Πανεπιστήμιο Πειραιώς - Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
« Προηγμένα Συστήματα Πληροφορικής »

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Ταξονομίες Απειλών και Αποτίμηση Κινδύνου Διαδικτυακών Εφαρμογών (Threat Taxonomies and Risk Assessment for Web Applications)
Ονοματεπώνυμο Φοιτήτριας	Δωρή Μαρία-Ελίζα
Πατρώνυμο	Μιχαήλ
Αριθμός Μητρώου	ΜΠΣΠ 16008
Επιβλέπων Καθηγητής	Δουληγέρης Χρήστος

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Χ. Δουληγέρης Καθηγητής	Δρ. Σ. Παπαστεργίου	Π. Κοτζανικολάου Επίκουρος Καθηγητής

Ευχαριστίες

Επιθυμώ να εκφράσω τις ευχαριστίες μου, στους καθηγητές μου κ. Δουληγέρη Χρήστο και στον Δρ. Παπαστεργίου Σπυρίδων, που με βοήθησαν στην εκπόνηση της Μεταπτυχιακής Διατριβής, με τις χρήσιμες επισημάνσεις και παρατηρήσεις τους.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένεια μου που με στήριξε καθ'όλη τη διάρκεια των μεταπτυχιακών μου σπουδών αλλά και στην προσπάθεια ολοκλήρωσης της Μεταπτυχιακής Διατριβής.

Τέλος, θα ήθελα να αφιερώσω τη Μεταπτυχιακή Διατριβή στον πατέρα μου που όσο ζούσε μου έμαθε ότι η διαρκής επιμόρφωση αποτελεί έναν καθοριστικό και καταλυτικό παράγοντα για την πορεία της ζωής και την εξέλιξη του ανθρώπου.

Περιεχόμενα

Περίληψη

Μέσα από την παρούσα διπλωματική εργασία, ο αναγνώστης μπορεί να ενημερωθεί για τις διάφορες ταξονομίες διαδικτυακών και φυσικών απειλών, τις μεθοδολογίες μοντελοποίησης των απειλών καθώς και για τη διαδικασία αποτίμησης κινδύνου των διαδικτυακών εφαρμογών.

Κάθε κεφάλαιο αποτελεί συνέχεια του προηγούμενου και όλα μαζί έχουν ως στόχο να μυήσουν τον αναγνώστη στις μεθοδολογίες και τεχνικές της αποτίμησης κινδύνου (risk assessment).

Πιο συγκεκριμένα, στα κεφάλαια που ακολουθούν:

- ορίζεται η αποτίμηση κινδύνου και αναλύεται η σπουδαιότητά της στη σημερινή εποχή
- πραγματοποιείται ανάλυση των διαφόρων μεθοδολογιών αποτίμησης κινδύνου, των ταξονομιών απειλών αλλά και των μεθόδων μοντελοποίησης απειλών
- γίνεται παρουσίαση της διαδικτυακής εφαρμογής uCMDB και διεξάγεται αποτίμηση κινδύνου για την εφαρμογή αυτή συνδυάζοντας μεθοδολογίες αποτίμησης κινδύνου και εργαλεία μοντελοποίησης απειλών

Κλείνοντας τη διπλωματική εργασία στο τελευταίο κεφάλαιο, παρουσιάζονται κάποια συμπεράσματα που προέκυψαν σχετικά με τη μελέτη των μεθοδολογιών αποτίμησης κινδύνου και μοντελοποίησης απειλών αλλά και τη διεξαγωγή εκτενούς έρευνας της αποτίμησης κινδύνου ως μεθοδολογία.

Abstract

Through this diploma thesis, the reader can be informed about the different taxonomies of cyber and physical threats, the threat modeling process, as well as the risk assessment procedure of web applications.

Each chapter is a continuation of the previous one and they all aim to initiate the reader in risk assessment methodologies and techniques.

More specifically, in the chapters that follow:

- the risk assessment is defined and its significance is analyzed in the current era
- the various risk assessment methodologies, threats taxonomies and threat modeling methods are thoroughly analyzed
- The uCMDB web application is presented and a risk assessment for this application is carried out by combining risk assessment methodologies and threat modeling tools

Concluding the diploma thesis in the last chapter, some conclusions have been drawn regarding the study of the risk assessment and threat modeling methodologies, as well as the conduct of the extensive risk assessment research as a methodology.

Βασικές 'Εννοιες

Αγαθά ή Περιουσιακά Στοιχεία (Assets)	Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία για τον οργανισμό (εκφραζόμενη σε χρηματικούς ή άλλους όρους)
Επίπτωση (Impact)	Η απώλεια μιας αξίας, η αύξηση του κόστους ή κάποια άλλη απώλεια που προκύπτει ως αποτέλεσμα μιας παραβίασης
Απειλή (Threat)	Μια πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσότερων χαρακτηριστικών ασφαλείας ενός πληροφοριακού συστήματος
Αδυναμία (Vulnerability)	Σημείο ενός ΠΣ που μπορεί να επιτρέψει να συμβεί μια παραβίαση
Κίνδυνος/Επικινδυνότητα (Risk)	Πιθανότητα πραγματοποίησης ενός περιστατικού σχετικού με το ΠΣ, που θα λεχει αρνητικές συνέπειες για την ομαλή λειτουργία του οργανισμού
Αποτίμηση Κινδύνου (Risk Assessment)	Η διαδικάσια αποτίμησης της σημαντικότητας των αγαθών ενός ΠΣ, των πιθανών απειλών και των αδυναμιών έναντι των απειλών αυτών με στόχο την εύρεση του επιπέδου επικινδυνότητας. Αποτελεί τη συνολική διαδικασία της ανάλυσης και εκτίμησης κινδύνου
Εμπιστευτικότητα (Confidentiality)	Διασφάλιση της προσπελασιμότητας της πληροφορίας μόνο από όσους έχουν τα απαιραίτητα δικαιώματα
Ακεραιότητα (Integrity)	Διαφύλαξη της πληρότητας και της ακρίβειας της πληροφορίας και των μεθόδων επεξεργασίας της
Διαθεσιμότητα (Availability)	Διασφάλιση της προσπελασιμότητας της πληροφορίας σε εξουσιοδοτημένους χρήστες όποτε απαιτείται
Ασφάλεια Πληροφοριών (Information Security)	Διασφάλιση εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών
Ανάλυση Κινδύνου (Risk Analysis)	Συστηματική χρήση των πληροφοριών για τον εντοπισμό των πηγών και την εκτίμηση του κινδύνου
Εκτίμηση Κινδύνου (Risk Evaluation)	Διαδικασία προσδιορισμού του βαθμού κινδύνου
Διαχείριση Κινδύνου (Risk Management)	Συντονισμένες δραστηρίοτητες για την καθοδήγηση και τον έλεγχο ενός οργανισμού όσον αφορά τον κίνδυνο
Αντιμετώπιση Κινδύνου (Risk Treatment)	Διαδικασία της επιλογής και εφαρμογής των μέτρων για τον περιορισμό του κινδύνου

Πρόλογος-Εισαγωγή

Τα τελευταία χρόνια, ολοένα και περισσότεροι οργανισμοί υφίστανται παραβίαση των πληροφοριακών τους συστημάτων (ΠΣ) με οικονομικές και λειτουργικές επιπτώσεις. Τα ρήγματα ασφαλείας που παρατηρούνται παραμένουν σε μεγάλο βαθμό τα ίδια και χαρακτηρίζονται από έντονη διαχρονικότητα. Ειδικότερα, τα ρήγματα ασφαλείας που οφείλονται σε εξωτερικούς παράγοντες έχουν σχέση με το ιομορφικό λογισμικό, με επιθέσεις άρνησης υπηρεσιών (denial of service attacks) και με επιθέσεις στους εξυπηρετητές Διαδικτύου (Web servers).

Οι μεγαλύτεροι σε μέγεθος οργανισμοί, οι οποίοι δραστηριοποιούνται μέσω του Διαδικτύου, δέχονται με μεγαλύτερη συχνότητα τέτοιου είδους επιθέσεις. Τα ρήγματα ασφαλείας, τυχαία ή όχι, που οφείλονται σε εσωτερικούς παράγοντες και παρουσιάζονται με τη μεγαλύτερη συχνότητα τα τελευταία χρόνια, σχετίζονται με προβλήματα στον έλεγχο πρόσβασης των εξουσιοδοτημένων χρηστών καθώς και με κακή χρήση των υπολογιστικών πόρων. Τα εσωτερικά ρήγματα ασφαλείας εμφανίζουν μια ισχυρή τάση παγίωσης και η κάλυψή τους δεν εξαρτάται μόνο από χρήση συγκεκριμένων τεχνολογιών αλλά έχει και κοινωνικές διαστάσεις, με ισχυρή την επίδραση του ανθρώπινου παράγοντα καθώς και του ευρύτερου κοινωνικο-οικονομικού περιβάλλοντος.

Οι ειδικοί του χώρου συμφωνούν ότι τα προβλήματα που καλούνται να αντιμετωπίσουν είναι διαρκή και πολλές φορές ανυπέρβλητα. Η θεμελίωση μιας κουλτούρας ασφάλειας στο πλαίσιο του οργανισμού που διευκολύνει την επίλυση των προβλημάτων είναι μια επίπονη διαδικασία, η οποία απαιτεί τη συνεχή υποστήριξη της διοίκησης και των τελικών χρηστών, σε συνδυασμό με τη διάθεση των αναγκαίων πόρων.

Υπό το πρίσμα των διαπιστώσεων των μελετών της τελευταίας πενταετίας, οι οποίες εστιάστηκαν σε μέγιστο βαθμό σε τεχνολογικά αναπτυγμένες χώρες (ΗΠΑ, Ηνωμένο Βασίλειο), εκτιμάται ότι τα κυριότερα ζητήματα και οι σημαντικότερες προκλήσεις που έχουν να αντιμετωπίσουν οι οργανισμοί σε θέματα ασφαλείας είναι τα εξής:

- Διασφάλιση επαρκούς επιπέδου ιδιωτικότητας και ασφάλειας ειδικά σε ΠΣ εστιασμένα στον παγκόσμιο ιστό (web-enabled).
- Διασφάλιση των απαραίτητων πόρων που πρέπει να δαπανηθούν σε τεχνολογίες, προϊόντα και υπηρεσίες ασφάλειας για τη μείωση της επικινδυνότητας (risk mitigation).
- Συστηματική προώθηση της κατάρτισης (training) και ενημέρωσης (awareness) των χρηστών σε θέματα ασφάλειας.
- Μεθοδική αντιμετώπιση περιστατικών ασφάλειας μέσω εκπόνησης σχεδίων συνέχισης λειτουργίας (continuity plans) και ανάκαμψης από καταστροφή (disaster recovery plan).

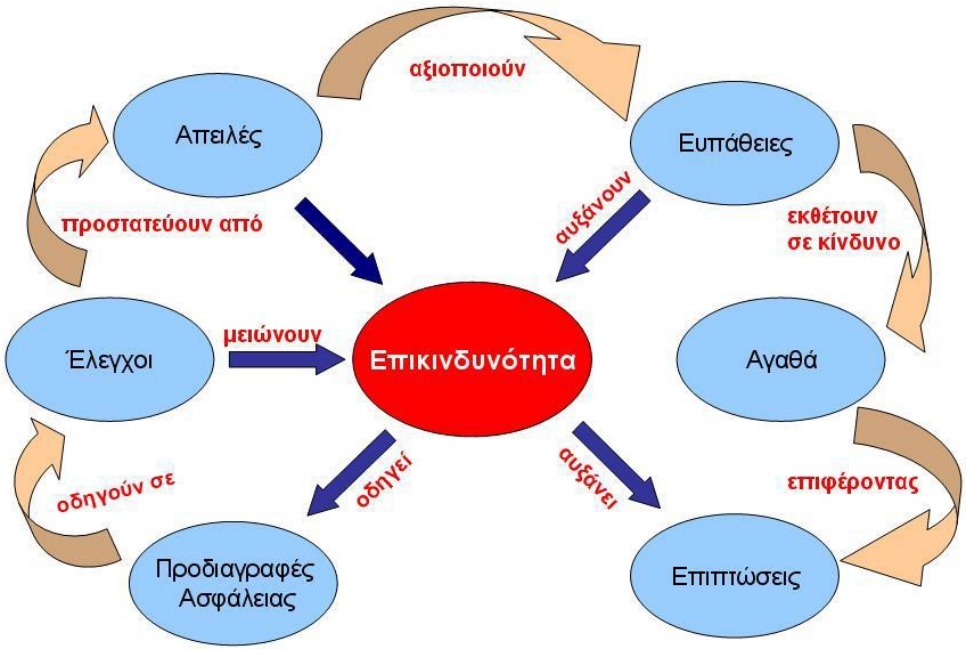
Οι απαντήσεις στις παραπάνω προκλήσεις δεν είναι απλές και εξαρτώνται από το εκάστοτε λειτουργικό περιβάλλον. Οι οργανισμοί πρέπει να ασχοληθούν συστηματικά και εμπεριστατωμένα με θέματα ασφάλειας, σε συνδυασμό με την επιχειρηματική τους στρατηγική και στόχευση. Πρέπει να προσδιορίσουν τα κρίσιμα ζητήματα ασφάλειας, να υιοθετήσουν τεχνολογίες και υπηρεσίες επαρκούς ασφάλειας και να υλοποιήσουν μια σαφή στρατηγική ασφάλειας την οποία θα υποστηρίζουν οι άμεσα εμπλεκόμενοι δικαιούχοι (stakeholders), συμπεριλαμβανομένων της διοίκησης, των εργαζομένων και των προμηθευτών.

1 ΚΕΦΑΛΑΙΟ 1: Ορισμός και ανάλυση της Αποτίμησης Κινδύνου

1.1 Τι είναι η Αποτίμηση Κινδύνου

Ερευνητικά, η ενσωμάτωση των ζητημάτων ασφαλείας στη διαδικασία ανάπτυξης των πληροφοριακών συστημάτων φαίνεται ότι πέρασε χρονικά από τρεις διαδοχικές φάσεις. Η πρώτη φάση περιλάμβανε εμπειρικές μεθόδους και μέσα προστασίας που καθορίζονταν ad hoc (π.χ. checklists). Στη δεύτερη φάση, η συσσωρευμένη γνώση για το πεδίο και η αυξανόμενη απαίτηση για την εξασφάλιση τω ΠΣ οδήγησε στη χρήση αυτοματοποιημένων πρακτικών και εργαλείων για την αποτίμηση του κινδύνου του ΠΣ και τον εντοπισμό επαρκών αντιμέτρων. Μερικές διαδεδομένες πρακτικές ασφάλειας ΠΣ είναι τα πρότυπα Ασφάλειας, η αποτίμηση κινδύνου και οι ολοκληρωμένες πρακτικές (ενσωμάτωση απαιτήσεων ασφάλειας).

Πιο συγκεκριμένα, η αποτίμηση κινδύνου περιλαμβάνει σειρά μεθόδων που στηρίζονται στη συνεργατική αποτίμηση παραμέτρων που αφορούν ένα ΠΣ. Οι παράμετροι περιλαμβάνουν απειλές (threats), ευπάθειες-αδυναμίες (vulnerabilities), συνέπειες, επιπτώσεις και ως συνάρτηση αυτών την κεντρική έννοια του κινδύνου (risk). Αποτέλεσμα της αποτίμησης του κινδύνου είναι η επιλογή των μέτρων ασφάλειας (τεχνικών, οργανωτικών, κλπ.) που είναι αναγκαία για την επαρκή προστασία ενός ΠΣ. Τα μέτρα ασφαλείας επιλέγονται από μια προ υπάρχουσα βάση που περιλαμβάνει ένα ευρύ σύνολο από αυτά. Για τη διεξαγωγή της αποτίμησης κινδύνου χρησιμοποιούνται συνήθως κατάλληλα εργαλεία λογισμικού, τα οποία διεκπεραιώνουν τους ενδιάμεσους ποσοτικούς υπολογισμούς.



Σχήμα 1: Ανάλυση Επικινδυνότητας

Σε μια τυπική διαδικασία αποτίμησης κινδύνου, θα πρέπει να αναπτυχθεί ένα σχέδιο προγράμματος το οποίο προσδιορίζει τι θα λάβει χώρα σε κάθε στάδιο της διαδικασίας, τις προγραμματισμένες ημερομηνίες για κάθε δραστηριότητα και τους απαιτούμενους πόρους.

Πιο αναλυτικά, η αποτίμηση του κινδύνου είναι ο προσδιορισμός της ποσοτικής ή ποιοτικής εκτίμησης του κινδύνου που σχετίζεται με μια σαφώς καθορισμένη κατάσταση και μια αναγνωρισμένη απειλή. Η ποσοτική αποτίμηση κινδύνου απαιτεί υπολογισμούς δύο συνιστωσών κινδύνου (R): το μέγεθος της

πιθανής απώλειας (L) και την πιθανότητα (p) ότι θα προκύψει η απώλεια. Ένας αποδεκτός κίνδυνος είναι ένας κίνδυνος που γίνεται κατανοητός και ανεκτός, συνήθως επειδή το κόστος ή η δυσκολία εφαρμογής ενός αποτελεσματικού αντιμέτρου για τη σχετική ευπάθεια υπερβαίνει την προσδοκία απώλειας.

Ο παρακάτω πίνακας παρουσιάζει έναν απλό τρόπο με τον οποίο μπορούμε να μεταβούμε σε αποτίμηση κινδύνου μιας κατάστασης. Παρατηρούμε ότι βασίζεται στον ορισμό του κινδύνου, καθώς οι δύο άξονες έχουν τις μεταβλητές της πιθανότητας του συμβάντος και τη σοβαρότητα των συνεπειών του. Επίσης, ο πίνακας διαφοροποιεί κάθε φορά το συμβάν με τρία βασικά χρώματα, αναδεικνύοντας με τον τρόπο αυτόν το βαθμό του κινδύνου που υπάρχει.

Ακριβέστερα, από το 0-3 ο κίνδυνος είναι χαμηλός και το συμβάν αναφέρεται σε αμελητέα μορφή συνεπειών, καθώς έχει και λίγες πιθανότητες να εμφανιστεί σε συνάρτηση με το χρόνο. Από το 4-14, ο κίνδυνος κινείται σε μέτρια επίπεδα με λίγο σοβαρότερες συνέπειες και περισσότερες στιγμές εμφάνισής του. Τέλος, σε επίπεδο πάνω από 15, οι καταστάσεις σοβαρεύουν γιατί μπορεί να υπάρξουν δυσχερείς συνέπειες, ακόμα και απώλεια ανθρώπινης ζωής.

	LIKELIHOOD					
SEVERITY		**1 Improbable**	**2 Remote**	**3 Possible**	**4 Likely**	**5 Certain**
	1 Negligible	1	2	3	4	5
	2 Minor	2	4	6	8	10
	3 Significant	3	6	9	12	15
	4 Critical	4	8	12	16	20
	5 Catastrophic	5	10	15	20	25

Σχήμα 2: Πίνακας Αποτίμησης Κινδύνου

Για παράδειγμα, αν έχουμε έναν κίνδυνο σε συχνότητα εμφάνισης του 3 και έχουν καταγραφεί από ιστορικά γεγονότα ότι η σοβαρότητα των συνεπειών του είναι επίσης σε βαθμό 3, τότε έχουμε 3*3=9. Άρα, οδηγούμαστε στο επίπεδο του μέτριου κινδύνου και οι συνέπειες είναι αρκετά σοβαρές.

Ερμηνεία παραπάνω πίνακα

Πιθανότητα	**Ποσοστό**	**Ορισμός**
Σχεδόν βέβαιο	> 80%	Αναμένεται να συμβεί στις περισσότερες περιπτώσεις.
Πολύ Πιθανό	51 – 80%	Ενδεχομένως να συμβεί στις περισσότερες περιπτώσεις.
Πιθανό	21 – 50%	Πιθανώς να συμβεί κάποια στιγμή.
Σπάνιο	6 – 20%	Μπορεί να συμβεί σε μερικές περιπτώσεις.
Απίθανο	0 – 5%	Μπορεί να συμβεί μόνο σε εξαιρετικές περιπτώσεις.

Σχήμα 3: Πίνακας Εκτίμησης Πιθανότητας

Συνέπεια	**Ορισμός**
Καταστροφική	Εάν συμβεί θα προκαλέσει καταστροφική συνέπεια – μη ανατρέψιμη ζημιά.
Σοβαρή	Εάν συμβεί θα προκαλέσει σημαντικές επιπτώσεις.
Μέτρια	Εάν συμβεί θα προκαλέσει σοβαρές επιπτώσεις, αλλά όχι τόσο κρίσιμες για τη λειτουργία.
Μικρή	Εάν συμβεί θα προκαλέσει κάποιες επιπτώσεις, αλλά η λειτουργία συνεχίζεται κανονικά.
Αμελητέα	Εάν συμβεί δε θα προκαλέσει επιπτώσεις.

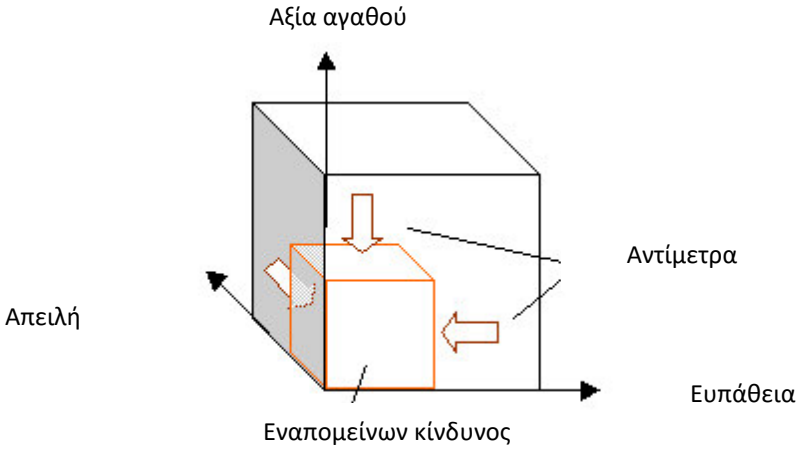
Σχήμα 4: Πίνακας Εκτίμησης Επιπτώσεων

Η αποτίμηση κινδύνου μπορεί να θεωρηθεί ως η δημιουργία ενός στιγμιότυπου των τρέχοντων κινδύνων. Πιο αναλυτικά, αποτελείται από τις ακόλουθες φάσεις:

- Προσδιορισμός απειλών: προσδιορίσμός όλων των σχετικών απειλών
- Χαρακτηρισμός απειλών: καθορισμός του αντίκτυπου και της πιθανότητας των σχετικών απειλών
- Εκτίμηση έκθεσης κινδύνων: προσδιορισμός της ευπάθειας των αγαθών

- Χαρακτηρισμός κινδύνου: καθορισμός των κινδύνων και αξιολόγηση των επιπτώσεών τους στην επιχείρηση

Το παρακάτω σχήμα δείχνει πώς ο κίνδυνος της ασφάλειας των πληροφοριακών συστημάτων μπορεί να θεωρηθεί ως η συνάρτηση της απειλής, της ευπάθειας και της αξίας του αγαθού. Δείχνει επίσης ότι υπάρχουν διάφοροι τρόποι μείωσης των κινδύνων καθώς μπορεί να υπάρξουν αντίμετρα τα οποία να μειώσουν την πιθανότητα μια απειλή να γίνει πραγματικότητα. Τα αντίμετρα αυτά, μπορούν να μειώσουν την ευπάθεια ή να συμβάλλουν στο να μειωθεί η επίπτωση που προκαλείται όταν πραγματοποιηθεί η απειλή.



Σχήμα 5: Κίνδυνος ως συνάρτηση της απειλής, της ευπάθειας και της αξίας του αγαθού

Ο κίνδυνος που εξακολουθεί να υφίστανται μετά την εφαρμογή αντιμέτρων ονομάζεται « εναπομείνων κίνδυνος ». Ο κίνδυνος αυτός πρέπει να είναι λαμβάνεται υπόψη από τη διοίκηση και να γίνεται δεκτός ή να απορρίπτεται (στην τελευταία περίπτωση τέτοιου είδους κίνδυνοι πρέπει να αντιμετωπίζονται ξανά).

1.2 Είδη Αποτίμησης Κινδύνου

Γενικά, υπάρχουν 2 τύποι αποτίμησης κινδύνου, η ποιοτική και η ποσοτική αποτίμηση κινδύνου. Στην ποσοτική αποτίμηση κινδύνου, οι αριθμητικές τιμές (π.χ. νομισματικές αξίες) είναι ανεξάρτητες των διαφορετικών συνιστωσών αξιολόγησης κινδύνου, καθώς και του επίπεδου των πιθανών απωλειών. Όταν όλα τα στοιχεία (αξία του αγαθού, συχνότητα απειλής, αποτελεσματικότητα διασφάλισης, κόστος διασφάλισης, αβεβαιότητα και πιθανότητα) αξιολογούνται ποσοτικά, η διαδικασία θεωρείται ότι είναι πλήρως ποσοτική.

Αντίθετα, η ποιοτική ανάλυση κινδύνου δεν αποδίδει αριθμητικές τιμές στην αποτίμηση κινδύνου των διάφορων συστατικών. Ουσιαστικά, βασίζεται σε σενάρια και οι αξιολογητές / συμμετέχοντες θα μελετήσουν διαφορετικά σενάρια απειλής-ευπάθειας και θα προσπαθήσουν να απαντήσουν σε ερωτήσεις τύπου "τι γίνεται αν". Γενικά, η ποιοτική αποτίμηση κινδύνου τείνει να είναι πιο υποκειμενική σε σχέση με την ποσοτική αποτίμηση.

Ο παρακάτω πίνακας παρουσιάζει τα πλεονεκτήματα και τα μειονεκτήματα της ποιοτικής και ποσοτικής αποτίμησης κινδύνου:

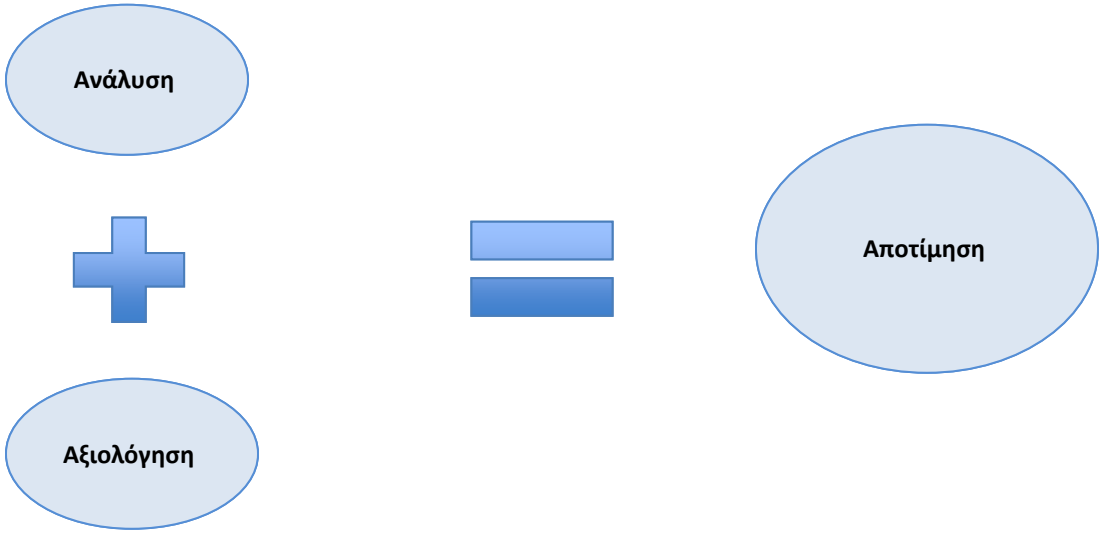
	Πλεονεκτήματα	**Μειονεκτήματα**
Ποσοτική	1. Τα αποτελέσματα βασίζονται σε ανεξάρτητες και αντικειμενικές διαδικασίες και μετρήσεις. 2. Καταβάλλεται μεγάλη προσπάθεια στον προσδιορισμό της αξίας του αγαθού και τη μετρίαση του κινδύνου. 3. Η αξιολόγηση κόστους /οφέλους είναι απαραίτητη και μπορεί να αποδεικνύεται χρήσιμη για τη λήψη αποφάσεων της διοίκησης. 4. Τα αποτελέσματα μπορεί να εκφράζονται σε συγκεκριμένη γλώσσα (π.χ. νομισματική αξία, ποσοστά, πιθανότητες).	1. Οι υπολογισμοί μπορεί να είναι σύνθετοι και χρονοβόροι. 2. Ιστορικά λειτουργεί μόνο καλά με ένα αναγνωρισμένο και αυτοματοποιημένο εργαλείο και σχετικές γνώσεις; έτσι μπορεί να συνεπάγεται υψηλότερο κόστος. 3. Απαιτεί μεγάλες ποσότητες προκαταρκτικής εργασίας για τη συλλογή και την ποσοτικοποίηση των διαφορετικών στοιχείων ανάλυσης κινδύνου. 4. Γενικά δεν παρουσιάζει κανένα επίπεδο προσωπικής συμμετοχής. Οι συμμετέχοντες δεν μπορούν να “προπονηθούν ”εύκολα μέσω της διαδικασίας αυτής.
Ποιοτική	1. Πιο απλή, καθώς δεν υπάρχουν σύνθετοι υπολογισμοί. 2. Δεν είναι απαραίτητο να καθοριστεί η νομισματική αξία των αγαθών, το οποίο μπορεί να είναι αρκετά κουραστικό και σε ορισμένες περιπτώσεις αδύνατο από έναν αξιολογητή. 3. Δεν είναι απαραίτητο να ποσοτικοποιηθεί η συχνότητα απειλών.	1. Είναι υποκειμενική. 2. Τα αποτελέσματα και ποιότητα της αποτίμησης κινδύνου εξαρτάται αποκλειστικά από την εμπειρογνωμοσύνη και ποιότητα της ομάδας διαχείρισης κινδύνου. 3. Η προσπάθεια ανάπτυξης χρηματική αξίας για τα στοχευμένα αγαθά είναι περιορισμένη. 4. Δεν υπάρχει καμία βάση για το κόστος / όφελος της ανάλυσης του μετριασμού του κινδύνου.

