ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Διαχείριση Κινδύνου στην Ασφάλεια Πληροφοριακών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Γ. Αϋφαντόπουλος

Επιβλέπων : Δ. Ασκούνης
Αναπληρωτής Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2014.

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Διαχείριση Κινδύνου στην Ασφάλεια Πληροφοριακών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Γ. Αϋφαντόπουλος

Επιβλέπων : Δ. Ασκούνης
Αναπληρωτής Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 29η Οκτωβρίου 2014.

.....	.....	.....
Δ. Ασκούνης	Ι. Ψαρράς	Β. Ασημακόπουλος
Αν. Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2014.

.....

Κωνσταντίνος Γ. Αϋφαντόπουλος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου, στα πλαίσια των ερευνητικών δραστηριοτήτων του Εργαστηρίου Συστημάτων Αποφάσεων και Διοίκησης.

Σκοπός της παρούσας διπλωματικής είναι να αναλύσει δύο μεθοδολογίες, την OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) και την PTA (Practical Threat Analysis), με τις οποίες μπορούμε να διαχειριστούμε πληροφοριακά συστήματα μεγάλων οργανισμών και να διασφαλίσουμε την πληροφορία που εμπεριέχεται σε αυτά, με κατάλληλες ενέργειες.

Αρχικά, θα παρουσιαστεί αναλυτικά η θεωρία των δύο μεθοδολογιών και μετά θα τις εφαρμόσουμε σε υπαρκτά πληροφοριακά συστήματα. Τέλος, θα αξιολογήσουμε τα αποτελέσματα και θα προτείνουμε λύσεις. Το επιλεχθέν έργο είναι ο Ελληνικός Οργανισμός Γεωργικών Ασφαλίσεων.

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Δ. Ασκούνη, που μου έδωσε την ευκαιρία να ασχοληθώ με ένα τέτοιο θέμα και για τη γενική του επίβλεψη, τον κ. Χρήστο Μπότσικα για την πολύτιμη βοήθειά του καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής εργασίας, τον φίλο μου Γρηγόρη για το έναυσμα που μου έδωσε να ασχοληθώ με το συγκεκριμένο θέμα αλλά και την οικογένειά μου για τη στήριξη που μου παρείχε όλο αυτό το διάστημα.

Οκτώβριος 2014

Κωνσταντίνος Γ. Αϋφαντόπουλος

Περίληψη

Πληροφοριακά συστήματα μεγάλου μεγέθους και πολυπλοκότητας εμπεριέχουν ποικίλους κινδύνους που απειλούν την ασφάλεια των πληροφοριών που βρίσκονται αποθηκευμένες μέσα σε αυτά. Σκοπός της Διπλωματικής Εργασίας ήταν η περιγραφή και ανάλυση μεθοδολογιών διαχείρισης κινδύνου στην ασφάλεια πληροφορίας και η εφαρμογή αυτών σε ένα υπαρκτό πληροφοριακό σύστημα.

Αρχικά, παρουσιάστηκε η τεχνική της μεθόδου OCTAVE, περιγράφοντας αναλυτικά τη διαδικασία που θα πρέπει να ακολουθείται για να γίνεται η αξιολόγηση κινδύνου σε οποιοδήποτε σύστημα. Μετέπειτα, με δεδομένο πως η εφαρμογή των μεθοδολογιών διαχείρισης κινδύνων έγινε στα πληροφοριακά συστήματα του Ελληνικού Οργανισμού Γεωργικών Ασφαλίσεων (ΕΛΓΑ), αναλύσαμε τις δομές και τη διάρθρωση του οργανισμού.

Κατά την εφαρμογή, έγινε παρουσίαση κάποιων πιθανών κινδύνων, αξιολογήθηκε η σοβαρότητα αυτών σύμφωνα με τους κανόνες της μεθόδου και προτάθηκαν λύσεις, όπου αυτό κρίθηκε αναγκαίο.

Επιπλέον, παρουσιάστηκε το λογισμικό πρόγραμμα PTA, που μπορεί να αποτελέσει, επίσης, χρήσιμο εργαλείο για τη διεξαγωγή μελετών διαχείρισης κινδύνων, στο οποίο εισήγαμε τους ίδιους κινδύνους και εξήγαμε αποτελέσματα παρόμοια με αυτά της πρώτης μεθόδου.

Τέλος, έγινε σύγκριση μεταξύ των δύο μεθοδολογιών και εξαγωγή συμπερασμάτων για την βέλτιστη χρησιμοποίηση τους.

Abstract

Information systems of high complex involve various risks that threaten the security of information stored in them. The aim of this thesis is to describe and analyze risk management techniques in information security and make them applicable to an existing information system.

Initially, the method OCTAVE was presented, describing in detail the procedure that has be followed to produce a risk assessment in any information system. Subsequently, given that the implementation of risk management methodologies concerned the information systems of the Greek Agricultural Insurance Organization (ELGA), we analyzed the structures of the organization.

In the implementation, some potential risks were presented, we assessed the significance of these in accordance with the rules of the method and proposed solutions, wherever necessary.

In addition, we analyzed the software PTA, which can also be a useful tool for studies of risk management, where we introduced the same risks as above and explain results similar to those of the first method.

Finally, a comparison was made between the two methodologies and conduction of conclusions for optimal use for each method.

Περιεχόμενα

Περιεχόμενα Εικόνων

Περιεχόμενα Πινάκων

ΕΙΣΑΓΩΓΗ Η σημασία της ασφάλειας πληροφοριακών συστημάτων

Στην σύγχρονη εποχή, η χρήση πληροφοριακών συστημάτων είναι δεδομένη για κάθε οργανισμό. Η επανάσταση της συνδεσιμότητας είναι πλέον γεγονός. Η ελεύθερη ροή πληροφοριών, οι ευκολίες που παρέχει το Internet καθώς και το ηλεκτρονικό εμπόριο έχουν ωθήσει μέχρι και τις μικρότερες επιχειρήσεις να επενδύσουν στην χρήση πληροφοριακών συστημάτων και διαδικτυακών εφαρμογών. Σαν αποτέλεσμα, στο μεγαλύτερο ποσοστό των οργανισμών η χρήση των πληροφοριακών συστημάτων είναι απολύτως αναγκαία για την επίτευξη των στόχων και της βασικής λειτουργικότητας τους. Έτσι, η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος, είτε από άμεσες οικονομικές απώλειες, είτε από την αδυναμία του οργανισμού να λειτουργήσει αποδοτικά.

Εκτός από τις οικονομικές επιπτώσεις όμως, τα προβλήματα ασφαλείας πληροφοριακών συστημάτων γίνονται ακόμα πιο αισθητά σε συστήματα που περιέχουν ευαίσθητα δεδομένα ή επιτελούν «ευαίσθητες» και σημαντικές λειτουργίες.

Διάφορα παραδείγματα τέτοιων συστημάτων είναι:

• Συστήματα με απόρρητα στρατιωτικά δεδομένα

• Συστήματα ελέγχου εναέριας κυκλοφορίας

• Συστήματα με ευαίσθητα ιατρικά δεδομένα

• Συστήματα που περιέχουν ευαίσθητα προσωπικά δεδομένα

Είναι φανερό ότι η ρήξη της ασφάλειας τέτοιων πληροφοριακών συστημάτων μπορεί να προκαλέσει σοβαρότατα προβλήματα που απειλούν άμεσα την ανθρώπινη ζωή και την ασφάλεια σε τοπικό, εθνικό αλλά και σε παγκόσμιο επίπεδο. Δεν υπάρχει λοιπόν αμφιβολία ότι η ασφάλεια των πληροφοριακών συστημάτων έχει τεράστια σημασία στην σύγχρονη κοινωνία και πρέπει να παίζει πρωτεύον ρόλο κατά την σχεδίαση, συντήρηση και χρήση τους.

ΚΕΦΑΛΑΙΟ 1 Η προσέγγιση της μεθόδου OCTAVE

1.1 Περίληψη

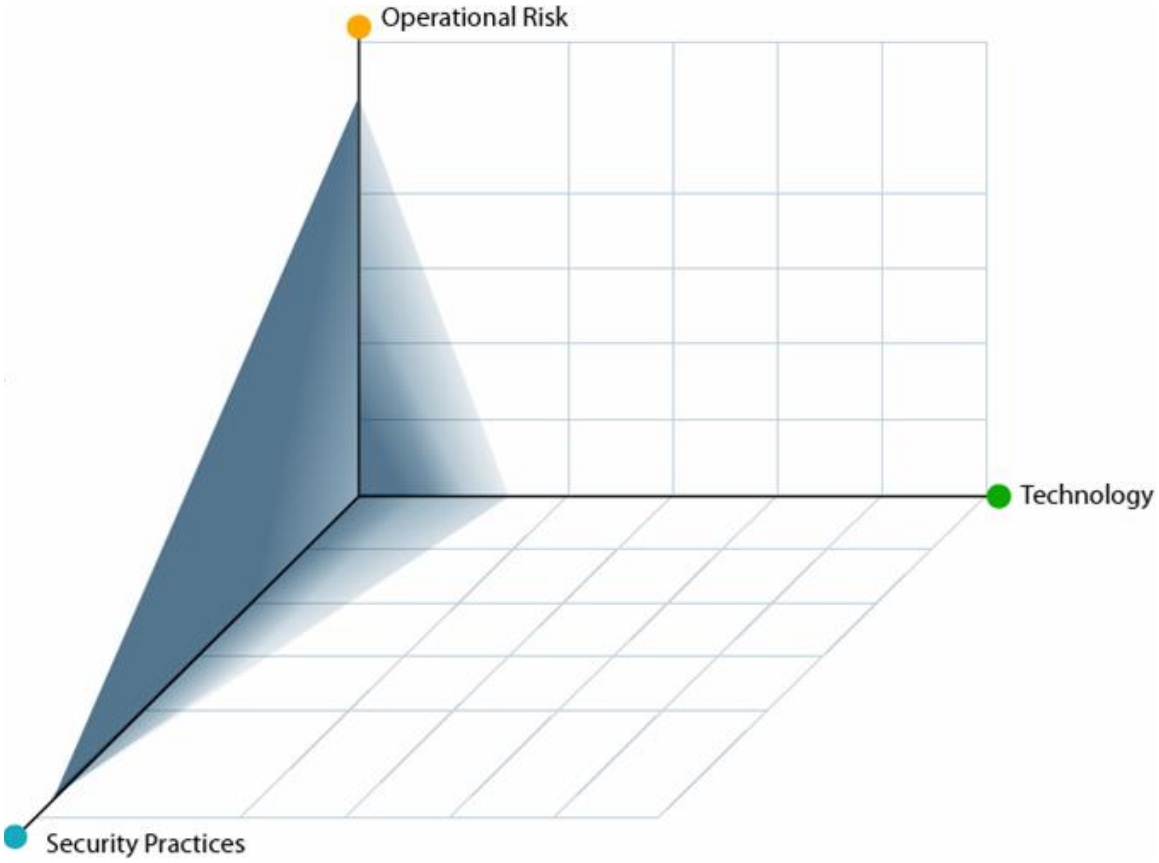
Μια αποτελεσματική μέθοδος αξιολόγησης κινδύνων για την ασφάλεια πληροφοριών, θεωρεί σημαντικά τόσο τα οργανωτικά όσο και τα τεχνολογικά θέματα, εξετάζοντας το πώς οι άνθρωποι χρησιμοποιούν τις υποδομές του οργανισμού τους σε καθημερινή βάση. Η αξιολόγηση είναι ζωτικής σημασίας για κάθε πρωτοβουλία που έχει σκοπό να βελτιώσει θέματα ασφαλείας, διότι δημιουργεί μια σαφή εικόνα των κινδύνων που διατρέχει η ασφάλεια των πληροφοριών μέσα στον οργανισμό, παρέχοντας μία βάση δεδομένων που μπορεί να φανεί πολύ χρήσιμη σε ενδεχόμενες μελλοντικές βελτιώσεις.

1.2 Τι είναι η OCTAVE

Για έναν οργανισμό που αναζητά να κατανοήσει τις ανάγκες της ασφάλειας των πληροφοριών του, η OCTAVE είναι μία στρατηγική αξιολόγησης ρίσκου και σχεδιασμού τεχνικών για την ασφάλεια. Η OCTAVE σε κάποιες εκδόσεις τις (τρεις είναι οι βασικότερες και θα αναλυθούν παρακάτω) μπορεί να είναι αυτο-κατευθυνόμενη, πράγμα που σημαίνει ότι ο ίδιος ο οργανισμός αναλαμβάνει την ευθύνη για τον καθορισμό της στρατηγικής ασφάλειας. Η τεχνική αξιοποιεί άλλοτε τη γνώση των ανθρώπων του οργανισμού, που σχετίζονται με τα θέματα ασφαλείας και άλλοτε τις γνώσεις εξωτερικών συνεργατών, για να αναγνωρίσει την τρέχουσα κατάσταση των πρακτικών ασφάλειας εντός του οργανισμού. Οι κίνδυνοι για τα πιο κρίσιμα περιουσιακά στοιχεία είναι χρήσιμοι, για να αντιληφθούμε που πρέπει να δοθεί προτεραιότητα βελτίωσης και για να ορίσουμε τη στρατηγική ασφαλείας για τον οργανισμό (1).

Σε αντίθεση με την τυπική τεχνολογία που έχει επίκεντρο την αξιολόγηση, η οποία απευθύνεται σε τεχνολογικό ρίσκο και επικεντρώνεται σε θέματα τακτικής, η OCTAVE εστιάζει στο οργανωτικό ρίσκο και επικεντρώνεται στην στρατηγική υλοποίησης πρακτικών ζητημάτων. Πρόκειται για ένα ευέλικτο τρόπο αξιολόγησης που μπορεί να προσαρμοστεί στους περισσότερους οργανισμούς και εταιρείες.

Κατά την εφαρμογή της OCTAVE, μια μικρή ομάδα ανθρώπων από το επιχειρησιακό περιβάλλον ή εξωτερικοί συνεργάτες, μαζί με το IT τμήμα συνεργάζονται για να αντιμετωπίσουν τις ανάγκες του οργανισμού, που αφορούν την ασφάλεια, εξισορροπώντας τα τρία βασικά στοιχεία που απεικονίζεται στην Εικόνα 1: επιχειρησιακός κίνδυνος (ρίσκο), πρακτικές ασφαλείας και την τεχνολογία.



Εικόνα 1: Σχέση ρίσκου, τεχνολογίας και πρακτικών ασφάλειας

Η προσέγγιση OCTAVE οδηγείται από δύο από τις πτυχές: του λειτουργικού κινδύνου και πρακτικές ασφαλείας. Η τεχνολογία εξετάζεται μόνο σε σχέση με τις πρακτικές ασφαλείας, επιτρέποντας στον οργανισμό να βελτιώσει τις πρακτικές ασφάλειας. Με τη χρήση της προσέγγισης OCTAVE, ένας οργανισμός λαμβάνει αποφάσεις για την προστασία της πληροφορίας, με βάση τους κινδύνους για την εμπιστευτικότητα, την ακεραιότητα, και τη διαθεσιμότητα των κρίσιμων περιουσιακών στοιχείων που σχετίζονται με την πληροφορία. Όλες οι πτυχές του κινδύνου (στοιχεία του ενεργητικού, οι απειλές, τα τρωτά σημεία και οι οργανωτικές επιπτώσεις) συνυπολογίζονται στη διαδικασία λήψης αποφάσεων, επιτρέποντας σε έναν οργανισμό να ταιριάξει μια πρακτική που βασίζεται στη στρατηγική με την προστασία από κινδύνους που αφορούν την ασφάλεια της πληροφορίας.

1.3 Βασικά χαρακτηριστικά της προσέγγισης OCTAVE

Η OCTAVE είναι μια μεθοδολογία για τον εντοπισμό και την αξιολόγηση των κινδύνων για την ασφάλεια των πληροφοριών. Προορίζεται για να βοηθήσει έναν οργανισμό:

- να αναπτύξει ποιοτικά κριτήρια αξιολόγησης των κινδύνων που περιγράφουν τον λειτουργικό κίνδυνο του οργανισμού
- να εντοπίσει τα περιουσιακά στοιχεία που είναι σημαντικά για την αποστολή του οργανισμού
- να εντοπίσει τα αδύνατα σημεία και τις απειλές για αυτά τα περιουσιακά στοιχεία

- να καθορίσει την αξιολόγηση των δυνητικών συνεπειών για τον οργανισμό εάν υλοποιηθούν οι απειλές (2)

1.4 Η ιστορία της OCTAVE

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.

Ο Πίνακας 1 παρέχει ένα σύντομο χρονολόγιο των σημαντικών γεγονότων που σχετίζονται με την OCTAVE.

Date Publication	**Title**
September 1999	OCTAVE Framework, Version 1.0
September 2001	OCTAVE Framework, Version 2.0
December 2001	OCTAVE Criteria, Version 2.0
September 2003	OCTAVE-S v0.9
March 2005	OCTAVE-S v1.0
June 2007	Introduction of OCTAVE Allegro v1.0

Πίνακας 1:Σύντομο χρονολόγιο εκδόσεων της octave

Υπάρχουν τρεις διακριτές μεθοδολογίες OCTAVE διαθέσιμες για χρήση από το κοινό:

- OCTAVE METHOD
- OCTAVE-S
- OCTAVE ALLEGRO

Θα αναλύσουμε κάθε μία από αυτές ξεχωριστά και θα διαλέξουμε αυτή που θεωρούμε πως ταιριάζει περισσότερο στις δικές μας ανάγκες, καθώς και στον οργανισμό που εξετάζουμε.

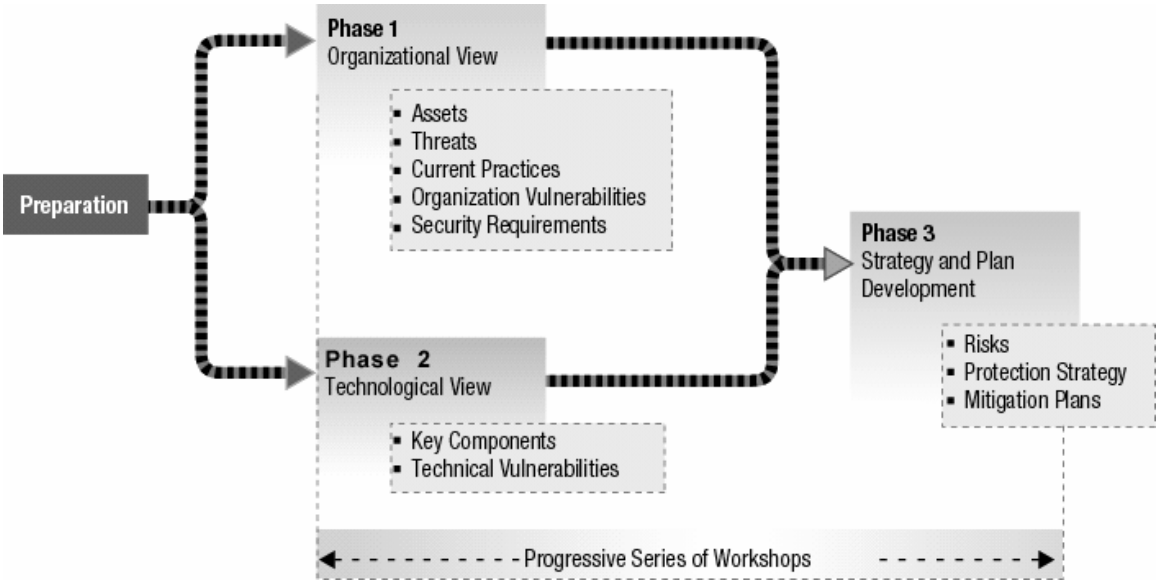
1.4.1 OCTAVE METHOD

Η OCTAVE METHOD αναπτύχθηκε για μεγάλους οργανισμούς (π.χ. 300 εργαζόμενοι ή περισσότερο). Το μέγεθος δεν είναι το μόνο που μας οδηγεί να τη χρησιμοποιήσουμε, καθώς οι μεγάλοι οργανισμοί έχουν γενικά μια πολυεπίπεδη ιεραρχία και μεγάλη γεωγραφική κατανομή. Τυπικές δραστηριότητες συλλογής στοιχείων, που καθορίζουν ποιες είναι οι πληροφορίες που σχετίζονται με τα περιουσιακά στοιχεία και είναι σημαντικές, πώς χρησιμοποιούνται και πώς τα στοιχεία απειλούνται, είναι βασικό κομμάτι

αυτής της μεθόδου. Τέλος, ένας μεγάλος οργανισμός είναι πιθανό να διατηρήσει τη δική του υποδομή πληροφορικής και να έχει την ικανότητα να τρέξει εργαλεία αξιολόγησης των αδυναμιών του και ερμηνείας των αποτελεσμάτων σε σχέση με τα κρίσιμα στοιχεία του ενεργητικού του.

Η μέθοδος έχει, επίσης, σχεδιαστεί για να επιτρέπεται η προσαρμογή της από οργανισμούς που την υιοθετούν. Οι περισσότεροι οργανισμοί που έχουν χρησιμοποιήσει την μέθοδο OCTAVE, υιοθετούν ειδικά την προσέγγιση που ταιριάζει στο δικό τους λειτουργικό περιβάλλον.

Η OCTAVE METHOD περιλαμβάνει τις τρεις φάσεις που απαιτούνται από τα κριτήρια OCTAVE.



Εικόνα 2:Σχηματική περιγραφή της octave method

Φάση 1 :Δημιουργία Προφίλ των Απειλών που σχετίζονται με τα σημαντικά asset

Οι δύο κύριες λειτουργίες αυτής της φάσης είναι:

- συλλογή πληροφοριών από όλη την οργάνωση
- καθορισμός προφίλ απειλής για τα στοιχεία κρίσιμης σημασίας του ενεργητικού.

Διαδικασία 1 :Αποκτώ καλή γνώση του οργανισμού από στοιχεία που διαθέτει η διοίκηση

Η ομάδα ανάλυσης συλλέγει πληροφορίες για τα σημαντικά περιουσιακά στοιχεία, τις απαιτήσεις ασφάλειας, τις απειλές, την τρέχουσα οργανωτική δύναμη και τα τρωτά σημεία από ένα αντιπροσωπευτικό σύνολο των ανώτερων διευθυντικών στελεχών.

Διαδικασία 2 : Προσδιορισμός του Επιχειρησιακό Χώρο που θα εστιάσω

Η ομάδα ανάλυσης συλλέγει πληροφορίες για τα σημαντικά περιουσιακά στοιχεία, απαιτήσεις ασφάλειας, απειλές, την τρέχουσα οργανωτική δύναμη και τις αδυναμίες τους από διαχειριστές των επιλεγμένων επιχειρησιακών τομέων.

Διαδικασία 3 : Προσδιορίζω τι γνώση έχει το προσωπικό

Η ομάδα ανάλυσης συλλέγει πληροφορίες για τα σημαντικά περιουσιακά στοιχεία, τις απαιτήσεις ασφάλειας, τις απειλές, την τρέχουσα οργανωτική δύναμη και τα τρωτά σημεία από το προσωπικό και τα μέλη του προσωπικού πληροφορικής του επιλεγμένου επιχειρησιακού τομέα.

Διαδικασία 4 : Δημιουργία προφίλ της απειλής

Η ομάδα ανάλυσης επιλέγει 3-5 περιουσιακά στοιχεία που σχετίζονται με κρίσιμες πληροφορίες και καθορίζει τα προφίλ απειλής για αυτά τα περιουσιακά στοιχεία.

Φάση 2: Προσδιορισμός Αδυναμιών στις Υποδομές

Κατά τη διάρκεια αυτής της φάσης, η ομάδα ανάλυσης αξιολογεί τα βασικά στοιχεία των συστημάτων που υποστηρίζουν τα περιουσιακά στοιχεία ζωτικής σημασίας για τις τεχνολογικές αδυναμίες.

Διαδικασία 5: Προσδιορισμός των Βασικών Στοιχείων

Ένα αντιπροσωπευτικό σύνολο των βασικών συστατικών από τα συστήματα που υποστηρίζουν ή επεξεργάζονται τα περιουσιακά στοιχεία, που σχετίζονται με ζωτικής σημασίας πληροφορίες, εντοπίζεται, και γίνεται μια προσέγγιση για την αξιολόγηση τους.

Διαδικασία 6: Αξιολόγηση Επιλεγμένα Στοιχείων

Εργαλεία 'τρέχουν' για να αξιολογήσουν τα επιλεγμένα στοιχεία και τα αποτελέσματα αναλύονται για να βελτιωθούν τα προφίλ των απειλή για τα κρίσιμα στοιχεία του ενεργητικού.

Φάση 3: Ανάπτυξη Στρατηγικής Ασφάλειας και Σχέδια

Ο πρωταρχικός σκοπός αυτής της φάσης είναι να αξιολογηθούν οι κίνδυνοι για τα περιουσιακά στοιχεία ζωτικής σημασίας και να αναπτυχθεί μια οργανωτική στρατηγική προστασίας και σχέδια μετριασμού του κινδύνου.

Διαδικασία 7: Ανάλυση Κινδύνου

Ένα οργανωτικό σύνολο των κριτηρίων αξιολόγησης της επίπτωσης του κινδύνου ορίζεται για τη δημιουργία μιας κοινής βάσης που θα προσδιορίζει την αξία των επιπτώσεων (υψηλή, μέση ή χαμηλή), λόγω απειλών σε κρίσιμα περιουσιακά στοιχεία. Όλες οι πιθανοί

κίνδυνοι αξιολογούνται για τις επιπτώσεις. (Σημειώστε ότι η πιθανότητα δεν περιλαμβάνεται επί του παρόντος, αλλά μπορεί να προστεθεί σε αυτή τη μέθοδο.)

Διαδικασία 8: Ανάπτυξη στρατηγικής για προστασία

Η ομάδα αναπτύσσει στρατηγική προστασίας, που αφορά ολόκληρο τον οργανισμό, και επικεντρώνεται στην βελτίωση των πρακτικών ασφάλειας του οργανισμού, καθώς και στον μετριασμό κινδύνου σε κρίσιμα περιουσιακά στοιχεία.

Η μέθοδος OCTAVE τεκμηριώνεται στον Οδηγό Εφαρμογής OCTAVE Μέθοδος (OMIG). Ο οδηγός αυτός περιλαμβάνει 18 τόμους των πληροφοριών τόσο σε Microsoft Word όσο και σε PowerPoint. (4)

1.4.2 OCTAVE S

Η OCTAVE-S αναπτύχθηκε και δοκιμάστηκε για μικρούς οργανισμούς, με αριθμούς εργαζομένων να κυμαίνεται από 20 έως 80 άτομα. 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. Για παράδειγμα, μια εταιρεία 200 ατόμων, που έχει έδρα σε μία μόνο τοποθεσία, θα μπορούσε να είναι σε θέση να συγκεντρώσει μια ομάδα από 5 άτομα που θα έχει επαρκή γνώση σε ολόκληρο τον οργανισμό και να βγάλει συμπεράσματα. Από την άλλη πλευρά, μια εταιρεία με 90 άτομα που εδράζει σε πολλές τοποθεσίες μπορεί να χρησιμοποιήσει τη μέθοδο OCTAVE-S για να εξασφαλίσει επαρκή δεδομένα από όλη την οργάνωση.

Μία άλλη διαφορά στο καθορισμό της OCTAVE-S σχετίζεται με την Φάση 2, που αφορά την αξιολόγηση της υπολογιστικής υποδομής. 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, αλλά η Φάση 2 της OCTAVE-S είναι μια συντετμημένη επιθεώρηση και αναθεώρηση των διαδικασιών που χρησιμοποιούνται για την εξασφάλιση της υπολογιστική υποδομής του οργανισμού.

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.

Η OCTAVE-S έχει τις ίδιες τρεις φάσεις που περιγράφονται στην προσέγγιση OCTAVE και στην OCTAVE METHOD. Ωστόσο, οι διαδικασίες είναι κάπως διαφορετικές από αυτές της OCTAVE METHOD. (5)

Φάση 1*:* Δημιουργία Προφίλ των Απειλών που σχετίζονται με τα σημαντικά asset

Κατά τη διάρκεια αυτής της φάσης, οργανωτικές πληροφορίες αντλούνται και χρησιμοποιούνται για να καθορίσουν τα προφίλ απειλής για τρία έως πέντε κρίσιμα assets.

Διαδικασία 1: Εντοπισμός Οργανωτικών Πληροφοριών

Η ομάδα ανάλυσης προσδιορίζει τα σημαντικά περιουσιακά στοιχεία πληροφοριών που σχετίζονται με τον οργανισμό, ορίζει ένα σύνολο κριτηρίων αξιολόγησης των επιπτώσεων, και καθορίζει την τρέχουσα κατάσταση των πρακτικών ασφάλειας του οργανισμού.

Διαδικασία 2: Δημιουργία προφίλ Απειλής

Η ομάδα ανάλυσης επιλέγει 3-5 περιουσιακά στοιχεία που σχετίζονται με κρίσιμες πληροφορίες και καθορίζει τις απαιτήσεις ασφαλείας και τα προφίλ απειλής για αυτά τα στοιχεία.

Φάση 2: Προσδιορισμός Αδυναμιών στις Υποδομές

Κατά τη διάρκεια αυτής της φάσης, η ομάδα ανάλυσης παίρνει μια υψηλού επιπέδου επισκόπηση των πρακτικών των υποδομών και των πρακτικών που σχετίζονται με το τεχνολογικό κομμάτι για να βελτιώσετε τα προφίλ των απειλών.

Διαδικασία 3: Εξετάστε τις υποδομές πληροφορικής σε σχέση με κρίσιμα στοιχεία του ενεργητικού

Η ομάδα ανάλυσης αναλύει τα μονοπάτια πρόσβασης στα συστήματα που αποτελούν τα κρίσιμα στοιχεία και καθορίζει το πόσο καλά οι διαδικασίες που σχετίζονται με την τεχνολογία μπορούν να τα προστατεύσουν.

Φάση 3: Ανάπτυξη Στρατηγικής Ασφάλειας και Σχέδια

Κατά τη διάρκεια αυτής της φάσης, οι κίνδυνοι για τα κρίσιμα στοιχεία αξιολογούνται και ορίζονται οργανωτικές στρατηγικές προστασίας και μέτρα άμβλυνσης του κινδύνου.

Διαδικασία 4: Προσδιορισμός και ανάλυση των κινδύνων

Η ομάδα ανάλυσης αξιολογεί όλους τους ενεργούς κινδύνους για την επίδραση και, προαιρετικά, την πιθανότητα εμφάνισης του κινδύνου.

