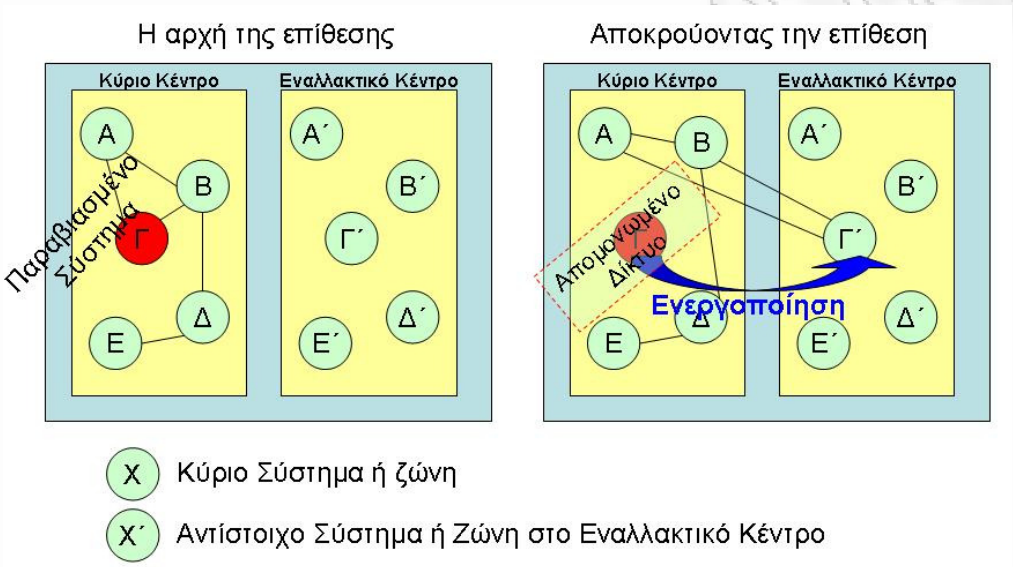
Το Κύριο Κέντρο της Πληροφοριακής Υποδομής του παραδείγματος αποτελείται από τα τμήματα δικτύων Α, Β, Γ, Δ και Ε. Αυτά τα τμήματα δικτύων διασυνδέονται μέσω μιας σειράς συσκευών όπως τα switches επιπέδου 3, hubs και τα firewalls επιπέδων 3 έως 7. Όταν το τμήμα δικτύου Γ δέχεται μια επίθεση, παραδείγματος χάριν μια επίθεση DDoS που βασίζεται σε ένα IP packet flooding, μόλις αυτή ανιχνευτεί, η συγκεκριμένη ζώνη απομονώνεται και το αντίστοιχο υπερκείμενο δίκτυο Γ΄ στην υποδομή Ανάκαμψης από Καταστροφή ενεργοποιείται, έτσι ώστε όλη η δικτυακή κίνηση να οδηγείται πλέον προς το τμήμα Γ΄ δικτύων.

Στην περίπτωση κατά την οποία οι απαιτήσεις για τη διαφορετική διευθυνσιοδότηση (δηλ. οι απαιτήσεις ε και στ) ικανοποιούνται, το υπόλοιπο δίκτυο θα πρέπει να ενημερωθεί για τις νέες διευθύνσεις IP που χρησιμοποιούνται για να εξυπηρετήσουν τη λειτουργία και τις υπηρεσίες της ζώνης Γ΄. Αυτό γίνεται με την άμεση ενημέρωση των εξωτερικών DNS κεντρικών υπολογιστών της επιχείρησης, δηλ. τους κεντρικούς υπολογιστές που είναι αρμόδιοι για τη διαχείριση των DNS πληροφοριών για τον οργανισμό. Μπορεί επίσης να υπάρχει ανάγκη να αλλαχτούν οι σχετικοί κανόνες και πολιτικές στα firewalls, έτσι ώστε επιτρέπουν την κυκλοφορία από και προς τη νέα διεύθυνση IP του υπερκείμενου δικτύου Γ'. Η δυναμική αλλαγή των πολιτικών των firewalls είναι δυνατή με την χρήση και παραμετροποίηση των πιο εξελιγμένων IDS.

Επιπλέον, ο μηχανισμός αντιμετώπισης ακραίων επιθέσεων πρέπει να είναι σε θέση να αντιμετωπίσει επιθέσεις που προκαλούνται εκ των έσω όπως εκείνοι που περιγράφονται στα διάφορα είδη των βυζαντινών επιθέσεων. Σε αυτές τις καταστάσεις, τα συστήματα ή ζώνες που έχουν παραβιαστεί, πρέπει να απομονωθούν από το υπόλοιπο δίκτυο, ενώ τα αντίστοιχα συστήματα ή ζώνες θα πρέπει να ενεργοποιηθεί αντ' αυτού. Προκειμένου να αποτραπεί ότι ο επιτιθέμενος δεν θα είναι σε θέση να παραβιάσει τα αντίστοιχα συστήματα και

ζώνες του υπερκείμενου δικτύου, θα πρέπει να υπάρχει για το τελευταίο ένας διαφορετικός μηχανισμός διαχείρισης και ελέγχου προσπέλασης .

Το Διάγραμμα 6.12 απεικονίζει τη γενική διαδικασία την απόκρουσης επιθέσεων εκ των έσω ακολουθώντας το παράδειγμα με τη διαδικασία που παρουσιάζεται στο Διάγραμμα 6.11.



Διάγραμμα 6.12 – Διαδικασία απόκρουσης ακραίων επιθέσεων εκ των έσω

Παρόμοια, το Κύριο Κέντρο της Πληροφοριακής Υποδομής του παραδείγματος αποτελείται από τα τμήματα δικτύων Α, Β, Γ, Δ και Ε. Αυτές οι ενότητες μπορούν να είναι τμήματα ή ζώνες δικτύων, συσκευές δικτύων, κεντρικοί υπολογιστές, ένα ενιαίο σύστημα ή ομάδα συστημάτων. Όταν το τμήμα Γ αντιμετωπίσει μια επίθεση και αυτή ανιχνευτεί, το συγκεκριμένο τμήμα θα απομονωθεί και το αντίστοιχό του Γ′ στην υποδομή Ανάκαμψης από Καταστροφή ενεργοποιείται, έτσι ώστε όλη η δικτυακή κίνηση να δρομολογείται πλέον προς το τμήμα Γ΄ δικτύων.

Όπως και στις εξωτερικές ακραίες επιθέσεις, μπορεί ακόμα να υπάρχει μια ανάγκη να αλλαχτούν οι σχετικοί κανόνες των firewalls, έτσι ώστε επιτρέπουν την κυκλοφορία από και προς τη νέα διεύθυνση IP. Σε αυτή την περίπτωση, η αλλαγή των πολιτικών των firewalls είναι ακόμα σημαντικότερη για την απομόνωση της πηγής της εσωτερικής επίθεσης. Η δυναμική αλλαγή των

πολιτικών των firewalls είναι επίσης δυνατή χρησιμοποιώντας και ρυθμίζοντας κατάλληλα τα πιο εξελιγμένα IDS.

6.3.2. Χρήση Παραγωγικών Υποδομών Ανεκτικών σε Σφάλματα

Οι υποδομές Ανάκαμψης από Καταστροφή, που έχουν γίνει κοινός τόπος όλων των μεγάλων Πληροφοριακών Υποδομών, θα μπορούσαν να μετασχηματιστούν σε Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα προκειμένου να αυξηθούν η παραγωγικότητα, η αποτελεσματικότητα και η διαθεσιμότητά τους. Η συγκεκριμένη προσέγγιση παρουσιάζει τα χαρακτηριστικά και τα πλεονεκτήματα των Παραγωγικών Υποδομών Ανεκτικών σε Σφάλματα (Fault Tolerant Production Infrastructures / FTPIs) προτείνοντας μια μεθοδολογία για το μετασχηματισμό των συστημάτων υψηλής διαθεσιμότητας στα οποία βασίζονται οι υποδομές Ανάκαμψης από Καταστροφή σε Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα.

6.3.2.1. Ανοχή σε σφάλματα

Έχοντας εξετάσει στο κεφάλαιο 2 τις βασικές έννοιες της διαθεσιμότητας, της ανοχής ελαττωμάτων καθώς επίσης και της εξισορρόπησης φορτίων, είναι πλέον δυνατό να παρουσιαστούν τα αντίστοιχα οφέλη μιας Υποδομής Ανεκτικής σε Σφάλματα η οποία θα μπορούσε να χρησιμοποιηθεί για παραγωγικούς σκοπούς.

Ένα από τα θεμελιώδη πλεονεκτήματα των συστημάτων υψηλής διαθεσιμότητας που είναι βασισμένα στις τεχνικές εξισορρόπησης φορτίων που αναφέρθηκαν στο κεφάλαιο 2 είναι η αυξημένη προστασία της λειτουργίας των συστημάτων.

Εκτός από αυτό, η υλοποίησή τους μπορεί να βελτιώσει επιπλέον και τη γενικότερη αποδοτικότητα. Όπως χαρακτηριστικά αναφέρει ο Miller στο [18] «Η παραχώρηση πόρων σύμφωνα με την πραγματική ζήτηση (Capacity on Demand), η εξισορρόπηση φορτίων, η παραχώρηση πόρων για τη συντήρηση

και η μηδενική απώλεια δεδομένων είναι όλα τα παραδείγματα της προστιθέμενης αξίας που μπορεί παράσχει μια αρχιτεκτονική συνεχούς λειτουργίας».

Όπου υπάρχει προστιθέμενη αξία, μπορεί να υπάρξει ROI. Ωστόσο, η ποσοτικοποίηση του ROI σε αυτή την κατάσταση δεν είναι απλή. Οι αυξήσεις στην αποδοτικότητα είναι συχνά ασαφείς κατά τη μέτρησή τους, με μοναδική ίσως εξαίρεση την περίπτωση που οδηγούν σε απτή εξοικονόμηση όπως οι μειώσεις προσωπικού ή άλλες τελικές δαπάνες. Εντούτοις, τα συστήματα υψηλής διαθεσιμότητας πρέπει να εξεταστούν για οποιαδήποτε πιθανή συμβολή ROI.

Δεδομένου ότι η συχνότητα των προγραμματισμένων περιόδων διακοπής των πληροφοριακών συστημάτων ενός οργανισμού έχει αυξητική τάση λόγω του αυξανόμενου αριθμού ανάπτυξης νέων εφαρμογών αλλά και των συνεχών αναβαθμίσεων και ενημερώσεων ασφάλειας, η ανάγκη να συμπιεστούν τα συγκεκριμένα χρονικά διαστήματα διακοπής όσο το δυνατόν περισσότερο έχει γίνει πιο επείγουσα. Σύμφωνα με τον Atwood στο [19] για κάποιες επιχειρήσεις, οι χρόνοι διακοπής ή ακόμα και η επιβράδυνση με μια ελάχιστη διάρκεια 5-10 λεπτών μπορούν να έχουν μια ουσιαστική επιρροή στα έσοδά τους.

Όπως έδειξε η προηγούμενη προσέγγιση, μπορεί να υπάρξει μια παράλληλη χρήση ενός τμήματος μιας υποδομής Ανάκαμψης από Καταστροφή προκειμένου να αντιμετωπιστούν οι ακραίες επιθέσεις. Αναπτύσσοντας περαιτέρω αυτή την προσέγγιση, τα οφέλη που περιγράφονται ανωτέρω πολλαπλασιάζονται όταν τα τμήματα του Κύριου Κέντρου λειτουργούν μαζί με τα αντίστοιχά τους στην υποδομή Ανάκαμψης από Καταστροφή, με τέτοιο τρόπο που να πραγματοποιούν εξισορρόπηση των δικτυακών φορτίων και των αιτημάτων προς τις εφαρμογές.

Είναι, επομένως, εμφανές ότι οι οργανώσεις έχουν περισσότερους από έναν λόγους να μετασχηματίσουν τις υπάρχουσες υλοποιήσεις τους και να επιλέξουν την προσέγγιση των Υποδομών Ανεκτικών σε Σφάλματα. Τα ίδια ακριβώς εργαλεία που χρησιμοποιούνται για την υψηλή διαθεσιμότητα όπως οι συστοιχίες εξυπηρετητών (clusters), η διαχείριση όγκου (volume management) και η εξισορρόπηση φορτίων, μπορούν να αυτοματοποιήσουν τις βασικές διαδικασίες που θα μείωναν το ΜΧΕ αλλά και το αντίστοιχο κόστος της διαχείρισης χρόνου διακοπής.

Η εξοικονόμηση που μπορεί να επιτευχθεί από αυτά τα χαρακτηριστικά προστιθέμενης αξίας είναι πολύ σημαντική και μπορεί να συνεισφέρει στη μείωση των δαπανών που συνδέονται με τους προγραμματισμένους χρόνους διακοπής. Επιπλέον, το χρονικό διάστημα διακοπής της λειτουργίας συμπιέζεται έτσι ώστε οι επιχειρησιακές λειτουργίες μπορούν να συνεχιστούν με ελάχιστη ή καθόλου διακοπή.

Επιπλέον των παραπάνω, οι Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα μπορούν επίσης να συνεισφέρουν στη συμμόρφωση με τις περιβαλλοντικές απαιτήσεις και τις διεθνείς οδηγίες που σχετίζονται με τις πράσινες τεχνολογίες (Green IT) με τη μείωση των απαιτήσεων κατανάλωσης ρεύματος. Η κατανάλωση του ρεύματος, όπως επίσης και οι σχετικές εκπομπές του διοξειδίου του άνθρακα που απαιτείται για την παροχή ρεύματος και τη λειτουργία των υποδομών από το Κύριο Μηχανογραφικό Κέντρο, διανέμεται στα γεωγραφικά διασκορπισμένα Εναλλακτικά Μηχανογραφικά Κέντρα τα οποία θα κατανάλωναν την συγκεκριμένη ενέργεια ακόμα και σε κατάσταση αναμονής.

Ο Πίνακας 6.18 αντιπαραβάλλει τα σημεία στα οποία διαφέρουν οι τρεις προσεγγίσεις.

	Υψηλή Διαθεσιμότητα	**Ανοχές σε βλάβες**	**Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα**
Σκοπός / Επίδραση	Να επιτρέψει τη γρηγορότερη ανάκαμψη χαμένων δεδομένων και των καθυστερημένων επιχειρηματικών λειτουργιών σε περίπτωση καταστροφής	Να προβλέπει και να αποφεύγει κάποια είδη καταστροφών πριν αυτές συμβούν	Να προβλέπει και να αποφεύγει τα περισσότερα είδη καταστροφών πριν αυτές συμβούν. Να αυξήσει την παραγωγικότητα των πληροφοριακών υποδομών του οργανισμού
Κόστος	Απτές Επενδύσεις Πληροφορικής	Απτές Επενδύσεις Πληροφορικής. Το ROI μπορεί να υπολογιστεί σε κάποιες περιπτώσεις	Απτές Επενδύσεις Πληροφορικής με υπολογίσιμο ROI
Οφέλη	Γρηγορότεροι χρόνοι ανάκαμψης, μείωση χαμένων εσόδων και παραγωγικότητας, μειωμένο κόστος ανάκαμψης	Μειωμένη πιθανότητα καταστροφής, βελτίωση της λειτουργικής αποδοτικότητας, μειωμένο ΜΧΕ και κόστος διαχείρισης της μη διαθεσιμότητας	Ελαχιστοποίηση της πιθανότητας καταστροφής, βελτίωση της λειτουργικής αποδοτικότητας, μειωμένο ΜΧΕ και κόστος διαχείρισης της μη διαθεσιμότητας
ROI	Θεωρητικό και δύσκολα υπολογίσιμο διότι μπορεί να μετρηθεί μόνο σε περίπτωση καταστροφής	Η Μείωση της πιθανότητας καταστροφής δεν είναι υπολογίσιμη. Ο μειωμένος ΜΧΕ συνεπάγεται πραγματική εξοικονόμηση των δαπανών με την αυτοματοποίηση των λειτουργιών, η οποία μειώνει τις ανάγκες σε πόρους αλλά και την πιθανότητα ανθρωπίνου λάθους.	Η Μείωση της πιθανότητας καταστροφής δεν είναι υπολογίσιμη. Η βελτίωση της λειτουργικής αποδοτικότητας μπορεί να έχει άμεσο αντίκτυπο στα έσοδα και τα έξοδα, ενώ μπορεί να έχει απτή συνεισφορά σε πωλήσεις και μείωση δαπανών. Ο μειωμένος ΜΧΕ συνεπάγεται πραγματική εξοικονόμηση των δαπανών με την αυτοματοποίηση των λειτουργιών, η οποία μειώνει τις ανάγκες σε πόρους αλλά και την πιθανότητα ανθρωπίνου λάθους. Αποτελούν απτά οφέλη που μεταφράζονται σε μείωση των χαμένων εσόδων καθώς και των λειτουργικών εξόδων.

Πίνακας 6.18 – Διαφορές προσεγγίσεων διαθεσιμότητας

6.3.2.2. Αρχές Μετασχηματισμού Υποδομών

Όταν ένας οργανισμός πάρει την απόφαση να ακολουθήσει την προσέγγιση που παρουσιάστηκε στην προηγούμενη παράγραφο θα πρέπει να επιλέξει και

την κατάλληλη μεθοδολογία για το μετασχηματισμό της υπάρχουσας πληροφοριακής του υποδομής σε μια Παραγωγικής Υποδομής Ανεκτικής σε Σφάλματα. Οι βασικές αρχές μιας τέτοιας μεθοδολογίας είναι η θεωρία της διαχείρισης των αλλαγών που περιγράφονται στο κεφάλαιο 3 αλλά και η σχετική τεχνική εμπειρία όπως αυτή περιγράφεται στα [21] και [22].

Στις σημερινές πληροφοριακές υποδομές, οι εφαρμογές είναι αλληλένδετες και ενσωματωμένες μεταξύ τους όσο ποτέ. Συγχρόνως, τα μοιραζόμενα στοιχεία των υποδομών είναι πιο κοινά, ενώ η διαχείριση του χρόνου συντήρησης μπορεί να είναι μια υπερβολικά σύνθετη διαδικασία.

Στο πλαίσιο αυτό, οι σημερινές πρακτικές της βιομηχανίας της πληροφορικής περιλαμβάνουν χρήσιμα σχετικά διδάγματα. Το πρώτο είναι ότι μια οργάνωση πρέπει πάντα να στοχεύσει να μειώσει το μη σχεδιασμένο χρόνο διακοπής, δεδομένου ότι ένα τέτοιο γεγονός κοστίζει σε χρήματα και φήμη.

Το σημείο που απορρέει από την τεχνική εμπειρία και συγκεκριμένα από τον Garbani στο [20] του όποιου η έρευνα έδειξε ότι «80% ή και περισσότερο του μη σχεδιασμένου χρόνου διακοπής είναι το αποτέλεσμα που οφείλεται στους ανθρώπους και στις διαδικασίες και όχι στο υλικό ή στις βλάβες του λογισμικού». Αυτό συνεπάγεται ότι ένας οργανισμός θα πρέπει να ασχολείται λιγότερο με θέματα όπως η αλλοίωση δεδομένων, τα σφάλματα των εφαρμογών και τις αστοχίες των υλικών, εστιάζοντας το ενδιαφέρον του στα λάθη από ρυθμίσεις, προγραμματιστικά λάθη, λάθη χειριστών, καθυστερημένες εργασίες κ.λπ. Έτσι, προκειμένου να αντιμετωπιστούν αυτές οι αιτίες διακοπών, μια οργάνωση θα πρέπει να χορηγήσει τα κατάλληλα κονδύλια και τον απαραίτητο χρόνο στους ανθρώπους και τις διαδικασίες. Παραδείγματα των θεμάτων που θα πρέπει να ληφθούν υπόψη είναι η επιλογή και κατάρτιση του ανθρώπινου δυναμικού, η διαχείριση των προβλημάτων, η διαχείριση των περιστατικών ασφάλειας, ο σχεδιασμός των εργασιών, οι δοκιμές ετοιμότητας και ο σχεδιασμός της διάθεσης πόρων.

