Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων
3η Εργασία

ΑΝΑΛΥΣΗ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Εισαγωγή

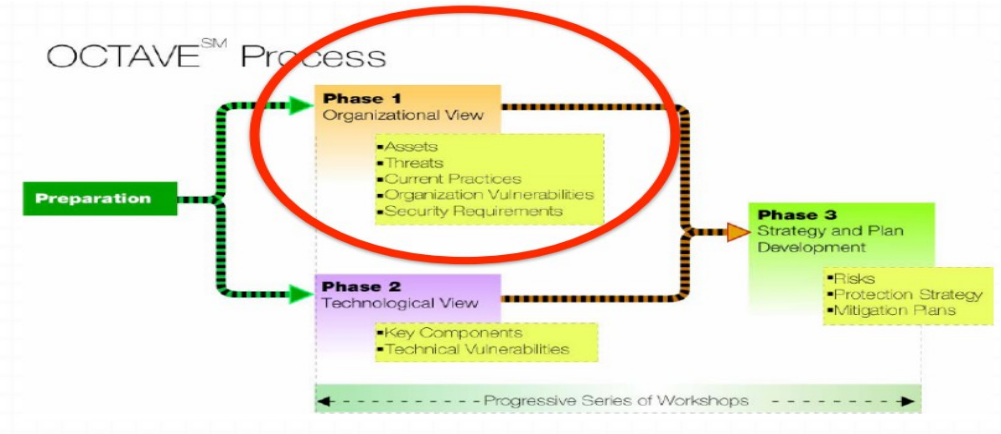
Το εννοιολογικό πλαίσιο που αποτέλεσε τη βάση της αρχικής προσέγγισης OCTAVE δημοσιεύθηκε από το Ινστιτούτο Μηχανικής (SEI) στο Πανεπιστήμιο Carnegie Mellon το 1999 (3). Σε συνεργασία με το Κέντρο Τηλεϊατρικής και Αναβαθμισμένης Τεχνολογικής Έρευνας (TATRC), η SEI ανέπτυξε τη μέθοδο OCTAVE για να αντιμετωπίσει τις προκλήσεις ασφαλείας που αντιμετώπιζε το Υπουργείο Άμυνας των ΗΠΑ (DoD), το οποίο ήθελε να διευθύνει τις προβλέψεις του HIPAA (Health Insurance Portability and Accountability Act) για την προστασία της ιδιωτικής ζωής και την ασφάλεια της προσωπικής υγείας. Από τότε που κυκλοφόρησε για πρώτη φορά το Σεπτέμβριο του 1999, υπήρξαν μια σειρά από ενημερώσεις και αλλαγές στην μεθοδολογία OCTAVE. Υπάρχουν τρεις διακριτές μεθοδολογίες OCTAVE διαθέσιμες για χρήση από το κοινό:

- OCTAVE METHOD
- OCTAVE-S
- OCTAVE ALLEGRO

Ο οργανισμός που επιλέξαμε να αναλύσουμε είναι το ***e-shop.gr***.Η συγκεκριμένη επιχείρηση είναι μια όχι τόσο μεγάλη επιχείρηση με λίγους υπαλλήλους και για αυτό χρησιμοποιείται η OCTAVE-S,καθώς οι υπάλληλοι δεν ξεπερνούν τους 100 σε όλες τις τοποθεσίες που εδράζει.Η OCTAVE-S είναι σχεδιασμένη για οργανισμούς που μπορούν να εξουσιοδοτήσουν μια ομάδα τριών έως πέντε ατόμων για τη διεξαγωγή όλων των δραστηριοτήτων αξιολόγησης, χωρίς την ανάγκη για επίσημη δραστηριότητα συλλογής δεδομένων.Μικροί οργανισμοί συχνά αναθέτουν, εν μέρει ή στο σύνολό τους, τη διατήρηση των υπολογιστικών συστημάτων τους. Για τις εταιρείες αυτές, ‘τρέχοντας’ εργαλεία αξιολόγησης, επιβαρύνουν σημαντικά τους πόρους τους. Η OCTAVE-S μπορεί να εντοπίσει την ανάγκη για αυτού του είδους τη ανάλυση.Η OCTAVE-S περιλαμβάνει επίσης μία προαιρετική, ποιοτική έκδοση των πιθανοτήτων. Απαιτεί κάποια γνώση των κινήτρων ενός ‘εχθρού’ (κατά περίπτωση), καθώς και ιστορικό των προηγούμενων περιστατικών ασφάλειας. Ενώ είναι προαιρετική αυτή η έκδοση, οι οργανισμοί πρέπει να ενδιαφέρονται να μάθουν τους τύπους των δεδομένων που θα πρέπει να συλλέξουν για να δημιουργήσουν μια αρκετά σίγουρη μέτρηση για την πιθανότητα να έχουμε κινδύνους στην ασφάλεια της πληροφορίας .

Φάση 1

Δημιουργία βασισμένων στα αγαθά προφίλ απειλών



Η πρώτη φάση είναι μια αξιολόγηση των οργανωτικών πτυχών. Κατά τη διάρκεια αυτής της φάσης η ομάδα ανάλυσης:
• καθορίζει τα κριτήρια αποτίμησης επιπτώσεων που θα χρησιμοποιηθούν αργότερα για την αξιολόγηση κινδύνων.
• προσδιορίζει σημαντικα αγαθά του οργανισμού και΄αξιολογει τις παρούσες πρακτικές ασφάλειας του οργανισμού.
• συμπληρώνει όλες τις δραστηριότητες μόνη της με τη συλλογη επιπρόσθετης πληροφορίας μόνο όταν κρίνεται απαραίτητο.
• επιλέγει τρία έως πέντε κρίσιμα αγαθά για να τα αναλύσει σε βάθος στηριζόμενη στη σχετική σημασία που έχουν για τον οργανισμό.
• καθορίζει τις προϋποθέσεις ασφάλειας καθώς και ένα προφίλ κινδύνου για κάθε κρίσιμο αγαθό.

Φάση 1- Ερωτήσεις

1.Ποιά είναι τα πιο κρίσιμα σχετικά με την πληροφορία αγαθά του οργανισμού (information related assets);

Α)Η ιστοσελίδα του συστήματος, η οποία είναι η εικόνα του και μέσω της οποίας μπορεί ο χρήστης να εγγραφεί, να αλλάξει το προσωπικό του menu κ.α.

Β)Η βάση δεδομένων, στην οποία αποθηκεύονται τα προσωπικά δεδομένα των χρηστών (όπως για παράδειγμα, το ονοματεπώνυμο,e-mail ή αριθμό κινητού τηλεφώνου, κ.ά.) αλλά και άλλες πληροφορίες .

Γ)Τα δεδομένα (ιστοσελίδα διαχείρισης), τα οποία αποθηκεύονται στον ηλεκτρονικό υπολογιστή του συστήματος . Επίσης λαμβάνεται σε αυτά και η ιστοσελίδα διαχείρισης η οποία είναι ζωτικής σημασίας για το σύστημα.

2.Τί είναι σημαντικό για κάθε κρίσιμο αγαθό;

1)Η ιστοσελίδα του ***e-shop.gr*** αποτελεί ένα σύστημα στο οποίο ο κάθε χρήστης αλλά και ο απλός επισκέπτης έχει τη δυνατότητα να παραγγείλει μέσω του διαδικτύου ό,τι χρειάζεται από μια μεγάλη γκάμα ηλεκτρονικών ειδών όπως κινητά τηλέφωνα,τηλεοράσεις,ψηφιακές μηχανές και άλλα πολλά είδη.Λαμβάνοντας υπόψη λοιπόν ότι η ιστοσελίδα είναι η εικόνα της συγκεκριμένης εταιρίας και αυτή είναι το μοναδικό μέσο παραγγελείας και λειτουργείας της εταιρίας , αυτή αποτελεί κρίσιμο αγαθό του συστήματος.

Οι απαιτήσεις ασφάλειας για την ιστοσελίδα είναι οι εξής:

Α)**Ακεραιότητα**: Δυνατότητα τροποποίησης της ιστοσελίδας αλλά και του τρόπου λειτουργίας της θα πρέπει να έχουν μόνο οι διαχειριστές της και όχι εξωτερικές οντότητες.

Β)**Διαθεσιμότητα**: Η ιστοσελίδα θα πρέπει να είναι διαθέσιμη επί εικοσιτετραώρου βάσεως και να λειτουργεί σωστά.

2)Σύμφωνα με τη διαδικασία Critical Asset Selection Worksheet της OCTAVE-s, η βάση δεδομένων αποτελεί σημαντικό αγαθό του συστήματος εφόσον η αποκάλυψή της σε μη εξουσιοδοτημένες οντότητες, η τροποποίησή της χωρίς εξουσιοδότηση, η καταστροφή της, καθώς και η διακοπή πρόσβασης – λειτουργίας της οδηγούν στη δυσλειτουργία και στη δυσφήμισή της. Η βάση δεδομένων διαθέτει ιστορικό προσπέλασης κάτι που είναι πάρα πολύ χρήσιμο όχι μόνο για την διατήρηση της ακεραιότητας της, αλλά και για την προστασία των δεδομένων που αποθηκεύονται.

<u>Οι απαιτήσεις ασφάλειας που μπορεί να παραβιαστούν είναι:</u>

Α)**Εμπιστευτικότητα**: Η πρόσβαση στη βάση δεδομένων, που έχουν μόνο οι διαχειριστές, διαβαθμίζεται με στόχο να προστατεύεται από κακόβουλες ενέργειες και να διασφαλίζεται η σωστή λειτουργία της.

Β)**Ακεραιότητα**: Δυνατότητα τροποποίησης έχουν μόνο οι διαχειριστές.

Γ)**Διαθεσιμότητα**: Βασικό πλεονέκτημα της βάσης δεδομένων είναι η διαθεσιμότητα της και η διαμοιρασμένη και ταυτόχρονη προσπέλαση των δεδομένων της.