	4. Είναι ευκολότερο να εμπλέκεται non-security και non-technical προσωπικό.	

Σχήμα 6: Ποιοτική και Ποσοτική Αποτίμηση κινδύνου

1.3 Βήματα της Αποτίμησης Κινδύνου (Risk Assessment)

Όπως απεικονίζεται και στο παρακάτω σχήμα, η διαδικασία της αποτίμησης του κινδύνου ενός ΠΣ ορίζεται ως το αποτέλεσμα της ανάλυσης του κινδύνου (Risk Analysis) και της αξιολόγησης του κινδύνου (Risk Evaluation).



Σχήμα 7: Αποτίμηση Κινδύνου

Η ανάλυση του κινδύνου περιλαμβάνει την αναγνώριση των κινδύνων και την αποτίμηση της επικινδυνότητας του ΠΣ. Αναλυτικότερα, περιλαμβάνει τα εξής στάδια:

- Προσδιορισμός και αποτίμηση αγαθών (assets)
- Εκτίμηση απειλής (threat)
- Εκτίμηση ευπάθειας (vulnerability)
- Εκτίμηση επιπτώσεων (impact)
- Εκτίμηση υφιστάμενων μέτρων προστασίας (countermeasure)
- Υπολογισμός επικινδυνότητας/κινδύνου (risk)

Η αξιολόγηση του κινδύνου έχει ως στόχο τη δημιουργία ενός καταλόγου με τους υφιστάμενους κινδύνους, σε ιεραρχημένη μορφή και με βάση συγκεκριμένα κριτήρια αξιολόγησης ανά σενάριο-περιστατικό.

Το τελικό στάδιο της διαδικασίας αποτίμησης κινδύνου είναι η αντιμετώπιση του κινδύνου/επικινδυνότητας (Risk Treatment), το οποίο αποτελεί την επιλογή των αντιμέτρων για τον περιορισμό της επικινδυνότητας σε αποδεκτά επίπεδα. Ο στόχος των αντιμέτρων αυτών μπορεί να είναι ένας από τους παρακάτω:

- Μείωση του κινδύνου π.χ. υιοθέτηση νέου αντίμετρου
- Μεταφορά κινδύνου σε τρίτους π.χ. ασφάλιση
- Διατήρηση κινδύνου, η αποδοχή των επιπτώσεων ενός περιστατικού
- Αποφυγή κινδύνου, η απόφαση μη εμπλοκής σε μια κατάσταση που ενέχει κίνδυνο

Τέλος, η αντιμετώπιση του κινδύνου περιλαμβάνει τη σύνταξη και την υλοποίηση του σχεδίου ασφαλείας για τη συνέχιση της λειτουργίας του οργανισμού καθώς και την καταγραφή του εναπομένοντος κινδύνου (εάν αυτός συνεχίζει να υπάρχει) από την ομάδα ασφάλειας του εκάστοτε οργανισμού.

1.4 Οφέλη από την αποτίμηση κινδύνου - Γιατί να διεξάγουμε αποτίμηση κινδύνου;

Μια αποτίμηση κινδύνου στα πληροφοριακά συστήματα ενός οργανισμού δεν μας εξηγεί μόνο την κατάσταση της ασφάλειας της υποδομής των συστημάτων, αλλά μπορεί να διευκολύνει και τη λήψη αποφάσεων σχετικά με την οργανωτική στρατηγική ασφαλείας του οργανισμού. Ορισμένα από τα πλεονεκτήματα της διεξαγωγής αποτίμησης κινδύνου των ΠΣ είναι:

1. **Προσδιορισμός των απειλών και των αδυναμιών**

Η διεξαγωγή μιας αποτίμησης κινδύνου πληροφοριακών συστημάτων μπορεί να βοηθήσει στον εντοπισμό τρωτών σημείων στην υπάρχουσα υποδομή και στις επιχειρησιακές εφαρμογές, πριν τα εκμεταλλευτούν οι κακόβουλοι. Εν συνεχεία, μπορούν να ληφθούν τα κατάλληλα μέτρα για να διορθωθούν αυτές οι ευπάθειες, μειώνοντας τον κίνδυνο και τις πιθανές επιπτώσεις οποιασδήποτε παραβίασης.

2. **Προσδιορισμός του επίπεδο ωριμότητας των υφιστάμενων ελέγχων ασφαλείας και εργαλείων**

Μια αποτίμηση κινδύνου ενός ΠΣ μπορεί να βοηθήσει στην αξιολόγηση των υφιστάμενων ελέγχων ασφαλείας και των προληπτικών ελέγχων που εφαρμόζονται. Οι υπάρχουσες περιοχές βελτίωσης μπορούν στη συνέχεια να χαρτογραφηθούν ενάντια στο σημερινό τεχνολογικό τοπίο για να διαπιστωθεί εάν είναι εφικτές οι βελτιώσεις. Η αξιολόγηση των ΠΣ υπογραμμίζει τα μέτρα αποκατάστασης για τη μεγιστοποίηση των τρεχουσών επενδύσεων.

3. **Βελτίωση των πολιτικών ασφαλείας σε επίπεδο επιχείρησης**

Η αποτίμηση κινδύνου όχι μόνο θα βοηθήσει στην αποκατάσταση τρωτών σημείων στην ασφάλεια των ΠΣ, αλλά, συνδέοντας τον κίνδυνο των πληροφοριακών συστημάτων με τη διαχείριση κινδύνων σε επίπεδο επιχείρησης, μπορεί να συμβάλλει στη δημιουργία ασφαλέστερων λύσεων, πρακτικών και πολιτικών εντός του οργανισμού. Αυτό θα βελτιώσει τη συνολική ασφάλεια των πληροφοριών στον οργανισμό και θα συμβάλλει στον προσδιορισμό της στρατηγικής ασφαλείας που ταιριάζει καλύτερα στον οργανισμό.

4. **Υπολογισμός της ασφάλειας και της ετοιμότητας της ασφάλειας**

Η αποτίμηση κινδύνου ενός ΠΣ απαιτεί τη συμμετοχή διαφόρων στελεχών της ασφάλειας, καθώς και άλλων υπαλλήλων και διευθυντικών στελεχών, που θα βοηθήσουν να υπολογιστεί πόσο ευαισθητοποιημένα είναι τα άτομα και τα τμήματα της ασφάλειας έναντι των απειλών, των τρωτών σημείων, αλλά και των πρακτικών και των λύσεων. Δίνει επίσης ένα μέτρο για το πόσο καλά οι εργαζόμενοι κατανοούν και ακολουθούν την ασφάλεια της επιχείρησης αλλά και τις επιχειρησιακές πολιτικές και τα πρότυπα. Επομένως, μια αποτίμηση κινδύνου ΠΣ μπορεί να υποδηλώνει την ανάγκη για εκστρατείες ευαισθητοποίησης σχετικά με την ασφάλεια των υπαλλήλων ενός οργανισμού.

5. **Δικαιολόγηση των επενδύσεων σε ασφάλεια**

Η επανεξέταση της υπάρχουσας υποδομής πληροφοριακών συστημάτων και η μελέτη του δυνητικού επιχειρηματικού αντίκτυπου ενός συστήματος μπορεί να βοηθήσει στην πραγματοποίηση μιας επιχειρηματικής περίπτωσης για δαπάνες ασφαλείας. Μια αξιολόγηση μπορεί να παρουσιάσει μια δίκαιη ανάλυση των επενδύσεων σε σχέση με τις πιθανές ζημίες και το κόστος από παραβιάσεις της ασφάλειας.

6. **Απόδειξη της δέουσας επιμέλειας ασφάλειας**

Με τους κανονισμούς αξιολόγησης των κινδύνων πληροφορικής που ενδέχεται να τεθούν σε λειτουργία τα επόμενα χρόνια, είναι σημαντικό να έχει ο οργανισμός τεκμηριωμένη απόδειξη της εκτέλεσης αξιολογήσεων σε τακτική βάση. Επιπλέον, αν υπάρχει ασφάλιση που ασχολείται με την απώλεια δεδομένων, οι ασφαλιστικοί οργανισμοί θα απαιτήσουν την απόδειξη ότι έχουν ληφθεί τα κατάλληλα μέτρα ασφάλειας (σε περίπτωση συμβάντος).
Η τεκμηρίωση σχετικά με την αξιολόγηση κινδύνου ΠΣ μπορεί να το αποδείξει αυτό.

7. Κατανόηση της ωριμότητας ασφάλειας των συνεργατών

Μια πρόσφατη μελέτη της PwC διαπίστωσε ότι η μεγαλύτερη πρόκληση για την ασφάλεια σήμερα είναι από το εσωτερικό μιας επιχείρησης (υπάλληλοι και εταίροι) και όχι από εξωτερικές απειλές. Μια αξιόπιστη αποτίμηση κινδύνου ενός ΠΣ περιλαμβάνει την αξιολόγηση των μέτρων ασφάλειας στο δίκτυο συνεργατών του οργανισμού. Μάλιστα, τα ευρήματα από την αξιολόγηση αυτή μπορεί να βοηθήσουν στην καλύτερη άμυνα κατά των επιθέσεων τρίτων.
Ο γενικός στόχος της στρατηγικής ασφάλειας ενός οργανισμού είναι η διασφάλιση της προστασίας της πληροφορίας (είτε της δικής της είτε αυτής των πελατών, των προμηθευτών και άλλων μερών) και των περιουσιακών της στοιχείων. Η αποτίμηση κινδύνου ΠΣ είναι ένα σημαντικό προληπτικό μέτρο που μετριάζει τον κίνδυνο τρωτών σημείων και απειλών που έχουν αρνητικό αντίκτυπο στην επιχείρηση.

1.5 Μειονεκτήματα Αποτίμησης κινδύνου

Όπως όλες οι μεθοδολογίες, έτσι και η αποτίμηση κινδύνου παρουσιάζει και κάποια μειονεκτήματα στην εφαρμογή της. Πιο αναλυτικά:

1. **Απλουστευμένο μοντέλο του ΠΣ**

Η μεθοδολογία αποτίμησης κινδύνου στηρίζεται σε ένα απλουστευμένο μοντέλο του πληροφοριακού συστήματος η οποία δεν λαμβάνει υπόψη της τη δυναμικότητα του ΠΣ αλλά και τη μεταβλητότητα που εισάγει σε αυτό ο ανθρώπινος παράγοντας.

2. **Υποκειμενικότητα στην αποτίμηση των αγαθών και των απειλών**

Η αποτίμηση κινδύνου εμπεριέχει την υποκειμενικότητα στην αποτίμηση των αγαθών καθώς και στην εκτίμηση των απειλών και των ευπαθειών. Αυτό συμβαίνει γιατί η κατάληξη σε ένα σύστημα ασφαλείας επέρχεται μέσω επάλληλων αμοιβαίων συμβιβασμών και μετά από συμφωνία μεταξύ των μερών για το ποιο αγαθό είναι σημαντικό και πόσο σημαντικό για το ΠΣ (asset evaluation), καθώς και για το ποιους κινδύνους υφίσταται το ΠΣ (risk analysis).

3. **Απλουστευμένες μέθοδοι για τον υπολογισμό του κίνδυνου**

Όπως αναφέρθηκε στην ενότητα 1.1, η αποτίμηση κινδύνου βασίζεται σε σχετικά απλές στατιστικές μεθόδους για τον υπολογισμό της πιθανότητας εμφάνισης μιας απειλής και επομένως, για τον υπολογισμό του ενδεχόμενου κινδύνου.

4. **Έλλειψη ανατροφοδότησης των αποτελεσμάτων**

Στη μεθοδολογία αυτή, απουσιάζει η δυνατότητα ανατροφοδότησης των αποτελεσμάτων της εφαρμογής αντιμέτρων καθώς και η υλοποίηση των αντιμέτρων αυτών πραγματοποιείται μετά την ανάπτυξη. Ο οργανισμός που πραγματοποιεί αποτίμηση κινδύνου στα ΠΣ που διαθέτει, δυστυχώς δεν ανατρέχει στα αποτελέσματα της κατά τη διεξαγωγή της ίδιας μεθοδολογίας πάνω σε νέα ΠΣ, προκειμένου να εφαρμόσει διαφορετικά αντίμετρα.

2 ΚΕΦΑΛΑΙΟ 2: Μεθοδολογίες και Πρότυπα Αποτίμησης Κινδύνου

Όπως προκύπτει από τις προηγούμενες ενότητες, η αποτίμηση κινδύνου αποτελεί μια συστηματική διαδικασία, όπου:

- Αποτιμάται και αναλύεται η επικινδυνότητα ενός ΠΣ και ικανοποιούνται οι απαιτήσεις που θέτει το ισχύον θεσμικό πλαίσιο για τα δεδομένα που επεξεργάζεται το ΠΣ.
- Δημιουργείται το σχέδιο ασφάλειας, δηλαδή εντοπίζονται και περιγράφονται τα οργανωτικά και τεχνικά μέτρα που πρέπει να ληφθούν για τη διαχείριση της επικινδυνότητας.
- Εφαρμόζεται και παρακολουθείται το σχέδιο ασφάλειας.

Η λήψη των μέτρων που προσδιορίζονται στο σχέδιο ασφάλειας εξασφαλίζει επαρκές επίπεδο προστασίας, ανάλογο προς τους κινδύνους που αντιμετωπίζει το ΠΣ.

Στο συγκεκριμένο κεφάλαιο παρουσιάζονται και αναλύονται ορισμένες από τις πιο γνωστές μεθοδολογίες αποτίμησης/αξιολόγησης κινδύνου των πληροφοριακών συστημάτων. Αξίζει να σημειωθεί εδώ ότι η επιλογή της καταλληλότερης μεθόδου δεν είναι προφανής. Πιο αναλυτικά:

- Δεν υπάρχει πλήρης και αναλυτικός κατάλογος με τα βασικά χαρακτηριστικά κάθε μεθόδου.
- Δεν υπάρχουν κοινά αποδεκτά κριτήρια αξιολόγησης.
- Τα στάδια της ανάλυσης και διαχείρισης επικινδυνότητας δεν καλύπτονται πλήρως από όλες τις μεθόδους.
- Οι μέθοδοι διαφέρουν ως προς το επίπεδο ανάλυσης του ΠΣ.
- Δεν διατίθενται όλες οι μέθοδοι στην ελεύθερη αγορά.

Παρακάτω παρατίθενται τα χαρακτηριστικά κάθε μεθόδου αποτίμησης κινδύνου καθώς και τα χαρακτηριστικά του οργανισμού που πρέπει να ληφθούν υπόψη για την επιλογή της μεθόδου:

Χαρακτηριστικά Μεθόδου:

1. Κόστος: κόστος αγοράς και εφαρμογής, χρόνος συλλογής δεδομένων, χρόνος εκτίμησης της επικινδυνότητας
2. Απαίτηση για συμφωνία διοίκησης και αναλυτών
3. Ευελιξία: προσαρμογή ως προς τον οργανισμό, προσαρμογή ως προς το ΠΣ, κάλυψη μελλοντικών αλλαγών, επιλογή συνδυασμού αντιμέτρων
4. Πολυπλοκότητα
5. Πληρότητα: ως προς τις τεχνολογικές παραμέτρους του ΠΣ, τις απαιτήσεις ασφάλειας, τις παραμέτρους επικινδυνότητας (απειλές, ευπάθειες, κλπ.)
6. Συνέπεια (ίδια αποτελέσματα για τα ίδια δεδομένα εισόδου)
7. Ευκολία χρήσης
8. Σκοπιμότητα (αρχή κόστους-ωφέλειας)
9. Εγκυρότητα
10. Αξιοπιστία
11. Υποστήριξη από κατάλληλο λογισμικό

Χαρακτηριστικά Οργανισμού:

1. Επίπεδο επικινδυνότητας (π.χ. κρίσιμες υποδομές)
2. Μέγεθος
3. Κουλτούρα ασφάλειας (π.χ. στρατιωτικός οργανισμός)
4. Εξωτερικές απαιτήσεις: νομοθεσία, Ευρωπαϊκές οδηγίες
5. Οργανωτική δομή

Συγκεκριμένα, στις ενότητες που ακολουθούν θα παρουσιαστούν οι παρακάτω μέθοδοι αποτίμησης κινδύνου:

Όνομα	**Δωρεάν Χρήση**	**Μέγεθος Οργανισμού**	**Ανακοίνωση**
ISO 27001		Όλα	2002
CYSM		Μεσαίο, Μεγάλο	2013
ENISA RM & IT Security	X	Μικρό, Μεσαίο	2016
CRAMM		Κυβέρνηση, μεγάλο	1985
Octave	X	Μικρό, Μεσαίο	1999
ISO 27005		Όλα	2002

Σχήμα 8: Μεθοδολογίες Αποτίμησης Κινδύνου

2.1 Πρότυπο ISO/IEC 27001

Το πρότυπο ISO/IEC 27001 "Information Technology – Security techniques – Information security management systems – Requirements" αποτελεί το πιο διαδεδομένο πρότυπο ασφάλειας πληροφοριακών συστημάτων.

Πιο συγκεκριμένα, το διεθνές αυτό πρότυπο στοχεύει στο να παρέχει ένα μοντέλο, δηλαδή μια σειρά απαιτήσεων για την εγκαθίδρυση, την υλοποίηση, την ανασκόπηση, τη διατήρηση και τη βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS). Ο σχεδιασμός και η υλοποίηση του ISMS ενός οργανισμού επηρεάζεται από τις ανάγκες και τους στόχους του οργανισμού, από τις απαιτήσεις ασφάλειας, το πεδίο εφαρμογής, το μέγεθος και τη δομή του οργανισμού.

Οι απαιτήσεις του προτύπου είναι γενικές και μπορούν να εκπληρωθούν από όλους τους οργανισμούς ανεξάρτητα του μεγέθους, της οργανωτικής δομής του αντικειμένου και του τομέα δραστηριοποίησης. Στο σημείο αυτό, πρέπει να επισημανθεί ότι σε κάθε σύστημα υποχρεωτική είναι η κάλυψη των απαιτήσεων των παραγράφων 4-10 ενώ όλα τα περιεχόμενα του Παραρτήματος Α είναι προαιρετικά και εξαρτάται από τη δυνατότητα εφαρμογής στον οργανισμό. Αυτή η εξαίρεση θα πρέπει να καταγράφεται και να αιτιολογείται κατάλληλα. Τέλος, οι όποιες εξαιρέσεις δε θα πρέπει να επηρεάζουν την ικανότητα να παρέχουν ένα επίπεδο ασφάλειας αντίστοιχο με αυτό που έχει προσδιοριστεί στην απότιμηση κινδύνου και πάντα σε συμφωνία με τις ισχύουσες νομικές απαιτήσεις.

Το πρότυπο ISO 27001 βασίζεται στη διαρκής βελτίωση (PDCA cycle) του οργανισμού, δηλαδή τις παρακάτω ενέργειες:

- **Σχεδιασμός (Plan)**: Είναι ο σχεδιασμός της πολιτικής ασφάλειας, των στόχων, των σκοπών, των διεργασιών και των διαδικασιών που είναι σχετικές με τη διαχείριση του κινδύνου και με τη βελτίωση της ασφάλειας προκειμένου να δώσει εκείνα τα αποτελέσματα που ανταποκρίνονται στους στόχους του οργανισμού. Ουσιαστικά, πρόκειται για τις απαιτήσεις/παραγράφους 4, 5 και 6 που θα δούμε παρακάτω.
- **Εκτέλεση (Do)**: Αποτελεί τη δημιουργία της πολιτικής ασφάλειας και την εφαρμογή της καθώς και των μηχανισμών, των διεργασιών και διαδικασιών. Πρόκειται για τις απαιτήσεις/παραγράφους 5, 7 και 8 του προτύπου.
- **Έλεγχος (Check)**: Είναι ο έλεγχος και η μέτρηση όπου αυτά είναι δυνατά της απόδοσης των διεργασιών ως προς την πολιτική ασφάλειας, τους στόχους και την καθημερινή εμπειρία. Τα αποτελέσματα του σταδίου αυτού καταγράφονται και τροφοδοτούνται στην ανασκόπηση από τη Διοίκηση. Αντιστοιχεί στην απαίτηση/παράγραφο 9 του προτύπου.
- **Δράση (Act)**: Είναι η λήψη προληπτικών και διορθωτικών ενεργειών βασισμένων στα αποτελέσματα της ανασκόπησης από τη Διοίκηση, προκειμένου να επιτευχθεί διαρκής βελτίωση. Αντιστοιχεί στην απαίτηση/παράγραφο 10 του προτύπου.

Οι απαιτήσεις (παράγραφοι) του προτύπου στις οποίες πρέπει να συμμορφώνεται ένας οργανισμός είναι οι παρακάτω:

1. **Παράγραφος 4: Context of the organization**
   - **i.** 4.1: Understanding the organization and its context
   - **ii.** 4.2: Understanding the needs and expectations of interested parties
   - **iii.** 4.3: Determining the scope of the information security management system
   - **iv.** 4.4: Information security management system

2. **Παράγραφος 5: Leadership**
   - i. 5.1: Leadership and commitment
   - ii. 5.2: Policy
   - iii. 5.3: Organizational roles, responsibilities and authorities

3. **Παράγραφος 6: Planning**
   i. 6.1: Actions to address risks and opportunities
   ii. 6.2: Information security objectives and planning to achieve them

4. **Παράγραφος 7: Support**
   i. 7.1: Resources
   ii. 7.2: Competence
   iii. 7.3: Awareness
   iv. 7.4: Communication
   v. 7.5: Documented Information

5. **Παράγραφος 8: Operation**
   i. 8.1: Operational planning and control
   ii. 8.2: Information security risk assessment
   iii. 8.3: Information security risk treatment

6. **Παράγραφος 9: Performance evaluation**
   i. 9.1: Monitoring, measurement, analysis and evaluation
   ii. 9.2: Internal audit
   iii. 9.3: Management review

7. **Παράγραφος 10: Improvement**
   i. 10.1: Nonconformity and corrective action
   ii. 10.2: Continual improvement

Από όλα τα παραπάνω, το πρότυπο απαιτεί να υπάρχουν καταγεγραμμένα (ISMS documentation) στον οργανισμό τα εξής:

a. Η πολιτική του ISMS (βλ. 4.2.1b) και οι στόχοι
b. Το πεδίο εφαρμογής του ISMS (βλ. 4.2.1a)
c. Οι διαδικασίες και οι έλεγχοι που υποστηρίζει το ISMS
d. Μια περιγραφή της μεθοδολογίας αποτίμησης κινδύνου (βλ. 4.2.1c)
e. Η αναφορά (βλ. 4.2.1c έως 4.2.1g) της αποτίμησης κινδύνου
f. Το πλάνο της εξάλειψης κινδύνου (risk treatment plan) (βλ. 4.2.2b)
g. Τη Δήλωση Εφαρμογής (Statement of Applicability)

Συμπερασματικά, ένας οργανισμός που επιθυμεί να διεξάγει αποτίμηση κινδύνου ακολουθώντας το πρότυπο ISO 27001 θα πρέπει να καθορίσει το δική του ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) και να ελέγξει εάν το επίπεδο ασφάλειας που έχει ορίσει είναι σύμφωνο με την πολιτική, τους στόχους και της διαδικασίες του οργανισμού πάντα σε πλήρη συμμόρφωση με τις απαιτήσεις του προτύπου.

2.2 Μεθοδολογία CYSM

2.2.1 Στόχοι και Αποτελέσματα του ευρωπαϊκού έργου CYSM

Λόγω των αυξημένων απαιτήσεων και αρμοδιοτήτων που αντιμετωπίζουν τα εμπορικά λιμάνια, η ανάγκη για αξιόπιστες και ασφαλείς εγκαταστάσεις αλλά και υπηρεσίες ηλεκτρονικής ναυτιλίας είναι μεγάλη. Πιο συγκεκριμένα, τα εμπορικά λιμάνια χαρακτηρίζονται από ένα διπλό χαρακτηριστικό "physical / cyber" : τα φυσικά χαρακτηριστικά τους που σχετίζονται με τη λιμενική υποδομή (συμπεριλαμβανομένων των εγκαταστάσεων, των κτηρίων, τις πλατφόρμες, τις πύλες, τις μαρίνες, τα κέντρα δεδομένων), ενώ τα χαρακτηριστικά του κυβερνοχώρου τους που σχετίζονται με τα συστήματά τους στις ΤΠΕ (συμπεριλαμβανομένων των δικτύων, του εξοπλισμού hardware ΤΠΕ, τα εσωτερικά συστήματα, τις υπηρεσίες, τα δεδομένα, τους χρήστες, τις διαδικασίες, τον έλεγχο πρόσβασης / έλεγχο ταυτότητας των χρηστών και του φορτίου).

Σε αυτό το πλαίσιο, το CYSM συμβάλλει στην ενίσχυση της συνεργασίας μεταξύ των ενδιαφερομένων ευρωπαϊκών λιμένων προς ένα πρακτικό, φιλικό προς το χρήστη και εναρμονισμένο με τα πρότυπα για τη διαχείριση της ασφάλειας των φυσικών και των ψηφιακών υποδομών πληροφοριών ζωτικής σημασίας των λιμένων. Έτσι, το ευρωπαϊκό έργο CYSM έχει δημιουργήσει ένα συνεργατικό εργαλείο αξιολόγησης της ασφάλειας των λιμένων, που στοχεύει στην ασφάλεια του κυβερνοχώρου και τη φυσική ασφάλεια των υποδομών πληροφοριών ζωτικής σημασίας των λιμένων (ΥΠΖΣ). Βασισμένο στη δυναμική μεθοδολογία Διαχείρισης Κινδύνου (CYSM-RM), το CYSM επιτρέπει στους χειριστές των υποδομών των λιμένων την αξιολόγηση των φυσικών και των κυβερνοαπειλών έναντι των απαιτήσεων που καθορίζονται στον κώδικα ISPS (φυσικός χώρος) και στο πρότυπο ISO27001 (κυβερνοχώρος).

Πιο συγκεκριμένα, οι στόχοι του έργου αυτού είναι οι εξής:

- Η ανάλυση όλου του φάσματος των απειλών των λιμενικών ΥΠΖΣ (είτε φυσικών είτε στον κυβερνοχώρο), άμεσα (από τα φυσικά και τα ψηφιακά αγαθά των λιμένων) και έμμεσα (από την αλληλεπίδραση από διάφορες οντότητες και άλλα ΥΠΖΣ), η συσχέτισή τους και ανάλυση των επιπτώσεων τους.

- Η παροχή μιας δυναμικής μεθοδολογίας διαχείρισης κινδύνων (CYSM-RM) για τις ΥΠΖΣ των λιμένων λαμβάνοντας υπόψη τη φυσική και ψηφιακή φύση τους.

- Η ανάπτυξη ενός συστήματος συλλογικής διαχείρισης της ασφάλειας (σύστημα CYSM), επιτρέποντας παράλληλα στους χειριστές των λιμένων να: μοντελοποιούν τα φυσικά αγαθά και τα αγαθά του κυβερνοχώρου, να αναλύουν και να διαχειριστούν τις εσωτερικές/εξωτερικές/ αλληλεξαρτώμενες φυσικές και ψηφιακές απειλές και τα τρωτά σημεία, να αξιολογούν και να διαχειρίζονται τους κινδύνους (χρησιμοποιώντας CYSMRM), να δημιουργούν αυτόματα εγχειρίδια ασφαλείας (π.χ. απειλές / αντίμετρα / σενάρια κρίσης / μηχανισμοί πρόληψης / πολιτικές ασφαλείας / σχέδια αποκατάστασης καταστροφών), καθώς και να αυξήσουν τη συνεργασία μεταξύ των συμμετεχόντων προς την κατανομή της ασφάλειας (θαλάσσιας γνώσης, πρότυπα, νομοθεσία, βέλτιστες πρακτικές, κατευθύνσεις).