Το τρίτο σημείο σχετίζεται περισσότερο με την τεχνολογία και αναφέρει ότι ένας οργανισμός πρέπει να ελαχιστοποιήσει τα μοναδικά σημεία της αποτυχίας (single points of failure), να φροντίσει τους περιβαλλοντικούς παράγοντες, τις απειλές στις εγκαταστάσεις και τα δίκτυα, να χρησιμοποιήσει ισορροπιστές φορτίων (Load Balancers), επιπλέον επιμελητές (Dispatchers), μηχανισμούς αντιγραφής δεδομένων, μηχανισμούς κλωνοποίησης, τεχνολογίες του RAID, όπως η αντανάκλαση (mirroring), η ράβδωση (striping) και η αλλαγή εν ώρα λειτουργίας (hot swap availability). Επιπλέον ένας οργανισμός πρέπει να στοχεύει στην χρήση των τεχνολογιών υψηλής διαθεσιμότητας, ή ακόμα καλύτερα με τεχνικές συστημάτων Ανεκτικών σε σφάλματα.

Προκειμένου να υλοποιηθούν οι υποδομές που θα μπορούσαν να αντιμετωπίσουν αυτά τα ζητήματα και να χρησιμοποιήσουν τις αναφερθείσες τεχνολογίες, ένας οργανισμός πρέπει να συνειδητοποιήσει τους αρχιτεκτονικούς περιορισμούς καθώς και όλες τις αλληλεξαρτήσεις των εφαρμογών και τις πιθανές εξαρτήσεις με άλλα υπο-συστήματα.

Επιπλέον, θα πρέπει να διαχειριστεί άλλες, παράλληλες, προγραμματισμένες αλλαγές, με την ανάπτυξη της κατάλληλης υποδομής και την αναβάθμιση των υλικών, των λειτουργικών συστημάτων, των βάσεων δεδομένων και των εφαρμογών. Μια άλλη ανάγκη που πρέπει να καλυφθεί είναι η ανάγκη δημιουργίας των κατάλληλων υποδομών δοκιμής. Μέσα σε αυτό το πλαίσιο η οργάνωση πρέπει να στοχεύσει σε μειωμένους χρόνους συντήρησης, ως αποτέλεσμα του καλυτέρου συντονισμού και αποδοτικότητας.

Λαμβάνοντας υπόψη τα παραπάνω ένας οργανισμός πρέπει να προσπαθεί να ακολουθεί τους παρακάτω κανόνες κατά την προσπάθειά του για την υλοποίηση μιας Παραγωγικής Υποδομής Ανεκτικής σε Σφάλματα. Αφενός, θα πρέπει να ενσωματώσει τη υψηλή διαθεσιμότητα των εφαρμογών και των υπηρεσιών από την φάση του σχεδιασμού, δεδομένου ότι αυτό μπορεί να είναι εξαιρετικά δύσκολο να ενσωματωθεί στις επόμενες φάσεις, όπως η υλοποίηση. Αφετέρου, θα πρέπει να αναπτυχθεί ένας καλός σχεδιασμός των

κρίσιμων υπηρεσιών ώστε μόνο αυτές να εξυπηρετούνται με τις υψηλού κόστους Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα. Το κόστος αυτών όπως υπολογίζεται από τον Scott στο [23] μπορεί να φτάσει και 3.5 φορές περισσότερο από μια κλασική υποδομή χωρίς τους αντίστοιχους μηχανισμούς.

6.3.2.3. Περιγραφή της μεθόδου μετασχηματισμού

Λαμβάνοντας υπόψη όλες τις παραπάνω πηγές, η προτεινόμενη στρατηγική μετασχηματισμού συνδυάζει τη θεωρία διαχείρισης αλλαγών αλλά και την τεχνική εμπειρία. Υπάρχουν επτά φάσεις που αποτελούν τη διαδικασία μετασχηματισμού από τα τις Υποδομές Υψηλής Διαθεσιμότητας στις Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα. Αυτές είναι:

- Φάση 1: Καθορισμός του αντικειμένου του μετασχηματισμού
- Φάση 2: Κατηγοριοποίηση των ομάδων συστημάτων
- Φάση 3: Ανάλυση εφαρμογών
- Φάση 4: Ανάλυση διαδικασιών
- Φάση 5: Ανάλυση κόστους
- Φάση 6: Επιχειρηματική απόφαση
- Φάση 7: Εκτέλεση του μετασχηματισμού

<u>Καθορισμός του αντικειμένου του μετασχηματισμού</u>

Είναι αυτονόητο ότι ένα πρόβλημα που είναι καλά καθορισμένο και οριοθετημένο είναι ένα πρόβλημα που μπορεί να λυθεί ευκολότερα. Κατά τη διάρκεια της πρώτης φάσης του μετασχηματισμού, ο οργανισμός πρέπει να αποφασίσει ποια συστήματα είναι υποψήφια για μετασχηματισμό. Κατά συνέπεια, για κάθε τομέα εφαρμογής, πρέπει να καθοριστεί ποιο είναι το πεδίο μετασχηματισμού, με τη συνεργασία και συμμετοχή των αρμοδίων αντιπρόσωπών των χρηστών. Συγχρόνως, ο στόχος που αφορά τον προγραμματισμό των εργασιών του μετασχηματισμού όπως και ο στόχος που αφορά τη διαθεσιμότητα θα πρέπει επίσης να συμφωνηθούν. Δεδομένου ότι είναι δαπανηρότερο να αλλάξει ξανά οποιαδήποτε υποδομή, είναι σημαντικό να καθοριστούν και να σχεδιαστούν εξαρχής οι δύο αυτοί στόχοι, όπως ακριβώς και οποιαδήποτε άλλη λειτουργική απαίτηση.

Κατηγοριοποίηση των ομάδων συστημάτων

Η δεύτερη φάση στοχεύει στην κατηγοριοποίηση των ομάδων συστημάτων. Για παράδειγμα ένας οργανισμός θα μπορούσε να διακρίνει μεταξύ των Συστημάτων Επιχειρησιακής Υποστήριξης, των Λειτουργικών Συστημάτων Υποστήριξης, τα Συστήματα Ηλεκτρονικού Εμπορίου και τα Συστήματα Διοικητικής Υποστήριξης. Αυτή η κατηγοριοποίηση θα δώσει στον οργανισμό μια ιδέα σχετικά με τον τρόπο με τον οποίο αυτά τα συστήματα πρέπει να υλοποιηθούν σε όρους διαθεσιμότητας, εμπλουτίζοντας τις αποφάσεις που λαμβάνονται στην πρώτη φάση.

Ανάλυση εφαρμογών

Κατά τη διάρκεια της τρίτης φάσης, ο οργανισμός πρέπει να καταλάβει την αρχιτεκτονική κάθε εφαρμογής, τους πρόσθετους περιορισμούς, τις τυχόν χρονικές ανοχές στη διάθεσή τους στην παραγωγή καθώς και την προσαρμοστικότητα στις αλλαγές που διαθέτει. Επιπλέον, θα πρέπει να συγκεντρωθούν οι αλληλεξαρτήσεις μεταξύ των εφαρμογών μαζί με τα διαγράμματα αρχιτεκτονικής και ροών δεδομένων. Τέλος, θα πρέπει να ληφθούν αποφάσεις σχετικά με το εάν η τυχόν τροποποίηση των εφαρμογών για θα πρέπει να υλοποιηθεί από τον ίδιο τον οργανισμό ή δοθεί ως εργασία σε τρίτο.

Ανάλυση διαδικασιών

Σε αυτή την φάση, θα πρέπει να απαντήθουν με τεχνικές λεπτομέρειες ερωτήσεις όπως ποιες είναι οι παρούσες διαδικασίες λειτουργίας και δοκιμών των συστημάτων. Η τρέχουσα διαθεσιμότητα κάθε λειτουργίας και της εφαρμογής θα πρέπει επίσης να προσδιοριστεί. Επιπλέον, σε τι μπορεί η οργάνωση να προσβλέπει με τον υπάρχοντα προϋπολογισμό. Προκειμένου να δοθεί ευκολότερα απάντηση σε αυτές τις ερωτήσεις, θα πρέπει να χρησιμοποιηθούν μετρήσεις σχετικές με τη διαθεσιμότητα, την αποδοτικότητα και την απόδοση. Η τελική εργασία αυτής της φάσης είναι να προσδιοριστούν οι πρωταρχικές αιτίες του μη σχεδιασμένου χρόνου διακοπής των υπηρεσιών.

Ανάλυση κόστους

Οι σημαντικότερες φάσεις είναι οι φάσεις 5 και 6. Από το αποτέλεσμα αυτών των φάσεων εξαρτάται η απόφαση για την πραγματοποίηση του μετασχηματισμού. Στη φάση ανάλυσης του κόστους, η βασική ερώτηση που θα θέσουν τα υψηλόβαθμα διοικητικά στελέχη είναι ποιες βελτιώσεις μπορούν να πραγματοποιηθούν με στον οργανισμό από τον υπάρχοντα προϋπολογισμό. Για την ορθή απάντηση σε αυτό το ερώτημα, ο οργανισμός θα πρέπει να αναλογιστεί ποιες είναι οι σωστές περιοχές που μπορεί να επενδύσει για να αυξήσει τη διαθεσιμότητά του. Επιπλέον, ο οργανισμός θα πρέπει να γνωρίζει τις δαπάνες που απαιτούνται για να εφαρμόσει το μετασχηματισμό και να πετύχει τους στόχους που έχει θέσει. Σε αυτήν τη φάση θα πρέπει να ενθαρρυνθεί η συμμετοχή από όλους τους τομείς της οργάνωσης.

Επιχειρηματική απόφαση

Αυτή είναι η τελευταία φάση πριν από την εκτέλεση του μετασχηματισμού. Κατά τη διάρκεια αυτής της φάσης, ο οργανισμός θα πρέπει να αναπτύξει μια συνεπή προσέγγιση για να σταθμίσει τα επιχειρησιακά οφέλη ενάντια στο κόστος, διατηρώντας την προσοχή του στο βασικό επιχειρησιακό ζήτημα, το οποίο είναι να αυξηθεί η διαθεσιμότητα και ο βαθμός χρησιμότητας των συστημάτων του. Προς αυτή την απόφαση, μια οργανωτική επιτροπή ή οι καθορισμένοι ιδιοκτήτες των εφαρμογών θα πρέπει να σταθμίσουν τις επιχειρησιακές ανάγκες. Στην περίπτωση που η προσπάθεια κοστολόγησης και σχεδιασμού κάθε εφαρμογής ξεχωριστά είναι ακατόρθωτη, η διαδικασία αυτή μπορεί να εφαρμοστεί ομαδοποιώντας τις εφαρμογές. Σε κάθε περίπτωση, η επιτροπή απόφασης θα πρέπει να γνωρίζει τις οικονομικές δυνατότητες και τις επιθυμίες των χρηματοδοτών του μετασχηματισμού οι οποίοι πιθανώς να επηρεάζονταν από μελλοντικές δαπάνες που μια Παραγωγική Υποδομή Ανεκτική σε Σφάλματα μπορεί να επιφέρει.

Εκτέλεση του μετασχηματισμού

Η τελική φάση της προτεινόμενης στρατηγικής μετασχηματισμού είναι η πραγματική εκτέλεση του μετασχηματισμού. Προκειμένου να επιτευχθεί αυτό, ο οργανισμός, και ειδικά οι άνθρωποι που εμπλέκονται και επηρεάζονται, πρέπει να είναι αφοσιωμένοι στο πρόγραμμα. Ένας λεπτομερής και ρεαλιστικός καθορισμός τόσο των ανθρώπινων όσο και των χρηματικών πόρων είναι απαραίτητος. Ένα άλλο πολύ σημαντικό ζήτημα είναι να καθοριστεί ο ιδιοκτήτης της νέας υποδομής προκειμένου να καθιερωθεί ένα κοινό σημείο επικοινωνίας που θα μπορεί να διαχειρίζεται, ρυθμίζει, αναπτύσσει, τεκμηριώνει το σχέδιο μετασχηματισμού, με τους σχετικούς στόχους, δραστηριότητες, ευθύνες, ημερομηνίες, κ.λπ.

Τέλος, ο οργανισμός θα πρέπει να μετρήσει τα πραγματικά οφέλη του μετασχηματισμού έναντι του αρχικού στόχου, για μελλοντική χρήση ή για την χρησιμοποίησης αυτής της εμπειρίας σε πιθανά παράλληλα προγράμματα μετασχηματισμού.

6.3.3. Αποδοτικότητα Επενδύσεων στην Ασφάλεια

Εκτός από τον μετασχηματισμό υποδομών, που ήδη υπάρχουν, σε άλλες ασφαλέστερες και αποδοτικότερες υποδομές, η διαχείριση της ασφάλειας των πληροφοριακών υποδομών, συμπεριλαμβανομένων και των κρίσιμων υποδομών, σχετίζεται άμεσα και με την αξιολόγηση των επενδύσεων που αφορούν την ασφάλεια.

Η δεύτερη εναλλακτική προσέγγιση για την αύξηση της ασφάλειας που βασίζεται στην μέθοδο που περιγράφεται στο κεφάλαιο 4.4.2.2. υπολογίζει την ασφάλεια ως μια συνάρτηση έμμεσα σχετιζόμενων παραγόντων όπως είναι η συμμόρφωση στη νομοθεσία, τα κανονιστικά πλαίσια και τα πρότυπα, η διαθεσιμότητα των επιχειρηματικών υπηρεσιών, η απόδοση μιας συγκεκριμένης υπηρεσίας, το παθητικό (απώλειες) λόγω της παροχής της υπηρεσίας και το δείκτη της μετοχής της εταιρίας.

Η συσχέτιση αυτής της μεθόδου με τη βελτιστοποίηση της διαχείρισης της ασφάλειας πραγματοποιείται με σκοπό την αιτιολόγηση των επενδύσεων στην ασφάλεια. Στο πλαίσιο της αποδοτικότητας των επενδύσεων στην ασφάλεια, το βασικό ερώτημα το οποίο καλείται να απαντήσει η μεθοδολογία υπολογισμού της ασφάλειας με τη χρήση έμμεσα σχετιζόμενων παραγόντων είναι ποια και πόσα είναι τα επιχειρηματικά οφέλη από μια επένδυση ενός οργανισμού με σκοπό την αύξηση της ασφάλειας.

Βασιζόμενη στους παράγοντες CARLS, η εκτίμηση των κερδών από την αύξηση της ασφάλειας αντισταθμίζονται με το κόστος της σχετικής επένδυσης. Η διαφορά των δύο αποτυπώνεται ως η προστιθέμενη αξία της ασφάλειας της υπηρεσίας. Η αξία αυτή μπορεί να οριστεί και ως συνάρτηση της φήμης της εταιρίας, του πόσο «ορατή» είναι η επένδυση ασφάλειας στους πελάτες / επενδυτές, των κερδών που σχετίζονται άμεσα ή έμμεσα με την επένδυση αλλά και των οικονομικών απωλειών που μπορεί να προκληθούν από την μη πραγματοποίηση της επένδυσης.

Όπως αναφέρθηκε και στο κεφάλαιο 4 ο τελικός στόχος είναι να ισορροπήσουν οι επενδύσεις της ασφάλειας σε κάθε υπηρεσία ώστε να μεγιστοποιηθούν τα κέρδη του οργανισμού, τα οποία εκφράζονται ως ROI της συγκεκριμένης υπηρεσίας αλλά και του συνόλου των υπηρεσιών που προσφέρονται. Αυτό επιτυγχάνεται με τον παρακάτω τύπο:

$$\max ROI(Sec_1, Sec_2, ..., Sec_n)$$

υπό τον όρο

$$\sum_{i=1}^{n} (R_i - I_i - L_i) > 0$$

.Όπου:

Sec_n : Το τρέχον επίπεδο ασφάλειας της υπηρεσίας n

R_i : Η τρέχουσα απόδοση της υπηρεσίας i

I_i : Οι συνολικές επενδύσεις στην υπηρεσία i (μέρος της οποίας είναι οι επενδύσεις και τα λειτουργικά έξοδα της ασφάλειας για αυτή την υπηρεσία)

L_i : Το τρέχον παθητικό της υπηρεσίας i

Η προσέγγιση αυτή είναι σχετική με τον υπολογισμού της Απόδοσης της Επένδυσης στην Ασφάλεια (Return On Security Investment / ROSI) που αναλύεται από τον Sonnenreich στο [24].

Εκεί υποστηρίζεται ότι τα μειονεκτήματα και τα πλεονεκτήματα των εναλλακτικών επιλογών σε μια επένδυση στην ασφάλεια μεταφράζονται σε συγκεκριμένα κόστη και οικονομικά οφέλη (Cost & Benefit), ώστε να μπορέσουν τελικά να συσχετιστούν και να οδηγήσουν στον υπολογισμό της Ανάλυσης Κόστους-Οφέλους (Cost Benefit Analysis / CBA) και του ROI. Στην περίπτωση της ασφάλειας το ROI εκφράζεται ως ROSI.

Η κύρια διαφορά των δύο είναι ότι στο CBA αφαιρούνται τα κόστη από τα οφέλη με το αποτέλεσμα να εκφράζεται ως καθαρό ποσό κέρδους, ενώ στο ROI διαιρούνται τα οφέλη με τα κόστη με το αποτέλεσμα να δείχνει την απόδοση της επένδυσης για κάθε ευρώ. Οι δύο δείκτες αποκαλύπτουν διαφορετικές πτυχές μιας επένδυσης και χρησιμοποιούνται συμπληρωματικά η μια με την άλλη.

Ένας άλλος συνήθης τρόπος υπολογισμού του συνολικού κόστους μιας τεχνολογικής επένδυσης, συμπεριλαμβανομένων και των επενδύσεων στην ασφάλεια, είναι η χρήση του ολικού κόστους ιδιοκτησίας (Total Cost of Ownership / TCO) δηλαδή το πλήρες κόστος μιας επένδυσης. Ειδικότερα το TCO μιας επένδυσης στην ασφάλεια θα πρέπει να περιλαμβάνει πέρα από τα άμεσα κόστη κάθε «παραδοσιακής» επένδυσης πληροφορικής, κόστη όπως τα παρακάτω:

- Το κόστος που σχετίζεται με την αλλαγή των διαδικασιών του οργανισμού.