Διαδικασία 5: Ανάπτυξη στρατηγικών προστασίας και σχέδια μετριασμού των επιπτώσεων

Η ομάδα αναπτύσσει σχέδια για στρατηγικές προστασίας και μετριασμό του κινδύνου που βασίζονται πρακτικές ασφάλειας.

Η μέθοδος OCTAVE-S τεκμηριώνεται στον Οδηγό Εφαρμογής OCTAVE Μέθοδος (OMIG) (4).

1.4.3 Εμπειρίες με octave-s και octave-method

Υπήρξε μια σημαντική ποικιλομορφία ως προς τον τύπο, το μέγεθος, και τις επιχειρηματικές αγορές των οργανισμών που έχουν χρησιμοποιήσει με επιτυχία τις υπάρχουσες μεθόδους OCTAVE. Μέσω αυτών, οι οργανισμοί έχουν επιτύχει αξιοθαύμαστα αποτελέσματα με την εφαρμογή, την προσαρμογή και τη θεσμοθέτηση της μεθόδου OCTAVE, είτε στην αρχική της μορφή (OCTAVE method) είτε με ανανεωμένη της (OCTAVE-S), για να ταιριάζει η φιλοσοφία της αξιολόγησης των κινδύνων τους με την οργανωτική δομή και τον πολιτισμό τους. Η δυνατότητα τους να συνδέσουν τους οργανωτικούς στόχους και αντικείμενα με τους στόχους της ασφάλειας της πληροφορίας είναι το κύριο όφελος της OCTAVE. Οργανισμοί που εφαρμόζουν με επιτυχία αυτή την προσέγγιση είναι συνεχώς σε θέση να φέρουν μια οργανωτική και επιχειρησιακή άποψη για τις δραστηριότητες διαχείρισης κινδύνων που αφορούν την ασφάλεια της πληροφορίας, επιτρέποντάς τους να εξελιχθούν από τη διαχειριστές των ευπαθειών και των αντιδραστικών δραστηριοτήτων σε διαχειριστές των κινδύνων για την ασφάλεια της πληροφορίας.

Η συλλογική άποψη της μεθόδου OCTAVE παρέχει μια διεπιστημονική προοπτική για τον εντοπισμό του κινδύνου, την αξιολόγηση και τη μείωση της επικινδυνότητας. Παρόλα αυτά η συλλογή των δεδομένων, που βασίζεται σε ομάδες ατόμων, και οι συνεχείς διεργασίες ανάλυσης των υφιστάμενων μεθόδων της OCTAVE συγκεντρώνει διαφορετικές ομάδες της οργάνωσης κάτω από ένα κοινό σκοπό. Ως αποτέλεσμα αυτής της συνεργασίας, ο οργανισμός περιορίζει την ικανότητα του να εντοπίζει και μειώνει κινδύνους, όπως

- ελλείψεις στους οργανωτικούς διαύλους επικοινωνίας
- ποικίλα επίπεδα κατανόησης και επικοινωνίας των πολιτικών σε οργανωτικό επίπεδο
- κενά στις πρακτικές και στα επιδιωκόμενα αποτελέσματά τους

Επιπλέον, αυτές οι δύο μεθοδολογίες εξασφαλίζουν διαφορετικότητα κατανόησης και ποικίλες απόψεις, που ενισχύουν περαιτέρω το εύρος και την ποιότητα της αξιολόγησης των κινδύνων καθώς τον μετριασμό του κινδύνου των δραστηριοτήτων.

1.4.4 Κίνητρο για μία νέα προσέγγιση που οδηγεί στην octave allegro

Ενώ οι οργανισμοί συνεχίζουν να εφαρμόζουν με επιτυχία την OCTAVE method και την OCTAVE-S, έχει περάσει σημαντικό χρονικό διάστημα από τότε που οι δυο μέθοδοι πρωτοεισήχθησαν. Το τοπίο των κινδύνων για την ασφάλεια της πληροφορίας που διαχειρίζονται οι οργανισμοί και οι ικανότητες τους για τη διαχείριση των κινδύνων αυτών έχει αλλάξει σημαντικά από τότε που εισήχθησαν αυτές οι μέθοδοι. Επιπλέον, υπάρχει σημαντική γνώση που αποκτήθηκε μέσα από την εφαρμογή και τη διδασκαλία της OCTAVE, καθώς και παρατηρώντας άλλους οργανισμούς κάνοντας χρήση της μεθόδου κατά τα τελευταία οκτώ χρόνια, που αποτελεί τη βάση για τη βελτίωση της. (6)

Μία από τις ιδέες που αποκτήθηκαν μέσω αυτών των εμπειριών, είναι η ανάγκη να προχωρήσουμε σε μια πιο πληροφοριοκεντρική εκτίμηση του κινδύνου. Όταν τα περιουσιακά στοιχεία που σχετίζονται με την πληροφορία είναι στο επίκεντρο της αξιολόγησης της ασφάλειας των πληροφοριών, όλα τα άλλα περιουσιακά στοιχεία μπορούν εύκολα να συμμετέχουν στη διαδικασία ως μέρη όπου τα περιουσιακά στοιχεία

με την πληροφορία αποθηκεύονται, μεταφέρονται, ή υποβάλλονται σε επεξεργασία. Ένα τέτοιο μέρος μπορεί να είναι ένα πρόσωπο (δεδομένου ότι οι άνθρωποι μπορούν να αποθηκεύουν πληροφορίες, όπως η γνώση, μεταφορά πληροφοριών από την επικοινωνία, ή τη διαδικασία σκέψης και δράσης), ένα αντικείμενο (π.χ. ένα κομμάτι χαρτί), ή μια τεχνολογία (π.χ. ένα database). Έτσι, οι απειλές για τα περιουσιακά στοιχεία πληροφοριών προσδιορίζονται και εξετάζονται μέσα από την εξέταση του 'τόπου κατοικίας' τους, η οποία περιορίζει ουσιαστικά τον αριθμό και το είδος των περιουσιακών στοιχείων που συμμετέχουν στη διαδικασία.

Επιπλέον, εστιάζοντας σε συγκεκριμένα περιουσιακά στοιχεία περιορίζονται αποτελεσματικά οι πληροφορίες που πρέπει να συγκεντρωθούν, επεξεργαστούν, οργανωθούν, αναλυθούν και κατανοηθούν για να εκτελεστεί μια αξιολόγηση του κινδύνου.

Τέλος, δεδομένου του μεγέθους και της πολυπλοκότητας της μεθόδου είναι εύκολο να φανταστούμε ότι ορισμένοι οργανισμοί έχουν σημαντικά προβλήματα όσον αφορά στην ενσωμάτωση και στην χρήση των προσεγγίσεων της OCTAVE. Η απορρόφηση σε εκατοντάδες σελίδες εγγράφων της διαδικασίας, η κατανόηση των συνοδευτικών φύλλων εργασίας και πώς να τα χρησιμοποιούν, καθώς και η συλλογή και οργάνωση των απαιτούμενων δεδομένων μπορεί να είναι μία επίπονη διαδικασία. Έπειτα από μελέτη, ο τεράστιος όγκος της συλλογής δεδομένων αποτελεί εμπόδιο για ορισμένους οργανισμούς, ώστε να φτάσουν στο στάδιο της ανάλυσης και μετριασμού των κινδύνων. Μια απλουστευμένη διαδικασία που μειώνει την ασάφεια και είναι πιο δομημένη μπορεί να είναι πιο εύκολο να εφαρμοστεί από οργανισμούς που βρίσκουν ότι οι υπάρχουσες μέθοδοι της OCTAVE είναι υπερβολικά δύσχρηστες.

Έχοντας λοιπόν ως βάση τις γνώσεις, τις ιδέες και τους προβληματισμούς που αποκτήθηκαν από τότε που η πρώτη μέθοδος OCTAVE εισήχθη, φάνηκε ότι απαιτείται μια αναθεωρημένη προσέγγιση για την εκτέλεση αξιολόγησης κινδύνων ασφάλειας πληροφοριών. Η εμπειρία που αποτελεί την προαναφερθείσα βάση βοηθά για τον καθορισμό συνόλου των απαιτήσεων στις οποίες η μέθοδος OCTAVE θα πρέπει να ανταποκρίνεται, μέσα σε μεταβαλλόμενες οργανωτικές ανάγκες και σε πιο σύνθετα λειτουργικά περιβάλλοντα κινδύνου. Έτσι, δημιουργήθηκε η OCTAVE ALLEGRO. (7).

1.4.5 Γενικές απαιτήσεις για octave allegro

Οι απαιτήσεις χρησιμεύουν όχι μόνο για να περιγράψει τι πρέπει να οικοδομήσουμε και γιατί είναι υπό κατασκευή αλλά είναι ένας τρόπος για να εκτιμηθεί αν μια δραστηριότητα υπήρξε επιτυχής. Το πρώτο βήμα στην ανάπτυξη μια ανανεωμένης προσέγγισης OCTAVE είναι να ενσωματώσει μια σειρά από απαιτήσεις σχεδιασμού (που προέρχεται από τη χρήση, την παρατήρηση, και την εμπειρία). Οι απαιτήσεις αυτές περιλαμβάνουν

- βελτίωση της ευκολίας της χρήσης
- βελτίωση του ορισμό του πεδίου εφαρμογής αξιολόγησης
- μείωση των απαιτήσεων κατάρτισης και γνώσης
- μείωση στη δέσμευση πόρων
- ενθάρρυνση θεσμοθέτησης
- παραγωγή συνεχών και συγκρίσιμων αποτελεσμάτων για ολόκληρη την επιχείρηση
- διευκόλυνση της ανάπτυξης ενός πυρήνα με ικανότητα αξιολόγησης του κινδύνου

- υποστήριξη των απαιτήσεων συμμόρφωσης των επιχειρήσεων

Κάθε μία από αυτές τις γενικές απαιτήσεις συζητείται στις ακόλουθες παραγράφους.

Βελτίωση της ευκολίας της χρήσης

Η πρώτη απαίτηση για μία βελτιωμένη μέθοδο είναι η ευκολία στη χρήση, όπως ορίζεται σε αρκετές διαστάσεις. Αυτές οι διαστάσεις περιλαμβάνουν:

- ελαχιστοποίηση του μεγέθους και της πολυπλοκότητας των διαδικασιών που πρέπει να εφαρμοστούν
- μείωση της ποσότητας των δεδομένων που πρέπει να συλλέγονται και να διαχειρίζονται κατά τη διάρκεια όλης της διαδικασίας
- έλεγχος του αριθμού και της ποικιλίας των φύλλων εργασίας που πρέπει να συμπληρωθούν
- εστίαση της διαδικασίας σε προσδιορίσιμες και διαχειρίσιμες πληροφορίες για τα περιουσιακά στοιχεία με την πληροφορία

Η μείωση των εγγενών προκλήσεων που τίθενται από τους μηχανικούς των παλιών μεθόδων OCTAVE διασφαλίζει ότι η διαδικασία αυτή εστιάζει στη δραστηριότητα αξιολόγησης του κινδύνου και τον προσδιορισμό και την ανάλυση πληροφοριών κινδύνων για την ασφάλεια και όχι στην ικανοποίηση ενός εκτεταμένου συνόλου κατευθυντήριων γραμμών και των δραστηριοτήτων.

Βελτίωση του ορισμό του πεδίου εφαρμογής αξιολόγησης

Ορίζοντας με ακρίβεια το πεδίο εφαρμογής της αξιολόγησης του κινδύνου δεν βελτιώνει μόνο τα αποτελέσματα της αξιολόγησης, αλλά οδηγεί δυνητικά σε λιγότερη συνολική προσπάθεια. Έτσι, πρωταρχική απαίτηση της OCTAVE Allegro είναι να επιτρέπει στους χρήστες να επικεντρώνονται στα περιουσιακά στοιχεία που είναι πιο σημαντικά, διασφαλίζοντας ότι έχουν επιλεγεί για έλεγχο μέσα από μια συστηματική και συνεπή διεργασία. Με την εστίαση αποκλειστικά και μόνο σε στοιχεία του ενεργητικού που περιέχουν πληροφορίες και σε άλλα στοιχεία, όπως οι άνθρωποι, η τεχνολογία, και τις εγκαταστάσεις που συνδέονται με τις πληροφορίες των περιουσιακών στοιχείων, η οργάνωση έχει μια καλύτερη ευκαιρία να καθορίσει ένα διαχειρίσιμο πεδίο εφαρμογής από την αρχή, μειώνοντας έτσι δυνητικά την προσπάθεια που απαιτείται για την αναγνώριση απειλών, την ανάλυση, και σχεδιασμό μετριασμού του κινδύνου.

Μείωση των απαιτήσεων κατάρτισης και γνώσης

Μια ενημερωμένη προσέγγιση της OCTAVE θα πρέπει να μπορεί να φτάσει στην μοντελοποίηση. Ένας τρόπος για να επιτευχθεί αυτό είναι μέσω της μείωσης των απαιτούμενων επιπέδων γνώσεων και κατάρτισης για τη διενέργεια αποτελεσματικής αξιολόγησης κινδύνων. Ελαχιστοποιώντας την γνώση της διαχείρισης κινδύνου και της τεχνολογίας της πληροφορίας που απαιτείται, αυξάνει αποτελεσματικά το εύρος του προσωπικού που μπορεί να συμμετάσχει στη διαδικασία αξιολόγησης με χαμηλή κατάρτιση και ελάχιστη καθοδήγηση. Η μειωμένη απαίτηση γνώσεων και κατάρτισης, όχι μόνο χαμηλώνει το κόστος που σχετίζεται με την αξιολόγηση των κινδύνων αλλά μπορεί να αυξήσει δυναμικά την εξάπλωση της μεθοδολογίας σε όλη την οργάνωση. Επιπλέον, στην περίπτωση της κανονιστικής συμμόρφωσης, η δυνατότητα να εκπαιδεύσει

περισσότερους ανθρώπους για να εκτελέσει εκτίμηση κινδύνου βελτιώνει αποτελεσματικά τη γενική ικανότητα του οργανισμού για τη διαχείριση της συμμόρφωσης.

Μείωση στη δέσμευση πόρων

Η εκτίμηση κινδύνου είναι μια απαραίτητη δραστηριότητα για τον οργανισμό, αλλά μια μέθοδος αξιολόγησης με έντονη εκμετάλλευση των πόρων του οργανισμού, μπορεί να μην είναι αρκετά αποτελεσματική ώστε να δικαιολογήσει την επένδυση των ανθρώπων. Για την βελτιστοποίηση της χρήσης των πόρων, μία ενημερωμένη προσέγγιση της OCTAVE πρέπει:

- να είναι λιγότερο δύσκολο να χρησιμοποιηθεί
- να απαιτεί λιγότερη χειραγώγηση των δεδομένων (με τη βελτίωση της ροής της διαδικασίας, την ιεράρχηση των δραστηριοτήτων, καθώς και την ποσότητα και το είδος των δεδομένων που συλλέγονται)
- να προβεί σε εξορθολογισμό των διαδικασιών για τον εντοπισμό και μείωσης των κινδύνων (εστιάζοντας αποκλειστικά σε στοιχεία του ενεργητικού που αφορούν πληροφορίες, με τη βελτίωση των μεθόδων ταυτοποίησης απειλών, και τη βελτίωση του τρόπου με τον οποίο οι κίνδυνοι τεκμηριώνονται και αναλύονται)
- να βελτιώσει την τεκμηρίωση και την οργάνωση των δεδομένων (με αποτελεσματικό και ουσιαστικό σχεδιασμό φύλλων εργασίας και μειώνοντας την ποσότητα των δεδομένων μεταφοράς)
- να είναι αυτοδιορθωτική (με την οικοδόμηση σημείων ελέγχου και τις ισορροπιών που επιτρέπουν στους χρήστες να συνειδητοποιήσουν ότι είναι εκτός θέματος, πριν προλάβουν να δαπανήσουν σημαντικούς πόρους)

Ενθάρρυνση θεσμοθέτησης

Για να είναι αποτελεσματικές, οι δραστηριότητες αξιολόγησης των κινδύνων πρέπει να είναι μέρος μιας μεγαλύτερης συνεχούς διαδικασίας διαχείρισης των κινδύνων. Τοποθετημένη σωστά, η εκτίμηση κινδύνου χρησιμεύει ως διαγνωστικό στοιχείο της συνεχούς διαχείρισης του κινδύνου. Ο οργανισμός χρησιμοποιεί την αξιολόγηση του κινδύνου να καθορίσει το καθεστώς των ελέγχων που έχει θέσει ήδη σε εφαρμογή για τη διαχείριση της ασφάλειας των πληροφοριών και προετοιμάζει και υλοποιεί σχέδια για την αντιμετώπιση όποιων κενών έχουν εντοπιστεί. Έτσι, η εκτίμηση του κινδύνου όχι μόνο βοηθά τον οργανισμό να καθορίσει μια τιμή αναφοράς από την οποία μπορεί να προέλθει μία μέτρηση, αλλά τον βοηθά επίσης στην τρέχουσα κατάσταση να κρατήσει τον παλμό της αποτελεσματικότητας της ασφάλειας μέσω της επαναλαμβανόμενης και της συνεπής χρήση μέσα από πάροδο του χρόνου.

Για να ενθαρρυνθεί η χρήση της εκτίμησης κινδύνου ως ένα εργαλείο συνεχούς διαδικασίας διαχείρισης κινδύνων, η εκσυγχρονισμένη μέθοδος OCTAVE πρέπει να δίνει πρόσβαση σε όσο το δυνατόν πιο πολλούς χρήστες της οργάνωσης, να απαιτεί χαμηλά επίπεδα προσπάθειας και των επενδύσεων, και να έχει ως στόχο να παράγει, με συνέπεια, σημαντικά αποτελέσματα.

Παραγωγή συνεχών και συγκρίσιμων αποτελεσμάτων για ολόκληρη την επιχείρηση

Ένας οργανισμός πρέπει να είναι σε θέση να κάνει χρήση των αποτελεσμάτων της αξιολόγησης των κινδύνων για την ασφάλεια πληροφοριών με έναν τρόπο που να υποστηρίζει και να επιτρέπει μια μεγαλύτερη επιχειρησιακή προσπάθεια διαχείρισης του κινδύνου. Αυτό προϋποθέτει η μεθοδολογία να επιτρέπει στον οργανισμό να επιτύχει όχι μόνο συνεπή αποτελέσματα την πάροδο του χρόνου, αλλά τα αποτελέσματα αυτά να είναι συγκρίσιμα μεταξύ διαφορετικών λειτουργικών μονάδων και τομέων δραστηριοτήτων του οργανισμού. Επιπλέον, τα αποτελέσματα που παράγονται από τη μεθοδολογία πρέπει να είναι ένας παράγοντας επιτυχούς εκτέλεση των βημάτων μεθοδολογίας, που δεν εξαρτάται αποκλειστικά από την ομάδα ανάλυσης που εκτελεί την αξιολόγηση.

Διευκόλυνση της ανάπτυξης ενός πυρήνα με ικανότητα αξιολόγησης του κινδύνου

Μια κουλτούρα που βασίζεται στην επίγνωση των κινδύνων προκύπτει όταν οι εργαζόμενοι σε όλη την οργάνωση καλλιεργούν ένα σύνολο ικανοτήτων που αφορά στη διαχείριση κινδύνου και χρησιμοποιούν αυτή τη γνώση ως κατευθυντήρια δύναμη για την εκτέλεση ευθυνών που προκύπτουν στη δουλειά τους σε καθημερινή βάση. Μαθαίνοντας να εκτελούν την εκτίμηση κινδύνου είναι ένα θεμελιώδης τρόπος για τη βελτίωση αυτών των ικανοτήτων και έτσι μπορούν να προωθήσουν μια κουλτούρα για την επίγνωση των κινδύνων μέσα στον οργανισμό. Ωστόσο, αυτό απαιτεί ότι η μεθοδολογία αξιολόγησης κινδύνου είναι προσβάσιμη, έχουν χαμηλά εμπόδια στη χρήση (όπως ο βαθμός στον οποίο η εξειδικευμένη εκπαίδευση είναι απαραίτητη), και παράγει σημαντικά αποτελέσματα που μπορούν να βοηθήσουν τους εργαζόμενους να αποδίδουν καλύτερα τη δουλειά τους.

Υποστήριξη των απαιτήσεων συμμόρφωσης των επιχειρήσεων

Οι δραστηριότητες, που αφορούν την ασφάλεια των πληροφοριών, σε πολλούς οργανισμούς που καθοδηγούνται από την ανάγκη τους να διαχειριστούν ένα όλο και πιο ελεγχόμενο περιβάλλον. Όσο οι οργανισμοί πρέπει να επικεντρώνονται στη διαχείριση των κινδύνων, θέλουν να είναι σε θέση να δρουν γρήγορα και να επιτυγχάνουν αποτελεσματική συμμόρφωση. Έτσι, μια μεθοδολογία αξιολόγησης του κινδύνου πρέπει να είναι σε θέση να υποστηρίξει εύκολα δραστηριότητες διαχείρισης κινδύνων ασφάλειας πληροφοριών, για τις οποίες μπορεί να απαιτηθεί η συμμόρφωση με διάφορους νόμους και κανονισμούς.

1.4.6 Ειδικές βελτιώσεις στην octave allegro

Η προηγούμενη ενότητα περιγράφει τις βασικές απαιτήσεις για την επικαιροποίηση των υφιστάμενων μεθόδων OCTAVE. Σε αυτή την ενότητα, συζητούνται συγκεκριμένες βελτιώσεις που έχουν ενσωματωθεί στην OCTAVE Allegro μεθοδολογία για να πληρούν αυτές τις απαιτήσεις.

Συλλογή δεδομένων και Βελτίωση Προσανατολισμού

Κατά την ανάπτυξη της OCTAVE Allegro, δόθηκε ιδιαίτερη προσοχή στην ελαχιστοποίηση του αποτυπώματος_της διαδικασίας. Αυτό συμβάλλει στην ευκολία της χρήσης, υποστηρίζει την επίτευξη ουσιαστικών αποτελεσμάτων με ελάχιστες δεσμεύσεις πόρων, και ενθαρρύνει την μακροπρόθεσμη επαναληψιμότητα της διαδικασίας.

Οι διαδικασίες συλλογής δεδομένων μέσω εργαστηρίου, αναπόσπαστα συνδεδεμένες με τις υπάρχουσες μεθόδους OCTAVE έχουν εξαλειφθεί και αντικατασταθεί με απλουστευμένα φύλλα εργασίας και δομημένη καθοδήγηση. Αυτό μειώνει την αναγκαία

δέσμευση πόρων για τη διαδικασία για τα άτομα εκτός της ομάδας ανάλυσης και εξαλείφει την δέσμευση αυτών που συμμετείχαν γενικά στον προγραμματισμό και συντονισμό των εργασιών. Επιπλέον, ο όγκος της καθοδήγησης και τα απαιτούμενα φύλλα εργασίας έχουν μειωθεί δραστικά για την παροχή μόνο των απαραίτητων θεμελιακών στοιχείων και των βημάτων της διαδικασίας. Έτσι, η χρησιμότητα της μεθόδου έχει βελτιωθεί μέσα από λιγότερα, περισσότερο εστιασμένα βήματα και έχει κατευθυνθεί στην ανάπτυξη δεξιοτήτων που αφορούν την διαχείριση κινδύνων, παρά στην καλλιέργεια βασικών εγκαταστάσεων και αρχών της μεθόδου.

Βελτιωμένη εστίασης στα περιουσιακά στοιχεία

Στις υπάρχουσες μεθόδους OCTAVE, τα περιουσιακά στοιχεία αποτελούνται από ανθρώπους, πληροφορίες, συστήματα, υπηρεσίες και εφαρμογές, μέχρι και λογισμικό. Ενώ όλοι αυτοί οι τύποι περιουσιακών στοιχείων είναι σημαντικοί για την εκτίμηση του κινδύνου, σε ορισμένους χρήστες προκαλείται σύγχυση να θεωρήσουν περιουσιακά στοιχεία άλλα, εκτός από αυτά που σχετίζονται με τις πληροφορίες, διότι οδηγούνται μερικές φορές σε ορισμό περιουσιακού στοιχείου που είναι πολύ ευρύς ή στενός για την εκτίμηση του κινδύνου. Ο πρωταρχικός στόχος της μεθόδου OCTAVE Allegro ο ορισμός του περιουσιακού στοιχείου πληροφοριών. Όλα τα υπόλοιπα περιουσιακά στοιχεία αναγνωρίζονται και αξιολογούνται στο πλαίσιο κατά το οποίο είναι συνδεδεμένα με τα περιουσιακά στοιχεία πληροφοριών. Αυτό εξαλείφει την πιθανή σύγχυση και μειώνει την πιθανότητα να πραγματοποιηθεί εκτεταμένη συλλογή και ανάλυση των δεδομένων για περιουσιακά στοιχεία που θα βρεθούν αργότερα να είναι ανεπαρκώς καθορισμένα, έξω από το πεδίο της εκτίμησης, ή χρειάζονται περαιτέρω αποσύνθεση. (7)

- *Φτιάχνοντας το προφίλ των περιουσιακών στοιχείων πληροφορίας*

Η OCTAVE Allegro απαιτεί από τους οργανισμούς που δημιουργούν προφίλ των περιουσιακών στοιχείων πληροφορίας να παρέχουν έναν πιο ακριβή ορισμό των ορίων αυτών των στοιχείων με τη δημιουργία συνεπών, ξεκάθαρων, και συμφωνηθέντων ορισμών για το περιουσιακό στοιχείο. Μέσα από το προφίλ αυτό, ένας οργανισμός αποδίδει την κυριότητα, ορίζει τις απαιτήσεις ασφάλειας, και συλλαμβάνει την αξία του περιουσιακού στοιχείου. Μόλις ένα προφίλ έχει δημιουργηθεί, μπορεί να επαναχρησιμοποιηθεί και να ενημερωθεί σε επόμενες αξιολογήσεις. Αυτό υποστηρίζει την καθιέρωση βάσεων πληροφοριών για τις μελλοντικές εκτιμήσεις και υποστηρίζει την επαναληψιμότητα της μεθόδου.

- *Ορισμός και χρησιμοποίηση των απαιτήσεων ασφάλειας των περιουσιακών στοιχείων πληροφοριών*

Απαιτήσεις ασφάλειας όπως, εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα, είναι μέρος του DNA ενός περιουσιακού στοιχείου πληροφοριών. Πρόκειται για απαιτήσεις του περιουσιακού στοιχείου που εξασφαλίζουν την προστασία και τη βιωσιμότητα του. Ανεξάρτητα από το πού το περιουσιακό στοιχείο αποθηκεύεται, μεταφέρεται, ή υποβάλλεται σε επεξεργασία, ή ακόμα που έχει θεματοφυλακή (είτε εντός είτε εκτός του οργανισμού), οι απαιτήσεις ασφάλειας του περιουσιακού στοιχείου ζουν με αυτό καθ' όλη την ωφέλιμη 'ζωή' του.

Ορίζοντας τις απαιτήσεων ασφαλείας για τα περιουσιακά στοιχεία πληροφοριών η OCTAVE Allegro μειώνει την πιθανή σύγχυση γύρω από τον ορισμό και την εφαρμογή

των απαιτήσεων ασφαλείας στη διαδικασία εκτίμησης κινδύνου. Στις υπάρχουσες μεθόδους OCTAVE, οι απαιτήσεις ασφαλείας δεν σχετίζονται ειδικά με περιουσιακά στοιχεία πληροφοριών και έτσι οι χρήστες συχνά αναπτύσσουν και προσπαθούν να εφαρμόσουν αυτές τις έννοιες στο ανθρώπινο δυναμικό και στην τεχνολογική υποδομή. Αυτό προκαλεί σε ορισμένους χρήστες προβλήματα στην αναγνώριση των κινδύνων και στην ανάλυση αυτών. Επιπλέον, οι απαιτήσεις ασφάλειας είναι ένα θεμελιώδες στοιχείο για το σχεδιασμό και την εφαρμογή σχεδίων μετριασμού του κινδύνου. Η OCTAVE Allegro απαιτεί ρητώς από τους χρήστες να λάβουν υπόψη τις επιπτώσεις των συνεπειών του κινδύνου σχετικά με τις απαιτήσεις ασφάλειας και τις δράσεις για τον μετριασμό αυτών.

Βελτιωμένη Αναγνώριση Απειλής

Οι υπάρχουσες μέθοδοι OCTAVE χρησιμοποιούν τα δέντρα απειλή ως οδηγό για τον εντοπισμό απειλών. Όσο κι αν αυτά τα δέντρα παρέχουν ένα δομημένο μέσο για τον εντοπισμό και την εξέταση διαφόρων σεναρίων περί απειλών, μπορούν μερικές φορές να προκαλέσουν σύγχυση στη χρήση, ειδικά για χρήστες με περιορισμένη εμπειρία διαχείρισης κινδύνων. Για παράδειγμα, κάθε μονοπάτι σε ένα δέντρο απειλή της OCTAVE είναι μια γενική διάρθρωση μιας απειλής- για να κάνουν αποτελεσματική χρήση αυτών των δέντρων, οι συμμετέχοντες στην εκτίμηση OCTAVE πρέπει να γίνει ειδήμονες στη μετάφραση αυτών των γενικών μονοπατιών σε σενάρια πραγματικού κόσμου. Όταν οι χρήστες αδυνατούν να κάνουν αυτή τη μετάφραση, επηρεάζεται σημαντικά η ευρωστία του εντοπισμού των κινδύνων και απειλών.

Επιπλέον, οι χρήστες συχνά αποτυγχάνουν να συνειδητοποιήσουν ότι κάθε διαδρομή στα δέντρα απειλή μπορεί να ισοδυναμεί με ένα ή περισσότερα από ένα σενάρια πραγματικού κόσμου. Αυτό είναι σημαντικό γιατί ακόμη κι αν πολλές απειλές μοιράζονται το ίδιο κίνητρο και αποτέλεσμα, μπορεί να απαιτείται σημαντικά διαφορετική προσέγγιση για μετριασμού. Επιπλέον, υπερβολική εξάρτηση από τα δέντρα απειλή για την αναγνώριση απειλών (αντί της ενεργού συζήτηση και ανάπτυξη σεναρίων) μπορεί να ελαττώσει σημαντικά τη συνολική αποτελεσματικότητα της διαδικασίας για την εκτίμηση του κινδύνου.