3)Σύμφωνα με τη διαδικασία Critical Asset Selection Worksheet της OCTAVE-s, τα δεδομένα αποτελούν εξαιρετικά ουσιαστικό αγαθό του συστήματος εφόσον η αποκάλυψή τους σε μη εξουσιοδοτημένες οντότητες, η τροποποίησή τους χωρίς εξουσιοδότηση, η καταστροφή τους, καθώς και η διακοπή πρόσβασης σε αυτά οδηγούν στη δυσλειτουργία και στη δυσφήμισή του.

Γενικότερα ως δεδομένα θεωρούνται τα δεδομένα που στέλνονται στο σύστημα με κάθε παραγγελεία όπως είναι η διεύθυνση του αγοραστή,το ονοματεπώνυμο του,το τηλέφωνό του και τα λοιπά.Εκτός από αυτά όμως δεδομένα του συστήματος επίσης είναι οι τιμές των προιόντων,οι προμηθευτές,ο τρόπος αποστολής των προιόντων και η εξέλιξη των παραγγελειών.Οι διαδικασίες κατά τις οποίες εμπλέκεται μεταφορά και αποθήκευση δεδομένων είναι πάρα πολλές και για αυτό το λόγο τα δεδομένα θεωρήθηκαν από την ομάδα ανάλυσης κρίσιμο αγαθό.

<u>Το σύστημα είναι υπεύθυνο για την ομαλή μεταφορά των δεδομένων και οι βασικές συνιστώσες της ασφάλειας που οφείλει να ακολουθεί είναι οι εξής:</u>

Α)**Εμπιστευτικότητα**: Η πρόσβαση στα δεδομένα που έχει ο διαχειριστής διαβαθμίζεται με στόχο να προστατεύονται από κακόβουλες ενέργειες.

Β)**Ακεραιότητα:**Δυνατότητα τροποποίησης έχουν μόνο οι διαχειριστές.

Γ)**Διαθεσιμότητα:**Όλα τα δεδομένα πρέπει να είναι διαθέσιμα ανά πάσα ώρα και στιγμή, καθώς από τις σωστές πληροφορίες κρίνεται η εύρυθμη λειτουργία του συστήματος.

3.Ποιος ή τι αποτελεί απειλή για κάθε κρίσιμο αγαθό;

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Οι διαχειριστές της ιστοσελίδας, δηλαδή οι υπεύθυνοι του συστήματος, μπορεί από απροσεξία κατά την διαδικασία ανανέωσής της να την τροποποιήσουν με λανθασμένο τρόπο ή να διακόψουν την λειτουργία της ή να την καταστρέψουν. Έτσι λοιπόν, οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Υψηλός

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Τροποποίηση	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή
Ασφάλεια	Υψηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Ο χρηματισμός και η διαφθορά των διαχειριστών της ιστοσελίδας είναι η κύρια απειλή για το σύστημα, δεδομένου ότι η ηθελημένη τροποποίηση της ιστοσελίδας ή η διακοπή της λειτουργίας της για κάποιο χρονικό διάστημα για λόγους κέρδους ή κακόβουλης πρόθεσης προκαλεί την μη σωστή λειτουργία ή τη μη διαθεσιμότητά της και επομένως την δυσφήμιση του ***E-SHOP.*** Οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Τροποποίηση	Υψηλός
Απώλεια ή καταστροφή	Υψηλός
Διακοπή Λειτουργίας	Υψηλός

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Τροποποίηση	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή
Ασφάλεια	Υψηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από εξωτερικούς παράγοντες:

Η ύπαρξη κακόβουλων προθέσεων εξωτερικών παραγόντων μπορεί να αποτελέσει απειλή. Η παραπάνω απειλή μπορεί να προέλθει και σε αυτήν την περίπτωση από μεγάλο αριθμό επισκέψεων στην ιστοσελίδα, αλλά με οργανωμένους τρόπους και διαδικασίες. Οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Απώλεια ή καταστροφή	Μέτριος
Διακοπή Λειτουργίας	Μέτριος

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Απώλεια / Καταστροφή	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Χαμηλή
Οικονομικά	Χαμηλή	Χαμηλή
Παραγωγικότητα	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή

Β)Απειλές για τη βάση δεδομένων

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Μία από τις πιο επίφοβες μη σκόπιμες απειλές που προέρχεται από το εσωτερικό του συστήματος είναι οι διαχειριστές του συστήματος, που είναι οι ίδιοι αρμόδιοι για τη βάση δεδομένων. Και αυτό γιατί μπορούν είτε από απροσεξία ή είτε από αμέλεια να τροποποιήσουν, να αποκαλύψουν ή και να διαγράψουν τα δεδομένα της. Έτσι με απόλυτη βεβαιότητα έχουμε:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Χαμηλός (χωρίς απόλυτη βεβαιότητα)
Διακοπή Λειτουργίας	Χαμηλός

Αυτές οι απειλές μπορούν να έχουν τα ακόλουθα κόστη:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Χαμηλή	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Τα παραπάνω φέρουν τις ακόλουθες αρνητικές συνέπειες.

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εξωτερικούς παράγοντες:

Ως σκόπιμη απειλή από εξωτερικούς παράγοντες μπορεί να θεωρηθεί όταν ένας κακόβουλος χρήστης προσπαθεί με διάφορα queries και χρησιμοποιώντας για παράδειγμα SQL Injection. Κατά

τη σχεδίαση του συστήματος για να αποφευχθούν πιθανές επιθέσεις στη βάση δεδομένων, αποφασίστηκε και πραγματοποιήθηκε να μην μπορεί ο χρήστης να εισάγει μεταχαρακτήρες όπου χρησιμοποιούνται κατά κόρον σε τέτοιου είδους επιθέσεις. Έτσι με απόλυτη βεβαιότητα έχουμε:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Αυτά θα επιφέρουν ζημίες στα παρακάτω:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Ο χρηματισμός κάποιων εκ των διαχειριστών του συστήματος για την πρόσβαση στη βάση δεδομένων αποτελεί πάντα μια απειλή για το σύστημα. Παρόλα αυτά η συγκεκριμένη απειλή έχει πολύ μικρή πιθανότητα να πραγματοποιηθεί.

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Τα κόστη των επιπτώσεων παρατίθενται παρακάτω:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Χαμηλή	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Παρ'όλα αυτά για το συγκεκριμένο δεν μπορεί να είναι κανείς σίγουρος για αυτό και οι τιμές παραπάνω δεν είναι σταθερές.

Γ)Απειλές για τα δεδομένα του συστήματος

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Όσον αφορά στις εσωτερικές μη σκόπιμες απειλές, παρατηρείται ότι η αποκάλυψη, η τροποποίηση, η απώλεια / καταστροφή ή η μη διαθεσιμότητα των δεδομένων μπορούν να έχουν αρνητικές επιπτώσεις για το σύστημα.Έτσι με απόλυτη βεβαιότητα:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Μέτριος
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Μέτριος

Και αυτό θα επιφέρει ζημίες στους παρακάτω τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Χαμηλή	Υψηλή	Μέτρια
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Χαμηλή	Υψηλή	Μέτρια
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Η τελική απόφαση που λαμβάνεται μετά από τον συμψηφισμό των αποτελεσμάτων είναι ότι πρέπει να ληφθούν από τους διαχειριστές του συστήματος μέτρα, ώστε να προστατευθούν τα δεδομένα από όλες τις εσωτερικές μη σκόπιμες απειλές μέσω δικτύου.

<u>Σκόπιμες απειλές από το εσωτερικό του συστήματος:</u>

Όπως με τις μη σκόπιμες απειλές έτσι και οι σκόπιμες εξετάζονται για τις συνέπειες που αποφέρουν στην περίπτωση αποκάλυψης, τροποποίησης, απώλειας ή καταστροφής και διακοπής του συστήματος. Καθώς οι διαχειριστές είναι ενήμεροι για την πολιτική ασφάλειας που εφαρμόζεται, η πιθανότητα να συμβεί κάτι σκόπιμα είναι χαμηλή. Ο ανθρώπινος παράγοντας είναι αστάθμητος και για αυτό γίνεται όλη αυτή η διαδικασία.

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

<u>Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:</u>

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Χαμηλή	Υψηλή	Μέτρια
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Χαμηλή	Υψηλή	Μέτρια
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

<u>Μη σκόπιμες απειλές από εξωτερικούς παράγοντες:</u>

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

<u>Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:</u>

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Χαμηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Χαμηλή	Χαμηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από εξωτερικούς παράγοντες:

Ενδεχομένως κάποιος κακόβουλος χρήστης επιθυμεί να βλάψει την υπόληψη του συστήματος. Ωστόσο λόγω του μεγέθους του, μπορεί να είναι λιγότερο δύσκολο να συμβεί, αλλά αν πράγματι συμβεί κρύβει πολλές ζημίες.

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

4)Τί κάνει ήδη ο οργανισμός για την προστασία κάθε κρίσιμου αγαθό;

Ο οργανισμός τηρεί μια πολιτική ασφαλείας την οποία φροντίζει να μην την παραβιάζει και να λειτουργεί συνεχόμενα και όπως ακριβώς πρέπει.Η πολιτική ασφάλειας είναι δυναμική και προσαρμόσιμη ακολουθώντας τις εκάστοτε αλλαγές της πληροφοριακής υποδομής. Σκοπός αυτής είναι η δρομολόγηση της λήψης αποφάσεων όλων των βαθμίδων της διοίκησης,καθώς με αυτή επιτυγχάνεται η συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο,η διασφάλιση της επιχειρησιακής ικανότητας στο βαθμό που εξαρτάται από την εμπιστευτικότητα,την ακεραιότητα και τη διαθεσιμότητα πληροφοριών και επικοινωνιών αλλά επίσης διασφαλίζει και την προστασία της επένδυσης που απαιτεί η λειτουργία της ιστοσελίδας του οργανισμού.