- Το κόστος πρόσληψης ή μετακίνησης ανθρώπινων πόρων του οργανισμού.
- Το κόστος εκπαίδευσης του προσωπικού.
- Το κόστος χρήσης ή αναβάθμισης των υπαρχόντων υποδομών.
- Το κόστος συμπληρωματικών υπηρεσιών για την ανάπτυξη και την υποστήριξη μιας νέας λύσης.
- Το κόστος που σχετίζεται με την παρακώλυση της ομαλής λειτουργίας του οργανισμού
- Το κόστος χρήσης υφιστάμενων εγκαταστάσεων

Ένα βασικό συμπέρασμα που προκύπτει είναι ότι ο βαθμός της μείωσης του κινδύνου δεν είναι και το συνολικό όφελος της εκάστοτε επένδυσης στην ασφάλεια. Θα πρέπει να επισημανθεί ότι μια επένδυση στην ασφάλεια δύναται να αποφέρει οφέλη σε πολλαπλές διαστάσεις. Πέρα από τη μείωση – αποφυγή του κινδύνου, η ασφάλεια μπορεί να συνεισφέρει και σε τομείς όπως η αύξηση της αξίας μιας επιχείρησης και η βοήθεια στην συμμόρφωση με κανονιστικές οδηγίες.

Το γεγονός είναι ότι πλέον η ασφάλεια δεν αντιμετωπίζεται ως τεχνολογική τάση αλλά ως αρωγός της επιχειρηματικής ανάπτυξης και αυτό θα πρέπει να λαμβάνεται υπόψη και στις σχετικές επενδύσεις. Το πιθανό κενό στην επικοινωνία, μεταξύ των ειδικών σε θέματα ασφάλειας και του διοικητικού προσωπικού μπορεί να γεφυρωθεί με την χρήση δεικτών όπως οι ROI (ROSI) , TCO και CBA.

6.4. Υπολογισμός οφελών των μεθοδολογιών

Με τις μεθόδους του κεφαλαίου 6.2 δημιουργούνται εύλογα ερωτήματα σχετικά με τα οφέλη που μπορούν να αποκομιστούν από αυτές. Για τον υπολογισμό των οφελών από τη μέθοδο της αντιμετώπισης Ακραίων Επιθέσεων χρησιμοποιείται η μεθοδολογία υπολογισμού της ασφάλειας με βάση τα δομικά στοιχεία της ασφάλειας που παρουσιάστηκε στο κεφάλαιο 4. Για τις Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα και την αντίστοιχη

μέθοδο μετασχηματισμού σε αυτές χρησιμοποιείται η βιβλιοθήκη ITIL και συγκεκριμένα ο τρόπος μέτρησης και παρακολούθησης με την χρήση των Βασικών Δεικτών Απόδοσης (Key Performance Indicators / KPIs).

Ο υπολογισμός των οφελών σε κάποιες περιπτώσεις είναι ισοδύναμος με τον υπολογισμό της ασφάλειας των πληροφοριακών υποδομών και συστημάτων που περιγράφονται στις παρακάτω παραγράφους. Η βασική άποψη που προκύπτει από τους παρακάτω υπολογισμούς είναι ότι η βελτίωση της ασφάλειας δεν μπορεί να επιτευχθεί χωρίς την ποσοτικοποίησή της.

6.4.1. Οφέλη μεθόδου αντιμετώπισης Ακραίων Επιθέσεων

Για τον υπολογισμό των οφελών από την εφαρμογή της μεθόδου αντιμετώπισης Ακραίων Επιθέσεων υπολογίζουμε και συγκρίνουμε την ασφάλεια δύο παρόμοιων υποδομών. Η υποδομή Α δεν κάνει χρήση των Εναλλακτικών Μηχανογραφικών Κέντρων για την αντιμετώπιση των Ακραίων Επιθέσεων ενώ η υποδομή Β κάνει χρήση.

Στην περίπτωση της υποδομής Α με τη χρήση των Εναλλακτικών Μηχανογραφικών Κέντρων και συγκεκριμένα στο παράδειγμα του Διαγράμματος 6.11, η επίθεση που δέχεται τμήμα του δικτύου μεταφράζεται σε μη διαθεσιμότητα, απώλεια εσόδων, όχι δημοσιοποίηση ή μείωση τιμών μετοχών και σταθερό επίπεδο συμμόρφωσης.

Στην περίπτωση της υποδομής Β που δεν γίνεται χρήση των Εναλλακτικών Μηχανογραφικών Κέντρων, η επίθεση που δέχεται το τμήμα δικτύου μιας παρόμοιας υποδομής μεταφράζεται σύμφωνα με τις διαφορές των δύο προσεγγίσεων που αναφέρθηκαν σε περισσότερη μη διαθεσιμότητα, μεγαλύτερη απώλεια εσόδων, πιθανή δημοσιοποίηση αλλά και μείωση των τιμών μετοχών και πιθανώς αποτελεί ένδειξη για την μη συμμόρφωση με πρότυπα και κανονισμούς ασφάλειας.

Για την εφαρμογή του τύπου του υπολογισμού της ασφάλειας με τους παράγοντες CARLS λαμβάνεται υπόψη ότι:

$C_A > C_B$

$A_A > A_B$

$R_A > R_B$

$L_A < L_B$

$S_A > S_B$

Κάνοντας την παραδοχή ότι οι στόχοι των δύο οργανισμών είναι ίδιοι, δηλαδή ότι:

$C_{TA} = C_{TB}$

$A_{TA} = A_{TB}$

$R_{TA} = R_{TB}$

$S_{TA} = S_{TB}$

και με την εφαρμοφή του τύπου

$$Sec_S = \frac{C}{C_T} \times \frac{A}{A_T} \times \frac{R-L}{R_T} \times \frac{S}{S_T}$$

διαπιστώνουμε τελικά ότι:

$Sec_A > Sec_B$

Άρα η διαφορά στους παράγοντες που σχετίζονται άμεσα με την ασφάλεια συνεπάγεται και διαφορά στο επίπεδο της ασφάλειας ως απόρροια της χρήσης της συγκεκριμένης μεθοδολογίας.

6.4.2. Οφέλη Παραγωγικών Υποδομών Ανεκτικών σε Σφάλματα

Η πρακτική εφαρμογή της συγκεκριμένης προσέγγισης που αναλύθηκε σε προηγούμενη παράγραφο, μπορεί να οδηγήσει σε ένα επιτυχημένο αποτέλεσμα. Εντούτοις, όπως επισημάνθηκε, προκειμένου να παρασχεθούν πιο συγκεκριμένα στοιχεία για τη δυνατότητα εφαρμογής της μεθοδολογίας, θα πρέπει να οριστούν κάποιου τύπου μετρήσεις της αποδοτικότητας της μεθοδολογίας. Αυτές οι μετρήσεις πρέπει να επιτρέπουν τη συνεπή μέτρηση των οφελών.

Στοχεύοντας προς αυτή την κατεύθυνση, εξετάστηκε η χρήση του ITIL. Όπως αναφέρθηκε και στο κεφάλαιο 3, το ITIL είναι ένα σύνολο βέλτιστων πρακτικών που χρησιμοποιούνται για τη διαχείριση των πληροφοριακών συστημάτων και υποδομών. Για τη βελτίωση του επιπέδου των υπηρεσιών που παρέχονται σε μια οργάνωση, το ITIL προτείνει την υιοθέτηση και το συνδυασμό μεθοδολογιών, εργαλείων, μετρήσεων και ρόλων.

Όπως μπορεί να γίνει κατανοητό, η προσαρμογή των μεθόδων μέτρησης του ITIL για να εξυπηρετήσει τις ανάγκες της μεθοδολογίας μετασχηματισμού, θα ενίσχυε την εμπιστοσύνη για τη δυνατότητα εφαρμογής της μεθοδολογίας. Επιπλέον, μια τέτοια προσαρμογή θα παρείχε εξ ορισμού μια γνωστή μεθοδολογία για τους ανθρώπους που είναι εξοικειωμένοι με τις μεθόδους μέτρησης του ITIL.

Στο πλαίσιο αυτό παρουσιάζονται οι βάσεις για την εφαρμογή των μεθόδων μέτρησης που είναι βασισμένες στο ITIL στη δική μας προσέγγιση μετασχηματισμού.

6.4.2.1. Μέθοδος Κύριων Δεικτών Απόδοσης

Κατά την ορολογία του ITIL οι Κύριοι Δείκτες Απόδοσης (Key Performance Indicators / KPIs) είναι «οικονομικά και μη οικονομικά μετρήσιμα μεγέθη που βοηθούν τους οργανισμούς να καθορίσουν και να μετρήσουν την πρόοδό τους

προς τους οργανωτικούς τους στόχους» [25]. Ο κύριος σκοπός των KPIs είναι να κρίνουν την τρέχουσα κατάσταση ενός οργανισμού και να παράσχουν τη βάση για το σχεδιασμό των ενεργειών βελτίωσης. Προκειμένου να εξαχθεί μια πιο αξιόπιστη εικόνα της κατάστασης του οργανισμού, τα KPIs θα πρέπει να ελεγχθούν σε πραγματικό χρόνο, μια διαδικασία που είναι γνωστή με τον όρο Παρακολούθηση Επιχειρηματικών Δραστηριοτήτων (Business Activity Monitoring / BAM). Οι κοινές χρήσεις των KPIs περιλαμβάνουν τη μέτρηση ασαφών οφελών ή τιμών όπως η ανάπτυξη ηγεσίας, το επίπεδο δέσμευσης, η παροχή υπηρεσιών και τα ποσοστά ικανοποίησης. Όντας σε θέση να καταγράψει τέτοιες πτυχές, τα διευθυντικά στελέχη έχουν ενσωματώσει τα KPIs στη στρατηγική διαχείριση του οργανισμού.

Τα επιλεγμένα KPIs μπορεί να διαφέρουν ανάλογα με τη φύση του οργανισμού και των στόχων του οργανισμού. Σε κάθε περίπτωση, η κατάλληλη χρήση τους μπορεί να βοηθήσει τον οργανισμό να μετρήσει την πρόοδο προς τους οργανωτικούς στόχους του και ειδικά τους στόχους εκείνους που περιλαμβάνουν διαδικασίες δύσκολες να ποσοτικοποιηθούν.

Κάθε KPI είναι ένα μέρος ενός «μετρήσιμου στόχου» που αποτελείται από μια κατεύθυνση, το KPI, μια συγκριτική μέτρηση επίδοσης (benchmark), έναν στόχο και ένα χρονικό πλαίσιο. Ένα παράδειγμα ενός στόχου είναι: «Να αυξηθεί η μέση χρησιμοποίηση των χώρων αποθήκευσης (storage) ανά κεντρικό υπολογιστή από 20% σε 60% μέχρι το τέλος του έτους 2010». Σε αυτήν την περίπτωση, η «μέση χρησιμοποίηση των χώρων αποθήκευσης ανά κεντρικό υπολογιστή» είναι το KPI.

Δεν θα πρέπει να υπάρχει σύγχυση των KPIs με τους Κρίσιμους Παράγοντες Επιτυχίας (Critical Success Factors) που χρησιμοποιούνται στις πωλήσεις προϊόντων. Στο προηγούμενο παράδειγμα, ένας Κρίσιμος Παράγοντας Επιτυχίας θα ήταν κάτι το οποίο θα έπρεπε να ενεργοποιηθεί ως καταλύτης για την επιτυχία εκείνου του στόχου, όπως ένα λογισμικό αρχειοθέτησης δεδομένων.

Οι Δείκτες Απόδοσης (Performance Indicators) πρέπει επίσης να διαφέρουν από τα επιχειρησιακά κίνητρα & στόχους. Ένας οικονομικός οργανισμός μπορεί να θεωρήσει το «ποσοστό αύξησης καταθέσεων» ως βασικό Δείκτη Απόδοσης που να βοηθήσει τον οργανισμό να καταγράψει τη θέση του στην αγορά, ενώ μια επιχείρηση τηλεπικοινωνιών θα μπορούσε να θεωρήσει το «ποσοστό των επιτυχών προσπαθειών κλήσης από τους πελάτες της» ως ένα πιθανό KPI το οποίο σχετίζεται και με την αγορά.

Εντούτοις είναι απαραίτητο για έναν οργανισμό να προσδιορίσει ο ίδιος τα KPIs του. Οι βασικοί κανόνες για τον καθορισμό των KPIs είναι:

- Να υπάρχουν προκαθορισμένες επιχειρησιακές διαδικασίες.
- Να υπάρχουν σαφείς απαιτήσεις των στόχων και της απόδοσης των επιχειρησιακών διαδικασιών.
- Να υπάρχει μια μέτρηση που θα μπορούσε να ποσοτικοποιήσει και να αναλύσει ποιοτικά τα αποτελέσματά της, και μπορεί να τα συγκρίνει με τους στόχους που έχουν οριστεί.
- Να εξετάζει τις διαφορές και να διευθετεί οποιεσδήποτε διαδικασίες ή πόρους απαιτούνται για την επίτευξη των βραχυπρόθεσμων στόχων.

Αντίστοιχα με το ειδικότερο ζήτημα της μέτρησης της ασφάλειας έτσι και για τον ορισμό οποιουδήποτε KPI, θα πρέπει να διαθέτει όλα τα παρακάτω χαρακτηριστικά:

- Συγκεκριμένο, έτσι ώστε να μη δημιουργείται σύγχυση με άλλα KPIs.
- Μετρήσιμο, έτσι ώστε να είναι εφικτό να μετρηθεί ή να υπολογιστεί με τη χρησιμοποίηση μιας συγκεκριμένης μονάδας μέτρησης.
- Επιτεύξιμο, έτσι ώστε να είναι εύκολο να ληφθούν οι απαραίτητες πληροφορίες.
- Σχετικό, έτσι ώστε να συνδέεται άμεσα με τον επιχειρησιακό στόχο.
- Τοποθετημένο χρονικά, έτσι ώστε να λαμβάνει υπόψη ότι τους χρονικούς περιορισμούς, προκειμένου να είναι σε θέση να

αντιμετωπίσει οποιαδήποτε ζητήματα σχετικά με αποτελέσματα που είναι εξαρτώμενα από το χρόνο.

Τα KPIs είναι σε όρους πρακτικής και στρατηγικής ανάπτυξης οι στόχοι που θα προσθέσουν την αξία σε μια επιχείρηση.

6.4.2.2. Καθορισμός Κύριων Δεικτών Απόδοσης

Έχοντας αναλύσει πώς καθορίζονται και χρησιμοποιούνται τα KPIs μέσα σε ένα κοινό οργανισμό, είναι πλέον δυνατό να χρησιμοποιηθούν αυτές οι αρχές στο πλαίσιο μιας πληροφοριακής υποδομής και μάλιστα υπό την οπτική της ασφάλειας. Στο πλαίσιο αυτό μπορούν θα καθοριστούν πιο συγκεκριμένα KPIs [26]. Αυτά τα KPIs θα χρησιμοποιηθούν για να μετρήσουν τα οφέλη από την υιοθέτηση των FTPIs καθώς επίσης και τα οφέλη από τη χρήση της προτεινόμενης προσέγγισης μετασχηματισμού.

Αν και η προσέγγιση μετασχηματισμού είναι αρκετά συγκεκριμένη όσον αφορά στα βήματα μετασχηματισμού, κάθε πληροφοριακή υποδομή περιλαμβάνει διαφορετικές ενότητες, διαδικασίες και συστήματα. Κατά συνέπεια, τα KPIs που επιλέχτηκαν να δημιουργηθούν στο πλαίσιο της διατριβής θα πρέπει να θεωρηθούν ως ένα πρώτο, γενικό, σύνολο KPIs. Συμπληρωματικά KPIs μπορεί και πρέπει να δημιουργηθούν προκειμένου να ικανοποιηθούν οι εξειδικευμένες ανάγκες κάθε οργανισμού. Ωστόσο, ο συνολικός αριθμός των KPIs που χρησιμοποιούνται για τη μέτρηση της επιτυχίας της υιοθέτησης των FTPIs δεν πρέπει να είναι πάρα πολύ μεγάλος δεδομένου ότι αυτό μπορεί να έχει επιπτώσεις στην απόδοση της υποδομής.

Τα KPIs για τη μέτρηση της επιτυχίας της υιοθέτησης των FTPIs μπορεί να διαιρεθούν σε τεχνικά και επιχειρησιακά KPIs. Αυτές οι δύο κατηγορίες KPIs δεν συσχετίζονται άμεσα η μια με την άλλη. Στοχεύουν να επιδείξουν διαφορετικές πτυχές των FTPIs και να μετρήσουν τα τεχνικά και επιχειρησιακά οφέλη της υιοθέτησής τους. Πρέπει να καταστεί σαφές ότι δεν υπάρχει καμία

ανάγκη για εναρμόνιση, συνδυασμό ή συγχρονισμό μεταξύ των αποτελεσμάτων αυτών των δύο κατηγοριών.

Παρά ταύτα, η μέτρηση των ακόλουθων KPIs πρέπει να πραγματοποιηθεί τόσο πριν όσο και μετά από το μετασχηματισμό, έτσι ώστε η σύγκριση να μπορεί να επιβεβαιώσει τα οφέλη των Παραγωγικών Υποδομών Ανεκτικών σε Σφάλματα.

Τεχνικά KPIs

Τα τεχνικά οφέλη από την υιοθέτηση των FTPIs είναι δυνατό να μετρηθούν με τη χρήση των εξειδικευμένων KPIs τα οποία δημιουργήθηκαν στο πλαίσιο της έρευνας.

1. Χρησιμοποιήσιμος χώρος αποθήκευσης σε ένα Μηχανογραφικό Κέντρο: Αυτό το KPI εκφράζει τον καθαρό αποθηκευτικό χώρο (Storage) που μπορεί να χρησιμοποιηθεί για την αποθήκευση δεδομένων σε ένα Μηχανογραφικό Κέντρο αφού έχει αφαιρεθεί ο χώρος που δεσμεύεται από την τεχνική αποθήκευσης όπως είναι η RAID. Το Μηχανογραφικό Κέντρο μπορεί να είναι Κύριο, Δευτερεύον ή Εναλλακτικό. Η μονάδα μέτρησης είναι σε MBs, GBs ή TBs.

2. Μέση χρησιμοποίηση της συνολικής επεξεργαστικής ισχύος ενός (ή όλων) Μηχανογραφικού Κέντρου: Αυτό το KPI είναι το μέσο ποσοστό της χρησιμοποίησης της επεξεργαστικής ισχύος όλων των πληροφοριακών συστημάτων σε ένα συγκεκριμένο (ή σε όλα) Μηχανογραφικά Κέντρα κατά τη διάρκεια της περιόδου μέτρησης. Το Μηχανογραφικό Κέντρο μπορεί να είναι Κύριο, Δευτερεύον ή Εναλλακτικό. Η μονάδα μέτρησης είναι ένα ποσοστό. . Η μονάδα μέτρησης της επεξεργαστικής ισχύος είναι εκατομμύρια οδηγίες ανά δευτερόλεπτο (Million Instructions Per Second / MIPS).

3. Μέσος ρυθμός εξυπηρέτησης (Throughput) του δικτύου μεταξύ των εξυπηρετητών και των σταθμών εργασίας: Ο όρος «ρυθμός εξυπηρέτησης»

αναφέρεται στην απόδοση της μετάδοσης στοιχείων, και μετριέται από τους χαρακτήρες που διαβιβάζονται πραγματικά ή που παραλαμβάνονται κατά τη διάρκεια μιας ορισμένης χρονικής περιόδου. Ο ρυθμός εξυπηρέτησης μετριέται συνήθως με bps (bits per second). Ένας αυξημένος ρυθμός εξυπηρέτησης προς τους σταθμούς εργασίας θα μπορούσε να υποδηλώνει την ύπαρξη μιας καλύτερης υποδομής.