2.2.2 Παράδειγμα ανάλυσης επικινδυνότητας σε λιμενική υπηρεσία- Εκτίμηση διαχείρισης του φορτίου (Cargo Assessment)

1ο βήμα: Στο πρώτο βήμα της μεθοδολογίας CYSM, γίνεται οριοθέτηση του συστήματος υπό μελέτη με βάση το αγαθό που έχει επιλεχθεί για τη διεξαγωγή αποτίμησης κινδύνου. Στο συγκεκριμένο παράδειγμα, το υπό μελέτη αγαθό είναι το φορτίο. Επομένως, επιλέγουμε ως αγαθό το **φορτίο** (Cargo) στην αποτίμηση κινδύνου.

2ο βήμα: Στο δεύτερο βήμα της μεθοδολογίας, πραγματοποιείται ο προσδιορισμός των πληροφοριακών αγαθών. Ουσιαστικά, γίνεται καταγραφή των υποδομών που ήδη υπάρχουν στο υπό μελέτη σύστημα όπου ανήκει και το επιλεγμένο αγαθό (φορτίο). Στο παράδειγμα αυτό, το υπό μελέτη σύστημα είναι το λιμάνι και επομένως, στον πίνακα που ακολουθεί γίνεται καταγραφή των υποδομών σε ένα λιμάνι.

Έχει αξιολογηθεί	**Όνομα**	**Τύπος**
ΝΑΙ	αποθήκη	κτήρια (φυσική στοιβάδα)
ΟΧΙ	κτήριο ηλεκτροπαραγωγής	κτήρια (φυσική στοιβάδα)
ΝΑΙ	φορτίο	τερματικά λιμανιού (φυσική στοιβάδα)
ΝΑΙ	αποθήκευση φορτίων	αποβάθρες λιμανιού(φυσική στοιβάδα)
ΟΧΙ	σταθμός φορτίων	τερματικά λιμανιού (φυσική στοιβάδα)
ΟΧΙ	Containers στοίβαξης με χαλίκι	κτήρια (φυσική στοιβάδα)
ΟΧΙ	Χώρος στάθμευσης για ρυμουλκούμενα	τερματικά λιμανιού (φυσική στοιβάδα)

3ο βήμα: Στο επόμενο βήμα, παρουσιάζεται το σύνολο των επιπτώσεων ως προς την ενδεχόμενη έλλειψη της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των αγαθών που εντοπίστηκαν στο προηγούμενο βήμα. Πιο συγκεκριμένα, οι επιπτώσεις διακρίνονται σε νομικές επιπτώσεις, ανθρώπινες απώλειες και οικονομικές απώλειες και η κάθε μία έχει και μια συγκεκριμένη αξία (υψηλή, μέτρια, χαμηλή) για το υπό μελέτη σύστημα. Για παράδειγμα, κάθε φορά που υπάρχουν ανθρώπινες απώλειες ως αποτέλεσμα της έλλειψης της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτίκοτητας του υπό μελέτη αγαθού, τότε η αξία είναι αυτόματα υψηλή. Στον παρακάτω πίνακα, αποτυπώνεται το σύνολο των επιπτώσεων συναρτήσει του αγαθού:

i. Ακεραιότητα:

Αγαθά	**Τύπος επίπτωσης**	**Αξία**
	Νομικές επιπτώσεις	
κτήριο ηλεκτροπαραγωγής		υψηλή
φορτίο		υψηλή
αποθήκη		χαμηλή
	Ανθρώπινες απώλειες	
κτήριο ηλεκτροπαραγωγής		υψηλή
φορτίο		υψηλή
αποθήκη		υψηλή
	Οικονομικές απώλειες	
κτήριο ηλεκτροπαραγωγής		υψηλή
φορτίο		υψηλή
αποθήκη		υψηλή

ii. Εμπιστευτικότητα:

Αγαθά	**Τύπος επίπτωσης**	**Αξία**
	Νομικές επιπτώσεις	
κτήριο ηλεκτροπαραγωγής		υψηλή

φορτίο		υψηλή
αποθήκη		υψηλή
	Ανθρώπινες απώλειες	
κτήριο ηλεκτροπαραγωγής		υψηλή
φορτίο		υψηλή
αποθήκη		υψηλή
	Οικονομικές απώλειες	
κτήριο ηλεκτροπαραγωγής		υψηλή
φορτίο		υψηλή
αποθήκη		μέτρια

iii. Διαθεσιμότητα:

Αγαθά	**Τύπος επίπτωσης**	**Αξία**
	Νομικές επιπτώσεις	
κτήριο ηλεκτροπαραγωγής		υψηλή
φορτίο		υψηλή
αποθήκη		μέτρια
	Ανθρώπινες απώλειες	
κτήριο ηλεκτροπαραγωγής		υψηλή
φορτίο		υψηλή
αποθήκη		υψηλή
	Οικονομικές απώλειες	
κτήριο ηλεκτροπαραγωγής		υψηλή
φορτίο		υψηλή
αποθήκη		υψηλή

4ο βήμα: Στη συνέχεια, γίνεται προσδιορισμός των μέτρων ελέγχου με βάση τα αγαθά που εντοπίστηκαν στο 2^{ο} βήμα αλλά και με τις επιπτώσεις στα αγαθά αυτά, σύμφωνα με το προηγούμενο βήμα. Για κάθε μέτρο ελέγχου που προτείνεται, παρατίθεται και παράδειγμα εφαρμογής του, όπως ακολουθεί στους παρακάτω πίνακες:

Όνομα	**Έλεγχος**	**Παράδειγμα**
κτήρια	φορητοί ανιχνευτές μετάλλων	ανίχνευση μεταλλικών στοιχείων (μαχαίρι, κλπ.)
	φράχτης/τοίχος	οποιοδήποτε είδος φράχτη με συγκεκριμένα χαρακτηριστικά: ύψος τουλάχιστον 2,5 μέτρα, χωρίς δυνατότητα υπερπήδησης, καλά στερεωμένο στο έδαφος κλπ.
	βιομετρικά συστήματα αναγνώρισης	δαχτυλικά αποτυπώματα, κόρη ματιού
	διάφορα είδη μπαρών ελέγχου πρόσβασης	ηλεκτρονικές μπάρες, περιστρεφόμενες πόρτες
	κολωνάκια	κολωνάκια σταθερά που εμποδίζουν την πρόσβαση μηχανοκίνητων οχημάτων σε συγκεκριμένες περιοχές

Όνομα	**Έλεγχος**	**Παράδειγμα**

δικτυακές υποδομές	σύστημα ελέγχου πρόσβασης που παρακολουθείται από ένα C4I	web-based εργαλείο δικτύου που παρέχει one-stop overview
	ασφάλεια σε περίπτωση πυρκαγιάς	ανιχνευτές καπνού, πυροσβεστικά μέσα
	διαδικασίες δημιουργίας αντιγράφων ασφαλείας των δεδομένων	backups
	εξοπλισμός που προστατεύεται από διακοπές ρεύματος	UPS σε servers, firewalls κλπ.

5ο βήμα: Στο τελευταίο βήμα της μεθοδολογίας CYSM, πραγματοποίεται αποτίμηση απειλών στο λιμάνι, όπου αναφέρονται ονομαστικά οι απειλές, περιγράφονται πιο λεπτομερώς και περιγράφεται επίσης και η συχνότητα εμφάνισής τους στο υπό μελέτη σύστημα:

Όνομα απειλής	**Περιγραφή**	**Συχνότητα εμφάνισης**
εμπρησμός	εσκεμμένη πυρκαγιά σε κτήρια, οχήματα κλπ. με σκοπό να προκληθεί ζημιά	όχι περισσότερο από μία φορά ανά 10 χρόνια
τυχαία πυρκαγιά	φωτιά σε εγκαταστάσεις/αγαθά που προκλήθηκε τυχαία	όχι περισσότερο από μία φορά ανά 10 χρόνια
βίαιη είσοδος	παράνομη είσοδος σε προσωπική ιδιοκτησία άλλου χρησιμοποιώντας βία	μια φορά το χρόνο
τρομοκρατική επίθεση	από την ξηρά ή/και από τη στεριά	όχι περισσότερο από μία φορά ανά 10 χρόνια
γείωση πλοίου	όταν βουλιάζει λόγω παγόβουνου κλπ.	όχι περισσότερο από μία φορά ανά 10 χρόνια
απώλεια της παροχής ρεύματος	διακοπή ηλεκτρικής ενέργειας που έχει σοβαρές επιπτώσεις στη διαθεσιμότητα	μια φορά το μήνα
αποτυχίες προσωπικού, μονάδων	εργαζόμενοι ή εξωτερικό προσωπικό χρησιμοποιεί τον λιμενικό εξοπλισμό χωρίς άδεια	μια φορά ανά τετράμηνο
μη εξουσιοδοτημένη χρήση του εξοπλισμού	εργαζόμενοι ή εξωτερικό προσωπικό χρησιμοποιεί τον λιμενικό εξοπλισμό χωρίς άδεια	μια φορά ανά τετράμηνο
απουσία του προσωπικού	κίνδυνοι από απουσία προσωπικού (έλλειψη προσωπικού λόγω ασθένειας ή άδειας)	μια φορά ανά τετράμηνο
ακραίες τιμές θερμοκρασίας και υγρασίας	σοβαρές απώλειες υποδομών (αποθηκεμένων φορτίων) λόγω υψηλής θερμοκρασίας/ υγρασίας	μια φορά το χρόνο
τεχνικές βλάβες	βλάβες στο μηχανολογικό εξοπλισμό (συσκευές ή δίκτυο) με αποτέλεσμα τη μη ομαλή λειτουργία τους	μια φορά το μήνα

2.3 Μεθοδολογία ENISA RM Information Packages for Small and Medium Sized Enterprises (SMEs)

Η μεθοδολογία ENISA RM Information packages for SMEs απευθύνεται στην αποτίμηση κινδύνου που διεξάγεται από μικρομεσαίες επιχειρήσεις, των οποίων τα πληροφοριακά συστήματα έχουν κινδύνους με μεγάλο ρίσκο (κίνδυνο) . Οι επιχειρήσεις αυτές συνήθως εργάζονται σε ένα πλαίσιο όπου η επεξεργασία των δεδομένων τους πραγματοποιείται σε ένα τυποποιημένο περιβάλλον αλλά σημαντικό για την επιχείρηση. Χρησιμοποιούν πακέτα όπως off-the-shelf προϊόντα που έχουν ή αποτελούνται αποκλειστικά από « μαύρο κουτί » (με όλους τους πιθανούς κινδύνους) και συνδέονται για την επιχείρησή τους στο Διαδίκτυο, όπου ελλωχεύουν πολλές απειλές για την ασφάλεια των πληροφοριακών τους συστημάτων.

Σύμφωνα με την επιχειρηματική τους δραστηριότητα, οι μικρομεσαίες επιχειρήσεις εξαρτώνται αρκετά από το πληροφοριακό τους σύστημα. Οι εταιρείες και τα ηλεκτρονικά καταστήματα, για παράδειγμα, προσφέρουν ηλεκτρονικές υπηρεσίες στους τελικούς χρήστες. Μια γρήγορη απάντηση στις ανάγκες της αγοράς είναι ασφαλώς ζωτικής σημασίας για την επιτυχία τους. Το πληροφοριακό σύστημα που σχετίζεται με αυτό, δηλαδή με την ικανότητα απόκρισης έχει μεγάλη σημασία για την επιχειρηματική τους διαδικασία. Παρόλ'αυτά, οι εταιρείες γενικά δεν αναλαμβάνουν να επενδύσουν αρκετούς πόρους στην ανάλυση και τη διαχείριση των κινδύνων των πληροφοριακών τους συστημάτων.

2.3.1 Τυπικές επιχειρηματικές διαδικασίες

Ορισμένες μικρού μεγέθους επιχειρήσεις μπορεί να θεωρηθεί ότι διαθέτουν διαδικασίες που εξαρτώνται σε μεγάλο βαθμό από τα πληροφοριακά τους συστήματα, όπως αναφέρθηκε και στην προγούμενη παράγραφο.

Οι τυπικές επιχειρηματικές διαδικασίες μιας μικρής εταιρείας με υψηλό κίνδυνο ΠΣ μπορούν να ταξινομηθούν στα ακόλουθες κατηγορίες:

- Παραγωγή: Διαδικασίες που είναι απαραίτητες για την παράδοση των προϊόντων ή των υπηρεσιών που πωλούνται στον πελάτη. Στις περισσότερες περιπτώσεις, είναι η κύρια δραστηριότητα μιας εταιρείας.
- Χρηματοδότηση: Οι εσωτερικές χρηματοοικονομικές διαδικασίες (επενδύσεις, πληρωμές)
- Ανθρώπινοι πόροι: Διαδικασίες διαχείρισης του ανθρώπινου δυναμικού
- Πωλήσεις, διανομή, μάρκετινγκ: Δραστηριότητες για την απόκτηση νέων πελατών και για τη διατήρηση των ήδη υφιστάμενων

Οι κίνδυνοι ασφάλειας των πληροφοριακών συστημάτων που εξετάζονται σε αυτό το πλαίσιο μπορούν να προκύψουν όχι μόνο από τεχνικές απειλές, αλλά και από άλλες απειλές όπως η κοινωνική μηχανική, από απειλές που σχετίζονται με την κινητικότητα των χρησιμοποιούμενων συσκευών κλπ.

Είναι απαραίτητο για μια εταιρεία να θέσει μία ελάχιστη υποδομή για να εξασφαλίσει την εσωτερική επικοινωνία και τη συνέχεια της επιχείρησης σε περίπτωση καταστροφής όπως δίκτυο, αντίγραφα ασφαλείας κλπ. Προκειμένου να προστατεύσουν τις εμπιστευτικές τους πληροφορίες (ευαίσθητες πληροφορίες) οι εταιρείες αυτού του τύπου μπορεί να χρειαστεί να επενδύσουν σε εργαλεία και γνώσεις για κρυπτογραφία που μπορεί να χρειάζονται κάποια εξειδικευμένη γνώση.

Συχνά, ωστόσο, η έλλειψη γνώσεων στο εσωτερικό του οργανισμού μπορεί να καταστήσει αναγκαία την εξωτερική ανάθεση αυτών των υπηρεσιών προς ένα τρίτο μέρος, το οποίο μπορεί να είναι μια μεγάλη εταιρεία.

Ακολουθεί ένα παράδειγμα χρήσης της μεθοδολογίας ENISA RM Information packages for SMEs για την περίπτωση ενός ηλεκτρονικού καταστήματος.

2.3.2 Παράδειγμα χρήσης της μεθοδολογίας: Ηλεκτρονικό κατάστημα

Θα θεωρήσουμε τώρα την ειδική περίπτωση ενός ηλεκτρονικού καταστήματος που πωλεί προϊόντα IT hardware που παρέχονται από συνεργαζόμενες εταιρίες με την μικρομεσαία επιχείρηση Χ. Το παρακάτω σχήμα δίνει ένα παράδειγμα βασικών επιχειρηματικών διαδικασιών και τη σημασία τους για την επιχείρηση:

Επιχειρηματική Διαδικασία	Σημασία για την επιχείρηση
Παραγωγή	Μεγάλης Σημασίας
Οικονομικά	Μεγάλης Σημασίας
Ανθώπινο Δυναμικό	Μικρής Σημασίας
Μάρκετινγκ	Μεσαίας Σημασίας

Σχήμα 9: Επιχειρηματικές διαδικασίες και η σημασία τους για την επιχείρηση

Για την πραγματοποίηση αυτών των διαδικασιών απαιτούνται ορισμένα ειδικά συστήματα πληροφορικής. Ο παρακάτω πίνακας (σχήμα 10) απεικονίζει την κρισιμότητα διαχείρισης κινδύνου για κάθε σύστημα / διαδικασία ΤΠ, λαμβάνοντας υπόψη τη σημασία τους και το βαθμό εξάρτησης τους (όπως απεικονίζεται στο σχήμα 9 παραπάνω).

Η τελευταία στήλη συνοψίζει την κρισιμότητα όσον αφορά τη διαχείριση του κινδύνου ως το μέγιστο των κρισιμοτήτων που βρέθηκαν στην ίδια σειρά. Αυτό οφείλεται στο γεγονός ότι η διαχείριση του κινδύνου εφαρμόζεται σε συστήματα πληροφορικής και όχι στις επιχειρηματικές διαδικασίες. Για παράδειγμα, αν ένα πληροφοριακό σύστημα έχει υψηλή κρισιμότητα για τουλάχιστον μία επιχειρηματική διαδικασία, τότε η συνολική κρισιμότητα του είναι υψηλή.

Πληροφοριακό Σύστημα	**Παραγωγή: *Υψηλής Σημασίας***	**Οικονομικά: *Υψηλής Σημασίας***	**Ανθρώπινο Δυναμικό: *Μέτριας Σημασίας***	**Μάρκετινγκ *Μεσαίας Σημασίας***	**Σχόλια**	**Συνολική Κρισιμότητα *(max. criticality)***
Παραγωγή Web Services: *high dependency*	Υψηλή κρισιμότητα				Η εταιρία πωλεί τα προϊόντα της κυρίως μέσω ενός ηλεκτρονικού καταστήματος	Υψηλή κρισιμότητα
Παραγωγή Βάση Δεδομένων: *high dependency*	Υψηλή κρισιμότητα				Αποθηκέυει τα δεδομένα των πωλήσεων (συμπεριλ. Και προσωπικών δεδομένων)	Υψηλή κρισιμότητα
Παραγωγή Αρχεία και Εκτύπωση: *medium dependency*	Μέτρια κρισιμότητα				Λειτουργία για την επεξεργασία παραγγελιών, την έκδοση αποδείξεων και την επικοινωνία με τους πελάτες	Μέτρια κρισιμότητα
Παραγωγή / Συγκεκριμένες διαδικασίες: *high dependency*	Υψηλή κρισιμότητα				Σύνολο προγραμμάτων που χρησιμοποιείται για την πρόσβαση και τη διαχείριση του production env.	Υψηλή κρισιμότητα
Οικονομικά και Έλεγχος εφαρμογών: *low dependency*		Μικρή κρισιμότητα			Αποθηκεύει δεδομένα για να υπολογίσει την εσωτερική απόδοση κόστους	Μικρή κρισιμότητα
Μάρκετινγκ Αρχεία και Εκτύπωση: *low dependency*				Καμία κρισιμότητα	Χρησιμοποιείται από τη μονάδα Μάρκετινγκ για να παράγουν το υλικό πληροφοριών τους	Καμία κρισιμότητα
E-Mail: *medium dependency*	Μεσαία κρισιμότητα	Μεσαία κρισιμότητα	Καμία κρισιμότητα	Χαμηλή κρισιμότητα	Η εταιρία έχει ένα κεντρικό σύτημα ηλεκτρονικού ταχυδρομείου. Αυτό είναι απαραίτητο για την εσωτερική και εξωτερική επικοινωνία	Μεσαία κρισιμότητα
IT Υποδομή: *high dependency*	Υψηλή κρισιμότητα	Υψηλή κρισιμότητα	Χαμηλή κρισιμότητα	Μεσαία κρισιμότητα	Αποτελείται από το hardware, το τοπικό δίκτυο, το λειτουργικό	Υψηλή κρισιμότητα

					σύστημα, το λογισμικό. Αυτά είναι απαραίτητα για τη λειτουργία των ΠΣ	

Σχήμα 10: Κρισιμότητα από τη διαχείριση κινδύνου

2.4 Μεθοδολογία CRAMM

Η μεθοδολογία CRAMM, δηλαδή CCTA Risk Analysis and Management Method αναπτύχθηκε από την κεντρική υπηρεσία πληροφορικής και τηλεπικοινωνιών της Μ.Βρετανίας (Central Computer and Telecommunication Agency). Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί κυρίως σε μεγάλης κλίμακας οργανισμούς όπως είναι δημόσιοι οργανισμοί, τράπεζες, νοσοκομεία και σε επιχειρήσεις κοινής ωφέλειας. Από το 1987 μέχρι σήμερα έχει εφαρμοστεί σε πλήθος περιπτώσεων, κάτι που την καθιστά μια ώριμη και δοκιμασμένη μέθοδο.

Η μέθοδος CRAMM συνοδεύεται από ένα αυτοματοποιημένο εργαλείο λογισμικού το οποίο υποστηρίζει όλα τα στάδια της εφαρμογής της καθώς και την επιλογή αντίμετρων. Επίσης, καλύπτει όλες τις συνιστώσες της ασφάλειας συμπεριλαμβανομένου του τεχνικού παράγοντα, θεμάτων διαδικασιών και προσωπικού, φυσικής ασφάλειας, ασφάλειας δικτύων κλπ.

Τα βασικά στάδια της CRAMM είναι τα παρακάτω:

1. Οριοθέτηση προβλήματος ασφάλειας: Στο αρχικό αυτό στάδιο, ουσιαστικά απαντάμε στην ερώτηση « Υπάρχει ανάγκη για ασφάλεια πάνω από ένα ανεκτό επίπεδο; » και γίνεται ο προσδιορισμός και η αποτίμηση των αγαθών.
2. Εκτίμηση επικινδυνότητας: Στο στάδιο αυτό που είναι και το πιο σημαντικό στη μέθοδο, απαντάμε στην ερώτηση « Ποιοι είναι και πού εντοπίζονται οι κίνδυνοι ασφάλειας; »
3. Επιλογή κατάλληλων αντιμέτρων: Στο τρίτο και τελευταίο στάδιο, απαντάμε στην ερώτηση « Πώς μπορούμε να διαχειριστούμε τον κίνδυνο; »

Ο συνδυασμός των τριών αυτών παραγόντων, δηλαδή η αποτίμηση αγαθών, το επίπεδο των απειλών και το επίπεδο των ευπαθειών, δίνει το βαθμό επικινδυνότητας του πληροφοριακού συστήματος, έτσι ώστε να επιλεγούν τα κατάλληλα αντίμετρα. Πιο συγκεκριμένα, η επικινδυνότητα προκύπτει ως εξής:

Απειλή Χ Αδυναμία = Πιθανότητα

Πιθανότητα Χ Επίπτωση = Επικινδυνότητα

Σχήμα 11: Υπολογισμός επικινδυνότητας

Τα βήματα της μεθόδου CRAMM παρουσιάζονται αναλυτικά παρακάτω:

Στάδιο	Βήματα
1. Προσδιορισμός και αποτίμηση αγαθών (identification and valuation of assets)	Βήμα 1.1: Προσδιορισμός επιμέρους πληροφοριακών και επικοινωνιακών αγαθών Βήμα 1.2: Αποτίμηση αγαθών ΠΣ Βήμα 1.3: Επιβεβαίωση και επικύρωση της αποτίμησης
2. Ανάλυση κινδύνου (risk analysis)	Βήμα 2.1: Προσδιορισμός απειλών που αφορούν κάθε αγαθό Βήμα 2.2: Εκτίμηση απειλών και αδυναμιών Βήμα 2.3: Υπολογισμός κινδύνου συνδυασμών Αγαθό - Απειλή - Αδυναμία Βήμα 2.4: Επιβεβαίωση και επικύρωση βαθμού κινδύνου
3. Διαχείριση κινδύνου (risk management)	Βήμα 3.1: Προσδιορισμός προτεινόμενων αντιμέτρων

	Βήμα 3.2: Σχέδιο ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων

Σχήμα 12: Βήματα μεθοδολογίας CRAMM

2.4.1 Παρουσίαση και Εφαρμογή των βημάτων της μεθοδολογίας CRAMM

- Στάδιο 1: Προσδιορισμός και αποτίμηση αγαθών (identification and valuation of assets)

i. **Βήμα 1.1**: Προσδιορισμός επιμέρους πληροφοριακών και επικοινωνιακών αγαθών

Το πρώτο βήμα αναφέρεται αναφέρεται στον προσδιορισμό των στοιχείων των Πληροφοριακών Συστημάτων που απαιτούν προστασία. Για παράδειγμα, τέτοια στοιχεία είναι τα φυσικά αγαθά όπως κτήρια, υπολογιστικά συστήματα αλλά και τα αγαθά λογισμικού και δεδομένων.

Στη συνέχεια, γίνεται εκτίμηση των άμεσων (οικονομικών) και έμμεσων συνεπειών όπως είναι για παράδειγμα το κόστος επαναγοράς (άμεση συνέπεια), η παρεμπόδιση λειτουργίας (έμμεση συνέπεια), οι νομικές συνέπειες (έμμεση συνέπεια), κλπ.

ii. **Βήμα 1.2**: Αποτίμηση αγαθών ΠΣ

Η αξία κάθε ομάδας / κατηγορίας δεδομένων αποτιμάται με βάση την επίπτωση (impact) που θα είχε η απώλειά της. Στον παρακάτω πίνακα παρουσιάζεται ο βαθμός (κλίμακα) της εκάστοτε οικονομικής επίπτωσης που θα είχε στον οργανισμό, η απώλεια κάθε ομάδας δεδομένων.

Βαθμός	Οικονομική Επίπτωση
1	<1000€
2	<10.000€
3	<30.000€
4	<100.000€
5	<300.000€
6	<1.000.000€
7	<3.000.000€
8	<10.000.000€
9	<30.000.000€
10	<100.000.000€

Σχήμα 13: Κλίμακα επιπτώσεων

Για κάθε περίπτωση εκτιμάται το δυσμενέστερο πιθανό σενάριο και υπολογίζονται οι επιπτώσεις από την πραγματοποίησή του. Το μέγεθος της επίπτωσης εκτιμάται αριθμητικά με βάση κλίμακα 1-10. Οι πιθανές επιπτώσεις είναι οι ακόλουθες:

- Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων
- Επιπτώσεις από την αποκάλυψη προσωπικών δεδομένων
- Νομικές επιπτώσεις
- Παρεμπόδιση εφαρμογής του νόμου

- Οικονομικές απώλειες
- Διεθνείς σχέσεις
- Εθνική άμυνα και ασφάλεια
- Εφαρμογή της πολιτικής του οργανισμού

Στη συνέχεια, παρουσιάζεται η κλίμακα της απώλειας της διαθεσιμότητας , της απώλειας της εμπιστευτικότητας και της απώλειας της ακεραιότητας των δεδομένων. Πιο συγκεκριμένα, οι κλίμακες αυτές καθορίζονται ως εξής:

- Απώλεια της διαθεσιμότητας των δεδομένων: μη διαθεσιμότητα για 15 λεπτά (15 Λ), μη διαθεσιμότητα για 1 ώρα (1 Ω), μη διαθεσιμότητα για 3 ώρες (3 Ω), μη διαθεσιμότητα για 12 ώρες (12 Ω), μη διαθεσιμότητα για 1 ημέρα (1 Η), μη διαθεσιμότητα για 2 ημέρες (2 Η), μη διαθεσιμότητα για 1 εβδομάδα (1 Ε), μη διαθεσιμότητα για 2 εβδομάδες (2 Ε), μη διαθεσιμότητα για 1 μήνα (1 Μ), μη διαθεσιμότητα για 2 μήνες (2 Μ)

- Απώλεια της εμπιστευτικότητας των δεδομένων: αποκάλυψη δεδομένων εντός του οργανισμού (Μη εξουσιοδοτημένη πρόσβαση από εσωτερικούς χρήστες - Εσωτερική Αποκάλυψη - ΑΕΣ), αποκάλυψη δεδομένων σε τρίτους εκτός του οργανισμού (Μη εξουσιοδοτημένη πρόσβαση από εξωτερικούς χρήστες - (Εξωτερική Αποκάλυψη - ΑΕΞ), μη εξουσιοδοτημένη πρόσβαση σε συνεργάτες εκτός του Οργανισμού (αποκάλυψη δεδομένων σε συνεργάτες - ΑΣΥΝ)

- Παραβίαση της ακεραιότητας των δεδομένων: καταστροφή πληροφοριακού πόρου, όχι όμως των εφεδρικών - μερική καταστροφή δεδομένων (ΜΚ), ολική καταστροφή πληροφοριακού πόρου και των εφεδρικών - ολική καταστροφή δεδομένων (ΟΚ), σκόπιμη αλλοίωση δεδομένων (ΣΑ)

iii. Βήμα 1.3: Επιβεβαίωση και επικύρωση της αποτίμησης

Στο στάδιο αυτό, παρουσιάζονται τα αποτελέσματα του πρώτου σταδίου τα οποία παρουσιάζονται σε σχετική έκθεση η οποία περιλαμβάνει τα εξής:

- Τον ορισμό του προς ανάλυση συστήματος και των ορίων του.
- Τη μέθοδο εργασίας που ακολουθήθηκε.
- Την αποτίμηση των αγαθών των Π.Σ.
- Γενικά συμπεράσματα του πρώτου σταδίου.