Οδηγίες και κανόνες ασφάλειας

1.Όλο το προσωπικό οφείλεται να ενημερώνεται για την πολιτική ασφαλείας του οργανισμού.
2.Η Πολιτική Ασφάλειας του οργανισμόυ καθορίζεται με βάση την επικινδυνότητα που ενέχεται στη λειτουργία του, όπως αυτή αποτιμάται με την εκπόνηση μελέτης ανάλυσης επικινδυνότητας.
3.Το προσωπικό του οργανισμού και οι διαχειριστές της ιστοσελίδας πρέπει να συμβουλεύονται την πολιτική ασφάλειας του **E-SHOP.GR** σε κάθε απόφασή τους, που αφορά ή μπορεί να επηρεάσει, άμεσα ή έμμεσα,την ασφάλεια του.
4.Η εφαρμογή της πολιτικής ασφάλειας του οργανισμού είναι υποχρεωτική.Σε περίπτωση παραβίασης της πολιτικής,ο οργανισμός έχει το δικαίωμα να επιβάλλει κυρώσεις.

Ιστοσελίδα του οργανισμού

*****Το σημαντικότερο μειονέκτημα του συστήματος είναι ότι σε περίπτωση καταστροφής του συστήματος (πυρκαγιά, σεισμός) δεν θα υπάρχει άμεση διαθεσιμότητα όλου του συστήματος καθώς δεν υφίσταται κάποιο εφεδρικό τερματικό που να αντικαθιστά το πρωτότυπο σύστημα.

Αντιμετώπιση

Είναι επιτακτική ανάγκη για την ομαλή λειτουργία του συστήματος να υπάρχει κάποιος εφεδρικός server σε διαφορετικό κτίριο του οργανισμού όπου θα είναι πλήρως λειτουργικός σε περίπτωση που καταστραφεί το αρχικό σύστημα.

*****Σε περίπτωση πρόσβασης στο **E-SHOP.GR** από κάποιο μη εξουσιοδοτημένο χρήστη υπάρχει περίπτωση να τροποποιήσει τα δεδομένα του συστήματος και να το θέσει εκτός λειτουργίας.

Αντιμετώπιση

Προτείνεται στους διαχειριστές του συστήματος να χρησιμοποιήσουν ειδικό λογισμικό όπου κρυπτογραφεί τον κώδικα του συστήματος και παράγει κάποιο εκτελέσιμο όπου είναι δύσκολο να επέμβει κάποιος εξωτερικός παράγοντας. Έτσι διαφυλάσσεται και ο κώδικας αλλά και η λειτουργικότητα του συστήματος.

Βάση δεδομένων

*Η Β.Δ αποτελεί είναι ένα από τα πιο κρίσιμα αγαθά και για αυτό πρέπει οι διαχειριστές να του δώσουν ιδιαίτερη έμφαση. Επίσης πρέπει να τονίσουμε ότι οι Β.Δ αποτελούν συνήθη στόχο των επιτιθέμενων. Έτσι πρέπει να διασφαλιστεί ότι δεν θα υπάρχει αποκάλυψη των στοιχείων της σε περίπτωση που το λάβει κάποιος μη εξουσιοδοτημένος χρήστης.

Αντιμετώπιση

Οι διαχειριστές αντιμετωπίζουν την κατάσταση αυτή κρυπτογραφώντας την Β.Δ με ισχυρές κρυπτογραφικές μεθόδους.

*Η Β.Δ κρατείται αυτοματοποιημένα αντίγραφο ασφάλειας καθημερινά, αλλά στο ίδιο τερματικό και ενίοτε μεταφέρεται σε διαφορετικό τερματικό και σε διαφορετικό κτίριο από αυτό που στεγάζεται το σύστημα.

Αντιμετώπιση

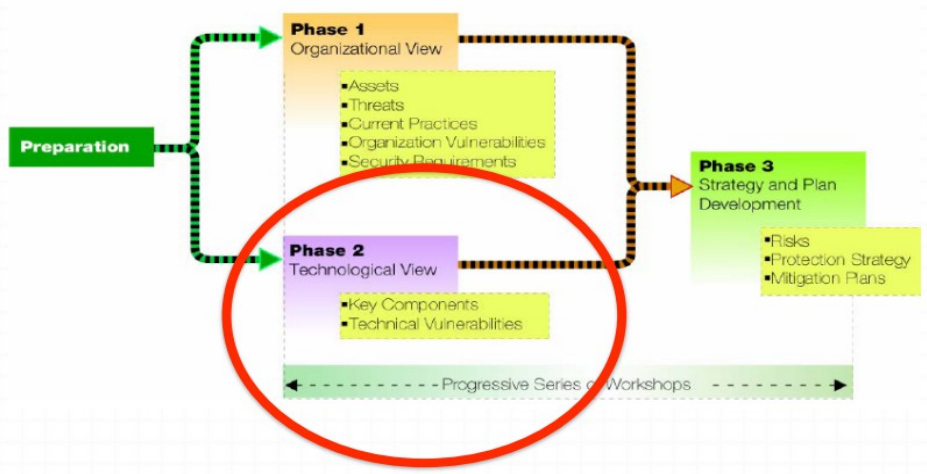
Οι διαχειριστές έχουν προγραμματίσει το σύστημα έτσι ώστε να αποστέλλεται καθημερινά και αυτοματοποιημένα backup σε διαφορετικό τερματικό και φυσικά σε άλλο κτίριο του οργανισμού.

5)Τί αδυναμίες πολιτικής και πρακτικών υπάρχουν ήδη στον οργανισμό;

Μπορεί ο οργανισμός να έχει καταφέρει να μετριάσει πολλούς από τους κινδύνους και τις επιθέσεις που δέχεται καθημερινά αλλά παρ'όλα αυτά δεν παύει να έχει ακόμα αδυναμίες.Κάποιες από αυτές τις αδυναμίες είναι οι παρακάτω:

- Ο έλεγχος των εμπορευμάτων από το προσωπικό και η σωστή διαχείριση του τιμολογίου.
- Η σωστή διαχείριση των παραγγελιών μέσω διαδικτύου και ο έλεγχος των στοιχείων κάθε πελάτη για τη μη ψευδή παραγγελία.
- Η σωστή διαχείριση των καταστατικών από όλα τα μέλη του οργανισμού για τη μη ύπαρξη μπερδέματος σε οποιονδήποτε τομέα.
- Το ποσοστό των τεχνικών της ιστοσελίδας του οργανισμού,καθώς είναι μικρό και δεν υπάρχει σωστή συνεργασία ανάμεσα στους εργαζόμενους του συγκεκριμένου τομέα.

Φάση 2



Κατά τη διάρκεια της φάσης αυτής η ομάδα ανάλυσης:
• πραγματοποιει υψηλού επιπέδου επανεξέταση των πληροφοριακών υποδομών του οργανισμού με ιδιαίτερη προσοχή στο βαθμό με τον οποίο η ασφάλεια μελετάται από τους τεχνικούς υπεύθυνους της υποδομής.
• αναλύει τον τρόπο με τον οποίο οι άνθρωποι χρησιμοποιούν τις πληροφοριακές υποδομές για να αποκτήσουν πρόσβαση σε κρίσιμα αγαθά δημιουργώντας βασικές κατηγορίες τμημάτων καθώς επίσης καθορίζοντας ποιος είναι υπεύθυνος για τη διαμόρφωση και συντήρηση αυτών των τμημάτων.
• εξετάζει το βαθμό στον οποίο κάθε υπεύθυνη πλευρά περιλαμβάνει ασφάλεια στις πληροφοριακές πρακτικές και διαδικασίες.

Φάση 2- Ερωτήσεις

1)Πως γίνεται η προσπέλαση κάθε κρίσιμου δεδομένου από τους εργαζόμενους;

Σε περιπτώσεις όπου οι κρίσιμοι πόροι είναι δύσκολο να προσδιοριστούν, οι ομάδες πρέπει να λάβουν υπόψη τους τις επιχειρηματικές λειτουργίες/τομείς εντός του οργανισμού. Αυτές μπορεί να είναι διαφορετικά έργα, ομάδες εργασίας (ομάδες ατόμων με διαφορετική περιγραφή εργασίας) ή ακόμα και ξεχωριστά οργανωτικά τμήματα (τμήμα ανθρώπινου δυναμικού, λογιστικό τμήμα, τμήμα εμπορίας, τμήμα πωλήσεων κτλ.). Στην συνέχεια, αυτοί οι πόροι πρέπει να συνταχθούν υπό την μορφή καταλόγου κατά επίπεδο σημασίας στην επιχειρηματική διαδικασία. Αφού προσδιοριστούν οι τομείς που απαιτούν διασφάλιση ή αναδιοργανωθούν οι πόροι του φορέα, το επόμενο στάδιο είναι να συνταχθούν υπό την μορφή καταλόγου όλοι οι πόροι σύμφωνα με τον αντίκτυπό τους στην επιχειρηματική διαδικασία. Ένας πιο εφικτός τρόπος για να πραγματοποιηθεί αυτό, είναι να ομαδοποιήσουμε τους πόρους κατά τμήμα ή λειτουργία οργανωτικής δομής. Ο κινητήριος μοχλός κατά τον προσδιορισμό των κρίσιμων πόρων είναι η βαρύτητα (κρισιμότητα) των πληροφοριών που επεξεργάζονται ή αποθηκεύονται από αυτόν. Μέσα από την διεξαγωγή της ανάλυσης διάσπασης, τα μέλη της ομάδας μπορούν εύκολα να προσδιορίσουν που και πως αποθηκεύονται ή χρησιμοποιούνται οι κρίσιμες πληροφορίες.

Στη συνέχεια ο προσδιορισμός και η προσπέλαση των κρίσιμων δεδομένων από τους εργαζομένους στο σύστημα γίνεται με διάφορους τρόπους καθώς κάθε τμήμα εργαζομένων έχει διαφορετική εδικότητα στον οργανισμό.

