Αλεξάνδρειο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Θεσσαλονίκης
Σχολή: Διοίκησης & Οικονομίας
Τμήμα: Διοίκησης Επιχειρήσεων
Κατεύθυνση: Μάρκετινγκ

Πτυχιακή εργασία
με θέμα:

Η ΑΣΦΑΛΕΙΑ

των λογιστικών πληροφοριακών συστημάτων σε επιχειρήσεις στην Ελλάδα

Επιβλέπων Καθηγητής: Τσιάκης Θεοδόσιος, Ph.d
Καθηγητής Εφαρμογών

Ο Φοιτητής: Καργίδης Παναγιώτης
ΑΜ: 033/13
Εξάμηνο: Η'

Σεπτέμβριος 2017, Θεσσαλονίκη

ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ: ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ: ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΚΑΤΕΥΘΥΝΣΗ: ΜΑΡΚΕΤΙΝΓΚ

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ: ΤΣΙΑΚΗΣ ΘΕΟΔΟΣΙΟΣ

Ο ΦΟΙΤΗΤΗΣ: Καργίδης Παναγιώτης

Σεπτέμβριος 2017, Θεσσαλονίκη

“Στ' αλήθεια, όπως κι ο ήλιος, αγαπώ τη ζωή κι όλες τις βαθιές θάλασσες.
Κι' αυτό για μένα λέγεται γνώση:
ό,τι βρίσκεται βαθιά πρέπει να υψωθεί - μέχρι το δικό μου ύψος!”

Νίτσε Φρίντριχ

Περιεχόμενα

Πίνακες & Σχήματα

Ευχαριστίες

Θα ήθελα να απευθύνω θερμές ευχές στον επιβλέποντα καθηγητή μου κ. Τσιάκη Θεοδόσιο, για την πολύτιμη καθοδήγηση που μου παρείχε προκειμένου να διεκπεραιώσω την πτυχιακή μου εργασία.

Επίσης, θέλω να ευχαριστήσω όλους εκείνους που με βοήθησαν για την ταχεία και ορθή υλοποίηση της έρευνας, δίνοντας μου την ευκαιρία να προσεγγίσω το δείγμα μου.

Τέλος, θέλω να ευχαριστήσω την οικογένεια και τους φίλους μου οι οποίοι μου προσέφεραν την απαραίτητη ηθική συμπαράσταση για την επίτευξη των στόχων μου.

Περίληψη

Η παρακάτω εργασία με θέμα «Η ασφάλεια των λογιστικών πληροφοριακών συστημάτων σε επιχειρήσεις στην Ελλάδα», υλοποιήθηκε στα πλαίσια της απόκτησης του πτυχίου από το τμήμα της Διοίκησης Επιχειρήσεων του ΑΤΕΙ Θεσσαλονίκης. Σκοπός της ίδιας ήταν, η συλλογή πρωτογενών στοιχείων τα οποία σχετίζονται με τα λογιστικά πληροφοριακά συστήματα, την λειτουργικότητα, τους κινδύνους καθώς και το ενδιαφέρον της διοίκησης των οργανισμών για αυτούς. Βασική δειγματοληπτική μέθοδος χρησιμοποιήθηκε αυτή της κρίσεως, έχοντας ως βασικές μεταβλητές, το επάγγελμα και την χώρα δραστηριοποίησης της επιχείρησης. Η εξέλιξη της τεχνολογίας έχει επιφέρει τεράστιες αλλαγές ανά τα χρόνια στην συλλογή καταγραφή και μεταφορά δεδομένων. Νέα μοντέλα και τρόποι ήρθαν στην επιφάνεια, γεγονός το οποίο δεν πέρασε απαρατήρητο από τους οργανισμούς.

Ωστόσο, η ταχεία εξέλιξη έχει επιφέρει και σημαντικά ζητήματα προς επίλυση, όπως είναι η διασφάλιση της ποιότητας των λογιστικών δεδομένων. Οι απειλές και οι εισβολείς έχουν πληθύνει, καθιστώντας ευάλωτες τις επιχειρήσεις που δεν λαμβάνουν μέτρα ασφαλείας, δεδομένου ότι αυξάνονται τα τρωτά σημεία των οργανισμών. Βέβαια, υπάρχουν και εταιρίες οι οποίες έχουν προνοήσει και έτσι κατάστρωσαν στρατηγικές ελέγχου και ασφαλείας έναντι των κινδύνων αυτών. Κρισιμότερο στοιχείο της υλοποίησης είναι η σωστή κατανομή των μέτρων ασφαλείας εν μέσω της αναγνώρισης των περιουσιακών στοιχείων, των κινδύνων καθώς και των τρωτών σημείων.

Καταλήγοντας, συνδυάζοντας αξιόπιστα στοιχεία μαζί με την υλοποίηση ενδελεχούς έρευνας δόθηκε μία εικόνα όσον αφορά την ασφάλεια και τους κινδύνους στα λογιστικά δεδομένα στις επιχειρήσεις στην Ελλάδα. Διασαφηνίστηκε, ο τρόπος καταγραφής δεδομένων, η λειτουργικότητα του λογιστικού πληροφοριακού συστήματος, το είδος των επιθέσεων που καλούνται να αμυνθούν οι οργανισμοί, η ευαισθητοποίηση της διοίκησης για τους κινδύνους. Έτσι, δόθηκαν συμπεράσματα και προτάσεις για την ενημέρωση των εταιριών προκειμένου να ληφθούν μέτρα ασφαλείας.

Abstract

The following research was conducted in order to graduate from Alexander Technological Institute of Thessaloniki. This research is about the “Security matters of Accounting Information Systems (AIS) of Greece-based businesses”. On purpose to fulfil this survey in a right way, we conducted a field research to compile data regarding to the AIS, their functionality, the risks and the sensitivity of the management concerning about the threats. In addition, for the collection of the data we used the method of judgement based on two basic variables, the professions of the sample and the country that the companies are operated. It is well known that technology development influences the collection, the recording and the transmission of data. Indeed, the last decades, new models came on the surface, as a result the organizations were enforced to monitor and to be adjusted to a new era.

However, this improvement caused some new issues that must be considered of the organizations, such as assurance of the accounting data quality. It is believed that countermeasures are the only way for the companies in order to be safe from the huge amount of threats and risks that they have to face. According to bibliography, some organizations adapted properly in the new era by creating strategies to improve the safety level against to their enemies. On purpose to build a strong strategy it is vital for them to identify their assets, the threats and their vulnerabilities.

Last but not least, we combined data from the desk and field research to have a better view regarding to the security and the threats that the companies in Greece have to face. The results have helped us to understand the methods that the companies use to record their accounting data, the level of functionality of the AIS that they use, the sorts of threats that they have faced and the level of sensitivity that the management has regarding the data assurance. Thus, the analysis of the data led us to some important conclusions that they gave us the capability to make some recommendations to the companies to take countermeasures.

Εισαγωγή

Η παρακάτω εργασία με θέμα «Η ασφάλεια των λογιστικών πληροφοριακών συστημάτων σε επιχειρήσεις στην Ελλάδα» πραγματοποιήθηκε στα πλαίσια της απόκτησης του πτυχίου από την σχολή Διοίκησης Επιχειρήσεων του Αλεξάνδρειου Τεχνολογικού Εκπαιδευτικού Ιδρύματος της Θεσσαλονίκης. Πρόκειται για μία έρευνα πεδίου (field research) για την συλλογή πρωτογενών στοιχείων από επαγγελματίες που εργάζονται στην Ελλάδα και έχουν άμεση ή έμμεση σχέση με τα λογιστικά πληροφοριακά συστήματα. Επιπλέον, πραγματοποιήθηκε και δευτερογενής έρευνα κυρίως από την ξένη βιβλιογραφία, αναζητώντας και συλλέγοντας πληροφορίες τόσο από βιβλία όσο και από επιστημονικά περιοδικά. Για την συλλογή των στοιχείων τα οποία αφορούν την έρευνα, υλοποιήθηκε πρωτογενής έρευνα με την μέθοδο της δημοσκόπησης, στην συνέχεια, πραγματοποιήθηκαν προσωπικές συνεντεύξεις χρησιμοποιώντας ως βασικό μέσο συλλογής των στοιχείων αυτών, ένα δομημένο ερωτηματολόγιο, εντοπίζοντας έτσι το επίπεδο χρήσης των λογιστικών πληροφοριακών συστημάτων στην Ελλάδα, καθώς επίσης και το ενδιαφέρον της διοίκησης των οργανισμών σχετικά με την ασφάλεια των λογιστικών δεδομένων. Τέλος, ερευνήθηκε η μορφή των επιθέσεων που έχουν δεχθεί οι επιχειρήσεις.

Σκοπός

Σκοπός της παρούσας έρευνας είναι η διερεύνηση του επιπέδου ασφαλείας των λογιστικών πληροφοριακών συστημάτων από επιχειρήσεις στην Ελλάδα. Ειδικότερα, η γνώση των επιθέσεων που δέχονται οι οργανισμοί προκειμένου να είναι σε θέση να πάρουν μέτρα προφύλαξης έναντι των εισβολέων.

Στόχοι Έρευνας

Γενικός Στόχος

Η διερεύνηση της ασφάλειας των δεδομένων στα λογιστικά πληροφοριακά συστήματα σε οργανισμούς στην Ελλάδα.

Ειδικοί Στόχοι

- ✓ Ποιες απειλές ελλοχεύουν για τους οργανισμούς, ποιοι είναι οι εισβολείς και ποια τα τρωτά σημεία;
- ✓ Ποια είναι η διαδικασία αναγνώρισης των κινδύνων και αξιολόγησης των απειλών;
- ✓ Ποιοι έλεγχοι πραγματοποιούνται για την ασφάλεια των λογιστικών πληροφοριακών συστημάτων;
- ✓ Χρησιμοποιούν λογιστικά πληροφοριακά συστήματα;
- ✓ Ποιοι έχουν πρόσβαση στα λογιστικά πληροφοριακά συστήματα;
- ✓ Παρέχει online υπηρεσίες το λογιστικό πληροφοριακό σύστημα;
- ✓ Έχουν πραγματοποιηθεί τροποποιήσεις στη αγορά του ERP;
- ✓ Με ποιους τρόπους καταγράφονται και μεταφέρονται τα λογιστικά δεδομένα;
- ✓ Το λογιστικό πληροφοριακό σύστημα που χρησιμοποιείται, είναι λειτουργικό;
- ✓ Ενδιαφέρεται η διοίκηση του οργανισμού για την ασφάλεια των λογιστικών πληροφοριακών συστημάτων και αν ναι, πραγματοποιούνται προγράμματα εκπαίδευσης των εργαζομένων και ποιο είναι το επίπεδο επάρκειας τους;
- ✓ Τι επιθέσεις έχουν κληθεί να αντιμετωπίσουν οι οργανισμοί;
- ✓ Υπάρχει σχέση ανάμεσα στο μέγεθος του οργανισμού και στην πιθανότητα να χρησιμοποιεί λογιστικό πληροφοριακό σύστημα;
- ✓ Υπάρχει σχέση ανάμεσα στο μέγεθος του οργανισμού και στην πραγματοποίηση προγραμμάτων εκπαίδευσης του προσωπικού;
- ✓ Υπάρχει σχέση ανάμεσα στο μέγεθος του οργανισμού και στον τρόπου καταγραφής των δεδομένων;

- ✓ Υπάρχει σχέση ανάμεσα στο φύλο και στον γνώμη που έχουν για την λειτουργικότητα του λογιστικού πληροφοριακού συστήματος;
- ✓ Υπάρχει σχέση ανάμεσα στο φύλο και στην γνώμη που έχουν για το ενδιαφέρον της διοίκησης του οργανισμού για θέματα ασφαλείας;
- ✓ Υπάρχει σχέση ανάμεσα στο μέγεθος και στην γνώμη στην λειτουργικότητα του λογιστικού πληροφοριακού συστήματος;
- ✓ Υπάρχει σχέση ανάμεσα στο μέγεθος και στην γνώμη στο ενδιαφέρον της διοίκησης του οργανισμού για θέματα ασφαλείας;

Κεφάλαιο 1

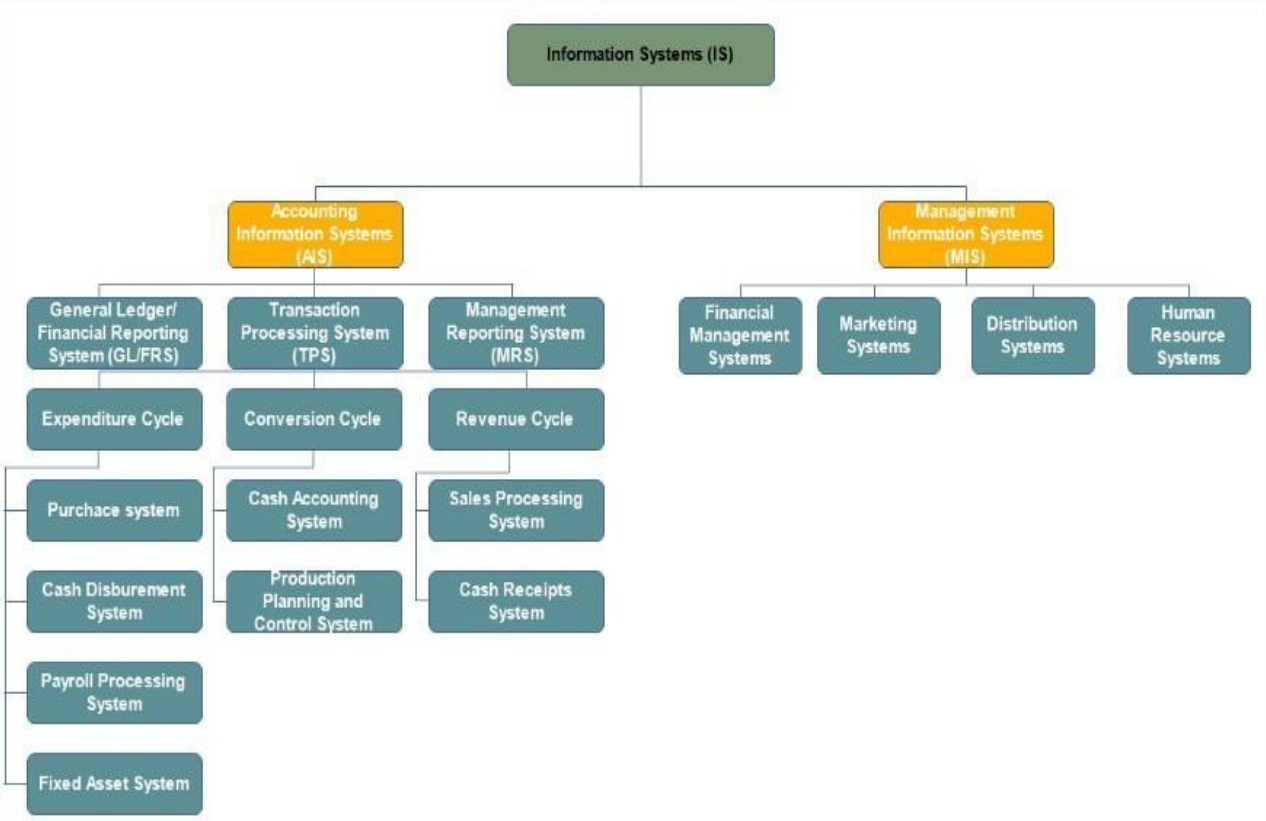
Εισαγωγή στα λογιστικά πληροφοριακά συστήματα (AIS)

1.1. Εισαγωγή

Η εποχή που διανύουμε είναι φρόνιμο να χαρακτηρισθεί ως η εποχή της τεχνολογίας και κατ' επέκταση της πληροφορίας. Η ταχύτατη διάδοση της τεχνολογίας κατέστησε ευκολότερη την πρόσβαση σε μεγάλο όγκο δεδομένων, με αποτέλεσμα αναπόφευκτα πολλοί κλάδοι αναπροσάρμοσαν την δομή και την λειτουργία τους. Χαρακτηριστικό παράδειγμα αποτελεί ο κλάδος της λογιστικής, καθώς σύμφωνα με την Maureen Link, παλιότερα κυρίαρχο ρόλο κατείχε το χαρτί, ενώ σήμερα η τεχνολογία (Bagranoff κ.α., 2010, σελ. 4).

Σήμερα η εύρεση μεγάλου όγκου δεδομένων αποτελεί μία εύκολη διαδικασία για τις επιχειρήσεις καθώς έρχονται σε επαφή με αυτά σε καθημερινή βάση. Η δυσκολία έγκειται στο γεγονός της αξιολόγησης τους, με την έννοια ότι, τα δεδομένα θα κριθούν με βάση κάποια χαρακτηριστικά για τον βαθμό στον οποίο αξίζει να υποστούν επεξεργασία, τέτοια ώστε να παραχθεί πληροφορία ωφέλιμη για την επιχείρηση (Κεχρής, 2005, σελ. 26).

Αυτή είναι και η δουλειά ενός πληροφοριακού συστήματος, η οποία ξεκινάει με την συλλογή διαφόρων δεδομένων, συνεχίζει με την επεξεργασία τους με σκοπό την παραγωγή πληροφορίας και εν συνεχεία καταλήγει στον διαμοιρασμό των πληροφοριών στα μέλη τα οποία έχουν την δυνατότητα να τις αξιοποιήσουν στον βέλτιστο βαθμό (Hall, 2010, σελ. 7). Συνεχίζοντας, από το παρακάτω διάγραμμα γίνεται αντιληπτό πως τα πληροφοριακά συστήματα (IS) αποτελούν ένα σύνολο το οποίο διαχωρίζεται στα λογιστικά πληροφοριακά συστήματα (AIS) και στα πληροφοριακά συστήματα μάρκετινγκ (MIS). Μάλιστα, αληθεύει πως και αυτά διασπώνται και σε άλλα υποσυστήματα (Hall, 2010, σελ. 8). Ειδικότερα, τα AIS πραγματεύονται δεδομένα τα οποία εισέρχονται στην επιχείρηση με την μορφή οικονομικών συναλλαγών. Βέβαια, είναι εφικτή η συλλογή δεδομένων τα οποία δεν παίρνουν την παραπάνω μορφή αλλά έχουν άμεσο αντίκτυπο στις οικονομικές συναλλαγές. Τέτοια συναλλαγή μπορεί να είναι η επεξεργασία των στοιχείων ενός πελάτη ο οποίος είναι καταγεγραμμένος στην εταιρική βάση δεδομένων (Hall, 2010, σελ. 7).



Σχήμα 1: Ο σκελετός ενός πληροφοριακού συστήματος.

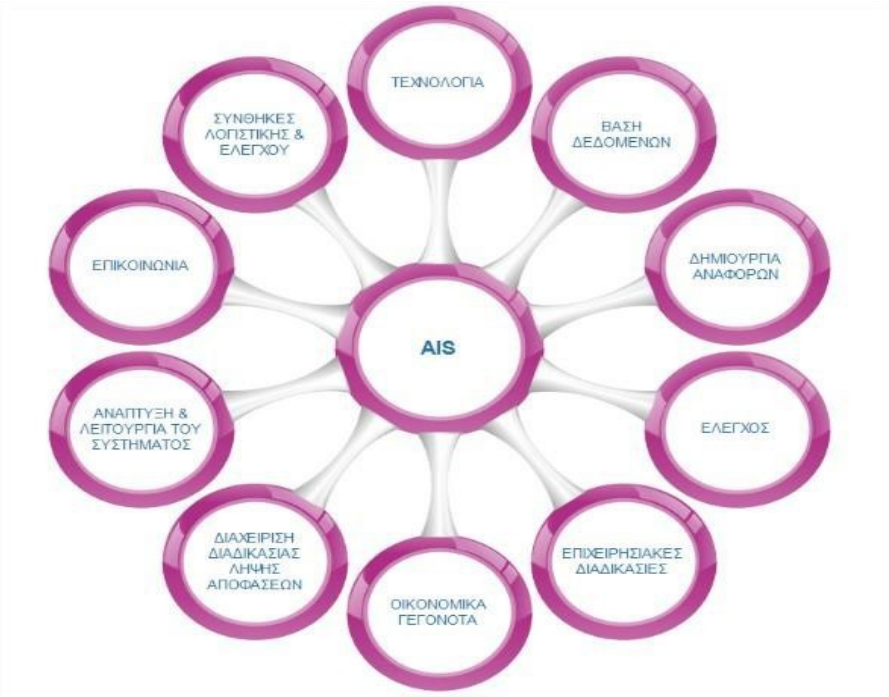
Πηγή: Hall, J. (2011). Accounting Information Systems 7e. U.S.A.: Cangage Learning, σελ.8.

Παραπάνω ειπώθηκε πως το AIS και το MIS αποτελούν υποσυστήματα του IS, τα οποία με την σειρά τους διασπώνται σε άλλα υποσυστήματα. Ειδικότερα το AIS, απαρτίζεται από τρία υποσυστήματα, κάτι το οποίο παριστάνεται γραφικά παραπάνω. Έτσι, το γενικό καθολικό μαζί με το MRS και το TPS συνθέτουν αυτό που αναφέρεται παραπάνω ως το AIS, γεγονός που αποδεικνύει την υψηλή σημασία που κατέχουν για το πληροφοριακό σύστημα (Hall, 2010, σελ. 9). Τούτο αποδεικνύεται από τις ευθύνες με τις οποίες είναι επιφορτισμένα τα προαναφερθέντα υποσυστήματα. Πιο εξειδικευμένα, το TPS πραγματεύεται οποιοδήποτε λογιστικό γεγονός παρατηρηθεί και ενημερώνεται σε καθημερινή βάση, καθώς ευθύνεται για την παροχή εγγράφων και αναφορών σε όλους τους ενδιαφερόμενους εντός και εκτός επιχείρησης. Συνεχίζοντας, ισχυρό ρόλο φαίνεται να έχει και το γενικό καθολικό το οποίο αφορά την παρουσίαση της εικόνας μιας επιχείρησης μέσα από διάφορες οικονομικές καταστάσεις (Hall, 2010, σελ. 10). Τέτοια αποτελεί η κατάρτιση του ισολογισμού ο οποίος μάλιστα αποτελεί υποχρέωση για κάθε επιχείρηση, μερικές από τις οποίες είναι υποχρεωμένες να προχωρούν σε δημοσίευση του, ειδάλλως υπάρχει η δυνατότητα να τους επιβληθούν κυρώσεις από τις νομικές αρχές. Μάλιστα, στην Αμερική, ο SOX

είναι ιδιαίτερα αυστηρός σχετικά με τις απαιτήσεις του, γεγονός το οποίο δεν αφήνει πολλά περιθώρια για τις επιχειρήσεις δεδομένου ότι πολλές φορές έχουν εμφανιστεί φαινόμενα διαστρέβλωσης των στοιχείων έχοντας ως στόχο την παρουσίαση μιας ενδεχομένως καλύτερης λογιστικής εικόνας η οποία πιθανότατα και να μην ανταποκρίνεται στην πραγματικότητα (Wallace, 2014, σελ. 255). Τέλος, το MRS ασχολείται με πληροφορίες οι οποίες διαμοιράζονται στο εσωτερικό περιβάλλον της επιχείρησης έχοντας ως απώτερο σκοπό την τροφοδότηση με πληροφορίες οι οποίες θα βοηθήσουν στην λήψη αποφάσεων, όπως η σύνταξη ενός προϋπολογισμού (Hall, 2010, σελ. 10).

1.2 Η Δομή των Λογιστικών Πληροφοριακών Συστημάτων

Η μελέτη των λογιστικών πληροφοριακών συστημάτων ολοκληρώνεται μέσα από την μελέτη 10 στοιχείων, τα οποία απεικονίζονται στο παρακάτω γράφημα.



Σχήμα 2: Τα δομικά στοιχεία ενός λογιστικού πληροφοριακού συστήματος.

Πηγή: Gelinas, U., Dull, R. & Wheeler, P. (2012). Accounting Information Systems. U.S.A.: Cengage Learning, σελ. 9. Από: The top ten IT issues, *CA Magazine*, September, 2009 (available at www.camagazine.com/archives/printedition/*2009/sep/features/camagazine29323.aspx, accessed, May 6, 2010)*.

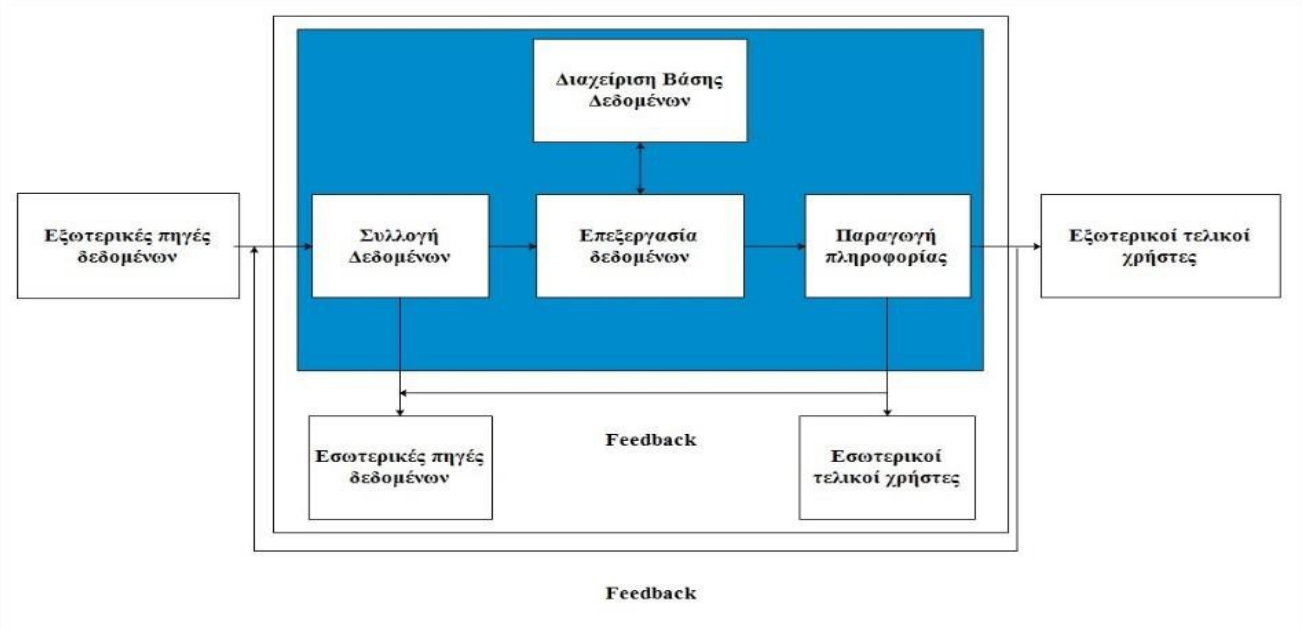
Στο σημείο αυτό θα πραγματοποιηθεί μια μικρή παρουσίαση των στοιχείων αυτών. Συνεπώς, η ανάλυση ξεκινάει με την ***τεχνολογία*** η οποία αποτελεί ένα πολύ σημαντικό στοιχείο, καθώς διαδικασίες όπως η διαχείριση, η παραγωγή και ο σχεδιασμός, εμφανίζουν υψηλό βαθμό σύνδεσης μαζί της. Εν

συνεχεία, επόμενο στοιχείο είναι η ύπαρξη ***βάσης δεδομένων*** μέσα στην οποία αποθηκεύονται τα διάφορα δεδομένα. Μάλιστα, πριν την αποθήκευση θα πρέπει να έχει αποφασισθεί η ποσότητα και η μορφή των δεδομένων που επιτρέπεται να αποθηκευτούν. Επίσης, απόφαση πρέπει να ληφθεί και για την κατάσταση της βάσης, δηλαδή εάν αυτή είναι διαθέσιμη για δημόσια ή μόνο για ιδιωτική χρήση. Απώτερος σκοπός είναι η επεξεργασία των δεδομένων για την παραγωγή πληροφορίας, η οποία θα χρησιμοποιηθεί για την λήψη αποφάσεων ή ακόμη και για την υλοποίηση διαφόρων ελέγχων. Συνεχίζοντας, ένα ακόμη σημαντικό στοιχείο αποτελούν ***οι αναφορές (reports)***, οι οποίες προβάλλουν τα αποτελέσματα των επεξεργασμένων δεδομένων. Είναι σημαντικό, το περιεχόμενο τους να στοχεύει στις ανάγκες και τις επιθυμίες των χρηστών αποφεύγοντας ανούσιες λεπτομέρειες. Η σημασία τους αποδεικνύεται από τον ρόλο που παίζουν στην λήψη των αποφάσεων καθώς αποτελούν την βάση. Επόμενο στοιχείο αποτελεί η ιδιαίτερα απαιτητική διαδικασία **του ελέγχου**, η οποία στοχεύει στην εποπτεία των λειτουργιών της επιχείρησης (Gelinas κ.α., 2012, σελ. 9) αλλά και της οικονομικής απόδοσης του οργανισμού, από την οποία μπορούν να βγουν σημαντικά συμπεράσματα (Marginson, 2006). Πρόκειται για ένα δύσκολο εγχείρημα αν αναλογιστούμε την συνεχόμενη εξέλιξη και μεταβολή που παρουσιάζουν οι επιχειρησιακές λειτουργίες. ***Οι επιχειρησιακές διαδικασίες*** αποτελούν το πέμπτο στοιχείο. Σύμφωνα με την βιβλιογραφία οι λειτουργίες του AIS συγχέονται με τις λειτουργίες όλης της επιχείρησης. Πιο συγκεκριμένα, υπάρχει μία γέφυρα επικοινωνίας μεταξύ του προγράμματος και του οργανισμού, με τον τελευταίο να κατέχει καθοδηγητικό ρόλο προετοιμάζοντας τόσο τις εισόδους, όσο και τις εξόδους του AIS. Τέλος, όπως είναι αναμενόμενο ο οργανισμός πρέπει να γνωρίσει τον τρόπο λειτουργίας του πληροφοριακού συστήματος προκειμένου να επωφεληθεί από αυτό. Προχωρώντας, παρακάτω εμφανίζονται ***οικονομικά φαινόμενα*** τα οποία είναι απαραίτητο να συλλέγονται και να καταγράφονται με σκοπό να χρησιμοποιηθούν μετέπειτα. Οι πωλήσεις μπορούν να θεωρηθούν ως ένα *οικονομικό φαινόμενο.* Μέχρι στιγμής είδαμε πως η λήψη απόφασης επηρεάζεται από πολλούς παράγοντες και δεν θα ήταν σφάλμα να ειπωθεί πως αποτελεί μία ιδιαίτερη διαδικασία. Επόμενο στοιχείο που προστίθεται είναι ***η διαχείριση της λήψης απόφασης***. Σύμφωνα με αυτήν, ο παροχέας της αναφοράς και κατ' επέκταση της πληροφορίας, οφείλει να γνωρίσει τα χαρακτηριστικά και τις προτιμήσεις των ατόμων που είναι επιφορτισμένα με την λήψη της απόφασης, για τον λόγο ότι είναι ορθό να τα έχουν στην διάθεση τους όπως αυτοί επιθυμούν

(Gelinas κ.α., 2012, σελ. 9). Μάλιστα, τα άτομα αυτά, είναι πολύ σημαντικά για τον εκάστοτε οργανισμό, για τον λόγο ότι η λήψη βέλτιστων αποφάσεων, αποσκοπεί στην επίλυση διαφόρων προβλημάτων του οργανισμού (Stair & Reynolds, 2016, σελ. 290). Όγδοο στοιχείο αποτελεί η σωστή ***ανάπτυξη και λειτουργία του συστήματος***. Είναι ένα στοιχείο ιδιαίτερα σημαντικό γιατί αφενός πραγματεύεται δεδομένα που προκύπτουν από *οικονομικά φαινόμενα* και αφετέρου επειδή είναι ικανό να παρέχει τις απαιτούμενες πληροφορίες, επομένως είναι σημαντικό να λειτουργεί στην εντέλεια. Στο σημείο αυτόακολουθούν τα δύο εναπομείναντα στοιχεία τα οποία είναι ***οι επικοινωνίες*** και ***οι συνθήκες λογιστικής και ελέγχου.*** Οι επικοινωνίες σχετίζονται άμεσα με την παρουσίαση των αποτελεσμάτων. Η επιτυχημένη παρουσίαση εξαρτάται σε μεγάλο βαθμό από τις ικανότητες του λογιστή. Τέλος, οι λογιστές πρέπει να είναι σε θέση να γνωρίζουν άριστα τις διαδικασίες ελέγχου όπως επίσης και τις πληροφορίες που είναι απαραίτητο να προβληθούν (Gelinas κ.α., 2012, σελ. 9).

1.3 Γενικό Μοντέλο Λειτουργίας Ενός AIS

Στην παρούσα ενότητα παρουσιάζεται το γενικό μοντέλο λειτουργίας του AIS. Στο μοντέλο αυτό περιλαμβάνονται διάφορα στάδια τα οποία απεικονίζουν την ροή των δεδομένων εντός και εκτός του AIS, από την έναρξη χρήσης η οποία ορίζεται ως την στιγμή της συλλογής των δεδομένων, μέχρις ότου την λειτουργία της ανατροφοδότησης του συστήματος αποσκοπώντας σε περαιτέρω βελτιώσεις.



Σχήμα 3: Γενικό Μοντέλο Λογιστικού Πληροφοριακού Συστήματος.