Η OCTAVE Allegro χρησιμοποιεί ερωτηματολόγια για σενάρια απειλής και όχι δέντρα, για να βοηθήσει τους χρήστες να εντοπίζουν τις απειλές που σχετίζονται με ένα περιουσιακό στοιχείο πληροφοριών. Τα ερωτηματολόγια βασίζονται στα δέντρα απειλή που συμπεριλαμβάνονται στη μέθοδο OCTAVE και έτσι εξασφαλίζουν μια ευρεία εξέταση των πιθανών απειλών. Ωστόσο, τα ερωτηματολόγια σχεδιάζονται γύρω από το μέρος στο οποίο φιλοξενείται το περιουσιακό στοιχείο, έτσι ώστε οι χρήστες να εστιάσουν στις απειλές που σχετίζονται με ένα περιουσιακό στοιχείο πληροφοριών όταν αποθηκεύονται, μεταφέρονται, ή υποβάλλονται σε επεξεργασία σε ένα συγκεκριμένο μέρος. Αυτό απλοποιεί τη δομή του ερωτηματολογίου και μειώνει το συνολικό χρόνο που απαιτείται για βρούμε μια αντιπροσωπευτική λίστα από πιθανές απειλές.

Προσέγγιση με χαμηλά τεχνολογικά στάνταρ

Η OCTAVE Allegro χρειάζεται μια ριζικά διαφορετική προσέγγιση για το τεχνολογικό περιβάλλον ενός οργανισμού, και για τη σχέση της με τα περιουσιακά στοιχεία πληροφοριών, σε σχέση με τις προσεγγίσεις που γίνονται από τις υπάρχουσες OCTAVE μεθόδους. Αντί να τρέχει εργαλεία για εύρεση αδυναμιών και να κάνει χρήση των

αποτελεσμάτων για την αναγνώριση της απειλής, στην OCTAVE Allegro οι χρήστες χαρτογραφούν ένα περιουσιακό στοιχείο πληροφοριών και αναγνωρίζουν το μέρος στο οποίο η πληροφορία είναι αποθηκευμένη, μεταφέρεται, ή υποβάλλεται σε επεξεργασία και εξετάζει τις απειλές σε κάθε μία από αυτές τις τοποθεσίες. Υπάρχει ακόμα μια τεχνολογική άποψη, αλλά δεν εμποδίζεται από την εκτέλεση δυσκίνητη εργαλείων που απαιτούν εξειδικευμένες γνώσεων και κατασπατάληση πόρων.

- *Εξάλειψη των τεστ αδυναμιών*

Ο προσδιορισμός των τρωτών σημείων είναι ένα σημαντικό μέσο για τον εντοπισμό του κινδύνου. Ωστόσο, μπορεί να είναι μια χρονοβόρα δραστηριότητα που παραπλανεί τελικά τη δραστηριότητα αξιολόγησης του κινδύνου. Η χρήση και η εκτέλεση των εργαλείων αυτών, καθώς και η ανάλυση των αποτελεσμάτων τους, αποτελούν δυσκίνητες εργασίες, ακόμη και για οργανισμούς που εκτελούν αυτές τις εργασίες σε τακτική βάση. Στην πράξη, πολλοί χρήστες των υφισταμένων μεθόδων OCTAVE διαπιστώνουν ότι η εκτέλεση τέτοιων εργαλείων στην πραγματικότητα οδηγεί σε απώλεια δυναμικής και δεν παρέχει πρόσθετες πληροφορίες, που δεν μπορούν να αποκτηθούν μέσω των σεναρίων απειλή. Αυτό είναι ιδιαίτερα σημαντικό για τους οργανισμούς που εκτελούν την πρώτη τους εκτίμηση κινδύνου ή για αυτές που δε έχουν εμπειρία στη χρήση αυτών των εργαλείων.

Επιπλέον, επειδή πολλοί οργανισμοί συγχέουν την εκτίμηση αδυναμιών με την εκτίμηση κινδύνου, οι οργανισμοί διακόπτουν μερικές φορές τις διαδικασίες της OCTAVE με την εσφαλμένη πεποίθηση ότι τα τρωτά σημεία που έχουν εντοπιστεί είναι κίνδυνοι. Αλλά μόνο μέσω της ανάλυσης των πιθανών αποτελεσμάτων και των επιπτώσεων των αδυναμιών μπορούν να θεωρηθούν κίνδυνοι που πρέπει να αντιμετωπιστούν.

Η απαίτηση για τη λειτουργία των εργαλείων εύρεσης αδυναμιών για να ολοκληρωθεί το προφίλ των κινδύνων που σχετίζονται με τις τεχνολογικές υποδομές του οργανισμού αποβάλλεται στην OCTAVE Allegro. Ωστόσο, εάν ένας οργανισμός έχει μια βασική και χρόνια ικανότητα στα εργαλεία αυτά μπορεί εύκολα να τα ενσωματώσει σε πολλές διαδικασίες της OCTAVE Allegro ώστε να παρέχουν μία πιο εύρωστη άρθρωση του κινδύνου. (8)

- *Εισαγωγή της έννοιας του μέρους που 'ζει' στο περιουσιακό στοιχείο πληροφοριών*

Όπως αναφέρθηκε προηγουμένως, η OCTAVE Allegro εισάγει της τοποθεσίας για την διαδικασία της αξιολόγησης. Η μέθοδος OCTAVE Allegro εξασφαλίζει την εξέταση όλων των τοποθεσιών στις οποίες είναι αποθηκευμένο, μεταφέρεται και υποβάλλεται σε επεξεργασία ένα περιουσιακό στοιχείο πληροφορίας, είτε εσωτερικά είτε εξωτερικά με την οργάνωση. Αυτό δεσμεύει αποτελεσματικά την αξιολόγηση και εξασφαλίζει την κατάλληλη εξέταση του πεδίου εφαρμογής.

- *Η προσθήκη της έννοιας του «χάρτη περιβάλλοντος"*

Η OCTAVE Allegro εισάγει την έννοια χάρτη που σχετίζεται με το περιβάλλον κινδύνου των πληροφοριών. Στην ουσία, αυτός ο χάρτης βοηθά το χρήστη να καθορίσει όλα τα μέρη όπου είναι αποθηκευμένο, μεταφέρεται και υποβάλλεται σε επεξεργασία ένα περιουσιακό στοιχείο πληροφορίας. Μέσα από τη δημιουργία αυτού του χάρτη, η ομάδα ανάλυσης καθορίζει τα όρια (εσωτερικά και εξωτερικά) του περιβάλλοντος απειλής και το πεδίο εφαρμογής της αξιολόγησης του κινδύνου. Αυτό επιτρέπει μια πιο συστηματική και συνεκτική διαδικασία για την εξέταση όλων των χώρων όπου το περιουσιακό στοιχείο

μπορεί να απειλείται και μια πιο ισχυρή εξέταση του κινδύνου. Επιπλέον, ο χάρτης χρησιμεύει ως βασική τεκμηρίωση του περιβάλλοντος κινδύνου για ένα περιουσιακό στοιχείο πληροφοριών για μελλοντική εξέταση των απειλών και άλλους ελέγχους.

Δυνατότητες για Βελτιωμένη Ανάλυση

Η OCTAVE Allegro βελτιώνει σημαντικά τις δυνατότητες ανάλυσης των υφιστάμενων μεθόδων OCTAVE μέσω της εισαγωγής των φύλλων κινδύνου και της συνιστώσας της ποσοτικής ανάλυση.

- *Ανάπτυξη φύλλων εργασίας κινδύνου των περιουσιακών στοιχείων πληροφορίας*

Στην OCTAVE Allegro όλες τις σχετικές πληροφορίες για ένα συγκεκριμένο κίνδυνο ενός περιουσιακού στοιχείου πληροφοριών συλλαμβάνονται σε ένα φύλλο εργασίας. Σε αυτό το φύλλο εργασίας, απειλές και επιπτώσεις ενός κινδύνου που σχετίζεται με πληροφορίες συλλαμβάνονται, η σχετική βαθμολόγηση κινδύνου υπολογίζεται, και τα σχέδια μετριασμού και οι δραστηριότητες που τα υλοποιούν τεκμηριώνονται. Αυτό μειώνει σημαντικά την τεκμηρίωση, την οργάνωση, και τον χειρισμό των δεδομένων που απαιτείται για την εκτέλεση της αξιολόγησης του κινδύνου και παράγει μια πολύ συμπυκνωμένη άποψη για τους κινδύνους που μπορεί να κοινοποιηθεί και να διαδοθεί. Επίσης βοηθά τον οργανισμό να οργανώσει τις πληροφορίες που αφορούν τον κίνδυνο κατά τρόπο τέτοιο που να επιτρέπει την ανάλυση των βαθύτερων αιτίων και την ανάπτυξη στρατηγικών μετριασμού, ιδιαίτερα όταν αυτές οι στρατηγικές μπορούν να αντιμετωπίσουν περισσότερους από έναν κινδύνους. Επιπλέον, η ανάπτυξη των φύλλων διευκολύνει την ικανότητα του οργανισμού να εκτελέσει την ανάλυση και την αξιολόγηση σε όλες τις οργανωτικές μονάδες λόγω της τυποποιημένης μορφής.

- *Εκτέλεση ποσοτικής ανάλυσης*

Οι μέθοδοι OCTAVE είναι σε μεγάλο βαθμό ποιοτικές μεθοδολογίες εκτίμησης κινδύνου. Δηλαδή, δανείζουν τους εαυτούς τους σε ποιοτικές εκτιμήσεις και περιγραφές του κινδύνου και όχι σε ποσοτικές. Παρόλο που ο λειτουργικός κίνδυνος είναι από τη φύση του δύσκολο να ποσοτικοποιηθεί, οι οργανισμοί με σημαντική εμπειρία σε μεθοδολογίες εκτίμησης κινδύνων βασισμένες σε αριθμούς, θεωρούν μεθόδους όπως η OCTAVE κάπως δύσκολο να θεσμοθετηθούν, επειδή τους λείπει μια έμφυτη διαδικασία για την ιεράρχηση των κινδύνων.

Η OCTAVE Allegro προβλέπει απλή ποσοτική ανάλυση των κινδύνων με την εισαγωγή μιας σχετικής βαθμολογίας κινδύνου. Μια σχετική βαθμολόγηση κινδύνου είναι μια τιμή που προκύπτει από την εξέταση της ποιοτικής περιγραφής της πιθανότητας κινδύνου σε συνδυασμό με την ιεράρχηση των οργανωτικών επιπτώσεων του κινδύνου με βάση τα κριτήρια μέτρησης κινδύνου του οργανισμού. Το σκορ μπορεί να χρησιμοποιηθεί για να συγκρίνει τη σχετική σημασία των επιμέρους κινδύνων. Για παράδειγμα, όταν συγκρίνουμε δύο κινδύνους, ο κίνδυνος με την υψηλότερη βαθμολογία θεωρείται ότι είναι πιο σημαντικός σε σχέση με άλλους κινδύνους. Δεδομένου ότι τα αποτελέσματα προέρχονται σταθερά από τα κριτήρια μέτρησης του κινδύνου σε ολόκληρο τον οργανισμό, μπορούν να συγκριθούν μεταξύ τους και στο πέρασμα του χρόνου, καθώς το περιβάλλον λειτουργίας του οργανισμού αλλάζει.

Βελτιωμένος Προσανατολισμός Μετριασμού του Κινδύνου

Αποτελεσματικές στρατηγικές μετριασμού του κινδύνου πρέπει να αναπτυχθούν, για να ικανοποιηθούν οι απαιτήσεις ασφάλειας και οι έλεγχοι που θα υλοποιηθούν στην τοποθεσία όπου είναι αποθηκευμένο, μεταφέρεται και υποβάλλεται σε επεξεργασία ένα περιουσιακό στοιχείο πληροφορίας. Η μέθοδος OCTAVE Allegro (μέσω της χρήση του φύλλου εργασίας κινδύνου) ορίζει ρητά ότι για να ικανοποιηθούν τα προηγούμενα, απαιτείται με ανάπτυξη συγκεκριμένων στρατηγικών μετριασμού για κάθε τοποθεσία, όπου το περιουσιακό στοιχείο ζει. Στην ουσία, αυτό αναγκάζει το χρήστη να εξετάσει και να ελέγχει την ασφάλεια στην τοποθεσία, αν αυτή είναι επαρκής για την πρόληψη ή την άμβλυνση του κινδύνου υπό εξέταση, και τι επιπλέον έλεγχοι θα πρέπει να εφαρμοστούν

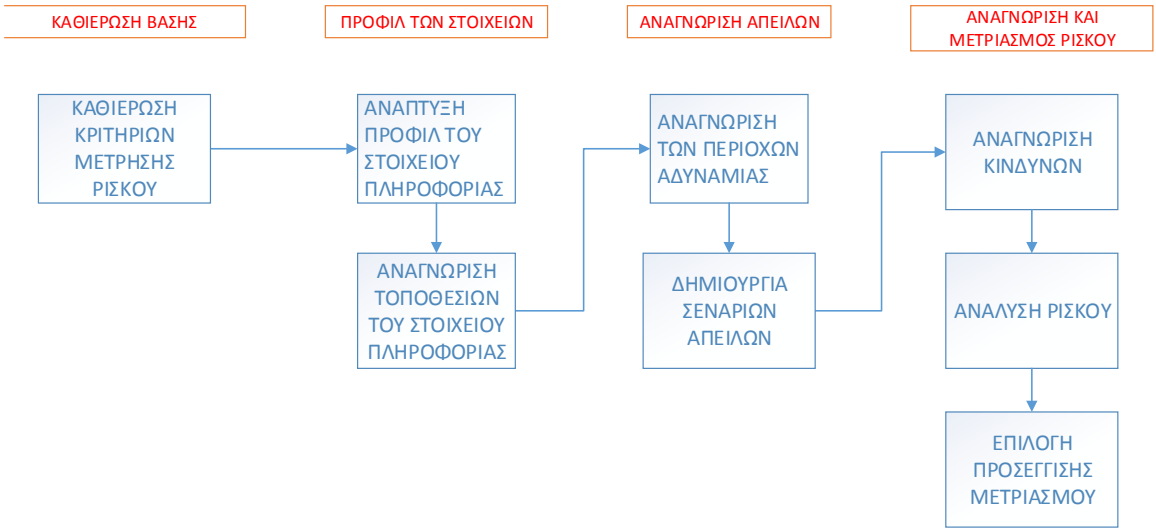
Λιγότερες Απαιτήσεις για Εκπαίδευση και Γνώση

Συνδυάζοντας μερικές από τις δομημένες έννοιες της OCTAVE–S, μαζί με μια βελτιωμένη και απλουστευμένη διαδικασία εκτίμησης και σχεδιασμού του μετριασμού των κινδύνων, η OCTAVE Allegro μειώνει σημαντικά τις απαιτήσεις γνώσεων και την κατάρτιση για την εκτέλεση μιας ισχυρής και αποτελεσματικής αξιολόγησης κινδύνων.

Η εκμάθηση της OCTAVE Allegro συνήθως διαρκεί λιγότερο χρόνο από αυτόν που χρειάζεται για τις υφιστάμενες μεθόδους, και το επίπεδο των απαιτούμενων διαδικασιών, της διαχείρισης κινδύνων, καθώς και των τεχνικών γνώσεων που απαιτούνται για τους συμμετέχοντες της ομάδας ανάλυσης σχετίζεται με την ανάπτυξη ικανοτήτων αξιολόγησης των κινδύνων και όχι στο να γίνει κάποιος επαγγελματίας διαχειριστής κινδύνου.

1.4.7 OCTAVE ALLEGRO

Η προσέγγιση της OCTAVE Allegro έχει σχεδιαστεί για να επιτρέψει ευρεία αξιολόγηση του περιβάλλοντος του λειτουργικού κινδύνου ενός οργανισμού με στόχο την παραγωγή πιο ισχυρών αποτελεσμάτων χωρίς την ανάγκη για εκτεταμένη γνώση εκτίμησης του κινδύνου. Η προσέγγιση αυτή διαφέρει από τις προηγούμενη OCTAVE προσεγγίσεις, εστιάζοντας κυρίως στα περιουσιακά στοιχεία που σχετίζονται με την πληροφορία, δηλαδή πώς χρησιμοποιούνται, πού είναι αποθηκευμένα, πού μεταφέρονται, πού γίνεται η επεξεργασία, και πώς είναι εκτεθειμένα σε απειλές, ποια είναι τα τρωτά τους σημεία, καθώς τι διαταραχές έχουμε ως αποτέλεσμα. Η OCTAVE Allegro είναι επίσης κατάλληλη για χρήση από άτομα που επιθυμούν να πραγματοποιήσουν εκτίμηση κινδύνου χωρίς εκτεταμένη οργανωτική συμμετοχή ή τεχνογνωσία. (1)



Εικόνα 3:Σχηματική απεικόνιση της octave allegro

Η προσέγγιση της OCTAVE Allegro αποτελείται από οκτώ βήματα που οργανώνονται σε τέσσερις φάσεις, όπως απεικονίζεται παραπάνω.

Στη φάση 1, ο οργανισμός αναπτύσσει κριτήρια μέτρησης του κινδύνου σύμφωνα με τους οργανωτικούς του οδηγούς.

Στη φάση 2, φτιάχνεται ένα προφίλ στα περιουσιακά στοιχεία που σχετίζονται με την πληροφορία και τα οποία θεωρούνται ύψιστης σημασίας. Αυτή η διαδικασία, καθορίζει σαφή σύνορα για το περιουσιακό στοιχείο, προσδιορίζει τις απαιτήσεις ασφαλείας, και προσδιορίζει όλες τις τοποθεσίες στις οποίες αποθηκεύεται, μεταφέρεται, ή επεξεργάζεται το στοιχείο αυτό.

Στη φάση 3, προσδιορίζονται οι απειλές που υπάρχουν για το στοιχείο στην τοποθεσία όπου αποθηκεύεται, μεταφέρεται, ή επεξεργάζεται.

Στη φάση 4, οι κίνδυνοι για τα περιουσιακά στοιχεία πληροφοριών εντοπίζονται και αναλύονται και αναπτύσσονται προσεγγίσεις μετριασμού των κινδύνων αυτών.

Η σχέση μεταξύ των φάσεων και των πραγματικών βημάτων της μεθοδολογίας απεικονίζονται στον οδικό χάρτη της OCTAVE Allegro και παρουσιάζονται στο παραπάνω σχήμα.

Τα αποτελέσματα που εξάγονται από κάθε βήμα της διαδικασίας λαμβάνονται από μια σειρά φύλλων εργασίας, τα οποίες στη συνέχεια χρησιμοποιούνται ως στοιχεία εισόδου στο επόμενο βήμα της διαδικασίας. Τα επιμέρους βήματα της μεθοδολογίας περιγράφονται με περισσότερη λεπτομέρεια παρακάτω.

Βήμα 1 - Καθιέρωση κριτηρίων μέτρησης του κινδύνου

Το πρώτο βήμα στη διαδικασία OCTAVE Allegro καθορίζει τους οργανωτικούς οδηγούς που θα χρησιμοποιηθούν για την αξιολόγηση των επιπτώσεων του κινδύνου για την

αποστολή και τους επιχειρηματικούς στόχους του οργανισμού. Αυτοί οι οδηγοί αντικατοπτρίζονται σε ένα σύνολο κριτηρίων μέτρησης του κινδύνου που δημιουργούνται ως αρχικό στάδιο του βήματος 1. Κριτήρια μέτρησης του κινδύνου είναι ένα σύνολο ποιοτικών μέτρων κατά των οποίων τα αποτελέσματα ενός υπαρκτού κινδύνου μπορούν να αξιολογηθούν και να αποτελέσουν τη βάση μιας αξιολόγησης του κινδύνου του ενεργητικού των πληροφοριών. Χρησιμοποιώντας συνεπή κριτήρια μέτρησης των κινδύνων που αντικατοπτρίζουν με ακρίβεια μια οργανωτική άποψη, διασφαλίζει ότι οι αποφάσεις σχετικά με το πώς πρέπει να μετριαστεί ο κίνδυνος, θα είναι συνεπής όσον αφορά στα περιουσιακά στοιχεία, που σχετίζονται με πολλαπλές πληροφορίες, καθώς και στις λειτουργικά ή άλλες υπηρεσιακές μονάδες.

Εκτός από την αξιολόγηση της έκτασης του αντίκτυπου του κινδύνου σε μια συγκεκριμένη περιοχή, ένας οργανισμός πρέπει να αναγνωρίσει ποιες περιοχές των επιπτώσεων είναι πιο σημαντικές για την αποστολή του και για τους επιχειρηματικούς του στόχους. Για παράδειγμα, σε ορισμένους οργανισμούς, το αντίκτυπο στη σχέση του με την πελατειακή του βάση μπορεί να είναι πιο σημαντική από ένα αντίκτυπο στη συμμόρφωση με τους κανονισμούς. Αυτή η ιεράρχηση των επιπτώσεων πραγματοποιείται επίσης σε αυτό το αρχικό στάδιο.

Η μέθοδος OCTAVE Allegro παρέχει ένα τυποποιημένο σύνολο από πρότυπα φύλλα εργασίας για να δημιουργηθούν αυτά τα κριτήρια σε διάφορους τομείς των επιπτώσεων και στη συνέχεια να τους δοθεί προτεραιότητα.

Διαδικασία 1

Ορίζεται ένα ποιοτικό σύνολο μέτρων (κριτήρια μέτρησης κινδύνου) έναντι του οποίου θα είμαστε σε θέση να αξιολογήσουμε τα αποτελέσματά ενός κινδύνου για την αποστολή και τους επιχειρηματικούς στόχους ενός οργανισμού. Τα κριτήρια τεκμηριώνονται με τα Κριτήρια φύλλα εργασίας μέτρηση του κινδύνου (***Risk Measurement Criteria Worksheets*).** Εξετάζουν, τουλάχιστον, τους παρακάτω τομείς:

- Φήμη / εμπιστοσύνη των πελατών (Φύλλο Εργασίας 1, Παράρτημα)
- Χρηματοοικονομικά (Φύλλο Εργασίας 2, Παράρτημα)
- Παραγωγικότητα (Φύλλο Εργασίας 3, Παράρτημα)
- Ασφάλεια και υγεία (Φύλλο εργασίας 4, Παράρτημα)
- Πρόστιμα / νομικές κυρώσεις (Φύλλο εργασίας 5, Παράρτημα)
- Περιοχή κρούσης που ορίζεται από το χρήστη (Φύλλο εργασίας 6, Παράρτημα)

Συμπληρώνουμε και άλλα τυχόν κενά φύλλα με δικά μας κριτήρια, που θεωρούμε σημαντικά για τον οργανισμό.. Μπορούμε επίσης να αλλάξουμε τις περιγραφές που παρέχονται ή να προσθέσουμε άλλες.

Διαδικασία 2

Δώστε προτεραιότητα τις περιοχές των επιπτώσεων από τις πιο σημαντικές προς τις λιγότερο σημαντικές χρησιμοποιώντας το Impact Ranking Φύλλο (Φύλλο Εργασίας 7,

Παράρτημα). Η πιο σημαντική κατηγορία θα πρέπει να λαμβάνει την υψηλότερη βαθμολογία ενώ η λιγότερο σημαντική την χαμηλότερη.

Βήμα 2 - Ανάπτυξη Προφίλ Περιουσιακού Στοιχείου Πληροφορίας

Η μεθοδολογία OCTAVE Allegro επικεντρώνεται σε περιουσιακά στοιχεία πληροφορίας του οργανισμού και το Βήμα 2 αρχίζει η διαδικασία δημιουργίας ενός προφίλ για αυτά τα περιουσιακά στοιχεία. Ένα προφίλ είναι μια αναπαράσταση ενός τέτοιου στοιχείου του ενεργητικού, περιγράφοντας τα μοναδικά χαρακτηριστικά του, τις ιδιότητες, τα χαρακτηριστικά και αξία του. Η διαδικασία δημιουργίας προφίλ εξασφαλίζει ότι ένα περιουσιακό στοιχείο περιγράφεται με σαφήνεια, ότι υπάρχει ένας σαφής ορισμός των ορίων του περιουσιακού στοιχείου, και ότι οι απαιτήσεις ασφαλείας για το στοιχείο αυτό ορίζονται επαρκώς. Το προφίλ για κάθε περιουσιακό στοιχείο περιγράφεται σε ένα μόνο φύλλο εργασίας που αποτελεί τη βάση για τον προσδιορισμό των κινδύνων και απειλών στα επόμενα στάδια.

Διαδικασία 1

Η πρώτη δραστηριότητα σε αυτό το στάδιο της αξιολόγησης κινδύνου περιλαμβάνει τον προσδιορισμό μιας συλλογής στοιχείων πληροφορίας στην οποία θα μπορούσε να πραγματοποιηθεί μια εκτίμηση. Η αξιολόγηση παρέχει βοήθεια όταν επικεντρώνεται στα περιουσιακά στοιχεία που είναι πιο σημαντικά για τον οργανισμό. Ανάλογα με το επίπεδο στο οποίο θα εκτελεστεί αυτή η εκτίμηση των κινδύνων, ο "οργανισμός" θα μπορούσε να χωριστεί σε πολλά υποτμήματα. Για γίνει αυτό, πρέπει να απαντηθούν τα ακόλουθα ερωτήματα:

- Ποια στοιχεία πληροφορίας έχουν τη μεγαλύτερη αξία για τον οργανισμό ;
- Ποια στοιχεία πληροφορίας χρησιμοποιούνται καθημερινώς σε διαδικασίες και λειτουργίες του οργανισμού ;
- Ποια στοιχεία πληροφορίας, αν χαθούν, θα διαταράξουν σημαντικά τον οργανισμό και την ικανότητα να επιτύχει τους στόχους ;
- Ποια άλλα στοιχεία πληροφορίας είναι στενά συνδεδεμένα με αυτά τα στοιχεία πληροφορίας ;

Οπότε φτιάχνουμε μια λίστα με τέτοια στοιχεία.

Διαδικασία 2

«Εστιάζοντας σε λίγα και κρίσιμα» είναι μια βασική αρχή της διαχείρισης του κινδύνου. Έτσι, θα πρέπει να εκτελέσετε τη δομημένη αξιολόγηση κινδύνου, μόνο για αυτά τα στοιχεία πληροφορίας που είναι ζωτικής σημασίας για την επίτευξη των στόχων, καθώς και για εκείνα που είναι σημαντικά λόγω παραγόντων όπως η ρυθμιστική συμμόρφωση.

Από τη λίστα στη διαδικασία 1, πρέπει να απαντηθούν τα ακόλουθα ερωτήματα:

- Ποια στοιχεία πληροφορίας στη λίστα σας θα έχουν αρνητικές επιπτώσεις στον οργανισμό (όπως αυτές ορίζονται από τα κριτήρια αξιολόγησης του κινδύνου σας), αν ένα ή περισσότερα από τα ακόλουθα συνέβη;
- Το στοιχείο ή τα στοιχεία πληροφορίας αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
- Το στοιχείο ή τα στοιχεία πληροφορίας έχουν τροποποιηθεί χωρίς άδεια.
- Το στοιχείο ή τα στοιχεία πληροφορίας χάθηκαν ή καταστράφηκαν.
- Η πρόσβαση στο στοιχείο ή στα στοιχεία πληροφορίας διακόπηκε.

Τα στοιχεία πληροφορίας που πληρούν ένα ή περισσότερα από τα κριτήρια αυτά θα πρέπει να θεωρούνται κρίσιμης σημασίας για τον οργανισμό και θα πρέπει να διενεργηθεί σε αυτά μια δομημένη αξιολόγηση κινδύνου. Ξεκινώντας με την επόμενη δραστηριότητα, θα αρχίσει η διαδικασία της εκτέλεσης μια αξιολόγησης του κινδύνου για ένα από τα κρίσιμα στοιχεία πληροφορίας. Απλά επαναλάβετε όλα τα βήματα για κάθε τέτοιο στοιχείο στο οποίο θέλετε να εκτελέσετε μια αξιολόγηση του κινδύνου.

Διαδικασία 3

Στις ακόλουθες δραστηριότητες (3-8) θα συγκεντρωθούν πληροφορίες σχετικά με τα στοιχεία πληροφορίας που είναι απαραίτητα για να ξεκινήσει η δομημένη διαδικασία εκτίμησης κινδύνου. Θα χρησιμοποιηθεί το προφίλ κρίσιμου στοιχείου πληροφορίας (Φύλλο εργασίας 8, Παράρτημα Β) για να καταγραφούν αυτές οι πληροφορίες. Για να ξεκινήσουμε, καταγράφουμε το όνομα των κρίσιμων στοιχείων πληροφορίας στη στήλη (1) του προφίλ κρίσιμου στοιχείου πληροφορίας.

Διαδικασία 4

Τεκμηριώνεται η λογική για την επιλογή του κρίσιμες στοιχείου πληροφορίας στη στήλη (2) του προφίλ κρίσιμου στοιχείου πληροφορίας. Καθώς γίνεται αυτό, πρέπει να εξεταστούν τα ακόλουθα ερωτήματα:

- Γιατί είναι αυτό το στοιχείο ζωτικής σημασίας για τον οργανισμό;
- Αυτό το στοιχείο υπόκειται σε κανονιστικές απαιτήσεις;

Διαδικασία 5

Καταγράφεται μια περιγραφή για το κρίσιμο στοιχείο πληροφορίας στη στήλη (3) του προφίλ κρίσιμου στοιχείου πληροφορίας. Βεβαιώνουμε πως έχουμε ορίσει το σκοπό του κρίσιμου στοιχείου πληροφορίας και χρησιμοποιούμε ένα συμφωνημένο, κοινό ορισμό. Εξετάζουμε τις ακόλουθες ερωτήσεις όταν περιγράφουμε το στοιχείο πληροφορίας:

- Ποιο είναι το κοινό όνομα για αυτό το στοιχείο ;(πώς οι άνθρωποι εντός του οργανισμού αναφέρονται σε αυτό);
- Είναι αυτό το στοιχείο σε ηλεκτρονική μορφή ή σε φυσική (δηλαδή, βρέθηκε σε χαρτί), ή και στις δύο;

Διαδικασία 6

Προσδιορίζουμε τους ιδιοκτήτες των κρίσιμων στοιχείων πληροφορίας και το Καταγράφουμε στη στήλη (4) του προφίλ κρίσιμου στοιχείου πληροφορίας. Εξετάζουμε τις ακόλουθες ερωτήσεις για την τεκμηρίωση του ιδιοκτήτη των κρίσιμων στοιχείων πληροφορίας:

- Ποιος έχει την πρωταρχική ευθύνη για αυτές τις πληροφορίες περιουσιακό στοιχείο;
- Ποιος κατέχει τις επιχειρηματικές διαδικασίες όπου χρησιμοποιούνται αυτές για το κρίσιμο στοιχείο πληροφορίας;
- Ποιος είναι υπεύθυνος για τον καθορισμό της αξίας (χρηματικό ή άλλο) των στοιχείων πληροφορίας;
- Ποιος θα επηρεαστεί περισσότερο, αν το στοιχείο πληροφορίας τεθεί σε κίνδυνο;
- Υπάρχουν διαφορετικοί ιδιοκτήτες για τα διάφορα στοιχεία των δεδομένων που συνθέτουν το περιουσιακό στοιχείο πληροφορίας;

Διαδικασία 7

Καταγράψτε τις απαιτήσεις ασφαλείας για την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα στη στήλη (5) του προφίλ κρίσιμου στοιχείου πληροφορίας. Αρχίζουμε με τον έλεγχο των απαιτήσεων που ισχύουν για το στοιχείο πληροφορίας, και συνεχίζουμε συμπληρώνοντας τις πληροφορίες που ολοκληρώνουν κάθε απαίτηση ασφάλειας. Στα δεξιά αυτών των καταστάσεων μπορεί να προστεθούν απαιτήσεις ή γίνουν οι απαιτήσεις πιο συγκεκριμένες. Είναι σημαντικό να θυμόμαστε κατά τη διάρκεια αυτού του σταδίου, πως, αν υπάρχουν περισσότεροι από ένας ιδιοκτήτες, οι απαιτήσεις ασφαλείας που αναπτύσσονται για το στοιχείο πρέπει να αντανακλούν τις απαιτήσεις όλων των ιδιοκτητών. Οι απαιτήσεις ασφάλειας για τα στοιχεία πληροφορίας προέρχονται συνήθως από τη νομοθεσία και από ρυθμίσεις. Θα πρέπει να βεβαιωθούμε ότι οι απαιτήσεις ασφαλείας που έχουν οριστεί υποστηρίζουν οποιεσδήποτε ισχύουσες διατάξεις.