Διοίκηση

Με ένα σύγχρονο μοντέλο διοίκησης και με πλήρη καταμερισμό των αρμοδιοτήτων, η Διοίκηση είναι εκεί που χτυπά η καρδιά της εταιρείας.
Η διοίκηση χρησιμοποιεί τη βάση δεδομένων και χρησιμοποιεί τα δεδομένα για την καλύτερη ανάπτυξη,λειτουργία και διαχείριση του οργανισμού καθώς είναι το κυριότερο μέρος μιας επιχείρησης.

Τμήμα Πωλήσεων

Το Τμήμα Πωλήσεων αναλαμβάνει να προωθήσει και να έρθει σε επαφή με τους πελάτες αξιολογώντας τις βασικές τους ανάγκες ώστε να στοιχειοθετηθεί εκείνη η Οικονομική και Τεχνική Προσφορά που θα ανταποκρίνεται απόλυτα στις απαιτήσεις των πλέον απαιτητικών πελατών.
Το τμήμα πωλήσεων λοιπόν,χρησιμοποιεί την ιστοσελίδα του οργανισμού τοποθετώντας δεδομένα σε αυτή τα οποία θα προσελκύσουν περισσότερους πελάτες αλλά θα "χτυπήσουν" και τις ανάγκες αυτών όπως είναι το οικονομικό πεδίο βάζοντας προσφορές σε πολλά προιόντα.Έτσι λοιπόν το τμήμα αυτό χρησιμοποιεί την ιστοσελίδα και τα δεδομένα του οργανισμού προωθώντας τον οργανισμό και αναπτύσσοντας τον.

Τμήμα Προσωπικού

Το Τμήμα Προσωπικού είναι υπεύθυνο για την διαχείριση του ανθρωπίνου δυναμικού της εταιρείας, βρίσκεται δίπλα στους εργαζόμενους της εταιρείας για να καλύπτει τις ανάγκες τους και να επιλύει τα προβλήματά τους. Συνδράμει στην εκτέλεση των αναλαμβανομένων έργων.Οι εργαζόμενοι του συγκεκριμένου τμήματος έχουν σκοπό την προσπέλαση τιμών,κωδικών προιόντων αλλά και αποδείξεων στο σύστημα με τρόπους όπως είναι το barcode,το scanner αλλά και χειροκίνητα ούτως ώστε να τοποθετηθούν τα πάντα στη βάση δεδομένων και να είναι όλα ταξινομημένα όπως είναι αναγκαίο σε έναν τέτοιο οργανισμό.

2)Τι τύποι στοιχείων υποδομής συνδέονται με κάθε κρίσιμο δεδομένο;

Για τη μεταφορά όλων των πληροφοριών στις βάσεις δεδομένων αλλά και γενικά σε όλο το σύστημα χρησιμοποιείται ασύρματο δίκτυο με ασύρματο δρομολογητή,ευρυζωνική σύνδεση αλλά και ασύρματο προσαρμογέα για κάθε υπολογιστή του οργανισμού.Τα ασύρματα δίκτυα είναι πολύ ελκυστικά για μικρές επιχειρήσεις. Είναι ανέξοδα στην εγκατάσταση, εύκολα στην διαμόρφωση, παρέχουν ευελιξία και μετριάζουν την δυσκολία και την δαπανηρή διαδικασία καλωδίωσης.Παρακάτω είναι σημειωμένες κάποιες τεχνικές παρατηρήσεις για την ασφάλεια αυτών:

• Κάθε μετάδοση δεδομένων είναι κρυπτογραφημένη.Δεν χρησιμοποιείται κρυπτογράφηση προστασίας ασύρματου ισοδύναμης με ενσύρματη (WEP). Χρησιμοποιήται, αντί γι' αυτή, ασύρματη προστατευόμενη πρόσβαση (WPA ή WPA2).
• Χρησιμοποιούναι προ-μοιρασμένα κλειδιά (PSK) για την δημιουργία μίας μορφής συνθηματικού ανάμεσα στους υπολογιστές και τον δρομολογητή. Συνιστάται η χρήση μίας μακροσκελούς κλείδας.
• Είναι δημιουργημένη μία μοναδική ονομασία για το WiFi δίκτυο μέσω της αντίστοιχης υπηρεσίας .
• Διαμόρφωση του WiFi δρομολογητή έτσι ώστε να μην εκπέμπεται το SSID σας.
• Μη χρησιμοποίηση της προτερόθετησ ονομασία του SSID του κατασκευαστή.
• Καταχώρηση των διευθύνσεων ελέγχου πρόσβασης μέσων (MAC) των υπολογιστών του γραφείου στον δρομολογητή και δημιουργεία ενός κανόνα όπου μόνο οι καταχωρημένες διευθύνσεις MAC μπορούν να συνδιαλέγονται με αυτόν.

Στα πληροφοριακά συστήματα της εταιρείας, για την σωστή και ασφαλή εκτέλεση των λειτουργιών της, υπάρχει συνεχή στήριξη και αναβάθμιση των πληροφοριακών συστημάτων από το προσωπικό που κατέχει την απαραίτητη γνώση. Στο κτήριο της εταιρείας υπάρχει ένας μικρός αυτόνομος χώρος (computer room) όπου στεγάζονται οι τηλεπικοινωνιακές και υπολογιστικές υποδομές. Συγκεκριμένα, υπάρχει ένα κέντρο επικοινωνίας, αρκετοί κεντρικοί εξυπηρετητές (backup servers, database server, file server κ.α) στους οποίους υπάρχουν διάφορα εξειδικευμένα λειτουργικά συστήματα όπως Windows Server, Linux κ.α για την υποστήριξη των λειτουργιών της.
Ίσως το σημαντικότερο στοιχείο υποδομής είναι το κτήριο που περιέχει μόνο το σύστημα υπολογιστών των βάσεων δεδομένων.Το συγκεκριμένο είναι εδικά φτιαγμένο για να φυλάσσονται μέσα σε αυτό οι υπολογιστές που είναι αναγκαίοι για την ασφαλή λειτουργία και κράτηση της βάσης δεδομένων.Η βάση δεδομένων για τον λόγο του ότι υπάρχουν σε αυτήν τα σημαντικότερα στοιχεία του οργανισμού την καθιστά και σημαντικότερο κρίσιμο αγαθό για τον οργανισμό.Για αυτόν τον λόγο το διαφορετικό κτίριο-δωμάτιο που υπάρχει ο κύριος πυρήνας των υπολογιστών το καθιστά και σημαντικότερο στοιχείο υποδομής του οργανισμού μαζί όμως με τους υπολογιστές που είναι ξεχωριστό κομμάτι στοιχείου υποδομής.

Άρα για να καταλήξουμε στα στοιχεία υποδομής του οργανισμού,τα σημαντικότερα είναι τρία:
1.Κτίριο αποθήκευσης υπολογιστικού σύστηματος για βάση δεδομένων.
2.Υπολογιστές για τη διαχείριση και την ασφαλή λειτουργία του οργανισμού.
3.Ασύρματο δίκτυο για την ασφαλή μεταφορά δεδομένων από το ένα υπολογιστικό κομμάτι στο άλλο.

3)Σε τι βαθμό είναι ασφαλής κάθε υποδομή;

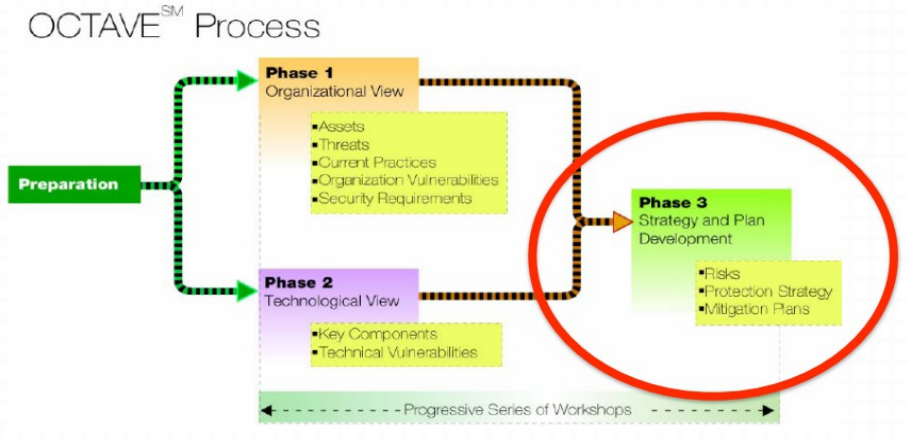
Η εταιρεία για να προστατέψει τους προσωπικούς της υπολογιστές από κακόβουλες επιθέσεις έχει εγκαταστήσει από τα δυνατότερα προγράμματα που περιέχουν antivirus , firewall, antispyware και antispam. Επίσης, χρησιμοποιούν αυτόματο backup της Seagate και των Windows. Όσο για την

προστασία των server της έχει εγκαταστήσει ασφάλεια Linux, Anticlam firewalls και σύστημα HID OSSEC, καθώς επίσης και Windows backups και την αντίστοιχη εφαρμογή για τον Linux server. Όλες οι βάσεις δεδομένων που χρησιμοποιούν οι υπηρεσίες του οργανισμού είναι κωδικοποιημένες, και δεν είναι δυνατή η προσπέλαση τους από οποιοδήποτε εκτός από το Διαχειριστή συστήματος μέσω της χρήσης πολλαπλών επιπέδων ασφαλείας (λειτουργικού συστήματος και βάσεως δεδομένων). Τα συστήματα ασφαλείας προστατεύουν από την μη εξουσιοδοτημένη πρόσβαση (hacking). Ένα από τα βασικά στοιχεία ασφαλείας είναι ότι δεν υπάρχει καμία δυνατότητα διαγραφής η παραμετροποίησης των δεδομένων εφόσον εισαχθούν στις βάσεις. Έτσι διασφαλίζεται η ακεραιότητα τους αλλά και το προσωπικό απόρρητο των χρηστών. Οι εξυπηρετητές (servers) είναι εγκατεστημένοι σε ειδικό διαμορφωμένο χώρο υψηλής ασφάλειας, ο οποίος λειτουργεί ως data center και είναι συνδεδεμένοι με το τοπικό δίκτυο της εταιρείας. Το λειτουργικό σύστημα που διαθέτουν είναι Windows και Linux.Οι εξυπηρετητές εκτός των άλλων χρησιμοποιούνται από τους χρήστες σε μεγάλο βαθμό και ως file servers για την αποθήκευση και τη διαχείριση των προσωπικών τους αρχείων αλλά και για τη δημιουργία αντιγράφων ασφαλείας. Οι servers του τοπικού δικτύου, οι εκτυπωτές και το rack των συνδέσεων, είναι τοποθετημένα σε ξεχωριστό χώρο εντός της εταιρείας (lab) και δίνουν την δυνατότητα κεντρικής διαχείρισης, διαμοιρασμού αρχείων/ εκτυπωτών, προστασίας – antivirus.