Ο παρακάτω πίνακας παρουσιάζει τα αποτελέσματα του πρώτου σταδίου για την αποτίμηση του αγαθού «Οικονομικά Δεδομένα» :

Συμβάν	Επίπτωση	Αποτίμηση (0-10)
Απώλεια Διαθεσιμότητας Δεδομένων	Η μη διαθεσιμότητα των Οικονομικών Δεδομένων θα έχει περιορισμένη επίπτωση στη λειτουργία της αρμόδιας Διεύθυνσης, προκαλώντας καθυστέρηση στη διεκπεραίωση των αντίστοιχων υπηρεσιών και οικονομικών υποχρεώσεων	Απώλεια διαθεσιμότητας για 3 ώρες: **1**
		Απώλεια διαθεσιμότητας για 1 ημέρα: **2**
		Απώλεια διαθεσιμότητας για 1 εβδομάδα : **3**
Ολική Καταστροφή Δεδομένων	Η ολική καταστροφή των Οικονομικών Δεδομένων, περιλαμβανομένων και των εφεδρικών αντιγράφων, συνεπάγεται την	**4**

	εκ νέου εισαγωγή των δεδομένων και θα δυσχεράνει την παρακολούθηση και διεκπεραίωση των οικονομικών συναλλαγών	
Σκόπιμη Αλλοίωση Δεδομένων	Η σκόπιμη αλλοίωση θα είχε ως αποτέλεσμα οικονομικές συνέπειες	**6**
Αποκάλυψη Δεδομένων	Ενδεχόμενη αποκάλυψη των δεδομένων αυτών εκτιμάται ότι θα έχει αρνητικές συνέπειες για τον οργανισμό	Μη εξουσιοδοτημένη πρόσβαση από εσωτερικούς χρήστες: **5**
		Αποκάλυψη δεδομένων σε συνεργάτες του Οργανισμού : **7**
		Αποκάλυψη δεδομένων σε τρίτους εκτός οργανισμού: **9**

Σχήμα 14: Αποτελέσματα πρώτου σταδίου μεθόδου CRAMM

- Στάδιο 2: Ανάλυση κινδύνου (risk analysis)

i. **Βήμα 2.2**: Εκτίμηση απειλών και αδυναμιών

Στο βήμα αυτό πραγματοποιείται η εκτίμηση των απειλών και των αδυναμιών όπου η απειλή εκτιμάται σε κλίμακα από 1-5 (1= very low, 2= low,3= medium, 4= high, 5=very high) και η αδυναμία σε κλίμακα 1-3 (1= low, 2= medium, 3= high). Παρακάτω, περιγράφεται αναλυτικά η διαβάθμιση των απειλών και των αδυναμιών και τι σημαίνει ουσιαστικά η κλίμακα που επιλέξαμε.

Βαθμός	Επίπεδο	Περιγραφή
1	**very low**	Αυτή η εκτίμηση απειλής δίδεται σε γεγονότα τα οποία αναμένεται να συμβούν το πολύ μέχρι 1 φορά το χρόνο
2	**low**	Αυτή η εκτίμηση απειλής δίδεται σε γεγονότα τα οποία αναμένεται να συμβούν 1 φορά το χρόνο.
3	**medium**	Αυτή η εκτίμηση απειλής δίδεται σε γεγονότα τα οποία αναμένεται να συμβούν από 2 μέχρι 3 φορές το χρόνο.
4	**high**	Αυτή η εκτίμηση απειλής δίδεται σε γεγονότα τα οποία αναμένεται να συμβούν από 4 μέχρι 5 φορές το χρόνο.
5	**very high**	Αυτή η εκτίμηση απειλής δίδεται σε γεγονότα τα οποία αναμένεται να συμβούν πάνω από 5 φορές το χρόνο.

Σχήμα 15: Επίπεδο Απειλής

Βαθμός	Επίπεδο	Περιγραφή
1	**low**	Σε περίπτωση που συνέβαινε μία απειλή, θα υπήρχε το πολύ 30% πιθανότητα να εκδηλωθεί το χειρότερο σενάριο συνεπειών, με βάση την εκτίμηση συνέπειας που έχει πραγματοποιηθεί.
2	**medium**	Σε περίπτωση που συνέβαινε μία απειλή, θα υπήρχε από 30% μέχρι 70% πιθανότητα να εκδηλωθεί το χειρότερο σενάριο συνεπειών, με βάση την εκτίμηση συνέπειας που έχει πραγματοποιηθεί.
3	**high**	Σε περίπτωση που συνέβαινε μία απειλή, θα υπήρχε πάνω από 70% πιθανότητα να εκδηλωθεί το χειρότερο σενάριο συνεπειών, με βάση την εκτίμηση συνέπειας που έχει πραγματοποιηθεί.

Σχήμα 16: Επίπεδο Αδυναμίας

ii. **Βήμα 2.3**: Υπολογισμός κινδύνου συνδυασμών Αγαθό - Απειλή - Αδυναμία

Στο βήμα αυτό πραγματοποιείται ο υπολογισμός του κινδύνου (από 1-7) σύμφωνα με τον συνδυασμό Αγαθό - Απειλή – Αδυναμία, δηλαδή υπολογίζεται η κλίμακα (βαθμός) του κινδύνου για κάθε συνδυασμό των τριών στοιχείων που προκύπτει από τις προηγούμενες μετρήσεις. Ακολουθεί παρακάτω ο πίνακας της κλίμακας του κινδύνου και στη συνέχεια ο τελικός πίνακας του κινδύνου (risk matrix) που λαμβάνει υπόψη το επίπεδο αδυναμίας και απειλής, όπως υπολογίστηκε στο προηγούμενο βήμα.

Βαθμός επικινδυνότητας	Περιγραφή
1	very low risk
2	low risk
3	medium risk
4	important risk
5	high risk
6	very high risk
7	critical risk

Σχήμα 17: Κλίμακα κινδύνου

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln. Asset Value	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Σχήμα 18: Πίνακας κινδύνου (risk matrix)

iii. **Βήμα 2.4**: Επιβεβαίωση και επικύρωση βαθμού κινδύνου

Στο βήμα αυτό, η ομάδα μελέτης μπορεί να χρησιμοποιήσει τις αναφορές που παράγει το λογισμικό της CRAMM. Έτσι, οι αναλυτές έχουν τη δυνατότητα :

- είτε να αλλάξουν τις τιμές του κινδύνου
- είτε να αλλάξουν τις τιμές που έχουν προκύψει από την εκτίμηση των απειλών και
- αδυναμιών
- να υπολογίσουν εκ νέου τον κίνδυνο.

➢ <u>Στάδιο 3: Διαχείριση κινδύνου (risk management)</u>

i. **Βήμα 3.1:** Προσδιορισμός προτεινόμενων αντίμετρων

Σε αυτό το βήμα προσδιορίζονται τα αντίμετρα (τεχνικά, διοικητικά και οργανωτικά) που θα ληφθούν προκειμένου να διαχειριστεί ο κίνδυνος που προέκυψε από το προηγούμενο στάδιο. Τα αντίμετρα χωρίζονται σε ομάδες ανάλογα με το είδος των απειλών που καλούνται να αντιμετωπίσουν και με το είδος των αγαθών που καλούνται να προστατέψουν. Επίσης, η βάση των αντιμέτρων περιλαμβάνει τόσο τις εναλλακτικές λύσεις όσο και τις επιλογές υλοποίησής τους.

Η μέθοδος CRAMM προτείνει με αυτόματο τρόπο τα αντίμετρα, σύμφωνα με τα αποτελέσματα της ανάλυσης κινδύνου. Συγκεκριμένα, ένα αντίμετρο μπορεί να είναι:

- Εγκατεστημένο (installed)
- Προς υλοποίηση (to be installed)
- Υπό υλοποίηση (implementing recommendation)
- Προτεινόμενο για υλοποίηση (implemented recommendation)
- Εφαρμοζόμενο (already covered)

ii. **Βήμα 3.2:** Σχέδιο ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων

Κατά τη διάρκεια του βήματος αυτού συγγράφεται το Σχέδιο Ασφάλειας που περιλαμβάνει τα εξής:

- (Σχέδιο) Πολιτικής Ασφάλειας
- Μέτρα Ασφάλειας
- Στρατηγική για την εφαρμογή του Σχεδίου Ασφάλειας

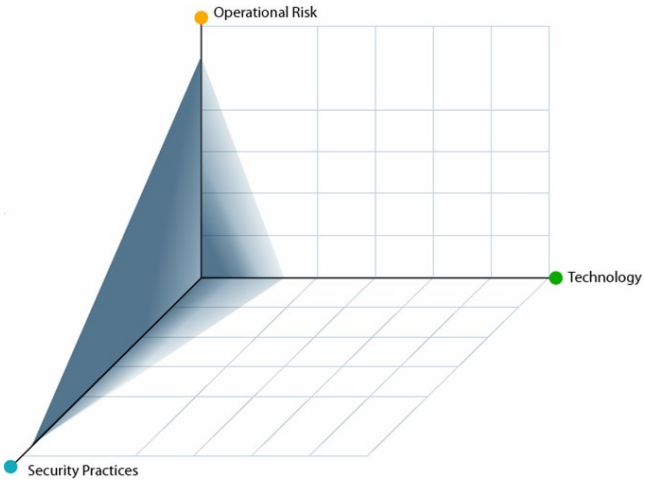
2.5 Μεθοδολογία Octave

Η μεθοδολογία OCTAVE αναπτύχθηκε στο Carnegie Mellon University το 1999. Για έναν οργανισμό που προσπαθεί να κατανοήσει τις ανάγκες του για την ασφάλεια των πληροφοριών, η OCTAVE είναι μια μέθοδος αποτίμησης κινδύνου που βασίζεται στην στρατηγική αξιολόγηση και τεχνική σχεδιασμού της ασφάλειας. Η OCTAVE είναι αυτοκατευθυνόμενη, που σημαίνει ότι οι άνθρωποι από έναν οργανισμό αναλαμβάνουν την ευθύνη για τον καθορισμό της στρατηγικής ασφάλειας του οργανισμού αυτού.

Η συγκεκριμένη μεθοδολογία αξιοποιεί την γνώση των ανθρώπων για την ασφάλεια του οργανισμού τους, δηλαδή αξιοποιεί σχετικές πρακτικές και διαδικασίες για την καταγραφή της τρέχουσας κατάστασης όσον αφορά την ασφάλεια στο πλαίσιο του οργανισμού. Οι κίνδυνοι για τα πιο κρίσιμα αγαθά χρησιμοποιούνται για να δοθεί προτεραιότητα στους τομείς βελτίωσης και για να καθοριστεί η στρατηγική ασφαλείας του οργανισμού.

Σε αντίθεση με την τυπική αποτίμηση κινδύνου η οποία στοχεύει στον τεχνολογικό κίνδυνο και επικεντρώνεται σε τακτικά ζητήματα, η OCTAVE στοχεύει στον οργανωτικό κίνδυνο και επικεντρώνεται στη στρατηγική, δηλαδή σε πρακτικά ζητήματα. Πρόκειται για μια ευέλικτη μεθοδολογία που μπορεί να προσαρμοστεί στους περισσότερους οργανισμούς. Πιο συγκεκριμένα, η OCTAVE έχει αναπτυχθεί για μικρής ή και μεσαίας κλίμακας οργανισμούς, δηλαδή η OCTAVE-S έχει αναπτυχθεί για οργανισμούς με 100 ή λιγότερους εργαζόμενους, ενώ η OCTAVE για οργανισμούς με 300 ή περισσότερους εργαζόμενους.

Κατά την εφαρμογή της OCTAVE, μια μικρή ομάδα ανθρώπων από την επιχειρησιακή (ή επιχειρηματική) μονάδα και το τμήμα πληροφορικής (IT) συνεργάζονται για την αντιμετώπιση των αναγκών της ασφάλειας του οργανισμού, εξισορροπώντας τις τρεις βασικές πτυχές που παρουσιάζονται στο σχήμα 19, τον επιχειρησιακό κίνδυνο, τις πρακτικές ασφάλειας και την τεχνολογία.



Σχήμα 19: Οι τρεις βασικές πτυχές της OCTAVE

Η μεθοδολογία ολοκληρώνεται με τη δημιουργία μιας στρατηγικής προστασίας για την οργανωτική βελτίωση αλλά και με τη μείωση του κινδύνου των κρίσιμων αγαθών.

2.5.1 Παρουσίαση και Εφαρμογή των σταδίων της μεθοδολογίας OCTAVE

Οι οργανωτικές, τεχνολογικές και αναλυτικές πτυχές μιας αποτίμησης κινδύνου ασφάλειας πληροφοριών συμπληρώνεται από μια προσέγγιση τριών φάσεων. Η μεθοδολογία OCTAVE οργανώνεται γύρω από αυτές τις τρεις βασικές πτυχές (που απεικονίζονται στο Σχήμα 20), επιτρέποντας στο οργανωτικό

προσωπικό να συγκεντρώσει μία ολοκληρωμένη εικόνα των αναγκών της επιχείρησης για την ασφάλεια των πληροφοριών. Οι φάσεις αυτές είναι οι εξής:

- Φάση 1: Δημιουργία προφίλ απειλών βασισμένων σε αγαθά

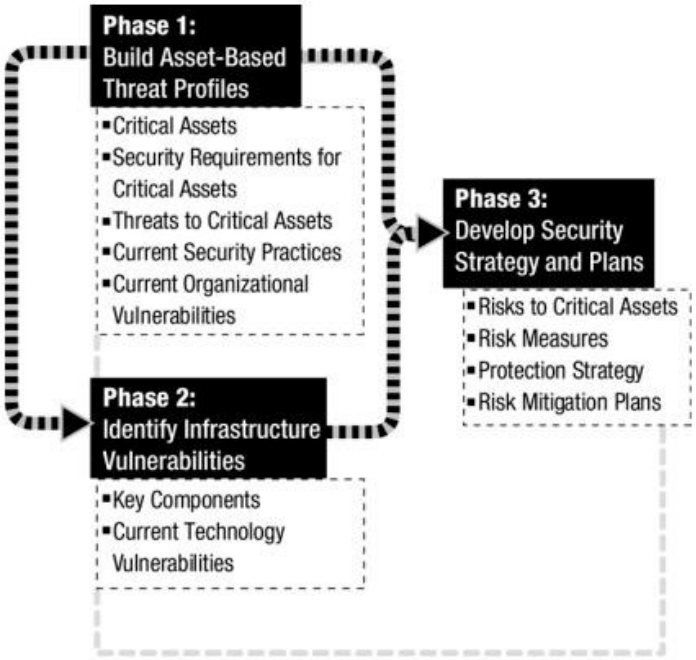
Στη φάση αυτή, η ομάδα ανάλυσης αξιολογεί ποια είναι τα σημαντικότερα αγαθά για τον οργανισμό και αναγνωρίζει ποια μέτρα εφαρμόζονται από τον οργανισμό για την προστασία τους. Ουσιαστικά, πρόκειται για μια οργανωτική αξιολόγηση. Η ομάδα ανάλυσης καθορίζει τι είναι σημαντικό για τον οργανισμό (αγαθά που σχετίζονται με την πληροφορία) και τι γίνεται επί του παρόντος για την προστασία αυτών των αγαθών. Η ομάδα επιλέγει έπειτα αυτά τα στοιχεία που είναι τα πιο σημαντικά για τον οργανισμό (κρίσιμα αγαθά) και περιγράφει τις απαιτήσεις ασφαλείας για κάθε κρίσιμο αγαθό. Τέλος, εντοπίζει απειλές για κάθε κρίσιμο αγαθό, δημιουργώντας ένα προφίλ απειλής για το εν λόγω στοιχείο.

- Φάση 2: Εντοπισμός των αδυναμιών της υποδομής

Στη δεύτερη φάση της μεθοδολογίας γίνεται αξιολόγηση των πληροφοριών ης υποδομής. Η ομάδα ανάλυσης εξετάζει θεμελιώδη στοιχεία για (τεχνικές) αδυναμίες που μπορούν να οδηγήσουν σε μη εξουσιοδοτημένες ενέργειες εναντίον κρίσιμων αγαθών του οργανισμού. Πιο συγεκριμένα, η ομάδα ανάλυσης εξετάζει τις διαδρομές πρόσβασης στο δίκτυο, προσδιορίζοντας τα components που σχετίζονται με κάθε κρίσιμο αγαθό. Η ομάδα καθορίζει στη συνέχεια το βαθμό στον οποίο κάθε κατηγορία component αντέχει σε επιθέσεις δικτύου.

- Φάση 3: Ανάπτυξη στρατηγικών και σχεδίων ασφάλειας

Κατά τη διάρκεια αυτού του μέρους της αξιολόγησης, η ομάδα ανάλυσης εντοπίζει τους κινδύνους για τα κρίσιμα αγαθά του οργανισμού και αποφασίζει τι πρέπει να κάνει για αυτά. Η ομάδα δημιουργεί μια στρατηγική προστασίας για την οργάνωση και ένα σχέδιο μετριασμού κινδύνου (mitigation plan) έτσι ώστε να αντιμετωπίσει τους κινδύνους για τα κρίσιμα αγαθά, με βάση την ανάλυση των πληροφοριών που συγκεντρώθηκαν στα προηγούμενα στάδια.



Σχήμα 20: Οι 3 φάσεις της OCTAVE

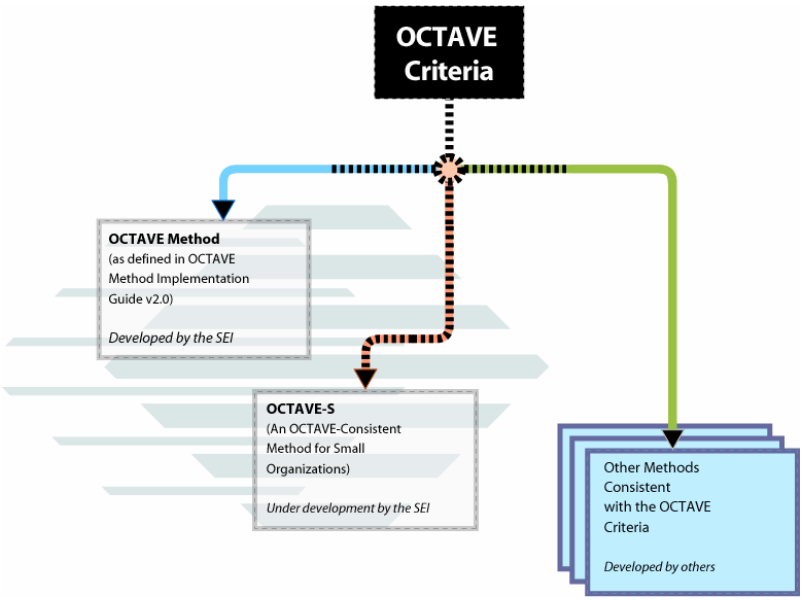
2.5.2 Οι διαδικασίες και τα κριτήρια της μεθοδολογίας OCTAVE

Τα πιο ουσιαστικά στοιχεία ή απαιτήσεις της προσέγγισης OCTAVE ενσωματώνονται σε ένα σύνολο από κριτήρια. Μπορούν να υπάρχουν πολλές μέθοδοι σύμφωνες με αυτά τα κριτήρια, αλλά υπάρχει μόνο ένα σύνολο κριτηρίων OCTAVE. Πιο συγκεκριμένα, δύο μέθοδοι είναι σύμφωνες με τα κριτήρια αυτά, η μέθοδος OCTAVE που σχεδιάστηκε με γνώμονα τους μεγάλους οργανισμούς, και η OCTAVE-S που αναπτύχθηκε για μικρούς οργανισμούς. Το σχήμα 21 παρακάτω απεικονίζει αυτά τα σημεία.

Τα κριτήρια OCTAVE είναι ένα σύνολο αρχών, χαρακτηριστικών και αποτελεσμάτων. Οι αρχές είναι οι θεμελιώδεις έννοιες που καθορίζουν την φιλοσοφία πίσω από αυτή διαδικασία αξιολόγησης. Διαμορφώνουν την προσέγγιση της αξιολόγησης και παρέχουν τη βάση για την διαδικασία της αποτίμησης των κινδύνων. Για παράδειγμα, η αυτό-κατεύθυνση είναι μία από τις αρχές της μεθοδολογίας OCTAVE. Η ιδέα της αυτό-κατεύθυνσης σημαίνει ότι οι άνθρωποι μέσα στον οργανισμό είναι σε καλύτερη θέση στο να οδηγήσουν την αξιολόγηση και τη λήψη αποφάσεων.

Οι απαιτήσεις της αξιολόγησης ενσωματώνονται στα στοιχεία και στα αποτελέσματα.Τα στοιχεία αυτά είναι οι διακριτές ιδιότητες ή τα χαρακτηριστικά της αξιολόγησης. Αυτές είναι και οι απαιτήσεις που ορίζουν τα βασικά στοιχεία της προσέγγισης OCTAVE και καθορίζουν τι είναι απαραίτητο για να πετύχει η αξιολόγηση.

Παρακάτω, στον πίνακα που ακολουθεί (σχήμα 22) παρουσιάζονται αναλυτικά οι διαδικασίες που ακολουθούνται ανά στάδιο στη μεθοδολογία OCTAVE.

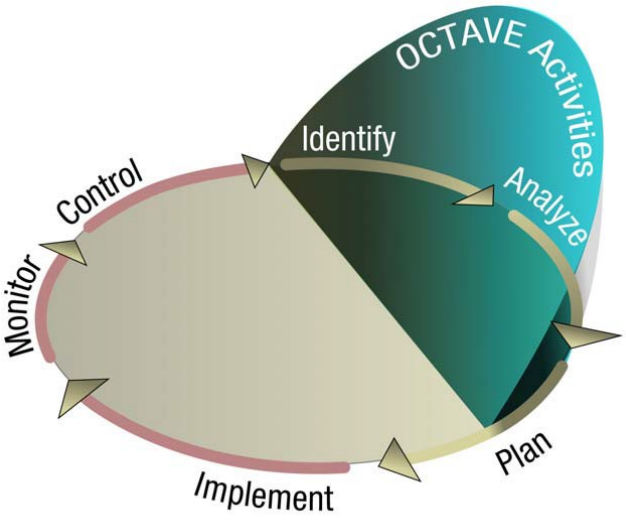


Σχήμα 21: Τα κριτήρια της μεθοδολογίας OCTAVE

Στάδιο	Διαδικασίες
1. Δημιουργία προφίλ απειλών βασισμένων σε αγαθά	1.1: Προσδιοριδμός γνώσης από το ανώτερο διευθυντικό προσωπικό
	1.2: Προσδιοριδμός γνώσης από το λειτουργικό διευθυντικό προσωπικό
	1.3: Προσδιοριδμός γνώσης από το απλό προσωπικό
	1.4: Δημιουργία προφίλ απειλών
2. Εντοπισμός των αδυναμιών της υποδομής	2.1: Προσδιοριδμός των κυρίων συνιστωσών της υποδομής
	2.2: Αξιολόγηση των επιλεγμένων συνιστωσών
3. Ανάπτυξη στρατηγικών και σχεδίων ασφάλειας	3.1: Διεξαγωγή ανάλυσης της επικινδυνότητας
	3.2: Ανάπτυξη στρατηγικών προστασίας

Σχήμα 22: Οι διαδικασίες ανά στάδιο της μεθοδολογίας OCTAVE

Μια αποτίμηση κινδύνων ασφάλειας πληροφοριών αποτελεί μέρος των δραστηριοτήτων ενός οργανισμού για τη διαχείριση των κινδύνων της ασφάλειας των πληροφοριών. Η μεθοδολογία OCTAVE είναι μια δραστηριότητα αξιολόγησης, όχι μια συνεχής διαδικασία. ‘Ετσι, έχει μια καθορισμένη αρχή και ένα καθορισμένο τέλος. Το σχήμα 23 δείχνει τη σχέση μεταξύ αυτών των δραστηριοτήτων. Αξίζει να σημειωθεί ότι οι δραστηριότητες διαχείρισης κινδύνου ορίζουν έναν κύκλο σχεδιασμού-εκτέλεσης-ελέγχου- πράξης (plan-do-check-act).



Σχήμα 23: Κύκλος plan-do-check-act της OCTAVE

2.6 Πρότυπο ISO/IEC 27005

Το πρότυπο ISO/IEC 27005 « Information Technology-Security Techniques-Information Security risk management » αποτελεί το πιο διαδεδομένο πρότυπο για τη διαχείριση των κινδύνων της ασφάλειας των πληροφοριακών συστημάτων ενός οργανισμού.

Πιο συγκεκριμένα, το διεθνές αυτό πρότυπο δε στοχεύει στο να παρέχει μια ακριβής καθοδήγηση σχετική με την υλοποίηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS), αλλά ούτε και στο να προτείνει κάποια συγκεκριμένη μεθοδολογία διαχείρισης κινδύνου σ'έναν οργανισμό. 'Ετσι, ο καθορισμός της διαχείρισης κινδύνου του οργανισμού εξαρτάται από τον ίδιο τον οργανισμό και μπορεί να επηρεάζεται για παράδειγμα από το έυρος του συστήματος ISMS, από τις ανάγκες και τους στόχους του οργανισμού ή από τον τομέα όπου δραστηριοποιείται ο οργανισμός αυτός.

Σε γενικές γραμμές, το πρότυπο ISO/IEC 27005 βασίζεται στη μεθοδολογία αναγώρισης κινδύνου η οποία πραγματοποείται με βάση την αναγνώριση του αγαθού, της απειλής και της ευπάθειας. Γι'αυτό και το πρότυπο αυτό, μπορεί να εφαρμοστεί από όλους τους οργανισμούς ανεξαρτήτου τύπου (π.χ. επιχειρήσεις εμπορικού χαρακτήρα, οργανισμοί κυβερνητικού χαρακτήρα, μη κερδοσκοπικούς οργανισμούς κλπ.), οι οποίοι στοχεύουν στο να διαχειστούν τους κινδύνους που σχετίζονται με την ασφάλεια των πληροφοριών του οργανισμού.

Το πρότυπο ISO/IEC 27005 για τη διαχείριση του κινδύνου προτείνει μια συνεχή διαδικασία που αποτελείται από μια δομημένη σειρά επαναληπτικών δραστηριοτήτων ως εξής:

- Καθιέρωση του πλαισίου διαχείρισης του κινδύνου (π.χ. το πεδίο εφαρμογής, οι υποχρεώσεις συμμόρφωσης, οι προσεγγίσεις / μέθοδοι που θα χρησιμοποιηθούν και οι σχετικές πολιτικές και κριτήρια όπως η ανοχή του οργανισμού στον κίνδυνο).
- Ποσοτική ή ποιοτική αξιολόγηση των σχετικών κινδύνων (π.χ. αναγνώριση, ανάλυση και εκτίμηση), λαμβάνοντας υπόψη τα πληροφοριακά αγαθά, τις απειλές, τους υφιστάμενους ελέγχους και τα τρωτά σημεία για τον προσδιορισμό της πιθανότητας συμβάντων και τις προβλεπόμενες συνέπειες για τους οργανισμούς εάν επρόκειτο να συμβούν. Ουσιαστικά, να καθορίσει ο οργανισμός ένα « επίπεδο κινδύνου ».
- Κατάλληλη αντιμετώπιση των κινδύνων δηλαδή τροποποίηση (με τη χρήση ελέγχων ασφάλειας πληροφοριών), διατήρηση (δηλαδή αποδοχή), αποφυγή ή/και εναπόθεση κινδύνου σε τρίτους], χρησιμοποιώντας τα « επίπεδα κινδύνου » που ορίστηκαν με σκοπό να τους δώσουν προτεραιότητα.
- Διαρκής ενημέρωση των ενδιαφερόμενων μερών καθόλη τη διάρκεια της διαδικασίας της διαχείρισης του κινδύνου.
- Παρακολούθηση και αναθεώρηση σε συνεχή βάση των κινδύνων, των επιλεγμένων αντίμετρων, των υποχρεώσεων και των αναγκών του οργανισμού, προσδιορίζοντας κατάλληλα τις σημαντικές αλλαγές.

Η ακολούθηση μιας συνεχούς διαδικασίας για τη διαχείριση της ασφάλειας πληροφοριών είναι απαραίτητη για τον εντοπισμό των στόχων του οργανισμού και για τη δημιουργία ενός αποτελεσματικού συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS). Η προσέγγιση αυτή πρέπει να ταιριάζει με το περιβάλλον του οργανισμού και πιο συγκεκριμένα, πρέπει να είναι συμβατή με τη διαχείριση του συνολικού κινδύνου του οργανισμού. Αξίζει να σημειωθεί ότι η διαχείριση των κινδύνων της ασφάλειας των πληροφοριών πρέπει να είναι αναπόστατο κομμάτι όλων των δραστηριοτήτων που σχετίζονται με την ασφάλεια των πληροφοριών.