Διαδικασία 8

Προσδιορίζουμε την πιο σημαντική προϋπόθεση για την ασφάλεια των πληροφοριών με σήμανση ένα «Χ» στο πλαίσιο δίπλα στην κατηγορία των απαιτήσεων ασφαλείας στη στήλη (6) του προφίλ κρίσιμου στοιχείου πληροφορίας. Θα χρησιμοποιήσουμε αυτές τις πληροφορίες για τον προσδιορισμό των δυνητικών επιπτώσεων ενός κινδύνου, γι' αυτό είναι σημαντικό να επιλέξουμε αυτή την απαίτηση ασφάλειας προσεκτικά.

Βήμα 3 - Εντοπισμός Θέσης Περιουσιακού Στοιχείου Πληροφορίας

Σε αυτό το βήμα, περιγράφονται τα μέρη όπου τα περιουσιακά στοιχεία πληροφορίας αποθηκεύονται, μεταφέρονται και επεξεργάζονται. Τα στοιχεία αυτά δεν βρίσκονται μόνο σε θέσεις εντός των ορίων ενός οργανισμού, αλλά και σε τοποθεσίες που δεν είναι στον άμεσο έλεγχο του οργανισμού. Τυχόν κίνδυνοι στο μέρος στο οποίο εδράζουν τα στοιχεία απειλούν την ίδια τους την ύπαρξη.

Για παράδειγμα, πολλοί οργανισμοί αναθέτουν κάποιες, αν όχι όλες τις υποδομές πληροφορικής τους, σε παρόχους. Αυτοί οι πάροχοι υπηρεσιών διαχειρίζονται το μέρος, στο οποίο περιέχονται πλέον τα στοιχεία πληροφορίας του οργανισμού. Εάν ένας πάροχος υπηρεσιών δεν είναι ενήμερος για τις απαιτήσεις ασφάλειας ενός περιουσιακού στοιχείου πληροφοριών που αποθηκεύεται, μεταφέρεται, ή υποβάλλεται σε επεξεργασία σε μέρος που διαχειρίζεται, τότε οι έλεγχοι που αναγκαίοι για την προστασία των περιουσιακών στοιχείων πληροφορίες ενδέχεται να μην είναι επαρκής, εκθέτοντας έτσι τα περιουσιακά στοιχεία σε κίνδυνο.

Αυτό το πρόβλημα μπορεί να γίνει ακόμη πιο έντονο εάν ο πάροχος υπηρεσιών, με τη σειρά του, κάνει συμβάσεις με άλλους παρόχους, για υπηρεσίες όπως η αποθήκευση δεδομένων, που μπορεί να είναι άγνωστοι στον ιδιοκτήτη των περιουσιακών στοιχείων. Έτσι, για να αποκτήσει ένα επαρκές προφίλ κινδύνου ενός περιουσιακού στοιχείου πληροφοριών, ένας οργανισμός πρέπει να αναφέρει όλα τα σημεία όπου τα περιουσιακά στοιχεία πληροφορίας αποθηκεύονται, μεταφέρονται, ή υποβάλλονται σε επεξεργασία, έστω και αν δεν βρίσκονται σε άμεσο έλεγχο του οργανισμού.

Στο Στάδιο 3 της μεθόδου OCTAVE Allegro, όλα τα μέρη στα οποία αποθηκεύεται ένα περιουσιακό στοιχείο, μεταφέρεται, και επεξεργάζεται, είτε εσωτερικά είτε εξωτερικά, εντοπίζονται. Σε αυτό το στάδιο η ομάδα ανάλυσης χαρτογραφεί ένα περιουσιακό στοιχείο πληροφοριών εντοπίζοντας το μέρος στο οποίο 'ζει', προσδιορίζοντας έτσι τα όρια και μοναδικές συνθήκες που πρέπει να εξεταστούν για τον κίνδυνο.

Διαδικασία 1

Χρησιμοποιώντας τις πληροφορίες από τα worksheets «χαρτογράφησης περιβάλλοντος του στοιχείου πληροφορίας» προσδιορίζουμε πού αποθηκεύονται, μεταφέρονται, ή μεταποιημένα τα στοιχεία πληροφορίας ως εξής:

- Χρησιμοποιούμε το Φύλλο 9α για την αναγνώριση του τεχνικού περιβάλλοντος, κάτω από τον άμεσο έλεγχο του οργανισμού (εσωτερικό) ή εκτός του οργανισμού (εξωτερικό).
- Χρησιμοποιούμε το Φύλλο 9β να εντοπίσει φυσικές τοποθεσίες, όπου οι πληροφορίες μπορεί να υπάρχουν είτε εντός είτε εκτός του οργανισμού.
- Χρησιμοποιούμε το Φύλλο εργασίας Χρήστη 9γ για τον εντοπισμό των ανθρώπων που βρίσκονται εσωτερικά ή εξωτερικά στον οργανισμό και μπορεί να έχουν μια λεπτομερή γνώση των στοιχείων πληροφορίας.

Βήμα 4 - Προσδιορισμός τομέων ενδιαφέροντος

Στο Βήμα 4 αρχίζει η διαδικασία εντοπισμού των κινδύνων μέσω του προβληματισμού για πιθανές συνθήκες ή καταστάσεις που μπορούν να απειλήσουν τα περιουσιακά στοιχεία πληροφορίας ενός οργανισμού. Αυτά τα σενάρια του πραγματικού κόσμου είναι οι τομείς ενδιαφέροντος και μπορούν να αντιπροσωπεύουν τις απειλές και τα αντίστοιχα ανεπιθύμητα αποτελέσματα τους. Τομέας ενδιαφέροντος μπορεί να χαρακτηριστεί μια απειλή, που είναι μοναδική σε έναν οργανισμό και τις συνθήκες λειτουργίας του. Ο σκοπός αυτού του βήματος δεν είναι να φτιάξει μια πλήρη λίστα όλων των πιθανών εκδοχών

απειλής για ένα περιουσιακό στοιχείο πληροφορίας, αλλά η ιδέα είναι να χαρτογραφήσει ποιες από αυτές τις καταστάσεις ή συνθήκες έρχονται αμέσως στο μυαλό της ομάδας ανάλυσης.

Διαδικασία 1

Για να εκτελεστεί αυτή η δραστηριότητα, θα χρησιμοποιήσουμε τις πληροφορίες από τα worksheets 9a, 9b, 9c για αναφορά και από το worksheet 10για να καταγράψουμε τις περιοχές ανησυχίας.

Για να εντοπιστούν οι τομείς που προκαλούν ανησυχία, ακολουθούμε τα παρακάτω βήματα:

1. Χρησιμοποιώντας τις πληροφορίες από τα worksheets 9a,9b,9c, επανεξετάζουμε κάθε πιθανό τομέα ανησυχίας σε σχέση με το πού βρίσκεται η πληροφορία.
2. Καταγράφουμε κάθε περιοχή ανησυχίας που προσδιορίζεται στο worksheet 10. Σε αυτό το φύλλο εργασίας, καταγράφουμε το όνομα του στοιχείο στοιχείου πληροφορίας και να ορίζουμε την περιοχή ανησυχίας με όσες περισσότερες λεπτομέρειες είναι δυνατόν.
3. Επεκτείνουμε περιοχές ανησυχίας για να δημιουργήσετε σενάρια απειλών. Ένα σενάριο απειλής είναι μια πιο λεπτομερής έκφραση των ιδιοτήτων του κινδύνου. Για κάθε περιοχή της ανησυχίας που έχουμε εγγράψει στο Φύλλο κινδύνου 10, συμπληρώνουμε τις στήλες (1) έως (4), καταγράφοντας τον δράστη, τα μέσα και το κίνητρο που έχει καθώς και το αποτέλεσμα που παράγεται. Εάν δεν μπορούμε να ολοκληρώσουμε κάποια από αυτά τα στοιχεία, τα αφήνουμε κενά.
4. Στη στήλη (5) καταγράφουμε πώς αυτή η απειλή θα μπορούσε να επηρεάσει τις απαιτήσεις ασφαλείας που έχουν οριστεί για το στοιχείο πληροφορίας. Συνεχίζουμε να εφαρμόζουμε αυτή την δραστηριότητα μέχρι όλοι οι τομείς ανησυχίας να έχουν εξαλειφθεί.

Βήμα 5 - Προσδιορισμός Σεναρίων Απειλής

Κατά το πρώτο μισό του Σταδίου 5, οι περιοχές της ανησυχίας που λαμβάνονται από το προηγούμενο βήμα επεκτείνονται σε σενάρια απειλής με την περαιτέρω λεπτομέρεια των ιδιοτήτων μιας απειλής. Αλλά η συλλογή των απειλών που αναπτύχθηκε από τους τομείς ενδιαφέροντος δεν αποτελούν απαραίτητα μια ισχυρή εκτίμηση πιθανών απειλών για τα περιουσιακά στοιχεία πληροφορίας ενός οργανισμού. Έτσι, στο δεύτερο μισό του Σταδίου 5, ένα ευρύ φάσμα επιπρόσθετων απειλών λαμβάνεται υπόψιν, εξετάζοντας σενάρια απειλών.

Μια σειρά από σενάρια απειλών μπορεί να αναπαρασταθεί οπτικά σε μια δομή δέντρου που συνήθως αναφέρονται ως ένα δέντρο-απειλή. Τα δέντρα-απειλή περιγράφονται στον παρακάτω πίνακα.

Δέντρο-απειλή	**Ορισμός**
Ανθρώπινοι παράγοντες χρησιμοποιούν τεχνικά μέσα	Οι απειλές σε αυτή την κατηγορία αποτελούν απειλές για το περιουσιακό στοιχείο πληροφορίας μέσω του τεχνικής υποδομής του οργανισμού, ή με άμεση πρόσβαση σε ένα μέρος (τεχνική φύσης) που φιλοξενεί ένα περιουσιακό στοιχείο πληροφορίας. Απαιτείται άμεση δράση από την άτομο και μπορεί να συμβεί σκόπιμα ή τυχαία στη φύση.
Ανθρώπινοι παράγοντες χρησιμοποιούν φυσικά μέσα	Οι απειλές σε αυτή την κατηγορία αποτελούν απειλές για το περιουσιακό στοιχείο πληροφορίας που προκύπτουν από τη φυσική πρόσβαση στο περιουσιακό στοιχείο ή σε ένα μέρος που φιλοξενεί πληροφορίες για το περιουσιακό στοιχείο. Απαιτείται άμεση δράση από ένα άτομο και μπορεί να συμβεί σκόπιμα ή τυχαία στη φύση.
Τεχνικά προβλήματα	Οι απειλές σε αυτή την κατηγορία είναι τα προβλήματα με τα πληροφοριακά συστήματα και την τεχνολογία ενός οργανισμού. Παραδείγματα περιλαμβάνουν ελαττωματικά υλικά προβλήματα λογισμικού, κακόβουλο κώδικα (π.χ. ιούς), και άλλα προβλήματα που σχετίζονται με το σύστημα.
Άλλα προβλήματα	Οι απειλές σε αυτή την κατηγορία είναι τα προβλήματα ή καταστάσεις που είναι έξω από το τον έλεγχο ενός φορέα. Αυτή η κατηγορία περιλαμβάνει τις απειλές των φυσικών καταστροφών (π.χ. πλημμύρες, σεισμοί) και τους κινδύνους αλληλεξάρτησης (π.χ. παροχή ρεύματος).

Πίνακας 2:Πίνακας δέντρο-απειλή

Τα σενάρια απειλής που προέρχεται από τις περιοχές της ανησυχίας αντιστοιχούν σε ένα ή σε περισσότερα παρακλάδια από αυτά τα δέντρα-απειλή. Για να εξασφαλιστεί μια πιο ισχυρή εκτίμηση των απειλών, κάθε κλαδί του δέντρου απειλής λαμβάνεται υπόψιν επίσης

για κάθε περιουσιακό στοιχείο πληροφορίας. Το να εργαστεί κανείς μέσα από κάθε κλαδί των δέντρων-απειλή για να προσδιορίσει τα σενάρια απειλής μπορεί να είναι μια επίπονη διαδικασία. Έτσι, έχουμε μια σειρά από ερωτηματολόγια με σενάρια απειλής που έχουν αναπτυχθεί και παρέχονται για να βοηθήσουν.

Αυτό το βήμα αποτελεί επίσης μια ευκαιρία για την εξέταση της πιθανότητας στην περιγραφή των σεναρίων απειλής. Πιθανότητα βοηθά έναν οργανισμό να καθορίσει ποια από τα σενάρια είναι περισσότερο πιθανά λόγω του μοναδικού περιβάλλοντος λειτουργίας του. Αυτό είναι χρήσιμο σε επόμενα βήματα, όταν αρχίζει ένας οργανισμός τη διαδικασία ιεράρχησης δραστηριοτήτων που σχετίζονται με τον μετριασμό του κινδύνου. Ωστόσο, επειδή είναι συχνά δύσκολο να αναπαρασταθεί ποσοτικά η πιθανότητα, ιδίως σε σχέση με τα τρωτά σημεία και τα γεγονότα της ασφάλειας, η πιθανότητα εκφράζεται στη μεθοδολογία OCTAVE Allegro ποιοτικά, ως υψηλή, μέση ή χαμηλή.

Βήμα 6 - Αναγνώριση κινδύνων

Στο Βήμα εντοπίστηκαν οι απειλές, και στο Βήμα 6 οι συνέπειες σε έναν οργανισμό, αν η απειλή πραγματοποιηθεί, οπότε ολοκληρώνεται η εικόνα του κινδύνου. Μια απειλή μπορεί να έχει πολλαπλές πιθανές επιπτώσεις σε έναν οργανισμό. Για παράδειγμα, η διακοπή του συστήματος e-commerce ενός οργανισμού μπορεί να επηρεάσει τη φήμη του οργανισμού με τους πελάτες της, καθώς και την οικονομική της θέση. Οι δραστηριότητες στο βήμα αυτό εξασφαλίζουν ότι οι διάφορες συνέπειες των κινδύνων έχουν ληφθεί υπόψιν.

Διαδικασία 1

Σε αυτή τη διαδικασία, θα καθοριστεί ο τρόπος με τον οποίον τα σενάρια απειλής που έχουμε εγγράψει στο worksheet 10 θα μπορούσαν να επηρεάσουν τον οργανισμό.

1. Για κάθε σενάριο απειλής που έχουμε εγγράψει, προσδιορίζουμε πως θα επηρεαστεί ο οργανισμός αν το σενάριο απειλή πραγματοποιηθεί. Αυτή είναι η συνέπεια της απειλής και ολοκληρώνει την εξίσωση κινδύνου.

2. Καταγράφουμε τουλάχιστον μία συνέπεια και προσθέτουμε όποιες είναι απαραίτητες. Είμαστε όσο πιο συγκεκριμένοι μπορούμε. Προσπαθούμε να εξετάσουμε τον αντίκτυπο στις θιγόμενες περιοχές των κριτηρίων αξιολόγησης των κινδύνων, όσο επεξεργαζόμαστε τις συνέπειες.

Βήμα 7 - Ανάλυση κίνδυνου

Στο Βήμα 7 της παρούσας μεθόδου, υπολογίζεται μια απλή ποσοτική μέτρηση του βαθμού στον οποίο η οργάνωση επηρεάζεται από μια απειλή. Αυτή η σχετική βαθμολογία του κινδύνου προέρχεται από το βαθμό στον οποίο θεωρούμε σημαντική μια συνέπεια επίπτωσης κινδύνων της οργάνωσης σε σχέση με διάφορους τομείς των επιπτώσεων, και, ενδεχομένως, και από τη πιθανότητα να συμβεί. Με άλλα λόγια, αν η φήμη είναι το πιο σημαντικό σε έναν οργανισμό, οι κίνδυνοι που έχουν αντίκτυπο στη φήμη του οργανισμού θα παράγουν υψηλότερες βαθμολογίες κινδύνων σε σχέση με αυτούς που συνδέονται με τις αντίστοιχες επιπτώσεις και πιθανότητες σε άλλη περιοχή. Με την ιεράρχηση αυτών των

προτεραιοτήτων για τα κριτήρια των επιπτώσεων, η οργάνωση αυτή εξασφαλίζει ότι οι κίνδυνοι θα έχουν προτεραιότητα στο πλαίσιο που έθεσαν οι οργανωτικοί οδηγοί της.

Διαδικασία 1

Αρχίζουμε παρατηρώντας τα κριτήρια μέτρησης ρίσκου που δημιουργήσαμε στο βήμα 1. Επικεντρωνόμαστε σχετικά με το πώς θα ορίζεται υψηλή, μεσαία και χαμηλή επιπτώσεις για τον οργανισμό. Ξεκινώντας με το πρώτο φύλλο του κινδύνου, εξετάζουμε τις συνέπειες που καταγράφονται. Χρησιμοποιώντας τα κριτήρια μέτρησης ρίσκου ως οδηγό, αξιολογούμε το αποτέλεσμα και καταγράφουμε μία τιμή "υψηλό", "μέσο" ή "Χαμηλό" στην "Αξία" περιοχή της στήλης (8). Μπορείτε να καταγράψετε μια τιμή σε κάθε ένα από τους τομείς επιπτώσεων.

Διαδικασία 2

Στη διαδικασία αυτή, μία σχετική βαθμολογία ρίσκου θα υπολογιστεί, η οποία μπορεί να χρησιμοποιηθεί για να αναλύσει τους κινδύνους και να βοηθήσει τον οργανισμό να καθορίσει μια κατάλληλη στρατηγική διαχείρισης των κινδύνων.

1. Υπολογίζουμε το σκορ για κάθε θιγόμενη περιοχή πολλαπλασιάζοντας το βαθμό κάθε θιγόμενης περιοχής (worksheet 7) με την αξία της επίπτωσης ("υψηλή", "μέση" ή "χαμηλή"). Καταγράφουμε το αποτέλεσμα του στη στήλη "σκορ". Οι τιμές των επιπτώσεων αποδίδονται ποσοτικά σε αξίες ως εξής:
   High=3, Medium=2, Low=1. Διατηρούμε αυτές τις αξίες συνεπείς καθ' όλη τη διαδικασία.
2. Αθροίζουμε τη στήλη σκορ. Αυτό το σύνολο είναι η σχετική βαθμολογία του κινδύνου.

Βήμα 8 - Επιλογή προσέγγισης μετριασμού

Στο Στάδιο 8, το τελικό βήμα της διαδικασίας OCTAVE Allegro, οι οργανισμοί καθορίζουν ποιοι από τους κινδύνους που έχουν εντοπιστεί απαιτούν μετριασμό και αναπτύσσουν μια στρατηγική για την αντιμετώπιση των κινδύνων αυτών. Αυτό επιτυγχάνεται με την πρώτη ιεράρχηση των κινδύνων με βάση τη σχετική βαθμολόγηση του κινδύνου τους. Μόλις οι κινδύνους ιεραρχηθούν, αναπτύσσονται στρατηγικές μετριασμού που λαμβάνουν υπόψιν τους την αξία του περιουσιακού στοιχείου και τις απαιτήσεις ασφάλειας του, τα μέρη στα οποία 'ζει', και το μοναδικό περιβάλλον λειτουργίας της οργάνωσης.

Διαδικασία 1

Η πρώτη δραστηριότητα στο Βήμα 8 είναι απλά να ταξινομήσουμε καθένα από τους κινδύνους που έχουν εντοπιστεί με βάση το σχετικό σκορ τους. Κατηγοριοποίηση των κινδύνων με ένα μεθοδικό τρόπο θα βοηθήσει στις αποφάσεις σχετικά με το καθεστώς μετριασμού τους. Υπάρχουν πολλοί τρόποι για έναν οργανισμό να ταξινομήσει τους κινδύνους του. Μια απλή μέθοδος είναι να ξεκινήσει από τη διαλογή τους κινδύνους κατά σειρά από την υψηλότερη στην χαμηλότερη. Μία άλλη είναι ο διαχωρισμός των κινδύνων

σε τέσσερις ομάδες με ίσο αριθμό των κινδύνων. Οι κίνδυνοι με την υψηλότερη βαθμολογία θα πρέπει να είναι στο pool 1, οι κίνδυνοι με ελαφρώς χαμηλότερο σκορ στο pool 2 και ομοίως ως το pool 4. Εάν ο οργανισμός χρησιμοποιεί πιθανότητα, ίσως εξεταστεί το ενδεχόμενο ανάπτυξης μιας μήτρας για την κατηγοριοποίηση των κινδύνων που έχουν εντοπιστεί. Ο Σχετικός πίνακας κινδύνου παρακάτω δείχνει ένα παράδειγμα του πώς να το κάνουμε αυτό.

ΠΙΝΑΚΑΣ ΣΧΕΤΙΚΟΥ ΡΙΣΚΟΥ			
ΠΙΘΑΝΟΤΗΤΑ	**ΣΚΟΡ ΡΙΣΚΟΥ**		
	30 ΤΟ 45	**16 ΤΟ 29**	**0 ΤΟ 15**
ΥΨΗΛΗ	POOL 1	POOL 2	POOL 2
ΜΕΤΡΙΑ	POOL 2	POOL 2	POOL 3
ΧΑΜΗΛΗ	POOL 3	POOL 3	POOL 4

Πίνακας 3:Πίνακας Σχετικού ρίσκου της octave allegro

Διαδικασία 2

Αντιστοιχίζουμε μια προσέγγιση μετριασμού για κάθε ένα από τους κινδύνους. Σκεφτόμαστε να χρησιμοποιήσετε τον παρακάτω πίνακα ως οδηγός, αλλά μια απόφαση σχετικά με τον μετριασμό εξαρτάται σε μεγάλο βαθμό το μοναδικό λειτουργικές συνθήκες του κάθε οργανισμού, οπότε ο πίνακας αυτός δεν αποτελεί κανόνα, αλλά προσαρμόζεται αναλόγως όπου χρειάζεται.

Pool	**Προσέγγιση**
Pool 1	Μετριασμός
Pool 2	Μετριασμός ή Αναβολή
Pool 3	Αναβολή ή Αποδοχή
Pool 4	Αποδοχή

Πίνακας 4: Οδηγός προσέγγισης με βάση το σχετικό σκορ ρίσκου

ΚΕΦΑΛΑΙΟ 2 Συνοπτική παρουσίαση του ΕΛ.Γ.Α.

2.1 Σκοπός του οργανισμού

Ο Οργανισμός Ελληνικών Γεωργικών Ασφαλίσεων (ΕΛ.Γ.Α.) αποτελεί τον κεντρικό φορέα ασφαλιστικής κάλυψης των γεωργικών εκμεταλλεύσεων στην Ελλάδα και επιδίωξή του είναι η στήριξη του γεωργικού εισοδήματος των ασφαλισμένων του.

Σκοπός του ΕΛ.Γ.Α. είναι η ασφάλιση της γεωργικής παραγωγής και του κεφαλαίου των αγροτικών εκμεταλλεύσεων, η διενέργεια ερευνών σχετικών με τους φυσικούς κινδύνους στη γεωργία, καθώς και η οργάνωση και εφαρμογή προγραμμάτων ενεργητικής προστασίας των καλλιεργειών. Στην ασφάλιση υπάγονται χωρίς εξαίρεση όλα τα φυσικά και νομικά πρόσωπα που έχουν την κυριότητα ή την εκμετάλλευση αγροτικών επιχειρήσεων. Οι σημερινές δραστηριότητες του ΕΛ.Γ.Α. εστιάζονται στην υποχρεωτική ασφάλιση των ζημιών η οποία περιλαμβάνει:

- Ασφάλιση των ζημιών στη φυτική παραγωγή από τους κινδύνους : χαλάζι, παγετό, ανεμοθύελλα, πλημμύρα, καύσωνας, υπερβολικές ή άκαιρες βροχοπτώσεις, χιόνι, θάλασσα, ζημιές από άγρια ζώα.
- Ασφάλιση των ζημιών του ζωικού κεφαλαίου από το σύνολο σχεδόν των φυσικών κινδύνων και ασθενειών - παθήσεων.
- Ενεργητική προστασία του φυτικού κεφαλαίου και της φυτικής παραγωγής κατά παγετού και χαλαζιού.
- Από τον ιδρυτικό του νόμο, προβλέπεται η επέκταση των δραστηριοτήτων του και σε άλλους κινδύνους και σε άλλα αντικείμενα.

Επιπλέον, από το 2002 ασκούνται πλέον μόνιμα από τον ΕΛ.Γ.Α. οι αρμοδιότητες που ανήκαν στη Διεύθυνση Πολιτικής Σχεδίασης Εκτάκτου Ανάγκης (Π.Σ.Ε.Α.) του Υπουργείου Γεωργίας, οι οποίες αφορούν στην παρακολούθηση των ζημιών που προκαλούνται από θεομηνίες, δυσμενείς καιρικές συνθήκες, πυρκαγιές και άλλα έκτακτα γεγονότα στην παραγωγή (φυτική, ζωική) και στο κεφάλαιο (φυτικό, ζωικό, πάγιο και έγγειο) των αγροτικών εκμεταλλεύσεων, στη μελέτη και αξιολόγηση τους και στην εισήγηση για τα κυβερνητικά μέτρα που πρέπει να ληφθούν, με υποκαταστήματα σε όλη την Ελλάδα. (9)

2.2 Διοικητική διάρθρωση

Ο ΕΛΓΑ διαρθρώνεται διοικητικά από:

1. Τις Υπηρεσίες και Διευθύνσεις της Κεντρικής Διοίκησης, ως εξής:
    - Νομική Υπηρεσία
    - Υπηρεσία Επιθεώρησης
    - Τμήμα Κοινοβουλευτικού Ελέγχου
    - Διεύθυνση Ασφάλισης και Ενισχύσεων
    - Διεύθυνση Διοικητικού
    - Διεύθυνση Οικονομικού
    - Διεύθυνση Πληροφορικής
    - Διεύθυνση Μελετών και Εφαρμογών

2. Τα 13 Περιφερειακά Υποκαταστήματα του ΕΛΓΑ με έδρες τις μεγαλύτερες πόλεις της Περιφέρειας και το Κέντρο Μετεωρολογικών Εφαρμογών, με έδρα το Αεροδρόμιο Μακεδονία στη Θεσσαλονίκη. Η έδρα και η γεωγραφική δικαιοδοσία των Υποκαταστημάτων του ΕΛΓΑ είναι στις εξής πόλεις: Αλεξανδρούπολη, Καβάλα, Θεσσαλονίκη, Κοζάνη, Λάρισα, Ιωάννινα, Αγρίνιο, Αθήνα, Πάτρα, Τρίπολη, Ηράκλειο, Λαμία και Βέροια.

Επίσης, σε κάθε Δήμο και Κοινότητα σ' όλη τη χώρα, έχουν ορισθεί «Ανταποκριτές» του ΕΛ.Γ.Α. για την άμεση εξυπηρέτηση των ασφαλισμένων παραγωγών. Όλες οι λειτουργίες που αφορούν στις ασφαλιστικές διαδικασίες εκτελούνται στην περιφέρεια, εκτός από την εκκαθάριση των ζημιών και την πληρωμή των αποζημιώσεων που γίνεται σε κεντρικό επίπεδο. Επιπλέον ο ΕΛ.Γ.Α. για την διεκπεραίωση των λειτουργικών του αναγκών, συνεργάζεται με το Υπουργείο Οικονομίας & Οικονομικών, την Αγροτική Τράπεζα Ελλάδας (ΑΤΕ) και τα Ελληνικά Ταχυδρομεία (ΕΛ.ΤΑ.).

2.3 Οι δομές του ΕΛ.Γ.Α.

Οι δομές του ΕΛ.Γ.Α. (μονάδες, διευθύνσεις, τμήματα) που θα χρησιμοποιήσουν άμεσα το προς υλοποίηση σύστημα του παρόντος Έργου είναι οι διευθύνσεις και τα αντίστοιχα τμήματα που βρίσκονται στην Κεντρική Υπηρεσία του Οργανισμού με έδρα την Αθήνα:

- Διεύθυνση Ασφάλισης & Ενισχύσεων

- Τμήμα Ασφάλισης και Πολιτικής Ενισχύσεων

- Τμήμα Εκτιμήσεων και Αποζημιώσεων Φυτικού Τομέα

- Τμήμα Εκτιμήσεων και Αποζημιώσεων Ζωικού Τομέα

- Τμήμα Εκτιμήσεων και Ενισχύσεων

- Τμήμα Δήλωσης Καλλιέργειας Εκτροφής

- Διεύθυνση Μελετών και Εφαρμογών

- Τμήμα Στατιστικής και Γεωγραφικών Συστημάτων Πληροφοριών

- Τμήμα Ενεργητικής Προστασίας και Εφαρμογών

- Διεύθυνση Πληροφορικής

- Τμήμα Ανάλυσης και Προγραμματισμού

- Τμήμα Τεχνικής Υποστήριξης

- Υπηρεσία Επιθεώρησης

- Τμήμα Ελέγχου Διαδικασιών Ασφάλισης, Ενισχύσεων και Εφαρμογών

- Τμήμα Κοινοβουλευτικού Ελέγχου

Οι υπάλληλοι του ΕΛΓΑ που θα χρησιμοποιήσουν άμεσα το σύστημα ανήκουν κυρίως στις εξής ειδικότητες:

- Πληροφορικής
- Χειριστών Η/Υ
- Γεωπονίας

- Διοικητικοί

2.4 Ανάλυση τεχνολογικών υποδομών του ΕΛ.Γ.Α.