Πως το γνωρίζετε;

Η επικοινωνία με γνωστό εργαζόμενο άτομο σε εμάς που εργάζεται στον συγκεκριμένο οργανισμό στο τμήμα πωλήσεων μας έδωσε τη δυνατότητα να μιλήσουμε μέσω διαδικτύου με άτομο από τη διοίκηση του οργανισμού και να μας δώσει όλες τις σημαντικές πληροφορίες που μας βοήθησαν να βγάλουμε εις πέραν την εργασία.

Φάση 3



Κατά την τρίτη φάση η ομάδα ανάλυσης:
• Αναγνωρίζει τους κινδύνους για τα κρίσιμα αγαθά του οργανισμού και λαμβάνει αποφάσεις για το τι μπορεί να κάνει για αυτά.
• Στηριζόμενη στην ανάλυση της πληροφορίας που έχει συγκεντρωθεί προβαίνει στη δημιουργία μιας στρατηγικής προστασίας του οργανισμού και σχεδίων μετριασμού αποτελεσμάτων που απευθύνονται στους κινδύνους των κρίσιμων αγαθών.
• Χρησιμοποιεί έγγραφα που είναι αυστηρά δομημένα και δίνουν της δίνουν τη δυνατότητα να συσχετίσει τις προτάσεις για βελτίωση σε ένα αποδεκτό πλαίσιο πρακτικών ασφάλειας.

Φάση 3 - Ερωτήσεις

1)Ποια είναι η ενδεχόμενη επίδραση στο οργανισμό από κάθε απειλή; Ποιοι είναι οι κίνδυνοι για τον οργανισμό;

Στην ασφάλεια, μια αποκάλυψη αποτελεί απειλή καθώς είναι ένας τρόπος για πιθανή απώλεια ή βλάβη του Πληροφοριακού Συστήματος. Παραδείγματα αποκαλύψεων είναι η μη εξουσιοδοτημένη αποκάλυψη των δεδομένων, τροποποίηση των δεδομένων ή άρνηση του νόμιμου δικαιώματος πρόσβασης στο σύστημα. Η ευπάθεια είναι η αχίλλειος πτέρνα στο σύστημα ασφάλειας που μπορεί να εκμεταλλευτεί από τρίτους για την πρόκληση απωλειών ή ζημίας Ένα πρόσωπο που εκμεταλλεύεται την ευπάθεια του συστήματος διαπράττει μια επίθεση στο σύστημα. Ο συνεχής έλεγχος είναι ένα προστατευτικό μέτρο, που μπορεί να είναι είτε μια ενέργεια ή μια συσκευή ή ακόμα και μια διαδικασία ή τεχνική μέθοδος, και που μειώνει την ευπάθεια του συστήματος. Υπάρχουν τέσσερα είδη απειλής στην ασφάλεια του Π.Σ. που είναι:

• **Διακοπή (interruption)**. Τα αντικείμενα του συστήματος χάνονται, δεν είναι διαθέσιμα ή είναι μη χρησιμοποιήσιμα. Παραδείγματα είναι η ηθελημένη καταστροφή μιας συσκευής, το σβήσιμο ενός προγράμματος ή ενός αρχείου δεδομένων, ή η δυσλειτουργία του διαχειριστή αρχείων του λειτουργικού συστήματος, έτσι ώστε να μην μπορεί να βρεθεί ένα συγκεκριμένο αρχείο στο δίσκο.

• **Παρεμπόδιση (interception)**. Σημαίνει πως μια μη εξουσιοδοτημένη ομάδα έχει κερδίσει το δικαίωμα πρόσβασης σε ένα αντικείμενο. Αυτή η εξωτερική ομάδα μπορεί να είναι είτε πρόσωπα, είτε προγράμματα ή ακόμα και παρέμβαση ενός άλλου πληροφοριακού συστήματος. Παραδείγματα αυτού του είδους της αποτυχίας είναι η παράνομη αντιγραφή των προγραμμάτων ή των αρχείων δεδομένων ή οι υποκλοπές των τηλεφωνημάτων για την απόκτηση δεδομένων από το δίκτυο. Παρόλο που μια απώλεια μπορεί να αποκαλυφθεί σχετικά γρήγορα, ο υποκλοπέας μπορεί να μην αφήσει καθόλου ίχνη για την ανίχνευση της ύπαρξης του.

• **Τροποποίηση (modification)**. Εάν μια μη εξουσιοδοτημένη ομάδα όχι μόνο προσπελάσει τα δεδομένα, αλλά ανακατευτεί και με κάποια αντικείμενα, τότε μιλάμε για τροποποίηση. Για παράδειγμα κάποιος μπορεί να αλλάξει τις τιμές σε μια βάση δεδομένων ή να μετατρέψει ένα πρόγραμμα έτσι ώστε να εκτελεί επιπλέον υπολογισμούς ή να τροποποιεί τα δεδομένα που μεταφέρονται ηλεκτρονικά. Είναι ακόμα δυνατό να τροποποιηθεί και το υλικό μέρος του συστήματος.

• **Πλαστοποίηση (fabricate)**. Τέλος μια μη εξουσιοδοτημένη ομάδα μπορεί να κατασκευάσει πλαστά αντικείμενα σε ένα Π.Σ. Ο εισβολέας μπορεί να προσθέσει εγγραφές σε μια υπάρχουσα βάση δεδομένων. Μερικές φορές αυτές οι προσθέσεις ανιχνεύονται σαν πλαστές, αλλά εάν έχουν γίνει περίτεχνα τότε είναι αδιαχώριστες από τα πραγματικά αντικείμενα.

2)Ποιοι είναι οι υψηλότερης προτεραιότητας κίνδυνοι για τον οργανισμό;

Οι κίνδυνοι για έναν οργανισμό είναι πολλοί και πολλοί από αυτούς είναι ικανοί να οδεύσουν έναν οργανισμό ακόμα και στην ολική του καταστροφή.Παρ΄όλα αυτά υπάρχουν κάποιοι κίνδυνοι που είναι υψηλότερης σημασίας από τους υπόλοιπους.

Α)Communications Interception: Η υποκλοπή των επικοινωνιών μεταξύ χρήστη και server μπορεί να οδηγήσει σε υποκλοπή κωδικών πρόσβασης.
Β)Communications Interception: Η υποκλοπή επικοινωνιών μεταξύ πελάτη (είτε αυτός είναι χρήστης είτε κάποιο σύστημα και backup server μπορεί να οδηγήσει σε κλοπή των δεδομένων που μεταφέρονται.
Γ)Masquerading of User Identity by Insiders / Outsiders: Η χρήση ενός username και password ενός άλλου μπορεί να προκαλέσει την κλοπή, μετατροπή ή διαγραφή των προσωπικών πληροφοριών του χρήστη. Επίσης, κάποιος που δεν έχει δικαίωμα μπορεί να χρησιμοποιήσει τα προγράμματα του οργανισμού, προκαλώντας μη διαθεσιμότητα. Τέλος, η χρήση κωδικού ενός administrator μπορεί να προκαλέσει πολύ σοβαρότατες απώλειες σε όλο το σύστημα
Δ)Server Room: Στο δωμάτιο αυτό βρίσκονται όλοι οι servers. Έτσι, όποιες απειλές αναφέρονται στο δωμάτιο απειλούν όλα τα υπολογιστικά συστήματα, τα δεδομένα που κατακρατούν καθώς και τις υπηρεσίες που προσφέρουν. Η φωτιά απειλεί να καταστρέψει όλα τα δεδομένα μέχρι το πιο πρόσφατο backup και επιπλέον όλα τα υλικά περιουσιακά στοιχεία που υπάρχουν στο server room.Εκτός από αυτό όμως,η ζημιά με πρόθεση από εσωτερικούς μπορεί να προκαλέσει φυσική καταστροφή υλικών στοιχείων, μη διαθεσιμότητα υπηρεσιών και καταστροφή δεδομένων μέχρι το πιο πρόσφατο backup.
Ε)Introduction of Damaging or Disruptive Software: Η εισαγωγή επιβλαβούς λογισμικού περιλαμβάνει ιούς, δούρειους ίππους, σκουλήκια (worms), λογικές βόμβες κτλ. Στην περίπτωση αυτή μπορεί να οδηγήσει στην καταστροφή των δεδομένων των χρηστών (μέχρι το πιο πρόσφατο backup), την υποκλοπή των δεδομένων και την μη διαθεσιμότητα της υπηρεσίας .