4. Μέσος ρυθμός εισόδου/εξόδου (I/O) στο σύστημα κεντρικής αποθήκευσης σε ένα (ή περισσότερα) Μηχανογραφικά Κέντρα: Αυτό το KPI αποκαλύπτει το μέσο ποσοστό της χρησιμοποίησης των δίσκων αποθήκευσης όλων των συστημάτων σε ένα (ή περισσότερα) Μηχανογραφικά Κέντρα κατά τη διάρκεια της περιόδου μέτρησης. Το Μηχανογραφικό Κέντρο μπορεί να είναι Κύριο, Δευτερεύον ή Εναλλακτικό. Η μονάδα μέτρησης είναι σε MBps, GBps.

5. Μέση χρησιμοποίηση μνήμης σε ένα (ή περισσότερα) Μηχανογραφικά Κέντρα: Η χρησιμοποίηση της προσωρινής μνήμης παρουσιάζει το μέσο ποσοστό της χρησιμοποίησης της μνήμης όλων των συστημάτων σε ένα συγκεκριμένο (ή σε όλα) τα Μηχανογραφικά Κέντρα. Το Μηχανογραφικό Κέντρο μπορεί να είναι Κύριο, Δευτερεύον ή Εναλλακτικό. Η μονάδα μέτρησης είναι ένα ποσοστό.

6. Αποτελεσματικότητα στη χρήση ρεύματος από ένα Μηχανογραφικό Κέντρο: Αυτό το KPI υπολογίζεται με τη διαίρεση του συνολικού ηλεκτρικού ρεύματος που καταναλώνει ένα Μηχανογραφικό Κέντρο με το ηλεκτρικό ρεύμα που καταναλώνουν μόνο τα πληροφοριακά συστήματα (υπολογιστές, αποθηκευτικά συστήματα, δικτυακός εξοπλισμός καθώς επίσης και όργανα ελέγχου και τερματικοί σταθμοί. Το Μηχανογραφικό Κέντρο μπορεί να είναι Κύριο, Δευτερεύον ή Εναλλακτικό. Η μονάδα μέτρησης είναι ένα ποσοστό.

7. Καλυπτόμενη επιφάνεια (Footprint) συστημάτων σε ένα (ή περισσότερα) Μηχανογραφικά Κέντρα: Το Footprint αντιπροσωπεύει τη φυσική περιοχή που καταλαμβάνουν τα συστήματα και μετριέται σε τετραγωνικά μέτρα ή

τετραγωνικά πόδια. Μια μείωση σε αυτό το KPI θα υποστήριζε τα οφέλη που κερδίζονται από την υιοθέτηση των FTPIs. Όμοια με προηγούμενα KPIs το Μηχανογραφικό Κέντρο μπορεί να είναι Κύριο, Δευτερεύον ή Εναλλακτικό.

8. Ποσοστό των κεντρικών υπολογιστών παραγωγής που βρίσκονται στο Κύριο/Δευτερεύον Μηχανογραφικό Κέντρο: Αυτό είναι ένα από τα σημαντικότερα οφέλη των FTPIs. Εκφράζεται ως λόγος των παραγωγικών εξυπηρετητών που βρίσκονται σε ένα συγκεκριμένο Μηχανογραφικό Κέντρο (Κύριο ή Δευτερεύον) προς το συνολικό αριθμό των παραγωγικών εξυπηρετητών όλων των Μηχανογραφικών Κέντρων.

Με τη χρήση των παραπάνω KPIs καθίσταται δυνατό να ανιχνευτούν και να ποσοτικοποιηθούν και τα οφέλη των FTPIs σε τεχνικό επίπεδο.

Επιχειρησιακά KPIs

Επιπλέον των τεχνικών οφελών, είναι δυνατό να μετρηθούν και τα επιχειρησιακά οφέλη από την υιοθέτηση των FTPIs με τη χρήση των εξειδικευμένων KPIs τα οποία δημιουργήθηκαν στο πλαίσιο της έρευνας.

1. Προγραμματισμένος χρόνος διακοπής των προσφερομένων υπηρεσιών: Ο προγραμματισμένος χρόνος διακοπής είναι ο χρόνος διακοπής οποιασδήποτε υπηρεσίας που προκαλείται από προσχεδιασμένες συντηρήσεις συστημάτων ή εφαρμογών. Μετριέται σε λεπτά ή ώρες ανά χρόνο.

2. Μη σχεδιασμένος χρόνος διακοπής των προσφερομένων υπηρεσιών: Αυτό το KPI είναι το ποσό χρόνου διακοπής οποιασδήποτε υπηρεσίας που προκύπτει από τους λόγους εκτός από τη συντήρηση. Μετριέται σε λεπτά ή ώρες ανά χρόνο.

3. Χρόνος αποκατάστασης των επιχειρησιακών κρίσιμων υπηρεσιών: Το συγκεκριμένο KPI προϋποθέτει ότι έχει αποφασιστεί που είναι οι επιχειρησιακά κρίσιμες υπηρεσίες. Ο χρόνος αποκατάστασης είναι η διάρκεια του χρόνου

μέσα στην οποία οι επιχειρησιακές κρίσιμες υπηρεσίες μπορούν να αποκατασταθούν μετά από μια καταστροφή προκειμένου να αποφευχθούν μη αποδεκτές επιχειρησιακές συνέπειες. Μετριέται σε λεπτά, ώρες ή μέρες.

4. Λειτουργικές δαπάνες της Διεύθυνσης Πληροφορικής: Οι λειτουργικές δαπάνες, που μπορούν να μετρηθούν σε οποιοδήποτε νόμισμα, είναι οι ετήσιες τρέχουσες δαπάνες οποιουδήποτε οργανισμού, ή τμημάτων του οργανισμού, όπως η Διεύθυνση Πληροφορικής. Μια μείωση σε αυτές θα μπορούσε να υποδηλώσει μια καλύτερη χρήση ή διαχείριση των υπαρχόντων πόρων.

5. Πάγιες δαπάνες της Διεύθυνσης Πληροφορικής: Αντίθετα με το προηγούμενο KPI, οι πάγιες δαπάνες είναι δαπάνες που πραγματοποιούνται κατά παραγγελία και αφορούν την προμήθεια προϊόντων και μη αναλωσίμων υλικών. Μετριέται σε οποιοδήποτε νόμισμα και μπορεί να σχετιστεί με τα οικονομικά οφέλη της υιοθέτησης των FTPIs.

6. Κόστος της επανάκαμψης των νέων υπηρεσιών: Αυτό είναι ένα πολύ σημαντικό KPI δεδομένου ότι μπόρεσε να απεικονίσει τις χαμηλού κόστους δυνατότητες επέκτασης των FTPIs. Η μονάδα μέτρησης είναι οποιοδήποτε νόμισμα.

7. Ποσοστό ικανοποίησης του προσωπικού πληροφορικής (ιδιοκτήτες συστημάτων): Αυτή είναι μια ποιοτική μέτρηση της ικανοποίησης του προσωπικού πληροφορικής. Το ποσοστό ικανοποίησης του προσωπικού μπορεί να βασιστεί σε περιοδικές έρευνες για τους υπαλλήλους μετά από μια εύλογη περίοδο ωρίμανσης της νέας υποδομής – για παράδειγμα 6 μήνες. Ο χρόνος ωριμότητας θα μπορούσε να ελαχιστοποιήσει τις μη στοιχειοθετημένες αρνητικές αντιδράσεις, που προκλήθηκαν από τη φυσική αντίσταση του προσωπικού στην αλλαγή [27]. Αυτό το KPI μετριέται ως ποσοστό των θετικών απαντήσεων επί του συνόλου των απαντήσεων.

8. Ποσοστό της ικανοποίησης από το προσωπικό που σχετίζεται με την επιχειρησιακή λειτουργία (ιδιοκτήτες επιχείρησης): Με τον ίδιο τρόπο όπως και στο προηγούμενο KPI, αυτή η μέτρηση συσχετίζεται με την ικανοποίηση του προσωπικού που μπορεί να έχει (ή να μην έχει) μια διαφορετική άποψη σχετικά με τα οφέλη της εφαρμοσμένης υποδομής. Αυτό το KPI μετριέται ως ποσοστό των θετικών απαντήσεων επί του συνόλου των απαντήσεων.

9. Μέση συχνότητα των ενημερώσεων των πλάνων ανάκαμψης από καταστροφή: Αυτό το KPI πρέπει να απεικονίσει το βαθμό της συνειδητοποίησης του προσωπικού σε σχέση με την ενημέρωση επί των πλάνων ανάκαμψης από καταστροφή. Δεδομένου ότι οι FTPIs ενισχύουν το ρόλο των Εναλλακτικών Κέντρων, αναμένεται ότι αυτή η συχνότητα των ενημερώσεων θα πρέπει να αυξηθεί. Μετριέται σε ημέρες.

10. Ποσοστό της αύξησης του προϋπολογισμού πληροφορικής: Μια ασυνήθιστη αύξηση του προϋπολογισμού ΤΠ μπορεί να συνδέεται κάπως με τη νέα αρχιτεκτονική υποδομής.

11. Ποσοστό προμήθειας νέων πληροφοριακών συστημάτων (ως ποσοστό των υπαρχόντων πληροφοριακών συστημάτων): Αυτό το KPI πρέπει να επιβεβαιώσει ότι η προμήθεια των νέων συστημάτων πρέπει να είναι λιγότερο συχνή δεδομένου ότι οι ελεύθεροι πόροι και οι δυνατότητες επέκτασης θα αυξάνονται (κυρίως στο Κύριο Κέντρο) μετά από έναν τέτοιο μετασχηματισμό.

12. Μέσος χρόνος παροχής νέων συστημάτων: Αυτός είναι ο μέσος χρόνος που απαιτείται για να δημιουργηθεί ένα νέο πληροφοριακό σύστημα και να αποδοθεί σε έναν ιδιοκτήτη εφαρμογής ή συστημάτων. Ο χρόνος αρχίζει να μετρά όταν το αίτημα σταλθεί και ολοκληρώνεται όταν παραδοθεί το πληροφοριακό σύστημα. Ο χρόνος μετριέται σε λεπτά, ώρες ή ημέρες. Μια δυναμικότερη υποδομή, όπως οι FTPIs στοχεύουν να είναι, θα πρέπει να πετύχει την μείωση του χρόνου αυτού.

13. Μέσος χρόνος παροχής νέων επιχειρηματικών υπηρεσιών: Αυτό το KPI διαφέρει από τον προηγούμενο επειδή περιλαμβάνει τόσο τις διαδικασίες όσο και το ανθρώπινο δυναμικό που είναι απαραίτητα για την παροχή μιας νέας επιχειρηματικής υπηρεσίας. Μετριέται σε λεπτά, ώρες ή ημέρες.

Όπως και με τη χρήση των τεχνικών KPIs έτσι και με τη χρήση των παραπάνω KPIs καθίσταται δυνατό να ανιχνευτούν και να ποσοτικοποιηθούν και τα οφέλη των FTPIs σε επιχειρησιακό επίπεδο.

6.4.3. Οφέλη μεθοδολογίας μετασχηματισμού

Χρησιμοποιώντας τις αρχές του καθορισμού των KPIs που αναφέρθηκαν στην παράγραφο 6.4.2.1, είναι δυνατό να μετρηθούν και τα οφέλη από τη χρησιμοποίηση της προτεινόμενης προσέγγισης μετασχηματισμού.

Σε αυτή την περίπτωση, τα KPIs που χρησιμοποιούνται για τη μέτρηση των οφελών από τη χρησιμοποίηση της προτεινόμενης προσέγγισης μετασχηματισμού εξαρτώνται λιγότερο από την πληροφοριακές υποδομές αλλά και τις επιχειρησιακές υπηρεσίες του οργανισμού που έχει επιλέξει να χρησιμοποιήσει αυτήν την προσέγγιση, συγκριτικά με τα KPIs που περιγράφονται στην προηγούμενη παράγραφο.

Δεδομένου ότι ο πυρήνας της προσέγγισης μετασχηματισμού βασίζεται και σε μια ομάδα διαδικασιών από τη θεωρία διαχείρισης αλλαγών, το ακόλουθα KPIs για την αξιολόγηση της επιτυχίας της προτεινόμενης μεθοδολογίας μετασχηματισμού κάνουν χρήση μόνο μετρήσεων που συσχετίζονται με τη διαχείριση έργων. Η μέτρηση των παρακάτω KPIs πρέπει να πραγματοποιηθεί κατά τη διάρκεια του μετασχηματισμού, και να συγκριθεί με τα παρόμοια έργα που χρησιμοποίησαν (ή θα χρησιμοποιήσουν) διαφορετικές μεθοδολογίες μετασχηματισμού. Αυτά τα έργα μπορούν να προέλθουν ακόμα και από άλλους τρίτους οργανισμούς που δεν σχετίζονται με τον οργανισμό που επέλεξε να ακολουθήσει τη συγκεκριμένη μεθοδολογία.

Και πάλι, ο αριθμός των επιλεγμένων KPIs θα πρέπει να περιοριστεί σε ένα επίπεδο που δεν θα επηρεάσει την πραγματική πρόοδο και την αποτελεσματικότητα της μεθοδολογίας.

KPIs Διαχείρισης Έργων

Τα οφέλη από την υιοθέτηση της μεθοδολογίας μετασχηματισμού σε FTPIs είναι δυνατό να μετρηθούν με τη χρήση των εξειδικευμένων KPIs Διαχείρισης Έργων τα οποία δημιουργήθηκαν στο πλαίσιο της έρευνας.

1. Απόδοση στην επένδυση της διαδικασίας του μετασχηματισμού: Αυτό το KPI επεξηγεί την κύρια ιδέα πίσω από αυτή την μεθοδολογία. Είναι ένα μάλλον δύσκολο KPI για να μετρηθεί δεδομένου ότι η πραγματική απόδοση δεν μπορεί να υπολογιστεί άμεσα. Εντούτοις, όλα τα άλλα KPIs που αναφέρονται σε αυτήν την παράγραφο θα μπορούσαν να χρησιμοποιηθούν ως μεταβλητές στον υπολογισμό του. Θα μπορούσε να μετρηθεί σε οποιεσδήποτε νόμισμα ή χρονικές μονάδες όπως οι ημέρες, οι εβδομάδες και οι μήνες. Όταν μετριέται σε χρονικές μονάδες η απόδοση αντιπροσωπεύει το χρόνο που εξοικονομείται με τη χρησιμοποίηση της προτεινόμενης μεθοδολογίας μετασχηματισμού.

2. Συνολικός χρόνος της διαδικασίας μετασχηματισμού: Αυτό είναι το χρονικό διάστημα που διαρκεί το έργο μετασχηματισμού και περιλαμβάνει και τις επτά φάσεις της προτεινόμενης στρατηγικής μετάβασης που περιγράφεται στην παράγραφο 6.3.3. Μετριέται σε ημέρες, εβδομάδες ή μήνες.

3. Ποσοστό χρησιμοποίησης ανθρώπινου δυναμικού στο πλαίσιο του έργου μετασχηματισμού: Αυτό είναι το ποσοστό του χρόνου που ένας εργαζόμενος θα αφιερώσει στο έργο του μετασχηματισμού σε σχέση με το συνολικό εργάσιμο χρόνο του. Είναι παρόμοιο με το Ισοδύναμο Πλήρους Απασχόλησης (Full-time equivalent / FTE) που είναι ένας τρόπος να μετρηθεί η εμπλοκή ενός ατόμου σε ένα έργο και χρησιμοποιείται από πολλές οργανώσεις παγκοσμίως.

4. Χρόνος διακοπής των υπηρεσιών επιχείρησης λόγω του έργου μετασχηματισμού: Μερικές από τις φάσεις μετασχηματισμού που περιγράφηκαν προηγουμένως θα μπορούσαν να επηρεάσουν τη λειτουργία μερικών υπηρεσιών και κατ' επέκτασης της διαθεσιμότητάς τους. Λιγότερος χρόνος διακοπής της παραγωγικής λειτουργίας κάθε υπηρεσίας συνεπάγεται και λιγότερα χαμένα έσοδα για τον οργανισμό και περισσότερη αξία για τη μεθοδολογία μετασχηματισμού. Μετριέται σε λεπτά, ώρες ή ημέρες.

5. Συνολικό κόστος του έργου μετασχηματισμού: Αυτό είναι πολύ σημαντικό δεδομένου ότι το έργο μετασχηματισμού πρέπει να κοστίζει λιγότερο από την αναμενόμενη απόδοσή του. Μετριέται σε οποιοδήποτε νόμισμα.

6. Αριθμός ανθρώπων που συμμετέχουν στο έργο μετασχηματισμού: Αυτό είναι επίσης σημαντικό προκειμένου να είναι σε θέση να εκτιμήσει τις ανάγκες επάνδρωσης του έργου.

7. Το ποσοστό των διοικητικών δραστηριοτήτων (administrative activities) που αφορά το έργο του μετασχηματισμού: Αυτό είναι ένα KPI που εκφράζεται με ποιοτικά κριτήρια για τη διαχείριση του έργου. Παρουσιάζει τον αριθμό των διοικητικών δραστηριοτήτων για το έργο του μετασχηματισμού σε σχέση με τις συνολικές δραστηριότητες του έργου που περιλαμβάνουν επίσης τις δραστηριότητες εφαρμογής. Μετριέται ως ποσοστό.

8. Προϋπολογισμένο κόστος της προβλεπόμενης εργασίας (Budgeted Cost of Work Scheduled): Αυτό είναι το άθροισμα των προϋπολογισμών των δραστηριοτήτων που προγραμματίστηκαν ή σχεδιάστηκαν να ολοκληρωθούν, αλλιώς γνωστό και ως «προγραμματισμένη αξία» (planned value). Μετριέται σε οποιοδήποτε νόμισμα.

9. Προϋπολογισμένο κόστος της εργασίας που διενεργήθηκε (Budgeted Cost of Work Performed): Αυτό το KPI, που μετριέται σε οποιοδήποτε νόμισμα,

είναι το προγραμματισμένο ή σχεδιασμένο κόστος των δραστηριοτήτων που ολοκληρώθηκαν, γνωστό επίσης ως «κερδισμένη αξία» (earned value). Μετριέται σε οποιοδήποτε νόμισμα.

10. Πραγματικό κόστος της εργασίας που διενεργήθηκε (Actual Cost of Work Performed): Είναι το ποσό των πραγματικών δαπανών των δραστηριοτήτων που ολοκληρώνονται. Μετριέται σε οποιοδήποτε νόμισμα.

11. Δείκτης Απόδοσης Χρονοδιαγράμματος (Schedule Performance Index): Αυτό υπολογίζεται με τη χρήση των προηγούμενων KPIs. Είναι η διαίρεση του «Προϋπολογισμένου κόστους της εργασίας που διενεργήθηκε» με το «Προϋπολογισμένο κόστος της προβλεπόμενης εργασίας».

12. Δείκτης απόδοσης δαπανών (Cost Performance Index): Αυτό υπολογίζεται με το συνδυασμό δύο προηγούμενων KPIs. Είναι το «Προϋπολογισμένο κόστος της εργασίας που διενεργήθηκε» διαιρεμένο με το «Πραγματικό κόστος της εργασίας που διενεργήθηκε».