Στο κτίριο της Κεντρικής Υπηρεσίας επί της οδού Μεσογείων 45, στον 3ο όροφο στεγάζεται το Computer Room (CM) του ΕΛΓΑ τηρώντας τους απαραίτητους κανόνες φυσικής και περιβαλλοντικής ασφάλειας (Σύστημα Ελεγχόμενης Πρόσβασης, Παρακολούθησης, Πυρόσβεσης - Πυροπροστασίας, Αδιάλειπτης Παροχής Ενέργειας και Κλιματισμού).

Το CM φιλοξενεί το βασικό-κύριο πληροφορικό σύστημα του Οργανισμού, το Ολοκληρωμένο Πληροφοριακό Σύστημα Ασφάλισης και Ενισχύσεων ΕΛΓΑ (Ο.Π.Σ.Α.Ε.), το οποίο υποστηρίζει τις ασφαλιστικές διαδικασίες του Οργανισμού, καθώς και άλλα συστήματα ανεξάρτητα μεταξύ τους και ανεξάρτητα από το Ο.Π.Σ.Α.Ε. τα οποία περιέχουν δεδομένα ασφαλιστικών διαδικασιών του ΕΛΓΑ. Στο Ο.Π.Σ.Α.Ε. έχουν ενοποιηθεί έως ένα βαθμό δεδομένα διαφορετικών υποσυστημάτων του ΕΛΓΑ.

Συγκεκριμένα το Ο.Π.Σ.Α.Ε. υποστηρίζει τις παρακάτω βασικές ασφαλιστικές διαδικασίες:

- **Ασφάλιση Γεωργικής Παραγωγής:** Υποσύστημα Ασφάλισης Φυτικής Παραγωγής και Ζωικού Κεφαλαίου για την διαχείριση των ζημιών που καλύπτονται από τον ΕΛΓΑ (τμήμα του Ολοκληρωμένου Πληροφοριακού Συστήματος (ΟΠΣ) για την υποστήριξη των ασφαλιστικών, διοικητικών και οικονομικών διαδικασιών της Κεντρικής Διοίκησης και των περιφερειακών υποκαταστημάτων του ΕΛ.Γ.Α.).
- **ΚΟΕ:** Υποσύστημα για την διαχείριση του Έργου των ΚΟΕ (ΠΣΕΑ)
- **Δήλωση Καλλιέργειας-Εκτροφής:** Υποσύστημα Δήλωσης Καλλιέργειας-Εκτροφής για την διαχείριση των ασφαλιστικών εισφορών των ασφαλισμένων (9)

Το Ο.Π.Σ.Α.Ε. είναι μία desktop εφαρμογή (Java Swing), διαθέσιμη μόνο στους χρήστες του ΕΛΓΑ σε όλη την επικράτεια μέσω του εσωτερικού δικτύου του Οργανισμού και αλληλοεπιδρά με την βάση δεδομένων (ΒΔ). Η ΒΔ είναι σε Oracle Database Server 10g Standard Edition και έχει εγκασταθεί σε διάταξη clustering.

Στην εφαρμογή αυτή αποτυπώνεται η σχετική επιχειρησιακή λογική διαχείρισης ασφαλίσεων και αποζημιώσεων του Οργανισμού.

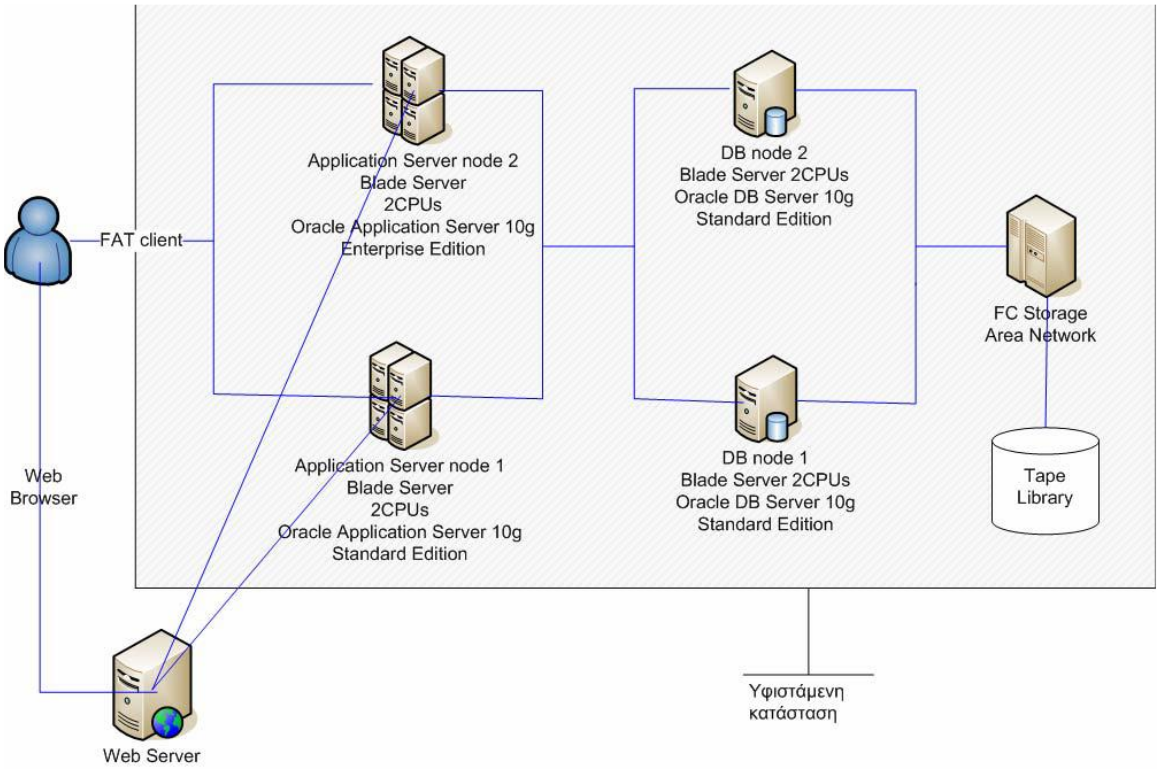
Για την υλοποίηση του περιβάλλοντος της εφαρμογής του ΕΛΓΑ έχει χρησιμοποιηθεί αποκλειστικά η γλώσσα προγραμματισμού Java 2 SDK Enterprise Edition και κλάσεις για τη δημιουργία των Enterprise Java Beans. Επιπλέον πακέτα - βιβλιοθήκες περιέχουν κλάσεις για τη δημιουργία και ανάγνωση XML εγγράφων και οδηγούς για την δημιουργία συνδέσεων με τη ΒΔ. Για την ανάπτυξη της έχει γίνει χρήση του Ανοικτού Λογισμικού (Open Source) Eclipse IDE (έκδοση 3.3.2 ή μεταγενέστερη). Για την ανάπτυξη της διεπαφής (user interface) της εφαρμογής έχει χρησιμοποιηθεί Java SWING σε συνδυασμό με μηχανισμό αυτοματοποιημένης δημιουργίας οθονών μέσω μεταδεδομένων (metadata driven layout engine). Για τη διασύνδεση με τη ΒΔ έχει χρησιμοποιηθεί Hibernate. Κάθε εφαρμογή του συστήματος ακολουθεί την αρχιτεκτονική MVC (Model View Controller) όπως αυτή υλοποιείται από το J2EE πρότυπο.

2.5 Δικτύωση

Την παρούσα στιγμή ο ΕΛΓΑ βρίσκεται σε διαδικασία αναβάθμισης της τεχνολογικής πλατφόρμας του τηλεπικοινωνιακού δικτύου με την διαδικασία της μετεγκατάστασης – μετάπτωσης στον εξοπλισμό και στο δίκτυο δεδομένων του ΥΠΑΑΤ τόσο για το κτίριο της Κεντρικής Διοίκησης καθώς και των 13 Υποκ/των του ΕΛΓΑ. Το επόμενο στάδιο αφορά στην αναβάθμιση της ταχύτητας των γραμμών του δικτύου ΕΛΓΑ σε ταχύτητα 6Mbps για την ΚΔ και σε 2Mbps για κάθε Υποκατάστημα.

2.6 Φυσική Αρχιτεκτονική Υλικοτεχνικής Υποδομής

Για το υποσύστημα ΕΛΓΑ παρουσιάζουμε μια ενδεικτική φυσική αρχιτεκτονική, συναρτήσει της υφιστάμενης κατάστασης, που θα προσαρμοστεί ανάλογα με τις ανάγκες που θα προκύψουν.



Εικόνα 4: Σχήμα απεικόνισης φυσικής αρχιτεκτονικής συστημάτων του ΕΛΓΑ

2.7 Χρήστες Έργου (Web Συστήματος ΕΛΓΑ)

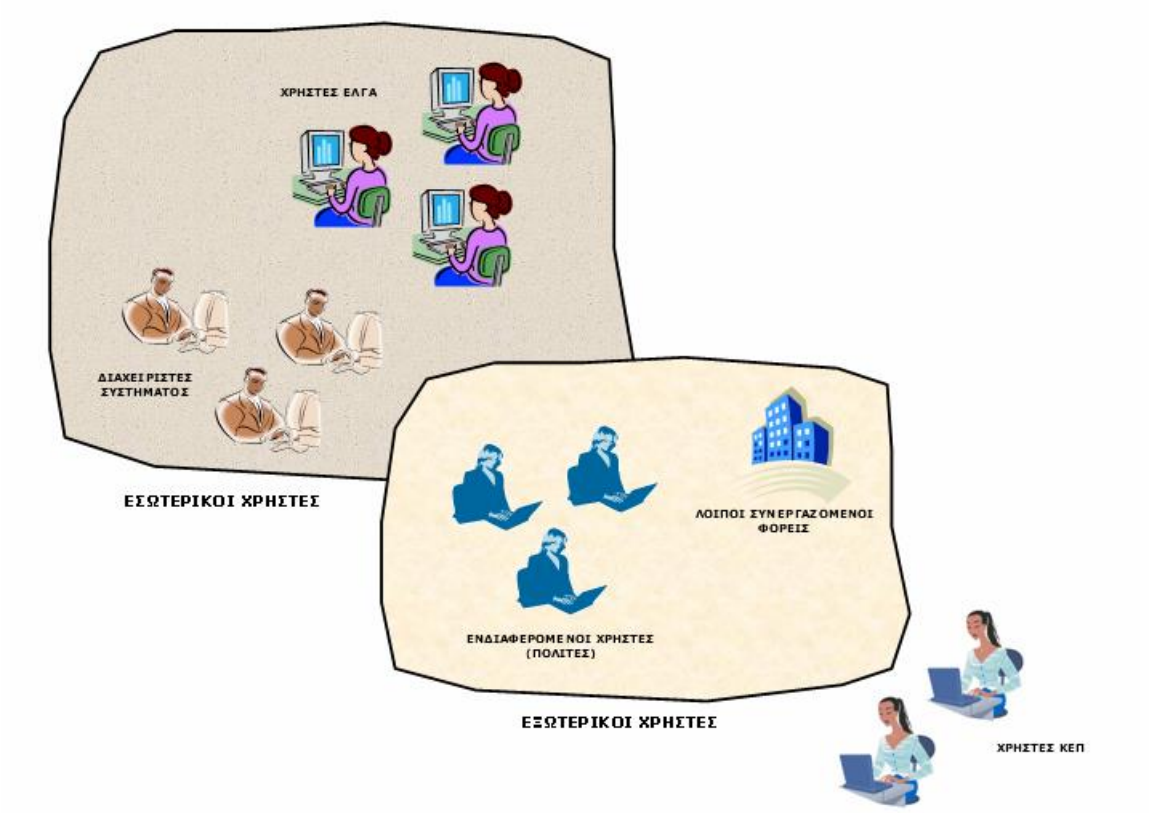
Προκειμένου να καταγραφεί η επιχειρησιακή λογική του συστήματος και ο τρόπος με τον οποίο πιθανόν θα διαχωριστεί σε διαφορετικά αλλά αλληλένδετα υποσυστήματα τα οποία στο σύνολό τους θα δομούν την λειτουργία του, κρίνεται σκόπιμο να παρουσιάσουμε τους εμπλεκόμενους χρήστες των εφαρμογών καθώς

και τις εργασίες – υπηρεσίες που πρέπει να τους παρέχει το σύστημα, οι ανάγκες των οποίων είναι αυτές οι οποίες θα καθορίσουν την τελική δομή του συστήματος.

Οι χρήστες του Πληροφοριακού Συστήματος, μπορούν να ομαδοποιηθούν σε δύο μεγάλες κατηγορίες.

- **Εσωτερικοί χρήστες.** Πρόκειται για το σύνολο των χρηστών- υπαλλήλων ΕΛΓΑ οι οποίοι αλληλοεπιδρούν με το Σύστημα και είναι υπεύθυνοι για την παραγωγική λειτουργία του. Ο αριθμός των χρηστών της κατηγορίας αυτής υπολογίζεται στους τριακοσίους **(300) χρήστες**. Οι χρήστες αυτοί με την σειρά τους, χωρίζονται στις παρακάτω κατηγορίες:
  1. **Χρήστες Εφαρμογής.** Πρόκειται για τους χρήστες που εργάζονται στους χώρους της παραγωγικής λειτουργίας του συστήματος και είναι υπεύθυνοι για την καθημερινή παραγωγή. Οι χρήστες ΕΛΓΑ θα χωριστούν σε υποομάδες ανάλογα με το αντικείμενο εργασίας τους π.χ. χρήστες καταχώρησης στοιχείων, χρήστες παροχής πληροφόρησης σε αγρότες, εκτιμητές ΕΛΓΑ κ.α.
  2. **Διαχειριστές Συστήματος.** Πρόκειται για τους χρήστες του Πληροφοριακού Συστήματος οι οποίοι είναι επιφορτισμένοι με την διαχείριση των εφαρμογών, του λογισμικού και του εξοπλισμού του συστήματος και είναι υπεύθυνοι για την εύρυθμη λειτουργία του. Επίσης θα πρέπει να γνωρίζουν τις βασικές λειτουργικότητες του συστήματος για να παρέχουν βοήθεια σε λοιπούς χρήστες (π.χ. αγρότες χρήστες ΕΛΓΑ κλπ.) στη την χρήση των προσφερόμενων υπηρεσιών (help desk). Οι διαχειριστές συστήματος είναι οι υπεύθυνοι υπάλληλοι από την πλευρά της Δ/νσης Πληροφορικής (DBA, System Administrator) καθώς και οι υπεύθυνοι υπάλληλοι από την πλευρά της Δ/νσης Ασφάλισης οι οποίοι θα παραμετροποιούν την εφαρμογή.
- **Εξωτερικοί χρήστες.** Πρόκειται για τους χρήστες οι οποίοι αλληλοεπιδρούν με το σύστημα αλλά δεν αποτελούν τμήμα της παραγωγικής αλυσίδας αυτού. Οι χρήστες αυτοί ως επί το πλείστων χρησιμοποιούν το σύστημα είτε για την καταχώρηση πρωτογενών πληροφοριών με την ηλεκτρονική υποβολή αιτήσεων τους είτε για την άντληση πληροφοριών και στοιχείων. Ο αριθμός των χρηστών της κατηγορίας αυτής υπολογίζεται πάνω από ένα εκατομμύριο **(>1.000.000) χρήστες.** Οι χρήστες αυτοί από τη μεριά τους διακρίνονται σε:
  1. **Χρήστες Portal ΥΠΑΑΤ- Παραγωγικοί Συντελεστές (Αγρότες).** Οι χρήστες του portal αποτελούν ιδιαίτερη κατηγορία χρηστών οι οποίοι παρότι δεν βρίσκονται στους χώρους της παραγωγικής λειτουργίας του συστήματος και δεν αποτελούν υπαλληλικό προσωπικό του ΕΛΓΑ, ωστόσο θα τροφοδοτούν το σύστημα του ΕΛΓΑ με ένα μεγάλο όγκο πληροφορίας
  2. **Ανταποκριτές ΕΛΓΑ.**
  3. **Ενδιαφερόμενοι (Πολίτες κλπ.**). Πρόκειται για την ομάδα χρηστών οι οποίοι μέσω του Διαδικτύου θα έχουν τη δυνατότητα για πρόσβαση σε μια σειρά ηλεκτρονικών υπηρεσιών με πρόσβαση στην Διαδικτυακή πύλη της εφαρμογής μέσω της οποίας και θα μπορούν είτε να καταχωρούν απευθείας αιτήματα τους προς τον ΕΛΓΑ είτε να ενημερώνονται για την εξέλιξη των διαδικασιών που αφορούν αιτήματά τους για εξυπηρέτησή τους από την Αναθέτουσα Αρχή.
  4. **Λοιποί Φορείς.** Πρόκειται για τους χρήστες φορέων του Ελληνικού Δημοσίου οι οποίοι συνεργάζονται με τα ΕΛΓΑ για διάφορους λόγους.

Η κατανομή των χρηστών του Πληροφοριακού Συστήματος, παρουσιάζεται στο παρακάτω διάγραμμα.



Εικόνα 5:Σχήμα απεικόνισης χρηστών των συστημάτων του ΕΛΓΑ

2.8 Απαιτήσεις Ασφάλειας

Κατά το σχεδιασμό του Έργου ο Ανάδοχος θα πρέπει να λάβει ειδική μέριμνα και να δρομολογήσει τις κατάλληλες δράσεις για :

- την Ασφάλεια των Πληροφοριακών Συστημάτων, Εφαρμογών, Μέσων και Υποδομών
- την προστασία της ακεραιότητας και της διαθεσιμότητας των πληροφοριών
- την προστασία των προς επεξεργασία και αποθηκευμένων προσωπικών δεδομένων
- την εξασφάλιση της μη αποποίησης ενεργειών
- την ταυτοποίηση- αυθεντικοποίηση χρήστη
- την εξασφάλιση διαθεσιμότητας συστήματος

Για το σχεδιασμό και την υλοποίηση των τεχνικών μέτρων ασφαλείας του Έργου, ο Ανάδοχος πρέπει να λάβει υπόψη του :

- το θεσμικό και νομικό πλαίσιο που ισχύει (π.χ. προστασία των προσωπικών δεδομένων Ν. 2472/97,
- προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα (Ν. 2774/99)
- τις σύγχρονες εξελίξεις στις ΤΠΕ
- τις βέλτιστες πρακτικές στο χώρο της Ασφάλειας στις ΤΠΕ (best practices)
- τα επαρκέστερα διατιθέμενα προϊόντα λογισμικού και υλικού

- τυχόν διεθνή de facto ή de jure σχετικά πρότυπα

Για την εφαρμογή, η ασφάλεια των εφαρμογών και των δεδομένων είναι πρώτιστης σημασίας και πρέπει κατ' ελάχιστο να καλύπτει:

- Τον έλεγχο της ασφάλειας στα δεδομένα για τη διασφάλιση της εγκυρότητάς τους.
- Την παροχή διαβαθμισμένης πρόσβασης στους χρήστες της εφαρμογής με ειδικά δικαιώματα χρήσης για κάθε κατηγορία χρηστών.
- Τη διασφάλιση των δεδομένων κατά την μεταφορά τους εσωτερικά στις οργανικές μονάδες του ΕΛΓΑ, αλλά και σε εξωτερικούς συνεργαζόμενους φορείς (π.χ. ΑΤΕ, Υπ. Αγροτικής Ανάπτυξης, ΥΠΕΣΔΔΑ).
- Τη θωράκιση των δεδομένων από εξωτερικούς κινδύνους ή εισβολείς.
- Την προστασία των τυχόν προσωπικών δεδομένων.
- Καταγραφή των κινήσεων/τροποποιήσεων των πινάκων (logging).

Ειδικότερα:

1. Για την εφαρμογή λογισμικού θα πρέπει να παρέχονται αυτόματοι μηχανισμοί ελέγχου της ακεραιότητας και εγκυρότητας των δεδομένων σε πραγματικό χρόνο κατά τις διαδικασίες καταχώρησης, τροποποίησης και διαγραφής, καθώς επίσης και μηχανισμοί ειδοποίησης των χρηστών σε πραγματικό χρόνο κατά την ανίχνευση σφαλμάτων, μέσα από την έγκαιρη προβολή στην οθόνη κατάλληλων μηνυμάτων. Για κάθε περίπτωση τα μηνύματα θα ταξινομούνται σε κατηγορίες (όπως για παράδειγμα σφάλματα, προειδοποίηση, πληροφορία) ανάλογα με το μηχανισμό ελέγχου και θα περιλαμβάνουν κατανοητές και λεπτομερείς οδηγίες ή πληροφορίες, όπως κωδικούς σφαλμάτων, αναλυτική περιγραφή σφαλμάτων, παραπομπή σε αρχείο βοήθειας. Τέλος τα μηνύματα θα πρέπει να επιτρέπουν την άμεση επέμβαση του χρήστη μέσω της διόρθωσης εσφαλμένων ενεργειών, της ακύρωσης ενεργειών, της διόρθωσης σφαλμάτων κ.α. σε πραγματικό χρόνο έτσι ώστε να εξασφαλίζεται η αδιάλειπτη λειτουργία των εφαρμογών.

Επίσης, θα πρέπει να τηρείται ημερολόγιο λειτουργίας για την καταγραφή σφαλμάτων ή δυσλειτουργιών. Το ημερολόγιο λειτουργίας μπορεί να είναι με τη μορφή αρχείου (log file) και υφίστανται οι παρακάτω δυνατότητες ως προς τη διαχείρισή του:

- Έλεγχος και καθορισμός της γραμμογράφησης και της δομής του.
- Ορισμός παραμέτρων όπως μέγιστο μέγεθος, μέγιστος αριθμός καταγεγραμμένων περιστατικών, παράμετροι ιστορικότητας, κτλ.
- Εξαγωγή του σε διαφορετικές μορφές (HTML, Word, Excel, Pdf).
- Επισκόπηση και εκτύπωση.

2. Αναφορικά με την πρόσβαση στα δεδομένα θα πρέπει να παρέχεται ομοιογενής και ενοποιημένος μηχανισμός διαχείρισης των χρηστών και των ρόλων. Ο διαχειριστής του συστήματος μπορεί να ορίσει χρήστες και να αντιστοιχήσει χρήστες σε ρόλους για κάθε διαδικασία διακριτά. Οι δυνατότητες που θα παρέχονται αφορούν:

Στη διαχείριση των κωδικών πρόσβασης σε επίπεδο χρήστη με δυνατότητες ενεργοποίησης /απενεργοποίησης λογαριασμών, αλλαγής κωδικών πρόσβασης, κλπ.

Στον ορισμό δικαιωμάτων πρόσβασης (access rights) και εξουσιοδοτήσεων για κάθε χρήστη και εφαρμογή ξεχωριστά

Η διαχείριση των δικαιωμάτων πρόσβασης θα πρέπει να γίνεται αποκλειστικά από το διαχειριστή του συστήματος μέσω κατάλληλης κεντρικής κονσόλας διαχείρισης για τον ορισμό παραμέτρων ασφαλείας

3. Η επικοινωνία των εφαρμογών για τη μεταφορά δεδομένων θα πρέπει να γίνεται μέσω μηχανισμών πιστοποίησης (authentication) και κρυπτογράφησης (encryption) με χρήση αξιόπιστων τεχνολογιών για τη διασφάλιση των δεδομένων.

ΚΕΦΑΛΑΙΟ 3 Εφαρμογή της octave allegro στον οργανισμό του ΕΛ.Γ.Α.

3.1 Γενικά

Εφαρμόσαμε την μέθοδο octave allegro όπως ακριβώς αυτή ορίζει.

ΒΗΜΑ 1

Αρχικά, θέσαμε τα κριτήρια μέτρησης ρίσκου στα μέτρα του οργανισμού. Ορίσαμε τις επιπτώσεις (χαμηλές, μέτριες, υψηλές) στους τομείς της φήμης-εμπιστοσύνης, της παραγωγικότητας και της ασφάλειας-υγείας σε συνεργασία με τη διοίκηση του οργανισμού που είναι αρμόδια για αυτές και συνεργαστήκαμε με το οικονομικό και νομικό τμήμα για να ορίσουμε τις επιπτώσεις στην περιοχή των οικονομικών και των προστίμων-κυρώσεων. Αυτές οι ενέργειες καταγράφονται στα πρώτα 5 worksheets της octave (ΠΑΡΑΡΤΗΜΑ).

Επιπλέον και πάλι σε συνεργασία με τον οργανισμό, ιεραρχήσαμε τους τομείς για τους οποίους θέσαμε τα κριτήρια παραπάνω. Η διαδικασία αυτή φαίνεται στο worksheet 7 της octave (ΠΑΡΑΡΤΗΜΑ).

ΒΗΜΑ 2

Το επόμενο στάδιο περιλάμβανε τον ορισμό του κρίσιμου στοιχείου πληροφορίας, που δεν είναι άλλο από τα δεδομένα ασφαλιστικών διαδικασιών. Μέσω του worksheet 8 της octave (ΠΑΡΑΡΤΗΜΑ) φτιάξαμε το προφίλ του κρίσιμου αυτού στοιχείου.

Τα δεδομένα αυτά αποτελούν τα στοιχεία που εξυπηρετούν τους πολίτες και κατ' επέκταση τον σκοπό του οργανισμού και αφορούν

- Δηλώσεις Καλλιέργειας-Εκτροφής
- Ασφαλίσεις Γεωργικών Παραγωγών

Ως ιδιοκτήτης του στοιχείου αυτού θεωρείται το πιο υψηλόβαθμο στέλεχος του οργανισμού, δηλαδή ο διευθυντής του ΕΛΓΑ.

Ως προς την ασφάλεια απαιτούμε:

- **εμπιστευτικότητα**, οπότε μόνο εξουσιοδοτημένο προσωπικό, όπως υπάλληλοι του ΚΕΠ και του ΕΛΓΑ μπορούν να δουν τις πληροφορίες του στοιχείου
- **ακεραιότητα,** οπότε μόνο εξουσιοδοτημένο προσωπικό, όπως υπάλληλοι του ΕΛΓΑ μπορούν να τροποποιήσουν τις πληροφορίες του στοιχείου
- **διαθεσιμότητα,** οπότε το στοιχείο είναι διαθέσιμο για 8 ώρες/ημέρα, 5 ημέρες/εβδομάδα, 48 εβδομάδες/χρόνο στους χρήστες του οργανισμού, που χωρίζονται σε χρήστες εφαρμογής και σε διαχειριστές

Ως πιο σημαντική απαίτηση ασφαλείας για τον οργανισμό του ΕΛΓΑ ορίζουμε την ακεραιότητα.

ΒΗΜΑ 3

Αφού φτιάξαμε το προφίλ του στοιχείου, θα πρέπει τώρα να χαρτογραφήσουμε το περιβάλλον μέσα στο οποίο 'ζει' (φυσικό, τεχνικό, ανθρώπινο δυναμικό).

Η καθεμία από τις 3 κατηγορίες χωρίζεται σε εσωτερικό και εξωτερικό και σε κάθε τοποθεσία αναφέρεται ο ιδιοκτήτης της, όπου αυτό είναι δυνατόν.

Ως φυσικό περιβάλλον

- εσωτερικό θεωρούνται φωτοτυπίες που εκτυπώνονται και διατηρούνται εντός οργανισμού περιέχουν δεδομένα ασφαλιστικών διαδικασιών με ιδιοκτήτη τον ΕΛΓΑ.
- εξωτερικό θεωρούνται φωτοτυπίες και πρωτότυπα που περιέχουν δεδομένα ασφαλιστικών διαδικασιών και κατέχουν οι αγρότες στα σπίτια τους με ιδιοκτήτες τους ίδιους τους αγρότες, καθώς και φωτοτυπίες και πρωτότυπα που περιέχουν δεδομένα ασφαλιστικών διαδικασιών διαβιβάζονται σε άλλες δημόσιες υπηρεσίες για έγκριση αποζημιώσεων και κονδυλίων με ιδιοκτήτη τις δημόσιες υπηρεσίες στις οποίες διαβιβάζονται.

Ως τεχνικό περιβάλλον

- εσωτερικό θεωρούνται η oracle database server 10g σε διάταξη clustering, το εσωτερικό δίκτυο ΕΛΓΑ (LAN) και οι θέσεις εργασίας (Η/Υ) με ιδιοκτήτη την Διεύθυνση Πληροφορικής ΕΛΓΑ, καθώς και κάποια routers που διαχειρίζεται ο ΟΤΕ.
- εξωτερικό θεωρείται η ηλεκτρονική πληροφορία για εκτύπωση επιστολών με άγνωστο ιδιοκτήτη και δεδομένα που παρέχονται μέσω internet από τον ΕΛΓΑ στα ΚΕΠ και στο ΥΠΑΤ με ιδιοκτήτη τις υπηρεσίες που τα λαμβάνουν.

Ως ανθρώπινο δυναμικό

- εσωτερικό θεωρούνται οι υπάλληλοι του ΕΛΓΑ.
- εξωτερικό θεωρούνται εξωτερικοί σύμβουλοι και τεχνικοί καθώς και διανομείς εγγράφων.

Έχοντας, λοιπόν, χαρτογραφήσει το περιβάλλον είμαστε έτοιμοι να βρούμε πιθανές αδυναμίες

Οι παραπάνω πληροφορίες ενσωματώνονται στα worksheets 9a, 9b, 9c της octave allegro (ΠΑΡΑΡΤΗΜΑ).

Τα βήματα 4, 5, 6,7,8 υλοποιούνται με το worksheet 10 της octave allegro (ΠΑΡΑΡΤΗΜΑ).

Έχοντας, λοιπόν, χαρτογραφήσει το περιβάλλον είμαστε έτοιμοι να βρούμε πιθανές αδυναμίες, που μπορούν να αποτελέσουν απειλές. Υπολογίζουμε για καθεμία από αυτές το σχετικό σκορ ρίσκου, σύμφωνα με την ιεράρχηση και την αξία της επίπτωσης, και παρατηρούμε, έχοντας προηγουμένως ορίσει την πιθανότητα πραγματοποίησης του σεναρίου απειλής, σε ποιο pool βρισκόμαστε για να αποφασίσουμε σε τι ενέργεια θα προβούμε.

3.2 Εφαρμογή των worksheets στον οργανισμό του ΕΛΓΑ

Το παρακάτω φύλλο εργασίας θέτει τα κριτήρια ρίσκου στην περιοχή της φήμης του οργανισμού καθώς και τις αναφορές των ΜΜΕ σε αυτόν.