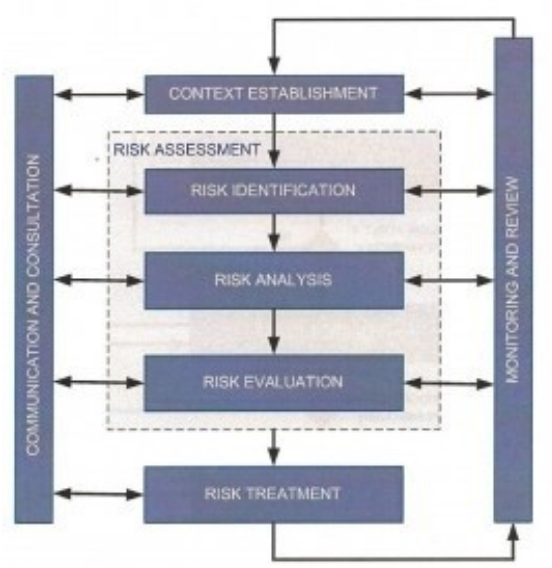
Όπως αναφέρθηκε παραπάνω και σύμφωνα με το πρότυπο ISO/IEC 27005 , η διαχείριση των κινδύνων της ασφάλειας των πληροφοριών πρέπει να είναι μια συνεχής διαδικασία. Η διαδικασία αυτή πρέπει να καθορίσει το εσωτερικό και εξωτερικό πλαίσιο του οργανισμού, να αξιολογήσει τους κινδύνους και να

αντιμετωπίσει τους κινδύνους χρησιμοποιώντας ένα σχέδιο αντιμετώπισης κινδύνου (risk treatment plan). Γενικά, η διαχείριση του κινδύνου περιγράφει το τι μπορεί να συμβεί και τις πιθανές επιπτώσεις αυτού, πριν αποφασιστεί τι πρέπει να γίνει και πότε, για να περιορίσει τον κίνδυνο σε ένα αποδεκτό επίπεδο.

Η διαχείριση των κινδύνων της ασφάλειας των πληροφοριών θα πρέπει να συμβάλλει στα ακόλουθα:

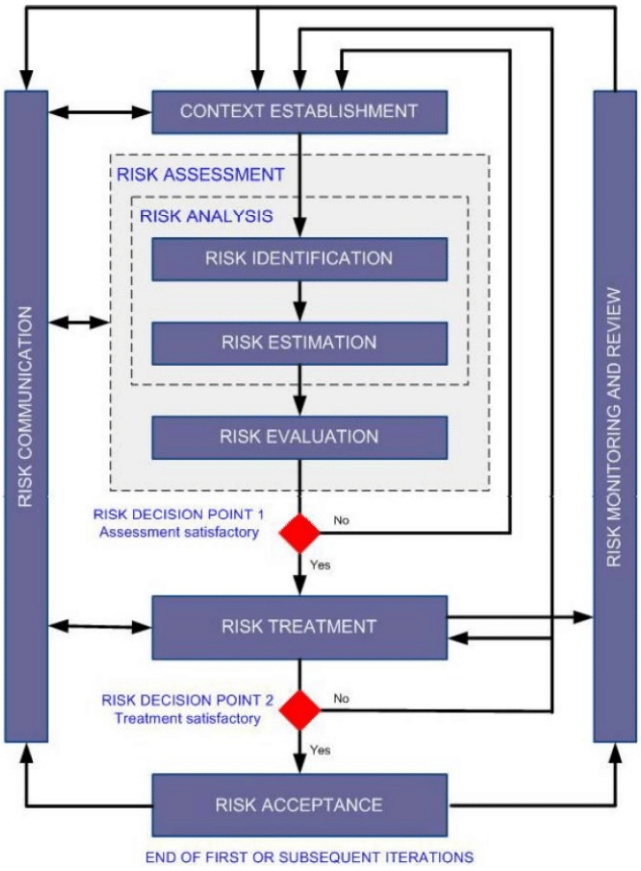
- Στην αναγνώριση των κινδύνων
- Στην αξιολόγηση των κινδύνων που εντοπίστηκαν ως προς τις επιπτώσεις τους στον οργανισμό και ως προς την πιθανότητα εμφάνισής τους
- Στη θέσπιση προτεραιοποιημένων κινδύνων και αντίστοιχων ενεργείων για την αντιμετώπισή τους
- Στη συμμετοχή των ενδιαφερόμενων μερών κατά τη λήψη αποφάσεων σχετικών με τη διαχείριση των κινδύνων και στην ενημέρωσή τους για την κατάσταση της διαχείρισης των κινδύνων
- Στην τακτική παρακολούθηση και επανεξέταση των κινδύνων που έχουν εντοπιστεί

Η διαδικασία της διαχείρισης των κινδύνων της ασφάλειας των πληροφοριών μπορεί να εφαρμοστεί στον οργανισμό ως σύνολο που περιλαμβάνει όλα τα διακριτά μέρη του οργανισμού (π.χ. ένα συγκεκριμένο τμήμα, μια υπηρεσία), όλες τις πληροφορίες του συστήματος και όλους τους υπαρκτούς μηχανισμούς ελέγχου (π.χ. business continuity planning). Στο παρακάτω σχήμα αποτυπώνεται η διαδικασία διαχείρισης των κινδύνων της ασφάλειας πληροφοριών σύμφωνα με τα παραπάνω αλλά και σύμφωνα με το πρότυπο ISO/IEC 27005:



Σχήμα 24: Διαδικασία διαχείρισης κινδύνων ασφάλειας πληροφοριών

Στο σχήμα που ακολουθεί, περιγράφεται πιο αναλυτικά πώς υλοποιείται η διαδικασία της διαχείρισης του κινδύνου σύμφωνα με το πρότυπο ISO/IEC 27005. Συγκεκριμένα, η διαδικασία αυτή αποτελείται από τον καθορισμό του πλαισίου του οργανισμού (εσωτερικό και εξωτερικό), από την αποτίμηση του κινδύνου, από την αντιμετώπιση του κινδύνου, από την αποδοχή του κινδύνου, από τη γνωστοποίηση του κινδύνου και από την παρακολούθησή του.



Σχήμα 25: Απεικόνιση της διαδικασίας διαχείρισης κινδύνου ασφάλειας πληροφοριών

'Οπως απεικονίζεται στο παραπάνω σχήμα , η διαδικασία διαχείρισης των κινδύνων της ασφάλειας πληροφοριών μπορεί να είναι επαναληπτική για την αποτίμηση του κινδύνου και για τις δραστηριότητες αντιμετώπισης του κινδύνου. Η επαναληπτική προσέγγιση της διεξαγωγής της αποτίμησης του κινδύνου καθιστά πιο αναλυτική και με μεγαλύτερη λεπτομέρεια την αποτίμηση σε κάθε επανάληψη. Επίσης, η επαναληπτική προσέγγιση προσδίδει μια καλή ισορροπία της ελαχιστοποίησης του χρόνου και της προσπάθειας που δαπανάται στον εντοπισμό των μέτρων αντιμετώπισης, ενώ διασφαλίζεται παράλληλα ότι οι υψηλοί κίνδυνοι αξιολογούνται κατάλληλα.

Στο πρώτο στάδιο, καθορίζεται το πλαίσιο του οργανισμού. Στη συνέχεια, διεξάγεται η αποτίμηση του κινδύνου. Σε περίπτωση που αυτό παρέχει επαρκείς πληροφορίες για τον αποτελεσματικό προσδιορισμό των απαιτούμενων ενεργειών για τη μείωση των κινδύνων σε αποδεκτό επίπεδο, τότε η εργασία αυτή ολοκληρώνεται και ακολουθεί η αντιμετώπιση των κινδύνων. Σε περίπτωση που οι πληροφορίες είναι ανεπαρκείς, διεξάγεται μια ακόμη επανάληψη της αποτίμησης κινδύνου με αναθεωρημένο πλαίσιο (π.χ.

κριτήρια αξιολόγησης κινδύνου, κριτήρια αποδοχής κινδύνου), ενδεχομένως σε περιορισμένα τμήματα του συνολικού πεδίου εφαρμογής.

Η αποτελεσματικότητα της αντιμετώπισης του κινδύνου εξαρτάται από τα αποτελέσματα της αποτίμησης του κινδύνου. Στο σημείο αυτό, αξίζει να σημειωθεί ότι η αντιμετώπιση του κινδύνου περιλαμβάνει μια κυκλική διαδικασία με τις παρακάτω ενέργειες:

- Αξιολόγηση της αντιμετώπισης του κινδύνου
- Απόφαση εάν είναι αποδεκτά τα υπολειπόμενα επίπεδα κινδύνου
- Δημιουργώντας ενός νέου πλάνου αντιμετώπισης κινδύνου εάν τα επίπεδα κινδύνου δεν είναι αποδεκτά και
- Αξιολόγηση της αποτελεσματικότητας της αντιμετώπισης του κινδύνου

Είναι πιθανόν η αντιμετώπιση του κινδύνου να μην οδηγήσει άμεσα σε ένα αποδεκτό επίπεδο εναπομείναντα κινδύνου. Σε αυτή την περίπτωση, μπορεί να απαιτηθεί μια ακόμη επανάληψη της αποτίμησης κινδύνου με διαφορετικές παραμέτρους πλαισίου (π.χ. αποτίμηση κινδύνου, αποδοχή κινδύνου ή κριτήρια επιπτώσεων), ακολουθούμενη από περαιτέρω αντιμετώπιση κινδύνου (βλ. Σχήμα 25 Risk Decision point 2).

Η δραστηριότητα αποδοχής του κινδύνου (risk acceptance activity) πρέπει να διασφαλίζει ότι οι εναπομείναντες κίνδυνοι γίνονται ρητά αποδεκτοί από τη Διοίκηση του οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σε μια κατάσταση όπου η εφαρμογή των ελέγχων/μέτρων αντιμετώπισης παραλείπεται ή αναβάλλεται (π.χ. λόγω κόστους).

Κατά τη διάρκεια ολόκληρης της διαδικασίας διαχείρισης κινδύνων για την ασφάλεια πληροφοριών, είναι σημαντικό οι κίνδυνοι και η αντιμετώπισή τους να κοινοποιούνται στα κατάλληλα πρόσωπα. Ακόμη και πριν από την αντιμετώπιση των κινδύνων, οι πληροφορίες σχετικά με τους εντοπισμένους κινδύνους μπορούν να είναι πολύτιμες για τη διαχείριση περιστατικών και μπορούν να συμβάλουν στη μείωση των πιθανών επιπτώσεων. Η ευαισθητοποίηση για τους κινδύνους από τη Διοίκηση, η φύση των ελέγχων που εφαρμόζονται για τον μετριασμό των κινδύνων και οι τομείς που απασχολούν τον οργανισμό συμβάλλουν στην αντιμετώπιση των περιστατικών κατά τον πλέον αποτελεσματικό τρόπο. Πρέπει να τεκμηριώνονται τα λεπτομερή αποτελέσματα κάθε δραστηριότητας της διαδικασίας διαχείρισης κινδύνου της ασφάλειας και των δύο κομβικών σημείων λήψης αποφάσεων σχετικά με τον κίνδυνο (βλ. Σχήμα 25).

Το πρότυπο ISO / IEC 27005 ορίζει ότι οι έλεγχοι που εφαρμόζονται στο πεδίο εφαρμογής, τα όρια και το πλαίσιο του ISMS πρέπει να βασίζονται στον κίνδυνο. Η εφαρμογή μιας διαδικασίας διαχείρισης κινδύνων ασφάλειας πληροφοριών μπορεί να ικανοποιήσει αυτήν την απαίτηση. Σε γενικές γραμμές, υπάρχουν πολλές προσεγγίσεις με τις οποίες μπορούν να καθοριστούν οι έλεγχοι για την εφαρμογή των επιλεγμένων τρόπων αντιμέτωπισης του κινδύνου.

3 ΚΕΦΑΛΑΙΟ 3: Ταξονομίες και Πρότυπα Απειλών

3.1 Εισαγωγή στις ταξονομίες απειλών

Κατά τη διεξαγωγή της αποτίμησης κινδύνου, όπως είδαμε και σε προηγούμενα κεφάλαια, στο στάδιο της ανάλυσης των κινδύνων γίνεται αποτίμηση των απειλών που βρέθηκαν για μία λίστα από αγαθά του υπό μελέτη οργανισμού. Οι απειλές αυτές προκειμένου να μελετηθούν και να αντιμετωπιστούν αποτελεσματικά, θα πρέπει να ταξινομούνται σε συγκεκριμένες κατηγορίες, έτσι ώστε να μπορούν να μελετηθούν ευκολότερα από την εκάστοτε ομάδα ανάλυσης.

Πιο συγκεκριμένα, οι ταξονομίες απειλών ανταποκρίνονται στην ανάγκη να διατίθεται μια κοινή « γλώσσα » για τη μεταφορά απειλών στα πληροφοριακά συστήματα που θα μπορούσαν να οδηγήσουν σε επιθέσεις στον κυβερνοχώρο ή περιστατικά κυβερνοχώρου οποιασδήποτε φύσης. Αρχικά, οι ταξονομίες απειλών αναπτύχθηκαν ως ένα εσωτερικό εργαλείο από διάφορους οργανισμούς που σχετίζονται με τις τεχνολογίες της πληροφορίας και της επικοινωνίας, οι οποίοι χρησιμοποιούνται στη συλλογή και την ενοποίηση των πληροφοριών απειλής.

Σε γενικές γραμμές, στο τεράστιο πεδίο των ΤΠΕ και της επιστήμης των υπολογιστών, υπάρχουν πολλοί τρόποι ταξινόμησης των απειλών στον κυβερνοχώρο που εξαρτώνται από πολλούς παράγοντες, ‘Ετσι, οι υπάρχουσες ταξονομίες περιστατικών ανήκουν σε μία από τις ακόλουθες ομάδες:

- Ειδικές ταξονομίες που αναπτύσσονται από μεμονωμένες ομάδες CERT (Computer Emergency Response Team)
- Παγκόσμιες, διεθνώς αναγνωρισμένες ταξονομίες

Αρκετές εθνικές ομάδες CERT ανέπτυξαν τον τρόπο τους για να ταξινομήσουν τις διάφορες απειλές στον κυβερνοχώρο, μερικές μόνο βασισμένες σε επιθέσεις ασφάλειας του Διαδικτύου (όπως αυτή που αναπτύχθηκε από τη Λετονική CERT NIC.LV, αποτελούμενη από έντεκα τύπους επιθέσεων), βασισμένες πιθανώς στις εμπειρίες της ομάδας. Άλλες ταξινομίες καθορίζονται σύμφωνα με το ποιος ανέφερε το περιστατικό, όπως στην περίπτωση της ομάδας CERT-Ουγγαρίας, η ταξινόμηση της οποίας αποτελείται από τέσσερις μόνο κατηγορίες (περιστατικά που αναφέρθηκαν από 1-Εθνικό CIIP, 2-CIIP εταίρων με SLA, 3-Διεθνές εταίροι, 4 συνεργαζόμενες οργανώσεις). Η αξία αυτών των ιδιόκτητων ταξινομιών είναι ότι μεγιστοποιούν τη συσχέτιση με τις ανάγκες και τις προσδοκίες της ομάδας, αλλά δεν συμφωνούν καθολικά ούτε είναι συγκρίσιμες με άλλες ταξινομίες.

Στην επόμενη ενότητα ακολουθεί περιγραφή διαφορετικών ταξονομιών απειλών, συμπεριλαμβανομένων ορισμένων διεθνώς συμφωνημένων και άλλων που αναπτύχθηκαν μέσω ευρωπαϊκών έργων.

3.2 Υπάρχουσες ταξονομίες απειλών

3.2.1 Ταξονομία απειλών ENISA

Ο Οργανισμός Πληροφοριών για το Δίκτυο και την Ασφάλεια της Ευρωπαϊκής Ένωσης (ENISA) δημοσίευσε την αρχική του έκδοση (1.0) για την ταξονομία των απειλών τον Ιανουάριο του 2016. Σε αυτή την ταξονομία, οι απειλές στον κυβερνοχώρο θα πρέπει να νοηθούν ως απειλές για τα αγαθά που σχετίζονται με την τεχνολογία της πληροφορίας και της επικοινωνίας. Τέτοιες απειλές υλοποιούνται κυρίως στον κυβερνοχώρο, ενώ ορισμένες απειλές περιλαμβάνονται στην πραγματικότητα στον φυσικό κόσμο αλλά επηρεάζουν τις πληροφορίες και τα αγαθά του κυβερνοχώρου. Αξίζει να σημειωθεί ότι η ταξονομία αυτή διατηρείται κυρίως μόνο για απειλές στον κυβερνοχώρο.

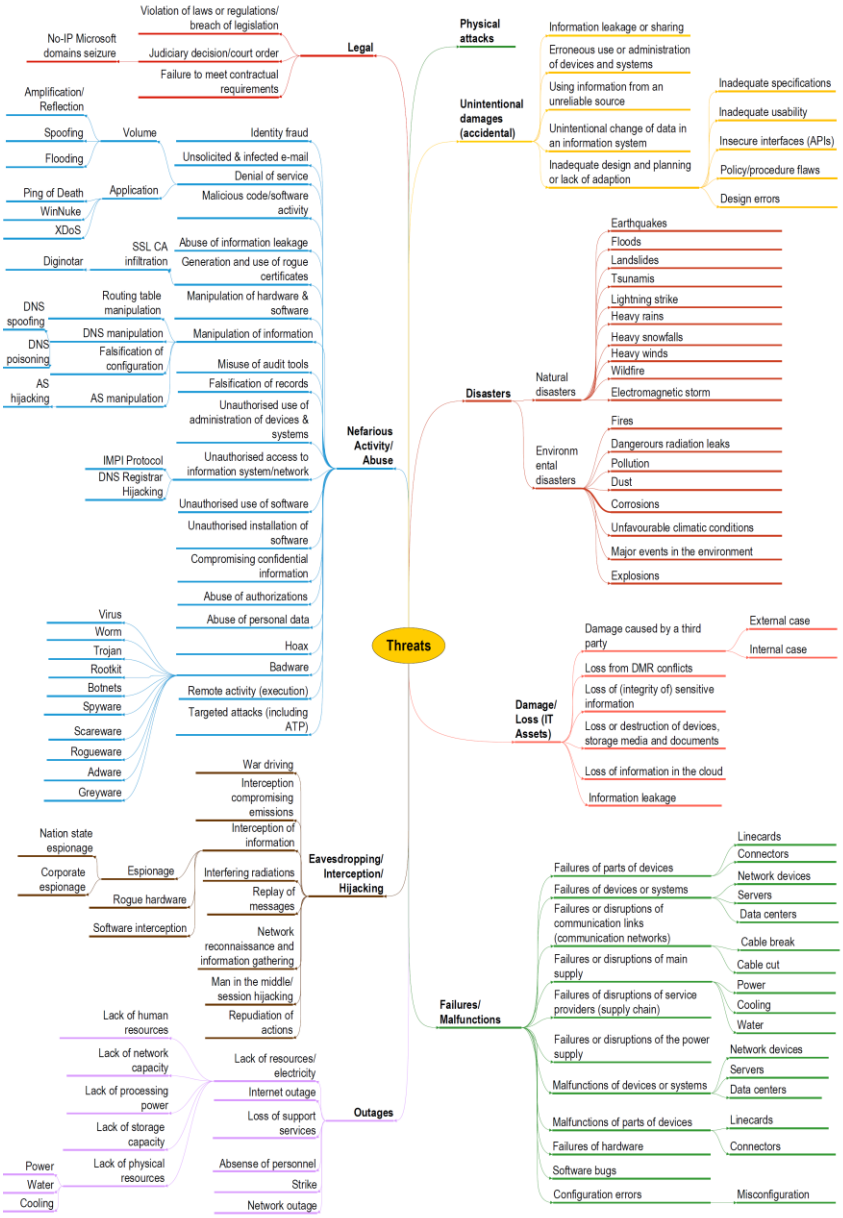
Η ταξονομία απειλών του ENISA έχει βασιστεί σε προηγούμενα έγγραφα ENISA, σε whitebooks, σε άλλες ταξονομίες και καταλόγους απειλών, ακόμη και σε έργα της ΕΕ όπως το Forward ή το VITA.

Θεωρείται ότι είναι έργο σε εξέλιξη, το οποίο θα επικυρωθεί και θα εμπλουτιστεί με πρόσθετες πληροφορίες.

Η ταξινόμηση απειλών που αναπτύχθηκε από τον ENISA αποτελείται από τα παρακάτω τρία πεδία:

- Απειλές υψηλού επιπέδου: Η κατηγορία απειλών υψηλού επιπέδου που χρησιμοποιείται για τη διάκριση διαφορετικών οικογενειών απειλών.
- Απειλές: Οι διάφορες απειλές σε μια οικογένεια / κατηγορία.
- Λεπτομέρειες απειλών: Περιγραφή των λεπτομερειών μιας συγκεκριμένης απειλής, με βάση συγκεκριμένο τύπο ή μέθοδο επίθεσης ή στόχευση συγκεκριμένου αγαθού.

Στο σχήμα που ακολουθεί αποτυπώνεται η ταξονομία απειλών του ENISA με βάση τα παραπάνω πεδία:



Σχήμα 26: Ταξονομία απειλών ENISA

Οι περιπτώσεις χρήσης για την ταξινόμηση απειλών περιελάμβαναν: i) Φάση συλλογής, στην οποία συνδέονται διάφορα ευρήματα κάτω από μια κοινή απειλή, ii) Φάση ταξινόμησης / ενοποίησης όπου η απειλή και οι περισσότερες πληροφορίες που συγκεντρώνονται, υπόκεινται σε περαιτέρω ομαδοποίηση, ανάλυση και ιεράρχηση και iii) Φάση έκθεσης, στην οποία οι απειλές μπορούν να αποδοθούν στα αγαθά. Παρακάτω ακολουθεί η αναλυτική ταξονομία απειλών που πρότεινε ο οργανισμός ENISA:

High level Threats	Threats	Threat details	Comments
Physical attack (deliberate/ intentional)			Threats of intentional, hostile human actions.
	Fraud		Fraud committed by humans.
		Fraud committed by employees	Fraud committed by employees or others that are in relation with entities, who have access to entities' information and IT assets.
	Sabotage		Intentional actions (non-fulfillment or defective fulfillment of personal duties) aimed to cause disruption or damage to IT assets
	Vandalism		Act of physically damaging IT assets.
	Theft (of devices, storage media and documents)		Stealing information or IT assets. Robbery.
		Theft of mobile devices (smartphones/ tablets)	Taking away another person's property in the form of mobile devices, for example smartphones, tablets.
		Theft of fixed hardware	Taking away another person's hardware property (except mobile devices), which often contains business-sensitive data
		Theft of documents	Stealing documents from private/company archives, often for the purpose of re-sale or to achieve personal benefits.
		Theft of backups	Stealing media devices, on which copies of essential information are kept.
	Information leak /sharing		Sharing information with unauthorised entities. Loss of information confidentiality due to intentional human actions (e.g., information leak may occur due to loss of paper

			copies of confidential information).
	Unauthorized physical access / Unauthorised entry to premises		Unapproved access to facility.
	Coercion, extortion or corruption		Actions following acts of coercion, extortion or corruption.
	Damage from the warfare		Threats of direct impact of warfare activities.
	Terrorist attack		Threats from terrorists.
Unintentional damage / loss of information or IT assets			Threats of unintentional human actions or errors
	Information leak /sharing due to human error		Information leak / sharing caused by humans, due to their mistakes.
		Accidental leaks/sharing of data by employees	Unintentional distribution of private or sensitive data to an unauthorized entity by a staff member.
		Leaks of data via mobile applications	Threat of leaking private data (a result of using applications for mobile devices).
		Leaks of data via Web applications	Threat of leaking important information using web applications.
		Leaks of information transferred by network	Threat of eavesdropping of unsecured network traffic.
	Erroneous use or administration of devices and systems	Information leak / sharing / damage caused by misuse of IT assets (lack of awareness of application features) or wrong / improper IT assets configuration or management.	
		Loss of information due to maintenance errors / operators' errors	Threat of loss of information by incorrectly performed maintenance of devices or systems or other operator activities.
		Loss of information due to configuration/ installation error	Threat of loss of information due to errors in installation or system configuration.
		Increasing recovery time	Threat of unavailability of information due to errors in the use of backup media and increasing information recovery time.
		Loss of information due to	Threat of unavailability of

		user errors	information or damage to IT assets caused by user errors (using IT infrastructure) or IT software recovery time.
	Using information from an unreliable source		Bad decisions based on unreliable sources of information or unchecked information.
	Unintentional change of data in an information system		Loss of information integrity due to human error (information system user mistake).
	Inadequate design and planning or improper adaptation		Threats caused by improper IT assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors).
	Damage caused by a third party	.	Threats of damage to IT assets caused by third party
		Security failure caused by third party	Threats of damage to IT assets caused by breach of security regulations by third party.
	Damages resulting from penetration testing		Threats to information systems caused by conducting IT penetration tests inappropriately.
	Loss of information in the cloud		Threats of losing information or data stored in the cloud.
	Loss of (integrity of) sensitive information		Threats of losing information or data, or changing information classified as sensitive.
		Loss of integrity of certificates	Threat of losing integrity of certificates used for authorization services.
	Loss of devices, storage media and documents		Threats of unavailability (losing) of IT assets and documents.
		Loss of devices/ mobile devices	Threat of losing mobile devices.
		Loss of storage media	Threat of losing data-storage media.
		Loss of documentation of IT Infrastructure	Threat of losing important documentation.
	Destruction of records		Threats of unavailability (destruction) of data and records (information) stored in devices and storage media.
		Infection of removable media	Threat of loss of important data due to using

			removable media, web or mail infection.
		Abuse of storage	Threat of loss of records by improper
Disaster (natural, environmental)			Threats of damage to information assets caused by natural or environmental factors.
	Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)		Large scale natural disasters.
	Fire		Threat of fire.
	Pollution, dust, corrosion		Threat of disruption of work of IT systems (hardware) due to pollution, dust or corrosion (arising from the air).
	Thunderstrike		Threat of damage to IT hardware caused by thunder strike (overvoltage).
	Water		Threat of damage to IT hardware caused by water.
	Explosion		Threat of damage to IT hardware caused by explosion.
	Dangerous radiation leak		Threat of damage to IT hardware caused by radiation leak.
	Unfavourable climatic conditions		Threat of disruption of work of IT systems due to climatic conditions that have a negative effect on hardware.
		Loss of data or accessibility of IT infrastructure as a result of heightened humidity	Threat of disruption of work of IT systems due to high humidity.
		Loss of data or accessibility of IT infrastructure as a result of very high temperature	Threat of disruption of work of IT systems due to high or low temperature.
	Threats from space / Electromagnetic storm		Threats of the negative impact of solar radiation to satellites and radio wave communication systems - electromagnetic storm.
	Wildlife		Threat of destruction of IT assets caused by animals: mice, rats, birds.
Failures/ Malfunction			Threat of failure/malfunction of IT supporting infrastructure (i.e. degradation of quality, improper working parameters, jamming). The cause of a failure is mostly an internal issue (e.g..

			overload of the power grid in a building).
	Failure of devices or systems		Threat of failure of IT hardware and/or software assets or its parts.
		Failure of data media	Threat of failure of data media.
		Hardware failure	Threat of failure of IT hardware.
		Failure of applications and services	Threat of failure of software/applications or services.
		Failure of parts of devices (connectors, plug-ins)	Threat of failure of IT equipment or its part.
	Failure or disruption of communication links (communication networks)		Threat of failure or malfunction of communications links.
		Failure of cable networks	Threat of failure of communications links due to problems with cable network.
		Failure of wireless networks	Threat of failure of communications links due to problems with wireless networks.
		Failure of mobile networks	Threat of failure of communications links due to problems with mobile networks.
	Failure or disruption of main supply		Threat of failure or disruption of supply required for information systems.
		Failure or disruption of power supply	Threat of failure or malfunction of power supply.
		Failure of cooling infrastructure	Threat of failure of IT assets due to improper work of cooling infrastructure.
	Failure or disruption of service providers (supply chain)	Threat of failure or disruption of third party services required for proper operation of information systems.	
	Malfunction of equipment (devices or systems)	Threat of malfunction of IT hardware and/or software assets or its parts (i.e. improper working parameters, jamming, rebooting).	
Outages			Threat of complete lack or loss of resources necessary for IT infrastructure. The cause of an outage is mostly an external issue (i.e electricity blackout in the whole city).