Πήγή: **Hall, J. (2011). Accounting Information Systems 7e. U.S.A.: Cangage Learning, σελ. 11.**

1.3.1. Τελικοί Χρήστες

Ξεκινώντας, οι χρήστες αποτελούν τα άτομα εκείνα τα οποία έρχονται σε άμεση επαφή με το πληροφοριακό σύστημα (Stair & Reynolds, 2016, σελ. 17). Αυτοί χωρίζονται σε εξωτερικούς και εσωτερικούς χρήστες, με τους πρώτους να αποτελούν οποιονδήποτε είναι άμεσα ενδιαφερόμενος με την επιχείρηση, όπως για παράδειγμα, οι πελάτες, οι προμηθευτές και οι φορολογικές υπηρεσίες. Επιπλέον, ως εξωτερικοί χρήστες νοούνται και τα διάφορα χρηματοπιστωτικά ιδρύματα, όπως είναι οι τράπεζες. Σχετικά με τους εσωτερικούς χρήστες είναι ορθό να ειπωθεί πως βρίσκονται διαμοιρασμένοι σε όλα τα ιεραρχικά επίπεδα της εκάστοτε επιχείρησης. Επιπλέον κρίνεται σκόπιμο να σημειωθεί πως δημιουργούν αναφορές τόσο για το εσωτερικό όσο και για το εξωτερικό περιβάλλον. Πιο συγκεκριμένα, οι αναφορές για τις εσωτερικές διαδικασίες, χρήζουν υψηλότερης δυσκολίας από ότι αυτές του εξωτερικού περιβάλλοντος, και έτσι, οι άνθρωποι που είναι επιφορτισμένοι για την υλοποίηση του ελέγχου στο εσωτερικό, είναι οι λογιστές και οι σχεδιαστές. Τέλος, στα καθήκοντα τους, προστίθενται και η έγκυρη και έγκαιρη τροφοδότηση των ενδιαφερόμενων μελών, με τις σωστές πληροφορίες, αλλά και η μέριμνα τους σε θέματα πρόληψης και ασφάλειας (Hall, 2012, σελ. 10).

1.3.2. Πηγές Δεδομένων

Σημαντικό στάδιο του μοντέλου βρίσκονται οι *πηγές άντλησης ακατέργαστων*

δεδομένων, τα οποία συνήθως προέρχονται από το ERP ή το TPS (Stair & Reynolds, 2016, σελ. 297). Όπως και στους χρήστες, έτσι και εδώ παρατηρούνται δύο περιβάλλοντα από τα οποία προέρχονται τα δεδομένα, ειδικότερα το εσωτερικό και το εξωτερικό περιβάλλον είναι ορθό να θεωρηθούν ως πηγές δεδομένων για την επιχείρηση (Hall, 2012, σελ. 11).

1.3.3. Συλλογή Δεδομένων

Έπειτα από την εύρεση πηγών από τις οποίες θα αντληθούν δεδομένα, ακολουθεί *η διαδικασία της συλλογής τους.* Είναι άξιο αναφοράς πως η συλλογή δεδομένων αποτελεί ένα από τα σημαντικότερα κομμάτια του παζλ, αν όχι το σημαντικότερο. Η σημαντικότητα του έγκειται στο γεγονός πως τα δεδομένα λειτουργούν καταλυτικά για την επιτυχία του μοντέλου. Ειδικότερα, υπάρχει μεγάλη πιθανότητα να προκληθούν σφάλματα στα αντλούμενα δεδομένα τα οποία ενδέχεται να μην γίνουν αντιληπτά από το σύστημα, έχοντας ως αποτέλεσμα την συνέχεια της διαδικασίας και την εξαγωγή λανθασμένων συμπερασμάτων. Αυτή η «εκδοχή» θα ζημιώσει την εταιρία, σε χρόνο, χρήμα και πόρους τόσο σε βραχυχρόνιο ορίζοντα όσο και μακροχρόνιο, καθώς η λήψη μιας απόφασης η οποία έχει βασισθεί κυρίως σε λανθασμένα δεδομένα, αυξάνει κατά πολύ τις πιθανότητες να χαρακτηρισθεί ως αναξιόπιστη με το αναμενόμενο αποτέλεσμα να τείνει προς την αποτυχία. Προκειμένου να αποφευχθούν τα παραπάνω, είναι ζωτικής σημασίας τα αντλούμενα δεδομένα να ικανοποιούν τα κριτήρια της συνάφειας και της αποτελεσματικότητας (Hawryszkiewycz, 1991, σελ. 33; Hall, 2012, σελ. 12).

Ο σχεδιαστής της βάσης δεδομένων θα πρέπει να είναι σε θέση να αξιολογήσει το πλήθος των δεδομένων τα οποία ικανοποιούν τα κριτήρια και επομένως είναι κατάλληλα για συγκομιδή, όπως επίσης να απομονώσει πλήρως τα άχρηστα δεδομένα τα οποία ενδέχεται να προκαλέσουν σημαντικά προβλήματα. Ο παραπάνω έλεγχος όπως γίνεται εύκολα κατανοητό θα έχει άμεσο αντίκτυπο και στο εξαγόμενο αποτέλεσμα, καθώς η πληροφορία θα πληρεί όλα τα παραπάνω κριτήρια και θα είναι ιδανική για χρήση (Hall, 2012, σελ. 12). Όπως έχει προαναφερθεί, ο έλεγχος αποτελεί έργο το οποίο είναι σωστό να χαρακτηρισθεί από υψηλό βαθμό δυσκολίας καθώς ο όγκος των δεδομένων τον οποίο καλείται ο σχεδιαστής να διαχειριστεί, είναι ιδιαίτερα μεγάλος, έχοντας ως αποτέλεσμα, η διαδικασία αξιολόγησης της καταλληλόλητας τους να γίνεται όλο και πιο δυσχαιρής.

Αναφορικά με την *αποτελεσματικότητα* στην συλλογή των δεδομένων, είναι κρίσιμο να τηρείται η μοναδικότητα των αντλούμενων δεδομένων και η αποφυγή επαναλήψεων καθώς κάτι τέτοιο μπορεί να προξενήσει προβλήματα τόσο στους χρήστες όσο και στο σύστημα. Τέτοια προβλήματα εμφανίζονται κυρίως με κατάληψη μεγάλου χώρου αποθήκευσης του συστήματος, επιδρώντας στην λειτουργία του, η οποία επιβραδύνεται και πιθανόν να μην πραγματοποιείται ορθά. Έτσι, είναι λίγο πολύ αναμενόμενο πως όσο μεγαλύτερη είναι η απόκλιση των αντλούμενων δεδομένων από τα θεμιτά επίπεδα, τόσο περισσότερο οξύνονται οι πιθανότητες για *ασυνέπεια* και *αναποτελεσματικότητα* του συστήματος. Κλείνοντας το στάδιο της συλλογής δεδομένων, εύλογο είναι να χαρακτηρισθεί ως στάδιο υψίστης σημασίας διότι ασκεί επιρροή τόσο στην λειτουργία της επιχείρησης όσο και στην διαδικασία λήψης αποφάσεων (Hall, 2012, σελ. 12).

1.3.4. Επεξεργασία Δεδομένων

Εφ' όσον τα παραπάνω στάδια έχουν υλοποιηθεί με επιτυχία είναι εφικτό να ξεκινήσει η επεξεργασία των συλλεχθέντων δεδομένων. Για την επιτυχημένη διεκπεραίωση της επεξεργασίας τους, χρησιμοποιούνται ειδικά στατιστικά προγράμματα τα οποία είναι σε θέση να εξάγουν ασφαλή και ως έναν βαθμό ακριβή, αποτελέσματα. Αυτά είναι ιδιαίτερα χρήσιμα για τους λογιστές αλλά και για κάθε χρήστη, καθώς οι δυνατότητες των προγραμμάτων αυτών ποικίλλουν, για του λόγου το αληθές, η πρόβλεψη των πωλήσεων για το ερχόμενο έτος είναι κάτι το οποίο καθίσταται εφικτό μέσω αυτών. Επιπλέον, ο χρήστης επωφελείται από τα προγράμματα καθώς είναι ικανά να εξάγουν χρήσιμες πληροφορίες μέσω διαφόρων γραφημάτων, με αποτέλεσμα να βελτιστοποιείται η διαδικασία κατανόησης και ερμηνείας των αποτελεσμάτων (Hall, 2012, σελ.12). Τέλος, στο στάδιο της επεξεργασίας των δεδομένων, πραγματοποιούνται οι πιο ενδελεχείς έλεγχοι, προκειμένου να ελαχιστοποιηθούν οι πιθανότητες για σφάλματα (Bagranoff κ.α., 2010, σελ. 396).

1.3.5. Διαχείριση Βάσης Δεδομένων

Συνεχίζοντας, το επόμενο στάδιο στο μοντέλο του AIS είναι η διαχείριση της αποθήκης δεδομένων. Η δημιουργία αποθήκης δεδομένων, θεωρείται ένα πολύ δύσκολο εγχείρημα προς υλοποίηση. Συγκεκριμένα, ακόμη και η εγκατάσταση της αποθήκης, είναι πιθανόν να είναι δυσλειτουργική (Takecian κ.α., 2013). Τα αποθηκευμένα δεδομένα εμφανίζονται χωρισμένα ιεραρχικά, σε μορφή 3

επιπέδων. Αρχικά, στο πρώτο επίπεδο παρουσιάζονται τα *χαρακτηριστικά των δεδομένων,* στην συνέχεια ακολουθεί το *μητρώο δεδομένων*, ενώ στο τελευταίο επίπεδο, βρίσκονται τα *αρχεία καταγεγραμμένων δεδομένων.*

Στο σημείο αυτό επιχειρείται εμβάθυνση στα προαναφερθέντα επίπεδα, ξεκινώντας από τα *χαρακτηριστικά των δεδομένων.* Πρόκειται για ένα στάδιο το οποίο με μια πρώτη σκέψη φαίνεται πως δεν κατέχει σημαντική θέση στο μοντέλο, παρ' όλα αυτά κάτι τέτοιο διαψεύδεται εύκολα καθώς η παραχθείσα πληροφορία δέχεται ισχυρή επιρροή από τα *χαρακτηριστικά των δεδομένων*. Μάλιστα, αυτά, είναι απαραίτητο να διακατέχονται από συνάφεια και λογική. Για του λόγου το αληθές, οποιαδήποτε απόκλιση θα οδηγήσει σε ασυνέπεια μεταξύ των οντοτήτων, κάτι το οποίο θα έχει ως αποτέλεσμα την "παραγωγή" ελλιπής, εσφαλμένης ή ακόμη και κατεστραμμένης πληροφορίας. Δεύτερο στην σειρά στοιχείο της ιεραρχίας, είναι το *μητρώο*, το οποίο αποτελεί το σύνολο των *χαρακτηριστικών* μίας οντότητας. Η ύπαρξη ενός ***μοναδικού χαρακτηριστικού*** λειτουργεί ως καταλύτης για την ομαλή λειτουργία του μοντέλου και την αποφυγή παρανοήσεων, σε περίπτωση που κάποιος από τους χρήστες θελήσει να πραγματοποιήσει αναζήτηση στην βάση δεδομένων (Hall, 2012, σελ. 12-13). Η λύση για το αναφερθέν πρόβλημα είναι η *χρήση πρωτεύοντος κλειδιού*, μάλιστα, ως πρωτεύον κλειδί προτιμάται να δηλώνεται κάποιο τεχνητό χαρακτηριστικό, για τον λόγο ότι είναι δύσκολο να υπάρξει επανάληψη του (Κεχρής, 2005, σελ. 45). Η ορθή επιλογή πρωτεύοντος κλειδιού αυξάνει την λειτουργικότητα και την αποτελεσματικότητα του συστήματος, έχοντας θετικό αντίκτυπο στην συνολική λειτουργία του AIS. Τρίτο και τελευταίο στοιχείο είναι το *αρχείο καταγεγραμμένων δεδομένων* το οποίο αποτελεί ένα ολοκληρωμένο σύνολο από *μητρώα δεδομένων* και κατ' επέκταση από *τα χαρακτηριστικά δεδομένων.* Στο σημείο αυτό, είναι ωφέλιμο να παρουσιασθούν διάφορα θέματα τα οποία προκύπτουν στην δημιουργία, την ανάπτυξη και την διαχείρισης της βάσης δεδομένων. Ειδικότερα, επικρατούν τρεις βασικές αρχές οι οποίες διέπουν την αποτελεσματική διαχείριση των βάσεων. Πρώτα, σημαντικό ρόλο διαδραματίζει *η λειτουργία της αποθήκης* η οποία μεταβάλλει τα εισερχόμενα κλειδιά σε μητρώα και ακολούθως φροντίζει για την μεταφορά τους στην καταλληλότερη τοποθεσία εντός της βάσης. Εν συνεχεία, *η λειτουργία της ανάκτησης* είναι υπεύθυνη για την επιλογή των μητρώων προς εξαγωγή, αποσκοπώντας στην επεξεργασίας τους. Με το πέρας της διαδικασίας, η αποθήκη είναι υπεύθυνη για την επαναπροσαρμογή των νέων μητρώων. Τέλος, ακολουθεί *η αρχή της διαγραφής* η διαθέτει καθοριστικό

ρόλο. Παραπάνω, αναφέρθηκε πως σε ένα σύστημα απαιτείται να πληρούνται τα κριτήρια της συνέπειας και της ισορροπίας των δεδομένων, αποφεύγοντας τους πλεονασμούς. Έτσι, με την "διαγραφή" ο χρήστης καταφέρνει να καταστρέφει μητρώα από την βάση δεδομένων τα οποία έχουν κριθεί ως παλαιά ή υπάρχοντα. Συμπερασματικά, γίνεται αντιληπτό πως οι 3 αρχές είναι αλληλένδετες καθώς συνεργάζονται για την σωστή λειτουργία του συστήματος (Hall, 2012, σελ. 13).

1.3.6. Παραγωγή Πληροφορίας & Ανατροφοδότηση

Δεν υπάρχει αμφιβολία πως τα στάδια του μοντέλου έχουν δημιουργήσει ισχυρούς δεσμούς μεταξύ τους και η επιτυχία του ενός επηρεάζει την μοίρα του επόμενο σταδίου. Αφού λοιπόν ολοκληρωθεί με επιτυχία το στάδιο της επεξεργασίας των δεδομένων, το μοντέλο προχωρά στο αμέσως επόμενο, το οποίο δεν είναι άλλο από την *παραγωγή της πληροφορίας* εκείνης την οποία καλούνται να δεχθούν οι χρήστες προκειμένου να πάρουν αποφάσεις.

Η παρούσα λειτουργία προκειμένου να είναι αποτελεσματική απαιτεί την πραγματοποίηση τεσσάρων μικρο – λειτουργιών. Πρωταρχική λειτουργία είναι η συλλογή των απαραίτητων πληροφοριών, έπειτα ξεκινούν οι διαδικασίες μορφοποίησης και ταυτοποίησης τους, ενώ ως τελική λειτουργία ορίζεται η προβολή του στον τελικό χρήστη (Hall, 2012, σελ. 13).

Στην βιβλιογραφία συχνά φαίνεται να χρησιμοποιούνται οι όροι χρήσιμες, κατάλληλες, απαραίτητες οι οποίοι καλούνται να περιγράψουν τις πληροφορίες αυτές που χρειάζεται η επιχείρηση. Προκειμένου, μια πληροφορία να χαρακτηρισθεί με τους παραπάνω όρους, είναι απαραίτητο να τηρεί κάποιες προδιαγραφές έτσι ώστε να μπορέσει να συμπεριληφθεί στην αναφορά. Αρχικά, μεγάλη σημασία όπως έχει προαναφερθεί, κατέχει η συνάφεια της παρεχόμενης πληροφορίας με το υπό εξέταση "πρόβλημα" που καλείται να λύσει ο χρήστης (Hall, 2012, σελ. 13). Αμέσως μετά, μελετάται η χρονολογία δημιουργίας της πληροφορίας διότι είναι απαραίτητο να είναι επίκαιρη, διαφορετικά αυτή θα κριθεί άχρηστη και θα απορριφθεί (Τηλικίδου, 2011, σελ. 33). Εκείνο που έχει ιδιαίτερη σημασία να λεχθεί είναι ότι η επικαιρότητα μιας πληροφορίας είναι κάτι τελείως υποκειμενικό το οποίο μάλιστα εξαρτάται από το έργο το οποίο έχει κληθεί να ολοκληρώσει ο χρήστης. Είναι πολύ πιθανόν πληροφορίες προερχόμενες από το ίδιο έτος να κριθούν ακατάλληλες για κάποιον χρήστη εν αντιθέσει με κάποιον άλλον που θα τις κρίνει θετικά (Hall, 2012, σελ. 14).

Συνάμα με τα παραπάνω, η πληρότητα και η στόχευση των πληροφοριών

είναι δύο χαρακτηριστικά τα οποία δεν θα μπορούσαν να λείπουν. Είναι υψίστης σημασίας να παρέχονται όλες οι πληροφορίες οι οποίες αφορούν άμεσα το υπό εξέταση θέμα. Κατά συνέπεια είναι ανάγκη, όλες αυτές οι ουσιώδεις πληροφορίες να είναι διαθέσιμες, ευανάγνωστες και ευκολονόητες προς αποφυγήν σφαλμάτων. Επιπρόσθετα, τυγχάνουν περιπτώσεις στις οποίες είναι αδύνατο να επιτευχθεί άριστη στόχευση των πληροφοριών, επίσης, μπορεί να μην είναι απαραίτητη η εξειδίκευση τους σε μεγάλο βαθμό (Hall, 2012, σελ. 14). Για τον λόγο αυτό, οι πολιτικές του εκάστοτε οργανισμού αποσκοπούν στην διασφάλιση στων δύο προαναφερθέντων χαρακτηριστικών (Stair & Reynolds, 2016, σελ. 438).

Τέλος, πρέπει να δοθεί προσοχή στην δομή και στο περιεχόμενο της αναφοράς καθώς αυτή, θα πρέπει να συνταχθεί με τέτοιο τρόπο που θα ικανοποιεί τις ανάγκες των ενδιαφερόμενων χρηστών αλλά και ταυτοχρόνως να είναι σε θέση να διατηρεί το μήνυμα αμετάβλητο στην πορεία του προς τα ανώτατα κλιμάκια. Ευκόλως συμπεραίνεται ότι η σύνταξη μιας αναφοράς προϋποθέτει σωστή μελέτη επί του θέματος. Καταλήγοντας, όπως σε κάθε μοντέλο έτσι και στο AIS, η λειτουργία της ανατροφοδότησης είναι παρούσα. Μέσω της ανατροφοδότησης η επιχείρηση είναι σε θέση να διορθώσει άμεσα κενά ή λάθη τα οποία ενδέχεται να εμφανισθούν. Εκείνο που έχει ιδιαίτερη σημασία να αναφερθεί είναι πως η ανατροφοδότηση μπορεί να προκληθεί τόσο μεταξύ του εσωτερικού περιβάλλοντος, όσο και του εξωτερικού. Έτσι ο οργανισμός, κατέχοντας τα καινούργια δεδομένα στα χέρια του, είναι ικανός να ανακατευθύνει τις κινήσεις προς όφελος του (Hall, 2012, σελ. 14).

1.4. Η Εξέλιξη των Λογιστικών Πληροφοριακών Συστημάτων

Από τις απαρχές της δημιουργίας του κόσμου μέχρι και σήμερα, η ιστορία μας έχει διδάξει πως ο άνθρωπος αποτελεί ένα ιδιαίτερα "ανήσυχο" ον, γεγονός το οποίο είναι άρρηκτα συνδεδεμένο με τις συνεχόμενες ανακαλύψεις, όπως επίσης και το πλήθος βελτιστοποιήσεων σε πολλούς επιστημονικούς κλάδους. Έτσι, και στον τομέα των πληροφοριακών συστημάτων, η δίψα και η ανησυχία των ερευνητών για την εύρεση του βέλτιστου λογιστικού μοντέλου, οδήγησε στην δημιουργία και συνύπαρξη 5 (πέντε) διαφορετικών μοντέλων. Στην ενότητα αυτήν επιχειρείται η περιγραφή τους.

1.4.1. Μη Αυτοματοποιημένη Καταγραφή Δεδομένων - Manual Processing System

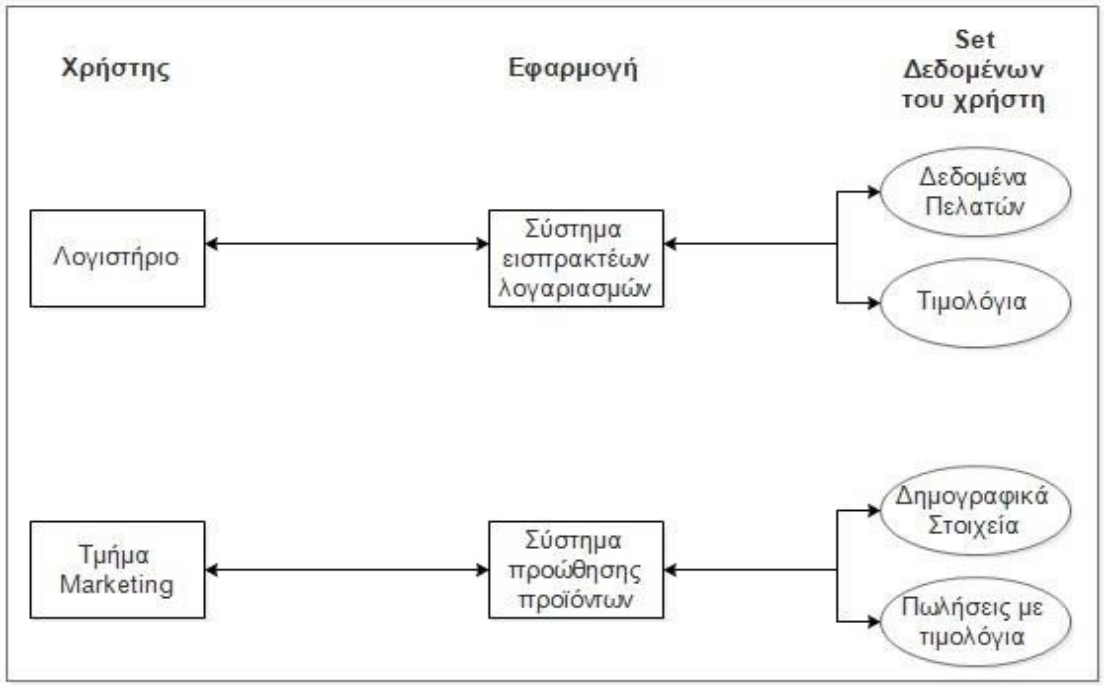
Ξεκινώντας, στην παράγραφο αυτήν παρουσιάζεται το παλαιότερο μοντέλο, του οποίοι οι λειτουργίες υλοποιούνται με τον *παλιό παραδοσιακό, μη αυτοματοποιημένο τρόπο* (Hall, 2012, σελ. 24; Κεχρής, 2005, σελ.29). Το μοντέλο αυτό πραγματεύεται πληροφορίες οι οποίες σχετίζονται με τους πόρους που διαθέτει η επιχείρηση και μπορεί να δαπανήσει. Επιπλέον, καταγράφονται φυσικά γεγονότα, τα οποία στην παρούσα ενότητα αφορούν τα λογιστικά γεγονότα που έχουν άμεση επίπτωση στην χρηματοοικονομική θέση της επιχείρησης. Επιπροσθέτως, το μοντέλο συμπληρώνουν λειτουργίες οι οποίες πραγματοποιούνται σε καθημερινή βάση από την επιχείρηση (Hall, 2012, σελ. 25). Πιο συγκεκριμένα, η λήψη των παραγγελιών ή η ενημέρωση της αποθήκης, αποτελούν ένα δείγμα από τις καθημερινές αυτές δραστηριότητες. Επίσης, μέσα στις δυνατότητες του μοντέλου μπορεί να συγκαταλεχθεί και η δυνατότητα συγκράτησης μητρώου (Κεχρής, 2005, σελ. 29). Δεν θα ήταν σφάλμα να λεχθεί πως το μοντέλο αυτό είναι απαρχαιωμένο αποτελώντας πηγή προβλημάτων και ζημιών για την επιχείρηση (Hall, 2012, σελ. 25).

1.4.2. Μοντέλο Επίπεδων Αρχείων - Flat – file model

Με το πέρας του χρόνου δημιουργήθηκε ένα νέο μοντέλο το οποίο ονομάζεται μοντέλο των *επίπεδων αρχείων ή legacy systems.* Πρόκειται για ένα μοντέλο το οποίο πρωτοεμφανίσθηκε τέλη 60’ με αρχές 80’. Αναντίρρητα το μοντέλο θεωρείται παλαιό, παρ’ όλα αυτά όμως φαίνεται να είναι ιδιαίτερα διαδεδομένο στις επιχειρήσεις λόγω της λειτουργικότητας του. Ένα σημαντικό χαρακτηριστικό του μοντέλου τούτου είναι η “ατομικότητα” που επικρατεί ανάμεσα στα αρχεία, δηλαδή κάθε αρχείο δρα ως μοναδικό με αποτέλεσμα να υπάρχει ασυνδετότητα μεταξύ των αρχείων και των επιμέρους στοιχείων τους. Κατά συνέπεια, η “ατομικότητα” στα αρχεία αποτελεί εμπόδιο για τους τελικούς χρήστες, δεδομένου ότι δεν είναι εφικτή η είσοδος σε αρχεία των οποίων τα δικαιώματα ανήκουν σε κάποιον άλλον χρήστη (Bagranoff κ.α., 2010, σελ. 154; Hall, 2012, σελ.25). Γίνεται αντιληπτό πως υπάρχει μία τάση απομόνωσης των χρηστών η οποία ακολούθως επιφέρει προβλήματα στο σύστημα. Συνεχίζοντας, η περιοριστική στάση του μοντέλου δεν σταματά εδώ, καθώς δεν επιτρέπεται η αλόγιστη χρήση δεδομένων από την βάση, όπως επίσης, δεν είναι εφικτή η ταυτόχρονη χρήση από πολλούς χρήστες. Σύμφωνα με τους Stallings & Brown (2008, σελ. 141), τα δεδομένα αποθηκεύονται σε έναν πίνακα. Έτσι, μπορεί να ειπωθεί πως η δομή της βάσης δεδομένων αναγκάζει τους χρήστες να γνωρίζουν

πλήρως την φύση των πληροφορίων που χρειάζονται έτσι ώστε να επιδιώξουν στοχευμένη αναζήτηση έχοντας ως κριτήριο την επίλυση του προβλήματος που τους έχεις ανατεθεί. Για να γίνει ευκολότερα κατανοητή η λειτουργία του μοντέλου, απεικονίζεται στο παρακάτω γράφημα (Hall, 2012, σελ. 25).

Ειδικότερα, εμφανίζονται 2 (δύο) διαφορετικοί χρήστες οι οποίοι εισέρχονται σε διαφορετικές εφαρμογές, οι οποίες με την σειρά τους διαθέτουν διαφορετικά δεδομένα. Η έλλειψη σύνδεσης αποτελεί πηγή πολλών θεμάτων προς επίλυση. Αναλυτικότερα παραπάνω ειπώθηκε πως τα δεδομένα απαιτείται να πληρούν κάποιες προϋποθέσεις, μία εξ' αυτών είναι και αποφυγή των επαναλήψεων. Όμως σε αυτό το μοντέλο όπως είναι αναμενόμενο κάτι τέτοιο δεν μπορεί να συμβεί, καθώς προκειμένου να ικανοποιηθούν οι χρήστες απαιτείται η επανάληψη στα εισερχόμενα δεδομένα, δημιουργώντας διπλότυπες εγγραφές (Stallings & Brown, 2008, σελ. 141; Hall, 2012, σελ.25). Επόμενο πρόβλημα εμφανίζεται στην ενημέρωση των δεδομένων. Πιο συγκεκριμένα, η ασύνδετη δομή του μοντέλου αναγκάζει τους χρήστες σε ξεχωριστή ενημέρωση των δεδομένων, γεγονός το οποίο εξαλείφεται σε βάσεις δεδομένων οι οποίες διαθέτουν το χαρακτηριστικό της ολότητας. Συνεπώς, η καθυστέρηση στην ενημέρωση των δεδομένων επιδρά αρνητικά και στις πληροφορίες για τον λόγο ότι για την ενημέρωση τους χρειάζεται να ξεκινήσουν νέες εργασίες, όπως είναι ο επανασχεδιασμός της βάσης, δαπανώντας έτσι πολύτιμο χρόνο (Hall, 2012, σελ. 25; Stallings & Brown, 2008, σελ. 141). Έτσι, στα αρνητικά του έρχονται να προστεθούν και τα πρόσθετα έξοδα τα οποία προκύπτουν από τον μεγάλο όγκο δεδομένων. Κλείνοντας, ο λόγος για τον οποίο πρόκειται για ένα διαδεδομένο μοντέλο, είναι η ικανότητα του να προσδίδει αξία στον κάθε χρήστη, είτε αυτός είναι λογιστής, είτε προέρχεται από άλλο πόστο. Σε πολλούς από τους χρήστες τα εισερχόμενα λογιστικά δεδομένα μπορεί να φαίνονται ασήμαντα, παρ' όλα αυτά, έχουν το δικαίωμα του ελέγχου και της παρακολούθησης τους. Επιπλέον, ως αντιλαμβανόμενη προστιθέμενη αξία για αυτούς εκλαμβάνεται το δικαίωμα τους να επεξεργασθούν και να προσαρμόσουν τα δεδομένα στις ανάγκες τους (Hall, 2012, σελ. 27).



Σχήμα 4: Μοντέλο Βάσεως Δεδομένων.

Πηγή Hall, J. (2011). Accounting Information Systems 7e. U.S.A.: Cangage Learning, σελ. 27

1.4.3. Διαχείριση Βάσης Δεδομένων - The Database Model

Στην αντίπερα όχθη από το *μοντέλο επίπεδων αρχείων,* βρίσκεται *μοντέλο της σχεσιακής βάσης δεδομένων,* το οποίο δίνει περισσότερες ελευθερίες στον χρήστη (Bagranoff κ.α., 2010, σελ. 158).

Από την πρώτη στιγμή που υλοποιήθηκε το μοντέλο αυτό, διαφαίνεται πως οι δημιουργοί του μερίμνησαν για την ομαλή μετάβαση από το επίπεδο μοντέλο, σε αυτό, αποσκοπώντας έτσι στην εξομάλυνση της διαδικασίας, όπως επίσης και στην χρήση λιγότερων πόρων καθώς είναι απαραίτητοι για τις επιχειρήσεις. Βέβαια, οφείλει να ειπωθεί πως το μοντέλο στα πρώιμα στάδια δεν εμφάνιζε την ίδια αποτελεσματικότητα αναφορικά με το τωρινό μοντέλο, όπως ήταν αναμενόμενο, υπήρξαν βελτιώσεις. Ειδικότερα οι βελτιώσεις αυτές επήλθαν μέσα από την προσθήκη πινάκων εντός της βάσης δεδομένων για την επίτευξη δεσμών μεταξύ των δεδομένων της (Hall, 2012, σελ. 28).

Σκοπός του είναι η ενοποίηση και συγκέντρωση όλων των δεδομένων εντός μίας κοινής βάσης (Hall, 2012, σελ. 28), η οποία διαφέρει από το λογιστικό λογισμικό, έχοντας έτσι θετικό αντίκτυπο σε λειτουργίες όπως η προσθήκη δεδομένων ή η τροποποίηση τους (Bargranoff κ.α., 2011, σελ 158). Αρχικά για την είσοδο στην βάση και την χρήση των δεδομένων της αποτελεί μονόδρομο η αποστολή αιτήματος προς των διαχειριστή της βάσης δεδομένων, ο οποίος θα κληθεί να εξετάσει το αίτημα για να δώσει την έγκριση ή όχι. Ο διαχειριστής θα

λέγαμε ότι κατέχει εποπτικό ρόλο καθώς είναι αρμόδιος για την παροχή δικαιωμάτων στους χρήστες αλλά και την παρακολούθηση τους προκειμένου να καθίστανται ορθές οι λειτουργίες της βάσης. Επίσης, είναι αρμόδιος για τον εντοπισμό και την εξάλειψη ανεπιθύμητων ενεργειών οι οποίες υπάρχει ενδεχόμενο να προκύψουν, όταν κάποιος χρήστης επιδιώκει να δραστηριοποιηθεί εκτός των ορίων που του έχουν τεθεί (Hall, 2012, σελ. 28). Επιπλέον, σύμφωνα με τους Stalling & Brown (2008, σελ. 140) είναι απαραίτητη η ύπαρξη μηχανισμών ασφαλείας.

Συνεχίζοντας, η ύπαρξη μίας κοινής βάσης δεδομένων γεννά πολλά πλεονεκτήματα τα οποία προέρχονται από την σημαντική μείωση των επαναλήψεων, την ταχύτερη ενημέρωση των αποθηκευμένων αρχείων καθώς πλέον η διαδικασία είναι αυτοματοποιημένη αλλά και από την ταχύτερη αλλαγή χαρακτηριστικών μιας οντότητας, διότι από την στιγμή που τα νέα δεδομένα θα αποθηκευτούν, αυτομάτως είναι διαθέσιμα για χρήση. Τέλος, αξίζει να τονιστεί πως η ύπαρξη μιας σχεσιακής βάσης δεδομένων βελτιώνει την λειτουργία της επιχείρησης, όμως, δεν εξασφαλίζει απόλυτα την επίτευξη ολοκλήρωσης (Hall, 2012, σελ. 28).

1.4.4. The R.E.A. Model

Ερχόμαστε στο 1982, χρονολογία στην οποία εμφανίσθηκε ένα θεωρητικό μοντέλο του AIS, το λεγόμενο Π.Γ.Π., τα οποία αποτελούν ακρωνύμια από τους **π**όρους (resources), τα **γ**εγονότα (events) και τους **π**ράκτορες (agents) (Hall, 2012, σελ.28).

Ξεκινώντας, πρόκειται για ένα μοντέλο ιδιαίτερα φιλικό και εύχρηστο για τους χρήστες καθώς επιτρέπει την παρουσίαση των αποτελεσμάτων (Hall, 2012, σελ.28). Μάλιστα, έχει την ικανότητα να προβάλλει τις μεταβολές στα οικονομικά δεδομένα των οργανισμών (Weigand & Elsas, 2012). Η παρουσίαση κατέχει διττό ρόλο, από την μία βοηθάει τους υπόλοιπους χρήστες εντός του οργανισμού επειδή εισερχόμενοι στην *μία και μοναδική βάση* έχουν πρόσβαση σε όλα τα δεδομένα, χαρακτηριστικό το οποίο διαφοροποιεί το παρόν μοντέλο με τα προαναφερθέντα, ενώ από την άλλη μεριά υποβοηθά την χρήση λογιστικών δεδομένων τα οποία προέρχονται από την πραγματοποίηση διαφόρων συναλλαγών, γεγονός το οποίο έχει αντίκτυπο στο AIS.