13. Δείκτης κόστους Χρονοδιαγράμματος (Cost Schedule Index): Αυτό είναι ο «Δείκτης απόδοσης δαπανών» που πολλαπλασιάζεται με το «Δείκτης Απόδοσης Χρονοδιαγράμματος». Ο Δείκτης κόστους Χρονοδιαγράμματος μετρά την πιθανότητα της επανάκαμψης ενός έργου που καθυστερεί ή/και έχει ξεπεράσει τον προϋπολογισμό του. Όσο πιο κοντά είναι ο δείκτης στο 1, τόσο πιθανότερο είναι για το έργο να επανέλθει στην πορεία του. Αυτό μπορεί να είναι χρήσιμο για οποιοδήποτε οργανισμό που θα αποφάσιζε να εφαρμόσει την προτεινόμενη μεθοδολογία μετασχηματισμού.

14. Ποσοστό του χρόνου για το συντονισμό του έργου: Αυτό είναι ένα KPI που σχετίζεται με την αποδοτικότητα της μεθοδολογίας και αναπαρίσταται ως το ποσοστό του χρόνου (σε ανθρωποημέρες) που χρησιμοποιείται για το συντονισμό του έργου σε σχέση με το συνολικό χρόνο που χρησιμοποιείται για να υλοποιηθεί και να συντονισθεί το έργο.

15. Ποσοστό των στόχων που χάθηκαν: Είναι το ποσοστό των κύριων σημείων του έργου που καταγράφεται σε όλες τις διαδικασίες και τις φάσεις ως παραλειπόμενο.

16. Αριθμός γεγονότων ασφάλειας που οφείλονται στο έργο του μετασχηματισμού: Θεωρητικά ο μετασχηματισμός όπως οποιαδήποτε άλλη προγραμματισμένη αλλαγή δεν θα πρέπει να προκαλέσει κανένα γεγονός ασφάλειας. Εντούτοις, μια πρακτικότερη αξιολόγηση της μεθοδολογίας θα πρέπει επίσης να καταγράψει τον αριθμό των γεγονότων που προκαλούνται από τη μεθοδολογία σε σχέση με το συνολικό αριθμό των γεγονότων που μπορεί να έχουν προκληθεί στο ίδιο χρονικό διάστημα.

17. Μέση επανάληψη εργασιών ανά φάση μετά από την υλοποίηση κάθε φάσης: Αυτή είναι μια σημαντική μέτρηση της ποιότητας των φάσεων Ανάλυσης και οι Σχεδιασμού που περιλαμβάνει η μεθοδολογία. Εάν η επανάληψη των εργασιών ανά φάση είναι σπάνια, αυτό θα μπορούσε αποτελεί μια ένδειξη ότι η μεθοδολογία παρέχει στερεά βάση για το μετασχηματισμό σε μια FTPI. Μετριέται σε ανθρωποημέρες, ανθρωποεβδομάδες ή ανθρωπομήνες.

Το σύνολο των παραπάνω KPIs Διαχείρισης Έργων καθιστά δυνατό να οριοθετηθούν και να ποσοτικοποιηθούν και τα οφέλη από τη μεθοδολογία μετασχηματισμού σε FTPIs.

6.5. Σύνοψη και συμπεράσματα

Στο κεφάλαιο 6 εξετάστηκαν τα θέματα βελτιστοποίησης της διαχείρισης της ασφάλειας των κρίσιμων πληροφοριακών υποδομών. Στο πλαίσιο αυτό αναλυθήκαν μια σειρά από ενδιαφέρουσες μεθοδολογίες διαχείρισης της ασφάλειας των Πληροφοριακών Υποδομών και προτάθηκαν τρόποι για την βελτιστοποίηση αυτών μέσα από το πλαίσιο της διαχείρισης της ασφάλειας των κρίσιμων πληροφοριακών υποδομών.

Επιπλέον, εκπονηθήκαν και αναλύθηκαν δύο εξελιγμένες μεθοδολογίες που βελτιστοποιούν τη διαχείριση της ασφάλειας των κρίσιμων πληροφοριακών υποδομών, τόσο από οικονομικής άποψης όσο και από λειτουργικής άποψης.

Η πρώτη από αυτές προτείνε τη χρήση των Εναλλακτικών Μηχανογραφικών Κέντρων για την αντιμετώπιση ακραίων επιθέσεων, οι οποίες και αναλύονται. Η δεύτερη μεθοδολογία επέκτεινε τα αποτελέσματα της πρώτης και προτείνε τη καλύτερη εκμετάλλευση των Εναλλακτικών Μηχανογραφικών Κέντρων με τον μετασχηματισμό τους σε Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα, προσαρμόζοντας τη θεωρία διαχείρισης αλλαγών σε μια νέα μεθοδολογία μετασχηματισμού κρίσιμων υποδομών.

Με σκοπό την καλύτερη διαχείριση της ασφάλειας συζητηθηκαν επίσης τα ζητήματα που σχετίζονται με την αποδοτικότητα των επενδύσεων της ασφάλειας.

Τέλος υπολογίστηκαν τα οφέλη από τις παραπάνω μεθοδολογίες με την χρήση των μεθόδων του κεφαλαίου 4 αλλά και με τα KPIs του ITIL, το οποίο παρουσιάστηκε στο κεφάλαιο 3.

6.6. Βιβλιογραφία κεφαλαίου

[1] R. Heath, "Crisis Management for managers and executives", Pearson Education Limited, 2005, ISBN 960-512-434-3

[2] C. Pommerening, "A Comparison of Critical Information Infrastructure Protection in the United States and Germany: An Institutional Perspective", Annual meeting of the American Political Science Association, 2004

[3] G. Pye και M. J. Warren, "Conceptual Modelling: Choosing a Critical Infrastructure Modelling Methodology", Journal of Information Warfare, Vol 5, Issue 1, pp. 46-61, Edith Cowan University, Western Australia

[4] M. J. Warren και S. Leitch, "Commercial Critical Systems and Critical Infrastructure Protection: A Future Research Agenda", 8th Australian Information Warfare and Security Conference, School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, 2007

[5] C. Schuba, I. Krsul, M. Kuhn, E. Spafford, A. Sundaram, και D. Zamboni, "Analysis of A Denial of Service Attack on TCP," Proc. Of IEEE Symposium on Security and Privacy, 1997.

[6] J. Lemon, "Resisting SYN Flood DoS Attacks with A SYN Cache," Proc. of USENIX BSDCON2002, 2002.

[7] H. Wang, D. Zhang, και K. G. Shin, "SYN-dog: Sniffing SYN Flooding Sources," Proc. of 22 nd International Conference on Distributed Computing Systems (ICDCS'02), 2002.

[8] D. Moore, G. Voelker, και S. Savage, "Inferring Internet Denial of Service Activity," USENIX Security Symposium, 2001.

[9] Y.-C. Hu, A. Perrig, και D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," ACM International Conference on Mobile Computing and Networking, 2002.

[10] Y.-C. Hu, D. B. Johnson, και A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", 4th IEEE Workshop on Mobile Computing Systems and Applications, 2002.

[11] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, και E. Belding-Royer, "A secure routing protocol for ad hoc networks," 10th IEEE International Conference on Network Protocols (ICNP'02), 2002.

[12] P. Papadimitratos και Z. Haas, "Secure routing for mobile ad hoc networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, σελ. 27–31, 2002.

[13] R. Hauser, T. Przygienda, , και G. Tsudik, "Reducing the cost of security in link-state routing," IEEE Computer Society, pp.93, ISBN:0-8186-7767-8, Symposium of Network and Distributed Systems Security, 1997.

[14] B. R. Smith, S. Murthy, και J. Garcia-Luna-Aceves, "Securing distance-vector routing protocols," pp.85, Symposium on Networks and Distributed Systems Security, 1997.

[15] S. Kent, C. Lynn, και K. Seo, "Secure border gateway protocol (s-bgp)," IEEE Journal on Selected Areas in Communication, vol. 18, no. 4, pp. 582 – 592, 2000.

[16] P. Kyasanur και N. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks," International Conference on Dependable Systems and Networks (DSN'03), 2003.

[17] An. D. Keromytis, V. Misra, και D. Rubenstein, "Using Overlay to improve Security", Columbia University in the City of New York, 2003.

[18] K. Miller, "Don't Recover-Failover", DM Direct, 2004

[19] S. Atwood, "Planned Downtime", DM Direct, Veritas Software, 2004

[20] J. P. Garbani, "Best Practices For Infrastructure Change Management: Regain Control Of Runaway IT Infrastructures", Forrester Research, ανακτήθηκε: 14/6/2009, http://www.forrester.com/Research/Document/Excerpt/0,7211,34048,00.html

[21] "Microsoft Operations Framework 4.0", Microsoft Corporation, ανακτήθηκε: 14/6/2009, http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfchgmg.mspx

[22] "Change Management (ITSM)", Wikipedia, ανακτήθηκε: 14/6/2009, http://en.wikipedia.org/wiki/Change_Management_%28ITSM%29

[23] D. Scott και Y. Natis, "Building Continuous Availability Into E-Applications", GartnerGroup, COM-12-1325, 29/9/2000

[24] W. Sonnenreich, J. Albabese, και B. Stout, 'Return On Security Investment (ROSI) - a practical quantitative model', Journal of Research and Practice in Information Technology, 2006, Vol. 38, No. 1, pp.55-66.

[25] F. John Reh, "Key Performance Indicators – What are Key Performance Indicators or KPI", About.com, http://management.about.com/cs/generalmanagement/a/keyperfindic.htm

[26] KPI Library, ανακτήθηκε: 14/6/2009, http://kpilibrary.com/

[27] A. J. Schuler, "Overcoming Resistance to Change: Top Ten Reasons for Change Resistance", ανακτήθηκε: 14/6/2009, http://www.schulersolutions.com/resistance_to_change.html

7. Αξιολόγηση έρευνας

Το αντικείμενο της έρευνας, όπως αυτό παρουσιάστηκε στα προηγούμενα κεφάλαια, παρουσιάζει μια σειρά από χαρακτηριστικά τα οποία θα πρέπει να αξιολογηθούν κριτικά. Το κεφάλαιο 7 περιλαμβάνει την αξιολόγηση της έρευνας διακρίνοντας τα οφέλη των μεθοδολογιών, τις πιθανές εφαρμογές αλλά και τους τυχόν περιορισμούς τους.

Τα οφέλη των μεθοδολογιών διακρίνονται σε διαχειριστικά και οικονομικά, η υλοποίηση των οποίων αναπτύσσεται στο επιμέρους αντικείμενο του κεφαλαίου 6 τη βελτίωση της διαχείρισης της ασφάλειας. Οι περιορισμοί των μεθοδολογιών διακρίνονται και εκείνοι σε τεχνικούς, διαδικαστικούς, νομικούς και οικονομικούς.

Το κεφάλαιο χωρίζεται σε τέσσερα μέρη. Το πρώτο μέρος αφορά τη μεθοδολογία Μέτρησης Ασφάλειας με συνδυασμό των δομικών της στοιχείων. Το δεύτερο περιλαμβάνει τη μεθοδολογία Μέτρησης Ασφάλειας με συνδυασμό παραγόντων που σχετίζονται έμμεσα με την ασφάλεια. Στο τρίτο μέρος περιγράφονται η αξιολόγηση των χαρακτηριστικών της μεθοδολογίας του εισήγαγε τη χρήση των Εναλλακτικών Κέντρων ως μέσων για την αντιμετώπιση ακραίων επιθέσεων. Στο τέταρτο και τελευταίο μέρος αξιολογείται η μεθοδολογία μετασχηματισμού σε Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα.

7.1. Μέτρηση Ασφάλειας με συνδυασμό δομικών στοιχείων

Η προτεινόμενη λύση στοχεύει στο να προσφέρει τη βάση για μια μεθοδολογία που θα μπορούσε να βοηθήσει τους αναλυτές ασφαλείας για να ποσοτικοποιήσουν και να υπολογίσουν την ασφάλεια συγκεκριμένων υπηρεσιών. Συγκρίνοντας με τις απαιτήσεις που τέθηκαν αρχικά στο κεφάλαιο 4, η προτεινόμενη μεθοδολογία υποστηρίζει την απαίτηση της συνέπειας με τη χρήση ερωτήσεων με αντικειμενικές απαντήσεις. Επίσης, οι ερωτήσεις στόχευσαν σε απαντήσεις με χαμηλό κόστος συλλογής, δεδομένου ότι οι

απαντήσεις μπορούν να προέλθουν από αυτοματοποιημένα συστήματα όπως τα IPSs. Επιπλέον η μεθοδολογία έχει κατορθώσει να εκφράσει την ασφάλεια ως αριθμό και μάλιστα ως ποσοστό. Ο υπολογισμός ασφάλειας έχει χρησιμοποιήσει τουλάχιστον μια μονάδα μέτρησης (όπως τα spam emails που εντοπίστηκαν στο παράδειγμα του κεφαλαίου 4) που ικανοποιεί άλλη μια απαίτηση των μεθοδολογιών μέτρησης της ασφάλειας. Αλλά και η τελευταία απαίτηση των μεθοδολογιών μέτρησης της ασφάλειας έχει επίσης καλυφθεί, δεδομένου ότι το συνολικό επίπεδο ασφάλειας του οργανισμού ή των μεμονωμένων υπηρεσιών έχει απόλυτα θετικό νόημα για τα διοικητικά στελέχη. Κατά συνέπεια, το πρότυπο μπορεί επίσης να υποστηρίξει ότι έχει σχέση με το ευρύτερο πλαίσιο.

Ως γενικότερη παρατήρηση, θα πρέπει να επισημανθεί ότι η μεθοδολογία δεν εξετάζεται τόσο πολύ σε σχέση με νέα προϊόντα και υπηρεσίες, αλλά κυρίως με υπάρχουσες υπηρεσίες. Αυτό συμβαίνει επειδή όλες οι ερωτήσεις του παραδείγματος συνδέονται με προηγούμενη καταγεγραμμένη εμπειρία. Για να υπολογιστεί το επίπεδο ασφάλειας νέων υπηρεσιών και προϊόντων είναι πιθανό να πρέπει να τεθεί ένας άλλος τύπος ερωτήσεων που δεν απαιτεί προηγούμενη εμπειρία για να απαντηθεί.

Υπάρχουν επίσης άλλα ζητήματα που θα μπορούσαν να είναι μέρος μιας σχετικής μελλοντικής έρευνας όπως ο χρόνος μέτρησης, η συχνότητα της μέτρησης καθώς επίσης και ο αριθμός των επαναλήψεων της μέτρησης.

Εν κατακλείδι θα πρέπει να αναφερθεί ότι οι τύποι ερωτήσεων που απαντώνται σε κάθε κατάσταση είναι αρκετά σημαντικοί, αλλά μέχρι τώρα υπάρχουν περιορισμένες οδηγίες για το γράψιμό τους. Μια πιθανή μελλοντική έρευνα μπορεί να περιλάβει μια πιο λεπτομερή ανάλυση για τη διατύπωση των σωστών ερωτήσεων σε κάθε κατάσταση ή υπηρεσία.

7.2. Μέτρηση Ασφάλειας με συνδυασμό παραγόντων που σχετίζονται έμμεσα με την ασφάλεια

Η δεύτερη προσέγγιση για την ποσοτικοποίηση της ασφάλειας πραγματοποιείται μέσω υπολογισμού. Οι μεταβλητές που χρησιμοποιούνται για τον υπολογισμό είναι τα μεγέθη CARLS, δηλαδή η Συμμόρφωση C με το νομικό και κανονιστικό πλαίσιο, η Διαθεσιμότητα A των υπηρεσιών, η απόδοση R κάθε υπηρεσίας, οι ζημιές L από τις υπηρεσίες και η τιμή της μετοχής S του κάθε οργανισμού όπως αυτή διαμορφώνεται ανάλογα με τη φήμη της. Η μεθοδολογία υποστηρίζει ότι η ασφάλεια επιδρά σε κάθε έναν από αυτούς τους παράγοντες και άρα οι παράγοντες σχετίζονται έμμεσα με εκείνη. Ο συσχετισμός αυτός εκφράζεται με ένα μαθηματικό τύπο δια του οποίου οι παράγοντες θεωρούνται ισοδύναμοι.

Ένα σημαντικό πλεονέκτημα της μεθοδολογίας είναι ότι με τη χρήση της τα διοικητικά στελέχη μπορούν να κατανοήσουν αμεσοτέρα τα μεγέθη που παράγονται από αυτή και να αξιολογήσουν καλύτερα πως και πού θα πρέπει να επικεντρωθούν οι επενδύσεις της ασφάλειας. Αυτό είναι ιδιαίτερα σημαντικό διότι η Ασφάλεια είναι μια αφηρημένη έννοια η οποία δεν ήταν εύκολο να εκφραστεί ως ένα αξιολογήσιμο μέγεθος.

Ένας από τους περιορισμούς της μεθόδου είναι το γεγονός ότι όλοι οι παράγοντες θεωρούνται ισοδύναμοι κατά τον υπολογισμό της ασφάλειας. Μια μελλοντική έρευνα θα μπορούσε να διερευνήσει περαιτέρω τον βαθμό που επηρεάζεται η ασφάλεια από κάθε μια παράμετρο καθώς και πως αυτός μεταβάλλεται ανά είδος υπηρεσίας, οργανισμού ή αγοράς.

Επιπλέον βήματα μπορούν να πραγματοποιηθούν με την διερεύνηση και άλλων συμπληρωματικών παραγόντων που θα έχουν όλα τα χαρακτηριστικά που απαιτούνται και αναφέρθηκαν για τα μετρήσιμα μεγέθη στο κεφάλαιο 4.

7.3. Χρήση Εναλλακτικών Μηχανογραφικών Κέντρων για την αντιμετώπιση Ακραίων Επιθέσεων

Μια λύση για τις ακραίες επιθέσεις όπως αυτή που περιγράψαμε στο κεφάλαιο 6 μπορεί να χρησιμοποιηθεί σε πολλούς τύπους βιομηχανιών. Οι οικονομικοί οργανισμοί, οι στρατιωτικές πληροφοριακές υποδομές, τα μεγάλα εταιρικά περιβάλλοντα μπορούν να είναι δυνητικοί χρήστες μιας υπερκείμενης υποδομής.

Αυτή η λύση χαρακτηρίζεται από μια σειρά πλεονεκτημάτων.
α. Μειωμένο κόστος. Χρησιμοποιώντας μια υπάρχουσα υποδομή για περισσότερες δραστηριότητες από αυτές για τις οποίες σχεδιάστηκε αρχικά, είναι πάντα μια απαίτηση των διοικούντων που αποβλέπουν σε μείωση του κόστους επενδύσεων. Μια υπάρχουσα υποδομή, ακόμα κι αν χρειάζεται μερικές ρυθμίσεις ή κάποιους μικρούς μετασχηματισμούς (που μπορούν να μεταφραστούν σε μερικές πρόσθετες ανθρωποώρες) είναι σημαντικά φτηνότερη από την ανάπτυξη μιας νέας ασύρματης υποδομής ως ένα πιθανό υπερκείμενο δίκτυο.

β. Μειωμένος χρόνος. Η διαδικασία ανάκαμψης από ένα περιστατικό ασφάλειας όπως μια επίθεση DDoS είναι πολύ λιγότερο χρονοβόρα όταν οι μόνες ενέργειες που απαιτούνται είναι εκείνες της απενεργοποίησης της δικτυακής ζώνης που δέχεται την επίθεση και της ενεργοποίηση της αντίστοιχης ζώνης στο υπερκείμενο δίκτυο.