	Absence of personnel		Unavailability of key personnel and their competences.
	Strike		Unavailability of staff due to a strike (large scale absence of personnel).
	Loss of support services		Unavailability of support services required for proper operation of the information system.
	Internet outage		Unavailability of the Internet connection.
	Network outage		Unavailability of communication links.
		Outage of cable networks	Threat of lack of communications links due to problems with cable network.
		Outage of short-range wireless networks	Threat of lack of communications links due to problems with wireless networks (802.11 networks, Bluetooth, NFC etc.).
		Outages of long-range wireless networks	Threat of lack of communications links due to problems with mobile networks like cellular network (3G, LTE, GSM etc.) or satellite links.
Eavesdropping/ Interception/ Hijacking			Threats that alter communication between two parties. These attacks do not have to install additional tools/software on a victim's site.
	War driving		Threat of locating and possibly exploiting connection to the wireless network.
	Intercepting compromising emissions		Threat of disclosure of transmitted information using interception and analysis of compromising emission.
	Interception of information		Threat of interception of information which is improperly secured in transmission or by improper actions of staff.
		Corporate espionage	Threat of obtaining information secrets by dishonest means.
		Nation state espionage	Threats of stealing information by nation state espionage (e.g. China based

			governmental espionage, NSA from USA).
		Information leakage due to unsecured Wi-Fi, rogue access points	Threat of obtaining important information by insecure network rogue access points etc.
	Interfering radiation		Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted by an outside source.
	Replay of messages		Threat in which valid data transmission is maliciously or fraudulently repeated or delayed.
	Network Reconnaissance, Network traffic manipulation and Information gathering		Threat of identifying information about a network to find security weaknesses.
	Man in the middle/ Session hijacking		Threats that relay or alter communication between two parties.
Nefarious Activity/ Abuse			Threats of nefarious activities that require use of tools by the attacker. These attacks require installation of additional tools/software or performing additional steps on the victim's IT infrastructure/software.
	Identity theft (Identity Fraud/ Account)		Threat of identity theft action.
		Credentials-stealing trojans	Threat of identity theft action by malware computer programs.
	Receiving unsolicited E-mail		Threat of receiving unsolicited email which affects information security and efficiency.
		SPAM	Threat of receiving unsolicited, undesired, or illegal email messages.
		Unsolicited infected e-mails	Threat emanating from unwanted emails that may contain infected attachments or links to malicious / infected web sites
	Denial of service		Threat of service unavailability due to massive requests for

			services.
		Distributed denial of network service (DDoS) (network layer attack i.e. Protocol exploitation / Malformed packets / Flooding / Spoofing)	Threat of service unavailability due to a massive number of requests for access to network services from malicious clients.
		Distributed denial of application service (DDoS) (application layer attack i.e. Ping of Death / XDoS / WinNuke / HTTP Floods)	Threat of service unavailability due to massive requests sent by multiple malicious clients.
		Distributed DoS (DDoS) to both network and application services (amplification/reflection methods i.e. NTP/ DNS /…/ BitTorrent)	Threat of creating a massive number of requests, using multiplication/amplification methods
	Malicious code/ software/ activity		Threat of malicious code or software execution.
		Search Engine Poisoning	Threat of deliberate manipulation of search engine indexes.
		Exploitation of fake trust of social media	Threat of malicious activities making use of trusted social media.
		Worms/ Trojans	Threat of malware computer programs (trojans/worms).
		Rootkits	Threat of stealthy types of malware software.
		Mobile malware	Threat of mobile malware programs.
		Infected trusted mobile apps	Threat of using mobile malware software that is recognised as trusted one.
		Elevation of privileges	Threat of exploiting bugs, design flaws or configuration oversights in an operating system or software application to gain elevated access to resources.
		Web application attacks / injection attacks (Code injection: SQL, XSS)	Threat of utilizing custom web applications embedded within social media sites, which can lead to installation of malicious code onto computers to be used to gain unauthorized access.
		Spyware or deceptive adware	Threat of using software that aims to gather

			information about a person or organization without their knowledge.
		Viruses	Threat of infection by viruses.
		Rogue security software/ Rogueware / Scareware	Threat of internet fraud or malicious software that mislead users into believing there is a virus on their computer, and manipulates them to pay money for fake removal tool.
		Ransomware	Threat of infection of computer system or device by malware that restricts access to it and demands that the user pay a ransom to remove the restriction.
		Exploits/Exploit Kits	Threat to IT assets due to the use of web available exploits or exploits software.
	Social Engineering	Phishing attacks	Threat of an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy websites.
		Spear phishing attacks	Spear-phishing is a targeted e-mail message that has been crafted to create fake trust and thus lure the victim to unveil some business or personal secrets that can be abused by the adversary.
	Abuse of Information Leakage	Leakage affecting mobile privacy and mobile applications	Threat of leaking important information due to using malware mobile applications.
		Leakage affecting web privacy and web applications	Threat of leakage important information due to using malware web applications.
		Leakage affecting network traffic	Threat of leaking important information in network traffic.
		Leakage affecting cloud computing	Threat of leaking important information in cloud computing.
	Generation and use of rogue certificates	Loss of (integrity of) sensitive information	Threat of loss of sensitive information due to loss of integrity.

		Man in the middle/ Session hijacking	Threat of attack consisting in the exploitation of the web session control mechanism, which is normally managed by a session token.
		Social Engineering / signed malware	Threat of install fake trust signed software (malware) e.g. fake OS updates.
		Fake SSL certificates	Threat of attack due to malware application signed by a certificate that is typically inherently trusted by an endpoint.
	Manipulation of hardware and software		Threat of unauthorized manipulation of hardware and software.
		Anonymous proxies	Threat of unauthorised manipulation by anonymous proxies.
		Abuse of computing power of cloud to launch attacks (cybercrime as a service)	Threat of using large computing powers to generate attacks on demand.
		Abuse of vulnerabilities, 0-day vulnerabilities	Threat of attacks using 0-day or known IT assets vulnerabilities.
		Access of web sites through chains of HTTP Proxies (Obfuscation)	Threat of bypassing the security mechanism using HTTP proxies (bypassing the website blacklist).
		Access to device software	Threat of unauthorized manipulation by access to device software.
		Alternation of software	Threat of unauthorized modifications to code or data, attacking its integrity.
		Rogue hardware	Threat of manipulation due to unauthorized access to hardware.
	Manipulation of information		Threat of intentional data manipulation to mislead information systems or somebody or to cover other nefarious activities (loss of integrity of information)
		Repudiation of actions	Threat of intentional data manipulation to repudiate action.
		Address space hijacking (IP prefixes)	Threat of the illegitimate takeover of groups of IP addresses.
		Routing table manipulation	Threat of route packets of network to IP addresses other than that was intended via sender by unauthorised manipulation

			of routing table.
		DNS poisoning / DNS spoofing / DNS Manipulations	Threat of falsification of DNS information.
		Falsification of record	Threat of intentional data manipulation to falsify records.
		Autonomous System hijacking	Threat of overtaking by the attacker the ownership of a whole autonomous system and its prefixes despite origin validation.
		Autonomous System manipulation	Threat of manipulation by the attacker of a whole autonomous system in order to perform malicious actions.
		Falsification of configurations	Threat of intentional manipulation due to falsification of configurations.
	Misuse of audit tools		Threat of nefarious actions performed using audit tools (discovery of security weaknesses in information systems).
	Misuse of information/ information systems (including mobile apps)		Threat of nefarious action due to misuse of information / information systems.
	Unauthorized activities		Threat of nefarious action due to unauthorised activities.
		Unauthorised use or administration of devices and systems	Threat of nefarious action due to unauthorised use of devices and systems.
		Unauthorised use of software	Threat of nefarious action due to unauthorised use of software.
		Unauthorized access to the information systems / networks (IMPI Protocol / DNS Registrar Hijacking)	Threat of unauthorised access to the information systems / network.
		Network Intrusion	Threat of unauthorised access to network.
		Unauthorized changes of records	Threat of unauthorised changes of information.
	Unauthorized installation of software		Threat of unauthorised installation of software.
		Web based attacks (Drive-by download / malicious URLs / Browser based attacks)	Threat of installation of unwanted malware software by misusing websites
	Compromising confidential information (data breaches)		Threat of data breach.
	Hoax		Threat of loss of IT assets

			security due to cheating.
		False rumour and/or fake warning	Threat of disruption of work due to rumours and/or a fake warning.
	Remote activity (execution)		Threat of nefarious action by attacker remote activity.
		Remote Command Execution	Threat of nefarious action due to remote command execution.
		Remote Access Tool (RAT)	Threat of infection of software that has a remote administration capabilities allowing an attacker to control the victim's computer.
		Botnets / Remote activity	Threat of penetration by software from malware distribution.
	Targeted attacks (APTs etc.)		Threat of sophisticated, targeted attack which combine many attack techniques.
		Mobile malware	Threat of mobile software that aims to gather information about a person or organization without their knowledge .
		Spear phishing attacks	Threat of attack focused on a single user or department within an organization, coming from someone within the company in a position of trust and requesting information such as login, IDs and passwords.
		Installation of sophisticated and targeted malware	Threat of malware delivered by sophisticated and targeted software.
		Watering Hole attacks	Threat of malware residing on the websites which a group often uses.
	Failed business process		Threat of damage or loss of IT assets due to improperly executed business process.
	Brute force		Threat of unauthorised access via systematically checking all possible keys or passwords until the correct one is found.
	Abuse of authorizations		Threat of using authorised access to perform illegitimate actions.
Legal	***Violation of rules and regulations / Breach of***		Threat of financial or legal penalty or loss of trust of

	legislation		customers and collaborators due to violation of law or regulations.
	Failure to meet contractual requirements		Threat of financial penalty or loss of trust of customers and collaborators due to failure to meet contractual requirements.
		Failure to meet contractual requirements by third party	Threat of financial penalty or loss of trust of customers and collaborators due to a third party's failure to meet contractual requirements
	Unauthorized use of IPR protected resources		Threat of financial or legal penalty or loss of trust of customers and collaborators due to improper/illegal use of IPR protected material (IPR-Intellectual Property Rights.
		Illegal usage of File Sharing services	Threat of financial or legal penalty or loss of trust of customers and collaborators due to improper/illegal use of file sharing services.
	Abuse of personal data		Threat of illegal use of personal data.
	Judiciary decisions/court order		Threat of financial or legal penalty or loss of trust of customers and collaborators due to judiciary decisions/court order.

Σχήμα 27: Ταξονομία απειλών ENISA – Αναλυτικός πίνακας

3.2.2 Ταξονομία απειλών WASC

Η ταξονομία απειλών WASC δημιουργήθηκε από τα μέλη της Κοινοπραξίας Εφαρμογών Ιστού σε μια προσπάθεια συνεργασίας για την αποσαφήνιση και την οργάνωση των απειλών για την ασφάλεια μιας ιστοσελίδας. Το έργο αυτό στοχεύει στην ανάπτυξη και την προώθηση της ορολογίας της βιομηχανίας για την περιγραφή αυτών των ζητημάτων, έτσι ώστε οποιοσδήποτε επαγγελματίας που σχετίζεται με την ασφάλεια ΠΣ να έχει τη δυνατότητα να αποκτήσει πρόσβαση σε μια κοινή « γλώσσα» και σε έναν κοινό « ορισμό » για τον τομέα ασφάλειας που σχετίζεται με το διαδίκτυο. Προς το παρόν είναι διαθέσιμη η έκδοση 2.0 της ταξινόμησης απειλών WASC, αν και η τελευταία ενημέρωσή της είναι από τον Ιανουάριο του 2010. Η ταξονομία αυτή περιγράφει τις επιθέσεις και τις αδυναμίες που μπορούν να οδηγήσουν σε εκμετάλλευση ενός ιστοτόπου, των δεδομένων του ή των χρηστών του από κακόβουλους.

Η ταξονομία WASC παρέχει δύο οπτικές, τη φάση απαρίθμησης και τη φάση ανάπτυξης (Enumeration and Development Phase). Κατά τη φάση της απαρίθμησης, εμφανίζονται οι επιθέσεις και οι αδυναμίες που φαίνεται να θέτουν σε κίνδυνο έναν ιστότοπο. Οι επιθέσεις ορίζονται ως « ένα σαφώς καθορισμένο σύνολο ενεργειών, το οποίο, εάν είναι επιτυχές, θα έχει ως αποτέλεσμα την αρνητική επίπτωση σε ένα αγαθό ή μια ανεπιθύμητη ενέργεια ». Οι αδυναμίες είναι ένας τύπος σφάλματος στο λογισμικό που υπό κατάλληλες συνθήκες θα μπορούσε να συμβάλει στην εισαγωγή ευπαθειών εντός αυτού του λογισμικού.

Στη συνέχεια, ακολουθεί ένας πίνακας που απαριθμεί τις επιθέσεις και τις αδυναμίες που μπορούν να οδηγήσουν σε εκμετάλλευση ενός ιστότοπου, των δεδομένων του ή των χρηστών του. Αυτό χρησιμεύει ως βάση για την ταξονομία WASC των απειλών:

Attacks	Weaknesses
Abuse of Functionality	Application Misconfiguration
Brute Force	Directory Indexing
Buffer Overflow	Improper Filesystem Permissions
Content Spoofing	Improper Input Handling
Credential/Session Prediction	Improper Output Handling
Cross-Site Scripting	Information Leakage
Cross-Site Request Forgery	Insecure Indexing
Denial of Service	Insufficient Anti-automation
Fingerprinting	Insufficient Authentication
Format String	Insufficient Authorization
HTTP Response Smuggling	Insufficient Password Recovery
HTTP Response Splitting	Insufficient Process Validation
HTTP Request Smuggling	Insufficient Session Expiration
HTTP Request Splitting	Insufficient Transport Layer Protection
Integer Overflows	Server Misconfiguration
LDAP Injection	
Mail Command Injection	
Null Byte Injection	
OS Commanding	
Path Traversal	
Predictable Resource Location	
Remote File Inclusion (RFI)	
Routing Detour	
Session Fixation	
SOAP Array Abuse	
SSI Injection	
SQL Injection	
URL Redirector Abuse	
XPath Injection	
XML Attribute Blowup	
XML External Entities	

XML Entity Expansion	
XML Injection	
XQuery Injection	

Σχήμα 28: Επιθέσεις και αδυναμίες ταξονομίας απειλών WASC

Η οπτική της φάσης ανάπτυξης επικεντρώνεται στο πού μπορεί να εμφανιστεί μια ευπάθεια κατά την περίοδο του κύκλου ανάπτυξης. Η πλήρης ταξονομία απειλών WASC παρουσιάζεται στον παρακάτω πίνακα:

Threat Type	Threat	Threat details
Attack	**Abuse of Functionality**	Abuse of Functionality is an attack technique that uses a web site's own features and functionality to attack itself or others.
Attack	**Brute Force**	A brute force attack is a method to determine an unknown value by using an automated process to try a large number of possible values.
Attack	**Buffer Overflow**	A Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold
Attack	**Content Spoofing**	Content Spoofing is an attack technique that allows an attacker to inject a malicious payload that is later misrepresented as legitimate content of a web application.
Attack	**Credential/Session Prediction**	Credential/Session Prediction is a method of hijacking or impersonating a web site user.
Attack	**Cross-Site Scripting**	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance.
Attack	**Cross-Site Request Forgery**	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim
Attack	**Denial of Service**	Denial of Service (DoS) is an attack technique with the intent of preventing a web site from serving normal user activity.
Attack	**Fingerprinting**	The most common methodology for attackers is to first footprint the target's web presence and enumerate as much information as possible.

Attack	**Format String**	Format String Attacks alter the flow of an application by using string formatting library features to access other memory space.
Attack	**HTTP Response Smuggling**	HTTP response smuggling is a technique to "smuggle" 2 HTTP responses from a server to a client, through an intermediary HTTP device that expects (or allows) a single response from the server.
Attack	**HTTP Response Splitting**	In the HTTP Response Splitting attack, there are always 3 parties (at least) involved: • Web server, which has a security hole enabling HTTP Response Splitting • Target - an entity that interacts with the web server perhaps on behalf of the attacker. Typically this is a cache server forward/reverse proxy), or a browser (possibly with a browser cache). • Attacker - initiates the attack
Attack	**HTTP Request Smuggling**	HTTP Request Smuggling is an attack technique that abuses the discrepancy in parsing of non RFC compliant HTTP requests between two HTTP devices (typically a front-end proxy or HTTP-enabled firewall and a back-end web server) to smuggle a request to the second device "through" the first device.
Attack	**HTTP Request Splitting**	HTTP Request Splitting is an attack that enables forcing the browser to send arbitrary HTTP requests, inflicting XSS and poisoning the browser's cache.
Attack	**Integer Overflows**	An Integer Overflow is the condition that occurs when the result of an arithmetic operation, such as multiplication or addition, exceeds the maximum size of the integer type used to store it. When an integer overflow occurs, the interpreted value will appear to have “wrapped around” the maximum value and started again at the

		minimum value, similar to a clock that represents 13:00 by pointing at 1:00.
Attack	**LDAP Injection**	LDAP Injection is an attack technique used to exploit web sites that construct LDAP statements from user-supplied input.
Attack	**Mail Command Injection**	Mail Command Injection is an attack technique used to exploit mail servers and webmail applications that construct IMAP/SMTP statements from user-supplied input that is not properly sanitized
Attack	**Null Byte Injection**	Null Byte Injection is an active exploitation technique used to bypass sanity checking filters in web infrastructure by adding URL-encoded null byte characters (i.e. %00, or 0x00 in hex) to the user-supplied data. This injection process can alter the intended logic of the application and allow malicious adversary to get unauthorized access to the system files.
Attack	**OS Commanding**	OS Commanding is an attack technique used for unauthorized execution of operating system commands.
Attack	**Path Traversal**	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory.
Attack	**Predictable Resource Location**	Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses via brute forcing an attacker can guess file and directory names not intended for public viewing.
Attack	**Remote File Inclusion (RFI)**	Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web applications.
Attack	**Routing Detour**	The WS-Routing Protocol (WS-Routing) is a protocol for exchanging SOAP messages from an initial message sender to an ultimate receiver,

		typically via a set of intermediaries.
Attack	**Session Fixation**	Session Fixation is an attack technique that forces a user's session ID to an explicit value. Depending on the functionality of the target web site, a number of techniques can be utilized to "fix" the session ID value.
Attack	**SOAP Array Abuse**	XML SOAP arrays are a common target for malicious abuse.
Attack	**SSI Injection**	SSI Injection (Server-side Include) is a server-side exploit technique that allows an attacker to send code into a web application, which will later be executed locally by the web server.
Attack	**SQL Injection**	SQL Injection is an attack technique used to exploit applications that construct SQL statements from user-supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database.
Attack	**URL Redirector Abuse**	URL redirectors represent common functionality employed by web sites to forward an incoming request to an alternate resource
Attack	**XPath Injection**	XPath Injection is an attack technique used to exploit applications that construct XPath (XML Path Language) queries from user-supplied input to query or navigate XML documents.
Attack	**XML Attribute Blowup**	XML Attribute Blowup is a denial of service attack against XML parsers. The attacker provides a malicious XML document, which vulnerable XML parsers process in a very inefficient manner, leading to excessive CPU load.
Attack	**XML External Entities**	This technique takes advantage of a feature of XML to build documents dynamically at the time of processing.
Attack	**XML Entity Expansion**	The XML Entity expansion attack, exploits a capability in XML DTDs that allows the creation of custom macros, called entities that can be used throughout a document.

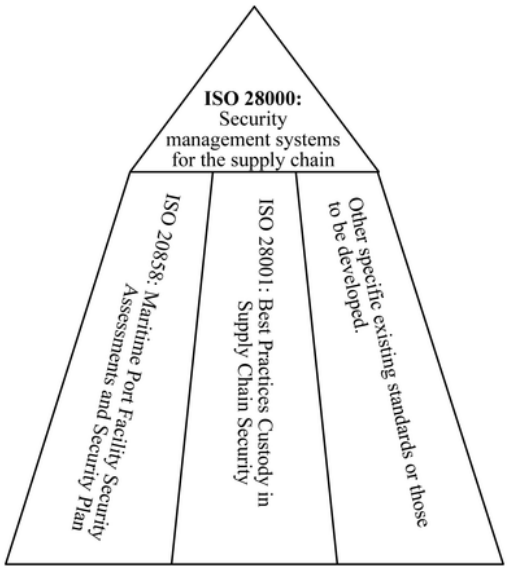
Attack	**XML Injection**	XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service
Attack	**XQuery Injection**	XQuery Injection is a variant of the classic SQL injection attack against the XML XQuery Language.
Weakness	**Insufficient Authentication**	Insufficient Authentication occurs when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate.
Weakness	**Insufficient Authorization**	Insufficient Authorization results when an application does not perform adequate authorization checks to ensure that the user is performing a function or accessing data in a manner consistent with the security policy
Weakness	**Insufficient Transport Layer Protection**	Insufficient transport layer protection allows communication to be exposed to untrusted third-parties, providing an attack vector to compromise a web application and/or steal sensitive information
Weakness	**Information Leakage**	Information Leakage is an application weakness where an application reveals sensitive data, such as technical details of the web application, environment, or user-specific data.
Weakness	**Improper Filesystem Permissions**	Improper filesystem permissions are a threat to the confidentiality, integrity and availability of a web application.
Weakness	**Improper Input Handling**	Improper input handling is one of the most common weaknesses identified across applications today. Poorly handled input is a leading cause behind critical vulnerabilities that exist in systems and applications.
Weakness	**Improper Output Handling**	Output handling refers to how an application generates outgoing data. If an application has improper output handling, the output data may be consumed leading to vulnerabilities and actions

		never intended by the application developer.
Weakness	**Insufficient Session Expiration**	Insufficient Session Expiration occurs when a Web application permits an attacker to reuse old session credentials or session IDs for authorization
Weakness	**Insecure Indexing**	Insecure Indexing is a threat to the data confidentiality of the web-site. Indexing web-site contents via a process that has access to files which are not supposed to be publicly accessible has the potential of leaking information about the existence of such files, and about their content.
Weakness	**Insufficient Password Recovery**	Insufficient Password Recovery is when a web site permits an attacker to illegally obtain, change or recover another user's password. Conventional web site authentication methods require users to select and remember a password or passphrase.

Σχήμα 29: Ταξονομία απειλών WASC

3.2.3 Πρότυπο ISO 28001: 2007 Συστήματα διαχείρισης ασφάλειας για την αλυσίδα εφοδιασμού

Σύμφωνα με το πρότυπο ISO 28001 για τα συστήματα διαχείρισης της ασφάλειας στην αλυσίδα εφοδιασμού, μια αλυσίδα εφοδιασμού (SC Supply Chain) είναι το σύνολο των πόρων και των διαδικασιών που αρχίζει με την παροχή πρώτων υλών και επεκτείνεται μέσω της παράδοσης προϊόντων ή υπηρεσιών στον πελάτη μέσω των διαφόρων μέσων μεταφοράς. Το πρότυπο αυτό παρέχει συγκεκριμένες οδηγίες για την εφαρμογή ενός συστήματος διαχείρισης της ασφάλειας για την αλυσίδα εφοδιασμού. Σκοπός του είναι να βοηθήσει τους οργανισμούς να καθιερώσουν λογικά επίπεδα ασφάλειας και να λαμβάνουν καλύτερες αποφάσεις με βάση τον κίνδυνο για την προστασία της αλυσίδας εφοδιασμού.



Σχήμα 30: Πρότυπο ISO 28001: 2007

Το πρότυπο ISO 28001: 2007 χρησιμοποιεί μια κατηγοριοποίηση απειλών με σαφή ορισμό που παρέχει συστηματικό ορισμό των κατηγοριών απειλών έτσι ώστε τα μεμονωμένα σενάρια απειλών μπορούν να προσδιοριστούν συστηματικά και να ταξινομηθούν για κάθε Υπηρεσία Εφοδιαστικής Αλυσίδας (SCS), με δομημένο και επαναλαμβανόμενο τρόπο. Επίσης, χάρη στο πρότυπο αυτό τα σενάρια απειλών μπορούν να χαρτογραφηθούν αποτελεσματικά στους κατάλληλους ελέγχους ασφάλειας και να αξιολογηθούν για την ευαισθησία τους σε κάθε επιχειρηματικό εταίρο που συμμετέχει στην Υπηρεσία Εφοδιαστικής Αλυσίδας. Ειδικότερα, όλα τα σενάρια απειλών χωρίζονται σε ακόλουθες κατηγορίες:

i. TC-1: Απειλές Υποδομών. Αυτή η κατηγορία περιλαμβάνει τις απειλές που αφορούν στα στοιχεία υποδομής ενός επιχειρηματικού εταίρου (κτήρια, πύλες, αποθήκες, κομμάτια, συστήματα CCTV κλπ.).
ii. TC-2: Απειλές Πληροφοριών και ΤΠΕ. Αυτή η κατηγορία περιλαμβάνει απειλές που στοχεύουν στα στοιχεία πληροφόρησης και ΤΠΕ ενός επιχειρηματικού εταίρου (δεδομένα, συστήματα, λογισμικό, υλικό κλπ.).
iii. TC-3: Απειλές που σχετίζονται με την ασφάλεια του προσωπικού. Αυτή η κατηγορία περιλαμβάνει απειλές οι οποίες επικεντρώνονται στον άνθρωπο.
iv. TC-4: Απειλές που σχετίζονται με την ασφάλεια των αγαθών και των μεταφορών. Με την έννοια « αγαθό » θεωρούμε οποιοδήποτε αντικείμενο, ανταλλάσσεται ή παραδίδεται μέσω της υπηρεσίας SC, π.χ. το φορτίο, τη μεταφορά και οποιεσδήποτε σχετικές επιχειρηματικές διαδικασίες.

v. TC-5: Άλλο. Στην κατηγορία αυτή υπόκεινται όλες οι άλλες απειλές με στόχο το ευρύτερο περιβάλλον SC, π.χ. οικονομικό περιβάλλον, εμπορική και πολιτική αστάθεια.

Πρέπει να σημειωθεί ότι για κάθε κατηγορία απειλών καθορίζονται συγκεκριμένα σενάρια απειλών, προκειμένου να βοηθηθούν οι εμπλεκόμενες οντότητες να εξετάσουν τα σενάρια απειλών που σχετίζονται με την υπό εξέταση υπηρεσία εφοδιαστικής αλυσίδας (SC). Σημειώστε ότι αυτή η κατηγοριοποίηση δεν είναι διακριτή και πολλά σενάρια απειλών μπορεί να ανήκουν εν μέρει σε περισσότερες από μία κατηγορίες.

3.2.4 Κατάλογος απειλών IT Grundsutz

Ο κατάλογος απειλών IT Grundschutz είναι μια μεθοδολογία που δημιουργήθηκε από το BSI (γερμανικά αρχικά για το Γερμανικό Ομοσπονδιακό Γραφείο για την Ασφάλεια Πληροφοριών). Σκοπός αυτής της μεθοδολογίας είναι να επιτευχθεί ένα κατάλληλο επίπεδο ασφάλειας για όλα τα είδη πληροφοριών ενός οργανισμού.

Το 2013 η IT Grundschutz παρείχε ένα μη τεχνικό κατάλογο 46 στοιχειωδών απειλών, τόσο φυσικών όσο και κυβερνητικών, συμπεριλαμβανομένων των περιγραφών των απειλών, παραδείγματα περιπτώσεων, αιτίες και συνέπειες των απειλών. Για παράδειγμα, για την απειλή « κοινωνική μηχανική », οι συγγραφείς παρέχουν τυπικές περιπτώσεις, όπως χειραγωγήσεις ατόμων με τηλεφωνήματα ή ανάπτυξη σχέσης με ένα στοχευόμενο θύμα.

Πολλά από τα παραδείγματα που παρέχονται σε αυτόν τον κατάλογο και ειδικά οι πιο συγκεκριμένες αιτίες των περιστατικών μπορούν να περιοριστούν σε πιο τεχνικούς όρους. Για παράδειγμα, η απώλεια της ακεραιότητας των ευαίσθητων πληροφοριών επισημαίνεται από τους συγγραφείς ότι προκαλείται από σφάλματα μετάδοσης ή/και από λανθασμένη εισαγωγή κακόβουλου λογισμικού.