Στο σημείο αυτό θα εντρυφήσουμε στα 3 (τρία) γρανάζια του μοντέλου αυτού, ξεκινώντας μάλιστα από την ακίνητη περιουσία της επιχείρησης ή διαφορετικά

τα στοιχεία του ενεργητικού της. Ακόμη καλύτερα, στην κατηγορία αυτή εντάσσεται οτιδήποτε ανήκει στον οργανισμό και μπορεί να συναλλαχθεί (Weigand & Elsas, 2012a). Τα παραπάνω αποτελούν τους λεγόμενους ***πόρους*** της επιχείρησης.

Συνεχίζοντας, ***τα οικονομικά γεγονότα*** αποτελούν το δεύτερο σημαντικό στοιχείο του μοντέλου. Αξίζει να αναφερθούμε στον ισχυρό δεσμό που επικρατεί αφενός με τους πόρους της επιχείρησης και αφετέρου με το σύνολο της λειτουργίας της. Μάλιστα, η παραδοχή αυτή αποδεικνύεται μέσω της ικανότητας τους προξενούν αλλαγές λόγω των δεδομένων που πραγματεύονται, τα οποία ενδέχεται να προέρχονται από μετρήσεις σχετικές με την παραγωγική δυναμικότητα ή τις πωλούμενες ποσότητες. Καταλαβαίνουμε ότι οι παραχθείσες πληροφορίες είναι επιτακτική ανάγκη να βρίσκονται εντός μίας ορθά δομημένης βάσης, η οποία μάλιστα εμπεριέχει και ένα ευρύ φάσμα πληροφοριών διαθέσιμο προς κάθε ενδιαφερόμενο (Hall, 2012, σελ. 29).

Προχωρώντας, το τρίπτυχο συμπληρώνεται με τους ***πράκτορες,*** οι οποίοι είναι ιδιαίτερα σημαντικοί αν αναλογιστεί κανείς πως ασκούν επιρροή τόσο *στους πόρους* της επιχείρησης, όσο και στα *οικονομικά γεγονότα*, στα οποία μάλιστα δύναται μερικές φορές να επιδρούν ως αυτόνομες μονάδες ή ως τμήματα αυτών (Hall, 2012, σελ. 29; Weigand & Elsas, 2012b).

Στο σημείο αυτό θα αναφερθούμε στις προϋποθέσεις που ορίζουν την ομαλή λειτουργία του μοντέλου ξεκινώντας από τα εισερχόμενα δεδομένα, πρόκειται για λογιστικά επιχειρησιακά δεδομένα τα οποία συνάδουν με τις απόψεις των χρηστών. Επιπλέον, απαιτείται η απουσία οποιασδήποτε τροποποίησης των δεδομένων, καθώς αυτή θα επιφέρει αλλαγές στο τελικό αποτέλεσμα, αυξάνοντας τις πιθανότητες για την δημιουργία σφαλμάτων και λανθασμένων εκτιμήσεων για οικονομικά γεγονότα τα οποία χρίζουν ιδιαίτερης σημασίας. Έτσι αποτελεί κοινή παραδοχή πως η δομή του ενδείκνυται προς μία προσαρμογή γύρω από τα διάφορα οικονομικά γεγονότα. Επίσης, αναφέρεται πως *η αμεσότητα και η ευελιξία* αποτελούν χαρακτηριστικά διαφοροποίησης από τις παραδοσιακές πρακτικές, διότι ο ενδιαφερόμενος οργανισμός κατέχει την ευχέρεια της σύνταξης σημαντικών οικονομικών καταστάσεων, αντλώντας πληροφορίες εισερχόμενος στην βάση (Hall, 2012, σελ. 30). Για την βέλτιστη κατανόηση του ΠΓΠ παρουσιάζεται στον παρακάτω πίνακα, όπου εμφανίζονται οι οντότητες μαζί με τα χαρακτηριστικά τους. Επιπρόσθετα, για κάθε οντότητα έχει δημιουργηθεί και ένας πίνακας στον οποία συνυπάρχει ένα χαρακτηριστικό που φέρει μία *μοναδική τιμή*, το λεγόμενο

πρωτεύον κλειδί. Προκειμένου να επικοινωνούν οι πίνακες μεταξύ τους, είναι απαραίτητο το πρωτεύον κλειδί του ενός πίνακα να εμφανισθεί στον πίνακα που μας ενδιαφέρει να επιτευχθεί επικοινωνία, αυτή τη φορά όμως έχει διαφορετική ιδιότητα, το μεταφερόμενο κλειδί ονομάζεται *ξένο κλειδί*. Βέβαια, ο δανεισμός του πρωτεύοντος κλειδιού δεν γίνεται στην τύχη, αντιθέτως καθορίζεται από τον *λόγο πολλαπλότητας* της σχέσης που υπάρχει μεταξύ των πινάκων, ο οποίος εμφανίζεται μέσω τριών μορφών. Πιο συγκεκριμένα, μπορεί να είναι "ένας προς ένα", "ένα προς πολλά" και "πολλά προς πολλά" (Κεχρής, 2014, σελ. 49). Αβίαστα καταλήγουμε στο συμπέρασμα πως η "επικοινωνία" μεταξύ των πινάκων αποτελεί καταλύτη για την λειτουργία του μοντέλου, χαρακτηριστικό που το διαφοροποιεί από τα κλασικά μοντέλα.

Πίνακας 1: Κλασσική Καταγραφή Δεδομένων (Non REA Database Model)

Αρχείο εισπρακτέων λογαριασμών		
Αριθμός πελάτη	Όνομα πελάτη	Διεύθυνση
23456	Smith	125 Elm St. City
Τιμολόγιο		
Αριθμός τιμολογίου	Ημερομηνία	Αριθμός πελάτη
98765	9/01/09	23456
Γραμμή προϊόντος		
Αριθμός	*Αριθμός*	Πωληθέντες
X21	98765	

Πηγή: **Hall, J. (2011). Accounting Information Systems 7e. U.S.A.: Cangage Learning, σελ.19.**

1.4.5. Enterprise Resource Planning

Η εξέλιξη των πληροφοριακών μοντέλων δεν σταμάτησε στο μοντέλο ΠΓΠ, αντιθέτως προχώρησε ένα νέο ικανότατο πληροφοριακό σύστημα, γνωστό και ως ERP. Τρανή απόδειξη αποτελεί η μετάβαση από τα παλαιά ασύνδετα μοντέλα, στα πιο σύγχρονα όπου η λειτουργία τους βασίσθηκε στην δημιουργία βάσεων, φθάνοντας έτσι σε ένα λογισμικό που ονομάζεται ERP. Η ικανότητα του να συντονίζει λειτουργίες βαρύνουσας σημασίας για την επιχείρηση το καθιστούν αυτομάτως ως ένα πολύ χρήσιμο εργαλείο. Μάλιστα, οι δυνατότητες τους ποικίλλουν, μερικές από τις οποίες είναι η ταχύτατη ροή πληροφοριών, η σύνδεση

των διαδικασιών της επιχείρησης, αλλά και η πολύτιμη βοήθεια του για δημιουργία και ισχυροποίηση των σχέσεων του οργανισμού με το εξωτερικό περιβάλλον του (Bagranoff κ.α., 2010, σελ. 5). Είναι γεγονός πως αποτελεί μία βάση δεδομένων που συνδυάζει πλήθος εφαρμογών, καθώς με την εγκατάσταση ενός ERP λογισμικού, ο οργανισμός αυτομάτως καταφέρνει να διαχειρίζεται το ανθρώπινο δυναμικό, τις σχέσεις με τους πελάτες του, όπως επίσης και την εφοδιαστική του αλυσίδα (Wallace, 2014, σελ. 283). Έτσι, εταιρίες όπως η SAP και η Oracle αποφάσισαν να δημιουργήσουν και να πωλούν τέτοιους είδους λογισμικά, αξίζει βέβαια να αναφερθεί και η ύπαρξη λογισμικών ανοιχτού κώδικα όπως το Dolibar, Opentaps κ.α. (Nesbitt, 2017). Επιπλέον, σημαντικό στοιχείο τους αποτελεί η προσαρμοστικότητα στις ανάγκες των οργανισμών καθώς αυτοσκοπός της δημιουργίας τους είναι η πλήρης ικανοποίηση των απαιτήσεων κάθε οργανισμού, μεγάλου ή μικρού (Wallace, 2014, σελ. 283). Φρόνιμο είναι να επιλεχθεί εκείνο το λογισμικό το οποίο αυτοματοποιεί πλήρως όλες τις διαδικασίες του οργανισμού, δεν θα ήταν σωστό να ειπωθεί πως πρόκειται για μια εύκολη απόφαση καθώς υπάρχει σοβαρό ενδεχόμενο αποτυχίας. Σημαντικό εμπόδιο αποτελεί η τυποποιημένη μορφή του λογισμικού, το οποίο μπορεί να ξεπεραστεί με την εγκατάσταση εφαρμογών και σύνδεση τους με το ERP, τα λεγόμενα bolts-on (Strategic Information Group, 2013). Τελειώνοντας αξίζει να αναφέρουμε πως πρόκειται για ένα ιδιαίτερα ακριβό λογισμικό το οποίο όμως εάν επιλεχθεί σύνεση είναι ικανό να προσδώσει σημαντικά οφέλη για τον οργανισμό (Hall, 2012, σελ. 31).

1.5. Δίαυλοι Επικοινωνίας και Μεταφοράς Δεδομένων

Στην ενότητα αυτή παρουσιάζονται οι διαθέσιμοι τρόποι μεταφοράς δεδομένων μέσα από τους διαύλους του τοπικού δικτύου ή ακόμη και μέσω των επιλογών που παρέχονται από το διαδίκτυο. Η μεταφορά τους επηρεάζεται από την φύση του μέσου που θα χρησιμοποιηθεί, όπως παραδείγματος χάριν, η μεταφορά με μικροκύματα είναι εφικτή υπό την χρήση του διαδικτύου, ενώ σε αντίθετη περίπτωση φαίνεται να μην ισχύει κάτι τέτοιο στα τοπικά δίκτυα. Όπως στην φυσική, έτσι και εδώ υπάρχουν διάφορες κλίμακες μέτρησης για τα διαφορετικά μέσα. Για παράδειγμα, προκειμένου να γίνει μετάφραση του ηλεκτρονικού μηνύματος σε μία γλώσσα γνωστή για τις τηλεπικοινωνίες, χρησιμοποιείται το modem, έχοντας ως κλίμακα μέτρησης το bps το οποίο παρουσιάζει τον ρυθμό μετάδοσης του μηνύματος. Επιπλέον, σε στιγμές όπου στην μετάδοση

δεδομένων ξεπερνιούνται τα 9 mb/s, εμφανίζεται το DSL. Πλέον, με την πάροδο των χρόνων και την εξέλιξη της τεχνολογίας, έχουν εμφανισθεί οι οπτικές ίνες στις οποίες οι ταχύτητες είναι τεράστιες. Συγκεκριμένα, η ταχύτητα μεταφοράς δεδομένων μπορεί να φτάσει και τα 2,2 δις bps/s γεγονός που καθιστά εύκολη την αποστολή δεδομένων σε πραγματικό χρόνο. Αφού πραγματοποιήθηκε μία μικρή εισαγωγή σχετικά με τις μεταφορές δεδομένων, είμαστε σε θέση να σχολιάσουμε τις διάφορες μορφές επικοινωνίας που είναι πιθανόν να εμφανισθούν εντός ενός οργανισμού (Bagranoff κ.α., 2010, σελ. 52-53).

1.5.1 Τοπικό Δίκτυο - Local Area Networks

Η σύνδεση LANs αποτελεί την δημοφιλέστερη σύνδεση δικτύου. Αφορά την μεταφορά δεδομένων σε επίπεδο τοπικού δικτύου. Η δομή του αποτελείται από έναν server στον οποίο είναι αποθηκευμένα τα αρχεία και τα λογισμικά. Δεν θα ήταν σφάλμα να ειπωθεί πως αποτελεί κυρίαρχο δίαυλο επικοινωνίας μεταξύ των υπολοίπων συσκευών του οργανισμού, όπως για παράδειγμα, του προσωπικούς υπολογιστές με τους εκτυπωτές (Bagranoff κ.α., 2010, 53-54). Γενικότερα, τέτοιου είδους σύνδεση χρησιμοποιείται κυρίως για την γρήγορη επικοινωνία μεταξύ των υπαλλήλων (Laudon & Laudon, 2011, σελ. 117).

Μερικά από τα πλεονεκτήματα του LANs είναι η ταυτόχρονη πρόσβαση σε αρχεία, στους εκτυπωτές και στο διαδίκτυο. Επιπλέον, το χαμηλό κόστος αγοράς του λογισμικού αποτελεί ένα δέλεαρ διότι ο οργανισμός μπορεί να έχει άριστα αποτελέσματα με χαμηλό κόστος, χωρίς μάλιστα να υπάρχει φόβος ασυμβατότητας καθώς με την δημιουργία νέας σύνδεσης LAN, αυτή λειτουργεί ως καταλύτης καλύπτοντας το χάσμα ανάμεσα στα διαφορετικά λογισμικά των υπολογιστών (Bagranoff κ.α., 2010, σελ. 54). Βέβαια, είναι απαραίτητη η καθοδήγηση του προσωπικού από ειδικούς, προκειμένου να είναι σε θέση να χρησιμοποιούν ορθά το LAN (Laudon & Laudon, 2011, σελ. 117).

1.5.2. Δίκτυο Ευρείας Περιοχής ή Ζώνης - Wide Area Networks

Στον αντίποδα, μία επιχείρηση η οποία δραστηριοποιείται σε παγκόσμιο επίπεδο προτιμάται να δημιουργεί WANs, καθώς επιτυγχάνεται συντονισμός των επιμέρους τμημάτων της. Η λειτουργία αυτής της σύνδεσης επιτυγχάνεται με την λειτουργία πολλαπλών καναλιών επικοινωνίας. Μάλιστα, συνηθίζεται πέρα από τα ιδιόκτητα κανάλια, να παρέχεται το έργο σε εξωτερικούς συνεργάτες. Όπως είναι αναμενόμενο, η μετάδοση των δεδομένων μπορεί να πραγματοποιηθεί και με

άλλους τρόπους πέρα του server, όπως είναι η τηλεφωνικό γραμμή, μικροκύματα ακόμη και την χρήση των δορυφόρων (Bagranoff κ.α., 2010, σελ. 54; Laudon & Laudon, 2011, σελ. 200). Σύμφωνα με τους Laudon & Laudon (2011, σελ. 200), το Internet αποτελεί την πιο δημοφιλή σύνδεση WANs. Συνήθως χρησιμοποιείται για την μεταφορά οικονομικών δεδομένων τα οποία μπορεί να είναι αποθηκευμένα σε κάποιον απομακρυσμένο server, παρ' όλα αυτά όμως είναι εφικτή η πολύπλευρη χρήση τους από τα χαμηλότερα έως και τα υψηλότερα κλιμάκια του οργανισμού (Bagranoff κ.α., 2010, σελ. 54).

1.5.3. Σύνδεση μέσω Server - Client/Server Computing

Συνεχίζοντας, το σύστημα αυτό είναι ιδιαίτερα αποτελεσματικό δεδομένου ότι συμβάλλει καταλυτικά για την υλοποίηση των επιχειρησιακών στόχων, καθώς μπορεί να δημιουργήσει γέφυρες με συνδέσεις από όλο τον κόσμο (Laudon & Laudon, 2011, σελ. 202).

Η δομή του συστήματος είναι απλή και μπορεί να γίνει εύκολα κατανοητή. Αρχικά, το λογισμικό είναι εγκατεστημένο σε έναν client ο οποίος επικοινωνεί με τον server στον οποίο είναι τοποθετημένα όλα τα αρχεία. Ο client με την σειρά του επικοινωνεί με το σύστημα των υπολογιστών στους οποίους διανέμονται τα δεδομένα καθώς επίσης και στο συνολικό σύστημα. Στο σημείο αυτό, αξίζει να τονιστούν δύο αυξημένης σημασίας χαρακτηριστικά του συστήματος. Πρώτα, αποτελεί ένα σύστημα το οποίο εμφανίζει υψηλό βαθμό προσβασιμότητας και κατά δεύτερον η επικοινωνία ανάμεσα στον client, στον server και τους υπολογιστές επικοινωνούν με αμφίδρομο τρόπο και έτσι ο οργανισμός επωφελείται από τα πλεονεκτήματα αυτού του τύπου επικοινωνίας. Εμβαθύνοντας ακόμη περισσότερο, το client computing απαρτίζεται από 3 (τρία) χαρακτηριστικά. Το πρώτο αφορά την προβαλλόμενη εικόνα στον χρήστη, δηλαδή ο βαθμός στον οποίο το «περιβάλλον» του υπολογιστή είναι ίδιο ή διαφορετικό από τον προσωπικό του υπολογιστή. Όπως γίνεται ευκόλως αντιληπτό, παραπάνω περιεγράφηκε το *στοιχείο της παρουσίασης*. Συνεχίζοντας, το δεύτερο στοιχείο σχετίζεται με την λογική ροή των διαδικασιών που ακολουθεί μία εφαρμογή. Αξίζει να ειπωθεί πως πλέον ο χρήστης είναι ικανός να εισέλθει στις αποθήκες δεδομένων και να προβεί σε επεξεργασίες και να πραγματοποιήσει συναλλαγές, ωστόσο, υπάρχει διαθέσιμη η επιλογή της παράθεσης ερωτήσεων στο σύστημα έτσι ώστε αυτό να του εξάγει τα απαιτούμενα δεδομένα από την βάση (Bagranoff κ.α., 2010, σελ. 55). Όμως, η μεταφορά δεδομένων εν μέσω client, έχει υψηλό

βαθμό επικινδυνότητας καθώς είναι πιθανόν, να χαθούν δεδομένα κατά την διάρκεια της μετάδοσης τους (Laudon & Laudon, 2011, σελ. 235). Κλείνοντας, το τελευταίο στοιχείο πραγματεύεται την διαχείριση των δεδομένων. Εδώ τίθενται θέματα ελέγχου και ασφαλείας για τα οποία πρέπει να μεριμνήσει ο οργανισμός. Αφορά τις βάσεις και τις αποθήκες δεδομένων οι οποίες μερικές φορές έχουν εγκατασταθεί σε μεγάλα συστήματα, τούτο συμβαίνει επειδή πολλές φορές δημιουργούνται αρκετές αντιγραφές της ίδιας βάσης δεδομένων προκειμένου να εξυπηρετούνται οι χρήστες με ταχύτερους ρυθμούς (Bagranoff κ.α., 2010, σελ. 56).

1.5.4. Εναλλακτική Τεχνολογία - Alternative Technology Mainframe

Σύμφωνα με τους Ebbers et. al. (2006) το σύστημα αυτό είναι πολύ ικανό διότι μπορεί να κάνει πολλά πράγματα ταυτόχρονα χωρίς να παρουσιάζονται προβλήματα. Ειδικότερα, είναι εφικτό να διαχειρίζονται πλήθος εφαρμογών ενώ ταυτόχρονα εξυπηρετούν χιλιάδες χρήστες. Επίσης, στις ικανότητες αυτού του τύπου συστήματος προστίθεται και σχεδόν άριστη μεταφορά δεδομένων χωρίς την δημιουργία του παραμικρού προβλήματος, τόσο για τους χρήστες, όσο κι για την ασφάλεια του συστήματος.

1.5.5. Ασύρματο Δίκτυο - Wireless & Data Communications

Η σύνδεση με wi-fi αποτελεί πλέον καθημερινή συνήθεια για τους περισσότερους ανθρώπους οι οποίοι συνδέονται στο διαδίκτυο από το κινητό ή τον προσωπικό τους υπολογιστή εκμεταλλευόμενοι την ικανότητα του wi-fi να μεταφέρει δεδομένα και ηχητικά μηνύματα υψηλής ποιότητας. Επίσης, αυξάνονται και οι επιχειρήσεις που χρησιμοποιούν PDA για την βελτιστοποίηση της διαδικασίας της λήψης παραγγελιών. Γενικότερα, το κλίμα είναι ιδιαίτερα θετικό για τις συσκευές wi-fi καθώς αποτελούν ένα ισχυρό χαρτί για τους οργανισμούς σε περίπτωση που χρησιμοποιούν ορθά. Ειδικότερα, οι λογιστές επωφελούνται από την δημιουργία γεφυρών επικοινωνίας με τους συνεργάτες, τους εργαζόμενους και με το γενικό επιχειρησιακό δίκτυο, σύμφωνα με τις οποίες διευθετούνται ταχύτερα οι οικονομικές συναλλαγές, όπως η πληρωμή του προσωπικού (Bagranoff κ.α., 2010, σελ. 57). Στο σημείο αυτό μπορεί να ειπωθεί πως η ταχύτατη εξέλιξη των χρηστών καθώς και των συσκευών με ικανότητα εισόδου στο Internet, βοήθησαν την ασύρματη σύνδεση να αποτελεί σημαντικό εργαλείο για τους οργανισμούς (Park κ.α., 2016), στον αντίποδα όμως σύμφωνα με τους Nejad κ.α. (2017), τα wifi δίκτυα δεν είναι πλήρως αξιόπιστα για την μεταφορά δεδομένων.

Επιπλέον, μέσω του ασύρματου δικτύου είναι εφικτή η σύνδεση με δίκτυα LAN και WAN, υπό την προϋπόθεση ότι οι συσκευές διαθέτουν WAP (Bagranoff, 2011, σελ. 57). Σύμφωνα με την βιβλιογραφία, το RFID και NFC αποτελούν δύο πολύ σημαντικούς τύπους ασύρματης επικοινωνίας, των οποίων η κύρια διαφορά έγκειται στον τρόπο χρήση τους. Ειδικότερα, το RFID εξυπηρετεί κυρίως τους οργανισμούς για την βέλτιστη οργάνωση της εφοδιαστικής αλυσίδας (Laudon & Laudon, 2011, σελ. 222) ενώ το NFC τους ανθρώπους ως άτομα. Κλείνοντας την παρούσα ενότητα, για να επιτευχθεί σύνδεση με NFC είναι απαραίτητο να υπάρχει NFC chip ανάμεσα στις συσκευές που θέλουν να επικοινωνήσουν (Bagranoff κ.α., 2010, σελ. 57).

1.5.6. Υπολογιστικό Νέφος - Cloud Systems

Αποτελεί ένα ιδιαίτερα αναπτυσσόμενο σύστημα σύνδεσης εντός της επιχείρησης. Αφορά μία νεωτεριστική μέθοδο σύνδεσης κατά την οποία αυξάνεται ο βαθμός προσβασιμότητας των ενδιαφερόμενων μελών καθώς η σύνδεση επιτυγχάνεται μέσω ενός "cloud" το οποίο επικοινωνεί άμεσα με όλους τους χρήστες (Bagranoff κ.α., 2010, σελ. 59), παρ' όλα αυτά η έκθεση των δεδομένων στον διαδίκτυο έχει θέσει την ασφάλεια ως επιτακτική ανάγκη (Moeti & Sigama, 2015).

Σύνηθες είναι το φαινόμενο του εξωπορισμού, με τις επιχειρήσεις να αναθέτουν σε τρίτους την παροχή των υπηρεσιών clouding. Η παραπάνω δυνατότητα δεν θα ήταν σφάλμα να χαρακτηρισθεί ως ισχυρό πλεονέκτημα για τον οργανισμό που κάνει outsourcing, συμπέρασμα που αποδίδεται στις μειώσεις χρόνου, εμποδίων και κόστους επειδή η πρόσβαση καθίσταται εύκολη ακόμη και στον μικρότερο και πιο απομακρυσμένο πελάτη του οργανισμού, σε πραγματικό χρόνο (Dhar, 2012). Για παράδειγμα, ο Dhar (2012a) η μείωση του κόστους προκύπτει από την μη δαπάνη μεγάλων χρηματικών ποσών για την αγορά ειδικού εξοπλισμού για την εφαρμογή του clouding. Επιπλέον, στους πελάτες χρεώνονται μόνο οι παρεχόμενες υπηρεσίες επιφέροντας κέρδη και για τις δύο συνεργαζόμενες πλευρές, διότι αναπτύσσονται σχέσεις πλήρους διαφάνειας. Επιπρόσθετα, προκύπτουν και λειτουργικά οφέλη από την αποφυγή υπερφορτώσεων του συστήματος αλλά και από την πιθανότητα να επιτευχθούν υψηλότερα επίπεδα ελέγχου με την αποθήκευση αντίγραφων ασφαλείας με την μορφή offsite backup τα οποίο σύμφωνα με τον κύριο Stone (2016) προστατεύει τα δεδομένα από τις απειλές του επιχειρησιακού περιβάλλοντος.

Στον αντίποδα, η χρήση του cloud κρύβει και κάποια μειονεκτήματα. Σημαντικότερο όλων είναι η πολυπλοκότητα και η δυσκολία διασφάλισης της ακεραιότητας, της εμπιστευτικότητας και της προσβασιμότητας, διότι απαιτεί ιδιαίτερη μεταχείριση (Arjun & Vinay, 2016). Ειδικότερα, δεν εγγυάται σε απόλυτο ποσοστό την επιτυχία της αποστολής του, με συνέπεια να αποδειχθεί ένα δαπανηρό project. Επίσης, η παροχή δεδομένων σε τρίτους απαιτεί την σύναψη ισχυρών σχέσεων εμπιστοσύνης, σε τέτοιο βαθμό που θα είναι εφικτό να παρέχονται υψηλής αξίας. Τέλος, η εγκατάσταση του απαιτεί επένδυση σε υλικοτεχνικά μέσα για την αποθήκευση δεδομένων αλλά και ταχύτατη ενημέρωση των αρχείων που θα προβάλλονται στους τελικούς χρήστες (Bagranoff κ.α., 2010, σελ. 59).

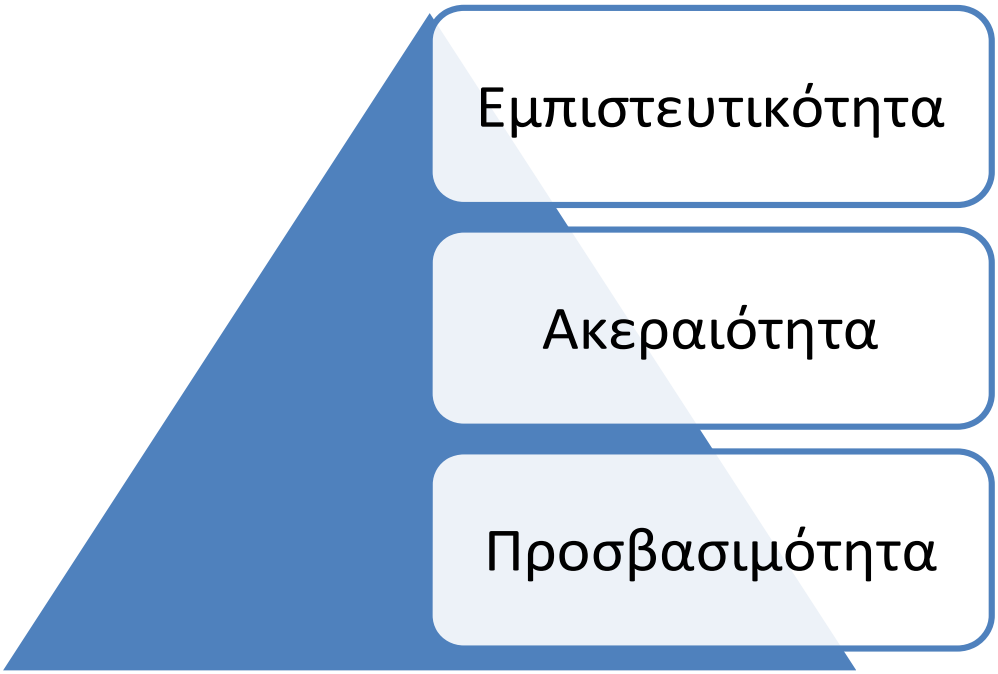
1.6. Οι Πυλώνες της Πληροφορίας – C.I.A. Triad

Αποτελεί γενική αλήθεια πως η πληροφορία αποτελεί σημαντικό πυλώνα για την λήψη αποφάσεων, έτσι κρίνεται ζωτικής σημασίας η διατήρηση της ασφάλειας του περιεχομένου της. Η σημασία τους καθώς και η ασφάλεια τους δεν είναι κάτι γενικό και αόριστο αλλά αποτελείται από τρεις βασικούς πυλώνες των οποίων η προστασία πρέπει να αποτελεί τον πρωταρχικό σκοπό κάθε σχεδίου ασφαλείας. Ειδικότερα, στην βιβλιογραφία οι τρεις πυλώνες είναι η εμπιστευτικότητα (confidentiality) ή ιδιωτικότητα (privacy), η ακεραιότητα (integrity) και η διαθεσιμότητα (availability) (Merkow & Breithaupt, 2014, σελ. 20). Ο Wheeler (2011, σελ. 10) στα παραπάνω στοιχεία προσθέτει και την υπευθυνότητα (accountability).

Στο σημείο αυτό θα ειπωθεί η σημασία των τεσσάρων στοιχείων. Αρχικά, ως εμπιστευτικότητα της πληροφορίας εννοείται ο υψηλός βαθμός βεβαιότητας ότι δεν θα υπάρξει διαρροή της σε τρίτα άτομα, διαδικασίες ή και συσκευές. Τα πιο συχνά εφαρμοζόμενα μέτρα πρόληψης είναι η κάρτα ταυτοποίησης ID και η χρήση κωδικών πρόσβασης. Προχωρώντας παρακάτω, μία πληροφορία λέμε ότι διακατέχεται από ακεραιότητα όταν δεν έχει υποστεί τροποποιήσεις και επεξεργασία από άτομα χωρίς εξουσιοδότηση. Έτσι, τα μέτρα διασφάλισης της ακεραιότητας πρέπει να είναι προσανατολισμένα ως προς αυτόν τον σκοπό.

Συνεχίζοντας, η διαθεσιμότητα αναφέρεται στην εύκολη πρόσβαση των

ενδιαφερόμενων χρηστών στα δεδομένα τα οποία επιθυμούν χωρίς χρονοτριβές. Τέλος, η υπευθυνότητα αναφέρεται στην σωστή καταγραφή και παρακολούθηση των γεγονότων – συναλλαγών σε μία αξιόπιστη πηγή έτσι ώστε να αποτελούν ορθολογικές πληροφορίες, κατάλληλες προς αξιοποίηση (Wheeler, 2011, σελ.10).



Σχήμα 5: Οι πυλώνες της πληροφορίας (CIA TRIAD)

Πηγή: Merkow S., M. & Breithaupt, J. (2014). *Information Security: Principles and Practices, 2nd Edition*. United States of America: Pearson Education, Inc.

1.7. Περιουσιακά Στοιχεία – Assets

Σύμφωνα με τον Landoll (2006, σελ. 31) , ως περιουσιακά στοιχεία λογίζονται τα στοιχεία εκείνα τα οποία έχουν αξία για τον οργανισμό, όπως είναι για παράδειγμα οι πόροι και τα δεδομένα του οργανισμού. Πρακτικά, οι οργανισμοί λαμβάνουν μέτρα ασφαλείας προκειμένου να διασφαλίσουν τα περιουσιακά τους στοιχεία (Landoll, 2006, σελ. 30).

Συνεχίζοντας, τα περιουσιακά στοιχεία διαχωρίζονται σε δύο κατηγορίες, σε απτά περιουσιακά στοιχεία (tangible assets) και στα άυλα περιουσιακά στοιχεία (intangible assets). Στα πρώτα συγκαταλέγονται, ο εξοπλισμός, τα κτήρια, οι υπολογιστές καθώς και οι υπάλληλοι του οργανισμού. Σύμφωνα με τους (Muhrtala & Ogundeji, 2013) οι υπάλληλοι αποτελούν το πιο σημαντικό περιουσιακό στοιχείο για το κάθε οργανισμό. Από την άλλη πλευρά, άυλα περιουσιακά

στοιχεία αποτελούν οι λογιστικές καταστάσεις καθώς επίσης και η πληροφορία, η οποία μάλιστα, σύμφωνα με τον Abu-Musa (2006), αποτελεί το περιουσιακό στοιχείο με την ύψιστη αξία για έναν οργανισμό. Έτσι, η εκάστοτε επιχείρηση υποχρεούται να διασφαλίσει το τρίπτυχο CIA που αναφέρθηκε.

Κεφάλαιο 2

Απειλές & Κίνδυνοι στα Λογιστικά Πληροφοριακά Συστήματα

2.1. Απειλές - Threats

Ξεκινώντας, στην παρούσα ενότητα πραγματοποιείται αναφορά σε έναν επιχειρησιακό τομέα ο οποίος είναι ιδιαίτερα σημαντικός, σε βαθμό τέτοιο που η παραβίαση του μπορεί να επιφέρει μεγάλες ζημίες για τον οργανισμό. Ο τομέας αυτός αφορά την ασφάλεια των πληροφοριών. Είναι απαραίτητη η υλοποίηση ενός περιεκτικού προγράμματος ασφάλειας γνωρίζοντας πως η πληροφορία είναι πολύτιμη (Abu-Musa, 2004).