γ. Αυξημένη Ασφάλεια. Η εισαγωγή των υπερκείμενων τμημάτων σε ένα δίκτυο, μπορεί ενδεχομένως να μειώσει το ποσό ασφάλειας ολόκληρης της υποδομής. Η πρόσβαση αυτού του τύπου στο ενσύρματο δίκτυο του Κύριου Κέντρου μπορεί να εξισορροπηθεί ως κίνδυνος συγκρινόμενος με τον κίνδυνο κατά τη χρήση κακώς διαμορφωμένων συσκευών δικτύων, ή των συσκευών ασύρματων δικτύων που ήταν «ξεχασμένες» μέσα στο κτήριο της επιχείρησης.

δ. Ευκολότερη διαχείριση. Μια ενσύρματη υποδομή μπορεί να είναι πιο εύκολα διαχειρίσιμη δεδομένου ότι είναι ήδη σε λειτουργία και δεν υπάρχει καμία ανάγκη (ή πολύ μικρή ανάγκη) να εισαχθούν πρόσθετα δίκτυα διαχείρισης για τον έλεγχο των μηχανισμούς αντιμετώπισης ακραίων επιθέσεων.

Η λύση αυτή όμως παρουσιάζει και κάποιους περιορισμούς:

α. Η πτυχή της φορητότητας δεν ικανοποιείται πλήρως κατά χρησιμοποίηση αυτής της λύσης. Η φορητότητα μπορεί να είναι χρήσιμη κυρίως για τις καταστάσεις όπου οι χρήστες επιθυμούν να κρατήσουν μυστική τη φυσική θέση της υπερκείμενης υποδομής τους. Μια τέτοια ανάγκη μπορεί να είναι πιθανή και να βρει κάποια χρήση στις στρατιωτικές εφαρμογές αλλά μπορεί να θεωρηθεί ως δευτερεύουσας σπουδαιότητας για άλλους τύπους οργανισμών. Στην περίπτωση που η υποδομή Ανάκαμψης από καταστροφή (δηλαδή το υπερκείμενο δίκτυο) υλοποιείται ως ασύρματο δίκτυο, η απαίτηση της φορητότητας θα μπορούσε να ικανοποιηθεί.

β. Η υποδομή Ανάκαμψης από καταστροφή θα πρέπει να έχει όσο το δυνατόν λιγότερα κοινά στοιχεία με την Κύρια υποδομή. Για παράδειγμα, εάν υπάρχει ένα κοινό δίκτυο αποθηκευτικού χώρου (SAN) και για το Κύριο και για το Εναλλακτικό Κέντρο τότε οποιαδήποτε χρήση της υποδομής Ανάκαμψης από καταστροφή ως υπερκείμενο δίκτυο για να αντιμετωπίσει τις ακραίες επιθέσεις θα αποτύχει.

γ. Μπορεί επίσης να υπάρξουν καταστάσεις όπου η λειτουργία του υπερκείμενου δικτύου (ή κάποιων τμημάτων του) περιορίζονται από το κανάλι επικοινωνίας μεταξύ της Κύριας και Εναλλακτικής Υποδομής. Οι συνδέσεις που δεν επιτρέπουν οποιαδήποτε άλλη κυκλοφορία εκτός από την κυκλοφορία IP επηρεάζουν τους τύπους ζωνών που μπορούν να μεταστραφούν από μια περιοχή σε άλλη. Για παράδειγμα, τα πρωτόκολλα δικτύων όπως το SNA της

IBM μπορούν να μην είναι χρησιμοποιήσιμα σε δίκτυα ευρείας περιοχής (SNA over WAN).

δ. Τέλος, οι επιθέσεις που βασίζονται στα χαρακτηριστικά που παραμένουν τα ίδια κατά τη λειτουργία και των δύο κέντρων απλώς θα περιορίσουν προσωρινά τις συνέπειες της επίθεσης. Σε εκείνες τις περιπτώσεις η χρήση των κατάλληλων μηχανισμών IDS και IPS θεωρείται αποφασιστικής σημασίας για την απομόνωση των συστημάτων που δέχονται την επίθεση.

7.4. Χρήση Παραγωγικών Υποδομών Ανεκτικών σε Σφάλματα

Ο προτεινόμενος μετασχηματισμός αποτελεί μια προσαρμοσμένη ιδέα. Εντούτοις η πραγματική εφαρμογή της θεωρίας διαχείρισης αλλαγών για τους συγκεκριμένους στόχους μετασχηματισμού που είναι βασισμένοι περισσότερο στην πρακτική εμπειρία είναι μια νέα προσθήκη στις μεθοδολογίες διαχείρισης και βελτιστοποίησης υποδομών.

Τα οφέλη που παρουσιάστηκαν περιλαμβάνουν τόσο τα τεχνικά οφέλη όσο και τα οικονομικά και διαχειριστικά οφέλη καθώς επίσης και τη συμβολή στις πράσινες τεχνολογίες.

Η θεωρία έχει υποστηριχθεί με την καθιέρωση μερικών μετρήσεων KPIs βασισμένων στο πλαίσιο του ITIL προκειμένου να δοκιμαστεί και να αποδειχθεί η δυνατότητα εφαρμογής της. Αυτές οι μετρήσεις στοχεύουν να καταγράψουν, να εξετάσουν και να αξιολογήσουν ουσιαστικά την συγκεκριμένη προσέγγιση κατά τρόπο επίσημο, ακριβή και συνεπή.

Χρησιμοποιώντας KPIs, όπως αυτά που προτάθηκαν, τα διοικητικά στελέχη των πληροφοριακών υποδομών είναι σε θέση να αξιολογήσουν τα αποτελέσματα του μετασχηματισμού των συστημάτων υψηλής διαθεσιμότητας σε FTPIs. Επιπλέον, η ίδια η μεθοδολογία μετασχηματισμού μπορεί επίσης να αξιολογηθεί και από την οπτική των τεχνολογικών και επιχειρησιακών οφελών.

Ως γενικότερη παρατήρηση, θα πρέπει να επισημάνει ότι η μεθοδολογία μετασχηματισμού μπορεί επίσης να ιδωθεί ως τμήμα του συνόλου εννοιών και πολιτικών του ITIL για τη διαχείριση των αλλαγών στις υποδομές και τις υπηρεσίες.

Ακολουθώντας αυτό τον τρόπο σκέψης, η μελλοντική έρευνα θα πρέπει να περιλάβει μια πιο λεπτομερή ανάλυση της σχέσης με τις διαδικασίες αλλαγών του ITIL, ευθυγραμμίζοντας το μετασχηματισμό των συστημάτων υψηλής διαθεσιμότητας σε FTPI με τα σχετικά τμήματα του πλαισίου του ITIL, όπως η στρατηγική των υπηρεσιών, το σχέδιο των υπηρεσιών και τη μετάβαση των υπηρεσιών.

Μια πιο λεπτομερής ανάλυση των επιλεγμένων KPIs και της χρήσης τους μπορεί επίσης να προσφέρει περισσότερες πληροφορίες για τους ενδεχόμενους χρήστες της μεθοδολογίας. Οι παράγοντες που είναι σχετικοί με τη χρήση των πόρων θα μπορούσαν να περιλάβουν συμπληρωματικές πληροφορίες σχετικά με το χρόνο μέτρησης, τη συχνότητα μέτρησης καθώς επίσης και τον αριθμό των επαναλήψεων της μέτρησης.

Υπάρχουν επίσης άλλες επεκτάσεις στην προτεινόμενη μεθοδολογία, η οποία μπορεί να ισχυροποιήσει τη σχέση με το ITIL. Αυτές οι επεκτάσεις μπορούν να περιλάβουν τη χρήση ενός Πίνακα Ισορροπημένης Μέτρησης Απόδοσης (Balanced Scorecard) καθώς επίσης και τη εναρμόνιση του καταλόγου υπηρεσιών (Service Catalog) της πληροφορικής. Το Balanced Scorecard προτείνει ότι μια οργάνωση πρέπει να αντιμετωπισθεί από τέσσερις διαφορετικές οπτικές (την οπτική της Εκμάθησης και της Ανάπτυξης, την οπτική των Επιχειρησιακών Διαδικασιών, την οπτική των Πελατών και την Οικονομική οπτική). Επιπροσθέτως, το Balanced Scorecard προτείνει την ανάπτυξη μερικών άλλων μετρήσιμων μεγεθών, τη συλλογή σχετικών δεδομένων και την κατάλληλη ανάλυση των σχέσεων των παραπάνω οπτικών. Το Service Catalog είναι ένας κατάλογος υπηρεσιών που μια οργάνωση

παρέχει στους υπαλλήλους ή τους πελάτες της. Κάθε υπηρεσία μέσα στον κατάλογο μπορεί να περιλαμβάνει:

- Μια περιγραφή της υπηρεσίας
- Τα χρονικά πλαίσια ή τα SLAs για την πραγματοποίηση της υπηρεσίας
- Ποιος έχει δικαίωμα για να ζητήσει/βλέπει την υπηρεσία
- Τις σχετικές δαπάνες (ενδεχομένως)
- Τους τρόπους εκπλήρωσης της υπηρεσίας

Συμπερασματικά, η προτεινόμενη προσέγγιση θα πρέπει να θεωρηθεί ως μια ολοκληρωμένη πρακτική πρόταση που περιλαμβάνει μια εισήγηση για την υποδομή – στόχος και την αντίστοιχη μεθοδολογία μετασχηματισμού, καθώς επίσης και την μεθοδολογία για τις μετρήσεις της αποδοτικότητας τόσο της υποδομής όσο και της ίδιας της μεθοδολογίας.

8. Επίλογος

8.1. Συμπεράσματα

Η μέτρηση της ασφάλειας πληροφοριακών συστημάτων είναι ένας αναδυόμενος τομέας μελέτης για τους επαγγελματίες ασφαλείας πληροφοριών. Λαμβάνοντας παραδείγματα από τους τομείς όπως οι κατασκευές, η διοικητική μέριμνα, και τα χρηματοοικονομικά, η μέτρηση της ασφάλειας προσπαθεί να συνδέσει απτούς αριθμούς με τις δραστηριότητες που προστατεύουν τις πηγές πληροφοριών.

Οι ορθές μετρήσεις διευκολύνουν τη συζήτηση, την πρόβλεψη, και την ανάλυση και θα πρέπει να διαθέτουν τα παρακάτω χαρακτηριστικά:

- Να είναι συνεπείς
- Να διαθέτουν χαμηλό κόστος συλλογής των πρωτογενών δεδομένων
- Να αναπαριστούν την ασφάλεια ως ποσοστό ή ως αριθμό
- Να κάνουν χρήση τουλάχιστον μιας μονάδας μέτρησης
- Να σχετίζονται με το ευρύτερο πλαίσιο του οργανισμού ή μιας επιχειρηματικής υπηρεσίας
- Να συνεκτιμούν τη βαρύτητα κάθε επιμέρους παράγοντα στη συνολική εκτίμηση της ασφάλειας

Ο υπολογισμός της ασφάλειας διαφοροποιείται από τη μέτρηση της ασφάλειας. Ενώ η μέτρηση βασίζεται στη λήψη και αποτύπωση πρωτογενών μεγεθών, ο υπολογισμός χρησιμοποιεί τα πρωτογενή μεγέθη με συνδυαστικό τρόπο ώστε να παράγει ένα αποτέλεσμα το οποίο και αποτυπώνει την ασφάλεια. Κρίνεται ότι λόγω της αφηρημένης φύσης της ασφάλειας των πληροφοριακών συστημάτων, μια απευθείας μέτρηση δεν θα έχει πραγματικά και αξιοποιήσιμα αποτελέσματα. Ο υπολογισμός όμως της ασφάλειας μπορεί να είναι αποδοτικότερος απαλείφοντας αυτό το μειονέκτημα χρησιμοποιώντας μετρήσιμα μεγέθη.

Σκοπός της ερευνητικής εργασίας είναι η ανάπτυξη των κατάλληλων μέσων και μεθόδων ποσοτικοποίησης, μέτρησης και υπολογισμού της ασφάλειας πληροφοριακών συστημάτων, με βάση τα οποία προτείνει πολιτικές, ενέργειες και μοντέλα που σχετίζονται με την προστασία και τη διαχείριση κρίσιμων πληροφοριακών υποδομών.

Έτσι με τη χρήση γνωστών μεθοδολογιών που προέρχονται τόσο από τον ακαδημαϊκό χώρο (όπως τα Υπερκείμενα δίκτυα, τη θεωρία διαχείρισης των αλλαγών κ.α.) όσο και από τη βιομηχανία (όπως τις υποδομές υψηλής διαθεσιμότητας, τα Εναλλακτικά Μηχανογραφικά Κέντρα κ.α.) αλλά και τη διεθνή πρακτική (όπως το ITIL, τη διαχείριση κινδύνων κ.α.) μπορούν να προταθούν δύο τύποι υποδομών οι οποίοι στοχεύουν στη βελτιστοποίηση της διαχείρισης της ασφάλειας των κρίσιμων πληροφοριακών υποδομών.

Ο πρώτος τύπος είναι οι Εναλλακτικές Υποδομές (Disaster Recovery Sites) ο οποίος διαχωρίζεται σε τμήματα και κάνει χρήση των μεθοδολογιών των Υπερκείμενων Δικτύων (Overlay Networks) για την αντιμετώπιση ακραίων επιθέσεων στα πληροφοριακά συστήματα και υποδομές.

Ο δεύτερος τύπος είναι οι Παραγωγικές Υποδομές Ανεκτικές σε Σφάλματα (FTPI) ο οποίος εισηγείται το μετασχηματισμό υπαρχόντων υποδομών Ανάκαμψης από Καταστροφή σε αυτό τον τύπο υποδομών. Στο πλαίσιο της έρευνας για το μετασχηματισμό σε FTPI, η έρευνα κατέληξε και καθόρισε τα ακριβή βήματα της μεθοδολογίας μετασχηματισμού που απαιτείται για την υλοποίηση των υποδομών αυτών. Η μεθοδολογία απαιτεί την εμπλοκή των ιδιοκτητών των επιχειρηματικών υπηρεσιών αλλά και των ανώτατων στελεχών του οργανισμού οι οποίοι θα συνεκτιμήσουν τα τεχνικά, κανονιστικά, εμπορικά και νομικά οφέλη της υιοθέτησης της μεθοδολογίας αλλά και της επένδυσης που αυτή απαιτεί.

Με σκοπό τη παροχή βοήθειας στους τελευταίους, η διατριβή εισηγείται ότι τα οφέλη από την αύξηση της ασφάλειας μπορούν να συγκριθούν άμεσα με το

κόστος της σχετικής επένδυσης. Εφόσον τα οφέλη από την αύξηση της ασφάλειας είναι περισσότερα, η διαφορά των δύο αποτυπώνεται ως η προστιθέμενη αξία της ασφάλειας της υπηρεσίας. Η αξία αυτή μπορεί να οριστεί και ως συνάρτηση της φήμης της εταιρίας, του πόσο «ορατή» είναι η επένδυση ασφάλειας στους πελάτες / επενδυτές, των κερδών που σχετίζονται άμεσα ή έμμεσα με την επένδυση αλλά και των οικονομικών απωλειών που μπορεί να προκληθούν από την μη πραγματοποίηση της επένδυσης.

Όπως αναφέρθηκε και στο κεφάλαιο 4 με τη χρήση της σχετικής μεθοδολογίας είναι δυνατό να ισορροπήσουν οι επενδύσεις της ασφάλειας σε κάθε υπηρεσία ώστε να μεγιστοποιηθούν τα κέρδη του οργανισμού, τα οποία εκφράζονται ως ROI (ή πιο συγκεκριμένα ROSI) της συγκεκριμένης υπηρεσίας αλλά και του συνόλου των υπηρεσιών που προσφέρονται.

Η βελτιστοποίηση της διαχείρισης της ασφάλειας των κρίσιμων πληροφοριακών υποδομών αλλά και των υπολοίπων λειτουργικών χαρακτηριστικών όλων των πληροφοριακών συστημάτων έχει πολλά πλεονεκτήματα και οφέλη.

Ένα βασικό όφελος είναι η αύξηση της ασφάλειας των πληροφοριακών υποδομών. Λόγω του γεγονότος ότι η ασφάλεια μπορεί να ποσοτικοποιηθεί με τη χρήση των μεθοδολογιών που αναπτύχθηκαν, η αύξησή της μπορεί να αποτυπωθεί ως συγκεκριμένο μέγεθος είτε με οικονομικούς όρους (κέρδη / έσοδα) είτε με όρους κανονιστικής συμμόρφωσης.

Η κανονιστική και νομική συμμόρφωση είναι ένα άλλο όφελος από την υιοθέτηση των Παραγωγικών Υποδομών Ανεκτικών σε Σφάλματα που προτάθηκαν.

Στα οικονομικά οφέλη συγκαταλέγεται η μεγαλύτερη αποδοτικότητα των πληροφοριακών υποδομών η οποία συνεπάγεται και αυξημένη

παραγωγικότητα. Ένα άλλο οικονομικό όφελος είναι η μείωση των λειτουργικών εξόδων που σχετίζονται με τις πληροφορικές υποδομές.

Εκτός από τα παραπάνω η διατριβή περιλαμβάνει και μια σειρά από μετρήσιμα μεγέθη τα οποία χρησιμοποιούνται για τη συγκέντρωση, την καταγραφή και τον υπολογισμό των οφελών των παραπάνω μεθοδολογιών. Τα μεγέθη αυτά βασίζονται στους Κύριους Δείκτες Απόδοσης (KPIs) από το πλαίσιο βέλτιστων πρακτικών του ITIL.

8.2. Ανοικτά πεδία για περαιτέρω έρευνα

Η διατριβή είναι το αποκορύφωμα της έρευνας μιας σειράς θεμάτων της ασφάλειας των πληροφοριακών συστημάτων. Στο σύνολο της πορείας της, η έρευνα επεδίωξε να διερευνήσει διαφορετικές πτυχές του αντικειμένου της, εξετάζοντας τις σχετικές επιστημονικές μεθοδολογίες και προσεγγίσεις, χωρίς όμως να αγνοήσει και τις πρακτικές της βιομηχανίας πληροφορικής. Όμως, η παρούσα έρευνα εξακολουθεί να διατηρεί το επιστημονικό της ενδιαφέρον αφήνοντας μια σειρά από ανοικτά πεδία, τα οποία θα μπορούσαν να θεωρηθούν φυσική εξέλιξη της συγκεκριμένης έρευνας. Αυτά σχετίζονται με τα παρακάτω ζητήματα:

1. Για τον υπολογισμό της ασφάλειας με τη χρήση των δομικών στοιχείων της ασφάλειας μια πιθανή μελλοντική έρευνα μπορεί να περιλάβει μια πιο λεπτομερή ανάλυση για τη διατύπωση των σωστών ερωτήσεων για κάθε επιχειρηματική υπηρεσία.

2. Μια άλλη ομάδα πιθανών ζητημάτων που θα μπορούσαν να είναι μέρος μελλοντικής έρευνας για τη μεθοδολογία υπολογισμού με τη χρήση των δομικών στοιχείων της ασφάλειας, αφορά τον καθορισμό παραγόντων όπως ο χρόνος μέτρησης, η συχνότητα της μέτρησης καθώς επίσης και ο αριθμός των επαναλήψεων της μέτρησης.