3)Τι πολιτικές και πρακτικές θα πρέπει να υιοθετήσει ο οργανισμός;
***4)*Τι ενέργειες μπορεί να κάνει ο οργανισμός για τον μετριασμό (mitigation) των πιο υψηλών κινδύνων;**

Ο οργανισμός είναι αναγκαίο εκτός από τις πολιτικές που έχει υιοθετήσει μέχρι τώρα να αναλάβει και άλλες πρακτικές που είναι πολυ σημαντικές για την αντιμετώμιση των παραπάνω κινδύνων.Αυτές φαίνονται παρακάτω:

- **Καταγραφή και αποτίμηση περιουσιακών στοιχείων**: Έχουν δημιουργηθεί εργαλεία για την εύκολη καταγραφή, κατηγοριοποίηση και αποτίμηση των περιουσιακών στοιχείων. Ως γνωστόν, στον πληροφοριακό τομέα τα περιουσιακά στοιχεία δεν είναι εύκολο να αποτιμηθούν λόγο της αφηρημένης έννοιας τους. Η πληροφορίες περιέχουν αξία που δεν εκφράζονται επιτυχώς με νομισματικά μεγέθη. Τα εργαλεία που περιέχονται στα πακέτα λογισμικού ανάλυσης κινδύνων βοηθούν στην αναγνώριση των διαφόρων μορφών αξίας και στην αποτίμηση τους, ακόμα και από ανθρώπους που δεν έχουν λάβει ειδική εκπαίδευση στα θέματα αυτά. Αυτό επιτυγχάνεται με διάφορους τρόπους όπως πχ. με λίστες από κατηγορίες αξιών και ειδικές κλίμακες για την αποτίμηση τους.
- **Λίστες απειλών**: Επειδή τα περισσότερα πακέτα λογισμικού ανάλυσης κινδύνων δεν απευθύνονται αποκλειστικά σε ειδικούς με την ασφάλεια πληροφοριακών συστημάτων, έχουν δημιουργηθεί λίστες με τις πιθανές απειλές που υπάρχουν. Οι λίστες αυτές έχουν

συμπληρωθεί από ειδικούς με βάση την πολύχρονη εμπειρία τους. Ο χρήστης του προγράμματος αρκείται στην επιλογή των απειλών που «ταιριάζουν» σε κάθε περιουσιακό στοιχείου του οργανισμού.

- **Αποτίμηση απειλών**: Υπάρχουν διάφοροι τρόποι που χρησιμοποιούνται από τα προγράμματα για την αποτίμηση των απειλών αλλά ο πιο δημοφιλής με διαφορά είναι τα ερωτηματολόγια. Το πρόγραμμα δημιουργεί αυτόματα μια σειρά ερωτηματολογίων τα οποία όταν απαντηθούν χρησιμοποιούνται για την αυτόματη αποτίμηση της πιθανότητας να συμβεί μια απειλή καθώς και το αντίκτυπο που θα έχει αυτή. Τα ερωτηματολόγια δημιουργούνται με βάση τα περιουσιακά στοιχεία και τις απειλές που έχουν ήδη εισαχθεί στο πρόγραμμα.
- **Υπολογισμός βαθμού κινδύνου**: Με την επεξεργασία των περιουσιακών στοιχείων, των απειλών και των ευπαθειών του πληροφοριακού συστήματος υπολογίζονται οι βαθμοί κινδύνου. Ο υπολογισμός γίνεται εντελώς αυτόματα από το πρόγραμμα από την στιγμή που εισαχθούν όλα τα απαραίτητα δεδομένα.
- **Αυτόματη επιλογή αντιμέτρων**: Έχουν δημιουργηθεί αλγόριθμοι για την αυτόματη επιλογή των κατάλληλων αντιμέτρων βάση των στοιχείων που έχουν συλλεχθεί κατά την διάρκεια της ανάλυσης. Η επεξεργασία του τύπου των απειλών, του βαθμού των κινδύνων, του κόστους των αντιμέτρων, τις αποτελεσματικότητας των αντιμέτρων, της ύπαρξης άλλων αντιμέτρων και πολλών άλλων παραμέτρων οδηγεί στην επιλογή αντιμέτρων που έχουν βέλτιστο λόγο απόδοσης/κόστους. Τα αντίμετρα που επιλέγονται χρειάζονται βέβαια επιπλέον «ξεκαθάρισμα» από ανθρώπους, καθώς δεν έχουν αναπτυχθεί ακόμα αλγόριθμοι που να πετυχαίνουν τέλεια αποτελέσματα. Όση προσπάθεια και αν έχει γίνει, το λογισμικό δεν μπορεί να έχει την ίδια αντίληψη για το πληροφοριακό σύστημα και τα προβλήματα του όπως ένας άνθρωπος που εργάζεται πάνω σε αυτό.
- **Δημιουργία αναφορών**: Τα περισσότερα πακέτα ανάλυσης κινδύνων δεν περιορίζονται στα τυπικά μέρη της ανάλυσης κινδύνων αλλά περιέχουν και εργαλεία για την γενικότερη διευκόλυνση των ανθρώπων που εργάζονται για αυτήν. Ένα από αυτά είναι και η δημιουργία αναφορών. Τα εργαλεία μπορούν να παράγουν αναφορές που περιλαμβάνουν πίνακες και έγχρωμα γραφήματα. Οι αναφορές είναι πλήρως παραμετροποιήσιμες ως προς το περιεχόμενο τους και την δομή τους. Στα πιο σύγχρονα προγράμματα υπάρχει και η δυνατότητα εξαγωγής των αναφορών σε διάφορες μορφές τυπικών αρχείων όπως rtf, doc κτλ.

- **Διαχείριση εγγράφων**: Ένα χαρακτηριστικό που δεν προσφέρουν πολλά πακέτα ανάλυσης κινδύνων αλλά είναι πολύ σημαντικό είναι η διαχείριση εγγράφων. Διατηρείται βάση δεδομένων με τις πολιτικές ασφαλείας, τις διαδικασίες που πρέπει να ακολουθούνται και άλλα έγγραφα σχετικά με την ασφάλεια του πληροφοριακού συστήματος. Η βάση δεδομένων δίνει την κατάλληλη πρόσβαση σε κάθε χρήστη, δίνοντας του μόνο τα στοιχεία που χρειάζεται έτσι ώστε να μην χάνει χρόνο στην αναζήτηση. Η βάση δεδομένων βρίσκεται μέσα στο τοπικό δίκτυο έτσι ώστε η πρόσβαση στα αρχεία αυτά να είναι εύκολη και γρήγορη από όλα τα μέλη του οργανισμού.

5)Τι τεχνολογικές αδυναμίες χρειάζεται να αντιμετωπιστούν άμεσα;

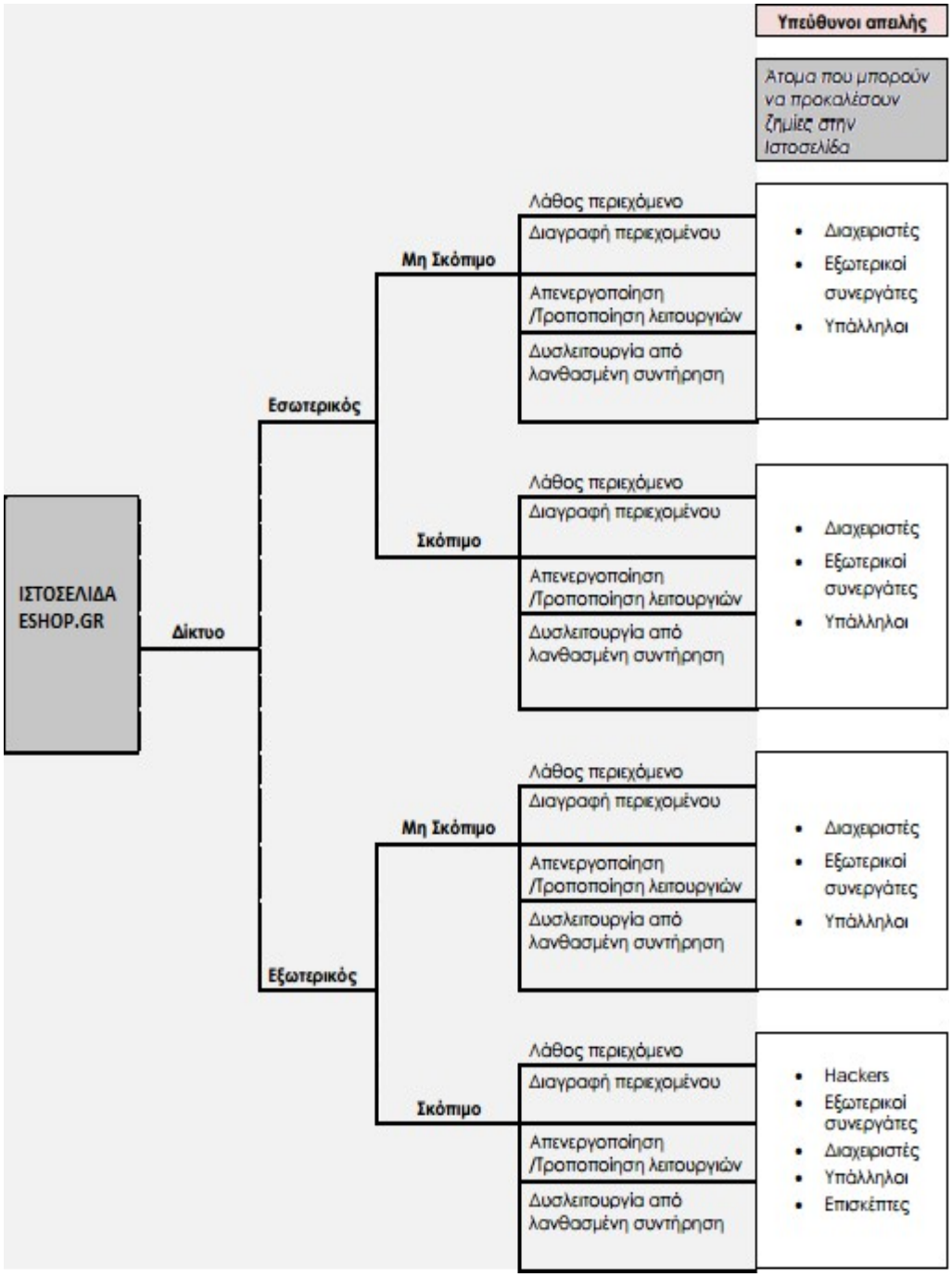
Τέλος,εκτός από τους κινδύνους και τα μέσα αντιμετώμισης αυτών,ο οργανισμός όπως και κάθε οργανισμός αντιμετωπίζει και κάποιες τεχνολογικές αδυναμίες.