Προτού όμως η επιχείρηση ξεκινήσει την υλοποίηση σχεδίου ασφαλείας, οφείλει να γνωρίσει τις απειλές που ελλοχεύουν στα περιβάλλοντα δραστηριοποίησης της. Αρχικά, η μορφή των απειλών διαφέρει. Ειδικότερα αυτές διαχωρίζονται σε φυσικές ή πολιτικές καταστροφές (natural & physical disasters), σε προβλήματα λογισμικού & εξοπλισμού (software errors & equipment malfunctions) και σε τυχαίες ενέργειες (unintentional acts) ή σκόπιμες ενέργειες (intentional acts) για την πρόκληση βλάβης στο σύστημα (Romney & Steinbart, 2003, σελ. 191).

2.1.1. Φυσικές Καταστροφές

Αναλυτικότερα, στην βιβλιογραφία ως *φυσικές καταστροφές* εννοούνται αυτές οι οποίες προκύπτουν από «ενέργειες Του Θεού», δηλαδή διάφοροι σεισμοί, πλημμύρες, δυνατοί άνεμοι, όπως και υψηλές θερμοκρασίες (Stallings & Brown, σελ. 481; Hawker, 2000, σελ. 51). Πράγματι, το 1993 στην Iowa καταστράφηκαν μονάδες υπολογιστών πολλών επιχειρήσεων λόγω της πλημμύρας που προέκυψε από την συνεχόμενη βροχόπτωση και την υπερχείλιση των ποταμών του Mississippi και του Missouri (Romney & Steinbart, 2003, σελ. 190).

2.1.2. Σφάλματα Λογισμικών & Δυσλειτουργίες Εξοπλισμού

Εν συνεχεία, στην κατηγορία αυτή περιλαμβάνονται οι διακοπές ή διακυμάνσεις του ηλεκτρικού ρεύματος, όπως επίσης και σφάλματα στο λειτουργικό σύστημα του

οργανισμού (Romney & Steinbart, 2003, σελ. 191). Η εμφάνιση των σφαλμάτων αυτών προξενεί μεγάλες ζημίες και προκαλείται κυρίως λόγω της *έλλειψης υποδομών* (Landoll, 2006, σελ. 33). Μάλιστα, στην Καλιφόρνια, οι υπεύθυνοι για την συλλογή των φόρων εισήγαγαν ένα νέο λογιστικό σύστημα το οποίο όμως παρουσίασε διάφορα κολλήματα (bugs), εξαιτίας τους συλλέχθηκαν $635 εκ. λιγότερα (Romney & Steinbart, 2003, σελ. 191).

2.1.3. Ενέργειες Χωρίς Πρόθεση

Στην κατηγορία αυτή ανήκουν *σφάλματα και παραλείψεις* κατά την εγγραφή (Landoll, 2006, σελ. 31) ή επεξεργασία (Romney & Steinbart, 2003, σελ. 192) των δεδομένων από τους χρήστες. Όπως είναι φυσικό τα κενά που θα προκύψουν απειλούν την *ακεραιότητα* και την *σταθερότητα* του συστήματος (Landoll, 2006, σελ. 32). Πηγή των σφαλμάτων αυτών αποτελεί η ανθρώπινη φύση. Συνηθίζονται λάθη από απροσεξία ή αδιαφορία από τους υπαλλήλους τα οποία έχουν ζημιώσει οργανισμούς με πολλά εκατομμύρια. Χαρακτηριστικό παράδειγμα αποτελεί ο λανθασμένος υπολογισμός μερισμάτων από έναν υπάλληλο της Giant Food, Inc. ο οποίος ανάγκασε τον οργανισμό να πληρώσει $10 εκατομμύρια δολάρια σε μερίσματα (Romney & Steinbart, 2003, σελ. 192).

2.1.4. Εμπρόθετες Ενέργειες & Απειλές

Συνεχίζοντας, *η απάτη και η κλοπή* αφορούν την άμεση ή έμμεση επίθεση για την κλοπή δεδομένων υψίστης ασφαλείας (Landoll, 2006, σελ. 32; Michalache, 2011). Στις Ηνωμένες Πολιτείες υπολογίζεται πως χάνονται $500 δις μέσω της απάτης. Σύμφωνα με τους Romney και Steinbart (2003, σελ. 277) η απάτη από το εσωτερικό του οργανισμού (internal fraud) χωρίζεται σε δύο κατηγορίες. Στην πρώτη κατηγορία εντάσσεται υπεξαίρεση των περιουσιακών στοιχείων (misappropriation of assets) ή η απάτη που προκαλείται από τους ίδιους τους εργαζόμενους (employee fraud). Η επίθεση στον οργανισμό μπορεί να γίνει από έναν υπάλληλο του ίδιου του οργανισμού αλλά και από κάποιον εξωτερικό συνεργάτη, όμως, οι πιθανότητες για ένα υπάλληλο είναι σαφώς αυξημένες, για τον λόγο ότι, οι υπάλληλοι γνωρίζουν τα πρωτόκολλα ασφαλείας και τις αδυναμίες του συστήματος (Romney & Steinbart, σελ. 277). Παλαιότερα ένας πρώην προγραμματιστής της HSBC επιχείρηση να κλέψει πληροφορίες για τους πελάτες της τράπεζας, ο οποίος σκόπευε να τις πουλήσει μεταγενέστερα (Wallace, 2014, σελ. 536). Η δεύτερη κατηγορία αφορά τις αναλήθειες στις χρηματοοικονομικές καταστάσεις του

οργανισμού (fraudulent financial reporting)**.** Κύριος στόχος των σφαλμάτων αυτών είναι η εξαπάτηση των μετόχων ή των δανειστών προκειμένου να ανέβει η τιμή της μετοχής του οργανισμού. Εν κατακλείδι, κάποιος οδηγείται στην εξαπάτηση για να αποκομίσει προσωπικό όφελος, είτε αυτό παίρνει οικονομικό χαρακτήρα ή την άνοδο στα διοικητικά κλιμάκια (Romney & Steinbart, 2003, σελ. 277).

2.1.5. Απειλές Ηλεκτρονικού Χαρακτήρα

Σε αυτήν την κατηγορία εντάσσονται οι μεθοδευμένες προσπάθειες για πρόσβαση, τροποποίηση (Romney, & Steinbart, 2003, σελ. 282) *και καταστροφή δεδομένων ή σαμποτάζ στον εξοπλισμό* του οργανισμού αλλά και των εγκαταστάσεων γενικότερα (Landoll, 2006, σελ. 33), όπως επίσης και την αθέμιτη εκμετάλλευση των τεχνικών πόρων του οργανισμού για την διάπραξη εγκλημάτων (Romney & Steinbart, 2003, σελ. 283).

Η πληροφορία είναι ένα περιουσιακό στοιχείο (asset) με τεράστια αξία, γεγονός που οδηγεί κυβερνήσεις και ανταγωνιστές στην *χρήση μεθόδων κατασκοπείας* αποσκοπώντας στην απόκτηση της (Landoll, 2006, σελ. 33). Μάλιστα, η οικονομική κατασκοπεία πρόκειται για έναν τύπο εξαπάτησης ο οποίος φαίνεται να αυξάνεται με ταχύτατους ρυθμούς (Romney & Steinbart, 2003, σελ. 284). Οι τεχνικές για την είσοδο στο σύστημα των υπολογιστών ποικίλλουν. Είναι πολύ πιθανό το σύστημα να τεθεί υπό κίνδυνο εξαιτίας απειλών με «ηλεκτρονικό χαρακτήρα» (Michalache, 2011), οι οποίες συνήθως πηγάζουν από εξωτερικές πηγές μολύνοντας το σύστημα.

Συγκεκριμένα, πρόκειται για *κακόβουλα λογισμικά* τα οποία καταστρέφουν ή καταγράφουν αρχεία. Τα λογισμικά αυτά εισέρχονται στο σύστημα με διάφορους τρόπους. Ειδικότερα, η είσοδος στο σύστημα μπορεί να επέλθει με την χρήση ενός απλού ιού, με ένα λογισμικό παρακολούθησης (spyware) ή ακόμη και με έναν δούρειο ίππο (trojan horse). Επίσης, με την χρήση λογισμικού keylogger καταγράφεται οτιδήποτε πληκτρολογεί ο χρήστης θέτοντας σε κίνδυνο τους κωδικούς ασφαλείας του συστήματος Συνηθίζεται οι hackers να επιδιώκουν την υποκλοπή των κωδικών πρόσβασης προκειμένου να εισέλθουν σε χρήσιμους πόρους του οργανισμού, όπως είναι τα αρχεία (Romney & Steinbart, 2003, σελ. 292; Wallace, 2014, σελ. 350). Οι κωδικοί είναι εύκολο να πέσουν στα χέρια αγνώστων, όταν αυτοί χρησιμοποιήσουν bots τα οποία μπορούν να καταγράψουν προσωπικές πληροφορίες και κωδικούς. Επιπλέον, ευθύνονται για το λεγόμενο spamming, κατά το οποίο αποστέλλονται τεράστιος όγκος e-mail (Stallings & Brown, 2012, σελ. 199) στον χρήστη, κάνοντας τον e-mail server να δυσλειτουργεί

(Romney & Steinbart, 2003, σελ. 292).

Η είσοδος στο εταιρικό σύστημα συνηθίζεται να πραγματοποιείται και με την χρήση *σκουληκιών* (worms) για την αντιγραφή και αποστολή σημαντικών αρχείων από την σκληρό δίσκο του χρήστη (Wallace, 2014, σελ. 350). Μάλιστα, μέσα στο σκουλήκι μπορεί να υπάρχει μια *λογική βόμβα* (Boyce & Jennings, 2002, σελ. 207) η οποία αποτελεί ένα πρόγραμμα το οποίο εφ' όσον ενεργοποιηθεί εγκαθιστά μολυσμένες εντολές (Champlain, 2003, σελ. 307) απειλώντας με καταστροφή σημαντικά αρχεία του συστήματος ή ακόμη και το ίδιο το σύστημα (Romney & Steinbart, 2003, σελ. 290). Τέλος, είναι σημαντικό να ειπωθεί η τεχνική του cracking (Romney & Steinbart, 2003, σελ. 287) η οποία παραβιάζει την *ιδιωτικότητα της πληροφορίας* (Landoll, 2006, σελ. 32). Αυτή προκύπτει όταν κάποιος χρήστης εισέρχεται σε δεδομένα για τα οποία δεν έχει δικαίωμα (Romney & Steinbart, 2003, σελ. 287). Αποτελεί ένα ιδιαίτερο θέμα προς επίλυση καθώς αυτομάτως κινδυνεύει να χαθεί η εμπιστευτικότητα (confidentiality) των πληροφοριών, η οποία αποτελεί ένα από τα τρία θεμελιώδη στοιχεία από τα οποία **πρέπει** να διακατέχεται η πληροφορία (Landoll, 2006, σελ. 32). Επιπλέον, συχνές τεχνικές επιθέσεων αποτελεί το clickjacking και malvertising, τα οποία έχουν πολλά κοινά στοιχεία. Ειδικότερα, οδηγούν τον τελικό χρήστη σε δράση (click) προκειμένου να ενεργοποιήσει κάποιον ιό (malware) ο οποίος θα εισβάλει στο σύστημα (Wong-Steele, 2017, σελ. 39). Παράλληλα, είναι πιθανόν οι hackers να επιχειρούν επιθέσεις spoofing οι οποίες στέλνουν στον χρήστη διάφορα παράνομα δεδομένα τα οποία έχουν ιούς, ενώ η πηγή των επιτιθέμενων είναι άγνωστη. Επιπλέον, οι spoofing επιθέσεις μπορεί να έχουν ως στόχο συστήματα GPS, προκειμένου να επηρεάσουν τα δεδομένα που μεταφέρονται (Fan κ.α., 2015).

Συνεχίζοντας, μία επιπλέον απειλή για τον οργανισμό και κυρίως για τους προσωπικούς υπολογιστές, είναι η επίθεση DoS (denial of service) η οποία αποτρέπει τον νόμιμο χρήστη από την είσοδο του σε αρχεία και υπηρεσίες (McDowell, 2009). Η επίθεση αυτή πραγματοποιείται με την αποστολή e-mail bombs τα οποία προξενούν προβλήματα στους servers, μάλιστα υπάρχουν πολλές πιθανότητες, οι servers να υπερφορτωθούν τόσο ώστε να απενεργοποιηθούν (Romney & Steinbart, 2003, σελ. 291). Επίσης, κίνδυνοι υπερφόρτωσης υφίστανται και για το όλο σύστημα μιας και είναι δύσκολο να διαχειρισθεί τον τεράστιο όγκο πληροφοριών που δέχεται το δίκτυο ή ο web server, με αποτέλεσμα να δυσχεραίνεται η λειτουργία του (Romney & Steinbart, 2003, σελ. 292). Σύμφωνα με έρευνα που πραγματοποιήθηκε το 2010 από την SCI Computer Crime Security, το 17% των ερωτηθέντων δήλωσε πως έχει αντιμετωπίσει επιθέσεις

DoS. Μάλιστα, είναι σημαντικό να αναφερθεί πως αυτές οι επιθέσεις συγκαταλέγονται στις 5 πιο ζημιογόνες από άποψη κόστους (Stallings & Brown, 2012, σελ. 221). Η παραπάνω παραδοχή γίνεται αντιληπτό ότι ισχύει αν αναλογιστούμε την ζημιά που προκάλεσε η επίθεση Syn – flood, η οποία έκλεισε 3.000 ιστοσελίδες για 40 ώρες, σε μία περίοδο της οποία η ζήτηση ήταν ιδιαίτερα υψηλή (Romney & Steinbart, 2003, σελ. 292). Τέλος, στην βιβλιογραφία προστίθενται οι επιθέσεις DDoS (distributed denial of service) σύμφωνα με την οποία ο επιτιθέμενος στον οργανισμό χρησιμοποιεί ένα σύμπλεγμα υπολογιστών, ακόμη και υπολογιστή της ίδιας της εταιρίας προκειμένου να επιτεθεί με DoS (McDowell, 2009).

2.2. Εισβολείς – Threat Agents

Στην ενότητα αυτοί θα αναλύσουμε τους παράγοντες εκείνους που τις πληροφορίες του οργανισμού. Αρχικά, όπως φαίνεται παρακάτω, οι απειλές προέρχονται από τον *ανθρώπινο παράγοντα ή από φυσικά φαινόμενα* (Wallace, 2014, σελ. 529). Η λίστα με τους εισβολείς ξεκινάει από την ίδια την *φύση* της οποίας οι δυνάμεις προκαλούν διάφορες φυσικές καταστροφές οι οποίες είναι επιβλαβείς για τους οργανισμούς. Εν συνεχεία, οι ίδιοι *οι υπάλληλοι, οι προμηθευτές καθώς και οι καταναλωτές* αποτελούν πηγή κινδύνου για τις εκάστοτε επιχειρήσεις (Michalache, 2011). Για του λόγου το αληθές, υπάρχει το ενδεχόμενο οι ίδιοι να κάνουν λανθασμένη εγγραφή ή να απατήσουν τον οργανισμό με πρόθεση. Επιπλέον, *οι hackers* εκμεταλλεύονται την σύνδεση των οργανισμών με το διαδικτυακό χώρο, γεγονός το οποίο καθιστά την ασφάλεια της δυσκολότερη με αποτέλεσμα να αυξάνονται τα τρωτά σημεία της και να είναι εκτεθειμένη. Τέλος, η επιδίωξη δημιουργίας συγκριτικού πλεονεκτήματος, ωθεί τις κυβερνήσεις και τις βιομηχανίες σε *κατασκοπεία* των αντιπάλων τους με αποστολή την υποκλοπή σημαντικών δεδομένων ή την δημιουργία προβλημάτων (Landoll, 2006, σελ. 31 – 32).

2.3. Τρωτά Σημεία - Vulnerabilities

Ως τρωτά σημεία η βιβλιογραφία αναφέρει τα κενά που εμφανίζονται στην αμυντική δομή ενός οργανισμού, δίνοντας έτσι την ευκαιρία σε χρήστες δίχως δικαιώματα να εισβάλλουν παράνομα στο σύστημα του οργανισμού (Landoll, 2006, σελ. 34). Ωστόσο, τα τρωτά σημεία μπορούν να χρησιμοποιηθούν και ως μέτρο αποτελεσματικότητας της ασφάλειας (Wallace, 2014, σελ. 534). Για αυτόν τον λόγο η αναγνώριση των τρωτών σημείων αποτελεί θεμελιώδης στοιχείο καθώς έτσι το επίπεδο του ρίσκου μειώνεται

σημαντικά.

Τα τρωτά σημεία χωρίζονται σε τρεις κατηγορίες, σε τρωτά σημεία διαχείρισης, φυσικά και τεχνικού πεδίου (Landoll, 2006, σελ. 34). Πρώτού όμως προχωρήσουμε στην ανάλυση τους θα επισημάνουμε την χρήση του «πίνακα κινδύνου» ο οποίος χρησιμοποιείται από τους μάνατζερς για την καταγραφή των τρωτών σημείων στα διάφορα επίπεδα κινδύνου (Wallace, 2014, σελ. 535).

2.3.1. Αδυναμίες Διαχείρισης

Πρόκειται για ελλείψεις και ασάφειες αναφορικά με τις διαδικασίες και τις πολιτικές γύρω από την ασφάλεια των πληροφοριών (Landoll, 2006, σελ. 34). Για την κάλυψη αυτών των κενών, οι οργανισμοί ακολουθούν πρωτόκολλα ασφαλείας (Wallace, 2014, σελ. 536).

2.3.2. Φυσικές Αδυναμίες

Οι φυσικές αδυναμίες είναι οι ελλείψεις και τα κενά σε απτά στοιχεία της αμυντικής δομής της επιχείρησης, όπως είναι για παράδειγμα η ύπαρξη ελαττωματικού φράχτη ή η έλλειψη εφεδρικών πηγών ενέργειας (Landoll, 2006, σελ. 34).

2.3.3. Τεχνικές Αδυναμίες

Τέτοιου είδους αδυναμίες εμφανίζονται κυρίως σε τεχνικά μέρη κάτι το οποίο φαίνεται και από την ονομασία άλλωστε. Τέτοιες είναι τα σφάλματα στου ελέγχους ασφαλείας, όπως για παράδειγμα στην χρήση ενός αδύναμου κωδικού πρόσβασης (Landoll, 2006, σελ. 34).

Κλείνοντας την ενότητα των τρωτών σημείων θα επισημάνουμε πως η έκθεση των οργανισμών στο διαδίκτυο δημιούργησε νέα τρωτά σημεία για αυτούς. Πιο συγκεκριμένα, σύμφωνα με τους Laudon & Laudon (2011, σελ. 236) οι συνδέσεις DSL που υπάρχουν στους οργανισμούς αποτελούν εύκολη λεία για τους hackers. Επίσης, τα e-mail μπορούν να αποτελέσουν πηγή κινδύνου, καθώς είναι πιθανό ένα e-mail με ευαίσθητα δεδομένα να αποσταλεί λανθασμένα με αποτέλεσμα να παραβιασθεί το περιεχόμενο του, ενώ κίνδυνοι υπάρχουν και στα εισερχόμενα e-mails τα οποία είναι πολύ πιθανό να συνοδεύονται από malware.

2.4. Αναγνωρίζοντας του Κινδύνους των Πληροφοριών

Σύμφωνα με την βιβλιογραφία ο *κίνδυνος* αφορά τις πιθανότητες που υπάρχουν έτσι ώστε ένα πραγματοποιθέν γεγονός να έχει αρνητικό αντίκτυπο για τον οργανισμό. Αναλυτικότερα, η έννοια του κινδύνου είναι πιο πολύπλοκη καθώς χωρίζεται σε πέντε κατηγορίες, όπως είναι *ο επιχειρησιακός κίνδυνος (business risk), ο κίνδυνος του λογιστικού ελέγχου (audit risk), ο κίνδυνος της ασφάλειας (security risk)*, *ο κίνδυνος της συνέχειας (continuity risk)* (Hunton, 2004, σελ. 48 - 51) καθώς *και ο κίνδυνος της διάγνωσης* (Andrew, 2000, σελ. 254). Παρακάτω πραγματοποιείται εκτενέστερη ανάλυση για τις προαναφερθείσες έννοιες.

Συγκεκριμένα, *ο επιχειρησιακός κίνδυνος (business risk)* αναφέρεται στην πιθανότητα να παρεκκλίνει η επιχείρηση από τους στόχους τους οποίους έχει θέσει. Μάλιστα, λέγεται πως η επίτευξη ή όχι του θεμιτού αποτελέσματος εξαρτάται από εξωγενείς και ενδογενείς παράγοντες αλλά και από τον ίδιο τον ελεγκτή, ο οποίος οφείλει να γνωρίζει πλήρως τον στρατηγικό σχεδιασμό του οργανισμού για τα επόμενα 3-5 χρόνια προκειμένου να είναι σε θέση να υλοποιήσει ορθά την διαδικασία του ελέγχου (Hunton κ.α., 2004, σελ. 48).

Στην συνέχεια, ο *κίνδυνος του λογιστικού ελέγχου (audit risk)* συνδέεται άμεσα με τους ελεγκτές. Για να γίνει κατανοητό, γίνεται αναφορά για τους εξωτερικούς ελεγκτές όσο και για του ΙΤ ελεγκτές. Μάλιστα, υπάρχουν πιθανότητες οι πρώτοι να σφάλουν σχετικά με τις λογιστικές καταστάσεις ενώ οι δεύτεροι αδυνατούν να ανακαλύψουν κάποια απάτη ή ένα σφάλμα. Επιπλέον, σύμφωνα με τον Hunton κ.α. (2004, σελ. 49) το παρόν ρίσκο αποτελεί ένα σύμπλεγμα από επιπλέον ρίσκα. Ειδικότερα, το περιβάλλον γύρω από το οποίο πράττει τις δραστηριότητες του ο οργανισμός αποτελεί ένα ρίσκο, το οποίο μάλιστα μεγεθύνεται όταν η αγορά είναι μεγάλη. Το ρίσκο αυτό ονομάζεται *εγγενής* και αφορά κυρίως τους κινδύνους που ελλοχεύον στο εξωτερικό περιβάλλον, γεγονός το οποίο τους καθιστά ιδιαίτερα δύσκολους στην διαχείριση τους, έτσι, είναι ζωτικής σημασίας η ταυτοποίηση τους από τον ελεγκτή. Συνεχίζοντας, επόμενο στοιχείο αποτελεί ο *κίνδυνος του ελέγχου (control risk)* το οποίο αναφέρεται σε παραλείψεις από το εσωτερικό σύστημα του ελέγχου οι οποίες οδηγούν σε εσφαλμένη καταγραφή στοιχείων που αφορούν συναλλαγές, πρόκειται για έναν τεστ το οποίο καλείται να αναμετρηθεί με κινδύνους οι οποίοι πρέπει να εξαλειφθούν πλήρως (Hawker, 2000, σελ. 254).

Γίνεται έντονη αναφορά στην ανάγκη για την λήψη μέτρων και εκτίμηση των ρίσκων προκειμένου ο κάθε οργανισμός να ισχυροποιήσει την ασφάλεια του, εκτιμώντας, αναγνωρίζοντας και απομονώνοντας περιστατικά τα οποία είναι ικανά να βλάψουν το

σύστημα του (Wilkinson, 1993, σελ. 333). *Ο κίνδυνος της ασφάλειας* αποτελεί έναν ιδιαίτερα κρίσιμο παράγοντα ο οποίος πρέπει να ληφθεί σοβαρά υπόψιν από τον οργανισμό, για τον λόγο ότι η πληροφορία κινδυνεύει να χάσει δύο πολύ σημαντικά στοιχεία όπως αυτά της **ακεραιότητας** και της **προσβασιμότητας.** Κύρια πηγή κινδύνου για τον οργανισμό αποτελεί η φυσική ή λογική είσοδος σε δεδομένα στα οποία ο χρήστης δεν έχει το δικαίωμα. Μάλιστα, το επίπεδο του κινδύνου αυξάνεται ολοένα κι περισσότερο σε περιπτώσεις στις οποίες ο οργανισμός χρησιμοποιεί ολοκληρωμένο σύστημα αλλά δεν διαθέτει ξεχωριστούς κωδικούς πρόσβασης. Έτσι, είναι εύκολο κάποιος επικίνδυνος χρήστης να εισέλθει σε ευαίσθητα δεδομένα, τα οποία κάλλιστα μπορεί να χειραγωγήσει όπως εκείνος επιθυμεί (Hunton κ.α., 2004, σελ. 50). Έτσι, στην καλύτερη περίπτωση, παραβιάζεται η **εμπιστευτικότητα** της πληροφορίας. Βέβαια, υπάρχουν και αυτοί οι οποίοι θα χρησιμοποιήσουν τις πληροφορίες για το προσωπικό τους συμφέρον. Ωστόσο το πρόβλημα μεγεθύνεται αν αναλογισθούμε την σημασία των πληροφοριών στην λήψη αποφάσεων, όπως έχει αναλυθεί και σε προηγούμενο κεφάλαιο.

Εμβαθύνοντας ακόμη περισσότερο, είναι ιδιαίτερα σημαντικό για ένα πληροφοριακό σύστημα η ύπαρξη συστήματος backup and recovery για την μη εξαφάνιση των δεδομένων αλλά και την εύκολα πρόσβαση των χρηστών σε αυτά. Είναι γνωστό πως η διαθεσιμότητα των δεδομένων πολλές φορές πλήττεται από τους hackers οι οποίοι χρησιμοποιώντας ποικίλους τρόπους φορτώνουν τους servers καθιστώντας την πρόσβαση των χρηστών, ιδιαίτερα δύσκολη ή και ακατόρθωτη. Για τον λόγο αυτό είναι ζωτικής σημασίας η ύπαρξη του παραπάνω συστήματος, προκειμένου η ανάκτηση των δεδομένων να επέλθει χωρίς μεγάλες καθυστερήσεις. Τρανταχτό παράδειγμα αποτελεί η ανάγνωση ενός e-mail από έναν ανυποψίαστο εργαζόμενο το οποίο συνοδεύεται από έναν ιό. Επιπρόσθετα, η παρούσα λειτουργία είναι ευέλικτη καθώς μπορεί να προσαρμοστεί στα «μέτρα» της κάθε επιχείρησης. Επομένως, μια μικρή επιχείρηση μπορεί να διατηρεί τα αρχεία της σε χαμηλού κόστους αποθηκευτικές συσκευές, ενώ ένας μεγαλύτερου μεγέθους οργανισμός να χρησιμοποιεί πιο πολύπλοκες διαδικασίες, όπως ένα σχέδιο ανάκτησης από διάφορες καταστροφές (Hunton κ.α., 2004, σελ. 51).

Τελευταία κατηγορία κινδύνου είναι αυτός της *διάγνωσης*, ο οποίος είναι ιδιαίτερα δυσνόητος επειδή δεν εξάγει μετρήσιμα αποτελέσματα αλλά και επειδή ο ελεγκτής καλείται να αντιμετωπίσει κινδύνους τους οποίους δεν έχει αναγνωρίσει. Παρ' όλα αυτά, δημιουργούνται διάφοροι στόχοι οι οποίοι μπορούν να εξουδετερωθούν (Hawker, 2000, σελ. 254).

2.5. Διαχείριση Κινδύνων - Risk Management

Στην ενότητα αυτή θα παρουσιασθεί η διαδικασία *διαχείρισης του κινδύνου (risk management),* η οποία πρόκειται για μία διαδικασία εύρεσης και ταυτοποίησης των κινδύνων που συνυπάρχουν στο περιβάλλον του οργανισμού (Pickett, 2010, σελ. 179; Boyce & Jennings, 2002, σελ. 25), οι οποίοι ως γνωστόν αποσκοπούν στην παραβίαση της ομαλότητας των διαδικασιών του οργανισμού (Boyce & Jennings, 2002, σελ. 25), αλλά και η κατάστρωση σχεδίου για την αντιμετώπιση των κινδύνων και την ισχυροποίηση των ελέγχων (Mazareanu, 2007). Επιπλέον, ο οργανισμός που διαθέτει τέτοια συστήματα διοίκησης επωφελείται μέσα από την γνώση των κινδύνων καθώς έτσι ισχυροποιεί την άμυνα της. Επίσης, όπως είναι αναμενόμενο, διαχειρίζεται καλύτερα τις ζημίες αλλά και του ίδιους τους κινδύνους καθώς έχει εκ των προτέρων μελετήσει τις πιθανές συνέπειες μιας παραβίασης του συστήματος της (Merkow & Breithaupt, 2014, σελ. 10).

Συνεχίζοντας, η διαδικασία διαχείρισης του κινδύνου αποτελείται από την ανάλυση του κινδύνου (risk analysis) και την εκτίμηση του κινδύνου (risk assessment), μέρη, τα οποία προσδίδουν μία αριθμητική/οικονομική αξία στα περιουσιακά στοιχεία, έτσι ώστε να ληφθούν τα απαραίτητα μέτρα πρόληψης (Merkow & Breithaupt, 2014, σελ. 10).

2.5.1. Ανάλυση των Κινδύνων – Risk Analysis

Η διαχείριση των κινδύνων ή διαφορετικά της ασφάλειας αποτελεί ένα ζήτημα του οποίου η σημασία αυξάνεται συνεχώς καθώς η έκθεση των οργανισμών στον χώρο του διαδικτύου δημιουργεί επιπλέον τρωτά σημεία όπως και κινδύνους (Stallings & Brown, 2012, σελ. 467). Η ανάλυση του κινδύνου αποτελεί μία ιδιαίτερα σημαντική πτυχή για την διαχείριση των κινδύνων, για τον λόγο ότι η αποστολή της ανάλυσης αυτής είναι η αναγνώριση των απειλών και των τρωτών σημείων του οργανισμού (Feng κ.α., 2014). Η διαδικασία τούτη αποτελείται από 3 στοιχεία, τα οποία ως σύνολο υλοποιούν μία πλήρη ανάλυση κινδύνου. Ειδικότερα, σύμφωνα με τους Rainer κ.α. (1991) τα στοιχεία της ανάλυσης είναι:

1. αναγνώριση & ανάλυση των περιουσιακών στοιχείων
2. αναγνώριση & ανάλυση των απειλών
3. αναγνώριση & ανάλυση των τρωτών σημείων

Σχήμα 6: Οι θεμελιώδεις διαδικασίες της ανάλυσης κινδύνου

Πηγή: Rainer, R., Snyder, C. & Carr, H. (1991). Risk Analysis for Infromation Technology. *Journal of Management Information Systems*. 8(1):129-147.

2.5.1.1. Αναγνώριση & Ανάλυση των Περιουσιακών Στοιχείων

Στο σημείο αυτό ο οργανισμός οφείλει να έχει πλήρη γνώση των περιουσιακών του στοιχείων έχοντας την προστασία τους ως πρώτιστο μέλημα. Όμως, όπως έχει ειπωθεί, το πλήθος των περιουσιακών στοιχείων είναι μεγάλο αν αναλογιστούμε πως έχουν άυλη και απτή μορφή. Έτσι είναι δύσκολο για τον οργανισμό να μεριμνήσει για όλα τα περιουσιακά στοιχεία, για αυτό είναι επιτακτική ανάγκη να πραγματοποιηθεί αυστηρά επιλεγμένη προστασία κρίνοντας με βάση παράγοντες όπως είναι η συνάφεια/συμμετοχή στους στόχους ή την πιθανή ζημία που θα έχει η επιχείρηση σε περίπτωση παραβίασης τους (Hawker, 2000, σελ. 480).

2.5.1.2. Αναγνώριση & Ανάλυση Απειλών

Στον προσδιορισμό των απειλών, ο οργανισμός καλείται να εξετάσει όλες τις πιθανές απειλές (Elky, 2007, σελ. 5). Η διαδικασία αυτή εξαρτάται από την ορθή εκμετάλλευση των πηγών των απειλών αλλά και την εμπειρία του ελεγκτή. Όπως παραπάνω, έτσι και εδώ ο οργανισμός πρέπει να διαχειριστεί τις απειλές αναλόγως με τον βαθμό επικινδυνότητας εν συγκρίσει με τα τρωτά σημεία του. Κάποια από τα κριτήρια τα οποία θα βοηθήσουν τον οργανισμό να διαχωρίσουν τις απειλές είναι το κίνητρο της επίθεσης, η ικανότητα αυτών να βλάψουν τον οργανισμό, οι πιθανότητες της επίθεσης και τέλος οι συνέπειες της επίθεσης (Hawker, 2000, σελ. 481).

2.5.1.3. Αναγνώριση & Ανάλυση των Τρωτών Σημείων

Η αναζήτηση των τρωτών σημείων αναφέρεται στην εύρεση κενών και αδυναμιών του συστήματος αλλά και στις διαδικασίες οι οποίες παρουσιάζουν σφάλματα εξαιτίας

των απειλών. Αξίζει να αναφερθεί πως τα τρωτά σημεία δεν είναι αυτόνομα, με την έννοια ότι η ύπαρξη τους και μόνο δεν βλάπτει το σύστημα. Στην περίπτωση που υπάρχει συνδυασμός «απειλής και τρωτού σημείου» τότε όπως είναι ευνόητο, ο οργανισμός πρέπει να προσέξει (Elky, 2007, σελ. 6). Η επιτυχής διαδικασία ταυτοποίησης θα πρέπει να εξάγει μια πλήρης λίστα με τα πιθανά τρωτά σημεία και τις απειλές καθώς τι πηγές και τις λειτουργίες (Stallings & Brown, 2012, σελ. 482).

2.6. Αξιολόγηση των Κινδύνων - Risk Evaluation or Risk Assessemnt

Η εκτίμηση του πιθανού κινδύνου αποτελεί μία διαδικασία ταυτοποίησης και κατανόησης του κινδύνου (Moyo κ.α., 2013) η οποία απαρτίζεται από δύο κατευθύνσεις, την πιθανότητα να συμβεί ένα γεγονός αλλά και το επίπεδο του κινδύνου ένα γεγονός να βλάψει το σύστημα και τα περιουσιακά στοιχεία του οργανισμού (Golub & Radojevic, 2014).