Allegro Worksheet 1	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ– ΦΗΜΗ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ**		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
ΦΗΜΗ	Η φήμη επηρεάζεται ελάχιστα, οπότε ελάχιστη ή καθόλου προσπάθεια και μηδαμινά έξοδα απαιτούνται για να επιδιορθώσουμε το πρόβλημα.	Η φήμη έχει καταστραφεί και απαιτείται μεγάλη προσπάθεια για να την επαναφέρουμε στα προηγούμενα επίπεδα.	Η φήμη έχει καταστραφεί ανεπανόρθωτα.
ΜΜΕ (ΚΑΝΑΛΙΑ, ΕΦΗΜΕΡΙΔΕΣ)	Καμία αναφορά δεν γίνεται σχετικά με τις ηλεκτρονικές υπηρεσίες του ΕΛΓΑ.	Γίνονται αναφορές σχετικά με τις ηλεκτρονικές υπηρεσίες του ΕΛΓΑ.	Οι ηλεκτρονικές υπηρεσίες του ΕΛΓΑ αποτελούν πρώτο θέμα.

Το παρακάτω φύλλο εργασίας θέτει τα κριτήρια ρίσκου στην περιοχή των οικονομικών του οργανισμού δίνοντας βάση στα λειτουργικά κόστη και στις στιγμιαίες οικονομικές απώλειες.

Allegro Worksheet 2	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ – ΟΙΚΟΝΟΜΙΚΑ**		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
Λειτουργικά Κόστη	Αύξηση λιγότερη από **5**% στα ετήσια λειτουργικά κόστη.	Αύξηση λιγότερη στα ετήσια λειτουργικά κόστη από **5** %μέχρι **10** %.	Τα ετήσια λειτουργικά κόστη αυξήθηκαν περισσότερο από **10**%.
Στιγμιαία οικονομική απώλεια	Στιγμιαία οικονομική απώλεια λιγότερο από 1% του οικονομικού κύκλου εργασιών.	Στιγμιαία οικονομική απώλεια από 1% μέχρι 5% του οικονομικού κύκλου εργασιών.	Στιγμιαία οικονομική απώλεια μεγαλύτερη από 5% του οικονομικού κύκλου εργασιών.

Το παρακάτω φύλλο εργασίας θέτει τα κριτήρια ρίσκου στην περιοχή της παραγωγικότητας των εργαζομένων του οργανισμού, όσον αφορά στην αύξηση των ωρών που μπορούν να αυξηθούν από πιθανά προβλήματα.

Allegro Worksheet 3	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ – ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ**		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
Ώρες Προσωπικού	Οι ώρες προσωπικού αυξήθηκαν λιγότερο από 10% για 1 μέχρι 5 μέρες.	Οι ώρες προσωπικού αυξήθηκαν από 10% μέχρι 20% για 1 μέχρι 5 μέρες.	Οι ώρες προσωπικού αυξήθηκαν περισσότερο από 20% για 1 μέχρι 5 μέρες.

Το παρακάτω φύλλο εργασίας θέτει τα κριτήρια στην περιοχή της ασφάλειας και της υγείας των εργαζομένων που μπορούν να επηρεαστούν από πιθανά προβλήματα.

Allegro Worksheet 4	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ – ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ**		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
Ζωή	Καμία απώλεια ή σημαντική απειλή στις ζωές των πελατών ή των μελών του προσωπικού.	Οι ζωές των πελατών ή των μελών του προσωπικού απειλούνται, αλλά μπορούν να συνέλθουν μετά από ιατρική βοήθεια.	Απώλεια ζωής πελάτη ή μέλους του προσωπικού.
Υγεία	Ελάχιστα και άμεσα θεραπεύσιμα τραύματα στην υγεία των πελατών ή των μελών του προσωπικού.	Προσωρινή δυσλειτουργία στην υγεία των πελατών ή των μελών του προσωπικού.	Μόνιμη δυσλειτουργία στην υγεία των πελατών ή των μελών του προσωπικού.
Ασφάλεια	Η ασφάλεια αμφισβητείται.	Η ασφάλεια επηρεάζεται.	Η ασφάλεια παραβιάζεται.

Το παρακάτω φύλλο εργασίας θέτει τα κριτήρια στην περιοχή των νομικών κυρώσεων, των προστίμων και των αγωγών που μπορούν να κάνουν τρίτα πρόσωπα απέναντι στον οργανισμό μετά πιθανά προβλήματα που μπορούν να τους επηρεάσουν.

Allegro Worksheet 5	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ–ΠΡΟΣΤΙΜΑ ΚΑΙ ΝΟΜΙΚΕΣ ΚΥΡΩΣΕΙΣ**		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
Πρόστιμα	Πρόστιμα λιγότερα από 50.000 € επιβάλλονται.	Πρόστιμα από 50.000 € μέχρι 200.000 € επιβάλλονται.	Πρόστιμα περισσότερα από 200.000 € επιβάλλονται.
Αγωγές	Αγωγές λιγότερες των 50.000 € εκδικάζονται εναντίον του οργανισμού.	Αγωγές μεταξύ 50.000 € και 200.000 € εκδικάζονται εναντίον του οργανισμού.	Αγωγές υψηλότερες των 200.000€ εκδικάζονται εναντίον του οργανισμού.
Έρευνες	Κανένα ερώτημα από την κυβέρνηση ούτε από άλλους ερευνητικούς οργανισμούς.	Η κυβέρνηση και άλλοι ερευνητικούς οργανισμοί ζητούν λίγες πληροφορίες.	Η κυβέρνηση και άλλοι ερευνητικούς οργανισμοί κάνουν σε βάθος έρευνα.

Το παρακάτω φύλλο εργασίας ιεραρχεί τους τομείς που πλήττονται σύμφωνα με τις ανάγκες του οργανισμού, με το σημαντικότερο τομέα να δέχεται τον υψηλότερο αριθμό και τον λιγότερο σημαντικό την μονάδα.

Allegro Worksheet 7a	**Ιεράρχηση των τομέων που πλήττονται**
ΠΡΟΤΕΡΑΙΟΤΗΤΑ	**Τομείς που πλήττονται**
5	**ΦΗΜΗ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ**
3	**ΟΙΚΟΝΟΜΙΚΑ**
2	**ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ**
1	**ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ**
4	**ΠΡΟΣΤΙΜΑ ΚΑΙ ΝΟΜΙΚΕΣ ΚΥΡΩΣΕΙΣ**

Το παρακάτω φύλλο εργασίας ορίζει το κρίσιμο στοιχείο πληροφορίας, δικαιολογεί την επιλογή του, κάνει περιγραφή του περιεχομένου και ορίζει τις απαιτήσεις ασφαλείας του.

<table>
<tr><td>Allegro Worksheet 8</td><td colspan="3">Προφίλ κρίσιμου στοιχείου πληροφορίας</td></tr>
<tr><td>(1) Κρίσιμο Στοιχείο
Ποιο είναι το κρίσιμο στοιχείο?</td><td colspan="2">(2) Αιτιολόγηση της επιλογής
Γιατί είναι σημαντικό για τον οργανισμό αυτό το στοιχείο πληροφορίας?</td><td>(3) Περιγραφή
Ποια είναι η προσυμφωνημένη περιγραφή αυτού του στοιχείου πληροφορίας?</td></tr>
<tr><td>Τα δεδομένα ασφαλιστικών διαδικασιών</td><td colspan="2">Αποτελούν τα στοιχεία που εξυπηρετούν τους πολίτες και κατ’ επέκταση τον σκοπό του οργανισμού</td><td>1)Ασφαλίσεις Γεωργικών Παραγωγών
2)Δηλώσεις Καλλιέργειας-Εκτροφής
3)ΚΟΕ</td></tr>
<tr><td colspan="4">(4) Ιδιοκτήτης(ες)
Σε ποιον ανήκει αυτό το στοιχείο πληροφορίας?</td></tr>
<tr><td colspan="4">Ο διευθυντής του ΕΛΓΑ</td></tr>
<tr><td colspan="4">(5) Απαιτήσεις Ασφάλειας
Ποιες είναι οι απαιτήσεις ασφάλειας για αυτό το στοιχείο πληροφορίας?</td></tr>
<tr><td>❑ Εμπιστευτικότητα</td><td colspan="2">Μόνο εξουσιοδοτημένο προσωπικό μπορεί να δείτε τις πληροφορίες αυτού του στοιχείου, όπως:</td><td>Υπάλληλοι του ΚΕΠ και του ΕΛΓΑ</td></tr>
<tr><td>❑ Ακεραιότητα</td><td colspan="2">Μόνο εξουσιοδοτημένο προσωπικό μπορεί να τροποποιήσει τις πληροφορίες αυτού του στοιχείου, όπως:</td><td>Υπάλληλοι του ΕΛΓΑ</td></tr>
<tr><td rowspan="2">❑ Διαθεσιμότητα</td><td colspan="2">Αυτό το στοιχείο πληροφορίας πρέπει να είναι διαθέσιμο στα μέλη του προσωπικού που φαίνονται δίπλα, ώστε να κάνουν σωστά τη δουλεία τους</td><td>Εσωτερικοί χρήστες του οργανισμού που χωρίζονται σε χρήστες εφαρμογής και σε διαχειριστές</td></tr>
<tr><td colspan="2">Αυτό το στοιχείο πληροφορίας πρέπει να είναι διαθέσιμο για 8 ώρες, 5 μέρες/εβδομάδα, 48 εβδομάδες/χρόνο.</td><td></td></tr>
<tr><td colspan="4">(6) Η πιο σημαντική απαίτηση ασφάλειας
Ποια είναι η πιο σημαντική απαίτηση ασφάλειας για αυτό το στοιχείο πληροφορίας?</td></tr>
<tr><td>❑ Εμπιστευτικότητα</td><td><u>Ακεραιότητα</u></td><td>❑ Διαθεσιμότητα</td><td>❑ Άλλα</td></tr>
</table>

Στα παρακάτω 3 φύλλα εργασίας χαρτογραφείται το περιβάλλον του κρίσιμου στοιχείου πληροφορίας (φυσικό, τεχνικό, ανθρώπινο δυναμικό), περιγράφοντας την τοποθεσία που φιλοξενείται, καθώς και τον ιδιοκτήτη αυτής.

Allegro Worksheet 9a	**ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΤΟΥ ΣΤΟΙΧΕΙΟΥ ΠΛΗΡΟΦΟΡΙΑΣ (ΦΥΣΙΚΟ)**
ΕΣΩΤΕΡΙΚΟ	
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία	**ΙΔΙΟΚΤΗΤΗΣ ΤΟΠΟΘΕΣΙΑΣ**
1. Φωτοτυπίες που εκτυπώνονται και διατηρούνται εντός οργανισμού περιέχουν δεδομένα ασφαλιστικών διαδικασιών.	Όλα τα τμήματα του ΕΛΓΑ
ΕΞΩΤΕΡΙΚΟ	
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία	**Ιδιοκτήτης Τοποθεσίας**
1. Φωτοτυπίες και πρωτότυπα που περιέχουν δεδομένα ασφαλιστικών διαδικασιών και κατέχουν οι αγρότες στα σπίτια τους.	Ιδιώτες (αγρότες)
2. Φωτοτυπίες και πρωτότυπα που περιέχουν δεδομένα ασφαλιστικών διαδικασιών διαβιβάζονται σε άλλες δημόσιες υπηρεσίες για έγκριση αποζημιώσεων και κονδυλίων.	Δημόσιες Υπηρεσίες

Allegro Worksheet 9b	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΤΟΥ ΣΤΟΙΧΕΙΟΥ ΠΛΗΡΟΦΟΡΙΑΣ (ΤΕΧΝΙΚΟ)	
ΕΣΩΤΕΡΙΚΟ		
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία		**ΙΔΙΟΚΤΗΤΗΣ ΤΟΠΟΘΕΣΙΑΣ**
1.Τα δεδομένα ασφαλιστικών διαδικασιών φιλοξενούνται σε oracle database server 10g σε διάταξη clustering.		Διεύθυνση Πληροφορικής ΕΛΓΑ
2.Εσωτερικό δίκτυο ΕΛΓΑ (LAN)		Διεύθυνση Πληροφορικής ΕΛΓΑ
3.Θέσεις εργασίας (Η/Υ)		Διεύθυνση Πληροφορικής ΕΛΓΑ
4.Routers που διαχειρίζεται εξωτερικός συνεργάτης		ΟΤΕ
ΕΞΩΤΕΡΙΚΟ		
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία		**Ιδιοκτήτης Τοποθεσίας**
1.Ηλεκτρονική πληροφορία για εκτύπωση επιστολών		Άγνωστος
2.Μέσω internet παίρνουν δεδομένα από τον ΕΛΓΑ τα ΚΕΠ και το ΥΠΑΤ		ΚΕΠ
		ΥΠΑΤ

Allegro Worksheet 9c	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΤΟΥ ΣΤΟΙΧΕΙΟΥ ΠΛΗΡΟΦΟΡΙΑΣ (ΑΝΘΡΩΠΙΝΟ ΔΥΝΑΜΙΚΟ)
ΕΣΩΤΕΡΙΚΟ	
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία	**ΙΔΙΟΚΤΗΤΗΣ ΤΟΠΟΘΕΣΙΑΣ**
1.Υπάλληλοι του ΕΛΓΑ	ΕΛΓΑ
ΕΞΩΤΕΡΙΚΟ	
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία	**Ιδιοκτήτης Τοποθεσίας**
1.Εξωτερικοί Σύμβουλοι	Άγνωστος
2.Εξωτερικοί Τεχνικοί	Άγνωστος
3.Διανομείς Εγγράφων	ΕΛΤΑ ή ιδιωτικές επιχειρήσεις ταχυμεταφορών

3.3 Εισαγωγή προβλημάτων στη μέθοδο

Τα προβλήματα εισάγονται στο worksheet 10 και κάθε πρόβλημα θα έχει το δικό του worksheet με δεδομένο πως το κρίσιμο στοιχείο πληροφορίας είναι τα δεδομένα ασφαλιστικών διαδικασιών.

Παρακάτω αναλύονται τα προβλήματα τα οποία εισήχθησαν στη μέθοδο και η αντιμετώπισή τους σύμφωνα με το pool.

3.3.1 Παλιές ηλεκτρονικές υπηρεσίες (worksheet 10a)

Οι παλιές ηλεκτρονικές υπηρεσίες (wis.elga.gr) αποτελούν απειλή για την ασφάλεια των δεδομένων. Εκεί γίνεται είσοδος χωρίς λογαριασμό και υπάρχει δυνατότητα ανάκτησης πληροφορίας με ΑΦΜ, ΑΔΤ.

Οπότε ένας υπάλληλος του οργανισμού ή ένας ιδιώτης που γνωρίζει τον τρόπο εισόδου στο σύστημα θα μπορούσε να ξέρει το ΑΦΜ και τον ΑΔΤ και να κινηθεί αναλόγως για να μάθει την περιουσιακή (οικόπεδα) και οικονομική (αποζημίωση) κατάσταση ενός ατόμου που έχει δώσει στοιχεία στον ΕΛΓΑ.

Με τον τρόπο αυτό θα αποκαλύπτονταν δεδομένα ασφαλιστικών διαδικασιών τα οποία μόνο οι ίδιοι οι αγρότες πρέπει να γνωρίζουν και το εξουσιοδοτημένο προσωπικό να τα διαχειρίζεται.

Η πιθανότητα να συμβεί ένα τέτοιο σενάριο κρίνεται υψηλή και οι συνέπειες που θα έχει για τον οργανισμό η παραβίαση των συνθηκών ασφάλειας από την συγκεκριμένη απειλή είναι νομικές κυρώσεις και χτύπημα στην φήμη του οργανισμού με υψηλές επιπτώσεις.

Μετριασμός του κινδύνου, αν κριθεί σκόπιμος, μπορεί να επιτευχθεί αν ‘κατέβει’ η wis.elga.gr που αποτελεί δυνητική απειλή και πλέον η πρόσβαση γίνεται αποκλειστικά μέσω της services.elga.gr όπου οι αγρότες και οι υπάλληλοι χρησιμοποιούν τα προσωπικά στοιχεία με τα οποία κάνουν login στις εφαρμογές της Γενικής Γραμματείας Πληροφοριακών Συστημάτων για να έχουν πρόσβαση στις ηλεκτρονικές υπηρεσίες του ΕΛΓΑ, και έτσι έχουμε αυθεντικοποίηση αλλά και ταυτοποίηση.

Allegro - Worksheet 10a			Κίνδυνοι για το στοιχείο πληροφορίας
Κίνδυνοι για το στοιχείο πληροφορίας	Απειλές	Στοιχείο Πληροφορίας	Δεδομένα Ασφαλιστικών Διαδικασιών
		Περιοχή ανησυχίας (αδυναμία)	Οι παλιές ηλεκτρονικές υπηρεσίες (wis.elga.gr) αποτελούν απειλή για την ασφάλεια των δεδομένων. Εκεί γίνεται είσοδος χωρίς λογαριασμό και υπάρχει δυνατότητα ανάκτησης πληροφορίας με ΑΦΜ, ΑΔΤ.
		(1) Δράστης *Ποιος θα μπορούσε να εκμεταλλευτεί αυτή την αδυναμία?*	Ένας υπάλληλος του οργανισμού ή ένας ιδιώτης που γνωρίζει τον τρόπο εισόδου στο σύστημα.
		(2) Μέσα *Πως θα μπορούσε να το κάνει αυτό ο δράστης?*	Θα μπορούσε να ξέρει το αφμ και τον ΑΔΤ.
		(3)Κίνητρο *Για ποιο λόγο θα το έκανε αυτό ο δράστης?*	Για να μάθει την περιουσιακή (οικόπεδα) και οικονομική (αποζημίωση) κατάσταση ενός ατόμου που έχει δώσει στοιχεία στον ΕΛΓΑ
		(4)Αποτέλεσμα *Ποιο θα ήταν το αποτέλεσμα της ενέργειας του δράστη στο στοιχείο πληροφορίας?*	❑ ***Αποκάλυψη*** ❑ **Καταστροφή** ❑ **Τροποποίηση** ❑ **Ενόχληση**
		(5) Απαιτήσεις Ασφάλειας *Πώς παραβιάστηκαν οι συνθήκες ασφαλείας?*	Μόνο οι ίδιοι οι αγρότες πρέπει να γνωρίζουν για τα στοιχεία αυτά και το εξουσιοδοτημένο προσωπικό να τα διαχειρίζεται.

		(6) Πιθανότητα *Ποια είναι η πιθανότητα αυτό το σενάριο-απειλή να πραγματοποιηθεί?*	❑ ***Υψηλή***	❑ **Μέτρια**	❑ **Χαμηλή**

(7) Συνέπειες *Τι συνέπειες θα έχει για τον οργανισμό η παραβίαση των συνθηκών ασφάλειας από την συγκεκριμένη απειλή?*	(8)Σοβαρότητα *Πόσο σοβαρές είναι οι συνέπειες σε κάθε θιγόμενη περιοχή?*		
	Περιοχή	**Αξία**	**Σκορ**
Νομικές κυρώσεις και οικονομικό πλήγμα μέσω μηνύσεων	Φήμη και Εμπιστοσύνη Πελατών	Υψηλή	15
	Οικονομικά	Χαμηλή	3
Χτύπημα στην αξιοπιστία και στην φήμη του οργανισμού	Παραγωγικότητα	Χαμηλή	2
	Ασφάλεια και Υγεία	Χαμηλή	1
	Πρόστιμα και Νομικές Κυρώσεις	υψηλή	12
Σχετικό σκορ ρίσκου			**33**

(9) Μετριασμός Κινδύνου *Βασιζόμενοι στο συνολικό σκορ για αυτό τον κίνδυνο, τι δράση θα πραγματοποιούσατε?*			
❑ **Αποδοχή**	❑ **Αναβολή**	❑ ***Μετριασμό***	❑ **Μεταφορά**
Για κινδύνους που αποφασίσατε να μετριάσετε, εφαρμόστε τα ακόλουθα:			
Που θα εφαρμόσετε τους ελέγχους?	*Τι ελέγχους θα εφαρμόσετε και ποιοι κίνδυνοι έχουν γίνει αποδεκτοί?*		
services.elga.gr	Οι αγρότες και οι υπάλληλοι χρησιμοποιούν τα προσωπικά στοιχεία με τα οποία κάνουν login στις εφαρμογές της Γενικής Γραμματείας Πληροφοριακών Συστημάτων για να έχουν πρόσβαση στις ηλεκτρονικές υπηρεσίες του ΕΛΓΑ, ώστε να επιτευχθεί αυθεντικοποίηση αλλά και ταυτοποίηση.		
Wis.elga.gr	Δεν χρησιμοποιείται ευρέως αφού η κύρια σελίδα είναι η services.elga.gr και επειδή αποτελεί δυνητική απειλή πρέπει να ‘κατέβει’.		

3.3.2 Φθορά και παλαιότητα του hardware infrastructure (worksheet 10b)

Το hardware infrastructure έχει να αντιμετωπίσει προβλήματα όπως η παλαιότητα των διακομιστών και του Microsoft ISA server, router με πολλά σφάλματα, που οδηγούν σε προσωρινή αδυναμία προσπέλασης των στοιχείων και σε καθυστέρηση.

Σε μία τέτοια περίπτωση, το αποτέλεσμα θα ήταν προσωρινή ενόχληση, χωρίς να αποκλείεται πιθανή καταστροφή δεδομένων, παραβιάζοντας έτσι την αρχή της διαθεσιμότητας και της ακεραιότητας των δεδομένων ασφαλιστικών διαδικασιών.

Η πιθανότητα να συμβεί ένα τέτοιο σενάριο κρίνεται υψηλή και οι συνέπειες που θα έχει για τον οργανισμό η παραβίαση των συνθηκών ασφάλειας από την συγκεκριμένη απειλή είναι προσωρινή αδυναμία προσπέλασης των στοιχείων που επηρεάζει τη φήμη του οργανισμού με μέτρια επίπτωση και καθυστερήσεις στις καθημερινές εργασίες των υπαλλήλων που επηρεάζουν την παραγωγικότητα με υψηλή επίπτωση.

Μετριασμός του κινδύνου, αν κριθεί σκόπιμος, μπορεί να επιτευχθεί αν παραγγείλουμε νέα routers ώστε να μπορούμε να δουλεύουμε με αξιοπιστία και ταχύτητα και αν πραγματοποιήσουμε hardware firewalls που προσθέτουν περαιτέρω ασφάλεια, αντισταθμίζοντας την παλαιότητα.

Allegro - Worksheet 10b			Κίνδυνοι για το στοιχείο πληροφορίας
Κίνδυνοι για το στοιχείο πληροφορίας	Απειλές	Στοιχείο Πληροφορίας	Δεδομένα Ασφαλιστικών Διαδικασιών
		Περιοχή ανησυχίας (αδυναμία)	Το hardware infrastructure έχει να αντιμετωπίσει προβλήματα όπως η παλαιότητα των διακομιστών και του ISA server, router με πολλά σφάλματα, που οδηγούν σε προσωρινή αδυναμία προσπέλασης των στοιχείων και σε καθυστέρηση.
		(1) Δράστης *Ποιος θα μπορούσε να εκμεταλλευτεί αυτή την αδυναμία?*	----------
		(2) Μέσα *Πως θα μπορούσε να το κάνει αυτό ο δράστης?*	----------
		(3)Κίνητρο *Για ποιο λόγο θα το έκανε αυτό ο δράστης?*	----------
		(4)Αποτέλεσμα *Ποιο θα ήταν το αποτέλεσμα της ενέργειας του δράστη στο στοιχείο πληροφορίας?*	❑ **Αποκάλυψη** ❑ ***Καταστροφή*** ❑ **Τροποποίηση** ❑ ***Ενόχληση***
		(5) Απαιτήσεις Ασφάλειας *Πώς παραβιάστηκαν οι συνθήκες ασφαλείας?*	Παραβιάζεται η αρχή της διαθεσιμότητας.

		(6) Πιθανότητα *Ποια είναι η πιθανότητα αυτό το σενάριο-απειλή να πραγματοποιηθεί?*	❑ **Υψηλή**	❑ ***Μέτρια***	❑ **Χαμηλή**

(7) Συνέπειες *Τι συνέπειες θα έχει για τον οργανισμό η παραβίαση των συνθηκών ασφάλειας από την συγκεκριμένη απειλή?*	(8)Σοβαρότητα *Πόσο σοβαρές είναι οι συνέπειες σε κάθε θιγόμενη περιοχή?*		
	Περιοχή	**Αξία**	**Σκορ**
Προσωρινή αδυναμία προσπέλασης των στοιχείων που επηρεάζει τη φήμη του οργανισμού.	Φήμη και Εμπιστοσύνη Πελατών	Μέτρια	10
	Οικονομικά	Χαμηλή	3
Καθυστερήσεις στις καθημερινές εργασίες των υπαλλήλων που επηρεάζουν την παραγωγικότητα.	Παραγωγικότητα	Υψηλή	6
	Ασφάλεια και Υγεία	Χαμηλή	1
	Πρόστιμα και Νομικές Κυρώσεις	χαμηλή	4
Σχετικό σκορ ρίσκου			**24**

(9) Μετριασμός Κινδύνου *Βασιζόμενοι στο συνολικό σκορ για αυτό τον κίνδυνο, τι δράση θα πραγματοποιούσατε?*			
❑ **Αποδοχή**	❑ **Αναβολή**	❑ ***Μετριασμό***	❑ **Μεταφορά**
Για κινδύνους που αποφασίσατε να μετριάσετε, εφαρμόστε τα ακόλουθα:			
Που θα εφαρμόσετε τους ελέγχους?	*Τι ελέγχους θα εφαρμόσετε και ποιοι κίνδυνοι έχουν γίνει αποδεκτοί?*		
routers	Πρέπει να παραγγείλουμε νέα routers ώστε μα μπορούμε να δουλεύουμε με αξιοπιστία και ταχύτητα.		
Διακομιστές	Θα πραγματοποιήσουμε hardware firewalls που προσθέτει περαιτέρω ασφάλεια, αντισταθμίζοντας την παλαιότητα.		

3.3.3 Απουσία disaster plan και ακαταλληλότητα χώρου του computer room (worksheet 10c)

Το hardware infrastructure έχει να αντιμετωπίσει ακραία καιρικά φαινόμενα, διακοπές ρεύματος και πιθανές καταστροφές στον, ακατάλληλο σήμερα και γεμάτο χάρτινα κουτιά, χώρο του computer room, όπου και βρίσκεται.

Σε μία τέτοια περίπτωση, το αποτέλεσμα θα ήταν ενόχληση για μεγάλο χρονικό διάστημα και σίγουρη καταστροφή δεδομένων, παραβιάζοντας έτσι την αρχή της ακεραιότητας των στοιχειών, καθώς πολλά μπορούν να χαθούν και της διαθεσιμότητας καθώς το σύστημα μπορεί να είναι πεσμένο για μεγάλο διάστημα.

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 καταστροφή και απώλεια των στοιχείων λόγω καταστροφής του hardware που θα αποτελέσει οικονομικό πλήγμα καθώς θα πρέπει να αντικατασταθεί με νέο εξοπλισμό με υψηλή επίπτωση στον οικονομικό τομέα, η φήμη του οργανισμού θα 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 και τέλος κάποιοι μπορούν να κινηθούν νομικά με μέτριες επιπτώσεις στον τομέα των προστίμων.

Μετριασμός του κινδύνου, αν κριθεί σκόπιμος, μπορεί να επιτευχθεί αν οργανώσουμε ένα disaster plan, ώστε σε περίπτωση σεισμού ή διακοπής ρεύματος ή κάποιας άλλης φυσικής καταστροφής διασφαλίσουμε πως όλα τα δεδομένα έχουν αντιγραφεί και βρίσκονται σε back-up tapes από όπου μπορούν να ανασυρθούν αμέσως και εάν ο χώρος είναι καθαρός και υπάρχουν μέσα που μπορούν να αποτρέψουν μια πυρκαγιά μέσα σε αυτόν, ενώ γίνεται παράλληλα έλεγχος με κάμερα στην είσοδο ώστε να έχουμε πλήρη καταγραφή των παρουσιών στο χώρο.

Allegro - Worksheet 10c			**Κίνδυνοι για το στοιχείο πληροφορίας**
Κίνδυνοι για το στοιχείο πληροφορίας	**Απειλές**	Στοιχείο Πληροφορίας	Δεδομένα Ασφαλιστικών Διαδικασιών
		Περιοχή ανησυχίας (αδυναμία)	Το hardware infrastructure έχει να αντιμετωπίσει ακραία καιρικά φαινόμενα, διακοπές ρεύματος και πιθανές καταστροφές στον, ακατάλληλο σήμερα και γεμάτο χάρτινα κουτιά, χώρο του computer room, όπου και βρίσκεται.
		(1) Δράστης *Ποιος θα μπορούσε να εκμεταλλευτεί αυτή την αδυναμία?*	----------
		(2) Μέσα *Πως θα μπορούσε να το κάνει αυτό ο δράστης?*	----------
		(3)Κίνητρο *Για ποιο λόγο θα το έκανε αυτό ο δράστης?*	----------
		(4)Αποτέλεσμα *Ποιο θα ήταν το αποτέλεσμα της ενέργειας του δράστη στο στοιχείο πληροφορίας?*	❑ **Αποκάλυψη** ❑ ***Καταστροφή*** ❑ **Τροποποίηση** ❑ ***Ενόχληση***
		(5) Απαιτήσεις Ασφάλειας *Πώς παραβιάστηκαν οι συνθήκες ασφαλείας?*	Παραβιάζεται η αρχή της ακεραιότητας των στοιχειών καθώς πολλά μπορούν να χαθούν και της διαθεσιμότητας καθώς το σύστημα μπορεί να είναι πεσμένο για μεγάλο διάστημα.

		(6) Πιθανότητα *Ποια είναι η πιθανότητα αυτό το σενάριο-απειλή να πραγματοποιηθεί?*	❑ **Υψηλή**	❑ ***Μέτρια***	❑ **Χαμηλή**

(7) Συνέπειες *Τι συνέπειες θα έχει για τον οργανισμό η παραβίαση των συνθηκών ασφάλειας από την συγκεκριμένη απειλή?*	(8)Σοβαρότητα *Πόσο σοβαρές είναι οι συνέπειες σε κάθε θιγόμενη περιοχή?*		
	Περιοχή	**Αξία**	**Σκορ**
Καταστροφή και απώλεια των στοιχείων λόγω καταστροφής του hardware θα αποτελέσει οικονομικό πλήγμα καθώς θα πρέπει να αντικατασταθεί με νέο εξοπλισμό	Φήμη και Εμπιστοσύνη Πελατών	Υψηλή	15
	Οικονομικά	Υψηλή	9
Η φήμη του οργανισμού θα χτυπηθεί καθώς και η εμπιστοσύνη των πολιτών απέναντι του λόγω των απωλειών στοιχείων σημαντικών για τις ασφαλίσεις.	Παραγωγικότητα	Χαμηλή	2
	Ασφάλεια και Υγεία	Χαμηλή	1
Ο οργανισμός θα δεχθεί κυρώσεις.	Πρόστιμα και Νομικές Κυρώσεις	Μέτρια	8

Σχετικό σκορ ρίσκου	**35**

(9) Μετριασμός Κινδύνου

Βασιζόμενοι στο συνολικό σκορ για αυτό τον κίνδυνο, τι δράση θα πραγματοποιούσατε?