- **Παλιές ηλεκτρονικές υπηρεσίες.**Είναι λογικό πολλά εξαρτήματα στο τεχνολογικό κομμάτι του να είναι πιο παλιά από τα άλλα δημιουργώντας έτσι το ρίσκο όπου όταν ένας που επιτίθεται στον οργανισμό μέσω διαδικτύου ή γενικά ηλεκτρονικά να έχει μελετήσει το πιο

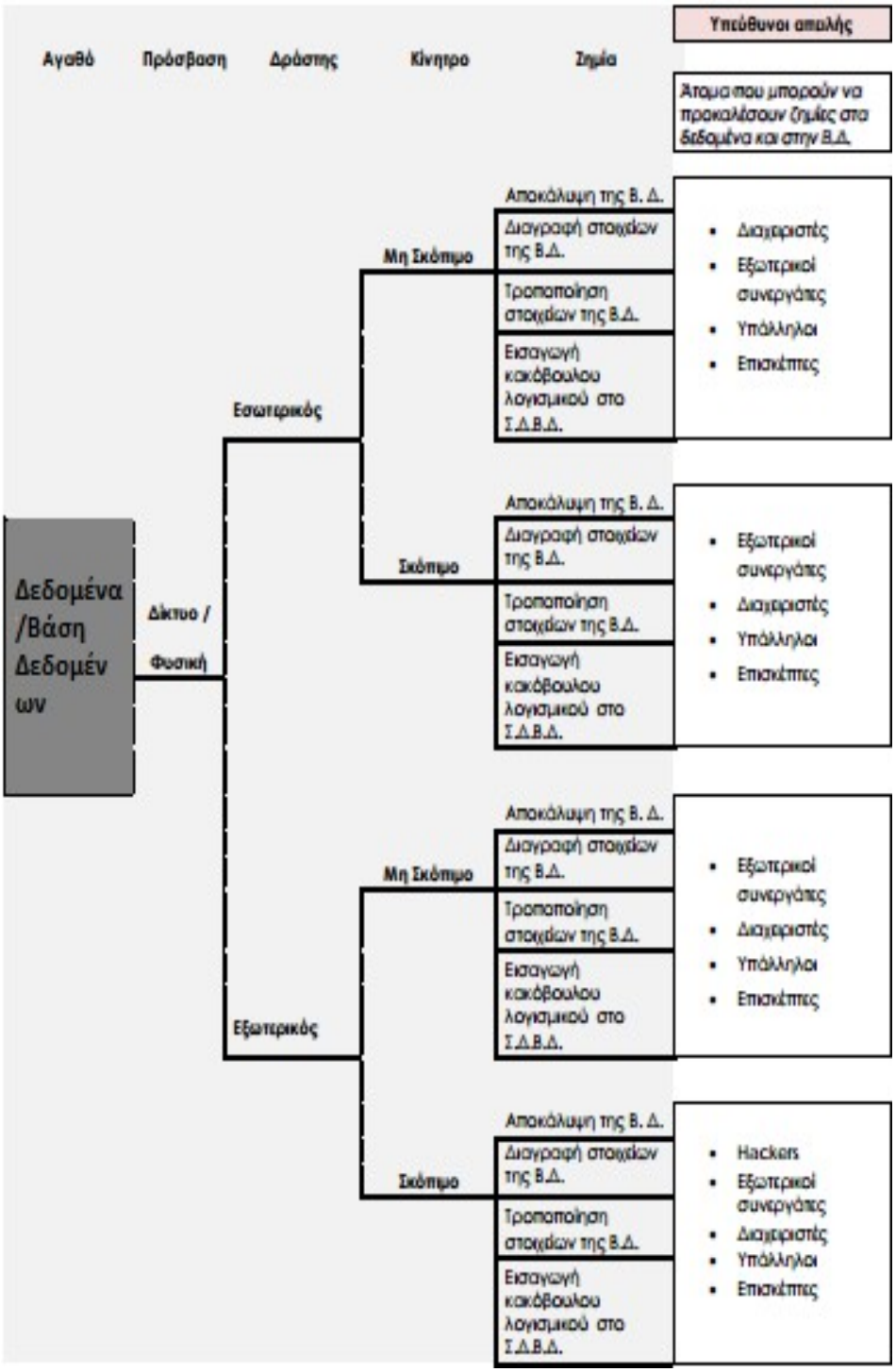
παλιό κομμάτι καλύτερα από τα άλλα και να εισβάλλει από εκεί.

- **Απουσία σχεδίου καταστροφής και ακαταλληλότητα χώρου του computer room.**Σίγουρα το δωμάτιο που περιέχει το υπολογιστικό σύστημα και τη βάση δεδομένων είναι από τα σημαντικότερα μέρη μέσα στον οργανισμό και αν αυτό δεν είναι καλύτερα φυλαγμένο και δεν έχει την ασφάλεια που πρέπει είναι πολυ εύκολο να παραβιαστεί.Στο συγκεκριμένο οργανισμό λοιπόν για τον λόγο του ότι έχει αρκετά χρόνια να ανανεωθεί αυτό το δωμάτιο αλλά και ότι δεν υπάρχει κάποιο άμεσο σχέδιο για την αντιμετώπιση τυχόν απειλών το καθιστά σημαντική τεχνολογική αδυναμία.
- **Απευθείας πρόσβαση στους servers του οργανισμού.**Οι υπάλληλοι έχουν απευθείας πρόσβαση στους servers του οργανισμού από τις θέσεις εργασίας τους, οπότε ένας από τους χρήστες του συστήματος με πρόσβαση στο σύστημα μπορεί να τροποποιήσει, να αποκαλύψει ή να καταστρέψει πληροφορίες έχοντας κάποιο προσωπικό όφελος μέσω αυτής της ενέργειας, παραβιάζοντας έτσι την ακεραιότητα της πληροφορίας αφού την διαχειρίστηκαν άτομα που δεν είχαν τέτοια αρμοδιότητα και εξουσιοδότηση. Η πιθανότητα να συμβεί ένα τέτοιο σενάριο κρίνεται μέτρια και οι συνέπειες που θα έχει για τον οργανισμό η παραβίαση των συνθηκών ασφάλειας από την συγκεκριμένη απειλή είναι η φήμη του οργανισμού να χτυπηθεί καθώς και η εμπιστοσύνη των πολιτών απέναντί του λόγω των απωλειών στοιχείων σημαντικών για τις ασφαλίσεις με υψηλή επίπτωση στον τομέα της φήμης του οργανισμού, κάποιοι μπορούν να κινηθούν νομικά με υψηλές επιπτώσεις στον τομέα των προστίμων λόγω αποκαλύψεων και μπορούμε να έχουμε σοβαρές οικονομικές απώλειες λόγω αλλοίωσης στοιχείων αποζημιώσεων.

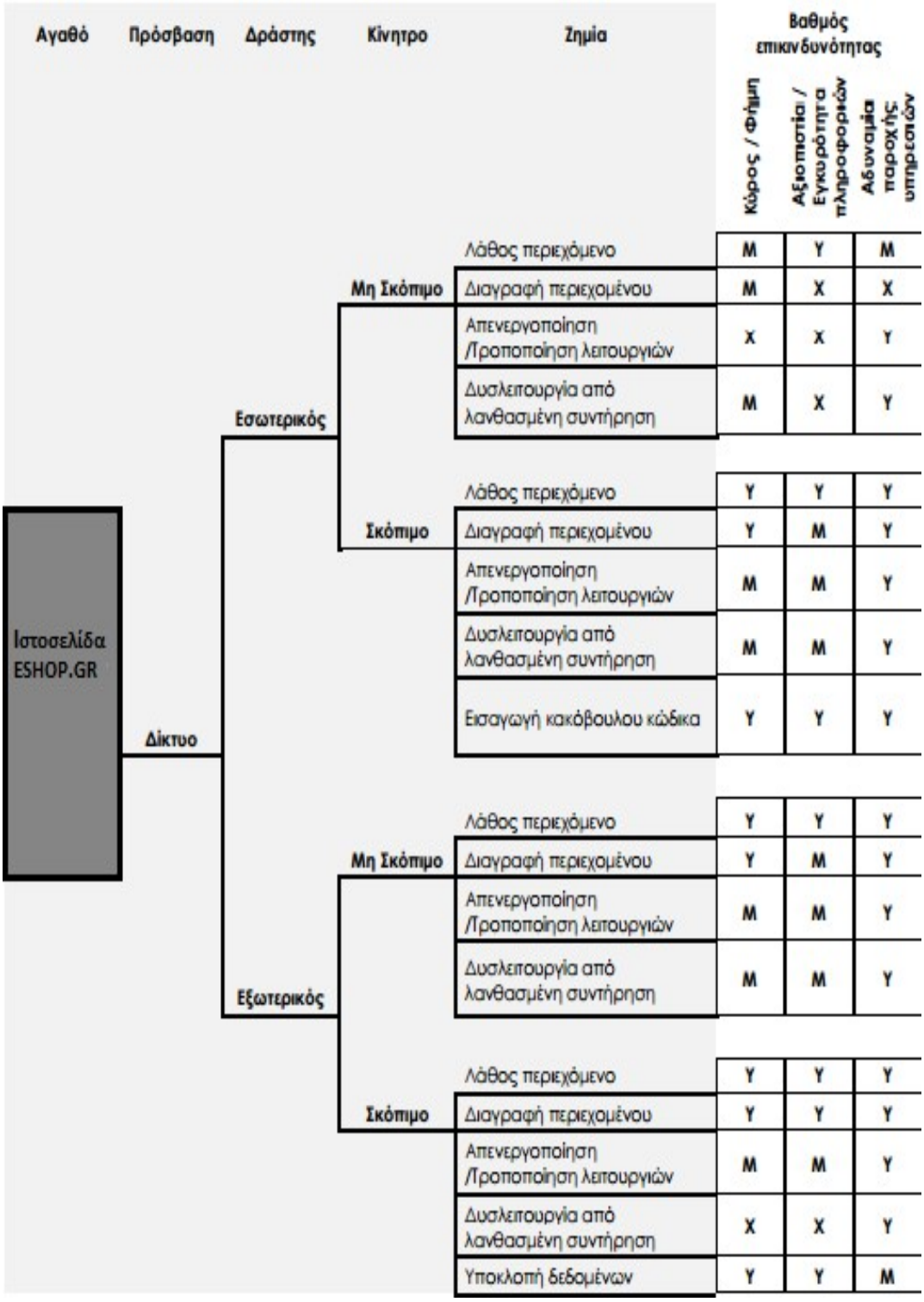
Σχηματική απεικόνιση παραγόντων κινδύνου ιστοσελίδας.