Σύμφωνα με την Mazareanu (2007) η εκτίμηση του κινδύνου αφορά την διαδικασία με την ισχυρότερη θέση μέσα στην διαχείριση του κινδύνου (risk management). Επιπροσθέτως, η ίδια υποστηρίζει ότι η διαδικασία της αξιολόγησης αποτελείται από πολύ σημαντικά βήματα. Αρχικά, ο εκάστοτε οργανισμός επιχειρεί να βρει τους κινδύνους και τις αδυναμίες του, προκειμένου να υπολογίσει τις ενδεχόμενες ζημίες του. Στην συνέχεια μελετάται η πιθανότητα να πραγματοποιηθεί ένα επιζήμιο γεγονός, όπου πρέπει να συγκαταλεχθούν τόσο εξωτερικοί όσο και εσωτερικοί παράγοντες. Το τρίτο βήμα αφορά το ηλεκτρονικό περιβάλλον της επιχείρησης όπου ο οργανισμός μελετά τις πιθανότητες να συμβεί ένα γεγονός που θα προξενούσε αποκλίσεις στις διαδικασίες. Εν συνεχεία, η εκτίμηση κινδύνου πρέπει να υλοποιηθεί πριν κινδυνεύσει η επιχείρηση, διαφορετικά χάνει την αξία της ως διαδικασία πρόληψης. Τέλος, είναι απαραίτητη η προσθήκη ποσοτικής και ποιοτικής προσέγγισης.

2.6.1. Ποσοτικές Μέθοδοι για την Εκτίμηση των Κινδύνων - Quantitative methods for risk assessment

Οι ποσοτικές μέθοδοι υπολογίζουν αριθμητικά τις πιθανότητες για οποιοδήποτε παράγοντα που θεωρείται επιζήμιος και ικανός να εμποδίσει τον οργανισμό να επιτύχει τους στόχους του (Anikin, 2015). Παρακάτω αναφέρονται και αναλύονται μερικές από τις διαθέσιμες ποσοτικές μεθόδους. Αυτές είναι, η Monte Carlo Method, η Annual Loss Expected, η Courtney & Fisher και τα μοντέλα ISRAM και LRAM.

2.6.2 Monte Carlo Method

Σύμφωνα με την Mazareanu (2007), αποτελεί μέθοδο η οποία χρησιμοποιείται για να υπολογίσει τις πιθανότητες που έχουν οι στόχοι να επιτευχθούν. Επιπλέον, υπολογίζεται ποσοτικά ο κίνδυνος όλου του project καθώς και τα επιπλέον κόστη. Τέλος, με την μέθοδο αυτή ταυτοποιούνται οι παράγοντες που συμμετέχουν σε ένα αρνητικό γεγονός, όπως επίσης και το ποσοστό συμμετοχής τους.

Ο τύπος που χρησιμοποιεί αυτή η μέθοδος είναι:

$$\Re = PxL$$

Όπου:

RE = η έκθεση στον κίνδυνο (**R**isk **E**xposure).

P = πιθανότητα να συμβεί ο κίνδυνος (**R**isk **P**robability).

L = ζημία (**L**oss).

2.6.3. Annual Loss Expected – ALE

Σύμφωνα με τον Rot (2008) είναι η πιο γνωστή και πιο πολυχρησιμοποιημένη μέθοδος η οποία αναζητά την «αναμενόμενη ζημία» που προκύπτει από την πιθανότητα να συμβεί ένα γεγονός το οποίο θα έχει αρνητικό αντίκτυπο για την πληροφορία του οργανισμού. Η μέθοδος αυτή χρησιμοποιεί τους παρακάτω τύπους:

$$ALE = (\pi\iota\theta\alpha\nu\acute{o}\tau\eta\tau\alpha\ \varepsilon\nu\acute{o}\varsigma\ \gamma\varepsilon\gamma o\nu\acute{o}\tau o\varsigma\ \nu\alpha\ \sigma\upsilon\mu\beta\varepsilon\acute{\iota})\, x\, (\alpha\xi\acute{\iota}\alpha\ \tau\eta\varsigma\ \zeta\eta\mu\acute{\iota}\alpha\varsigma)$$

$$\acute{H}$$

$$ALE = \sum_{i=1}^{n} I(Oi)\, fi$$

Όπου:

[O1, O2,……, On] = το πλέγμα των αρνητικών αποτελεσμάτων ενός γεγονότος.

I(Oi) = η αξία της ζημιάς εξαιτίας των αρνητικών γεγονότων.

F = η συχνότητα εμφάνισης ενός γεγονότος.

2.6.4. Courtney Method

Οι Rot (2008) και Rainer κ.α. (1991a) υποστηρίζουν πως η μέθοδος αυτή πήρε το όνομα του δημιουργού της και έχει πολλά κοινά σημεία με την παραπάνω μέθοδο (ALE). Σύμφωνα με τον Courtney, η αξία του κινδύνου είναι αποτέλεσμα του γινομένου μεταξύ της πιθανότητας εμφάνισης ενός γεγονότος για περισσότερες από μία φορές μέσα στον χρόνο, την απώλεια που θα προκαλέσει καθώς και την συνολική απώλεια που προκλήθηκε από το γεγονός. Ο τύπος της μεθόδου είναι:

$$R = P \, x \, C$$

$$Ή$$

$$\boldsymbol{ALE} = \frac{10^{f+i-3}}{3}$$

Όπου

f = δείκτης εκτιμώμενης συχνότητας για την εμφάνιση ενός γεγονότος.

i = δείκτης χρηματικής επίδρασης από την πρόκληση του συμβάντος.

2.6.5. ISRAM Method

Στο ίδιο άρθρο ο Rot (2008) μας παρουσιάζει και την ISRAM method, η οποία είναι θεμιτό να ειπωθεί πως η παρούσα μέθοδος βασίζεται σε μεγάλο βαθμό στην ALE και επιλέγεται από πολλούς ερευνητές. Η σχέση που χρησιμοποιείται για την εύρεση του κινδύνου είναι πιο πολύπλοκη από τις προαναφερθείσες και παρουσιάζεται παρακάτω. Πιο συγκεκριμένα:

$$Risk = ¿$$

Όπου τα i και j αναφέρονται στον αριθμό των ερωτήσεων που αφορούν την πιθανότητα να συμβεί ένα περιστατικό και τις συνέπειες που έχει εκτιμηθεί πως θα συμβούν, αντίστοιχα. Ως m και n ορίζεται ο αριθμός των ατόμων αυτών που απάντησαν στις ερωτήσεις της έρευνας. Συνεχίζοντας, wi και wj αντικατοπτρίζουν την βαρύτητα των ειδικών ερωτήσεων που αναφέρθηκαν και ανώτερα. Ως pi και pj είναι η τιμή των απαντήσεων στις επιλεγμένες

ερωτήσεις. Τέλος, τα Τ1 και Τ2 παριστάνουν την πιθανότητα ενός γεγονότος να συμβεί και τα αρνητικά αποτελέσματα που θα προκύψουν από την πραγματοποίηση των γεγονότων αυτών.

2.6.6. LRAM – Livermore Risk Analysis Method

Σύμφωνα με τον Guarro (1987) η μέθοδος LRAM αναπτύχθηκε το 1985 και πρόκειται για ένα ιδιαίτερα ευέλικτο εργαλείο που εξυπηρετεί τα άτομα που είναι επιφορτισμένα με την λήψη αποφάσεων και την διαχείριση των κινδύνων. Η σχέση που αντικατοπτρίζει τη μέθοδο είναι η ακόλουθη:

$$R\left[R_{ei}\right]=MPL\left[C_i\right]x\,PCF\left[PMC\,O_i\right]x\,EF\left[T_i\right]$$

Ειδικότερα η σχέση αναφέρει πως ο ετήσιος κίνδυνος προκύπτει μέσω ενός γινομένου τριών στοιχείων. Το $MPL\left[C_i\right]$ προκύπτει εν μέσω των προσδοκώμενων συνεπειών. Συνεχίζοντας, πολλαπλασιάζεται με την πιθανότητα να αποτύχουν οι έλεγχοι, η οποία προκύπτει από το πλέγμα των προληπτικών ελέγχων $PMC\,O_i$**.** Τελευταίο στοιχείο στην σχέση είναι η προβλεπόμενη συχνότητα εμφάνισης μιας απειλής.

2.7. Ποιοτική Μέθοδος - Qualitive methods for risk assessment

Η ποιοτική μέθοδος διαφέρει από την ποσοτική στο εξαχθέν αποτέλεσμα καθώς δεν παρουσιάζει αριθμητικά δεν παρουσιάζει αριθμητικά δεδομένα αλλά τα αποτελέσματα εμφανίζονται με την μορφή περιγραφών. Επιπλέον, τέτοιου είδους μέθοδοι συνηθίζεται να χρησιμοποιούνται για την περιγραφή της ευαισθησίας και της κατάστασης ενός συστήματος το οποίο έχει δεχθεί επίθεση. Επιπλέον, αξιοποιώντας τις μεθόδους αυτές, ο εκάστοτε οργανισμός είναι σε θέση να δημιουργεί και να εξετάζει όλα τα πιθανά σενάρια κινδύνου, προβλέποντας τις απειλές και τους βασικούς παράγοντες που πιθανότατα θα τον βλάψουν (Mazareanu, 2007). Παρακάτω παρατίθενται μερικές ποιοτικές μέθοδοι, όπως είναι η FMEA (Failure mode & effects analysis), FMECA, NIST SP 800 – 30, CRAMM method.

2.7.1. FMEA & FMECA

Οι μέθοδοι αυτές δημιουργήθηκαν αρκετά χρόνια πριν με σκοπό να αυξηθεί το επίπεδο αξιοπιστίας στις αναλύσεις των οπλικών συστημάτων. Αποστολή τους είναι η

μελέτη των ελαττωμάτων εκείνων τα οποία επηρεάζουν αρνητικά την λειτουργία ολόκληρου του συστήματος. Η διαφορά ανάμεσα στις δύο μεθόδους είναι η προσθήκη μίας επιπλέον ανάλυσης. Ειδικότερα, η FMCEA αναλύει την σοβαρότητα των ελαττωμάτων και εξετάζει τον βαθμό στον οποίο επηρεάζει την ολική δράση των λειτουργιών. Τέλος, αξίζει να αναφερθεί πως πρόκειται για δύο μεθόδους οι οποίες είναι απαιτητικές διότι δεν μπορούν να χρησιμοποιηθούν δίχως ειδικές γνώσεις και εμπειρία (Rot, 2008a).

2.7.2. NIST SP 800 – 30

Η παρούσα μέθοδος αποτελείται από 9 βασικά βήματα τα οποία πρέπει να ληφθούν σοβαρά υπόψιν για την επιτυχή εκτίμηση του κινδύνου. Στην πρώτη φάση πρέπει αν αποφασισθεί *το σύστημα* το οποίο θα εκτιμηθεί. Στην συνέχεια, πρέπει *να εξακριβωθεί ο σκοπός* της αξιολόγησης προκειμένου να συλλεχθούν οι απαιτούμενες πληροφορίες. Με το πέρας των παραπάνω σταδίων ο οργανισμός ταυτοποιεί τόσο τις *απειλές* όσο και την *ευαισθησία* του συστήματος. Γίνεται εύκολα κατανοητό πως αυτές οι δύο έννοιες συνδέονται άρρηκτα καθώς η ύπαρξη υψηλής ευαισθησίας, αυξάνει την «δύναμη» των απειλών. Συνεχίζοντας, ο οργανισμός οφείλει να καταγράψει τους μηχανισμούς ασφάλειας και ελέγχου που ήδη εφαρμόζονται από πλευράς της αλλά και τις πιθανότητες που υπάρχουν μία απειλή να εκμεταλλευθεί τα τρωτά σημεία του. Η πιθανότητα αυτή χαρακτηρίζεται ως χαμηλή, μέτρια και υψηλή. Εν συνεχεία, αναλύεται η *επίδραση διαφόρων περιστατικών και των οργανισμών ως σύνολο*. Εφ' όσον όλα τα προηγούμενα στάδια έχουν υλοποιηθεί με επιτυχία, δημιουργούμε έναν πίνακα μέτρησης του κινδύνου. Όπως φαίνεται πίνακα 2, στις στήλες έχει τοποθετηθεί ο βαθμός επίδρασης του περιστατικού. Στις γραμμές, δηλώνεται η πιθανότητα του περιστατικού να συμβεί.

Πλέον η επιχείρηση έχει μία σαφή εικόνα για το περιβάλλον της και τους κινδύνους που υπάρχουν σε αυτό. Έτσι, αναπόφευκτα οδηγείται στην επεξεργασία και αναπροσαρμογή των μηχανισμών του ελέγχου και της ασφάλειας προκειμένου να μειωθεί το επίπεδο κινδύνου στο ελάχιστο δυνατό, έτσι ώστε να μην προκληθούν μεγάλες απώλειες από μία ενδεχόμενη επίθεση. Τέλος, η καταγραφή των αποτελεσμάτων της εκτίμησης του κινδύνου και η δημιουργία ορθής αναφοράς (report), αποστέλλεται στα ανώτερα στελέχη προκειμένου να την μελετήσουν και να αποφασίσουν βασισμένοι σε στοιχεία και όχι σε διαίσθηση (Rot, 2008b).

Πίνακας 2: Παράδειγμα MATRIX σύμφωνα με την μεθοδολογία NIST

Probability of threat appearance	Results		
	Low (10)	Medium (50)	High (100)
High (1,0)	Low 10*1,0=10	Medium 50*1,0=50	High 100*1,0=100
Medium (0,5)	Low 10*0,5=5	Medium 50*0,5=25	High 100*0,5=50
Low (0,1)	Low 10*0,1=1	Medium 50*0,1=5	High 100*0,1=10

Πηγή: Rot, A., 2008. IT risk assessment: Quantitative and qualitative approach. In: the World Congress on Engineering and Computer Science (WCECS). pp. 1–6.

2.7.3. CRAMM Methodology

Πρόκειται για μία μέθοδο η οποία έχει δημιουργηθεί από το CCTA του Ηνωμένου Βασιλείου και αποτελεί την βασική μέθοδο εκτίμησης, η οποία απαρτίζεται από 3 στάδια. Πρωταρχικά, ο οργανισμός οφείλει να ταυτοποιήσει και να αξιολογήσει τους πόρους που κατέχει ήδη. Στην συνέχεια, δόκιμο είναι να προχωρήσει σε αξιολόγηση των απειλών και των τρωτών σημείων, ενώ στο τελευταίο στάδιο είναι σε θέση να προτείνει ένα σύνολο από μηχανισμούς για την αύξηση των επιπέδων ασφαλείας και ελέγχου, εκ των οποίων θα επιλέξει τους καταλληλότερους. Καταλήγοντας, επισημαίνεται ότι η μεθοδολογία CRAMM είναι κατάλληλη για την εκτίμηση κινδύνων σε λογισμικά, ενώ χρησιμοποιεί επίπεδα 5 βαθμών για την δήλωση τους (Rot, 2008b).

2.8. Ποσοτικές Μέθοδοι VS Ποιοτικές Μέθοδοι

Κλείνοντας την παρούσα ενότητα παρουσιάζονται μερικά πλεονεκτήματα και μειονεκτήματα για τις δύο κατηγορίες ανάλυσης.

Ένα ισχυρό πλεονέκτημα από την χρήση ποσοτικών μεθόδων πηγάζει από την αριθμητική μορφή του τελικού αποτελέσματος καθώς είναι εύκολο να εξετασθεί και να αναλυθεί. Για παράδειγμα, είναι ευκολότερο για τον οργανισμό να καταγράψει περαστικά και τον βαθμό που τον επηρεάζουν, δημιουργώντας αναλύσεις κόστος – ωφέλειας. Επιπλέον, η ποσοτική αναπαράσταση των κινδύνων παρουσιάζει μία πληρέστερη εικόνα στον οργανισμό, μειώνοντας έτσι το ρίσκο για να ανεπιτυχείς αποφάσεις. Στον αντίποδα, τα δύο ισχυρά πλεονεκτήματα των ποιοτικών μεθόδων αφορούν την απλότητα κα το χαμηλό κόστος υλοποίησης και ανάλυσης των δεδομένων και περιοχών υψηλού κινδύνου

(Mazareanu, 2007; Slah & Murtaza, χχ).

Στα αρνητικά της χρήσης των ποσοτικών μεθόδων αναφέρεται το υψηλότερο κόστος. Το υψηλός κόστος δεν μαρτυράτε μόνο σε χρηματικές μονάδες αλλά και στην απαιτούμενη εμπειρία, στον χρόνο και στα ειδικά εργαλεία που είναι απαραίτητα για την επιτυχή έκβαση τέτοιου είδους μεθόδων. Μάλιστα, το κόστος αυξάνεται όταν τα προς ανάλυση δεδομένα είναι ανακριβή, πολύπλοκα και μεγάλο όγκο, δαπανώντας έτσι πολύτιμο χρόνο ο οποίος θα μπορούσε να αποδοθεί κάπου αλλού. Επιπλέον, πιστεύεται πως πολλές ποσοτικές μέθοδοι δεν μπορούν να λειτουργήσουν αυτόνομα διότι τα τελικά αποτελέσματα δεν επικαλύπτουν πλήρως τους στόχους, με αποτέλεσμα τα κενά να συμπληρώνονται από ποιοτικές μεθόδους. Αξίζει να τονίσουμε πως το ίδιο συμβαίνει και στις ποιοτικές μεθόδους, καθώς ο γενικός χαρακτήρας των εξαγόμενων αποτελεσμάτων και η έλλειψη αριθμών καλύπτεται από τις ποσοτικές μεθόδους. Καταλήγοντας, αντιλαμβανόμαστε πως το ιδανικό αποτέλεσμα μπορεί να αποτελέσει παράγωγο της συνεργασίας των δύο διαφορετικών κατηγοριών (Rainer, 1991; Slah & Murtaza, χχ).

Κεφάλαιο 3

Έλεγχοι & Ασφάλεια στα Λογιστικά Πληροφοριακά Συστήματα

3.1. Έλεγχοι στα Λογιστικά Πληροφοριακά Συστήματα

Ο έλεγχος στα λογιστικά πληροφοριακά συστήματα αποτελεί μία διαδικασία η οποία αποσκοπεί στην προστασία των περιουσιακών στοιχείων του οργανισμού. Ακόμη πιο περιγραφικά, αφορά όλες τις διαδικασίες και τα μέτρα που θα ληφθούν αποσκοπώντας στην επίτευξη των στόχων που έχουν τεθεί (Landoll, 2006, σελ. 162). Ειδικότερα επιδιώκεται η διασφάλιση των περιουσιακών στοιχείων καθώς επίσης, η αξιοπιστία και η αποτελεσματική λειτουργία έπειτα από την χρήση των θεσπισμένων πολιτικών και διαδικασιών από την διοίκηση. Στην βιβλιογραφία εμφανίζεται να υπάρχει μία «σύγχυση» αναφορικά με τους τύπους των ελέγχων. Αναφορικά, ο Pickett (2002, σελ. 280) στο βιβλίο του, δανείστηκε τον διαχωρισμό που έχει πράξει ο COBIT, ο οποίος και περιέχει 6 τύπους ελέγχων.

Ειδικότερα, αναφέρονται οι : 1) έλεγχος εφαρμογών, 2) έλεγχος κινδύνων, 3) λεπτομερείς έλεγχοι, 4) γενικός έλεγχος, 5) εσωτερικός έλεγχος και 6) persuasive IS controls.

Από την άλλη οι περισσότεροι από τους παραπάνω τύπους ελέγχου, στο βιβλίο του Landoll (2006, σελ. 437), εμπεριέχονται στους γενικούς ελέγχους. Πιο συγκεκριμένα στον γενικό έλεγχο ανήκουν ο έλεγχος στα λογισμικά (software controls), έλεγχοι στον εξοπλισμό, έλεγχοι για την επίβλεψη των λειτουργιών των υπολογιστών, τον βαθμό στον οποίο λειτουργούν ορθά αλλά και τον βαθμό στον οποίο επιδιώκεται και είναι εφικτή η δημιουργία backup (computer operational controls), έλεγχοι στην ασφάλεια των δεδομένων και κατά συνέπεια την διασφάλιση των τριών θεμελιωδών στοιχείων τους (data security controls), έλεγχος στις εφαρμογές και στην παρακολούθηση της ορθότητας των διαδικασιών (implementation controls) και διαχειριστικοί έλεγχοι για την διαβεβαίωση πως όλοι οι κανόνες καθώς και οι διαδικασίες που έχουν δυσπιστεί, τηρούνται ευλαβικά από όλους στο εσωτερικό του οργανισμού (administrative controls). Στο σημείο αυτό θα δανειστούμε από τους Hunton κ.α. (2004) τον διαχωρισμό των ελέγχων ασφαλείας σε λογικούς και φυσικούς.

3.1.1. Φυσική Ασφάλεια

Η φυσική ασφάλεια έχει ως αποστολή την προστασία της τεχνολογική υποδομής του οργανισμού, επικεντρώνοντας το ενδιαφέρον στα απτά στοιχεία του, όπως είναι ο εξοπλισμός ή οι εγκαταστάσεις (Fang & Shu, 2016). Παραδείγματος χάριν, η είσοδος στον οργανισμό χωρίς εξουσιοδότηση είναι επικίνδυνη, έτσι οποιοσδήποτε εισέρχεται πρέπει να ελέγχεται. Για την εξάλειψη αυτών των φαινομένων χρησιμοποιούνται διάφορες τεχνικές, όπως η χρήση φύλακα ή ακόμη και ειδικές κάρτες εισόδου αλλά και συσκευές που ελέγχουν τα βιομετρικά χαρακτηριστικά (Muhrtala & Ogundeji, 2013).

Επιπλέον, ως μέτρο πρόληψης θεωρείται και η εγκατάσταση συστημάτων τα οποία καταγράφουν και ελέγχουν την «κίνηση» στην επιχείρηση όπως είναι για παράδειγμα οι κάμερες ασφαλείας και οι συναγερμοί (Wong-Steele, 2017, σελ. 31). Ωστόσο, ο έλεγχος ενός επισκέπτη πρέπει να ξεκινάει από το σημείο της εισόδους του, με την χρήση υπογραφής και την καταγραφή των στοιχείων του, έτσι ώστε να του παρασχεθεί η ειδική κάρτα που αναφέρθηκε παραπάνω. Βέβαια ευκόλως αντιλαμβανόμαστε τον σημαντικό ρόλο που διαδραματίζουν οι ελεγκτές στην συνολική διαδικασία καθώς κρίνεται απαραίτητο να ελέγχουν τακτικά τα τους υφιστάμενους ελέγχους, αποσκοπώντας στην συνεχή βελτίωση τους (Champlain, 2003, σελ. 109). Συνεχίζοντας, ο ίδιος (2003, σελ. 110) υποστηρίζει ότι, είναι απαραίτητη η ύπαρξη δύο παροχέων, από τους οποίους ο ένας λειτουργεί ως εφεδρικός και έχει εγκατασταθεί σε διαφορετική περιοχή (UPS sytems). Είναι φρόνιμο να ειπωθεί πως η παραπάνω διαδικασία είναι όμοια με την λογική του offsite backup.

3.1.2. Λογική Ασφάλεια

Αποτελεί την ασφάλεια που εστιάζει σε λιγότερο απτά στοιχεία, όπως είναι τα δεδομένα και τα λογισμικά που κατέχει ο εκάστοτε οργανισμός (Stallings & Brown, 2012, σελ. 517; Boyce & Jennings, 2002, σελ. 114). Βέβαια, αξίζει να επισημανθεί πως τα στοιχεία αυτά συνδέονται με τα απτά στοιχεία που αναφέρθηκαν στην προηγούμενη ενότητα. Σε αυτού του τύπου τον έλεγχο, ο υπεύθυνος καλείται να πράξει όμοια με την φυσική ασφάλεια, αλλά προσαρμόζοντας τις κινήσεις του στα δεδομένα και στα λογισμικά. Ειδικότερα, για την διασφάλιση των στοιχείων ο οργανισμός πρέπει να λάβει κάποια μέτρα προκειμένου να αποκρούσει τις διαδικτυακές επιθέσεις. Η χρήση του firewall και anti-virus

μπλοκάρουν την αθέμιτη είσοδο στα εταιρικά συστήματα. Επιπλέον, για την ενίσχυση της άμυνας συνήθως χρησιμοποιείται ID ή κάποιος κωδικός πρόσβασης ή ακόμη και κρυπτογράφηση των μηνυμάτων. Επιπρόσθετα, εύκολα μπορούμε να πούμε πως η εκπαίδευση του προσωπικού αποτελεί έναν ιδιαίτερα σημαντικό παράγοντα για την διασφάλιση των αμυντικών συστημάτων (Wallace, 2014, σελ. 536). Πρόκειται για τεχνικές οι οποίες θα εξετασθούν αναλυτικότερα σε επόμενη ενότητα. Ωστόσο, αυτό που οφείλουμε να προσθέσουμε είναι πως απαραίτητη η ενοποιητική λειτουργία όλων των συστημάτων ασφαλείας (Hunton κ.α., 2004, σελ.110).

Εμβαθύνοντας ακόμη περισσότερο, στην βιβλιογραφία γίνεται ιδιαίτερη αναφορά στον έλεγχο της πληροφορίας (Hunton κ.α., 2004, σελ.110) ή στον έλεγχο των εφαρμογών (Bagranoff κ.α., 2010,σελ. 395). Παρ' αυτά ως προς την λειτουργία των ελέγχων αυτών, αναφέρεται πως τα επίπεδα κινδύνου είναι αρκετά υψηλός και είναι σημαντικό να πραγματοποιούνται έλεγχοι σε 3 στάδια, στην είσοδο της πληροφορίας, στις διαδικασίες και στην έξοδο της πληροφορίας (Hunton κ.α., 2004, σελ.110; Bagranoff κ.α., 2010,σελ. 395).

3.1.3. Έλεγχοι στην Είσοδο της Πληροφορίας

Το σημείο της εισόδου αποτελεί ίσως το πιο ευαίσθητο από τα υπόλοιπα δύο διότι είναι πιθανό να υπάρχουν μη αναγνωρισμένα σφάλματα τα οποία με την σειρά τους θα επηρεάσουν αρνητικά τα επόμενα στάδια. Για τον λόγο αυτόν, πρέπει να υλοποιούνται έλεγχοι εισόδου έτσι ώστε τα δεδομένα να είναι έγκυρα και ορθά, βοηθώντας τον οργανισμό να διορθώσει τυχόν λάθη τα οποία θα ήταν οικονομικά ζημιογόνα (Bagranoff κ.α., 2010, σελ. 396). Σύμφωνα, με τους (Bagranoff κ.α., 2010, σελ. 397) όλοι οι οργανισμοί υιοθετούν *μηχανισμούς έγκρισης* όπως είναι για παράδειγμα, η υπογραφή σε μία πώληση. Η έλλειψη της υπογραφής θα δημιουργεί αυτομάτως, πρόβλημα στην καταγραφή της συναλλαγής. Προκειμένου η συναλλαγή να πραγματοποιηθεί με υψηλή ποιότητα, από την πλευρά της ορθής καταγραφής των λογιστικών δεδομένων, οι επιθεωρητές των εργαζομένων επιβλέπουν τις διαδικασίες προκειμένου να είναι σίγουροι πως τα συλλεχθέντα δεδομένα είναι έγκυρα. Επίσης, για την βελτίωση της ταχύτητας αλλά και της ακρίβειας οι συσκευές POS συμμετέχουν ενεργά στην μείωση των σφαλμάτων, χωρίς βέβαια η χρήση της τεχνολογίας να αποκόπτει πλήρως τον ανθρώπινο παράγοντα του οποίου οι ενέργειες λειτουργούν καταλυτικά.

3.1.3.1. Έλεγχοι Κατά την Επεξεργασία της Πληροφορίας - Edit Tests

Τα τεστς αυτά πραγματοποιούνται μόλις τα δεδομένα εισέλθουν στον οργανισμό όπου επανεξετάζονται για να πιστοποιηθεί ο βαθμός ακρίβειας τους. Για την εργασία τούτη χρησιμοποιούνται εξειδικευμένα μηχανήματα τα οποία και ονομάζονται *ρουτίνες επικύρωσης των εισροών (input validation routines).* Πρόκειται για προγράμματα τα οποία λειτουργούν σε πραγματικό χρόνο και είναι υπεύθυνα για τον έλεγχο συγκεκριμένων συναλλαγών οι οποίες πληρούν τα απαιτούμενα επίπεδο ποιότητας (Bagranoff κ.α., 2010, σελ. 397) καθώς έχει παρατηρηθεί πολλές φορές οι εργαζόμενοι να προξενούν προβλήματα σε αυτό το στάδιο (Muhrtala & Ogundeji, 2013).

3.1.3.2. Επιπλέον Έλεγχοι στην Είσοδο - Additional Input Controls

Είναι απαραίτητο να πράττονται επιπρόσθετοι έλεγχοι επειδή τα παραπάνω μέτρα δεν εξασφαλίζουν την απόλυτη επιτυχία. Έτσι, διενεργείται μία σειρά από ελέγχους. Αρχικά, το unfound record test ενημερώνει την ρουτίνα και το κεντρικό αρχείο του συστήματος με τα νέα δεδομένα. Επιπρόσθετα, είναι εφικτό να χρησιμοποιηθούν διάφορα μοντέλα όπως είναι το Modulous 11 technique, σύμφωνα με το οποίο πραγματοποιούνται πράξεις ανάμεσα στα διάφορα ψηφία (check digit) του προϊόντος (Bagranoff κ.α., 2010, σελ.397). Σύμφωνα με τον Hall (2010, σελ 745), κατά την είσοδο των δεδομένων τα πιο γνωστά σφάλματα εμφανίζονται κατά την αντιγραφή ή την αλλαγή θέσης ψηφίων. Για την εξάλειψη τέτοιου είδους σφαλμάτων, πράττονται έλεγχοι των ψηφίων, με διάφορες τεχνικές, όπως είναι για παράδειγμα ο έλεγχος του αθροίσματος πριν και μετά την είσοδο.

3.1.4. Έλεγχοι στις Διαδικασίες Παραγωγής Πληροφορίας - Processing Controls

Εφ' όσον τα δεδομένα περάσουν με επιτυχία τους ελέγχους στο στάδιο της εισόδου, ξεκινούν νέες διαδικασίες ελέγχων τα οποία αποσκοπούν στην εξασφάλιση της ακρίβειας των δεδομένων για την εξαγωγή ωφέλιμης πληροφορίας (Abu-Musa, 2006). Ο Hall (2010, σελ. 747) διαχωρίζει τους ελέγχους σε 3 μεγάλες κατηγορίες, τους ομαδικούς ελέγχους (batch controls), run-to-run controls και τους ελέγχους της διαδρομής (audit trail controls).

3.1.4.1. Έλεγχοι Παρτίδων - Batch Controls

Οι έλεγχοι αυτοί είναι κατάλληλοι για μεγάλου όγκου συναλλαγές διότι

χαρακτηρίζονται από ταχύτητα αλλά και ακρίβεια. Πιο συγκεκριμένα, οποιαδήποτε εγγραφή έχει συμπεριληφθεί εντός της παρτίδας (batch) είναι σίγουρο ότι θα ελεγχθεί και ο έλεγχος θα πραγματοποιηθεί για μία και μόνο φορά (Hall, 2010, σελ. 748). Σύμφωνα με τους Bagranoff κ.α. (2010, σελ. 401) τα αποτελέσματα της διαδικασίας, δηλαδή η εύρεση ή όχι του σφάλματος προκύπτει από την σύγκριση της ολικής παρτίδας (total) με τις επιμέρους παρτίδες, ενώ αυτές χωρίζονται βασιζόμενες σε όμοια χαρακτηριστικά.

3.1.4.2. Run-to-run Controls

Είναι εφικτό να ειπωθεί πως αφορούν ελέγχους στις παρτίδες που υλοποιούνται σε πραγματικό χρόνο. Η διαδικασία αυτή απαρτίζεται από την «είσοδο των δεδομένων», την ενημέρωση των λογαριασμών, την ενημέρωση των αποθεμάτων και την έξοδο με την μορφή αναφοράς (report). Επίσης, εμφανίζονται και τα σφάλματα στο κάθε στάδιο. Την στιγμή της εμφάνισης των σφαλμάτων, ο οργανισμός αποφασίζει εάν θα αφήσει την διαδικασία να εξελιχθεί και έπειτα να προσθέσει τα σωστά δεδομένα ή να επανεκκινήσει ορθά την διαδικασία (Hall, 2010, σελ. 748).

3.1.4.3. Έλεγχοι της Διαδρομής - Audit Trail Controls

Αποτελούν ελέγχους στα δεδομένα σε όλη την διαδρομή τους μέχρι να καταλήξουν στο τελευταίο στάδιο. Στους παρόντες ελέγχους ενδεχομένως υπάρχει η πιθανότητα να υπάρξουν προβλήματα κατά την εύρεση καθώς τα δεδομένα καταγράφονται σε ηλεκτρονική μορφή και όχι στο χαρτί (Hunton κ.α., 2004, σελ. 7) όπως ήταν σύνηθες στα λογιστικά πληροφοριακά συστήματα του απλού χειρωνακτικού μοντέλου (manual model) (Hall, 2010, σελ. 749). Οι έλεγχοι υλοποιούνται με την δημιουργία logs των συναλλαγών, βοηθώντας έτσι τον αρμόδιο να έχει πλήρη επίγνωση της καθολικής διαδικασίας μέχρι και την δημιουργία του τελικού ισολογισμού (Hall, 2010, σελ. 749).