❑ **Αποδοχή**	❑ **Αναβολή**	❑ ***Μετριασμό***	❑ **Μεταφορά**

Για κινδύνους που αποφασίσατε να μετριάσετε, εφαρμόστε τα ακόλουθα:

Που θα εφαρμόσετε τους ελέγχους?	*Τι ελέγχους θα εφαρμόσετε και ποιοι κίνδυνοι έχουν γίνει αποδεκτοί?*
Disaster Plan	Σε περίπτωση σεισμού ή διακοπής ρεύματος ή κάποιας άλλης φυσικής καταστροφής πρέπει να διασφαλίσουμε πως όλα τα δεδομένα έχουν αντιγραφεί και βρίσκονται σε back-up tapes από όπου μπορούν να ανασυρθούν αμέσως.
Καταλληλόλητα Χώρου στο cm	Ο χώρος θα πρέπει να είναι καθαρός, να υπάρχουν μέσα που μπορούν να αποτρέψουν μια πυρκαγιά μέσα σε αυτόν και να γίνεται έλεγχος με κάμερα στην είσοδο ώστε να έχουμε πλήρη καταγραφή των παρουσιών στο χώρο.

3.3.4 Απευθείας πρόσβαση στους servers του οργανισμού (worksheet 10d)

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.

Μετριασμός του κινδύνου, αν κριθεί σκόπιμος, μπορεί να επιτευχθεί αν στο Εσωτερικό Δίκτυο Οργανισμού εφαρμόσουμε τη λύση DMZ (demilitarized zone) που σε όρους security information είναι ένα φυσικό ή λογικό υποδίκτυο που εκθέτει στοιχεία του εσωτερικού δικτύου σε ένα εξωτερικό, μεγάλο και αναξιόπιστο δίκτυο. Το υποδίκτυο αυτό προσφέρει ένα επιπλέον δίχτυ ασφαλείας στα LAN του οργανισμού, αφού ο δράστης μπορεί να επιτεθεί μόνο στην DMZ και όχι στο ίδιο το LAN. Επιπλέον, για τους servers μπορούμε να εφαρμόσουμε CMZ (classified militarized zones). Σε μία τέτοια αρχιτεκτονική η DMZ παίζει το ρόλο του firewall για το CMZ, ενώ το CMZ φιλοξενεί τους servers.

Allegro - Worksheet 10d			Κίνδυνοι για το στοιχείο πληροφορίας
Κίνδυνοι για το στοιχείο πληροφορίας	**Απειλές**	Στοιχείο Πληροφορίας	Δεδομένα Ασφαλιστικών Διαδικασιών
		Περιοχή ανησυχίας (αδυναμία)	Οι υπάλληλοι έχουν απευθείας πρόσβαση στους servers του οργανισμού από τις θέσεις εργασίας τους.
		(1) Δράστης *Ποιος θα μπορούσε να εκμεταλλευτεί αυτή την αδυναμία?*	Ένας από τους χρήστες του συστήματος
		(2) Μέσα *Πως θα μπορούσε να το κάνει αυτό ο δράστης?*	Με πρόσβαση στο σύστημα
		(3)Κίνητρο *Για ποιο λόγο θα το έκανε αυτό ο δράστης?*	Για να τροποποιήσει ή να καταστρέψει πληροφορίες έχοντας κάποιο προσωπικό όφελος μέσω αυτής της ενέργειας
		(4)Αποτέλεσμα *Ποιο θα ήταν το αποτέλεσμα της ενέργειας του δράστη στο στοιχείο πληροφορίας?*	❑ ***Αποκάλυψη*** ❑ ***Καταστροφή*** ❑ ***Τροποποίηση*** ❑ **Ενόχληση**
		(5)Απαιτήσεις Ασφαλείας *Πώς παραβιάστηκαν οι συνθήκες ασφαλείας?*	Παραβιάζεται η ακεραιότητα της πληροφορίας αφού την διαχειρίστηκαν άτομα που δεν είχαν τέτοια αρμοδιότητα και εξουσιοδότηση.

		(6) Πιθανότητα *Ποια είναι η πιθανότητα αυτό το σενάριο-απειλή να πραγματοποιηθεί?*	❑ **Υψηλή**	❑ ***Μέτρια***	❑ **Χαμηλή**

(7) Συνέπειες *Τι συνέπειες θα έχει για τον οργανισμό η παραβίαση των συνθηκών ασφάλειας από την συγκεκριμένη απειλή?*	(8)Σοβαρότητα *Πόσο σοβαρές είναι οι συνέπειες σε κάθε θιγόμενη περιοχή?*		
	Περιοχή	**Αξία**	**Σκορ**
Η φήμη του οργανισμού θα χτυπηθεί καθώς και η εμπιστοσύνη των πολιτών απέναντι του λόγω των απωλειών.	Φήμη και Εμπιστοσύνη Πελατών	Υψηλή	15
	Οικονομικά	Υψηλή	9
Κάποιοι μπορεί να κινηθούν νομικά με μηνύσεις και να υπάρξουν κυρώσεις.	Παραγωγικότητα	Χαμηλή	2
	Ασφάλεια και Υγεία	Χαμηλή	1
Οικονομικές απώλειες λόγω αλλοίωσης στοιχείων αποζημιώσεων	Πρόστιμα και Νομικές Κυρώσεις	Υψηλή	12

Σχετικό σκορ ρίσκου	**39**

(9) Μετριασμός Κινδύνου *Βασιζόμενοι στο συνολικό σκορ για αυτό τον κίνδυνο, τι δράση θα πραγματοποιούσατε?*			
❑ **Αποδοχή**	❑ **Αναβολή**	❑ ***Μετριασμό***	❑ **Μεταφορά**
Για κινδύνους που αποφασίσατε να μετριάσετε, εφαρμόστε τα ακόλουθα:			
Που θα εφαρμόσετε τους ελέγχους?	*Τι ελέγχους θα εφαρμόσετε και ποιοι κίνδυνοι έχουν γίνει αποδεκτοί?*		
Εσωτερικό Δίκτυο Οργανισμού	Μπορούμε να εφαρμόσουμε τη λύση DMZ (demilitarized zone) που σε όρους security information είναι ένα φυσικό ή λογικό υποδίκτυο που εκθέτει στοιχεία του εσωτερικού δικτύου σε ένα εξωτερικό, μεγάλο και αναξιόπιστο δίκτυο. Το υποδίκτυο αυτό προσφέρει ένα επιπλέον δίχτυ ασφαλείας στα LAN του οργανισμού, αφού ο δράστης μπορεί να επιτεθεί μόνο στην DMZ και όχι στο ίδιο το LAN. Επιπλέον, για τους servers μπορούμε να εφαρμόσουμε CMZ (classified militarized zones). Σε μία τέτοια αρχιτεκτονική η DMZ παίζει το ρόλο του firewall για το CMZ, ενώ το CMZ φιλοξενεί τους servers.		

3.3.5 Απουσία IT administrator (worksheet 10e)

Δεν υπάρχει διαχείριση των logs (ηλεκτρονικά ‘ίχνη’), οπότε δεν μπορεί να ανιχνευθεί και να αποτραπεί επίθεση από hackers. Σε περίπτωση επίθεσης, είναι πιθανό να επιτύχουν καθώς δεν έχουν γίνει updates στο σύστημα με αποτέλεσμα να υπάρχουν security holes, δεν έχουν ανανεωθεί οι άδειες για τα antivirus και δεν υπάρχει το σωστό firewall.

Ένας threat intruder με γνώσεις πληροφορικής υψηλού επιπέδου έχοντας πολιτικό ή οικονομικό κίνητρο μπορεί να προβεί σε τροποποιήσεις, καταστροφές, αποκαλύψεις δεδομένων και ενοχλήσεις του συστήματος, παραβιάζοντας την ακεραιότητα, την διαθεσιμότητα και το απόρρητο της πληροφορίας.

Η πιθανότητα να συμβεί ένα τέτοιο σενάριο κρίνεται υψηλή 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 τέλος αν το σύστημα είναι πεσμένο για ώρα έχουμε μέτριες επιπτώσεις στον τομέα της παραγωγικότητας.

Μετριασμός του κινδύνου, αν κριθεί σκόπιμος, μπορεί να επιτευχθεί με ανάθεση, από την διοίκηση σε εξωτερικούς συνεργάτες, του monitoring των IDS (intrusion detection system)/IPS (intrusion protection system) συσκευών, της διαχείρισης των logs και της μέριμνας για τα system updates και τις ανανεώσεις των αδειών των antivirus.

Allegro - Worksheet 10e			Κίνδυνοι για το στοιχείο πληροφορίας
Κίνδυνοι για το στοιχείο πληροφορίας	Απειλές	Στοιχείο Πληροφορίας	Δεδομένα Ασφαλιστικών Διαδικασιών
		Περιοχή ανησυχίας (αδυναμία)	Δεν υπάρχει διαχείριση των logs (ηλεκτρονικά 'ίχνη'), οπότε δεν μπορεί να ανιχνευθεί και να αποτραπεί επίθεση από hackers. Σε περίπτωση επίθεσης, είναι πιθανό να επιτύχουν καθώς δεν έχουν γίνει updates στο σύστημα με αποτέλεσμα να υπάρχουν security holes, δεν έχουν ανανεωθεί οι άδειες για τα antivirus και δεν υπάρχει το σωστό firewall.
		(1) Δράστης *Ποιος θα μπορούσε να εκμεταλλευτεί αυτή την αδυναμία?*	Ένας threat intruder
		(2) Μέσα *Πως θα μπορούσε να το κάνει αυτό ο δράστης?*	Γνώσεις πληροφορικής υψηλού επιπέδου
		(3)Κίνητρο *Για ποιο λόγο θα το έκανε αυτό ο δράστης?*	Για να τροποποιήσει ή να καταστρέψει πληροφορίες έχοντας πολιτικό ή οικονομικό κίνητρο.
		(4)Αποτέλεσμα *Ποιο θα ήταν το αποτέλεσμα της ενέργειας του δράστη στο στοιχείο πληροφορίας?*	❑ ***Αποκάλυψη*** ❑ ***Καταστροφή*** ❑ ***Τροποποίηση*** ❑ ***Ενόχληση***
		(5) Απαιτήσεις Ασφάλειας *Πώς παραβιάστηκαν οι συνθήκες ασφαλείας?*	Παραβιάζεται η ακεραιότητα και η διαθεσιμότητα και το απόρρητο της πληροφορίας.

		(6) Πιθανότητα *Ποια είναι η πιθανότητα αυτό το σενάριο-απειλή να πραγματοποιηθεί?*	❑ **Υψηλή**	❑ ***Μέτρια***	❑ **Χαμηλή**

(7) Συνέπειες *Τι συνέπειες θα έχει για τον οργανισμό η παραβίαση των συνθηκών ασφάλειας από την συγκεκριμένη απειλή?*	(8)Σοβαρότητα *Πόσο σοβαρές είναι οι συνέπειες σε κάθε θιγόμενη περιοχή?*		
	Περιοχή	**Αξία**	**Σκορ**
Η φήμη του οργανισμού θα χτυπηθεί καθώς και η εμπιστοσύνη των πολιτών απέναντι του λόγω των απωλειών.	Φήμη και Εμπιστοσύνη Πελατών	Υψηλή	15
	Οικονομικά	Χαμηλή	3
Κάποιοι μπορεί να κινηθούν νομικά με μηνύσεις και να υπάρξουν κυρώσεις.	Παραγωγικότητα	Μέτρια	4
	Ασφάλεια και Υγεία	Χαμηλή	1
Εάν το σύστημα είναι πεσμένο για ώρα επηρεάζεται αρνητικά η παραγωγικότητα των εργαζομένων.	Πρόστιμα και Νομικές Κυρώσεις	Υψηλή	12

Σχετικό σκορ ρίσκου **35**

(9) Μετριασμός Κινδύνου *Βασιζόμενοι στο συνολικό σκορ για αυτό τον κίνδυνο, τι δράση θα πραγματοποιούσατε?*			
❑ **Αποδοχή**	❑ **Αναβολή**	❑ ***Μετριασμό***	❑ ***Μεταφορά***
Για κινδύνους που αποφασίσατε να μετριάσετε, εφαρμόστε τα ακόλουθα:			
Που θα εφαρμόσετε τους ελέγχους?	*Τι ελέγχους θα εφαρμόσετε και ποιοι κίνδυνοι έχουν γίνει αποδεκτοί?*		
Διοίκηση Οργανισμού	Πρέπει να ανατεθεί από την διοίκηση σε εξωτερικούς συνεργάτες το monitor IDS (intrusion detection system)/IPS (intrusion protection system) συσκευών, η διαχείριση των logs και η μέριμνα για τα system updates και τις ανανεώσεις των αδειών των antivirus.		

3.4 Συμπεράσματα

Αφού εφαρμόσαμε τη μέθοδο εισάγοντας τα προβλήματα του οργανισμού, παρατηρούμε πως το πιο σημαντικό βήμα είναι η σωστή ιεράρχηση των τομέων που πλήττονται. Εφαρμόζοντας την μέθοδο με την ιεράρχηση του worksheet 7a, συμπεραίνουμε πως για τα 5 βασικά προβλήματα οδηγούμαστε σε μετριασμό για τα πρώτα 4 και σε μεταφορά σε εξωτερικό συνεργάτη για το τελευταίο.

Σε εφαρμογή της μεθόδου με διαφορετική ιεράρχηση που θέτει ως ύψιστης σημασίας την υγεία και την παραγωγικότητα (worksheet 7b, Παράρτημα), παρατηρούμε σύμφωνα με το σχετικό σκορ ρίσκου πως γίνεται αποδοχή ή αναβολή των προβλημάτων, με αποτέλεσμα η σύσταση να είναι να μην αντιμετωπιστούν τα προβλήματα.

Τελικώς, συμπεραίνουμε πως τα προβλήματα που ανιχνεύθηκαν είναι κρίσιμα για συγκεκριμένους τομείς, όπως η φήμη και τα οικονομικά του οργανισμού και αδιάφορα για άλλους, όπως η υγεία και η παραγωγικότητα. Η φύση, όμως, του οργανισμού δείχνει να θέλει την πρώτη ιεράρχηση, άρα θα πρέπει να προβούμε στην αντιμετώπιση που παρουσιάστηκε.

ΚΕΦΑΛΑΙΟ 4 Παρουσίαση του λογισμικού Practical Threat Analysis

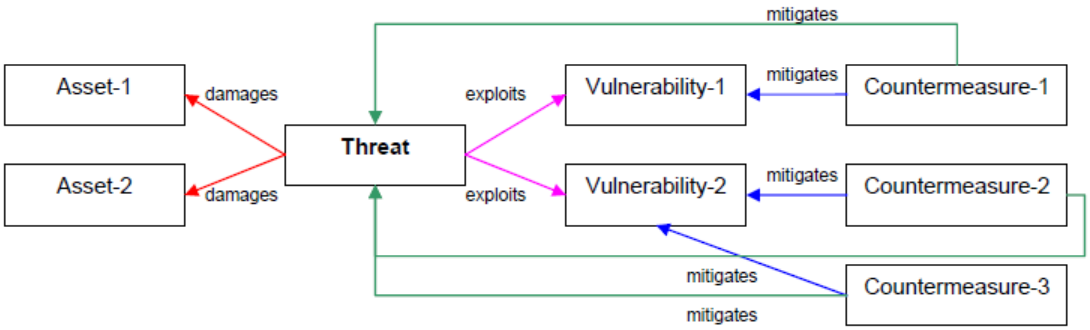
4.1 Μεθοδολογία Μοντελοποίησης και Υπολογισμού Απειλών

Η μεθοδολογία ανάλυσης PTA επιτρέπει την αποτελεσματική διαχείριση των κινδύνων λειτουργίας και ασφάλειας σε πολύπλοκα συστήματα. Παρέχει έναν εύκολο τρόπο για να διατηρήσει τα μοντέλα δυναμικών απειλών ικανά να αντιδρούν σε αλλαγές πάνω σε στοιχεία του ενεργητικού και σε τρωτά σημεία του συστήματος. Επιπλέον ένας αναλυτής, με τη βοήθεια του PTA, μπορεί να διατηρήσει μια βάση δεδομένων με απειλές, να δημιουργήσει αρχείο με εκθέσεις για την ασφάλεια και να παράξει νέες, που δείχνουν τη σημασία των διαφόρων απειλών και τις προτεραιότητες των αντίστοιχων αντιμέτρων.

Το PTA υπολογίζει τις απειλές και τα αντίμετρα και παρέχει στους φορείς λήψης αποφάσεων με ενημερωμένα, όσον αφορά στον κίνδυνο, σχέδιο μετριασμού των επιπτώσεων που αντανακλούν τις μεταβολές στις πραγματικές απειλές. Οι προτεραιότητες των αντιμέτρων είναι μια λειτουργία των αξιών των περιουσιακών στοιχείων του συστήματος, το επιπέδου των πιθανών ζημιών, των πιθανοτήτων των απειλών και των βαθμών άμβλυνσης που παρέχονται από τα αντίμετρα. Το συνιστάμενο σχέδιο μετριασμού αποτελείται από τα αντίμετρα που είναι τα πιο οικονομικά αποδοτικά ενάντια στις προσδιορισμένες απειλές.

4.2 Το μοντέλο του PTA

Το παρακάτω σχήμα περιγράφει τις διασυνδέσεις μεταξύ απειλή και τα περιουσιακά στοιχεία, τα τρωτά σημεία και αντίμετρα.



Εικόνα 6:Σχηματική περιγραφή των διασυνδέσεων μεταξύ απειλών, περιουσιακών στοιχείων, αδυναμιών και αντιμέτρων στο PTA

Το μοντέλο του PTA λειτουργεί ως εξής:

- Οι απειλές εκμεταλλεύονται τις αδυναμίες και καταστρέφουν τα περιουσιακά στοιχεία πληροφορίας.
- Τα αντίμετρα μετριάζουν τις αδυναμίες και, επομένως, μετριάζουν τις απειλές. (10)

4.3 Οι διαδικασίες στο μοντέλο του PTA

1 Προσδιορισμός των περιουσιακών στοιχείων πληροφορίας

Χαρτογράφηση των οικονομικών αξιών των περιουσιακών στοιχείων του συστήματος και πιθανές ζημίες που οφείλονται σε καταστροφές. Οι αξίες των περιουσιακών στοιχείων είναι η βάση για τον υπολογισμό των απειλών, των κινδύνων και των προτεραιοτήτων των αντιμέτρων.

2.Προσδιορισμός των αδυναμιών

Προσδιορισμός των πιθανών τρωτών σημείων απαιτεί γνώση της λειτουργικότητας, της αρχιτεκτονικής, και των επιχειρησιακές διαδικασιών του συστήματος και γνώση των τύπων των χρηστών του συστήματος. Αυτή είναι μια συνεχής επαναληπτική εργασία σε συνδυασμό με το στάδιο του εντοπισμού απειλών (στάδιο 4).

3.Καθορισμός Αντιμέτρων

Καθορισμός των αντιμέτρων σχετικά με τα τρωτά σημεία του συστήματος. Η σχέση κόστους-αποτελεσματικότητας των αντιμέτρων υπολογίζεται με βάση το εκτιμώμενο της κόστος υλοποίησης.

4.Σχεδιασμός σεναρίων απειλών και πλάνων μετριασμού

Γίνεται σύνθεση σεναρίων πιθανών απειλών και εντοπισμός στοιχείων απειλών και παραμέτρων ως εξής:

- Εισάγεται μια σύντομη περιγραφή του σεναρίου απειλής.

- Προσδιορίζονται τα απειλούμενα περιουσιακά στοιχεία και το επίπεδο των ζημιών που προκλήθηκαν σε κάθε περιουσιακό στοιχείο.

- Προσδιορισμός των τρωτών σημείων του συστήματος που εκμεταλλεύεται η απειλή. Η αναγνώριση αυτή συμπληρώνει αυτόματα μια λίστα των προτεινόμενων αντιμέτρων.

- Ρύθμιση της πιθανότητας εμφάνισης της απειλής. Το επίπεδο κινδύνου της απειλής υπολογίζεται αυτόματα με βάση το σύνολο των ζημιών που μπορεί να προκληθεί από την απειλή και πραγματοποίησής της.

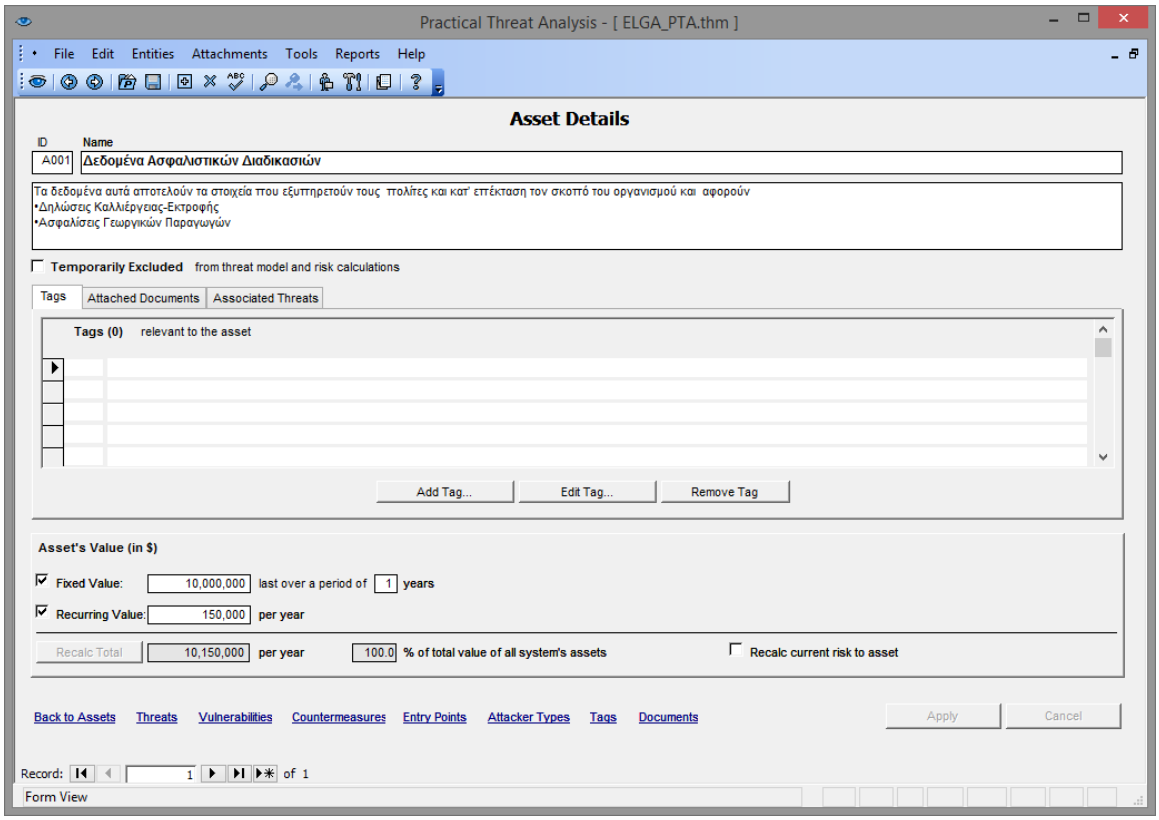
- Αποφασίζεται το πραγματικό σχέδιο μετριασμού επιλέγοντας τον πιο αποτελεσματικό συνδυασμό αντιμέτρων.

4.4 Εφαρμογή του PTA στον οργανισμό του ΕΛΓΑ

Για να εφαρμόσουμε το λογισμικό στα προβλήματα του οργανισμού πρέπει να ορίσουμε το critical asset, τις αδυναμίες του οργανισμού και τις απειλές που μπορούν να εκμεταλλευτούν αυτές τις αδυναμίες. Τέλος, ορίζουμε τα αντίμετρα που μπορούν να μετριάσουν τις απειλές αυτές. Κατά τη διάρκεια αυτής της διαδικασίας, εισάγουμε αξίες, κόστη (ετήσια), ποσοστά καταστροφής από την απειλή για το asset, συχνότητα εμφάνισης της απειλής και για το συγκεκριμένο asset συνδέουμε τις αδυναμίες με τις απειλές και τα αντίμετρα.

Asset

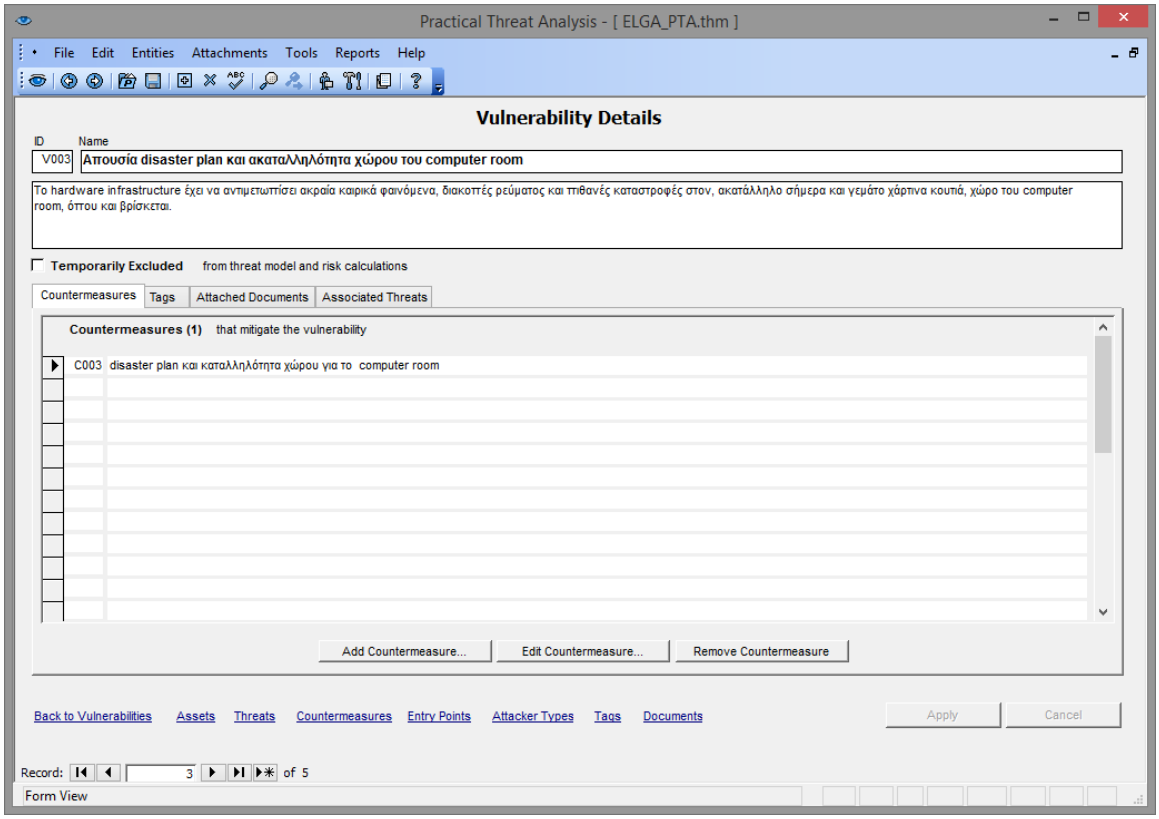
Το critical asset για τον οργανισμό του ΕΛΓΑ είναι τα δεδομένα ασφαλιστικών διαδικασιών. Αυτά αποτελούν το 100% των περιουσιακών στοιχείων πληροφορίας, απαιτούν ένα ετήσιο κόστος συντήρησης 150.000€ και η αξία τους υπολογίζεται στα 10.000.000€ σε περίπτωση ολικής απώλειας. Τέλος, συνδέονται με όλες τις απειλές που θα αναφέρουμε παρακάτω.



Εικόνα 7:Screenshot από τη διαδικασία εκχώρησης στοιχείων για το critical asset

Αδυναμίες

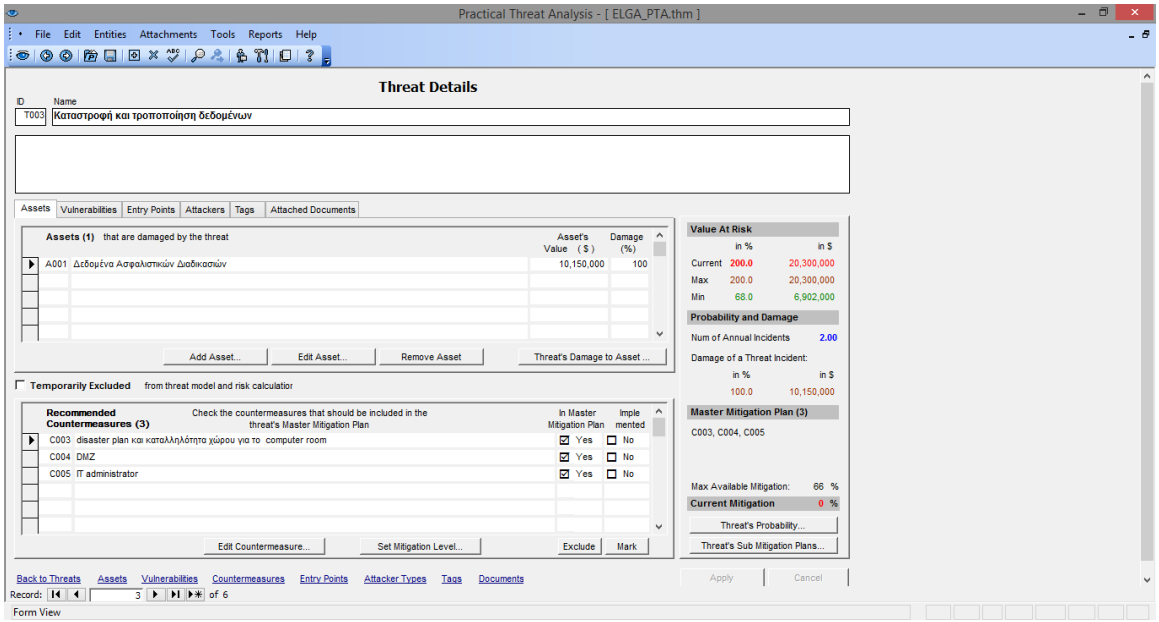
Ανιχνεύθηκαν 5 σημαντικές αδυναμίες που αφορούσαν τις ηλεκτρονικές υπηρεσίες, την φθορά και την παλαιότητα του hardware infrastructure, την απουσία disaster plan και την ακαταλληλότητα του χώρου στο computer room, την απευθείας πρόσβαση στους servers, και την απουσία του IT τμήματος. Έγινε αναλυτική περιγραφή και συνδέθηκε η καθεμία μία με τα αντίστοιχο αντίμετρα που ορίσαμε στο τελευταίο βήμα.