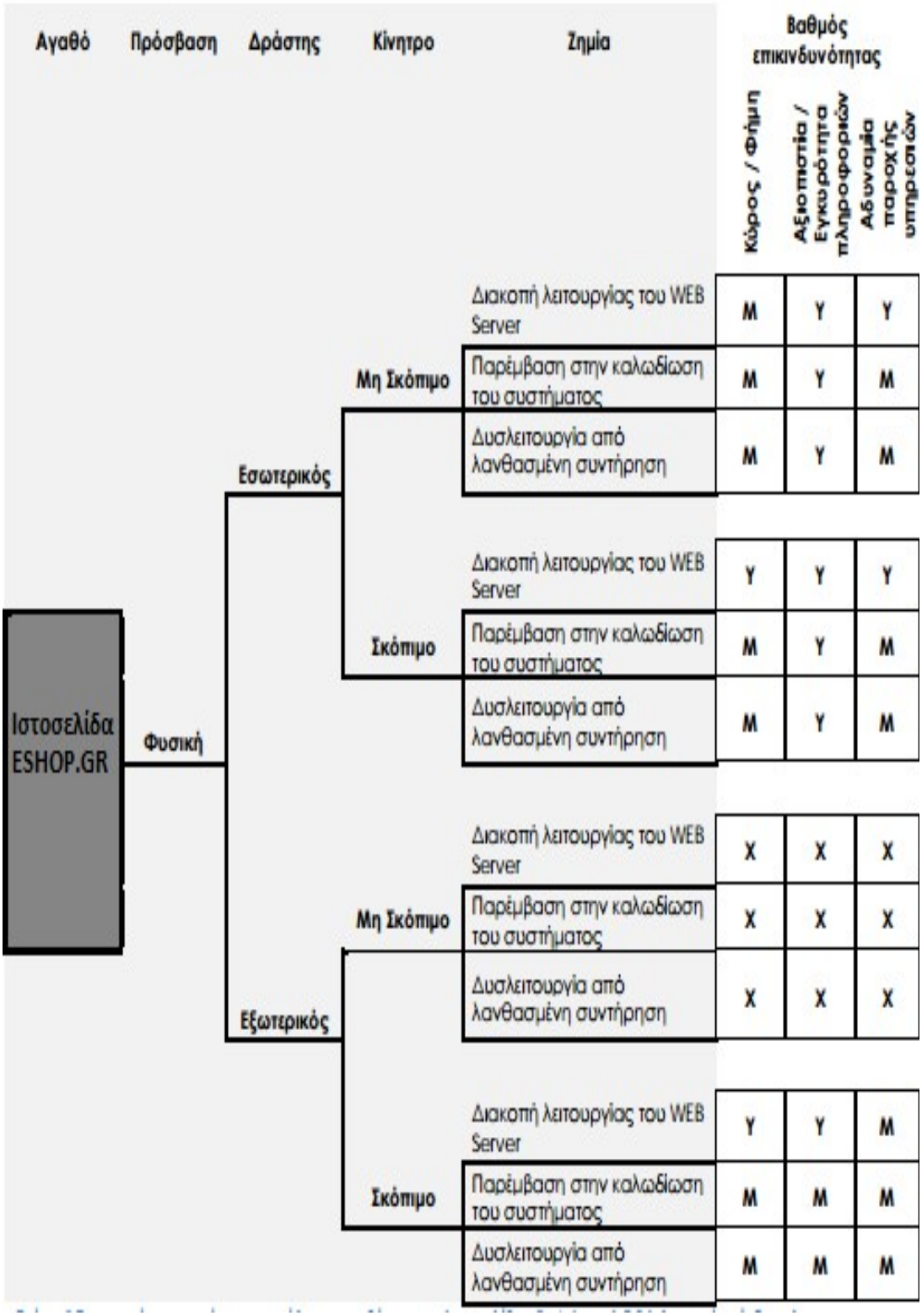
Σχηματική απεικόνιση παραγόντων κινδύνου δεδομένων και βάσης δεδομένων.



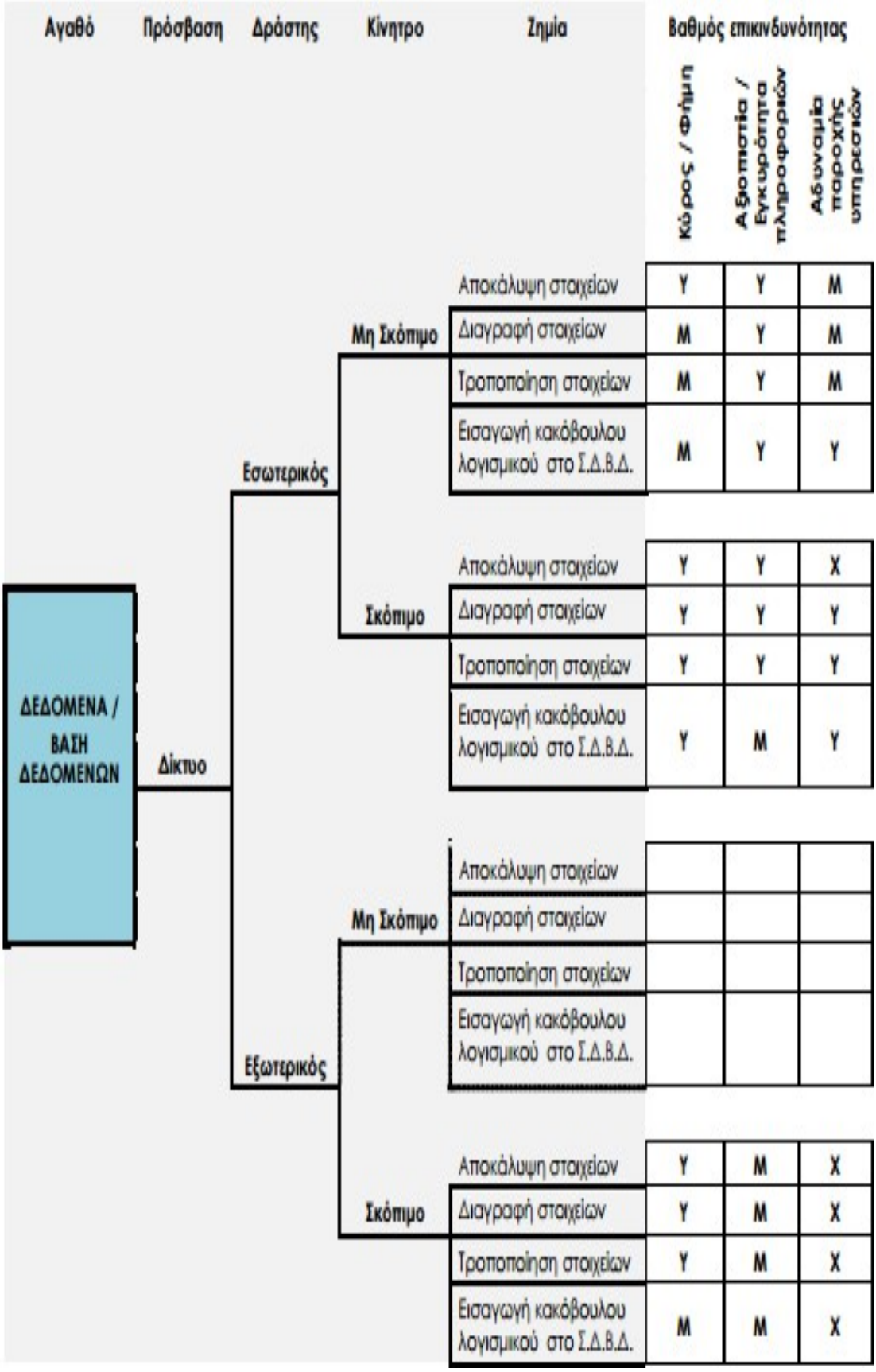
Σχηματική απεικόνιση ανάλυσης κινδύνων της ιστοσελίδας (πρόσβαση μέσω δικτύου)



Σχηματική απεικόνιση ανάλυσης κινδύνων της ιστοσελίδας (φυσική επέμβαση)



Σχηματική απεικόνιση ανάλυσης κινδύνων δεδομένων και βάσης δεδομένων (πρόσβαση μέσω δικτύου)



Σχηματική απεικόνιση ανάλυσης κινδύνων δεδομένων και βάσης δεδομένων (φυσική επέμβαση)