3.1.5. Έλεγχοι στην Έξοδο της Πληροφορίας - Output Controls

Αποτελούν το τελικό στάδιο των ελέγχων στις εφαρμογές (Pickett, 2010, σελ. 875), στο οποίο εξάγεται το τελικό αποτέλεσμα (Bagranoff κ.α., 2010, σελ. 395). Στο στάδιο αυτό παρουσιάζονται στους χρήστες οι πληροφορίες, ωστόσο, στόχος των ελέγχων στο σημείο αυτό είναι η προστασία και η διασφάλιση της πληρότητας των πληροφοριών, έτσι ώστε να είναι κατάλληλες προς αξιοποίηση, εξαλείφοντας τα προβλήματα ανακρίβειας (Hall, 2010, σελ. 750). Για την βέλτιστη κατανόηση παρατίθεται ένα απλό παράδειγμα κατά το οποίο αν για κάποια αιτία χαθούν οι εγγραφές των εκταμιεύσεων τότε αυτό θα

οδηγήσει σε προβλήματα αναπλήρωσης των οφειλών, με συνέπεια να υπάρξει ζημία τόσο στην εικόνα όσο και στα ταμεία της εταιρίας.

Η χρήση των καταγραφών από την πραγματοποίηση των καταχωρήσεων αποτελεί ένα χρήσιμο εργαλείο για να εξεταστεί η ακρίβεια του εξαγόμενου αποτελέσματος. Στην πραγματικότητα, πρόκειται για την λεπτομερή καταγραφή όλων των αλλαγών σε ένα αρχείο το οποίο θα παρακολουθείται συνεχώς καθώς θα γίνουν οι έλεγχοι σε όλη την διαδρομή (audit trail). Κατανοούμε λοιπόν, πως οι πιθανότητες να σφάλουν οι πληροφορίες μειώνονται εν μέσω της συνεχούς παρακολούθησης (Bagranoff κ.α., 2010, σελ. 402).

3.2. Έλεγχοι στην Βάση Δεδομένων - Database Controls

Η αποστολή του ελέγχου στις βάσεις δεδομένων είναι διττή, αφενός επιχειρείται η προστασία των δεδομένων από φυσικές απειλές, όπως είναι για παράδειγμα η προβολή δεδομένων σε ανθρώπους δίχως εξουσιοδότηση που πιθανώς θα έχουν την πρόθεση να παραβιάσουν τα δεδομένα αυτά ενώ αφετέρου γίνεται η προσπάθεια για την επιφύλαξη των δεδομένων σε περίπτωση που υποστεί καταστροφές ο εξοπλισμός (Hall, 2010, σελ. 710). Γίνεται λόγος λοιπόν για ελέγχους **πρόσβασης** και **back-up** (Hall, 2010, σελ. 710; Hunton κ.α., 2004, σελ. 115), με τους δεύτερους να αποτελούν μέρος των ελέγχων της συνέχειας.

3.2.1. Έλεγχοι Πρόσβασης

Επιχειρούν να μειώσουν την ανεπιθύμητη είσοδο ανθρώπων που θέλουν να κλέψουν ή να καταστρέψουν ευαίσθητα δεδομένα (Hall, 2010, σελ. 710), όπως επίσης και να εγκαταστήσουν ιούς, σκουλήκια (worms) κ.α. στο λειτουργικό σύστημα του οργανισμού (Wang, 2017).

Σύμφωνα με τους Zhu κ.α. (2009), μία πολύ επικίνδυνη απειλή για τα δεδομένα του οργανισμού είναι οι ίδιοι οι υπάλληλοι, οι οποίοι έχουν την δυνατότητα να μεταφέρουν εκτός επιχείρησης λογιστικά δεδομένα με μεγάλη ευκολία, με ή δίχως πρόθεση. Το φαινόμενο αυτό ενδέχεται να οφείλεται και στα χαμηλά επίπεδα εκπαίδευσης των εργαζομένων ή και στην έλλειψη ενδιαφέροντος για την εταιρία (Knapp κ.α., 2006). Έρευνες έδειξαν πως η παραβίαση των μέτρων ασφαλείας και κατ' επέκταση η παράνομη είσοδος σε σημαντικά δεδομένα έχει αρνητικό αντίκτυπο για την αγορά (Ko & Dorantes, 2006). Μάλιστα, σύμφωνα με τους Kavusoglu κ.α. (2004), η παραβίαση των

αμυντικών συστημάτων οδηγεί αναπόφευκτα και σε μακροχρόνια προβλήματα για τον οργανισμό δεδομένου ότι δημιουργείται αρνητική φήμη για αυτόν τόσο στην αγορά όσο και στους συνεργάτες του. Όμως, σύμφωνα με τους Ko & Dorantes (2006) είναι πιο δύσκολο να εμφανισθούν μακροπρόθεσμου ορίζοντα προβλήματα στην ασφάλεια καθώς η ανάγκη για την αντιμετώπιση θεμάτων με μικρότερο ορίζοντα, όπως τα κόστη για επισκευές ή αγορά εξοπλισμού, υποβοηθά την ενίσχυση της άμυνας των παραπάνω προβλημάτων.

3.2.2. Έλεγχος των Προβολών στον Χρήστη

Ο διαχειριστής της βάσης δεδομένων, καθορίζει τα σύνορα πρόσβασης τα οποία έχει ο χρήστης, δηλαδή σε ποια δεδομένα έχει το δικαίωμα να εισέλθει από το σύνολο των δεδομένων που είναι στην κατοχή της βάσης δεδομένων (Hall, 2010, σελ. 710).

3.2.3. Πίνακας Εξουσιοδότησης στα Δεδομένα

Στον πίνακα αυτόν, ξεκαθαρίζονται τα δικαιώματα των χρηστών σε ότι αφορά την δράση που μπορούν να έχουν εφόσον είναι εντός της βάσης δεδομένων. Ειδικότερα, είναι πιθανό ένας χρήστης να μπορεί μόνο να διαβάσει τα δεδομένα αλλά να μην έχει δικαίωμα για να διαγράψει, να τροποποιήσει ή και να εισάγει νέα δεδομένα. Όλες οι παραπάνω ενέργειες διευκρινίζονται εν μέσω του πίνακα τούτου (Hall, 2010, σελ. 711).

3.2.4. Πιστοποίηση Χρηστών - User-defined procedures

Είναι καλό πολλές φορές να δημιουργούνται επιπρόσθετα μέτρα ασφαλείας από τους ίδιους τους χρήστες για την ενίσχυση της άμυνας. Πολλές φορές η ύπαρξη ενός κωδικού πρόσβασης δεν εγγυάται τα μέγιστα αποτελέσματα (Hall, 2010, σελ. 714), είναι καλό για παράδειγμα η συχνή αλλαγή των κωδικών προγραμματισμένα και μη. Αυτό θα δημιουργήσει εμπόδια σε οποιονδήποτε θελήσει να εισέλθει στην βάση δεδομένων και επίσης δεν θα μπορεί να βρει τα μοτίβα αλλαγής των κωδικών (the analysis and design of accounting).

3.3. Κρυπτογράφηση - Data Encryption

Η κρυπτογράφηση των δεδομένων αποτελεί ένα πολύ ισχυρό εργαλείο για την προστασία της βάσης δεδομένων και συνίσταται κυρίως για την πρόληψη ευαίσθητων δεδομένων (Wong-Steele, 2017, σελ. 42). Ειδικότερα, υπάρχουν διάφορες τεχνικές οι

οποίες χρησιμοποιούν ειδικούς αλγόριθμους οι οποίοι «ανακατεύουν» τις λέξεις και τα δεδομένα σε τέτοιο βαθμό που είναι πολύ δύσκολο για τον εισβολέα να κατανοήσει το περιεχόμενο τους. Επίσης, προφυλάσσουν τα δεδομένα και κατά την μεταφορά τους εν μέσω των διαφόρων δικτύων (Hall, 2010, σελ. 711). Γενικότερα, οι τεχνικές κρυπτογράφησης είναι κατάλληλες για την απόκρουση εισβολέων που επιχειρούν άμεση πρόσβαση στα υπολογιστικά συστήματα των οργανισμών (Wong-Steele, 2017, σελ. 42).

Για του λόγου το αληθές ο αλγόριθμος AES βραβεύθηκε και κυκλοφόρησε από την NIST το 2001, όντας μια τεχνική η οποία συνδύαζε ασφάλεια, χαμηλό κόστος αλλά και ευκολότερη εφαρμογή (NIST, 2001). Βέβαια η παρούσα τεχνική εμφανίζει αδυναμίες στην χρήση του «σύννεφου» κάτι το οποίο είναι λίγο πολύ αναμενόμενο καθώς η τεχνολογία προχωρά με ταχύτατους ρυθμούς. Για αυτό οι Huang κ.α. (2015) προτείνουν μία νέα προσέγγιση που ονομάζεται SeFEM (Secure Feedback Encryption Method), η οποία μάλιστα βάσει αναλύσεων εμφανίσθηκε να είναι πιο αποτελεσματική, πιο ευέλικτη και ασφαλής από την AES. Συνεχίζοντας, αξίζει να αναφέρουμε πως οι τεχνικές κρυπτογράφησης χωρίζονται σε δύο γενικές κατηγορίες, του ιδιωτικού κλειδιού και του δημοσίου κλειδιού (Hall, 2010, σελ. 716).

3.3.1. Κρυπτογράφηση με Ιδιωτικό Κλειδί

Για την κατανόηση της λειτουργίας αυτής της προσέγγισης θα παραθέσουμε ένα παράδειγμα με την χρήση τους AES. Αυτή η τεχνική χρησιμοποιεί ένα κλειδί το οποίο είναι κοινό για τους «συναλλασόμενους» και εμπεριέχεται μέσα στον αλγόριθμο από τον οποίο μεταφέρεται το κρυπτογραφημένο μήνυμα.

Μία άλλη τεχνική είναι η Triple – DES encryption η οποία αποτελεί μια αναβαθμισμένη μορφή της παλαιότερης τεχνικής, DES (Hall, 2010, σελ. 716), η οποία κυκλοφόρησε το 1977 (Katz & Lindell, 2008, σελ. 173).

Σύμφωνα με τον Hall (2010, σελ. 716) το εξελιγμένο μοντέλο εμφανίζεται σε δύο μορφές, EEE3 και EDE3. Από την ονομασία αντιλαμβανόμαστε ότι χρησιμοποιούνται τρία κλειδιά για την κρυπτογράφηση, αλλά με διαφορετικό τρόπο στην καθεμία. Αναλυτικότερα, στην πρώτη μορφή χρησιμοποιεί τρία διαφορετικά κλειδιά για να κρυπτογραφήσει το μήνυμα τρεις φορές, ενώ στην δεύτερη μορφή το πρώτο κλειδί κωδικοποιεί το μήνυμα και το δεύτερο κλειδί το αποκωδικοποιεί. Ωστόσο, η ύπαρξη δύο διαφορετικών κλειδιών οδηγεί σε προβλήματα στο μήνυμα, έτσι, είναι απαραίτητη η ύπαρξη ενός τρίτου κλειδιού για να αποκρυπτογραφηθεί το μήνυμα. Καταλήγοντας, το

πρόβλημα σε τούτες τις μεθόδους έγκειται στην εύκολη παραβίαση του κρυπτογραφημένου μηνύματος, καθώς ο εισβολέας μπορεί να τις παραβιάσει εφόσον δεχθεί το κλειδί από τον αποστολέα ή τον παραλήπτη.

3.3.2. Κρυπτογράφηση με Δημόσιο Κλειδί

Αποστολή αυτής της τεχνικής είναι η διασφάλιση ευαίσθητων δεδομένων μεριμνώντας για την ασφάλεια και την ιδιωτικότητα τους (Hu κ.α., 2016). Στην τεχνική αυτήν χρησιμοποιούνται δύο κλειδιά, το ένα για την κωδικοποίηση του μηνύματος και το δεύτερο για την αποκωδικοποίηση. Οι εμπλεκόμενοι διαθέτουν από ένα ιδιωτικό κλειδί το οποίο είναι απόρρητο και από ένα δημόσιο κλειδί το οποίο όπως αντιλαμβανόμαστε είναι γνωστό και χρησιμοποιείται από τον αποστολέα για την διαδικασία της κρυπτογράφησης. Ωστόσο, για να μπορέσει ο δέκτης να διαβάσει το κρυπτογραφημένο μήνυμα πρέπει να χρησιμοποιήσει το ιδιωτικό κλειδί.

Στην τεχνική του δημοσίου κλειδιού χρησιμοποιείται η μέθοδος RSA (Rivest -Shamir - Adleman) η οποία πήρε την ονομασία της από τους εφευρέτες της και πρόκειται για μία μέθοδο η οποία έχει ως αποστολή την προστασία δεδομένων τα οποία μπορεί να προέρχονται από τις πιστωτικές κάρτες των χρηστών ή από τους κωδικούς για την πρόσβαση τους στα social media (Alcantara κ.α., 2016). Η μέθοδος αυτή σε ότι αφορά την ταχύτητα της είναι πιο αργή από την DES, ωστόσο, ο Hall (2010, σελ. 716) διατυπώνει πως υπάρχει μια συνεργασία μεταξύ των δύο εργαλείων. Πιο συγκεκριμένα, η όλη διαδικασία την κρυπτογράφησης και της αποστολής πραγματοποιείται με DES, όμως, κατά την διαδικασία της μετάδοσης του μηνύματος εμφανίζεται η RSA προκειμένου να αποκρυπτογραφήσει την DES.

3.4. Βιομετρικοί Έλεγχοι

Οι βιομετρικοί έλεγχοι βασίζονται τόσο στα συμπεριφορικά όσο και στα σωματικά χαρακτηριστικά του ανθρώπου. Συμπεριφορικά χαρακτηριστικά αναφέρονται ως η υπογραφή ή ο λόγος ενώ ως σωματικό είναι, το πρόσωπο, το αποτύπωμα, η ίριδα κ.α. (Esan κ.α., 2015; Hawker, 2005, σελ. 93). Πρωταρχικά, συνηθιζόταν τέτοιου είδους έλεγχος σε δεδομένα υψηλής αξίας, καθώς το κόστος εγκατάστασης ήταν ιδιαίτερα υψηλό (Champlain, 2003, σελ. 115).

Τα χαρακτηριστικά αυτά προβάλλονται σε ειδικές συσκευές τα βιομετρικά scanners (Bagranoff κ.α., 2009, 45) τα οποία τα αποθηκεύουν στα αρχεία ασφαλείας ή σε

μία κάρτα ταυτοποίησης. Επομένως, όταν ο υπάλληλος επιθυμεί να έχει πρόσβαση σε μία βάση, τότε συγκρίνονται τα αρχεία που έχουν αποθηκευτεί με το ID στην κάρτα του (Hall, 2010, σελ. 711).

3.5. Δημιουργία Αντιγράφων Ασφαλείας - Backup Controls

Κρίνεται ζωτικής σημασίας η ύπαρξη αντιγράφων ασφαλείας των δεδομένων που κατέχει ο οργανισμός και ιδιαίτερα των ευαίσθητων δεδομένων, για τον λόγο ότι πρέπει να είναι πλήρως προετοιμασμένος σε μία ενδεχόμενη καταστροφή έτσι ώστε να μην χαθούν όλα και η ανάκτηση τους να είναι εφικτή (Hunton κ.α., 2004, σελ. 115). Επομένως, πρέπει να υιοθετηθούν πολιτικές και διαδικασίες οι οποίες θα είναι σε θέση να ανακτούν τα σημαντικά δεδομένα (Hall, 2010, σελ. 712) λαμβάνοντας υπόψιν και τον χρόνο που είναι απαραίτητος για την πλήρη επαναφορά (recovery time objective) (Landoll, 2006, σελ. 220).

Η διαδικασία δημιουργία αντιγράφων ασφαλείας αποτελείται από, τα αντίγραφα ασφαλείας της βάσης δεδομένων (database backup), την καταγραφή των συναλλαγών (transaction log), το χαρακτηριστικό checkpoint (checkpoint feature) και την μονάδα μέτρησης για την ανάκτηση, το οποίο χρησιμοποιεί τα αντίγραφα ασφαλείας για να επανεκκινήσει το σύστημα σε περίπτωση βλάβης (recovery module) (Hall, 2010, σελ. 713).

3.5.1. Αντίγραφα Ασφαλείας της Βάσης Δεδομένων - Database backup

Πρόκειται για μία αυτόματη διαδικασία η οποία υλοποιείται σε καθημερινή βάση για την δημιουργία και αποθήκευση αντιγράφων ασφαλείας (Hall, 2010, σελ. 713), στα οποία διατηρούνται οι καθημερινές συναλλαγές (incremental backup), καθιστώντας αυτομάτως την ανάκτηση τους ταχύτερη αλλά και εφικτή, διότι πάντοτε ελλοχεύουν κίνδυνοι οι οποίοι μπορεί να καταστρέψουν τα δεδομένα. Επιπλέον, ενδέχεται να εμφανισθούν διάφορες ανάγκες οι οποίες απαιτούν την ανάκτηση αρχείων τουλάχιστον επτά ημερών. Τότε, κρίνεται απαραίτητο να διατηρείται αντίγραφο ασφαλείας μίας εβδομάδος (full - time backup). Αξίζει να αναφέρουμε πως τα καθημερινά αντίγραφα ασφαλείας αποθηκεύονται σε διαφορετικά αρχεία από τα εβδομαδιαία αντίγραφα (Hunton κ.α., 2004, σελ.116) και η αποθήκευση τους πρέπει να πραγματοποιείται σε διαφορετικές τοποθεσίες οι οποίες είναι ασφαλείς και εύκολα προσβάσιμες (Landoll, 2006, σελ. 167).

Συμπληρωματικά με τα παραπάνω, η δημιουργία αντιγράφων ασφαλείας μπορεί να γίνει με την βοήθεια εξωτερικών συσκευών, όπως είναι για παράδειγμα η αντιγραφή σε

δίσκους. Αναλυτικότερα, η τεχνική ονομάζεται RAID (Redundant array of independent disks) και η λειτουργία της μπορεί να γίνει με δύο τρόπους (Landoll, 2006, σελ. 220; Hunton κ.α., 2004, σελ. 117). Η μία επιλογή είναι να αντιγραφούν τα δεδομένα σε έναν δίσκο και από εκεί και πέρα σε παραπάνω δίσκους (disk mirroring). Η δεύτερη επιλογή είναι η αντιγραφή των δεδομένων σε 3 ή 5 δίσκους σε ομάδες, δηλαδή ο κάθε δίσκος περιέχει και διαφορετικό block δεδομένων (disk striping) (Hunton κ.α. 2004, σελ. 117).

3.5.2. Καταγραφή των Συναλλαγών (transaction log) & το Χαρακτηριστικό Checkpoint (checkpoint feature)

Κάθε μία από τις συναλλαγές που πραγματοποιούνται εγγράφονται σε ένα αρχείο καταγραφής (log file) στο οποίο μπορεί να πραγματοποιηθεί ο έλεγχος και η παρακολούθηση τους.

Το χαρακτηριστικό checkpoint αναφέρεται στο σημείο κατά το οποίο σταματούν όλες οι λειτουργίες επεξεργασίας και το σύστημα βρίσκεται σε κατάσταση αδράνειας (Hall, 2010, σελ. 713).

3.5.3. Εφεδρικός Εξοπλισμός - Hardware Backup

Αφορά την ύπαρξη εφεδρικού εξοπλισμού (routers, servers) για την άμεση αντιμετώπιση πιθανών δυσλειτουργιών που μπορεί να εμφανισθούν εξαιτίας επιθέσεων (Boyce & Jennings, 2002, σελ. 142).

Σύμφωνα με τους Martinez κ.α. (2014) η λειτουργία και ο σκοπός της διαχείρισης του διαδικτύου (network management) έχει διαφοροποιηθεί καθώς τα νέα μοντέλα αναπτύσσονται υποβοηθούν την συνολική αμυντική στάση του οργανισμού απέναντι στους διαδικτυακούς εισβολείς. Επίσης, μέριμνα των οργανισμών είναι και η αντιμετώπιση των κινδύνων που προέρχονται από τα κινητά τηλέφωνα χρησιμοποιώντας τις «ρίζες εμπιστοσύνης» (roots of trust) οι οποίες ειδικεύονται στην παροχή ασφάλειας για τα δεδομένα συμμετέχοντας ενεργά στην πρόληψη για την αποφυγή παραβίασης της ακεραιότητας τους (Wong-Steele-Steele, 2017a, σελ. 32).

3.6. Μέτρα Ασφαλείας για τους Εργαζόμενους - Human Security

Σε προηγούμενο κεφάλαιο αναφερθήκαμε για τις επιθέσεις DDoS οι οποίες πλήττουν

σε μεγάλο βαθμό τα συστήματα του οργανισμού. Έτσι, είναι πολύ σημαντική η στάση η οποία επιθυμεί να κρατηθεί απέναντι σε τέτοιου είδους επιθέσεις. Αρχικά, μπορούν να χρησιμοποιηθούν εφαρμογές όπως front-end hardware, οι οποίες ελέγχουν εάν το σημείο πρόσβασης είναι επικίνδυνο η όχι (Wong-Steele-Steele, 2017b, σελ. 40). Επιπλέον, είναι εφικτός ο έλεγχος της κίνησης (traffic) είτε με την χρήση ειδικών δεικτών όπως είναι ο KCIs (Key completion indicator), ο οποίος εξειδικεύεται στην απόκρουση επιθέσεων σε περιβάλλοντα σύννεφου (Wong-Steele, 2017c, 2017, σελ. 40) ή μέσω συστημάτων όπως το IPS (Intrusion prevention system), τα οποία πρόκειται για δίκτυα τα οποία ενημερώνουν τον διαχειριστή για την ύπαρξη μολυσμένων στοιχείων (Wong-Steele, 2017, σελ. 40).

Επόμενα μέτρα που πιθανώς υιοθετούνται από τους οργανισμούς είναι το «φιλτράρισμα εισόδου» (ingress filtering) με το οποίο αναγνωρίζει τις ψεύτικες IP και ανακατευθύνει το δίκτυο προς την αυθεντική πηγή (Wong-Steele, 2017, σελ. 41). Επίσης, η τεχνική της «καθυστέρησης» (connection timeout) αποκόπτει την σύνδεση καθώς θεωρείται ύποπτη εμποδίζοντας έτσι τον DoS να λειτουργήσει επιθετικά.

Επισημαίνονται έλεγχοι και άμυνες σε προαναφερθείσες απειλές, όπως είναι το ψάρεμα (phising), το clickjacking, το malvertising και το spoofing. Είναι θεμιτό να αναφέρουμε πως και οι τρεις τεχνικές εισβολής έχουν ως κοινό παρανομαστή τον ανθρώπινο παράγοντα. Ειδικότερα, είναι πολύ σημαντικό ο οργανισμός να μεριμνήσει προκειμένου να απωθήσει τέτοιου είδους επιθέσεις. Αναλυτικότερα, η εκπαίδευση του προσωπικού και η προετοιμασία τους για την αντιμετώπιση του «ψαρέματος» κρίνεται ως ένα μέτρο υψίστης σημασίας (Wong-Steele, 2017, σελ. 45).

Στο σημείο αυτό επισημαίνεται πως η έλλειψη ενδιαφέροντος και εκπαίδευσης του προσωπικού αποτελεί έναν πολύ σημαντικό παράγοντα κατάρριψης των συστημάτων ασφαλείας. Ειδικότερα, σύμφωνα με έρευνες οι παραπάνω ελλείψεις αποτελούν την δεύτερη σημαντικότερη αιτία πίσω από την υποστήριξη από τα ανώτερα κλιμάκια (Knapp κ.α., 2006). Επιπρόσθετα, η ύπαρξη διπλού παράγοντα πιστοποίησης (two-factor authentication) αποκρούει τις προσπάθειες ψαρέματος (Wong-Steele, 2017d, σελ. 45), και μάλιστα η τεχνική αυτή μπορεί να αντιμετωπίσει πολλά είδη ψαρέματος που έχουν ως στόχο την είσοδο στο κινητό (Grzonkowski κ.α., 2011). Επιπλέον, η συχνή ενημέρωση των συστημάτων ασφαλείας και η ύπαρξη anti-virus και τείχους προστασίας συμπληρώνουν την αμυντική προσπάθεια έναντι του ηλεκτρονικού ψαρέματος (phising) (Wong-Steele, 2017, σελ. 45) αλλά και του malvertising (Wong-Steele, 2017, σελ. 44).

Για την αντιμετώπιση των επιθέσεων clickjacking στην βιβλιογραφία παρατίθενται πλήθος επιλογών. Αρχικά, μπορεί να ζητηθεί στον χρήστη να επιβεβαιώσει ξανά τα στοιχεία του (Wong-Steele, 2017, σελ. 39) ή να αλλάζει συχνά το UI (User Interface) έτσι ώστε ο εισβολέας να μην μπορεί να ανακαλύψει την σωστή τοποθεσία (Wong-Steele, 2017e, σελ. 39). Μάλιστα, και ο σχεδιασμός του interface παίζει σημαντικό ρόλο για την βελτιστοποίηση της ασφάλειας (Mohamed κ.α., 2016). Εν συνεχεία, κάποια μέτρα σχετίζονται με την εικόνα και τον δείκτη του ποντικιού του χρήση. Πιο συγκεκριμένα, ο χρήστης μπορεί να παρατηρήσει ένα πάγωμα στην οθόνη του (freeze screen) ή καθυστέρηση στην φόρτωση για να τον αποτρέψει από το click σε ανεπιθύμητα κουμπιά, ενώ ακόμη ενδέχεται να συναντήσει αδυναμία επιλογής, δηλαδή, το πρώτο κλικ δεν είναι έγκυρο και επομένως δεν θα ανοίξει νέο σύνδεσμο, σε αντίθεση με το δεύτερο κλικ το οποίο θα δώσει την έγκριση (Wong-Steele-Steele, 2017f, σελ. 39).

Αναφορικά με τις επιθέσεις spoofing, μπορούν να παρθούν μέτρα τα οποία σχετίζονται με τον τρόπο σύνδεσης στον οργανισμό. Για του λόγου το αληθές στις ασύρματες συνδέσεις χρησιμοποιούντα εφαρμογές WSN (wireless sensors network) (Yilmaz & Arslan, 2015) ή με εφαρμογές HTTPD οι οποίες ανατρέχουν στον web server ελέγχουν όλες τις αιτήσεις που γίνονται από τον οργανισμό την ώρα της περιήγησης (Gupta & Gola, 2016). Επιπλέον, η ύπαρξη proxy server σε πολλούς περιηγητές αποτελεί ένα μέτρο αντιμετώπισης των επιθέσεων τούτων ελέγχοντας τα URL και την HTTP. Καταλήγοντας, δεν θα μπορούσε να λείπει η εκπαίδευση και η προσωπική προσπάθεια για την ανάληψη μέτρων έναντι του spoofing. Ειδικότερα, προτείνεται οι χρήστες να μην αποθηκεύουν το όνομα χρήστη και τον κωδικός πρόσβασης, να πραγματοποιούν περιήγηση από διαφορετικά μέσα κάθε φορά (Mozilla, Chrome κ.α.) ενώ παράλληλα να μεριμνούν, κλείνοντας τις εφαρμογές πριν ξεκινήσουν μία νέα διαδικασία (Wong-Steele-Steele, 2017, σελ. 47).

Κεφάλαιο 4

Πρωτογενής Έρευνα

4.1.Συγκέντρωση Πρωτογενών Στοιχείων

4.1.1 Μονάδα Δειγματοληψίας

Αποτέλεσε ο εν ενεργεία επαγγελματίας που εργάζεται στην Ελλάδα.

4.1.2 Μέθοδος Δειγματοληψίας

Η μέθοδος δειγματοληψίας που εφαρμόσθηκε ήταν αυτή της κρίσεως.

4.1.3 Μέγεθος του Δείγματος

Το μέγεθος του δείγματος ορίσθηκε στα 136 άτομα.

4.1.4 Πλάνο Δειγματοληψίας

Η ερευνητική ομάδα προσέγγιζε τα άτομα του δείγματος ηλεκτρονικά καθώς το ερωτηματολόγιο δημιουργήθηκε με την χρήση της πλατφόρμας google docs. Έτσι, το ερωτηματολόγιο αποστελλόταν απευθείας μέσω των social media (facebook ή linkedin) σε άτομα τα οποία γνωρίζαμε πως πληρούσαν τα κριτήρια προκειμένου να μπορούν να συμπεριληφθούν στο δείγμα. Επιπλέον, το ερωτηματολόγιο στάλθηκε και στα προσωπικά e-mails των επαγγελματιών κατ' όπιν δικού τους αιτήματος. Ωστόσο, για την αποφυγή σφαλμάτων, οι ερωτηθέντες γνώριζαν πως μπορούσαν να εκφράσουν οποιαδήποτε απορία, αποσκοπώντας στην βελτίωση της ποιότητας των απαντήσεων τους. Συνολικά, τα ερωτηματολόγια που στάλθηκαν ξεπερνούν τα 250, ενώ απαντήθηκαν 140. Έπειτα, η ερευνητική ομάδα προχώρησε στον έλεγχο των ερωτηματολογίων. Από αυτήν την διαδικασία, 4 (τέσσερα) ερωτηματολόγια κρίθηκαν άκυρα καθώς δεν είχαν συμπληρωθεί ορθά ή τα άτομα που τα συμπλήρωσαν δεν πληρούσαν τα κριτήρια για να συμπεριληφθούν στο τελικό δείγμα. Για την ανάλυση των δεδομένων χρησιμοποιήθηκαν δύο λογισμικά. Σε πρώτη φάση, χρησιμοποιήθηκε το excel για την μορφοποίηση και τον έλεγχο των

δεδομένων, ενώ η τελική ανάλυση των συχνοτήτων και των διασταυρώσεων υλοποιήθηκε με την χρήση του SPSS. Τέλος, συμπληρώνεται πως η διαδικασία συμπλήρωσης των ερωτηματολογίων διήρκησε 30 ημέρες.

4.2. Κωδικοποίηση των Μεταβλητών στο SPSS

1. Όσον αφορά την ερώτηση για χρησιμοποίηση AIS από την επιχείρηση χρησιμοποιήθηκε η μεταβλητή **XRHSH.**
2. Όσον αφορά την ερώτηση για το ποιοι έχουν πρόσβαση στο AIS χρησιμοποιήθηκε η μεταβλητή **PROSBASH.**
3. Όσον αφορά την ερώτηση για την παροχή ή όχι online υπηρεσιών από το AIS χρησιμοποιήθηκε η μεταβλητή **ONLINE.**
4. Όσον αφορά την ερώτηση για τον τρόπο καταγραφής δεδομένων από τον οργανισμό χρησιμοποιήθηκε η μεταβλητή **KATAGRAFH.**
5. Όσον αφορά την ερώτηση για το αν έχει υποστεί επεξεργασία ή όχι το erp χρησιμοποιήθηκε η μεταβλητή **LOGISMIKO.**
6. Όσον αφορά την ερώτηση για τους τρόπους μεταφοράς λογιστικών δεδομένων εντός του οργανισμού χρησιμοποιήθηκαν οι μεταβλητές **METAFORA1**, **METAFORA2**.
7. Όσον αφορά την ερώτηση για την φιλικότητα του AIS ως προς τον χρήστη χρησιμοποιήθηκε η μεταβλητή **FILIKOTHTA**.
8. Όσον αφορά την ερώτηση για την ευκολία στην χρήση του AIS ως προς τον χρήστη χρησιμοποιήθηκε η μεταβλητή **EUKOLO.**
9. Όσον αφορά την ερώτηση για την ταχύτητα AIS χρησιμοποιήθηκε η μεταβλητή **TAXYTHTA.**
10. Όσον αφορά την ερώτηση για την αποτελεσματικότητα αναφορών χρησιμοποιήθηκε η μεταβλητή **REPORTS.**
11. Όσον αφορά την ερώτηση για την επίγνωση της διοίκησης για τους κινδύνους χρησιμοποιήθηκε η μεταβλητή **EPIGNWSH.**
12. Όσον αφορά την ερώτηση για το ενδιαφέρον της διοίκησης για θέματα ασφαλείας χρησιμοποιήθηκε η μεταβλητή **ENDIAFERON.**
13. Όσον αφορά την ερώτηση για την σημασία ύπαρξης backup χρησιμοποιήθηκε η μεταβλητή **BACKUP.**

14. Όσον αφορά την ερώτηση για την αλλαγή κωδικών ανά τακτά χρονικά διαστήματα χρησιμοποιήθηκε η μεταβλητή **PASSWORDS.**
15. Όσον αφορά την ερώτηση για την πραγματοποίηση εκπαιδευτικών προγραμμάτων σε θέματα ασφαλείας χρησιμοποιήθηκε η μεταβλητή **TRAIN.**
16. Όσον αφορά την ερώτηση για την επάρκεια προγραμμάτων εκπαίδευσης χρησιμοποιήθηκε η μεταβλητή **EPARKEIA.**
17. Όσον αφορά την ερώτηση για τις απειλές που έχει δεχθεί ο οργανισμός χρησιμοποιήθηκαν οι μεταβλητές **APEILH1, APEILH2**.
18. Όσον αφορά την ερώτηση για τις απειλές που έχει δεχθεί ο οργανισμός από το εσωτερικό του χρησιμοποιήθηκαν οι μεταβλητές **ESWTERIKO1, ESWTERIKO2, ESWTERIKO3.**
19. Όσον αφορά την ερώτηση για ηλεκτρονικές απειλές που έχει δεχθεί ο οργανισμός χρησιμοποιήθηκαν οι μεταβλητές **EATTACK1, EATTACK2, EATTACK3.**
20. Όσον αφορά την ερώτηση για το φύλο χρησιμοποιήθηκε η μεταβλητή **FYLO.**
21. Όσον αφορά την ερώτηση για την ηλικιακή ομάδα χρησιμοποιήθηκε η μεταβλητή **AGE.**
22. Όσον αφορά την ερώτηση για την εμπειρία στην παρούσα θέση χρησιμοποιήθηκε η μεταβλητή **EMPEIRIA.**
23. Όσον αφορά την ερώτηση για την εμπειρία στην παρούσα θέση, στην παρούσα εταιρία χρησιμοποιήθηκε η μεταβλητή **ETAIRIA.**
24. Όσον αφορά την ερώτηση για τον τίτλος θέσης χρησιμοποιήθηκε η μεταβλητή **TITLOS.**
25. Όσον αφορά την ερώτηση για το μέγεθος οργανισμού χρησιμοποιήθηκε η μεταβλητή **MEGETHOS.**
26. Όσον αφορά την LIKERT σχετικά με την λειτουργικότητα του AIS χρησιμοποιήθηκε η μεταβλητή **Xrhsh_logismikou.**
27. Όσον αφορά την LIKERT, αναφορικά με το ενδιαφέρον της διοίκησης σε θέματα ασφαλείας χρησιμοποιήθηκε η μεταβλητή **Asfaleia_dioikisi.**

4.3. Πίνακες Μονής Εισόδου

Πίνακας 3: Χρησιμοποιούν Λογιστικό Πληροφοριακό Σύστημα;

		Frequency	Percent	Valid percent	Cumulative Percent
Valid	Ναι	129	94,9	94,9	94,9
	Όχι	7	5,1	5,1	**100,0**
	Total	**136**	**100,0**	**100,0**	

Στον παραπάνω πίνακα οι επαγγελματίες ερωτήθηκαν για το αν χρησιμοποιούν λογιστικό πληροφοριακό σύστημα στον οργανισμό στον οποίο εργάζονται. Πιο συγκεκριμένα, το 95% (129/136) απάντησε θετικά στην παραπάνω ερώτηση ενώ μόλις το 5% (7/136) απάντησε «όχι».