3. Για τον υπολογισμό της ασφάλειας με τη χρήση των παραγόντων CARLS το τρέχον επίπεδο της συμμόρφωσης αναπαρίσταται με ένα «Ναι» ή ένα «Όχι», για την απλοποίηση του μοντέλου. Μια μελλοντική επέκταση του μοντέλου μπορεί να είναι η μετατροπή του συγκεκριμένου παράγοντα C (Compliance) σε ποσοστό, το οποίο θα υποδηλώνει ότι η υπηρεσία καλύπτει μέρος των απαιτήσεων συμμόρφωσης.

4. Ένας από τους περιορισμούς της μεθόδου για τον υπολογισμό της ασφάλειας με τους παράγοντες CARLS είναι το γεγονός ότι όλοι οι παράγοντες θεωρούνται ισοδύναμοι. Μια μελλοντική έρευνα θα μπορούσε να διερευνήσει περαιτέρω τον βαθμό που επηρεάζεται η ασφάλεια από κάθε μια παράμετρο και να προτείνει τρόπους στάθμισης των παραγόντων.

5. Σε ότι αφορά τη μεθοδολογία μετασχηματισμού σε FTPIs, μια μελλοντική έρευνα μπορεί να περιλάβει πιο λεπτομερή ανάλυση της σχέσης της συγκεκριμένης μεθοδολογίας με τις διαδικασίες αλλαγών του ITIL, ευθυγραμμίζοντας το μετασχηματισμό των συστημάτων υψηλής διαθεσιμότητας σε FTPI με τα σχετικά τμήματα του πλαισίου του ITIL, όπως η στρατηγική των υπηρεσιών, το σχέδιο των υπηρεσιών και τη μετάβαση των υπηρεσιών.

6. Μια πιο λεπτομερής ανάλυση των επιλεγμένων KPIs και της χρήσης τους μπορεί επίσης να προσφέρει περισσότερες πληροφορίες για τους ενδεχόμενους χρήστες της μεθοδολογίας μετασχηματισμού. Οι παράγοντες που είναι σχετικοί με τη χρήση των πόρων θα μπορούσαν να περιλάβουν συμπληρωματικές πληροφορίες σχετικά με το χρόνο μέτρησης, τη συχνότητα μέτρησης καθώς επίσης και τον αριθμό των επαναλήψεων της μέτρησης.

7. Υπάρχουν ακόμα άλλες επεκτάσεις στην προτεινόμενη μεθοδολογία, οι οποίες μπορούν να ισχυροποιήσουν τη σχέση της μεθοδολογίας μετασχηματισμού με το ITIL. Αυτές οι επεκτάσεις μπορούν να περιλάβουν τη χρήση ενός Balanced Scorecard καθώς επίσης και τη εναρμόνιση του Service Catalog της πληροφορικής με τις νέες υπηρεσίες που προσφέρονται από την μετασχηματισμένη υποδομή.

8. Τέλος οι FTPIs μπορούν να συνδυαστούν με τεχνολογίες που θα έχουν επίγνωση των περιεχομένων της μεθοδολογίας της επίθεσης. Αυτό θα έχει ως αποτέλεσμα την αντιμετώπιση των ακραίων επιθέσεων όχι μόνο σε δικτυακό ή επίπεδο συστημάτων αλλά και σε λογικό επίπεδο που θα μπορεί να διαφοροποιεί κατάλληλα τις εφαρμογές και τα δικαιώματα πρόσβασης αντίστοιχα με τις στρατηγικές επιδιώξεις του επιτιθέμενου.

Τα παραπάνω ανοικτά θέματα αποτελούν κάποιες πιθανές, αλλά όχι τις μοναδικές, επεκτάσεις στο ερευνητικό πεδίο της διατριβής. Η γενική θεματική ενότητα της ασφάλειας των πληροφοριακών συστημάτων αλλά και οι επιμέρους θεματικές ενότητες της μέτρησης της ασφάλειας και της διαχείρισης των Κρίσιμων Πληροφοριακών Υποδομών θεωρούνται πολύ ενδιαφέρουσες τόσο από την ακαδημαϊκή κοινότητα όσο και από την επιχειρηματική αγορά.

Βιβλιογραφία

Andress, M., "Surviving Security, How to Integrate People, Process and Technology", Sams, 2001, ISBN 978-0672324789

Gordon, St. R. και Gordon Judith R., "Information Systems: A management approach", International Edition, Wiley, 1996, ISBN 0-03-016314-5

Heath, R., "Crisis Management for managers and executives", Pearson Education Limited, 2005, ISBN 960-512-434-3

Hiles, An. και Barnes, P., "The Definitive Handbook of Business Continuity Management", Wiley, 1999, ASIN: B001C6JCPU

Jaquith, A., "Security Metrics: Replacing Fear, Uncertainty, and Doubt", Addison-Wesley Professional, 2007, ISBN 978-0321349989

Maizlitsh, B. και Handler, R., "IT Portfolio Management: Step by Step", John Wiley & Sons, 2005, ISBN: 978-0-471-64984-7

Martin, J., "Organisational Behaviour", Thomson Business Press, 1998, ISBN 1-86152-180-4

McClure, St., "Hacking Exposed 4th Edition: Network Security Secrets And Solutions", McGraw-Hill Osborne Media, 2005, ISBN 978-0072260816

Mullins, L. J., "Management and Organisational Behaviour", 5th Edition, Pitman Publishing, 1999, ISBN 0-273-63552-2

Schneier, B., "Secrets & Lies, Digital Security in a Networked World", John Wiley & Sons, 2000, ISBN 0-471-25311-1

Tipton, H. F. και Krause M., "Information Security Management Handbook", Auerbach Publications, 2007, ISBN 978-1420067088

Zikmund, W., "Business Research Methods", Chapter 7, Dryden Press, 2000, ISBN 0-03-025817-0

Κάτσικας, Σ. Κ. και Γκρίτζαλης, Δ. Α., "Ασφάλεια πληροφοριακών συστημάτων", Εκδόσεις Νέων Τεχνολογιών, 2004, ISBN: 9789608105577

Πάγκαλος, Γ. και Μαυρίδης Ι., "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων", Εκδόσεις Ανικούλα, 2002, ISBN 960-516-018-8

Συντομεύσεις και Ακρωνύμια

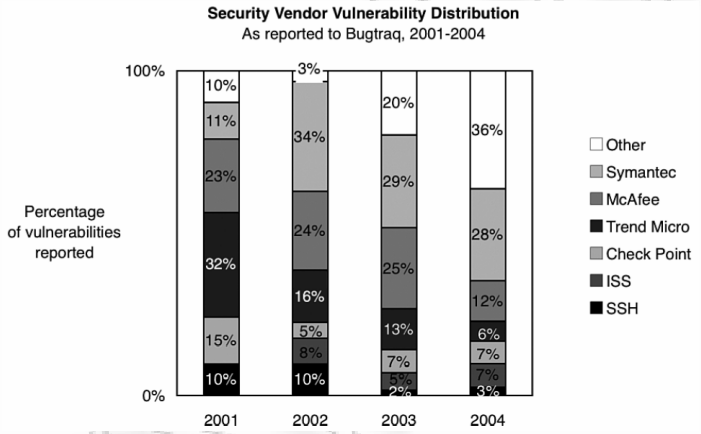
BAM	Business Activity Monitor / Παρακολούθηση Επιχειρηματικών Δραστηριοτήτων
BCP	Business Continuity Planning / Σχεδιασμός Επιχειρηματικής Συνέχειας
BS	British Standard / Βρετανικό Πρότυπο
CARLS	Compliance / Συμμόρφωση, Availability / Διαθεσιμότητα, Return / Απόδοση, Liabilities / Παθητικό, Stock value / Τιμή μετοχής
CBA	Cost Benefit Analysis / Ανάλυση Κόστους - Οφέλους
DDoS	Distributed Denial of Service / Κατανεμημένες Επιθέσεις Άρνησης Εξυπηρέτησης
DNS	Domain Name Service / Υπηρεσία Ονοματολογίας
DoS	Denial of Service / Επιθέσεις Άρνησης Εξυπηρέτησης
DR	Disaster Recovery / Ανάκαμψη από Καταστροφή
DRP	Disaster Recovery Plan / Πλάνο Ανάκαμψης από Καταστροφή
FTE	Full Time Equivalent / Ισοδύναμο Πλήρους Απασχόλησης
FTPI	Fault Tolerant Production Infrastructure / Παραγωγικες Υποδομές Ανεκτικές σε Σφάλματα
GB	Gigabyte / Γιγα-μπάιτ
IDS	Intrusion Detection System / Σύστημα Ανίχνευσης Εισβολών
IP	Internet Protocol / Πρωτόκολλο Διαδικτύου
IPS	Intrusion Prevention System / Σύστημα Αποτροπής Εισβολών
ISO	International Standards Organisation / Διεθνής Οργανισμός Προτύπων
ITIL	Information Technology Infrastructure Library / Βιβλιοθήκη Υποδομής Τεχνολογίας Πληροφοριών
KPI	Key Performance Indicator / Βασικοί Δείκτες Απόδοσης
MB	Megabyte / Μέγκα-μπάιτ
MIPS	Million Instructions Per Second / Εκατομμύρια Εντολές ανά δευτερόλεπτο
MTBF	Mean Time Before Failure / Μέσος Χρόνος Πριν από την

	εμφάνιση Αστοχίας
MTTR	Mean Time to Repair / Μέσος Χρόνος Επιδιόρθωσης
O/S	Operating System / Λειτουργικό Σύστημα
RAID	Redundant Array of Inexpensive Disks / Συστοιχία Πλεοναζόντων Φθηνών Δίσκων
RAM	Random Access Memory / Μνήμη Τυχαίας Προσπέλασης
ROI	Return On Investment / Απόδοση Επένδυσης
RON	Resilient Overlay Network / Ευπροσάρμοστο Υπερκείμενο Δίκτυο
ROSI	Return On Security Investment / Απόδοση Επένδυσης στην Ασφάλεια
RPO	Recovery Point Objective / Σημείο Στόχου Ανάκαμψης
RTO	Recovery Time Objective / Μέγιστος Αποδεκτός Χρόνος Αποκατάστασης
SAN	Storage Area Network / Δίκτυο αποθήκευσης δεδομένων
SLA	Service Level Agreement / Συμβολαιοποιημένη Συμφωνία
SNA	Systems Network Architecture / Αρχιτεκτονική Δικτυακών Συστημάτων
SOX	Sarbanes – Oxley / Πράξη Σαρμπάνη - Όξλεϋ
TB	Terabyte / Τερα-μπάιτ
TCO	Total Cost of Ownership / Ολικό Κόστος Ιδιοκτησίας
TCP	Transmission Control Protocol / Πρωτόκολλο Ελέγχου Μεταφοράς
VPN	Virtual Private Network / Εικονικό Ιδιωτικό Δίκτυο
WAN	Wide Area Network / Δίκτυο Ευρείας Περιοχής
ΕΠΙ	Εξοικείωση, Πρόβλεψη, Ικανότητα
ΜΑΧΑ	Μέγιστος Αποδεκτός Χρόνος Αποκατάστασης
ΜΧΕ	Μέσος Χρόνος Επιδιόρθωσης
ΜΧΠΑ	Μέσος Χρόνος Πριν από την εμφάνιση Αστοχίας
ΣΣΑ	Σημείο Στόχου Ανάκαμψης

Παράρτημα Α: Παραδείγματα οπτικοποίησης της ασφάλειας

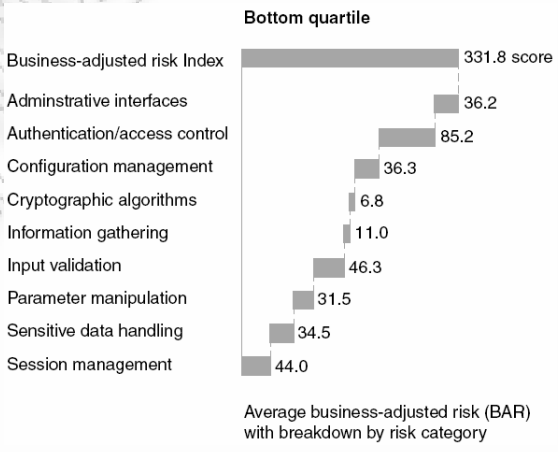
Το παράρτημα αυτό περιλαμβάνει οπτικά παραδείγματα των απεικονιστικών μεθόδων που περιγράφηκαν στο κεφάλαιο 4.4.3. Τα παραδείγματα έχουν εξαχθεί από το βιβλίο του A. Jaquith «Security Metrics: Replacing Fear, Uncertainty, and Doubt». Όπως αναφέρθηκε και στο κεφάλαιο 4, οι τύποι των διαθεσίμων απεικονιστικών μεθόδων ποικίλουν. Τα παραδείγματα των μεθόδων οπτικοποίησης της ασφάλειας είναι:

1. Τα συσσωρευμένα ραβδοδιαγράμματα (Stacked bar charts), τα οποία παρουσιάζουν τη συνεισφορά κάθε σειράς δεδομένων επί του απόλυτου συνόλου ανά συγκεκριμένα χρονικά διαστήματα.



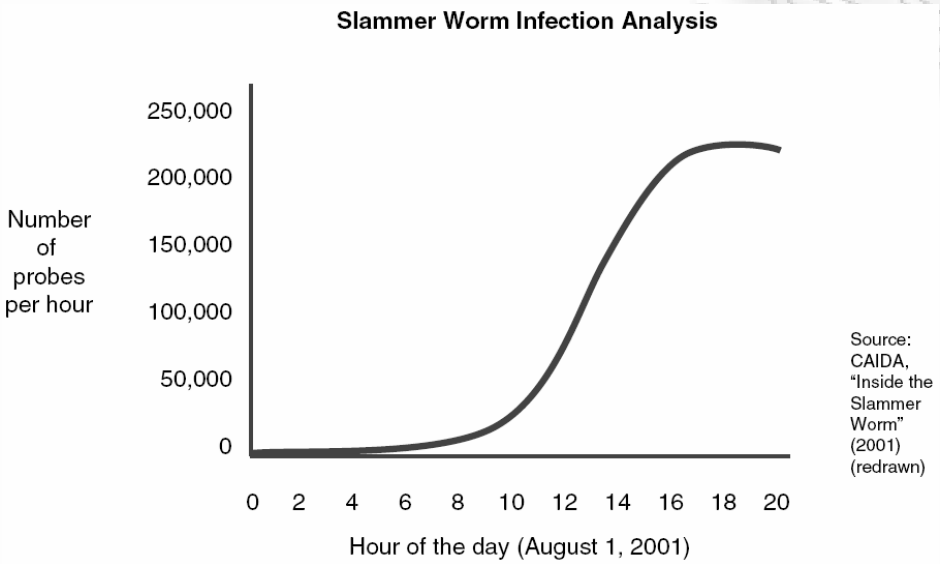
Διάγραμμα Α 1 – Παράδειγμα συσσωρευμένου ραβδοδιαγράμματος

2. Τα διαγράμματα – καταρράκτες (Waterfall charts), τα οποία παρουσιάζουν πως πολλαπλές κατηγορίες συγκεντρώνονται για να σχηματίσουν ένα γενικό σύνολο σε μια συγκεκριμένη χρονική στιγμή.



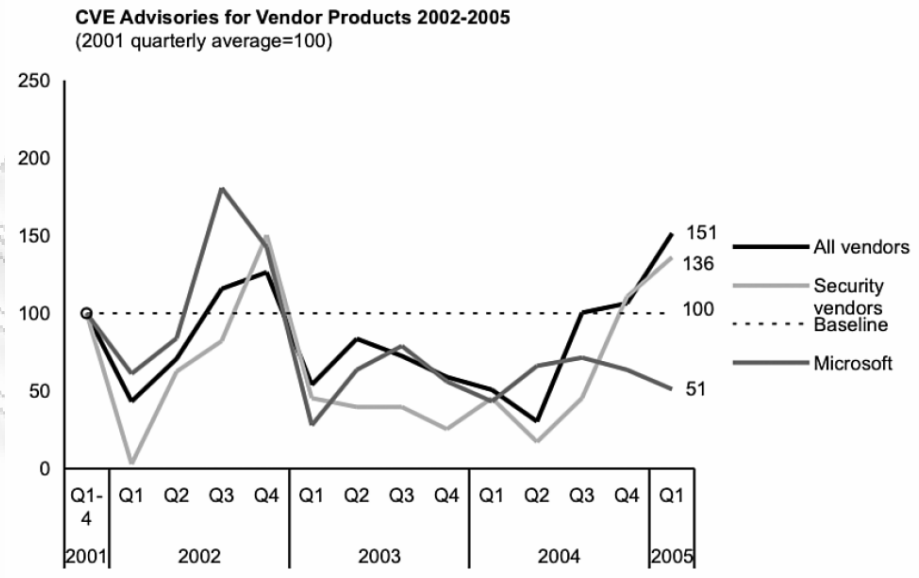
Διάγραμμα Α 2 – Παράδειγμα διαγράμματος – καταρράκτη

3. Τα διαγράμματα χρονολογικών σειρών (Time series charts), τα οποία παρουσιάζουν πως μια ή περισσότερες σειρές μεταβάλλονται σε μια συγκεκριμένη χρονική περίοδο, π.χ. σε 1 ώρα, 1 μήνα, 1 τρίμηνο ή 1 έτος.



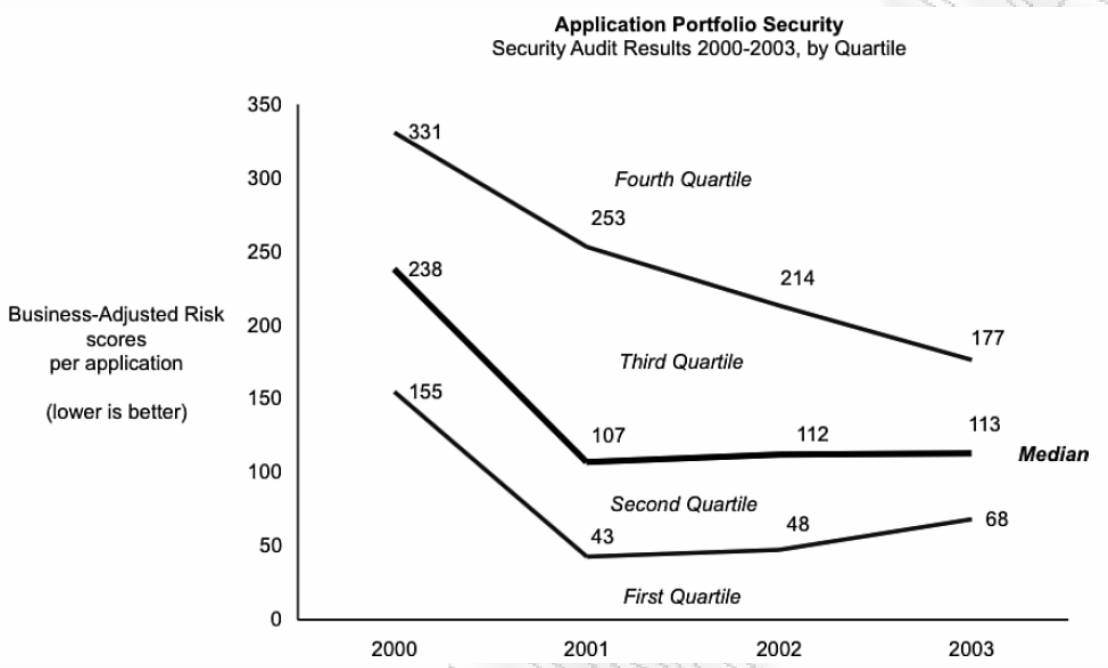
Διάγραμμα Α 3 - Παράδειγμα διαγράμματος χρονολογικής σειράς

4. Τα διαγράμματα χρονολογικών σειρών με δείκτη (Indexed time series charts), τα οποία εκφράζουν κάθε σημείο ως πολλαπλάσιο της αρχικής τιμής του.