Παρακάτω ακολουθεί ο ολοκληρωμένος κατάλογος απειλών IT Grundschutz:

High level Threats	Threat details - examples
Fire	
Unfavourable Climatic Conditions	
Water	
Pollution, Dust, Corrosion	
Natural Disasters	
Environmental Disasters	
Major Events in the Environment	
Failure or Disruption of the Power Supply	
Failure or Disruption of Communication Networks	
Failure or Disruption of Mains Supply	
Failure or Disruption of Service Providers	
Interfering Radiation	
Intercepting Compromising Emissions	
Interception of Information / Espionage	Many IT systems are protected against unauthorised access by identification and authentication mechanisms, e. g. in the form of user name and password verification. If the password is transmitted over the wire in an unencrypted form, it is under certain circumstances possible for an attacker to retrieve it.
	To be able to withdraw money out of an automatic teller machine, the correct PIN for the used electronic cash card or credit card must be entered. Unfortunately, the visual protection available for this equipment is frequently insufficient, so that an attacker can look over the shoulder of a customer entering the pin without much effort. If the attacker steals the card afterwards, he can plunder the account this way.
	To receive access rights to a PC or to otherwise manipulate it, an attacker can send the user a Trojan

	Horse which he has enclosed within an email as a supposedly useful program.
	In many offices, workplaces are not sufficiently protected in terms of acoustics. As a consequence, colleagues and also visitors could possibly listen to conversations and come to know information which is not meant for them or is even confidential.
Eavesdropping	In the case of telephone calls, it is not only eavesdropping on conversations that can be of interest to an attacker. The information which is transmitted in signalling can be misused by an attacker as well e. g. due to an incorrect setting in the terminal resulting in the password being transmitted in plain text at the time of login.
	An attacker can easily eavesdrop on the entire communication if wireless transmission is unprotected or insufficiently protected (e. g. if a WLAN is protected only with WEP).
	Emails can be read throughout their entire journey through the network if they are not encrypted. Unencrypted emails should therefore not be compared with conventional letters but with postcards.
Theft of Devices, Storage Media and Documents	A notebook computer disappeared from the U.S. Department of State in the spring of 2000. In an official statement, it was not ruled out that the device could contain confidential information. Nor was there information given as to whether the device was protected by cryptographic or other measures against unauthorised access.
	A German Federal Office was repeatedly broken into through the same unsecured windows. Mobile IT systems disappeared along with other valuables. It could not be ruled out without a doubt that files were copied or manipulated.
	There were a number of data leaks in Great Britain, in which confidential documents were disclosed because data storage media were stolen. In one case, several computer hard disks were stolen from the British Air Force which contained personal information, collected by employees for security screening purposes.
	An employee of a call centre prepared copies of a large set of confidential customer data shortly before he had to leave the company. After leaving the company, he then sold this data to competitors. Since details about the incident were then published by the press, the call centre lost many important customers

Loss of Devices, Storage Media and Documents	An employee uses the journey in the tramway to her workplace to read over some documents. When getting off the tram in a hurry at her destination stop, she leaves the documents inadvertently on her neighbouring place. Although the documents are not confidential, several signatures of high-profile executives must nevertheless be collected once again as a consequence.
	At a major event, while searching through his briefcase, an employee inadvertently drops a memory card with confidential calculations on the ground without noticing. The finder views its contents on his laptop and sells the information to the competition.
	A manufacturer sends CDs with software updates for bug fixing by post to his customers. Some of these CDs are lost in the post. Neither the sender nor the recipients are informed about it. As a consequence, the effected customers experience malfunctions in the software.
Bad Planning or Lack of Adaption	
Disclosure of Sensitive Information	
Information or Products from an Unreliable Source	
Manipulation of Hardware or Software	In a Swiss financial company, an employee had manipulated the software used for certain financial services. This made it possible for him to illegally gain large amounts of money.
	By manipulating ATMs, attackers succeeded several times to illegally read the data stored on payment cards. In conjunction with PINs spied out, this data was then misused to withdraw money at the expense of the cardholder.
Manipulation of Information	An employee was so annoyed at the promotion of her roommate in the accounting department that during the short absence of her colleague, she illegally gained access to her computer. Here she has caused, by changing some figures in the monthly balance sheet, enormous negative impact on the published financial results of the company.
Unauthorised Access to IT Systems	If a user ID and password have been spied out, any unauthorised use of the applications or IT systems protected by them is well possible.
	Using inadequately safeguarded remote maintenance access, hackers could gain unauthorised access to IT systems.
	When interfaces of active network components are inadequately safeguarded, it is possible that an attacker gains unauthorised access to the network

	component. If they also manage to overcome the local security mechanisms, e. g. obtain administrative privileges, they could perform all administrative activities.
	Many IT systems have interfaces for the use of interchangeable data storage, such as extra memory cards or USB storage media. In an unattended IT system with the corresponding hardware and software, there is a risk that large amounts of data can be retrieved or malicious software can be introduced this way.
Destruction of Devices or Storage Media	In a company an internal perpetrator used his knowledge about an important server being sensitive to too high operating temperatures and blocked the ventilation slits for the power supply fan using an object hidden behind the server. Two days later, the hard drive in the server suffered a temperature-caused defect, and the server was down for several days
	Humidity ingressing into an IT system, due to knocked-over coffee cups or watering the flowers can cause short circuits.
Failure of Devices or Systems	Firmware has been installed on an IT system which is not designed for this type of system. The IT system will then no longer start without errors and must be made operational by the manufacturer.
	A power failure in a memory system at the site of an Internet Service Provider (ISP) resulted in having to switch it off. Although the actual error could be corrected quickly, the affected IT systems could not start again due to inconsistencies in the file system. As a result, several Web servers operated by the ISP were not available for days.
Malfunction of Devices or Systems	
Lack of Resources	
Software Vulnerabilities or Errors	The most frequent warnings of the Computer Emergency Response Teams (CERTs) in recent years were related to security-relevant programming errors. These are errors made during programming of software which allow attackers to misuse it. A large proportion of these errors are caused by buffer overflows.
	Internet browsers are nowadays an important software component on clients. Browsers frequently do not only access the Internet but are also used for internal web applications in companies and public bodies. This is why software vulnerabilities or errors in browsers can impair information security overall particularly strongly.
Violation of Laws or Regulations	

Unauthorised Use or Administration of Devices and Systems	When examining log files, a network administrator came across inexplicable events occurring on different days but often early in the morning and in the afternoon. After a closer examination, it turned out that a wireless router was not configured properly. People waiting at the bus stop outside the office building have used this access to surf with their mobile devices on the Internet while waiting for the bus.
Incorrect Use or Administration of Devices and Systems	
Abuse of Authorisations	
Absence of Personnel	
Attack	In the 1980s, a bomb attack was perpetrated on the data centre of a large federal agency in Cologne. Due to the large penetrating power of the explosive device, not only windows and walls, but also many information systems in the data centre were destroyed.
	In the attack on the World Trade Center in New York on the 11th of September 2001, not only were many people killed but also were a number of IT facilities destroyed. As a result, several companies had considerable difficulty in continuing their business activities.
Coercion, Extortion or Corruption	
Identity Theft	To register with various email providers or auction platforms on the Internet, it sufficed to invent a fictitious name and to provide a suitable address from the phone book with it. At first, attackers could register using recognisable fictitious names, for example, derived from cartoon characters. As stronger plausibility checks were later introduced for this purpose, names, addresses and account numbers of real people have been used. Those affected have only learned about a fraud, when the first claims for payment arrived.
	The sender address of emails can be easily spoofed. It happens again and again that users are this way fooled into believing that an email comes from a trusted communication partner. Similar attacks are possible by manipulation of caller ID for voice calls or by manipulating the sender identity for fax connections.
	An attacker may use a masquerade to try to enter into an already existing connection without having to authenticate himself, since this step has already been performed by the original communication participants.
Reputation of Actions	An urgently needed spare part has been ordered electronically. After a week it is claimed still to be missing, in the meantime high losses due to

	production outage are incurred. The supplier denies having ever received an order.
Abuse of Personal Data	Personal data may be processed only for the purpose for which it was collected or stored for the first time. It is therefore inadmissible to use log files for attendance and monitoring conduct, if they were designed to store information on users' logging on to an IT system and logging off merely for access control.
	Persons who have access to personal data could disclose them in an unauthorised manner. For example, an employee at the front desk of a hotel could sell the guests' registration information to advertising companies.
Malicious Software	In the past, the malicious software W32/Bugbear was spread in two ways: it searched in local area networks for computers with shares, where write access was possible, and made copies of itself on each share found. Moreover, it sent itself as an HTML-email to recipients in the email address books of infected computers. Due to an error in the HTML routines of certain email programs, the malicious software was executed upon opening the message without further action by the recipient.
	The malicious software W32/Klez spread in different variants. Infected computers sent the virus to all recipients in the email address book of the computer. After this virus had infected a computer, by continuous manipulation of the operating system it prevented the installation of anti-virus programs from most popular manufacturers and made it significantly more difficult to perform disinfection of the infected computers.
Denial of Service	In spring 2007 in Estonia strong DoS attacks on numerous Internet sites over a prolonged period of time took place. This led to significant impairments in the use of information services and Internet services in Estonia.
Sabotage	In a mainframe computer centre, a manipulation of the uninterrupted power supply led to a temporary total failure. The perpetrator had repeatedly manually switched the uninterrupted power supply to bypass mode and then manipulated the main power supply of the building. Altogether there were four failures within three years. Even hardware was partially damaged. The disruption took between 40 and 130 minutes.
	Sanitary facilities were also located within a data centre. Due to blockage of the drains and the simultaneous opening of the water supply, water penetrated into central technology components.

	Damage caused this way resulted in interruptions of operation in the production system.
	Electronic archives present a particular risk of sabotage, since there, many sensitive documents are kept on a small floor space. Because of this aspect, by targeted unsophisticated manipulation a great deal of damage can be incurred under certain circumstances.
Replaying Messages	Replay attack: In a "replay attack" (replay of messages) attackers record valid messages and play this information at a later time almost unchanged.Also only part of a message may suffice, such as a password, to enter into an IT system without authorisation.
	Man-in-the-middle: In a "man-in-the-middle attack" the attacker assumes unnoticed a mediating position in the communication among various participants. In general, the attacker pretends here to be the sender of a message to the intended recipient, and he pretends to the recipient that he is the actual sender. If successful, the attacker can receive messages, which are not intended for him, evaluate them and purposefully manipulate them before they are forwarded to the intended recipient.
Unauthorised Entry to Premises	
Data Loss	
Loss of Integrity of Sensitive Information	

Σχήμα 31: Κατάλογος απειλών IT Grundschutz

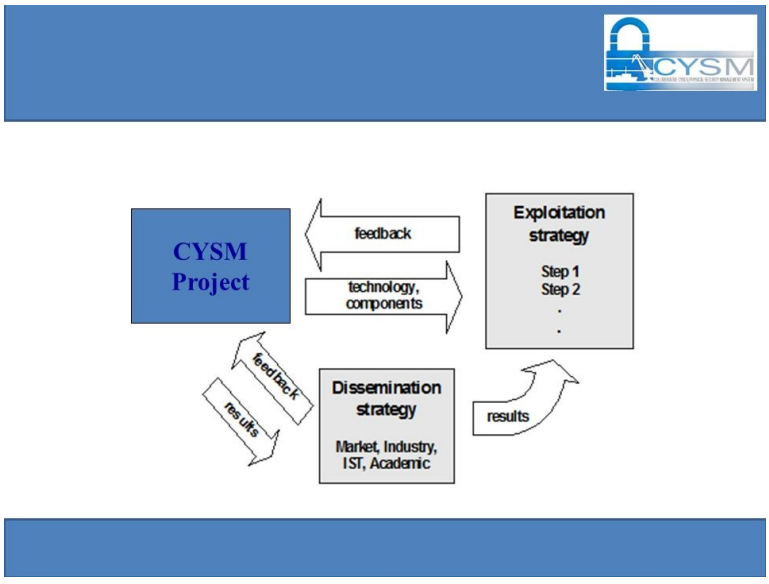
3.2.5 Κατάλογος απειλών για το έργο CYSM

Το CYSM (Collaborative Cyber/Physical Security Management System) όπως αναφέρθηκε και σε προηγούμενη ενότητα, είναι ένα έργο που συγχρηματοδοτείται από το πρόγραμμα πρόληψης, ετοιμότητας και διαχείρισης συνεπειών της τρομοκρατίας και άλλων σχετιζόμενων με την ασφάλεια κινδύνων της Ευρωπαϊκής Ένωσης, το οποίο αναπτύχθηκε μεταξύ 2013 και 2015. Το έργο αυτό στοχεύει στην παροχή μιας κοινής μεθοδολογίας διαχείρισης κινδύνων (CYSM-RM) για τους λιμένες που βασίζονται σε τεχνικές μοντελοποίησης και ομαδικής λήψης αποφάσεων, χρησιμοποιώντας τη συλλογική γνώση όλων των χρηστών, εκτιμώντας όλους τους κινδύνους (φυσικούς και σχετικούς με τον κυβερνοχώρο) σε διάφορους τύπους στόχων και με διάφορους τρόπους επίθεσης.

Το CYSM-RM εφαρμόστηκε μέσω ενός συνεργατικού συστήματος διαχείρισης της ασφάλειας (σύστημα CYSM) το οποίο επιτρέπει στους φορείς εκμετάλλευσης των λιμένων να μοντελοποιούν τα φυσικά και κυβερνητικά αγαθά και τις αλληλεξαρτήσεις, να αναλύει και να διαχειρίζεται εσωτερικές, εξωτερικές, και αλληλοεξαρτώμενες απειλές, αλλά και να αξιολογεί και να διαχειρίζεται τους φυσικούς και σχετικούς με τον κυβερνοχώρο κινδύνους σε σχέση με τις απαιτήσεις που καθορίζονται στον Κώδικα ISPS και στο πρότυπο ISO 27001.

Κατά τη διάρκεια της ανάπτυξης του έργου, πραγματοποιήθηκε μια δραστηριότητα για τον εντοπισμό απειλών και τρωτών σημείων. Η μεθοδολογία για τον εντοπισμό των απειλών βασίστηκε σε διάφορες γνωστές τεχνικές κατηγοριοποίησης απειλών (OCTAVE, CRAMM, NIST κ.λπ.). Το αποτέλεσμα είναι ένας μεγάλος αριθμός απειλών ομαδοποιημένων στις ακόλουθες κατηγορίες:

- Φυσικές απειλές όπως σεισμοί, πλημμύρες, τυφώνες, αστραπές
- Τεχνολογικές απειλές, όπως δυσλειτουργία υλικού
- Περιβαλλοντικές απειλές όπως ρύπανση, χημικές ουσίες
- Ανθρώπινες απειλές όπως επιθέσεις δικτύου, επιθέσεις ιών, μη εξουσιοδοτημένη πρόσβαση
- Οργανωμένη ή σκόπιμη επίθεση όπως τρομοκρατική επίθεση - Εκρηκτικός μηχανισμός, σαμποτάζ, εμπρησμός
- Απειλές σχετικά με τα δεδομένα, όπως η διαφθορά κακόβουλων δεδομένων, η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα



Σχήμα 32: Έργο CYSM

Οι ευπάθειες εντοπίστηκαν από προηγούμενους ελέγχους, από παγκόσμιους καταλόγους σε σχέση με τα τρωτά σημεία συγκεκριμένων αγαθών, από προηγούμενες δοκιμές διείσδυσης και άλλους διαθέσιμους πόρους. Το αποτέλεσμα ήταν ένας κατάλογος των ευπαθειών που σχετίζονται με τη συγκεκριμένη απειλή κάθε αγαθού. Τα προσδιορισθέντα αγαθά κατηγοριοποιήθηκαν ως εξής:

- Υποδομές ΤΠΕ
- Πληροφορίες και ηλεκτρονικά δεδομένα
- Φυσική υποδομή
- Λογισμικό (Software)
- Υλικό (Hardware)
- Οργάνωση τοποθεσίας

Επίσης, τα αντίμετρα (έλεγχοι) κατηγοριοποιήθηκαν σύμφωνα με την ακόλουθη ταξινόμηση:

- Γενικά
- Αποθαρρυντικά μέτρα και μέτρα καθυστέρησης. Συστήματα φυσικής προστασίας
- Ανίχνευση παράνομων ενεργειών και παρεμπόδιση εισβολής. Ηλεκτρονικά συστήματα προστασίας
- Παρακολούθηση βίντεο
- Συστήματα αναγνώρισης
- Μέτρα προστασίας δεδομένων
- Συστήματα απόκρισης
- Λειτουργίες του πλοίου και εγκαταστάσεις του τερματικού σταθμού

3.2.6 FORWARD Consortium Whitebook

Το κίνητρο του προγράμματος FORWARD για το 2010 ήταν να εντοπίσει σχετικές μελλοντικές απειλές που έχουν τη δυνατότητα να διακυβεύσουν την εμπιστευτικότητα και την ακεραιότητα των υποδομών των ευρωπαϊκών τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ). 28 απειλές σε 8 κατηγορίες συγκεντρώθηκαν με τη βοήθεια διεθνών εμπειρογνωμόνων, τόσο από τον ακαδημαϊκό χώρο όσο και από τη βιομηχανία, καθώς και με εργαστήρια και συζητήσεις για ενδεχόμενες απειλές, εστιάζοντας σε εκείνες τις απειλές που χρειάζονται άμεση προσοχή. Τρεις ομάδες μελέτησαν απειλές κακόβουλων προγραμμάτων και απάτης, αναδυόμενα έξυπνα περιβάλλοντα και κρίσιμα συστήματα. Όλες οι έρευνες διεξήχθησαν γύρω από τέσσερις άξονες: Νέες τεχνολογίες, νέες εφαρμογές, νέα επιχειρηματικά μοντέλα και νέα κοινωνική δυναμική.

Οι κατηγορίες απειλών υψηλού επιπέδου από τη FORWARD ήταν:

- Δικτύωση
- Υλικό και οπτικοποίηση
- Αδύναμες συσκευές
- Πολυπλοκότητα
- Οπτικοποίηση δεδομένων
- Χειραγώγηση δεδομένων
- Υποδομές επίθεσης
- Ανθρώπινοι παράγοντες
- Ανεπαρκείς απαιτήσεις ασφαλείας

Μετά τον προσδιορισμό, οι εμπειρογνώμονες κατέταξαν τις 28 απειλές με βάση τον επείγοντα χαρακτήρα τους για την ανάγκη μετριασμού τους. Η διαδικασία αυτή βασίστηκε σε τέσσερις παράγοντες: i) στη βαρύτητα της απειλής, ii) στη δυνατότητα εξάπλωσης της απειλής, iii) στην έλλειψη ευαισθητοποίησης στην κοινότητα και iv) στις υφιστάμενες προσπάθειες για το μετριασμό της απειλής. Βάσει αυτής της ανάλυσης, οι ακόλουθες πέντε απειλές θεωρήθηκαν ως οι πιο επείγουσες για να μετριαστούν:

1. Απειλές που σχετίζονται με τον παραλληλισμό: Ο κώδικας που γράφτηκε για παράλληλο προγραμματισμό ενδέχεται να μην είναι ασφαλής.
2. Απειλές που σχετίζονται με την κλίμακα: Υπάρχει αύξηση των συσκευών που είναι συνδεδεμένες σε ένα δίκτυο και του μεγέθους των πακέτων λογισμικού.
3. Υποδομές στήριξης της Υπόγειας Οικονομίας: Οι επιθέσεις στο Διαδίκτυο που προκαλούνται από την υπόγεια οικονομία έχουν αυξηθεί και η φύση τους δεν είναι πάντα εύκολη στην αποκρυπτογράφηση.
4. Κακόβουλο λογισμικό κινητής συσκευής: Υπάρχει μια ταχεία αύξηση του αριθμού τους και των κρίσιμων εφαρμογών που κατεβάζουν οι χρήστες (π.χ. e-banking).
5. Απειλές που σχετίζονται με τα κοινωνικά δίκτυα: Υπάρχει αύξηση στον αριθμό των χρηστών και των παρόχων κοινωνικών δικτύων που δεν παρέχουν επαρκή προστασία της ιδιωτικής ζωής.

Παρακάτω παρατίθεται ολόκληρος ο κατάλογος απειλών FORWARD Consortium Whitebook:

Threat Category	Threat	comments
Networking		Threats that are related to the introduction and deployment of new (often wireless) network technologies, but it also covers emerging threats against infrastructure services (routing, DNS) on the current Internet.

	Routing infrastructure	
	IPv6 and direct reachability of hosts	
	Naming (DNS) and registrars	
	Wireless communication	
	Denial of service	
Hardware and virtualization		Threats due to new hardware and software developments that allow computation to be moved to virtual computers, and ultimately, the cloud. It also covers malicious hardware.
	Malicious hardware	
	Virtualization and cloud computing	
Weak devices		Threats that are introduced with new computing devices that are limited, both computationally and because of power constraints. The problem is that security is "expensive," and weak devices might not be able to afford to implement and run adequate protection mechanisms.
	Sensors and RFID	
	Mobile device malware	
Complexity		Threats that emerge due to the fact that some future systems will contain billions of components. Another source of complexity are large monolithic systems that offer more and more functionality. The increased complexity leads to unexpected and unintended dependencies, interactions, and security consequences.
	Unforeseen cascading effects	
	Threats due to scale	
	System maintainability and verifiability	
	Hidden functionality	
	Threats due to parallelism	
Data Manipulation		Threats that stem from the fact that people (and systems) store more data online, and this data is becoming increasingly valuable and sensitive.
	Privacy and ubiquitous sensors	
	False sensor data	
	Threats related to social networks	
	Online games	
Attack infrastructures		Threats that are related to the fact that adversaries actively develop and deploy offensive platforms (such as botnets). That is, 7adversaries no longer perform hit-and-run attacks, but they establish operational bases on the Internet used to carry out malicious campaigns.
	Underground economy support structures	
	Advanced malware	
Human factors		Human factors always played a role in security. This category covers threats

		that are due to increasing concerns over insider attacks, especially in the context of outsourcing. The category also covers threats that are related to new social engineering attacks.
	User interface	
	The insider threat	
	Safety takes priority over security	
	New vectors to reach victims	
	Targeted attacks, spear phishing	
Insufficient security requirements		This category covers problems and threats related to legacy and commercial-off-the-shelf systems that have not been built with sufficient protection and are now used and deployed in scenarios for which their protection mechanisms are inadequate.
	Retrofitting security to legacy systems	
	Use of COTS components	
	Next generation networks	
Threats related to parallelism		Single processors have hit the CPU speed wall. However, Moore's law continues to hold, and processor manufacturers are now shipping machines with many CPU cores. These multi-cores need to be programmed, and the paradigm shift from sequential to parallel programming will likely bring a wide range of new vulnerability classes that we need to mitigate. Thus, we require new techniques to help developers write correct code and to detect bugs in parallel programs
Threats related to scale		The effects of scale can be felt everywhere on the Internet. This ranges from the sheer number of devices connected to the network to the size and complexity of individual software packages. We need ways to manage the complexity, scale, and security of such systems
Underground economy support structures		Many attacks on the Internet are driven and fueled by a thriving underground economy. This is the result of a paradigm shift from "hacking for fun" to "hacking for profit." Unfortunately, the mechanics of the underground economy and its support structures are poorly understood. However, it is necessary to study and actively combat the root cause that drives such diverse threats as botnets, phishing, and spam.
Mobile device malware		Malware is already a significant problem on today's Internet. Consider that the number of mobile devices is

		growing rapidly, users get more comfortable downloading and installing applications (e.g., via Apple's AppStore), and phones are increasingly used for critical applications.(e.g., for online banking). Thus, it is just a matter of time before mobile device malware will become mainstream. Unfortunately, mobile devices are constrained, both computationally and because of power limitations, making it hard to deploy costly, traditional anti-malware techniques. As a result, better malware defenses are crucially required for mobile devices.
Threats related to social networks		Social networks are regularly used byhundreds of millions of users who provide a wealth of private information online that could be abused. In addition, social network providers have been notoriously unwilling to provide sufficient privacy protection for their users, and they are looking for ways to monetize their audience and the data they upload. This is a dangerous combination that provides attackers with new ways to reach (and scam) victims, and it can lead to severe, large-scale data theft.

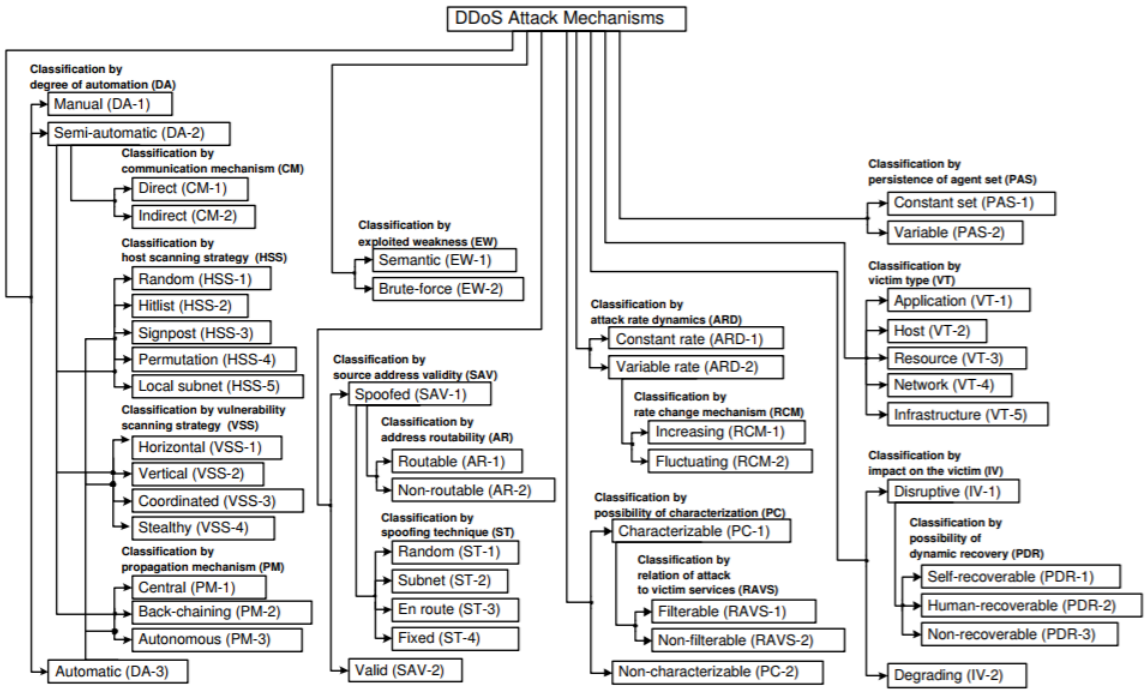
Σχήμα 33: Κατάλογος απειλών FORWARD Consortium Whitebook

3.2.7 Ταξονομία των μηχανισμών επίθεσης DDoS και άμυνας DDoS

Το 2004, οι Jelena Mircovic και Peter Reiher παρουσίασαν δύο ταξονομίες για την ταξινόμηση επιθέσεων και άμυνων στον εξειδικευμένο τομέα των επιθέσεων Distributed Denial of Service (DDoS). Τα βασικά κριτήρια για την ταξονομία των μηχανισμών επίθεσης ήταν τα κοινά στοιχεία που εντοπίστηκαν σε μία επίθεση αλλά και τα σημαντικά χαρακτηριστικά σε μια επίθεση. Από την άλλη πλευρά, οι μηχανισμοί άμυνας ταξινομούνται βάσει των αποφάσεων σχεδιασμού τους.

- **Επίθεση**

Όπως φαίνεται στο ακόλουθο σχήμα, οι συγγραφείς χρησιμοποίησαν οκτώ διαστάσεις για να ταξινομήσουν τις επιθέσεις DDos, μερικές από τις οποίες περιέχουν και δευτερεύουσες κατηγορίες:



Σχήμα 34: Ταξονομία των μηχανισμών επίθεσης DDoS

Οι κατηγοριοποιήσεις στις οποίες ταξινομήθηκαν οι μηχανισμοί επίθεσης DDoS είναι οι παρακάτω:

1. Βαθμός αυτοματισμού

Η πρώτη ταξινόμηση που προτείνεται είναι από το βαθμό αυτοματισμού, αναφορικά με το αν η επίθεση γίνεται χειρωνακτικά ή αυτόματα. Μετά, κάθε επίθεση χαρακτηρίζεται περαιτέρω με βάση τον μηχανισμό επικοινωνίας μεταξύ του πράκτορα και του χειριστή. Έτσι, οι επιθέσεις μπορούν να είναι χειροκίνητες, ημιαυτόματες ή αυτόματες.

Σε περίπτωση ημιαυτόματης επίθεσης, οι επιθέσεις χαρακτηρίζονται επίσης από:

- Μηχανισμό Επικοινωνίας, ο οποίος είναι είτε άμεσος είτε έμμεσος
- Στρατηγική Σάρωσης Host. Αναφέρεται στην επιλογή ευάλωτων μηχανών
- Στρατηγική σάρωσης ευπάθειας. Αναφέρεται στη στόχευση των τρωτών σημείων εντός των ευάλωτων μηχανών.
- Μηχανισμό διάδοσης

2. Σημασιολογική ή Brute Force

    - Σημασιολογική: εκμετάλλευση ενός συγκεκριμένου χαρακτηριστικού ή αδυναμίας
    - Brute Force: παρέχει πολύ μεγάλο όγκο επισκεψιμότητας σε ένα στοχευμένο δίκτυο

3. Σύμφωνα με την εγκυρότητα της διεύθυνσης προέλευσης, έχοντας υπόψη το πλεονέκτημα που διατηρεί ένας εισβολέας εάν πλαστογραφεί τη διεύθυνσή του. Η Spoofed Source Address ταξινομείται περαιτέρω από τη δυνατότητα διευθυνσιοδότησης διευθύνσεων και από την τεχνική spoofing (Address Routability and Spoofing Technique).

4. Στη συνέχεια, οι επιθέσεις χαρακτηρίζονται από το ρυθμό δυναμικής τους, που είναι σταθερός ή μεταβλητός. Στην περίπτωση του μεταβλητού ρυθμού, μπορεί τότε να αυξάνεται ή να κυμαίνεται.

5. Οι επιθέσεις μπορούν επίσης να χαρακτηριστούν ή όχι. Αυτό συμβαίνει σε επίπεδο πακέτων και ο χαρακτηρισμός μπορεί να οδηγήσει σε καλύτερο φιλτράρισμα.