Πίνακας 4: Ποιοι χρήστες έχουν πρόσβαση στο λογιστικό πληροφοριακό σύστημα

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Εσωτερικούς χρήστες	78	57,4	60,5	60,5
	Και τα δύο	51	37,5	39,5	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Στην ερώτηση για τους χρήστες που έχουν πρόσβαση στο λογιστικό πληροφοριακό σύστημα, η πλειοψηφία (60,5%) δήλωσε πως μόνο εσωτερικοί χρήστες έχουν πρόσβαση, ενώ το υπόλοιπό ποσοστό (39,5%) δήλωσε πως πρόσβαση στο AIS έχουν τόσο εσωτερικοί όσο και εξωτερικοί χρήστες.

Πίνακας 5: Παροχή online υπηρεσιών από το Λογιστικό Πληροφοριακό Σύστημα

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	89	65,4	69,0	69,0
	Όχι	40	29,4	31,0	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Στην ερώτηση 3, οι επαγγελματίες κλήθηκαν να απαντήσουν για το αν το λογιστικό πληροφοριακό σύστημα, τους παρέχει Online υπηρεσίες. Καταφατικά απάντησε το μεγαλύτερο ποσοστό από αυτούς (69%), ενώ το 31% (40/136) έδωσε αρνητική απάντηση.

Πίνακας 6: Τρόπος καταγραφής δεδομένων από τον οργανισμό

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Χειρωνακτική καταγραφή δεδομένων	8	5,9	6,2	6,2
	Ατομικές βάσεις δεδομένων για το κάθε ξεχωριστό τμήμα του οργανισμού	11	8,1	8,5	14,7
	Κοινή βάση δεδομένων εντός του οργανισμού	34	25,0	26,4	41,1
	Ενοποίηση των ξεχωριστών αρχείων αποθήκευσης	1	,7	,8	41,9
	Χρήση συστήματος ERP	75	55,1	58,1	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Στον παραπάνω πίνακα εμφανίζονται οι τρόποι με τους οποίους καταγράφονται τα λογιστικά δεδομένα. Ειδικότερα, το μεγαλύτερο ποσοστό (58,1%) δήλωσε πως χρησιμοποιεί κάποιο ERP σύστημα ενώ το 26% απάντησε πως χρησιμοποιεί μία κοινή βάση δεδομένων. Άξιο αναφοράς είναι το γεγονός πως 6% δήλωσε πως καταγράφουν τα δεδομένα με τον παραδοσιακό τρόπο.

Πίνακας 7: Κατάσταση αγοράς ERP συστήματος, με ή χωρίς τροποποίηση;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Έχει αγοραστεί	27	19,9	33,3	33,3
	Custom	54	39,7	66,7	**100,0**
	Total	81	59,6	**100,0**	
Missing	System	55	40,4		
Total		**136**	**100,0**		

Στην ερώτηση 5 απάντησαν μόνο όσοι δήλωσαν πως χρησιμοποιούν σύστημα ERP. Το 33,3% (27/81) δήλωσε πως το σύστημα ERP αγοράστηκε δίχως τροποποιήσεις ενώ το 66,7% (54/81) δήλωσε πως πραγματοποιήθηκαν τροποποιήσεις πριν την αγορά προκειμένου να ταιριάζει στα χαρακτηριστικά του οργανισμού.

Πίνακας 8: Μεταφορά δεδομένων από τον οργανισμό

		Responses		Percent of Cases
		N	Percent	
Valid	WAN	8	5,1%	6,2%
	LAN	55	35,0%	42,6%
	CLOUD	14	8,9%	10,9%
	Wireless	14	8,9%	10,9%
	Server	65	41,4%	50,4%
	Άλλο	1	0,6%	0,8%
Total		**157**	**100,0%**	**121,7%**

Στην 6η ερώτηση, οι επαγγελματίες ερωτήθηκαν για τον τρόπο με τον οποίο αποστέλλουν τα λογιστικά δεδομένα εντός του οργανισμού. Ειδικότερα το μεγαλύτερο ποσοστό αυτών (41,4%), δήλωσε πως κατέχουν έναν κεντρικό server ενώ αμέσως μετά το 35% δήλωσε πως χρησιμοποιούν LAN δίκτυο. Στην συνέχεια από 8,9% συγκέντρωσαν οι απαντήσεις Cloud systems καθώς και η wireless σύνδεση.

Πίνακας 9: Φιλικότητα του λογισμικού ως προς τους χρήστες

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Διαφωνώ	3	2,2	2,3	2,3
	Ούτε συμφωνώ/Ούτε διαφωνώ	16	11,8	12,4	14,7
	Συμφωνώ	80	58,8	62,0	76,7
	Συμφωνώ πολύ	30	22,1	23,3	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Σχετικά με το πόσο φιλικό είναι το περιβάλλον του software για τους χρήστες, οι περισσότεροι ερωτηθέντες δήλωσαν ευχαριστημένοι από το AIS (85,3%) ενώ μόλις 2,3% δήλωσε δυσαρεστημένο από το λογισμικό.

Πίνακας 10: Ευκολία στην χρήση του λογισμικού

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Διαφωνώ πολύ	1	,7	,8	,8
	Διαφωνώ	3	2,2	2,3	3,1
	Ούτε συμφωνώ/Ούτε διαφωνώ	17	12,5	13,2	16,3
	Συμφωνώ	80	58,8	62,0	78,3
	Συμφωνώ πολύ	28	20,6	21,7	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Αναφορικά με την ευκολία στην χρήση του, το 83,7% απάντησε θετικά ενώ μόλις το 3,1% δήλωσε δυσαρεστημένο.

Πίνακας 11: Εκτίμηση ταχύτητας του λογισμικού

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Διαφωνώ πολύ	2	1,5	1,6	1,6
	Διαφωνώ	9	6,6	7,0	8,5
	Ούτε συμφωνώ/Ούτε διαφωνώ	23	16,9	17,8	26,4
	Συμφωνώ	74	54,4	57,4	83,7
	Συμφωνώ πολύ	21	15,4	16,3	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Σχετικά με την ταχύτητα του λογιστικού πληροφοριακού συστήματος, το μεγαλύτερο ποσοστό του δείγματος (73,7%) έδειξε θετική στάση ενώ μόλις το 7,6% δήλωσε δυσαρεστημένο από τις επιδόσεις του.

Πίνακας 12: Επάρκεια των αναφορών του λογισμικού

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Διαφωνώ πολύ	2	1,5	1,6	1,6
	Διαφωνώ	10	7,4	7,8	9,3
	Ούτε συμφωνώ/Ούτε διαφωνώ	22	16,2	17,1	26,4
	Συμφωνώ	70	51,5	54,3	80,6
	Συμφωνώ πολύ	25	18,4	19,4	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Το 73,7% των ερωτηθέντων δήλωσε πως οι αναφορές του συστήματος είναι ικανοποιητικές ενώ μόλις το 9,4% είχε αντίθετη γνώμη.

15,69

4 6 8 12 16 **20**

7,2 10, 13, 16,

Από το παραπάνω σχήμα κατανοούμε πως οι ερωτηθέντες έχουν θετική γνώμη αναφορικά με την χρηστικότητα του πληροφοριακού συστήματος που χρησιμοποιεί ο οργανισμός στον οποίο εργάζονται.

Πίνακας 13: Compute από την Likert σχετικά με την λειτουργικότητα του AIS

	N	Minimum	Maximum	Mean	Std. Deviation
Xrhsh_logismikou	129	6,00	20,00	15,6977	2,46730

Πίνακας 14: Επίγνωση διοίκησης για τους κινδύνους

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Διαφωνώ πολύ	2	1,5	1,6	1,6
	Διαφωνώ	22	16,2	17,1	18,6
	Ούτε συμφωνώ/Ούτε διαφωνώ	39	28,7	30,2	48,8
	Συμφωνώ	47	34,6	36,4	85,3
	Συμφωνώ πολύ	19	14,0	14,7	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Στον παραπάνω πίνακα, εμφανίζονται τα ποσοστά για την ερώτηση σχετικά με την επίγνωση της διοίκησης για τους κινδύνους που ελλοχεύουν. Ειδικότερα, το 51,1% υποστηρίζει πως η διοίκηση του οργανισμού είναι ενήμερη για τους κινδύνους ενώ το 18,7% πιστεύει το αντίθετο.

Πίνακας 15: Σημασία ύπαρξης back - up

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Διαφωνώ πολύ	1	,7	,8	,8
	Διαφωνώ	2	1,5	1,6	2,3
	Ούτε συμφωνώ/Ούτε διαφωνώ	2	1,5	1,6	3,9
	Συμφωνώ	26	19,1	20,2	24,0
	Συμφωνώ πολύ	98	72,1	76,0	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Στον παραπάνω πίνακα φαίνεται πως το 96,2% δήλωσε πως είναι σημαντική η ύπαρξη back-up ενώ μόλις το 0,8% των ερωτηθέντων κατείχε, διαφορετική άποψη.

Πίνακας 16: Ενδιαφέρον της διοίκησης για την ασφάλεια του οργανισμού

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Διαφωνώ πολύ	2	1,5	1,6	1,6
	Διαφωνώ	9	6,6	7,0	8,5
	Ούτε συμφωνώ/Ούτε διαφωνώ	26	19,1	20,2	28,7
	Συμφωνώ	52	38,2	40,3	69,0
	Συμφωνώ πολύ	40	29,4	31,0	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Παραπάνω φαίνεται πως το 71,3% πιστεύει πως ο οργανισμός στον οποίο εργάζεται δηλώνει έμπρακτο ενδιαφέρον για τους κινδύνους εν αντιθέσει με το 8,6% να διαφωνεί.

Πίνακας 17: Αλλαγή κωδικών πρόσβασης σε τακτά χρονικά διαστήματα

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Διαφωνώ πολύ	2	1,5	1,6	1,6
	Διαφωνώ	5	3,7	3,9	5,4
	Ούτε συμφωνώ/Ούτε διαφωνώ	21	15,4	16,3	21,7
	Συμφωνώ	50	36,8	38,8	60,5
	Συμφωνώ πολύ	51	37,5	39,5	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Στον παραπάνω πίνακα η συντριπτική πλειοψηφία 78,3% θεωρεί πως οι κωδικοί πρόσβασης πρέπει να αλλάζουν συχνά ενώ το 5,5% κατέχει αρνητική στάση.

16,17

4 6 8 12 16 **20**

7,2 ***10,*** ***13,*** ***16,***

Από το παραπάνω σχήμα γίνεται αντιληπτό πως οι περισσότερες απαντήσεις σχετικά με την ύπαρξη ενδιαφέροντος της διοίκησης του οργανισμού αναφορικά με τους κινδύνους που ελλοχεύουν, είναι θετικές.

Πίνακας 18: Compute από την Likert σχετικά με το ενδιαφέρον της διοίκησης για τους κινδύνους

	N	Minimum	Maximum	Mean	Std. Deviation
Asfaleia_dioikisi	129	6,00	20,00	16,1783	2,38959

Πίνακας 19: Πραγματοποίηση ή μη, εκπαιδευτικών προγραμμάτων για θέματα ασφαλείας

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	42	30,9	32,6	32,6
	Όχι	87	64,0	67,4	**100,0**
	Total	129	94,9	**100,0**	
Missing	System	7	5,1		
Total		**136**	**100,0**		

Στην 15η ερώτηση, οι επαγγελματίες κλήθηκαν να δηλώσουν για το αν ο οργανισμός στον οποίο εργάζονται πραγματοποιεί προγράμματα εκπαίδευσης των εργαζομένων για θέματα ασφαλείας των λογιστικών πληροφοριακών συστημάτων. Ειδικότερα, μόλις το 32,6% απάντησε θετικά με το υπόλοιπο 67,4% να έδωσε αρνητική απάντηση.

Πίνακας 20: Βαθμός επάρκειας των εκπαιδευτικών προγραμμάτων

		Frequency	Percent	Valid Percent	Cumulative Percent
	Λίγο	1	,7	2,4	2,4
	Μέτρια	16	11,8	38,1	40,5
	Πολύ	14	10,3	33,3	73,8
	Σε μεγάλο βαθμό	11	8,1	26,2	**100,0**
	Total	42	30,9	**100,0**	
Missing	System	94	69,1		
Total		**136**	**100,0**		

Από τον παραπάνω πίνακα παρατηρείται μια θετική στάση των ερωτηθέντων απέναντι στα εκπαιδευτικά προγράμματα, καθώς το 59,5% έχει πολύ θετική γνώμη για αυτά. Το 38,1% του δείγματος απάντησε μέτρια ενώ μόλις το 2,4% τα θεωρεί λίγο σημαντικά.

Πίνακας 21: Επιθέσεις που έχει κληθεί να αντιμετωπίσει ο οργανισμός

		Responses		Percent of Cases
		N	Percent	
Valid	Φυσικές καταστροφές	16	8,7%	12,4%
	Σφάλματα στα λογισμικά	52	28,4%	40,3%
	Σφάλματα ή παραλείψεις κατά την εγγραφή των λογιστικών δεδομένων	50	27,3%	38,8%
	Απάτη από το εσωτερικό του οργανισμού	5	2,7%	3,9%
	Επιθέσεις ηλεκτρονικού χαρακτήρα	28	15,3%	21,7%
	Δεν έχουν σημειωθεί επιθέσεις	30	16,4%	23,3%
	Άλλο	2	1,1%	1,6%
Total		**183**	**100,0%**	**141,9%**

Στην παραπάνω ερώτηση, οι επαγγελματίες ερωτήθηκαν για τις επιθέσεις που έχουν κληθεί να αντιμετωπίσει ο οργανισμός που εργάζονται. Πιο συγκεκριμένα, τα μεγαλύτερα ποσοστά συγκέντρωσαν τα σφάλματα στα λογισμικά ή σφάλματα κατά την εγγραφή των λογιστικών δεδομένων, με 28,4% και 27,3% αντίστοιχα. Επιπλέον, το 16,4% των ερωτηθέντων υποστήριξε πως δεν έχει δεχθεί επίθεση ενώ το 15,3% αυτών, δήλωσε πως έχουν βρεθεί θύματα ηλεκτρονικής επίθεσης.

Πίνακας 22: Εσωτερικές Απειλές

		Responses		Percent of Cases
		N	Percent	
Valid	Χωρίς πρόθεση λανθασμένη εισαγωγή δεδομένων	2	28,6%	40,0%
	Με πρόθεση λανθασμένη εισαγωγή δεδομένων	1	14,3%	20,0%
	Με πρόθεση καταστροφή δεδομένων	2	28,6%	40,0%
	Είσοδος στα δεδομένα χωρίς εξουσιοδότηση	1	14,3%	20,0%
	Υποκλοπή των κωδικών πρόσβασης	1	14,3%	20,0%
Total		**7**	**100,0%**	**140,0%**

Αναφορικά με τις απειλές που προήλθαν από το εσωτερικό του οργανισμού, από 28,6% συγκέντρωσαν οι απαντήσεις χωρίς πρόθεση λανθασμένη εισαγωγή δεδομένων και η καταστροφή δεδομένων με πρόθεση. Ενώ οι υπόλοιπες απαντήσεις συγκέντρωσαν από 14,3%.

Πίνακας 23: Απειλές ηλεκτρονικού χαρακτήρα

		Responses		Percent of Cases
		N	Percent	
Valid	Λογισμικό παρακολούθησης	8	15,7%	27,6%
	Δούρειος ίππος	12	23,5%	41,4%
	Παράνομη καταγραφή πληκτρολογίου	1	2,0%	3,4%
	Τεράστιος όγκος ασήμαντων email	21	41,2%	72,4%
	worms	5	9,8%	17,2%
	Αποτυχία εισόδου στα αρχεία και στις υπηρεσίες	3	5,9%	10,3%
	Άλλο	1	2,0%	3,4%
Total		**51**	**100,0%**	**175,9%**

Παρατηρώντας τον πίνακα 23 φαίνεται πως το 41,2% δήλωσε πως έχει πέσει θύμα spamming ενώ το 23,5% δήλωσε πως έχει κολλήσει ιό (trojan horse). Το 15,7% δήλωσε πως έχει δεχθεί επίθεση με λογισμικό παρακολούθησης ενώ το 9,8% ιό (worms). Με τις επιθέσεις DoS να αποτελούν μόλις το 5,9%.

Πίνακας 24: Φύλο

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Άνδρας	74	54,4	54,4	54,4
	Γυναίκα	62	45,6	45,6	**100,0**
	Total	**136**	**100,0**	**100,0**	

Στον παραπάνω πίνακα φαίνεται πως το 54,4% του δείγματος αποτελείται από άνδρες ενώ το 45,6% από γυναίκες.

Πίνακας 25: Ηλικιακή ομάδα

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	17	12,5	12,5	12,5
	25-34	52	38,2	38,2	50,7
	35-44	36	26,5	26,5	77,2
	45-54	23	16,9	16,9	94,1
	55 και άνω	8	5,9	5,9	**100,0**
	Total	**136**	**100,0**	**100,0**	

Αναφορικά με τις ηλικίες που πήραν μέρος στην έρευνα, το μεγαλύτερο ποσοστό συγκέντρωσαν οι 25-34 (38,2%), 26,5% οι 35-44 ενώ 16,9% οι 45-54. Τέλος, οι ηλικιακές ομάδες 18-24 και 55 και άνω συγκέντρωσαν από 12,5% και 5,9% αντίστοιχα.

Πίνακας 26: Εμπειρία στην παρούσα θέση

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-3	26	19,1	19,1	19,1
	4-7	32	23,5	23,5	42,6
	8-11	27	19,9	19,9	62,5
	12-15	15	11,0	11,0	73,5
	15 και άνω	36	26,5	26,5	**100,0**
	Total	**136**	**100,0**	**100,0**	

Στον πίνακα 26, εμφανίζονται τα χρόνια εμπειρίας που κατέχουν οι ερωτηθέντες στην παρούσα θέση. Το 26,5% δήλωσε πως εργάζεται για πάνω από 15 χρόνια ενώ το 23,5% από 4-7 χρόνια. Στην συνέχεια, το 19,9% και 19,1% από 8-11 και 1-3 χρόνια αντίστοιχα. Τέλος, το 11% εργάζεται από 12-15 χρόνια.

Πίνακας 27: Εμπειρία στην παρούσα θέση, στην παρούσα εταιρία

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-3	48	35,3	35,3	35,3
	4-7	32	23,5	23,5	58,8
	8-11	19	14,0	14,0	72,8
	12-15	13	9,6	9,6	82,4
	15 και άνω	24	16,6	16,6	**100,0**
	Total	**136**	**100,0**	**100,0**	

Στον πίνακα 27, εμφανίζονται τα χρόνια εμπειρίας που κατέχουν οι ερωτηθέντες στην παρούσα θέση, στην παρούσα εταιρία. Το 35,3% δήλωσε πως εργάζεται για 1-3 χρόνια ενώ το 23,5% από 4-7 χρόνια. Στην συνέχεια, το 16,6% και 14% για περισσότερα από 15 χρόνια και 8-11 χρόνια αντίστοιχα. Τέλος, το 9,6% εργάζεται από 12-15 χρόνια.

Πίνακας 28: Τίτλος θέσης εργασίας

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Λογιστής	57	41,9	41,9	41,9
	Βοηθός λογιστή	59	43,4	43,4	85,3
	Διευθύνων σύμβουλος	10	7,4	7,4	92,6
	Εσωτερικός ελεγκτής	7	5,1	5,1	97,8
	ΙΤ	1	,7	,7	98,5
	Άλλο	2	1,5	1,5	**100,0**
	Total	**136**	**100,0**	**100,0**	

Σχετικά με την θέση που κατείχαν τα άτομα του δείγματος, το 43,4% και το 41,9% αυτού αποτελείται από βοηθούς λογιστές και λογιστές αντίστοιχα. Το 7,4% αποτελείται από διευθυντικά στελέχη ενώ το 5,1% από εσωτερικούς ελεγκτές. Τέλος, μόλις 0,5% συγκέντρωσαν επαγγελματίες IT.

Πίνακας 29: Μέγεθος οργανισμού

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-9	66	48,5	48,5	48,5
	10-19	11	8,1	8,1	56,6
	20-49	13	9,6	9,6	66,2
	50-249	24	17,6	17,6	83,8
	250 και άνω	22	16,2	16,2	**100,0**
	Total	**136**	**100,0**	**100,0**	

Η τελευταία ερώτηση αφορούσε το μέγεθος του οργανισμού στον οποίο εργάζονται οι ερωτώμενοι. Το μεγαλύτερο ποσοστό αυτών εργάζονται σε επιχειρήσεις (48,5%) από 0-9 άτομα. Στην συνέχεια, το 17,6% και το 16,2% απάντησε πως εργάζεται σε εταιρίες με 50-249 και από 250 και άνω, αντίστοιχα. Τέλος, το 9,6% δήλωσε πως εργάζεται σε εταιρία με 20-49 άτομα προσωπικό, ενώ το 8,1% από 10-19 άτομα.

4.4. Πίνακες Διπλής Εισόδου

Πίνακας 30: Διασταύρωση μεταβλητών XRHSH και MEGETHOS

		MEGETHOS					Total
		0-9	10-19	20-49	50-249	250 και άνω	
XRHSH	Ναι	60	11	13	24	21	129
	Όχι	6	0	0	0	1	7
Total		66	11	13	24	22	136

Πίνακας 31: Test X^2 μεταβλητών XRHSH και MEGETHOS

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4,724[a]	4	**,317**
Likelihood Ratio	6,820	4	,146
Linear-by-Linear Association	2,217	1	,136
N of Valid Cases	136		

1. Έχουμε την υπόθεση μηδέν Η0: οι μεταβλητές **MEGETHOS** και **XRHSH** δεν έχουν καμία σχέση μεταξύ τους. Επιπλέον, υποθέτουμε την εναλλακτική υπόθεση Η1: Οι δύο μεταβλητές **MEGETHOS** και **XRHSH** έχουν σχέση μεταξύ τους.
2. *Η μεταβλητή **MEGETHOS** ανήκει στο τακτικό επίπεδο και η μεταβλητή **XRHSH** ανήκει στο ονομαστικό επίπεδο.*
3. Για την μέτρηση της σχέσης μεταξύ των δύο μεταβλητών χρησιμοποιούμε το test X^2.
4. Ορίζουμε ως επίπεδο σημαντικότητας 0,05 ή 5%
5. Από τον παρακάτω πίνακα διακρίνουμε <u>ότι δεν υπάρχει σχέση</u> καθώς 0,317>0,05. Επομένως δεχόμαστε την Η0.

Πίνακας 32: Διασταύρωση μεταβλητών TRAIN και MEGETHOS

		MEGETHOS					Total
		0-9	10-19	20-49	50-249	250 και άνω	
TRAIN	Ναι	19	1	5	7	10	42
	Όχι	41	10	8	17	11	87
Total		**60**	**11**	**13**	**24**	**21**	**129**

Πίνακας 33: Test X^2 μεταβλητών XRHSH και MEGETHOS

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5,282[a]	4	**,260**
Likelihood Ratio	5,815	4	,213
Linear-by-Linear Association	1,163	1	,281
N of Valid Cases	129		

1. Έχουμε την υπόθεση μηδέν Η0: οι μεταβλητές **MEGETHOS** και **TRAIN** δεν έχουν καμία σχέση μεταξύ τους. Επιπλέον, υποθέτουμε την εναλλακτική υπόθεση Η1: Οι δύο μεταβλητές **MEGETHOS** και **TRAIN** έχουν σχέση μεταξύ τους.
2. *Η μεταβλητή **MEGETHOS** ανήκει στο τακτικό επίπεδο και η μεταβλητή **TRAIN** ανήκει στο ονομαστικό επίπεδο.*
3. Για την μέτρηση της σχέσης μεταξύ των δύο μεταβλητών χρησιμοποιούμε το test X^2.
4. Ορίζουμε ως επίπεδο σημαντικότητας 0,05 ή 5%
5. Από τον παρακάτω πίνακα διακρίνουμε <u>ότι δεν υπάρχει σχέση</u> καθώς 0,260>0,05. Επομένως δεχόμαστε την Η0.

Πίνακας 34: Διασταύρωση μεταβλητών KATAGRAFH και MEGETHOS

		MEGETHOS					**Total**
		0-9	10-19	20-49	50-249	250 και άνω	
KATAGRAFH	Χειρωνακτική καταγραφή δεδομένων	4	2	1	1	0	**8**
	Ατομικές βάσεις δεδομένων για το κάθε ξεχωριστό τμήμα του οργανισμού	7	1	1	0	2	**11**
	Κοινή βάση δεδομένων εντός του οργανισμού	24	3	0	3	4	34
	Ενοποίηση των ξεχωριστών αρχείων αποθήκευσης	0	0	1	0	0	1
	Χρήση συστήματος ERP	25	5	10	20	15	75
Total		**60**	**11**	**13**	**24**	**21**	**129**

Πίνακας 35: Test X^2 μεταβλητών XRHSH και MEGETHOS

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	32,771[a]	16	**,008**
Likelihood Ratio	34,070	16	,005
Linear-by-Linear Association	11,587	1	,001
N of Valid Cases	129		

1. Έχουμε την υπόθεση μηδέν Η0: οι μεταβλητές **MEGETHOS** και **KATAGRAFH** δεν έχουν καμία σχέση μεταξύ τους. Επιπλέον, υποθέτουμε την εναλλακτική υπόθεση Η1: Οι δύο μεταβλητές **MEGETHOS** και **KATAGRAFH** έχουν σχέση μεταξύ τους.
2. *Η μεταβλητή **MEGETHOS** ανήκει στο τακτικό επίπεδο και η μεταβλητή **KATAGRAFH** ανήκει στο ονομαστικό επίπεδο.*
3. Για την μέτρηση της σχέσης μεταξύ των δύο μεταβλητών χρησιμοποιούμε το test X^2.
4. Ορίζουμε ως επίπεδο σημαντικότητας 0,05 ή 5%
5. Από τον παρακάτω πίνακα διακρίνουμε <u>ότι υπάρχει σχέση</u> καθώς 0,008<0,05. Επομένως δεχόμαστε την Η1.

Πίνακας 36: Διασταύρωση μεταβλητών FYLO και Xrhsh_logismikou

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2,416	1	2,416	,395	**,531**
Within Groups	776,793	127	6,116		
Total	**779,209**	**128**			

1. Έχουμε την υπόθεση μηδέν Η0: οι μεταβλητές **FYLO** και **Xhsh_logismikou** δεν έχουν καμία σχέση μεταξύ τους. Επιπλέον, υποθέτουμε την εναλλακτική υπόθεση Η1: Οι δύο μεταβλητές **FYLO** και **Xhsh_logismikou** έχουν σχέση μεταξύ τους.
2. *Η μεταβλητή **FYLO** ανήκει στο ονομαστικό επίπεδο και η μεταβλητή* **Xhsh_logismikou** *ανήκει στο διαστημικό επίπεδο.*
3. Για την μέτρηση της σχέσης μεταξύ των δύο μεταβλητών χρησιμοποιούμε το test ONEWAY ANOVA.
4. Ορίζουμε ως επίπεδο σημαντικότητας 0,05 ή 5%
5. Από τον παρακάτω πίνακα διακρίνουμε <u>ότι δεν υπάρχει σχέση</u> καθώς 0,531>0,05. Επομένως δεχόμαστε την Η0.

Πίνακας 37: Διασταύρωση μεταβλητών FYLO και Asfaleia_dioikisi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4,650	1	4,650	,813	**,369**
Within Groups	726,249	127	5,718		
Total	**730,899**	**128**			

1. Έχουμε την υπόθεση μηδέν Η0: οι μεταβλητές **FYLO** και **Asfaleia_dioikisi** δεν έχουν καμία σχέση μεταξύ τους. Επιπλέον, υποθέτουμε την εναλλακτική υπόθεση Η1: Οι δύο μεταβλητές **FYLO** και **Asfaleia_dioikisi** έχουν σχέση μεταξύ τους.
2. *Η μεταβλητή **FYLO** ανήκει στο ονομαστικό επίπεδο και η μεταβλητή **Asfaleia_dioikisi** ανήκει στο διαστημικό επίπεδο.*
3. Για την μέτρηση της σχέσης μεταξύ των δύο μεταβλητών χρησιμοποιούμε το test ONEWAY ANOVA.
4. Ορίζουμε ως επίπεδο σημαντικότητας 0,05 ή 5%
5. Από τον παρακάτω πίνακα διακρίνουμε ότι δεν υπάρχει σχέση καθώς 0,369>0,05. Επομένως δεχόμαστε την Η0.

Πίνακας 38: Διασταύρωση μεταβλητών MEGETHOS και Xrhsh_logismikou

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	20,770	4	5,192	,849	**,497**
Within Groups	758,440	124	6,116		
Total	**779,209**	**128**			

1. Έχουμε την υπόθεση μηδέν Η0: οι μεταβλητές **MEGETHOS** και **Xrhsh_logismikou** δεν έχουν καμία σχέση μεταξύ τους. Επιπλέον, υποθέτουμε την εναλλακτική υπόθεση Η1: Οι δύο μεταβλητές **MEGETHOS** και **Xrhsh_logismikou** έχουν σχέση μεταξύ τους.
2. *Η μεταβλητή **MEGETHOS** ανήκει στο τακτικό επίπεδο και η μεταβλητή **Xrhsh_logismikou** ανήκει στο διαστημικό επίπεδο.*
3. Για την μέτρηση της σχέσης μεταξύ των δύο μεταβλητών χρησιμοποιούμε το test ONEWAY ANOVA.
4. Ορίζουμε ως επίπεδο σημαντικότητας 0,05 ή 5%
5. Από τον παρακάτω πίνακα διακρίνουμε ότι δεν υπάρχει σχέση καθώς 0,497>0,05. Επομένως δεχόμαστε την Η0.

Πίνακας 39: Διασταύρωση μεταβλητών MEGETHOS και Asfaleia_dioikisi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	16,939	4	4,235	,736	**,569**
Within Groups	713,960	124	5,758		
Total	**730,899**	**128**			

1. Έχουμε την υπόθεση μηδέν Η0: οι μεταβλητές ***MEGETHOS*** και **Asfaleia_dioikisi** δεν έχουν καμία σχέση μεταξύ τους. Επιπλέον, υποθέτουμε την εναλλακτική υπόθεση Η1: Οι δύο μεταβλητές ***MEGETHOS*** και **Asfaleia_dioikisi** έχουν σχέση μεταξύ τους.
2. *Η μεταβλητή* ***MEGETHOS*** *ανήκει στο τακτικό επίπεδο και η μεταβλητή* **Asfaleia_dioikisi** *ανήκει στο διαστημικό επίπεδο.*
3. Για την μέτρηση της σχέσης μεταξύ των δύο μεταβλητών χρησιμοποιούμε το test ONEWAY ANOVA.
4. Ορίζουμε ως επίπεδο σημαντικότητας 0,05 ή 5%
5. Από τον παρακάτω πίνακα διακρίνουμε <u>ότι δεν υπάρχει σχέση</u> καθώς 0,569>0,05. Επομένως δεχόμαστε την Η0.

Συμπεράσματα

Ξεκινώντας, η βιβλιογραφία μας έδωσε μία εικόνα για την σημασία των λογιστικών πληροφοριακών συστημάτων, η οποία είναι υψηλή δεδομένου ότι η πληροφορία αποτελεί βασικό γρανάζι για την λήψη αποφάσεων από τα στελέχη του οργανισμού.

Τα αποτελέσματα της πρωτογενούς έρευνας έδειξαν πως το μεγαλύτερο ποσοστό των ερωτηθέντων χρησιμοποιεί λογιστικό πληροφοριακό σύστημα για την καταγραφή των λογιστικών γεγονότων (94,9%). Ωστόσο, υπάρχει ακόμη ένα μικρό ποσοστό (6,2%) το οποίο προτιμάει τον παραδοσιακό τρόπο καταγραφής των δεδομένων, ενώ το 58,1% χρησιμοποιεί σύστημα ERP, το οποίο μάλιστα έχει τροποποιηθεί για να ικανοποιεί τις ανάγκες του οργανισμού (66,7%). Τέλος, αναφορικά με το λογιστικό πληροφοριακό σύστημα, παρατηρήθηκε μία θετική στάση απέναντι στην χρηστικότητα του (15,69%).