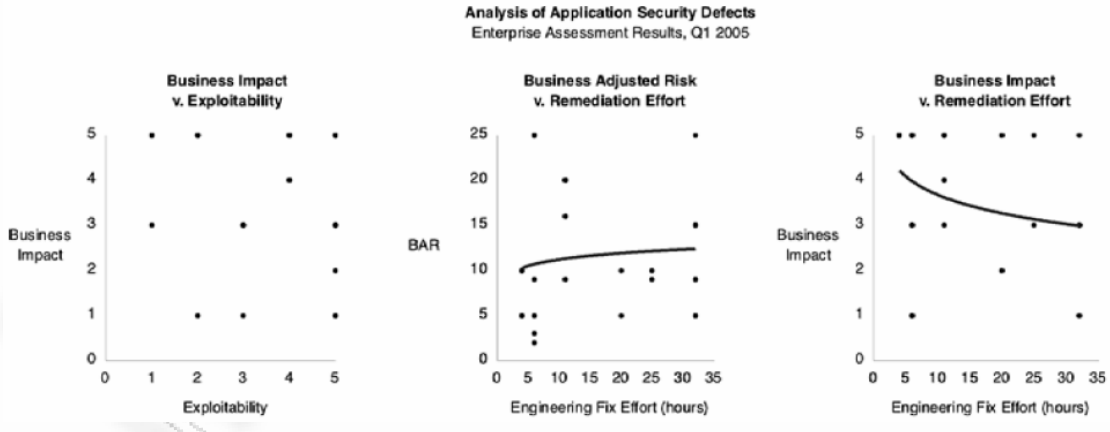
Διάγραμμα Α 4 – Παράδειγμα διαγράμματος χρονολογικής σειράς με δείκτη

5. Τα διαγράμματα χρονολογικών σειρών με τεταρτημόρια (Quartile time series charts), τα οποία σχεδιάζουν τις τιμές ανά τεταρτημόριο για μια σειρά δεδομένων σε ένα συγκεκριμένο χρονικό διάστημα.



Διάγραμμα Α 5 – Παράδειγμα διαγράμματος χρονολογικής σειράς με τεταρτημόρια

6. Τα διαγράμματα διπλών μεταβλητών (Bivariate charts), τα οποία δείχνουν πως δύο μεταβλητές συμπεριφέρονται συγκριτικά μεταξύ τους.



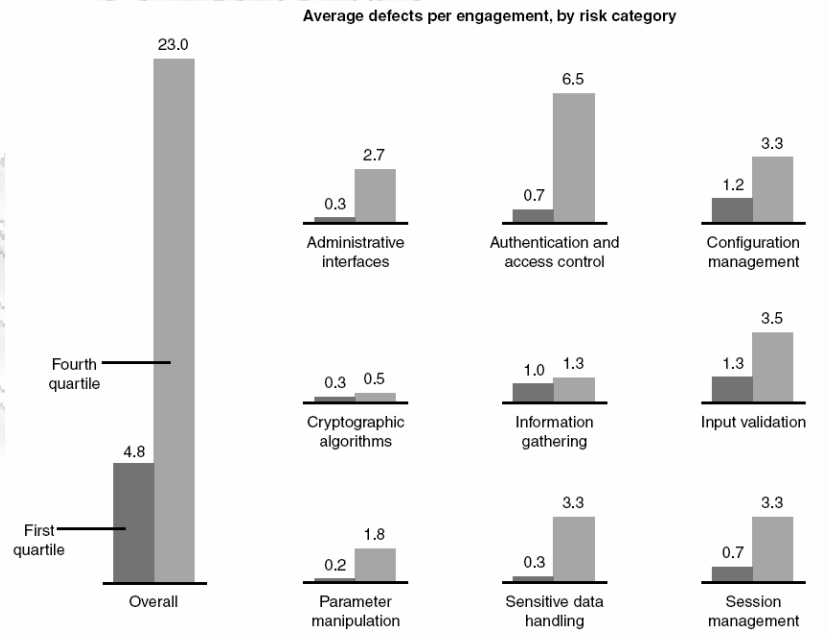
Διάγραμμα Α 6 – Παράδειγμα διαγράμματος διπλών μεταβλητών

7. Οι πολλαπλοί μικρο-πίνακες (Small multiples), οι οποίοι σχεδιάζουν παρόμοια μικρά διαγράμματα στον ίδιο πίνακα, επιτρέποντας τη γρήγορη επισκόπηση και την αναζήτηση τάσεων, ομοιοτήτων και διαφορών.

Service Name	Port Number	Activity Past Month	Explanation
epmap	135		DCE endpoint resolution
microsoft-ds	445		Win2k+ Server Message Block
---	1026		
icq	1027		icq instant messanger
ms-sql-s	1433		Microsoft-SQL-Server
ms-sql-m	1434		Microsoft-SQL-Monitor
radmin	4899		Remote Administrator default port
netbios-ssn	139		NETBIOS Session Service
---	1028		
smtp	25		Simple Mail Transfer

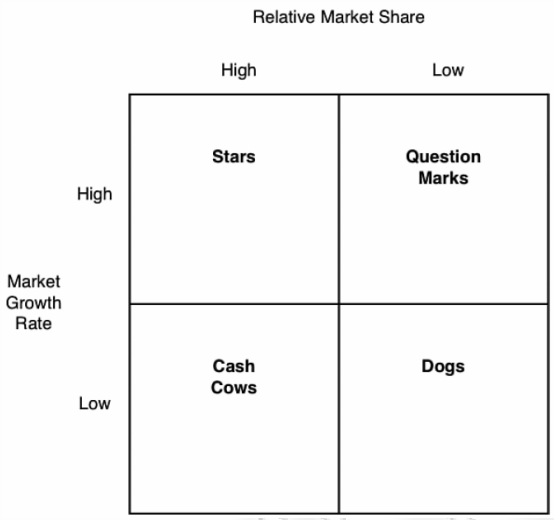
Διάγραμμα Α 7 – Παράδειγμα πολλαπλού μικρο-πίνακα

8. Οι πολλαπλοί μικρο-πίνακες με τεταρτημόρια (Quartile-plot small multiples), οι οποίοι συνδυάζουν τη συγκριτική δύναμη των πολλαπλών μικρο-πινάκων με την ευκολία των τερτατημορίων.



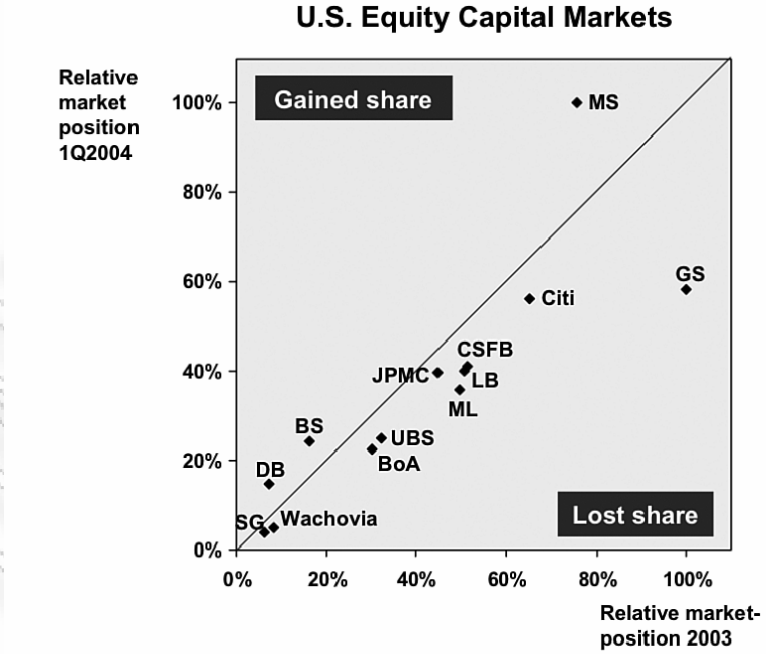
Διάγραμμα Α 8 – Παράδειγμα πολλαπλού μικρο-πίνακα με τεταρτημόρια

9. Οι πίνακες δυο-επί-δυο (Two-by-two matrices), τα οποία επεκτείνουν τα διαγράμματα διπλών μεταβλητών ομαδοποιώντας τα αποτελέσματα σε τεταρτημόρια.



Διάγραμμα Α 9 – Παράδειγμα πίνακα δυο-επί-δυο

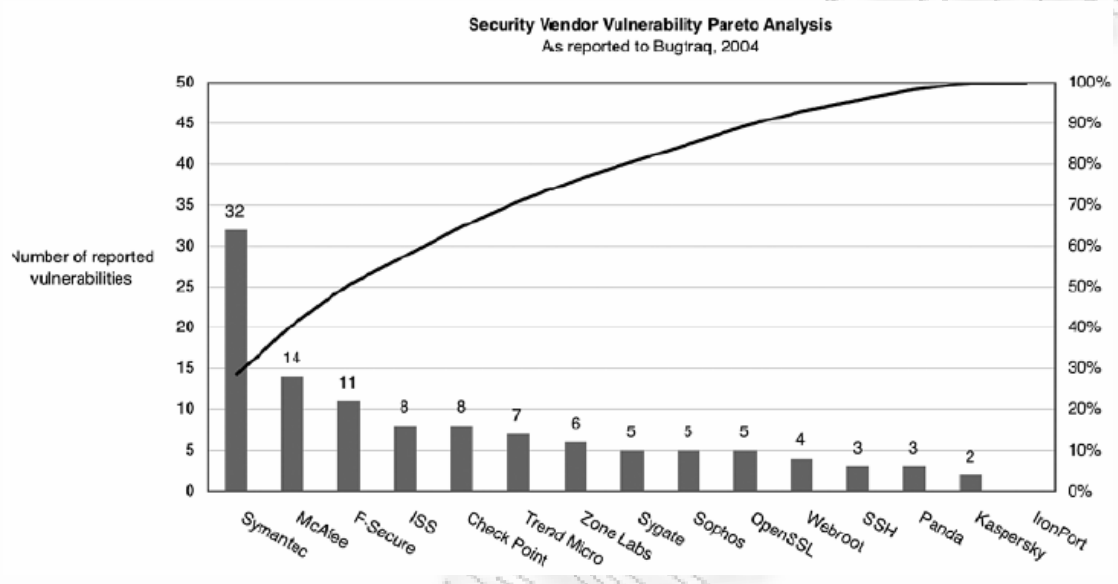
10. Τα διαγράμματα μοιρασμένων περιόδων (Period-share charts), στα οποία διακρίνονται τα σημεία βελτίωσης και επιδείνωσης σε δύο συνεχόμενες χρονικές περιόδους.



Note: Share relative to market leader
JPMC volumes include Bank One
Sources: Dealogic; SDC; BCG analysis

Διάγραμμα Α 10 – Παράδειγμα διαγράμματος μοιρασμένων περιόδων

11. Τα διαγράμματα Παρέτο (Pareto charts), τα οποία παρουσιάζουν ταξινομημένα δεδομένα με τη μορφή ράβδων. Στο δευτερεύοντα άξονα, χρησιμοποιείται μια γραμμή η οποία εκφράζει το συνολικό άθροισμα της κάθε τιμής ως ποσοστό τοις εκατό.



Διάγραμμα Α 11 – Παράδειγμα διαγράμματος Παρέτο

12. Οι πίνακες (Tables), οι οποίοι δειχνουν τα δεδομένα με διάταξη πλέγματος.

Network zones: order of implementation

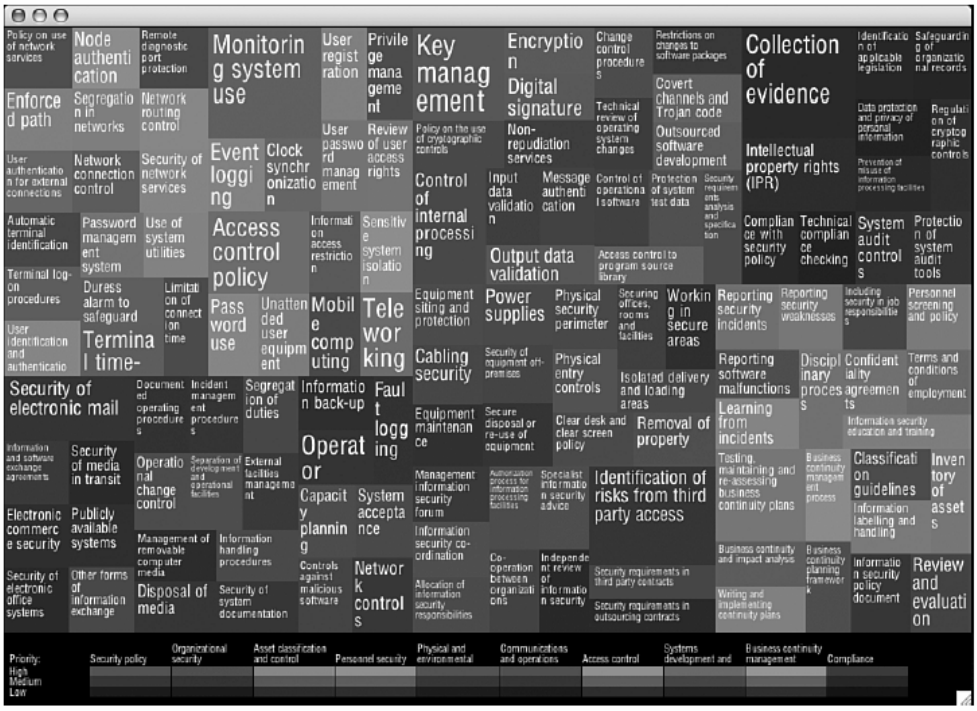
Minimize risks from untrusted sources first, then secure sensitive data.

Zone	Traffic type	Degree of trust***	Risks	Data sensitivity	Dependencies
DMZ*	Many-to-many	●	Unquantified risks, denial of service	●	Feeds from outside Framingham
Data	Many-to-few	● ● ●	IP theft, reputation	● ● ●	Applications, cultural
IT Admin	Few-to-few	● ● ●	Rogue admins, denial of service, eavesdropping	● ●	Hardware upgrades, cultural
Serverland	Many-to-few	● ● ●	Fraud, IP theft, denial of service	● ● ●	App-to-app communications
Userland**	Many-to-many	● ●	IP theft, denial of service	● ●	Cultural, function-specific protections

Implementation order

Διάγραμμα Α 12 – Παράδειγμα Πίνακα με διάταξη πλέγματος

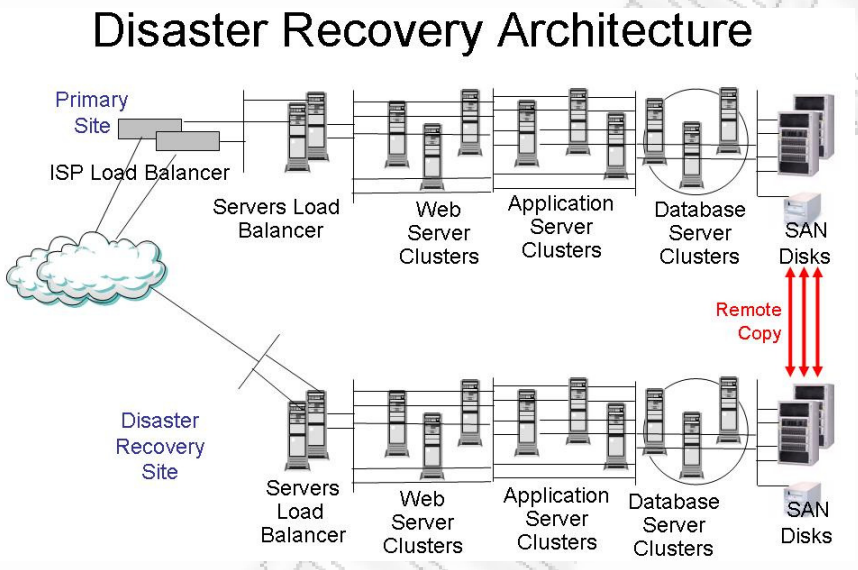
13. Οι δενδροειδείς χάρτες (Treemaps), οι οποίοι δείχνουν τις ιεραρχικές σχέσεις σε ομάδες δεδομένων ως σειρές επαναλαμβανόμενων παραλληλόγραμμων.



Διάγραμμα Α 13 – Παράδειγμα δενδροειδή χάρτη

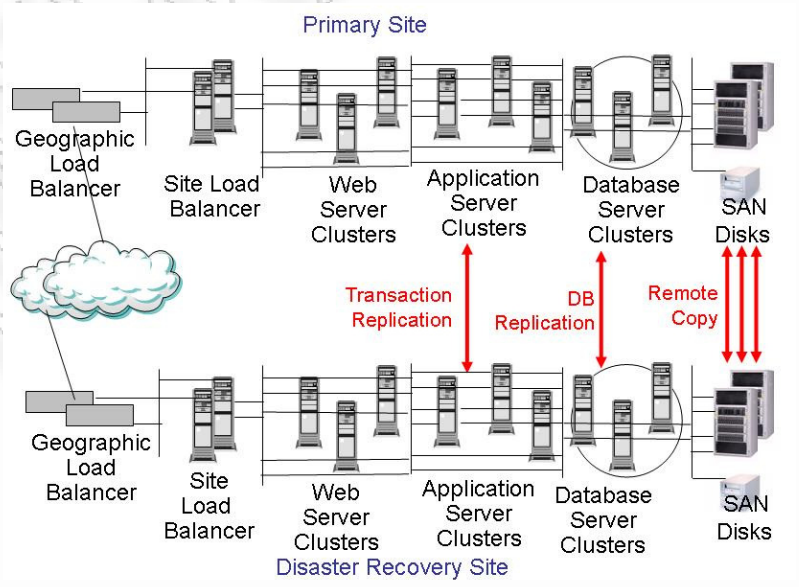
Παράρτημα Β: Παράδειγμα εφαρμογής μεθόδου μετασχηματισμού

Ένα παράδειγμα της μεθοδολογίας μετασχηματισμού απεικονίζεται με τη χρήση μιας πληροφορικής υποδομής που αποτελείται από ένα Κύριο Μηχανογραφικό Κέντρο και από ένα Εναλλακτικό Μηχανογραφικό Κέντρο. Τα δύο μηχανογραφικά κέντρα πριν τον μετασχηματισμό έχουν την παρακάτω μορφή:



Διάγραμμα Β 1 – Μηχανογραφικά κέντρα πριν τον μετασχηματισμό

Μετά τον μετασχηματισμό σε FTPI η πληροφοριακή υποδομή απέκτησε την παρακάτω μορφή, η οποία μετέτρεψε το Disaster Recovery Site σε Secondary Site.



Διάγραμμα Β 2 – Μηχανογραφικά κέντρα μετά τον μετασχηματισμό