Εικόνα 8:Screenshot από τη διαδικασία εκχώρησης στοιχείων για τις αδυναμίες

Απειλές

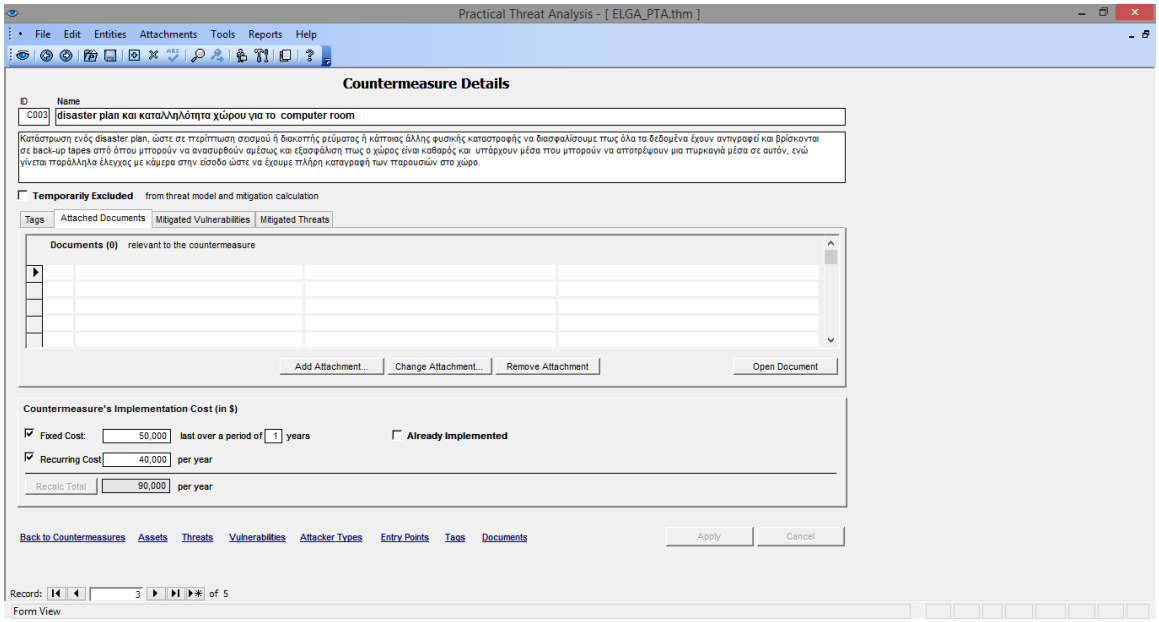
Αναγνωρίστηκαν απειλές που μπορούν να εκμεταλλευτούν τις παραπάνω αδυναμίες, όπως προσωρινή αδυναμία προσπέλασης στοιχείων και καθυστέρηση με medium damage (50%) και υψηλή πιθανότητα εμφάνισης, καταστροφή και τροποποίηση δεδομένων με ultimate damage (100%) και δύο περιστατικά το χρόνο, καταστροφές στον κρίσιμο όροφο του computer room με very high damage (80%) και έως ένα παρόμοιο περιστατικό ανά έτος, καθώς και πρόστιμα λόγω αποκάλυψης στοιχείων και συνδέθηκαν με τις αδυναμίες που αναφέρθηκαν παραπάνω. Όπως είναι εμφανές σε αυτό το κομμάτι του λογισμικού, εισάγαμε την πιθανότητα εμφάνισης της απειλής (πόσες φορές εμφανίστηκε στο έτος), καθώς και το ποσοστό της καταστροφής που θα έχει πάνω στο asset εάν πραγματοποιηθεί η απειλή. Με αυτό τον τρόπο εξάγεται από το πρόγραμμα και το value at risk. Τέλος, συνδέσαμε τις απειλές με τα αντίστοιχα αντίμετρα που προτίνονται.



Εικόνα 9:Screenshot από την εισαγωγή απειλών και τη διασύνδεσή τους με τα αντίμετρα

Αντίμετρα

Αφού αναγνωρίστηκαν οι απειλές και οι αδυναμίες, καταγράψαμε και τα αντίμετρα που μετριάζουν τις απειλές, ορίζοντας το κόστος επισκευής (fixed cost) και το ετήσιο κόστος συντήρησης (recurring cost).



Εικόνα 10:Screenshot από την εισαγωγή αντιμέτρων και του κόστους αυτών

Αποτελέσματα

Έχοντας περιγράψει αναλυτικά και συνδέσει μεταξύ τους. το critical asset, τις αδυναμίες του οργανισμού, τις απειλές που μπορούν να εκμεταλλευτούν αυτές τις αδυναμίες και τα αντίμετρα που συστήνονται να εφαρμοστούν, το λογισμικό μας αποδίδει τα παρακάτω αποτελέσματα.

Εικόνα 11:Screenshot με τα αποτελέσματα του PTA για τον ΕΛΓΑ

Το πρόγραμμα, έχοντας ενσωματώσει τα οικονομικά μεγέθη και το ρίσκο κάθε απειλής, θεωρεί την απειλή ενός threat intruder πολύ σημαντική με το value at risk να ανέρχεται στα 80.000.000 € και την προσωρινή αδυναμία προσπέλασης στοιχείων και τις καθυστερήσεις να θεωρείται εξίσου υψηλής σημασίας με 40.000.000 € value at risk. Οι παραπάνω παρατηρήσεις μας οδηγούν στην πρόταση εφαρμογής των αντιμέτρων που έχουμε ορίσει για τις απειλές αυτές. Συγκεκριμένα, η ανάθεση, από την διοίκηση σε εξωτερικούς συνεργάτες, του monitoring των IDS (intrusion detection system)/IPS (intrusion protection system) συσκευών, της διαχείρισης των logs και της μέριμνας για τα system updates και τις ανανεώσεις των αδειών των antivirus θα ελαχιστοποιούσε την πιθανότητα να πραγματοποιηθούν οι παραπάνω απειλές.

ΚΕΦΑΛΑΙΟ 5 Σύγκριση αποτελεσμάτων των μεθοδολογιών και συμπεράσματα

5.1 Σύγκριση

Κάθε μια από τις δύο μεθοδολογίες έχει διαφορετική προσέγγιση όσον αφορά στην ασφάλεια της πληροφορίας.

Στην octave allegro δίνεται μεγάλη βάση στο κρίσιμο περιουσιακό στοιχείο και μέσα από την ανάλυση αυτού αναγνωρίζονται οι σημαντικές απειλές και αδυναμίες. Σύμφωνα με τις προτεραιότητες που έχουν τεθεί αποφασίζεται αν θα μετριαστεί ο κίνδυνος, και σε περίπτωση αδυναμίας υψηλού σκορ που αντιμετωπίζεται με μετριασμό, προτείνεται το κατάλληλο αντίμετρο.

Από την άλλη πλευρά, η μέθοδος PTA που υποστηρίζεται από λογισμικό δίνει μεγάλη βάση σε θέματα κόστους, περιμένει έτοιμα ποσοτικά στοιχεία για απειλές, αδυναμίες και αντίμετρα και θεωρεί δεδομένο πως όλα αυτά έχουν αναγνωριστεί σε προηγούμενες διαδικασίες. Μέσω αυτής της μεθόδου, έχουμε αποτελέσματα που εμπεριέχουν κόστος και μας δείχνουν το value at risk κάθε απειλής, οπότε σύμφωνα με την πολιτική του εκάστοτε οργανισμού και τα οικονομικά του μεγέθη αποφασίζεται στο τέλος αν θα γίνει ο μετριασμός, βήμα που δεν φαίνεται στο λογισμικό.

Στην εφαρμογή που κάναμε, οι αδυναμίες που εισαγάγαμε στην octave allegro προκρίθηκαν όλες για μετριασμό σύμφωνα με τις προτεραιότητες που αρχικά θέσαμε, ενώ στο PTA εμφανίστηκε το value at risk κάθε απειλής και θα μετριαστούν μόνον αυτές που ξεπερνούν το κατώφλι ελάχιστης αξίας.

Γενικότερα, η octave allegro προτείνεται για οργανισμούς που δεν έχουν ξανακάνει αξιολόγηση των συστημάτων τους και τα συστήματα αυτά να έχουν λίγα άλλα σοβαρά προβλήματα που πρέπει να αναγνωριστούν και αναλόγως να μετριαστούν με μοναδικό μειονέκτημα την χρήση πολλών φύλλων εργασίας. Το PTA, από την άλλη, χρειάζεται έτοιμα κάποια δεδομένα από τον οργανισμό, προϋποθέτει να έχει γίνει αναγνώριση των προβλημάτων και δίνει τελικώς το κοστολόγιο της λύσης.

5.2 Συμπεράσματα

Λόγω της ευαίσθητης πληροφορίας που εμπεριέχεται στα πληροφοριακά συστήματα και του μεγέθους των οργανισμών απαιτείται μια μεθοδευμένη διαχείριση κινδύνου που πρέπει να αναπτυχθεί εντός των οργανισμών. Άτομα με εξιδεικευμένες γνώσεις σε τεχνικά ζητήματα, καθώς και άνθρωποι του οργανισμού θα πρέπει να απασχολούνται εξ' ολοκλήρου με την διαχείριση αυτών των κινδύνων αφού είναι απειλές ύψιστης σημασίας για τον εκάστοτε οργανισμό.

Όσον αφορά στις μεθοδολογίες, μεταξύ των πολλών εκδόσεων της octave επιλέχθηκε η allegro, καθώς κάνει πληροφοριοκεντρική εκτίμηση του κινδύνου. Όταν τα περιουσιακά στοιχεία που σχετίζονται με την πληροφορία είναι στο επίκεντρο της αξιολόγησης της ασφάλειας των πληροφοριών, όλα τα άλλα περιουσιακά στοιχεία μπορούν εύκολα να συμμετέχουν στη διαδικασία ως μέρη όπου τα περιουσιακά στοιχεία με την πληροφορία αποθηκεύονται, μεταφέρονται, ή υποβάλλονται σε επεξεργασία. Ένα τέτοιο μέρος μπορεί να είναι ένα πρόσωπο (δεδομένου ότι οι άνθρωποι μπορούν να αποθηκεύουν πληροφορίες, όπως η γνώση, μεταφορά πληροφοριών από την επικοινωνία, ή τη διαδικασία σκέψης και δράσης), ένα αντικείμενο (π.χ. ένα κομμάτι χαρτί), ή μια τεχνολογία (π.χ. ένα database). Έτσι, οι απειλές για τα περιουσιακά στοιχεία πληροφοριών προσδιορίζονται και εξετάζονται μέσα από την εξέταση του 'τόπου κατοικίας' τους, η οποία περιορίζει ουσιαστικά τον αριθμό και το είδος των περιουσιακών στοιχείων που συμμετέχουν στη διαδικασία. Επιπλέον, εστιάζοντας σε συγκεκριμένα περιουσιακά στοιχεία περιορίζονται αποτελεσματικά οι πληροφορίες που πρέπει να συγκεντρωθούν, επεξεργαστούν, οργανωθούν, αναλυθούν και κατανοηθούν για να εκτελεστεί μια αξιολόγηση του κινδύνου.

Εφαρμόζοντας την allegro, καταλήξαμε σε πρόταση για μετριασμό όλων των προβλημάτων με βάση τις ανάγκες του οργανισμού που τέθηκαν αρχικά. Παρόλα αυτά, πρέπει να σημειωθεί πως γίνεται διαφορετική προσέγγιση ρίσκου στα προβλήματα ανάλογα με τις διαφορετικές ιεραρχήσεις στην μέθοδο της allegro.

Εφαρμόζοντας το PTA δεν έχουμε συγκεκριμένη πρόταση για μετριασμό ή οχί, αλλά εικόνα για την σημασία της απειλής, σημασία που θα κριθεί από τον οργανισμό και τον εκάστοτε manager. Συνεπώς το PTA δεν προτείνει αλλά παρουσιάζει ολοκληρωμένα την εικόνα των απειλών και αφήνει την πρόταση όπως και την απόφαση για βελτίωση ή μετριασμό στον οργανισμό.

Ένας συνδυασμός αυτών των δύο μεθοδολογιών, δηλαδή, αναγνώριση των σοβαρών κινδύνων μέσα από την προσέγγιση που κάνει στο κρίσιμο στοιχείο η allegro και μία κοστολογημένη λύση αυτών των κινδύνων που μας δίνει το PTA αποτελεί μία ιδανική αξιολόγηση ρίσκου για πολλούς οργανισμούς.

5.3 Προοπτικές

Με δεδομένα τα πολλά φύλλα της allegro το να εφαρμόσουμε τη μέθοδο για οργανισμούς μεγαλύτερου μεγέθους από τον ΕΛΓΑ και δεδομένης της έλλειψη πρότασης μετριασμού από την πλευρά του PTA, θα προτείναμε να γίνει μία επέκταση του ήδη υπάρχοντος λογισμικού.

Το νέο λογισμικό θα πρέπει να ενσωματώνει καλύτερα την τοποθεσία της πληροφορίας, να είναι δηλαδή πιο έξυπνο και να μπορεί να αναγνωρίζει προβλήματα μέσα από αυτό το βήμα, κάτι το οποίο κάνει η allegro. Επιπλέον θα πρέπει να λαμβάνει υπόψιν τους τομείς ενδιαφέροντος του οργανισμού και όχι μόνο οικονομικά στοιχεία, τομείς όπως φήμη και εμπιστοσύνη, υγεία κλπ. και να ενσωματώνει την σημασία αυτών στην απειλή πριν δώσει σαν αποτέλεσμα το value at risk.

Τέλος, θα πρέπει να μπορεί να τεθεί κατώφλι βελτίωσης όσον αφορά στο value at risk κάθε απειλής και να εμφανίζεται στο τέλος, όπου δίνεται το κοστολόγιο της λύσης. και να δικαιολογείται ποια απειλή πρέπει να μετριαστεί και ποια όχι με βάση το κατώφλι.

Ανακεφαλαιώνοντας, προτείνεται δηλαδή μία βελτιωμένη έκδοση του PTA με εισαγωγή κατωφλίου και ενσωμάτωση των σημαντικών βημάτων της allegro, των οποίων υπολείπεται, έτσι ώστε να αποτελεί ιδανική λύση για οργανισμούς μεγαλύτερου μεγέθους και συνθετότερων προβλημάτων σε σχέση με την εφαρμογή μας.

ΠΑΡΑΡΤΗΜΑ

OCTAVE Allegro Worksheets

Allegro Worksheet 1	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ– ΦΗΜΗ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
ΦΗΜΗ	Η φήμη επηρεάζεται ελάχιστα, οπότε ελάχιστη ή καθόλου προσπάθεια και μηδαμινά έξοδα απαιτούνται για να επιδιορθώσουμε το πρόβλημα.	Η φήμη έχει καταστραφεί και απαιτείται μεγάλη προσπάθεια για να την επαναφέρουμε στα προηγούμενα επίπεδα.	Η φήμη έχει καταστραφεί ανεπανόρθωτα.
ΑΠΩΛΕΙΑ ΠΕΛΑΤΩΝ	Λιγότερο από_____% μείωση στους πελάτες λόγω απώλειας εμπιστοσύνης	_____μέχρι _____% μείωση στους πελάτες λόγω απώλειας εμπιστοσύνης	Περισσότερο από _____% μείωση στους πελάτες λόγω απώλειας εμπιστοσύνης

Allegro Worksheet 2	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ – ΟΙΚΟΝΟΜΙΚΑ**		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
Λειτουργικά Κόστη	Αύξηση λιγότερη από _____% στα ετήσια λειτουργικά κόστη	Αύξηση λιγότερη στα ετήσια λειτουργικά κόστη από _____μέχρι _____%.	Τα ετήσια λειτουργικά κόστη αυξήθηκαν περισσότερο από_____%.
Απώλεια εσόδων	Λιγότερο από _____% ετήσια απώλεια εσόδων	_____ μέχρι _____% ετήσια απώλεια εσόδων	Περισσότερο από _____% ετήσια απώλεια εσόδων
Στιγμιαία οικονομική απώλεια	Στιγμιαία οικονομική απώλεια λιγότερο από _____	Στιγμιαία οικονομική απώλεια από_____ μέχρι _____	Στιγμιαία οικονομική απώλεια μεγαλύτερη από _____

Allegro Worksheet 3	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ – ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ**		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
Ώρες Προσωπικού	Οι ώρες προσωπικού αυξήθηκαν λιγότερο από _____% για _____μέχρι _____ μέρα/ες.	Οι ώρες προσωπικού αυξήθηκαν από _____% μέχρι _____% για _____ μέχρι _____ μέρα/ες.	Οι ώρες προσωπικού αυξήθηκαν περισσότερο από _____% για _____μέχρι _____ μέρα/ες.
Άλλα			
Άλλα			
Άλλα			

Allegro Worksheet 4	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ – ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ**		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
Ζωή	Καμία απώλεια ή σημαντική απειλή στις ζωές των πελατών ή των μελών του προσωπικού	Οι ζωές των πελατών ή των μελών του προσωπικού απειλούνται, αλλά μπορούν να συνέλθουν μετά από ιατρική βοήθεια	Απώλεια ζωής πελάτη ή μέλους του προσωπικού
Υγεία	Ελάχιστα και άμεσα θεραπεύσιμα τραύματα στην υγεία των πελατών ή των μελών του προσωπικού	Προσωρινή δυσλειτουργία στην υγεία των πελατών ή των μελών του προσωπικού	Μόνιμη δυσλειτουργία στην υγεία των πελατών ή των μελών του προσωπικού
Ασφάλεια	Η ασφάλεια αμφισβητείται	Η ασφάλεια επηρεάζεται	Η ασφάλεια παραβιάζεται
Άλλα			

Allegro Worksheet 5	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ–ΠΡΟΣΤΙΜΑ ΚΑΙ ΝΟΜΙΚΕΣ ΚΥΡΩΣΕΙΣ**		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**
Πρόστιμα	Πρόστιμα λιγότερα από _____ επιβάλονται.	Πρόστιμα από _____ μέχρι _____ επιβάλονται.	Πρόστιμα περισσότερα από _____ επιβάλονται.
Αγωγές	Αγωγές λιγότερες των _____ εκδικάζονται εναντίον του οργανισμού.	Αγωγές μεταξύ _____ και _____ εκδικάζονται εναντίον του οργανισμού.	Αγωγές υψηλότερες των _____ εκδικάζονται εναντίον του οργανισμού.
Έρευνες	Κανένα ερώτημα από την κυβέρνηση ούτε από άλλους ερευνητικούς οργανισμούς.	Η κυβέρνηση και άλλοι ερευνητικούς οργανισμοί ζητούν λίγες πληροφορίες.	Η κυβέρνηση και άλλοι ερευνητικούς οργανισμοί κάνουν σε βάθος έρευνα.
Άλλα::			

Allegro Worksheet 6	ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΡΙΣΚΟΥ–<Καθορισμένο από τον χρήστη>		
ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΕΡΙΟΧΗ	**ΧΑΜΗΛΕΣ**	**ΜΕΤΡΙΕΣ**	**ΥΨΗΛΕΣ**

Allegro Worksheet 7	Ιεράρχηση των τομέων που πλήττονται
ΠΡΟΤΕΡΑΙΟΤΗΤΑ	Τομείς που πλήττονται
	ΦΗΜΗ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ
	ΟΙΚΟΝΟΜΙΚΑ
	ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ
	ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ
	ΠΡΟΣΤΙΜΑ ΚΑΙ ΝΟΜΙΚΕΣ ΚΥΡΩΣΕΙΣ
	<Καθορισμένο από τον χρήστη>

Allegro Worksheet 8	**Προφίλ κρίσιμου στοιχείου πληροφορίας**	
(1) Κρίσιμο Στοιχείο *Ποιο είναι το κρίσιμο στοιχείο?*	**(2) Αιτιολόγηση της επιλογής** *Γιατί είναι σημαντικό για τον οργανισμό αυτό το στοιχείο πληροφορίας?*	**(3) Περιγραφή** *Ποια είναι η προσυμφωνημένη περιγραφή αυτού του στοιχείου πληροφορίας?*
(4) Ιδιοκτήτης(ες) *Σε ποιον ανήκει αυτό το στοιχείο πληροφορίας?*		
(5) Απαιτήσεις Ασφάλειας *Ποιες είναι οι απαιτήσεις ασφάλειας για αυτό το στοιχείο πληροφορίας?*		
❑ **Εμπιστευτικότητα**	Μόνο εξουσιοδοτημένο προσωπικό μπορεί να δείτε τις πληροφορίες αυτού του στοιχείου, όπως:	
❑ **Ακεραιότητα**	Μόνο εξουσιοδοτημένο προσωπικό μπορεί να τροποποιήσει τις πληροφορίες αυτού του στοιχείου, όπως:	
❑ **Διαθεσιμότητα**	Αυτό το στοιχείο πληροφορίας πρέπει να είναι διαθέσιμο στα μέλη του προσωπικού που φαίνονται δίπλα, ώστε να κάνουν σωστά τη δουλεία τους	
	Αυτό το στοιχείο πληροφορίας πρέπει να είναι διαθέσιμο για _____ώρες, _____ μέρες/εβδομάδα, _____εβδομάδες/χρόνο.	
❑ **Άλλα**	Αυτό το στοιχείο πληροφορίας έχει ειδικές κανονιστικές απαιτήσεις προστασίας συμμόρφωσης, ως εξής:	
(6) Η πιο σημαντική απαίτηση ασφάλειας *Ποια είναι η πιο σημαντική απαίτηση ασφάλειας για αυτό το στοιχείο πληροφορίας?*		
• **Εμπιστευτικότητα**	❑ **Ακεραιότητα**	❑ **Διαθεσιμότητα** ❑ **Άλλα**

Allegro Worksheet 9a	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΤΟΥ ΣΤΟΙΧΕΙΟΥ ΠΛΗΡΟΦΟΡΙΑΣ (ΦΥΣΙΚΟ)	
ΕΣΩΤΕΡΙΚΟ		
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία		**ΙΔΙΟΚΤΗΤΗΣ ΤΟΠΟΘΕΣΙΑΣ**
1.		
2.		
3.		
4.		
ΕΞΩΤΕΡΙΚΟ		
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία		**Ιδιοκτήτης Τοποθεσίας**
1.		
2.		
3.		
4.		

Allegro Worksheet 9b	ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΤΟΥ ΣΤΟΙΧΕΙΟΥ ΠΛΗΡΟΦΟΡΙΑΣ (ΤΕΧΝΙΚΟ)	
ΕΣΩΤΕΡΙΚΟ		
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία		**ΙΔΙΟΚΤΗΤΗΣ ΤΟΠΟΘΕΣΙΑΣ**
1.		
2.		
3.		
4.		
ΕΞΩΤΕΡΙΚΟ		
Περιγραφή της τοποθεσίας στην οποία φιλοξενείται η πληροφορία		**Ιδιοκτήτης Τοποθεσίας**
1.		
2.		
3.		
4.		

Allegro Worksheet 9c	Χαρτογράφηση περιβάλλοντος του στοιχείου πληροφορίας (Ανθρώπινο Δυναμικό)
Εσωτερικό Ανθρώπινο Δυναμικό	
Όνομα και ρόλος/ευθύνες	**ΤΜΗΜΑ Η ΜΟΝΑΔΑ**
1.	
2.	
3.	
4.	
Εξωτερικό Ανθρώπινο Δυναμικό	
Ανάδοχος, Πωλητής, κ.λπ.	**Οργανισμός**
1.	
2.	
3.	
4.	

Allegro - Worksheet 10		Κίνδυνοι για το στοιχείο πληροφορίας			
Κίνδυνοι για το στοιχείο πληροφορίας	**Απειλές**	Στοιχείο Πληροφορίας			
		Περιοχή ανησυχίας (αδυναμία)			
		(1) Δράστης *Ποιος θα μπορούσε να εκμεταλλευτεί αυτή την αδυναμία?*			
		(2) Μέσα *Πως θα μπορούσε να το κάνει αυτό ο δράστης?*			
		(3)Κίνητρο *Για ποιο λόγο θα το έκανε αυτό ο δράστης?*			
		(4)Αποτέλεσμα *Ποιο θα ήταν το αποτέλεσμα της ενέργειας του δράστη στο στοιχείο πληροφορίας?*	❑ **Αποκάλυψη** ❑ **Τροποποίηση**	❑ **Καταστροφή** ❑ **Ενόχληση**	
		(5) Απαιτήσεις Ασφάλειας *Πώς παραβιάστηκαν οι συνθήκες ασφαλείας?*			
		(6) Πιθανότητα *Ποια είναι η πιθανότητα αυτό το σενάριο-απειλή να πραγματοποιηθεί?*	❑ **Υψηλή**	❑ **Μέτρια**	❑ **Χαμηλή**

	(7) Συνέπειες *Τι* συνέπειες *θα έχει για τον οργανισμό η παραβίαση των συνθηκών ασφάλειας από την συγκεκριμένη απειλή?*	(8)Σοβαρότητα *Πόσο σοβαρές είναι οι συνέπειες σε κάθε θιγόμενη περιοχή?*		
		Περιοχή	**Αξία**	**Σκορ**
		Φήμη και Εμπιστοσύνη Πελατών		
		Οικονομικά		
		Παραγωγικότητα		
		Ασφάλεια και Υγεία		
		Πρόστιμα και Νομικές Κυρώσεις		
		<Καθορισμένη από το χρήστη περιοχή>		
		Σχετικό σκορ ρίσκου		

(9) Μετριασμός Κινδύνου

Βασιζόμενοι στο συνολικό σκορ για αυτό τον κίνδυνο, τι δράση θα πραγματοποιούσατε?

❑ **Αποδοχή**	❑ **Αναβολή**	❑ **Μετριασμό**	❑ **Μεταφορά**

Για κινδύνους που αποφασίσατε να μετριάσετε, εφαρμόστε τα ακόλουθα:

Που θα εφαρμόσετε τους ελέγχους?	*Τι ελέγχους θα εφαρμόσετε και ποιοι κίνδυνοι έχουν γίνει αποδεκτοί?*

Allegro Worksheet 7b	Ιεράρχηση των τομέων που πλήττονται
ΠΡΟΤΕΡΑΙΟΤΗΤΑ	**Τομείς που πλήττονται**
1	**ΦΗΜΗ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗ ΠΕΛΑΤΩΝ**
2	**ΟΙΚΟΝΟΜΙΚΑ**
4	**ΠΑΡΑΓΩΓΙΚΟΤΗΤΑ**
5	**ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ**
3	**ΠΡΟΣΤΙΜΑ ΚΑΙ ΝΟΜΙΚΕΣ ΚΥΡΩΣΕΙΣ**

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. **Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson.** *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* 2007.

2. **Alberts, C., & Dorofee.** *Managing information security risks: The OCTAVE* . Boston : Addison-Wesley, 2003.

3. **Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson.** *Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, 1.0* . Pittsburgh : Software Engineering Institute: Carnegie Mellon University., 1999.

4. **cert.** www.cert.org/octave. [Ηλεκτρονικό]

5. **Alberts, C., Dorofee, A., Stevens, J., & Woody.** *OCTAVE-S implementation* . Pittsburgh : Software Engineering Institute, Carnegie Mellon University, 2005.

6. **Beachboard, J., Cole, A., Mellor, M., Hernandez, S., Aytes, K., & Massad, N.** Improving information security risk analysis practices for small- and medium-sized enterprises: A research agenda. *Issues in Informing Science and Information* . 2008, σσ. 73-85.

7. **Dhillon, G., & Torkzadeh, G.** Value-focused assessment of information system security in organizations. *Information Systems Journal.* 2006, σσ. 293-314.

8. **Curtis, P. D.** OCTAVE Allegro speeds up the risk assessment process. *News at SEI.* [Ηλεκτρονικό] 2008. Retrieved from http://www.sei.cmu.edu/library/abstracts/news-at-sei/01feature200705.cfm .

9. **Ελληνικός Οργανισμός Γεωργικών Ασφαλίσεων.** [Ηλεκτρονικό] 2014. www.elga.gr.

10. **Technologies, PTA.** [Ηλεκτρονικό] 2005-2008. www.ptatechnologies.com.

11. *Addressing information security risks by adopting standards.* **Al-Ahmad, W., & Mohammad, B.** 2013, International Journal of Information Security Science,.

12. *"Covering Your Assets in Software Engineering"*. **Artin Gilje Jaatun, Inger Anne Tindel.** ARES : s.n., 2008. Seventh International Conference on Availability, Reliability and Security,.

13. **Allen, J. H.** Risk-centered practices. *Build security in.* s.l. : Retrieved from https://buildsecurityin.us-cert.gov/articles/best-practices/deployment-and-operations/risk-centered-practices, 2013.

14. *Information security and privacy in healthcare: Current state of research.* **Appari, A., & Johnson, M. E.** 4, s.l. : International Journal of Internet and Enterprise, 2010, Τόμ. 6.

15. **EDUCAUSE/Internet2 Computer and Network Security Task Force.** Security task force 2008-2009 strategic plan: Safeguarding our IT assets, protecting our community's privacy. [Ηλεκτρονικό] 2008. http://net.educause.edu/ir/library/pdf/CSD5494.pdf.

16. **EDUCAUSE/Internet2 Computer and Higher Education Information Security Council.** Risk management framework, version 2.0. [Ηλεκτρονικό] 2013. https://wiki.internet2.edu/confluence/display/itsg2/Risk+Management+Framework.

17. *AURUM: A framework for information security risk management.* **Ekelhart, A., Fenz, S., & Neubauer, T.** Waikoloa, Big Island, Hawaii. : s.n., 2009. 42nd Hawaii International Conference on System Sciences.

18. **Johnson, E. M., Goetz, E., & Pfleeger, S. L.** Security through information risk management. *IEEE Security and Privacy.* 2009, σσ. 45-52.

19. **Fenz, S., & Ekelhart, A.** Verification, validation, and evaluation in information security risk management. *IEEE Security & Privacy.* 2009, 9, σσ. 58-65.

20. **Keating, C.** Information systems risk assessment. *EDUCAUSE Center for Applied Research.* [Ηλεκτρονικό] 2012. http://www.educause.edu/library/resources/information-systems-risk-assessment.