Ωστόσο, η υψηλή σημασία τους τα καθιστά αυτομάτως σε συνεχή κίνδυνο. Ειδικότερα, από τα δευτερογενή στοιχεία γνωρίσαμε ένα μικρό ποσοστό των πιθανών κινδύνων και των επιθέσεων που μπορεί να δεχθεί ένας οργανισμός. Έτσι, είναι πάρα πολύ σημαντική η ύπαρξη σχεδίου ασφαλείας για την προφύλαξη των δεδομένων αυτών. Το γεγονός αυτό αποδεικνύεται και από την πρωτογενή έρευνα καθώς μόλις το 16,4% του δείγματος δήλωσε πως δεν έχει δεχθεί κάποια επίθεση. Σημαντικό εύρημα αποτελεί πως υψηλό ποσοστό (27,3%) δήλωσε πως έχουν υποστεί καταστροφές στα λογιστικά δεδομένα κατά την εγγραφή τους, έτσι, η ύπαρξη προγραμμάτων εκπαίδευσης των υπαλλήλων είναι πολύ σημαντική. Βέβαια, μόλις το 32,6% δήλωσε πως η επιχείρηση που εργάζονται υλοποιεί τέτοιου είδους προγράμματα, τα οποία όμως θεωρήθηκαν επαρκή. Ωστόσο, κάτι τέτοιο αντιβαίνει με τα υψηλά ποσοστά που συγκεντρώθηκαν στην ερώτηση σχετικά με το ενδιαφέρον της διοίκησης του οργανισμού για τους κινδύνους που ελλοχεύουν. Έτσι, συμπεραίνουμε πως η διοίκηση ενδιαφέρεται αλλά δεν χρησιμοποιεί τα προγράμματα εκπαίδευσης ως πρωταρχικό εργαλείο. Επιπλέον, πρέπει να τονισθεί και το υψηλό ποσοστό στην ύπαρξη επιθέσεων ηλεκτρονικού χαρακτήρα, καθώς όπως ήταν αναμενόμενο ένα σημαντικό ποσοστό δήλωσε πως έχει αντιμετωπίσει τέτοιου είδους απειλές (15,3%), με την μορφή τεράστιου όγκου ασήμαντων email (41,2%).

Στο σημείο αυτό αξίζει να αναφερθούμε στην σημασία της λειτουργικότητας του πληροφοριακού συστήματος και ειδικότερα στις αναφορές (reports). Η βιβλιογραφία τονίζει πως οι αναφορές (reports) αποτελούν ένα από τα σημαντικότερα στοιχεία που πρέπει να έχει ένα λογιστικό πληροφοριακό σύστημα καθώς δίνει την ολική εικόνα στα άτομα που είναι

επιφορτισμένα με την λήψη αποφάσεων. Σύμφωνα με τα αποτελέσματα μας, σε γενικό επίπεδο, υπάρχει θετική στάση σχετικά με την λειτουργικότητα του λογιστικού πληροφοριακού συστήματος που χρησιμοποιούν. Πιο ειδικά, περισσότερο από 70% των ερωτηθέντων υποστηρίζει πως οι αναφορές που εξάγει το λογιστικό πληροφοριακό σύστημα επαρκούν.

Κλείνοντας, οφείλει να ειπωθεί ότι τα tests δεν παρουσίασαν σχέσεις μεταξύ των μεταβλητών, παρά μόνο μεταξύ των **MEGETHOS** και **KATAGRAFH.**

Προτάσεις Προς τους Φορείς

Έπειτα από την ανάλυση των δεδομένων, η ερευνητική ομάδα είναι σε θέση να προχωρήσει στην πραγματοποίηση κάποιων προτάσεων. Αρχικά, είναι πολύ σημαντική η ύπαρξη λογιστικού πληροφοριακού συστήματος εντός του οργανισμού όπως επίσης και συστήματος ERP. Όμως, είναι σημαντικό να πραγματοποιούνται τροποποιήσεις προκειμένου να καλύπτει στον μέγιστο βαθμό τις ανάγκες του οργανισμού.

Αναφορικά με την ασφάλεια των δεδομένων του οργανισμού, θεωρούμε πως η ενημέρωση για του κινδύνους που ελλοχεύουν πρέπει να αποτελεί το πρώτο μέτρο ασφαλείας για τους οργανισμούς. Κρίνεται απαραίτητη η ύπαρξη ελέγχων στην βάση δεδομένων καθώς επίσης και στην πρόσβαση σε αυτήν. Εν συνεχεία, είναι απαραίτητη η εκπαίδευση του προσωπικού ως προς την χρήση των λογιστικών πληροφοριακών συστημάτων για την αποφυγή σφαλμάτων στην καταγραφή των δεδομένων. Επιπλέον, η εκπαίδευση θα πρέπει να εμβαθύνει και στην αντιμετώπιση των ηλεκτρονικών επιθέσεων, καθώς είναι απαραίτητο να γνωρίζουν οι εργαζόμενοι πως να κινηθούν σε περίπτωση που πέσουν θύματα τέτοιου είδους επιθέσεων. Ειδικότερα, θεωρείται δεδομένη η ύπαρξη antivirus και firewall για την προστασία από viruses. Παραδείγματος χάριν, η δημιουργία της «τεχνητής καθυστέρησης» αποκοπεί να αποκρούσει τις DoS επιθέσεις. Κλείνοντας, θεωρείται απαραίτητη η εστίαση των εταιριών στις επιθέσεις ηλεκτρονικού και ανθρώπινου χαρακτήρα, χωρίς όμως να παραγκωνίζονται τα μέτρα για άλλες μορφές επιθέσεων, καθώς όπως παρατηρήθηκε οι πηγές κινδύνου είναι πολλές.

Περιορισμοί Έρευνας

Μεθοδολογικοί

Αυτό που μας δημιούργησε το μεγαλύτερο πρόβλημα είναι το γεγονός πως λόγω της μεθόδου, ήταν δύσκολη η προσέγγιση των επαγγελματιών προκειμένου να συμπληρωθεί ο απαραίτητος αριθμός του δείγματος.

Πρακτικοί

Κατά την διάρκεια του πρακτικού μέρους της έρευνας, αντιμετωπίσαμε προβλήματα λόγω της άρνησης των επαγγελματιών να απαντήσουν στο ερωτηματολόγιο λόγω υψηλού φόρτου εργασίας.

Θεωρητικοί

Σχετικά με το θεωρητικό κομμάτι της εργασίας μας, δεν είχαμε στην διάθεση μας πολλά στοιχεία για την κατάσταση στην Ελλάδα σχετικά με τα λογιστικά πληροφοριακά συστήματα. Το κενό ήταν ακόμη μεγαλύτερο, όταν αναζητούσαμε πληροφορίες για την ασφάλεια των δεδομένων αυτών. Επιπλέον, αντιμετωπίσαμε προβλήματα με την εύρεση επιστημονικών άρθρων που δημοσιεύθηκαν τα τελευταία δύο έτη καθώς δεν είχαμε την πρόσβαση στα περισσότερα από αυτά.

Προτάσεις για Μελλοντική Έρευνα

Η ερευνητική ομάδα προτείνει την περαιτέρω διερεύνηση της ασφάλειας των λογιστικών δεδομένων στην Ελλάδα, εστιασμένη στις εταιρίες που χρησιμοποιούν cloud computing για την μεταφορά των δεδομένων τους εντός του οργανισμού. Επιπλέον, η νέα έρευνα είναι φρόνιμο να επικεντρωθεί στις επιθέσεις ηλεκτρονικού χαρακτήρα καθώς επίσης και στα σφάλματα που προκύπτουν από την έλλειψη ενημέρωσης και εκπαίδευσης του προσωπικού. Κλείνοντας, απαιτείται η διερεύνηση του βαθμού στον οποίο οι οργανισμοί πραγματοποιούν security management.

Βιβλιογραφία

Βιβλία

Bagranoff, N., Simkin, M. & Norman, C. (2010). *Core Concepts of ACCOUNTING INFORMATION SYSTEMS*. U.S.A.: John Wiley & Sons, Inc..

Boyce, J. & Jennings, D. (2002). Information Assurance - Managing Organizational IT Security Risks. U.S.A.: Elsevier Science.

Champlain, J. (2003). Auditing Information Systems. Canada: John Wiley & Sony, Inc..

Gelinas, U., Dull, R. & Wheeler, P. (2012). Accounting Information Systems. U.S.A.: Cengage Learning.

Hall, J. (2011). Accounting Information Systems 7e. U.S.A.: Cangage Learning.

Hawker, A. (2000). Security and control in information systems- A guide for a business and accounting. U.S.A.: Routledge.

Hawryszkiewycz, I. (1991). Database Analysis and Design. U.S.A.: Macmillan Publishing Company.

Hunton, J., Bryant, S. & Bagranoff, N. (2004). CORE CONCEPTS OF INFORMATION TECHNOLOGY AUDITING. U.S.A.: John Wiley & Sons, Inc..

Katz, J. & Lindell, Y. (2008). INTRODUCTION TO MODERN CRYPTOGRAPHY. US: Taylor & Francis Group, LLC.

Kechris, E. (2005). Renational Model. Athens. Kritiki Publications.

Landoll, D. (2006). The security risk assessment handbook - A complete guide for performing security risk assessments. U.S.A.: Taylor & Francis Group, LLC.

Laudon, K. & Laudon, J. (2011). Essentials of MANAGEMENT INFORMATION SYSTEMS. U.S.A.: Pearson Education, Inc..

Merkow, M. & Breithaupt, J. (2014). Information Security - Principles and practices 2ed. U.S.A.: Pearson Education, Inc..

NIST (2001). Advanced Encryption Standard (AES). *Federal Information Processing Standards Publication.* 197

Pickett, S. (2010). The internal auditing handbook. U.K.: John Wiley & Sons Ltd.

Romney, M. & Steinbart, P. (2003). ACCOUNTING INFORMATION SYSTEMS - 9th edition. New Jersey: Pearson Eduvation, Inc..

Stair, R. & Reynolds, G. (2016). Fundamentals of information systems. U.S.A.: Cengage Learning.

Stallings, W. & Brown, L. (2012). Computer Security - Principles and practice 2ed. U.S.A.: Pearson Education, Inc..

Stallings, W. & Brown, L. (2012). COMPUTER SECURITY PRINCIPLES AND PRACTICE 2E. U.S.A.: Pearsons Education, Inc.

Tilikidou, E. (2011). Research of Marketing. Thessaloniki: Sofia Publications.

Wallace, P. (2014). Πληροφοριακά συστήματα διοίκησης. Αθήνα: Εκδόσεις Κριτική ΑΕ.

Wheeler, E. (2011). Security Risk Management - Building an information security risk management program from the ground up. U.K.: Elsevier Inc.

White, J. (2014). Security Risk Assessment - Managing Physical and Operational Security. Oxford: Elsevier.

Wilkinson, J. & Cerullo, M. (1997). ACCOUNTING INFORMATION SYSTEM - ESSENTIAL CONCEPTS AND APPLICATIONS - 3rd edition. U.S.A.: John Wiley & Sons, Inc..

Wong-Steele, Y. (2017). ACCOUNTING INFORMATION SYSTEMS AND CYBER SECURITY. Florida: Astro Arpanet LLC.

Wong-Steele, Y. (2017a). ACCOUNTING INFORMATION SYSTEMS AND CYBER SECURITY. Florida: Astro Arpanet LLC. Από: Pathan A.S.K. (2011). Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, Boca Raton: CRC Press, Taylor & Francis Group

Wong-Steele, Y. (2017b). ACCOUNTING INFORMATION SYSTEMS AND CYBER SECURITY. Florida: Astro Arpanet LLC. Από: Chouhan P. and Singh R. (2016). Security Attacks on Cloud Computing with Possible Solution. International Journal of Advanced Research in Computer Sciences and Software Engineering. 6(1), pp.93-96.

Wong-Steele, Y. (2017c). ACCOUNTING INFORMATION SYSTEMS AND CYBER SECURITY. Florida: Astro Arpanet LLC. Από: Khan, M.A. (2016). A Survey of Security Issues for Could Computing, Journal of Network and Computer Applications, Elsevier, 71, pp.11-29.

Wong-Steele, Y. (2017d). ACCOUNTING INFORMATION SYSTEMS AND CYBER SECURITY. Florida: Astro Arpanet LLC. Από: Bicakci K., Unal D. and Ascioglu N. (2014). Mobile Authentication Secure Against Man-in-the-Middle Attacks.

Proceedings of 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud'2014. 7-10. April. Oxford, UK.

Wong-Steele, Y. (2017e). ACCOUNTING INFORMATION SYSTEMS AND CYBER SECURITY. Florida: Astro Arpanet LLC. Από: Nagarhalli T.P., Bakal J.W. and Jain N. (2016). A Brief Survey of Detection and Mitigation Techniques for Clickjacking and Drive-by Download Attack. International Journal of Computer Applications. 138(2). pp.44-48.

Wong-Steele, Y. (2017f). ACCOUNTING INFORMATION SYSTEMS AND CYBER SECURITY. Florida: Astro Arpanet LLC. Από: AlJarrah A. and Shehab M. (2016). Maintaining User Interface Integrity on Android. Proceedings of IEEE 40th Annual Computer Software and Applications (COMPASC'16), 10-14 June. Atlanta, Georgia.

Επιστημονικά Άρθρα

A. U and V. S. (2016). A short review on data security and privacy issues in cloud computing, *2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, Bangalore, 2016:1-5.

Abu-Musa, A. (2004). Investigating The Security Policies Of Computerized Accounting Information Systems In The Banking Industry Of An Emerging Economy: The Case Of Egypt. *The Review of Business Information Systems*. 8(4):83-102.

Abu-Musa, A. (2006). Evaluating the Security Controls of CAIS in Saudi Organizations: The Case of Saudi Arabia. *The International Journal of Digital Accounting Research,* 6(11):25-64

Alcantara, N., Cabilatzan, J., Mayugba, J. & Disu, D. (2016). On lucky primes and their application to Rivest, Shamir, and Adleman (RSA) cryptosystem. *AIP Conference Proceedings*. 1775 (1):χ.σ

Anikin, I. (2015). Information security risk assessment and management method in computer networks, *2015 International Siberian Conference on Control and Communications (SIBCON)*, Omsk.:1-5.

Dhar, S. (2012) "From outsourcing to Cloud computing: evolution of IT services", Management Research Review, Vol. 35(8):664-675.

Dhar, S. (2012a) "From outsourcing to Cloud computing: evolution of IT services", Management Research Review, Vol. 35(8):664-675. Από: Alvares, K., Chapman, T., Comerford, J., Hovey, V., Kovner, A.R., Peisch, R., Pisano, G.P. and Puryear, R.

(1995), “When outsourcing goes awry”, Harvard Business Review, 73(3):24-37.

Esan, O., Osunmakinde, I. & Ngwira, S. (2015). Perfomance Evaluation of Fingerprint Biometics Systems for e-Business Access Control. *e-Infrastructure and e-Services for Developing Countries*. 147:269-281.

Fan, Y., Zhang, Z., Trinkle, M., Dimitrovski, A., Song, J., and Li. H. (2015). A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids, in *IEEE Transactions on Smart Grid*, 6(6):2659-2668.

Fang, J. & Shu, L. (2016). Modern Accounting Information System Security (AISS) Research Based on IT Technology. *Advanced Science and Technology Letters*. 121:163-170.

Feng, N., Wang, H. & Li, M. (2014). A securit risk analysis model for information systems: Causal relationships of risk factros and vulnerability proagation analysis. *Journal of Information Sciences*. 256:57-73.

Golub, I. and Radojević., B. (2014). Information system infrastructure planning-threshold setting based on risk analysis, *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija:524-528.

Grzonkowski, S., Corcoran P. and Coughlin,T. (2011). Security analysis of authentication protocols for next-generation mobile and CE cloud services, *2011 IEEE International Conference on Consumer Electronics -Berlin (ICCE-Berlin)*, Berlin.:83-87.

Guarro, S. (1987). Principles and procedures of the LRAM approach to information systems risk analysis and management. Computers & Security. 6(6):493-504.

Gupta J. and Gola (2016) Server Side Protection Against Cross Site Request Forgery Using CSFR Gateway, Journal of Information Technology and Software. 6:128.

Hu, C., Liu, P., Zhou, Y., Guo, S., Wang, Y., & Xu, Q. (2016). Public-key encryption for protecting data in cloud system with intelligent agents against side-channel attacks. *Soft computing*. 20(12):4919-4932.

Huang, Y., Dai, C. & Leu, F. (2015). A secure data encryption method employing a sequential-logic style mechanism for a cloud system. *Int. J. Web and Grid Services*. 11(1):102-123.

Knapp, K., Marshall, T., Rainer, R. & Morrow, D. (2006). The Top Information Security Issues Facing Organizations: What Can Goverment Do to Help?. *Information Systems Security*. 15(4):51-58.

Ko, M. & Dorantes, C. (2006). THE IMPACT OF INFORMATION SECURITY BREACHES ON FINANCIAL PERFORMANCE OF THE BREACHED FIRMS: AN EMPIRICAL INVESTIGATION. *Journal of Information Technology Management*. 17(2):13-22.

Marginson, D. (2006). Information processing and management control: A note exploring the role played by information media in reducing role ambiguity. *Management Accounting Research.* 14(2):187-197.

Măzăreanu, V. (2007) Risk management and analysis: risk assessment (qualitative and quantitative), Analele Stiintifice ale Universitatii "Alexandru Ioan Cuza" din Iasi - Stiinte Economice, 54:42-46

Mihalache, A.S. (2011), Risk Analysis of Accounting Information System Infrastructur, *MPRA (Munich Personal RePEc Archive), paper 28874*

Moeti, M. and Sigama, K. (2015). Information Security Management Issues in a Cloud-based environment, *2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim)*, Cambridge, 2015:349-354.

Mohamed, M., Chakraborty, J. & Dehlinger, J. (2016). Trading off usability and security in user interface designh through mental models. *Behaviour & Information Technology*. 36(5):493-516.

Moyo, M., Abdullah, H. and Nienaber, R. (2013), "Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems," *2013 Information Security for South Africa:*1-6.

Muhrtala, T. & Ogundeji, M. (2013). Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case. *Universal Journal of Accounting and Finance*. 1(1):9-18.

Nejad, H., Movahhedinia, N. & Khayyambashi, M. (2017). Improving the reliability of wireless data communication in Smart Grid NAN. *Peer-to-peer Networking and Applications.* 10(4):1021-1033.

Park, S., Kim, Y., Jeong, S. & Hong, C. (2016). A Case Study on Effective Technique of Distributed Data Storage for Big Data Processing in the Wireless Internet Environment. Wireless Pers Commun. 86:239-253.

Rainer, R.K., JR., Snyder, C.A., Carr, H..H. (1991), Risk Analysis for Information Technology, Journal of Management Information Systems, 8:129-147.

Rainer, R.K., JR., Snyder, C.A., Carr, H..H. (1991a), Risk Analysis for Information

Technology, Journal of Management Information Systems, 8:129-147. Από: Perschke, G.A.; Karabin, S.J.; and Brock, T.L. (1986). Four steps to infonnation security. *Journal of Accountancy.* 104-111.

Rot, A., (2008). IT risk assessment: Quantitative and qualitative approach. In: the World Congress on Engineering and Computer Science (WCECS):1–6.

Rot, A., (2008a). IT risk assessment: Quantitative and qualitative approach. In: the World Congress on Engineering and Computer Science (WCECS):1–6. Από: Bialas, A. (2006). Security of information and services in modern institution and company (In Polish), WNT, Warsaw

Rot, A., (2008b). IT risk assessment: Quantitative and qualitative approach. In: the World Congress on Engineering and Computer Science (WCECS):1–6. Από: Ryba, M. (2006). Multidimensional methodology of analysis and management of IT systems risk - MIR-2m (In Polish), Doctoral thesis GH, Cracow.

Shah, J. & Murtaza, M. (2006). Information System Risk Assessment Methods, Southwest Decision Sciences Institute Thirty-Seventh Annual Conference.

Stone, R. (2016). Solving E-mail and Access Problems While Traveling; "Offsite" Backup Onsite. *IEEE Antennas & Propa gation Magazine*:114-117.

Takecian, P., Oikawa, M., Braghetto, K., Rocha, P., Lucena, F., Kavounis, K., Schlumpf, K., Acker, S., Carneiro-Proietti, A., Sabino, E., Custer, B., Busch, M. & Ferreira, J. (2013). Methodological guidelines for reducing the complexity of data warehouse development for transactional blood bank systems.*Decision Support Systems*. 55(3):728-739.

Weigand, H. & Elsas, P. (2012). Model-based auditinig using REA. *International Journal of Accounting Information Systems*. 13(3):287-310.

Weigand, H. & Elsas, P. (2012a). Model-based auditinig using REA. *International Journal of Accounting Information Systems*. 13(3):287-310. Από: Andersson B, et al. Towards a reference ontology for business models. In: Embley DW, Olivé A, Ram S, editors. Proceedings of the 25th International Conference on Conceptual Modeling. Heidelberg: Springer-Verlag; 2006:482–96. (LNCS, 4215).

Weigand, H. & Elsas, P. (2012b). Model-based auditinig using REA. *International Journal of Accounting Information Systems*. 13(3):287-310. Από: McCarthy WE. The REA accounting model: a generalized framework for accounting systems in a shared data environment. Account Rev 1982:544–77.

Yılmaz, M. and Arslan, H. (2015). A survey: Spoofing attacks in physical layer security, *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, Clearwater Beach, FL:812-817.

Zhu, Q., Li, L., Liu, J., and Xu. N., (2009). "The analysis and design of accounting information security system based on AES algorithm," *2009 International Conference on Machine Learning and Cybernetics*, Baoding:2713-2718.

Ιστοσελίδες

McDowell, M. (2009). *US-SERTI.* Διαθέσιμο σε: https://www.us-cert.gov/ncas/tips/ST04-015 (Ανακτήθηκε 18 Ιανουαρίου, 2017).

Nesbitt, S. ([χ.χ.]). *Opensource.com*. Διαθέσιμο σε: https://opensource.com/resources/top-4-open-source-erp-systems (Ανακτήθηκε 18 Ιανουαρίου, 2017).

Strategic Information Group (2003). Διαθέσιμο σε: http://www.strategic.com/blog/2013/truth-about-erp-bolt-ons/ (Ανακτήθηκε 18 Ιανουαρίου, 2017).

Πίνακες – Σχήματα

Gelinas, U., Dull, R. & Wheeler, P. (2012). Accounting Information Systems. U.S.A.: Cengage Learning.

Hall, J. (2011). Accounting Information Systems 7e. U.S.A.: Cangage Learning.

Merkow, M. & Breithaupt, J. (2014). Information Security - Principles and practices 2ed. U.S.A.: Pearson Education, Inc..

Rainer, R.K., JR., Snyder, C.A., Carr, H..H. (1991), Risk Analysis for Information Technology, Journal of Management Information Systems, 8:129-147.

Rot, A., (2008). IT risk assessment: Quantitative and qualitative approach. In: the World Congress on Engineering and Computer Science (WCECS):1–6.

Παράρτημα

Αξιότιμοι/ες κύριοι/ες,

Το παρακάτω ερωτηματολόγιο, αποτελεί μέρος της έρευνας που πραγματοποιείται στα πλαίσια της εκπόνηση της πτυχιακής μου εργασίας για την παραλαβή του πτυχίου μου, με θέμα «Κίνδυνοι και έλεγχοι των Λογιστικών Πληροφοριακών Συστημάτων στις ελληνικές επιχειρήσεις», για την σχολή διοίκησης και οικονομίας, του ΑΤΕΙ Θεσσαλονίκης.

Το παρόν ερωτηματολόγιο απαρτίζεται στο σύνολο του από 25 ερωτήσεις. Πιο συγκεκριμένα, αποτελείται από τις παρακάτω ενότητες:

- Η πρώτη ενότητα περιλαμβάνει γενικές ερωτήσεις για το λογιστικό πληροφοριακό σύστημα που χρησιμοποιείτε.
- Η δεύτερη ενότητα, αφορά την λειτουργικότητα & ασφάλεια του λογιστικού πληροφοριακού συστήματος.
- Στην τρίτη ενότητα εξετάζονται οι κίνδυνοι και οι απειλές που έχει δεχθεί ο οργανισμός.
- Η τέταρτη ενότητα περιέχει δημογραφικές ερωτήσεις.

Επίσης, θα ήθελα να σας ενημερώσω πως οι απαντήσεις του ερωτηματολογίου είναι ανώνυμες και το περιεχόμενο τους άκρως εμπιστευτικό και απόρρητο. Υπεύθυνα δηλώνω πως τα στοιχεία θα χρησιμοποιηθούν προς στατιστική και μόνο ανάλυση.

Σας ευχαριστώ εκ των προτέρων για τον χρόνο σας.

Με εκτίμηση,
Καργίδης Παναγιώτης

ΘΕΜΑ: *"Η ασφάλεια των λογιστικών πληροφοριακών συστημάτων σε επιχειρήσεις στην Ελλάδα".*

Εισαγωγικές Ερωτήσεις

1) Χρησιμοποιείτε λογιστικό πληροφοριακό σύστημα στην επιχείρησή σας;

1. Ναι O

2. Όχι O

2) Η πρόσβαση στο λογιστικό πληροφοριακό σύστημα επιτυγχάνεται από:
Μέχρι 2 απαντήσεις

2□

1. Εσωτερικούς χρήστες O

2. Εξωτερικούς χρήστες O

3. Και τα δύο O

3) Το λογιστικό πληροφοριακό σύστημα που χρησιμοποιείτε στην εταιρία σας, έχει την ικανότητα παρουσίασης των δεδομένων online;

1. Ναι O

2. Όχι O

4) Με ποιον τρόπο καταγράφετε και αποθηκεύετε τα λογιστικά δεδομένα του οργανισμού;

1. Μη αυτοματοποιημένη καταγραφή δεδομένων (Manual Processing System) O

2. Ατομικές βάσεις δεδομένων για το κάθε ξεχωριστό τμήμα του οργανισμού (Flat – file model) O

3. Κοινή βάση δεδομένων εντός του οργανισμού (Database) O

4. Ενοποίηση των ξεχωριστών αρχείων αποθήκευσης (R.E.A. model) O

5. Χρήση συστήματος ERP O

5)Αν στην ερώτηση 4 απαντήσατε «Χρήση συστήματος ERP», παρακαλούμε δηλώστε μας αν το λογισμικό έχει:

1. Έχει αγοραστεί από τον οργανισμό, χωρίς τροποποιήσεις Ο

2. Προηγήθηκαν τροποποιήσεις στο λογισμικό προκειμένου να ταιριάζει απόλυτα στα χαρακτηριστικά του οργανισμού (customization) Ο

6) Με ποιον από τους παρακάτω τρόπους σύνδεσης επιλέγετε να μεταφέρετε τα λογιστικά δεδομένα εντός του οργανισμού;
Μέχρι 2 (δύο) απαντήσεις

1. WAN (Δίκτυο ευρείας περιοχής ή ζώνης) Ο

2. LAN (Τοπικό δίκτυο) Ο

3. Cloud Systems (Υπολογιστικό νέφος) Ο

4. Wireless (Ασύρματο δίκτυο) Ο

5. Client server computing (Σύνδεση μέσω server) Ο

6. Άλλο Ο

Παρακαλούμε δηλώστε τον βαθμό συμφωνίας ή διαφωνίας με τις παρακάτω προτάσεις, οι οποίες σχετίζονται με την ασφάλεια στα λογιστικά πληροφοριακά συστήματα (AIS).

	Διαφωνώ Πολύ	Διαφωνώ	Ούτε Συμφωνώ/ Ούτε Διαφωνώ	Συμφωνώ	Συμφωνώ Πολύ	
7. Το περιβάλλον του πληροφοριακού συστήματος είναι φιλικό προς τον χρήστη	O	O	O	O	O	8□
8. Το σύστημα είναι εύκολο στην χρήση	O	O	O	O	O	9□
9. Η ταχύτητα ανάκτησης των δεδομένων είναι ικανοποιητική	O	O	O	O	O	10□
10. Οι αναφορές (reports) του συστήματος είναι ικανοποιητικές	O	O	O	O	O	11□

Παρακαλούμε δηλώστε τον βαθμό συμφωνίας ή διαφωνίας με τις παρακάτω προτάσεις, οι οποίες σχετίζονται με την ασφάλεια στα λογιστικά πληροφοριακά συστήματα (AIS).

	Διαφωνώ Πολύ	Διαφωνώ	Ούτε Συμφωνώ/ Ούτε Διαφωνώ	Συμφωνώ	Συμφωνώ Πολύ	
11. Η διοίκηση και οι υπάλληλοι έχουν πλήρη επίγνωση για τους κινδύνους που ελλοχεύουν.	Ο	Ο	Ο	Ο	Ο	12□
12. Πιστεύω ότι, η διοίκηση του οργανισμού ενδιαφέρεται πολύ για τα θέματα ασφαλείας των λογιστικών πληροφοριακών συστημάτων.	Ο	Ο	Ο	Ο	Ο	13□
13. Πιστεύω ότι, η ύπαρξη εφεδρικής βάσης δεδομένων (back – up) είναι ζωτικής σημασίας για τον οργανισμό	Ο	Ο	Ο	Ο	Ο	14□
14. Θεωρώ ότι, οι κωδικοί πρόσβασης των χρηστών, πρέπει να αλλάζουν ανά τακτά χρονικά διαστήματα	Ο	Ο	Ο	Ο	Ο	15□

15) Παρακαλούμε δηλώστε μας, αν πραγματοποιούνται προγράμματα εκπαίδευσης, σχετικά με την ασφάλεια των λογιστικών πληροφοριακών συστημάτων;

1. Ναι o 16

2. Όχι o

16) Αν στην παραπάνω ερώτηση, απαντήσατε το "1" (Ναι), παρακαλούμε δηλώστε μας τον βαθμό στον οποίο θεωρείτε πως το πρόγραμμα εκπαίδευσης είναι επαρκές.

	1	2	3	4	5
ΚΑΘΌΛΟΥ	**O**	**O**	**O**	**O**	**O**

17□

17) Παρακαλούμε επιλέξτε ποιες από τις παρακάτω απειλές έχει κληθεί να αντιμετωπίσει ο οργανισμός σας.

Μέχρι 2 (δύο) απαντήσεις

1. Φυσικές καταστροφές (πλημμύρες, σεισμοί κ.α.). o
18□

2. Σφάλματα στα λογισμικά (bugs). o
19□

3. Σφάλματα ή παραλείψεις κατά την εγγραφή των λογιστικών δεδομένων. o

4. Απάτη από το εσωτερικό του οργανισμού (υπεξαίρεση των info assets ή απάτη από τους εργαζόμενους – υψηλά κόστη). o

5. Επιθέσεις ηλεκτρονικού χαρακτήρα (hackers, virus). o

6. Δεν έχουν σημειωθεί επιθέσεις. o

7. Άλλο o

18) Αν στην παραπάνω ερώτηση επιλέξατε την απάντηση "4" (Απάτη από το εσωτερικό του οργανισμού), παρακαλούμε δηλώστε μας την μορφή των επιθέσεων απάτης που αντιμετωπίσατε.

Μέχρι 3 (τρεις) απαντήσεις

1. Εσφαλμένη εισαγωγή δεδομένων στο σύστημα (χωρίς πρόθεση) o
20□

2. Εσφαλμένη εισαγωγή δεδομένων στο σύστημα (με πρόθεση) o
21□

3. Καταστροφή δεδομένων (χωρίς πρόθεση) o
22□

4. Εκ προθέσεως καταστροφή δεδομένων o

5. Είσοδος στα δεδομένα τους συστήματος από υπαλλήλους χωρίς εξουσιοδότηση o

6. Υποκλοπή των κωδικών πρόσβασης (sharing passwords) o

7. Άλλο o

19) Αν στην ερώτηση 17 επιλέξατε την απάντηση "5" (Επιθέσεις ηλεκτρονικού χαρακτήρα), παρακαλούμε δηλώστε μας τους τύπους των ηλεκτρονικών επιθέσεων που έχει δεχθεί ο οργανισμός σας.

Μέχρι 3 (τρεις) απαντήσεις

1. Λογισμικό παρακολούθησης (spyware) o
24□

2. Δούρειος ίππος (Trojan horse) o
25□

3. Παράνομη καταγραφή οτιδήποτε πληκτρολογεί ο χρήστης (keylogger) o
26□

4. Υποδοχή τεράστιου όγκου ασήμαντων e-mail (spamming) o

5. Είσοδος στον σκληρό δίσκο και στα αρχεία του συστήματος με την χρήση σκουληκιού (worms) o

6. Αποτυχία εισόδου από τον χρήστη στα αρχεία και στις υπηρεσίες του οργανισμού (Dos) o

7. Αλλό o

Δημογραφικά Στοιχεία

20) Φύλο:

27□

1. Άνδρας o

2. Γυναικά o

21) Ηλικιακή Ομάδα:

28□

1. 18-24 o

2. 25-34 o

3. 35-44 o

4. 45-54 o

5. 55 και άνω o

22) Παρακαλούμε δηλώστε μας την εμπειρία που κατέχεται στην παρούσα θέση;

1. 1 – 3 o 29□

2. 4 – 7 o

3. 8 – 11 o

4. 12 – 15 o

5. Περισσότερα από 15 χρόνια o

23) Παρακαλούμε δηλώστε μας την εμπειρία που κατέχεται στην παρούσα θέση, στην παρούσα εταιρία.

1. 1 – 3 o 30□

2. 4 – 7 o

3. 8 – 11 o

4. 12 – 15 o

5. Περισσότερα από 15 χρόνια o

24) Παρακαλούμε δηλώστε μας τον τίτλο της θέσης που εργάζεστε.

1. Λογιστής	o	31□
2. Βοηθός λογιστή	o	
3. Διευθύνων σύμβουλος/Διευθυντής τμήματος	o	
4. Εσωτερικός ελεγκτής	o	
5. IT	o	
6. Άλλο	o	

25) Παρακαλούμε δηλώστε μας το μέγεθος του οργανισμού στον οποίον εργάζεστε.

1. 0 - 9 εργαζόμενους	o	32□
2. 10 - 19 εργαζόμενους	o	
3. 20 - 49 εργαζόμενους	o	
4. 50 - 249 εργαζόμενους	o	
5. 250 και άνω	o	

Ευχαριστούμε πολύ!