6. Μια άλλη κατηγοριοποίηση είναι από το Persistence of Agent Set, το οποίο αναφέρεται στις εντολές που εμφανίζονται κατά τη διάρκεια της επίθεσης. 'Ετσι:
    - Το σταθερό σύνολο παραγόντων σημαίνει ότι οι επιθέσεις είναι ίδιου τύπου και συμβαίνουν με τον ίδιο ρυθμό.
    - Σύνολο μεταβλητών παραγόντων σημαίνει ότι η επίθεση είναι πιο πολύπλοκη και απρόβλεπτη και ο στρατός στον οποίο τα τάγματα επιτίθενται βρίσκεται σε διαφορετικό τόπο και χρόνο.

7. Επιπλέον, οι συγγραφείς ταξινομούν τις επιθέσεις και με βάση τον τύπο θύματος, οι οποίες περιλαμβάνουν τα εξής:
    - Εφαρμογή (Application)
    - Υποδοχή (Host)
    - Επιθέσεις πόρων (Resource Attacks)
    - Επιθέσεις δικτύου (Network Attacks)
    - Υποδομή (Infrastructure)

8. Η τελευταία κατηγοριοποίηση των επιθέσεων DDoS είναι με βάση το αντίκτυπο που έχει η επίθεση στο θύμα. Το « καταστροφικό » αντίκτυπο κατηγοριοποιείται περαιτέρω ανάλογα με τη δυνατότητα δυναμικής αποκατάστασης από τον εαυτό του, από τον άνθρωπο ή αν είναι μη ανακτήσιμο.

- **Άμυνα**

Οι αμυντικοί μηχανισμοί των επιθέσεων DDoS χαρακτηρίζονται από τα παρακάτω:

1. Επίπεδο δραστηριότητας

    Η διάκριση αυτή επικεντρώνεται στην προληπτική και αντιδραστική άμυνα (preventive and reactive)

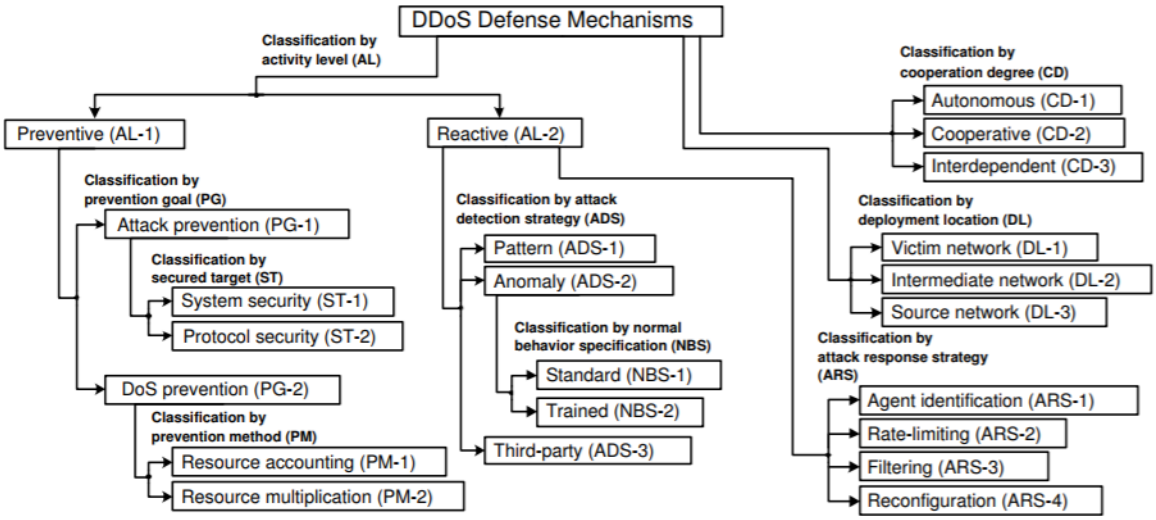
2. Βαθμός συνεργασίας

    Στον αμυντικό μηχανισμό αυτό, οι στοχοθετημένες οντότητες μπορούν να συνεργαστούν ή όχι με άλλες οντότητες. Με βάση αυτή τη διάκριση, οι συγγραφείς απαριθμούν αυτόνομους, συνεργατικούς και αλληλένδετους μηχανισμούς.

3. Τοποθεσία εγκατάστασης

   Αυτή η κατηγοριοποίηση αναφέρεται στην τοποθεσία της υπηρεσίας άμυνας. Οι περιπτώσεις είναι το *Victim Network*, όπου ιστορικά βρίσκονταν οι περισσότεροι αμυντικοί μηχανισμοί, το *Intermediate Network*, όπου το θύμα έρχεται σε επαφή με την υποδομή και ζητά την υπηρεσία και τέλος το *Source Network*. Αυτή η τελευταία περίπτωση σημαίνει ότι το δίκτυο πηγής εφαρμόζει μηχανισμούς για την αποτροπή επιθέσεων από μέσα.

Και οι τρεις ταξονομίες περιέχουν υποκατηγορίες που φαίνονται στο επόμενο σχήμα:



Σχήμα 35: Ταξονομία των μηχανισμών άμυνας DDoS

3.2.8 Οδηγός NIST για τη διενέργεια Αποτίμησης Κινδύνου

Το 2012, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας της Αμερικής (NIST) προέβη σε ειδική αναθεώρηση της δημοσίευσης για τη διεξαγωγή της αποτίμησης κινδύνου. Στις περιπτώσεις χρήσης που περιλαμβάνονται σε αυτό το έγγραφο χρησιμοποιήθηκε μια υποδειγματική ταξονομία των πηγών των απειλών και των συναφών χαρακτηριστικών των απειλών αυτών. Ο κύριος λόγος για την ύπαρξη, τη δομή και τα χαρακτηριστικά αυτής της ταξονομίας ήταν να δοθούν σε έναν οργανισμό τα απαραίτητα στοιχεία για την αποτίμηση κινδύνου.

Συγκεκριμένα, ο οδηγός αυτός παρέχει καθοδήγηση για τη διεξαγωγή καθενός από τα βήματα της διαδικασίας αποτίμησης κινδύνου (π.χ. προετοιμασία της αποτίμησης, διεξαγωγή της αποτίμησης, κοινοποίηση των αποτελεσμάτων της αποτίμησης και διατήρηση της αποτίμησης) καθώς και τον τρόπο με τον οποίο οι αποτιμήσεις των κινδύνων και άλλων οργανωτικών διαδικασιών διαχείρισης κινδύνου συμπληρώνονται και αλληλοενημερώνονται. Η ειδική αυτή έκδοση παρέχει επίσης καθοδήγηση σε οργανισμούς σχετικά με τον εντοπισμό συγκεκριμένων παραγόντων κινδύνου που πρέπει να παρακολουθούν σε συνεχή βάση, έτσι ώστε να μπορούν να καθορίσουν εάν οι κίνδυνοι έχουν αυξηθεί σε μη αποδεκτά επίπεδα (δηλαδή, να υπερβαίνουν το risk tolerance του οργανισμού).

Η ταξονομία χωρίζεται στους τύπους πηγών των απειλών, στις περιγραφές των απειλών και στα χαρακτηριστικά των απειλών. Οι τύποι πηγών απειλών οργανώνονται ιεραρχικά και οι κατηγορίες ανώτατου επιπέδου είναι οι εξής:

1. Ανταγωνιστικές (Adversarial), που πρόκειται για τύπους απειλών που προσπαθούν να εκμεταλλευτούν την εξάρτηση του οργανισμού από τους ψηφιακούς πόρους.
2. Τυχαίες (Accidental), που σημαίνει απειλές που προκαλούνται από εσφαλμένες ενέργειες ανθρώπων κατά την καθημερινή τους εργασία.
3. Διαρθρωτικές (Structural), οι οποίες αναφέρονται στην αποτυχία του εξοπλισμού, των περιβαλλοντικών ελέγχων, της παρακμής του λογισμικού.
4. Περιβάλλοντικές (Environmental), οι οποίες επικεντρώνονται σε φυσικές καταστροφές που επηρεάζουν τις κρίσιμες υποδομές αλλά είναι εκτός του ελέγχου του οργανισμού.

Αυτή η ιεραρχία αποτελείται από τρία επίπεδα το πολύ. Για παράδειγμα, υπάρχουν περιπτώσεις που περιλαμβάνουν τις απειλές Insider και Outsider, οι οποίες είναι μέλη της κλάσης Individual, η οποία είναι μέλος της κατηγορίας Adversarial ενώ ο User και ο Administrator είναι μέλη της κατηγορίας Accidental (ιεραρχική βαθμίδα δύο).

Παρακάτω ακολουθεί ο πλήρης οδηγός NIST για την αποτίμηση κινδύνου:

Threat Source Type (high level)	**Threat Source Type**	**Threat**
Adversarial	Individual	Outsider
		Insider
		Trusted Insider
		Privileged Insider
	Group	Ad hoc
		Established
	Organization	Competitor
		Supplier
		Partner
		Customer
	Nation-State	
Accidental	User	
	Privileged User/Administrator	
Structural	Information Technology (IT) Equipment	Storage
		Processing
		Communications

		Display
		Sensor
		Controller
	Environmental Controls	Temperature/Humidity Controls
		Power Supply
	Software	Operating System
		Networking
		General-Purpose Application
		Mission-Specific Application
Environmental	Natural or man-made disaster	Fire
		Flood/Tsunami
		Windstorm/Tornado
		Hurricane
		Earthquake
		Bombing
		Overrun
	Unusual Natural Event (e.g., sunspots)	
	Infrastructure Failure/Outage	Telecommunications
		Electrical Power

Σχήμα 36: Πλήρης οδηγός NIST για την αποτίμηση κινδύνου

3.2.9 Ταξονομία περιστατικών Ecsirt.net

Το ευρωπαϊκό έργο CSIRT (eCSIRT) ήταν μια κοινοπραξία καθιερωμένων CSIRTs (ομάδα για την αντιμετώπιση περιστατικών ασφάλειας των υπολογιστών) από την ευρωπαϊκή κοινότητα CSIRT που προσπάθησε να αυξήσει την ευαισθητοποίηση και την κατανόηση του έργου των ομάδων αντιμετώπισης των περιστατικών ασφάλειας των υπολογιστών. Το 2003, πρότεινε έναν πίνακα ταξονομίας συμβάντων που θα χρησιμοποιείται για την κατηγοριοποίηση δεδομένων των απειλών που συλλέγονται από τις συμμετέχουσες ομάδες στο έργο, βάσει κανόνων και επικύρωσης.

Ο πίνακας που χρησιμοποιείται από το eCSIRT περιέχει τύπους περιστατικών που όλα ανήκουν στις κλάσεις συμβάντων. Οι συγγραφείς παρέχουν επίσης λεπτομερείς περιγραφές των τύπων συμβάντων (ή μόνο των τάξεων). Παραδείγματα τύπων είναι το Worm and Virus, που αποτελούν μέρος της κλάσης του κακόβουλου κώδικα.

Ακολουθεί ο πίνακας της ταξονομίας των περιστατικών eCSIRT:

Incident Class	Incident Type	Description / Examples
Abusive Content	Abusive Content	"Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having an identical content.
	Harassment	Discreditation or discrimination of somebody (i.e. Cyberstalking)
	Child/Sexual/Violence/...	Child Pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, etc.).
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats)
Intrusion Attempts	Exploiting of known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as

		CVE name (e.g. buffer overflow, backdoors, cross side scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	new attack signature	An attempt using an unknown exploit.
Intrusions	Privileged Account Compromise	A successful compromise of a system or application (service). This can have been caused remote by a known or new vulnerability, but also by an unauthorized local access.
	Unprivileged Account Compromise	
	Application Compromise	
Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYS- a. PING-flooding or E-mail bombing (DDoS: TFN, Trinity, etc.). However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.).
	DDoS	
	Sabotage	
Information Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore attacks are possible that intercepts and access information during transmission (wiretapping, spoofing or hijacking).
	Unauthorised modification of information	
	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Selling or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
Other	All incidents which don't fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

Σχήμα 37: Ταξονομία περιστατικών eCSIRT

3.2.10 Κατηγορίες απειλών OWASP και Μοντελοποίηση Απειλών των Εφαρμογών (περιλαμβάνει λίστα απειλών STRIDE)

Το OWASP είναι μια ανοιχτή κοινότητα αφιερωμένη στο να επιτρέπει στους οργανισμούς τη σύλληψη, ανάπτυξη, απόκτηση, λειτουργία και συντήρηση ασφαλών διαδικτυακών εφαρμογών. Όλα τα εργαλεία, τα έγγραφα, τα φόρουμ και τα κεφάλαια του OWASP είναι δωρεάν και ανοιχτά σε όσους ενδιαφέρονται να βελτιώσουν την ασφάλεια των εφαρμογών. Υποστηρίζουν την προσέγγιση της ασφάλειας των εφαρμογών ως προβλήμα των ανθρώπων, των διαδικασιών και της τεχνολογίας, καθώς οι πιο αποτελεσματικές προσεγγίσεις της ασφάλειας των διαδικτυακών εφαρμογών περιλαμβάνουν βελτιώσεις σε όλους αυτούς τους τομείς.

Η μοτελοποίηση απειλών των εφαρμογών OWASP (Application Threat Modeling) είναι μια προσέγγιση για την ανάλυση της ασφάλειας μιας εφαρμογής. Πρόκειται για μια δομημένη προσέγγιση που επιτρέπει τον εντοπισμό, την ποσοτικοποίηση και την αντιμετώπιση των κινδύνων ασφαλείας που σχετίζονται με μια εφαρμογή. Η μοντελοποίηση απειλών δεν αποτελεί προσέγγιση για την αναθεώρηση του κώδικα, αλλά συμπληρώνει τη διαδικασία αναθεώρησης του κώδικα ασφαλείας. Με άλλα λόγια, μπορεί να βοηθήσει να διασφαλιστεί ότι οι εφαρμογές αναπτύσσονται με ενσωματωμένη ασφάλεια από την αρχή. Αυτό, σε συνδυασμό με την τεκμηρίωση που παράγεται στο πλαίσιο της διαδικασίας μοντελοποίησης απειλών, μπορεί να δώσει στον ενδιαφερόμενο μεγαλύτερη κατανόηση του συστήματος που μελετά.

Το μοντέλο STRIDE (βλ. Ενότητα 4) είναι μια κατηγοριοποίηση απειλών που χρησιμοποιείται από το OWASP. Αυτή η κατηγοριοποίηση προέρχεται από τη διατύπωση ερωτήσεων όπως:

- Πώς μπορεί ένας εισβολέας να αλλάξει τα δεδομένα ελέγχου ταυτότητας;
- Ποιο είναι το αντίκτυπο εάν ένας εισβολέας μπορεί να διαβάσει τα δεδομένα του προφίλ κάποιου χρήστη;
- Τι συμβαίνει εάν δεν επιτρέπεται η πρόσβαση στη βάση δεδομένων του προφίλ ενός χρήστη;

‘Ετσι, είναι χρήσιμο για τον εντοπισμό των απειλών, να κατατάσσονται οι στόχοι των εισβολέων όπως ακολουθεί:

- Πλαστογράφηση ταυτότητας (Spoofing identity): Ένα παράδειγμα πλαστογράφησης ταυτότητας είναι η παράνομη πρόσβαση και στη συνέχεια, η χρήση πληροφοριών ταυτότητας άλλου χρήστη, όπως όνομα χρήστη και κωδικό πρόσβασης.
- Αλλοίωση δεδομένων (Tampering with data): Η αλλοίωση των δεδομένων συνεπάγεται την κακόβουλη τροποποίηση των δεδομένων. Για παράδειγμα, μη εξουσιοδοτημένες αλλαγές στα δεδομένα, όπως αυτές που διατηρούνται σε μια βάση δεδομένων, αλλά και η μεταβολή των δεδομένων καθώς ανταλάσσονται μεταξύ δύο υπολογιστών μέσω ενός ανοικτού δικτύου, όπως το Internet.
- Αποποίηση (Repudiation): Οι απειλές της αποποίησης συνδέονται με χρήστες που αρνούνται την εκτέλεση μιας ενέργειας, χωρίς άλλα μέρη να έχουν κάποιο τρόπο να αποδείξουν το αντίθετο - για παράδειγμα, ένας χρήστης εκτελεί μια παράνομη λειτουργία σε ένα σύστημα το οποίο δεν έχει τη δυνατότητα εντοπισμού των απαγορευμένων λειτουργιών. Αντιθέτως, η μη αποποίηση (Non repudiation) αναφέρεται στην ικανότητα ενός συστήματος να αντιμετωπίσει τις απειλές αποποίησης Για παράδειγμα, ένας χρήστης που αγοράζει ένα αντικείμενο ενδέχεται να χρειαστεί να υπογράψει το αντικείμενο αυτό κατά την παραλαβή. Ο πωλητής μπορεί στη συνέχεια να χρησιμοποιήσει την υπογεγραμμένη απόδειξη ως απόδειξη ότι ο χρήστης έλαβε το πακέτο.
- Αποκάλυψη πληροφοριών (Information disclosure): Οι απειλές που σχετίζονται με την αποκάλυψη πληροφοριών συνεπάγονται την έκθεση πληροφοριών σε άτομα που δεν υποτίθεται ότι έχουν πρόσβαση σε αυτές. Για παράδειγμα, η ικανότητα των χρηστών να διαβάζουν ένα αρχείο στο οποίο δεν τους έχει χορηγηθεί πρόσβαση ή η δυνατότητα ενός εισβολέα να διαβάζει δεδομένα κατά τη μεταφορά τους μεταξύ δύο υπολογιστών.
- Άρνηση εξυπηρέτησης (Denial of service): Οι επιθέσεις του τύπου άρνηση εξυπηρέτησης (DoS) απορρίπτουν την υπηρεσία σε έγκυρους χρήστες, για παράδειγμα, κάνοντας έναν

διακομιστή Web προσωρινά μη διαθέσιμο ή μη χρησιμοποιήσιμο. Πρέπει να προστατεύονται γενικά οι υποδομές από ορισμένους τύπους απειλών DoS, έτσι ώστε να βελτιώθεί η διαθεσιμότητα και η αξιοπιστία του συστήματος.

- Αύξηση προνομίων (Elevation of privilege): Σε αυτόν τον τύπο απειλής, ένας μη προνομιούχος χρήστης αποκτά πρόσβαση με δικαιώματα admin και επομένως έχει επαρκή πρόσβαση για να θέσει σε κίνδυνο ή να καταστρέψει ολόκληρο το σύστημα. Οι απειλές αυτού του τύπου περιλαμβάνουν εκείνες τις καταστάσεις στις οποίες ο εισβολέας έχει διεισδύσει αποτελεσματικά σε όλες τις αμυντικές εγκαταστάσεις του συστήματος και αποτελεί μέρος του ίδιου του trusted συστήματος.

Γενικά, το OWASP Top Ten Project είναι ένα έγγραφο για την ασφάλεια των διαδικτυακών εφαρμογών. Αντιπροσωπεύει μια ευρεία συναίνεση για τους πιο κρίσιμους κινδύνους για την ασφάλεια των εφαρμογών ιστού. Τα μέλη του έργου αυτού αποτελούν μια γκάμα από ειδικούς ασφαλείας από όλο τον κόσμο που μοιράστηκαν την εμπειρία τους για την παραγωγή αυτού του καταλόγου. Η πιο πρόσφατη λίστα των κινδύνων ασφαλείας των εφαρμογών OWASP (Top Ten Application Security Risks) είναι από το 2017.

Παρακάτω ακολουθεί η λίστα απειλών STRIDE καθώς και η ταξονομία απειλών OWASP:

Type	Example	Security Control
Spoofing	Threat action aimed to illegally access and use another user's credentials, such as username and password.	Authentication
Tampering	Threat action aimed to maliciously change/modify persistent data, such as persistent data in a database, and the alteration of data in transit between two computers over an open network, such as the Internet.	Integrity
Repudiation	Threat action aimed to perform illegal operations in a system that lacks the ability to trace the prohibited operations.	Non-Repudiation
Information disclosure	Threat action to read a file that one was not granted access to, or to read data in transit.	Confidentiality
Denial of service	Threat aimed to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of privilege	Threat aimed to gain privileged access to resources for gaining unauthorized access to information or to compromise a system.	Authorization

Σχήμα 38: Λίστα απειλών STRIDE

High level Threats	Threats
Denial of Service	Improper Null Termination
	Uncaught Exception
	Divide By Zero
	J2EE Bad Practices: Use of System.exit()
	Uncontrolled Resource Consumption ('Resource Exhaustion')
	Improper Release of Memory Before Removing Last Reference ('Memory Leak')
	Improper Resource Shutdown or Release
	Asymmetric Resource Consumption (Amplification)
	Insufficient Resource Pool
	Unrestricted Externally Accessible Lock
	NULL Pointer Dereference
	Uncontrolled Recursion
Insecure Storage	Compiler Removal of Code to Clear Buffers
	Sensitive Information Uncleared Before Release
	Weak Cryptography for Passwords
	Missing Encryption of Sensitive Data
	Use of Hard-coded Cryptographic Key
	Inadequate Encryption Strength
	Use of a Broken or Risky Cryptographic Algorithm
	Information Exposure Through Persistent Cookies
	Sensitive Data Storage in Improperly Locked Memory
	Information Exposure Through Query Strings in GET Request
Injection Flaws	Improper Output Neutralization for Logs
	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
	Improper Neutralization of Special Elements used in a Command ('Command Injection')
	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
	XML Injection (aka Blind XPath Injection)
	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')
	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')
OWASP Top Ten 2004 Category A5 - Buffer Overflows	Improper Restriction of Operations within the Bounds of a Memory Buffer
	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
	Use of Externally-Controlled Format String
Cross-Site Scripting (XSS) Flaws	Improper Neutralization of HTTP Headers for Scripting Syntax
	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Invalidated Input	Struts: Duplicate Validation Forms
	Struts: Incomplete validate() Method Definition
	Struts: Form Bean Does Not Extend Validation Class
	Struts: Plug-in Framework not in Use

	Struts: Validator Turned Off
	Improper Handling of Missing Special Element
	Improper Handling of Additional Special Element
	Incorrect Behavior Order: Early Validation
	Incorrect Behavior Order: Validate Before Canonicalize
	Incorrect Behavior Order: Validate Before Filter
	Collapse of Data into Unsafe Value
	Permissive Whitelist
	Improper Input Validation
	Improper Input Validation
	External Control of Assumed-Immutable Web
	URL Redirection to Untrusted Site ('Open Redirect')
	Client-Side Enforcement of Server-Side Security
Improper Error Handling	Error Handling
	Information Exposure Through Discrepancy
	Information Exposure Through an Error Message
	Improper Handling of Syntactically Invalid Structure
	Unchecked Return Value
	Detection of Error Condition Without Action
	Unchecked Error Condition
	Unexpected Status Code or Return Value
	Not Failing Securely ('Failing Open')
	J2EE Misconfiguration: Missing Custom Error Page
Broken Access Control	Permission Issues
	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
	Incorrect Privilege Assignment
	Privilege Chaining
	Unverified Ownership
	Improper Access Control
	Improper Authorization
	Use of Insufficiently Random Values
	Improper Resolution of Path Equivalence
	Direct Request ('Forced Browsing')
	Information Exposure Through Browser Caching
	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization
	ASP.NET Misconfiguration: Use of Identity Impersonation
	Authorization Bypass Through User-Controlled Key
	Incorrect Ownership Assignment
	External Control of File Name or Path
	J2EE Misconfiguration: Weak Access Permissions for EJB Methods
Broken Authentication and Session Management	Credentials Management
	Use of Hard-coded Password
	Improper Authentication
	Improper Following of a Certificate's Chain of Trust
	Improper Validation of Certificate Expiration
	Authentication Bypass by Assumed-Immutable Data
	Missing Critical Step in Authentication
	Improper Restriction of Excessive Authentication Attempts
	Use of Password System for Primary Authentication
	insufficient Verification of Data Authenticity
	Weak Password Requirements
	Insufficiently Protected Credentials

	Authentication Bypass Issues
	Insufficient Session Expiration
	Unverified Password Change
	Weak Password Recovery Mechanism for Forgotten Password
	Use of Hard-coded Credentials
	Session Fixation
Insecure Configuration Management	ASP.NET Environment Issues
	J2EE Environment Issues
	Information Exposure Through Debug Information
	Sensitive Data Under Web Root
	Improper Certificate Validation
	Incomplete Cleanup
	Leftover Debug Code
	Information Exposure Through Environmental Variables
	Exposure of CVS Repository to an Unauthorized Control Sphere
	Exposure of Core Dump File to an Unauthorized Control Sphere
	Exposure of Access Control List Files to an Unauthorized Control Sphere
	Exposure of Backup File to an Unauthorized Control Sphere
	Information Exposure Through Test Code
	Information Exposure Through Log Files
	Information Exposure Through Server Log Files
	information Exposure Through Debug Log Files
	Information Exposure Through Source Code
	Information Exposure Through Include Source Code
	information Exposure Through Cleanup Log Files
	Information Exposure Through Directory Listing
	Files or Directories Accessible to External Parties

Σχήμα 39: Ταξονομία απειλών OWASP

3.2.11 Ταξονομία κακόβουλων προγραμμάτων (Malware) του Sans Institute

Το Sans Institute είναι ένας αμερικανικός μη κερδοσκοπικός οργανισμός που ειδικεύεται στην εκπαίδευση στον τομέα της ασφάλειας στον κυβερνοχώρο. Το 2008, δημοσίευσε ένα έγγραφο (white paper) για τη διαχείριση διαδικασιών αντιμετώπισης διαφόρων ειδών κακόβουλου λογισμικού. Σε αυτό το έγγραφο, οι συγγραφείς τόνισαν αυτούς τους τύπους κακόβουλου λογισμικού και τους μηχανισμούς διάδοσης τους. Επιπλέον, στο έγγραφο αυτό προτείνεται μια μέθοδος χειρισμού των κακόβουλων προγραμμάτων η οποία αποτελείται από έξι στάδια: Προετοιμασία, Ταυτοποίηση, Περιορισμός, Εξάλειψη, Ανάκτηση, Διδάγματα (*Preparation, Identification, Containment, Eradication, Recovery, Lessons Learnt*).

Σε αυτή τη δημοσίευση οι συγγραφείς παρουσιάζουν επίσης μια ταξονομία κακόβουλου λογισμικού υψηλού επιπέδου που φαίνεται στον παρακάτω πίνακα:

name	Property	examples
Virus	Copies itself to other files; Needs a host file to propagate and execute.	CIH, Virut, Redlof, Autorun.abt, Peacomm, NewHeur_PE
Worm	Exploits the vulnerabilities that are present and can spread over the network.	Code red, Netsky, Stration, Sasser, Bagle, Skipi, no_virus
Logic Bomb	Triggers a specific code on meeting conditions as per the logic written by its author.	Michelangelo
Backdoor	Listens on certain ports so that the attacker can gain access through them later.	Xhaker, sub7, Beast, Ginwui, Rexob, Hupigon
Trojan	Deceptive program that spoofs a harmless or useful program; but, actually stores other malware.	Limbo/NetHell, Pidief, ZeuS/PRG, Banker.bdn, PGPCoder, Torpig, Gozi
Spyware	Software used to spy on victim's activities and also used to steal sensitive information.	WhenUSave, PuritySCAN Virtumonde, SecurityToolbar
Rootkit	Set of programs that alter the OS functionality to hide themselves.	LRK, AFX, SInAR, Rustock, Mebroot
Bot / Botnet	Program that do the work on behalf of its master. A master may control millions of such bots and can use them for malicious purposes.	Agobot, Slackbot, Mytob, Rbot, SdBot, poebot, IRCBot, VanBot, Mpack, Storm

Σχήμα 40: Ταξονομία κακόβουλου λογισμικού Sans Institute

Επιπλέον, στη δημοσίευση αυτή κατηγοριοποιούν τους ιούς βάσει διαφορετικών κατηγοριών για να τους περιγράψουν, ως εξής:

- Με βάση τη μνήμη

Αυτή η ταξινόμηση περιγράφει τον τρόπο λειτουργίας των ιών στη μνήμη. Υπάρχουν ιοί που παραμένουν στη μνήμη όσο το δυνατόν περισσότερο ή προσωρινά ή καθόλου. Επιπλέον, μπορεί να βρίσκονται σε επίπεδο διαδικασίας (level process) ή στο επίπεδο του πυρήνα (process in the kernel).

- Με βάση τον στόχο

Αυτό αναφέρεται στο πώς εξαπλώνεται ο ιός και στον στόχο που επιτίθεται. Οι κύριες κατηγορίες αυτής της διάκρισης είναι οι Compiled, Interpreted και η Multipartite. Οι Compiled ιοί μετατρέπονται σε εκτελέσιμες οδηγίες του μηχανήματος, ενώ ο κώδικας των Interpreted ιών πραγματοποιείται από μια εφαρμογή. Τέλος, οι Multipartite ιοί περιλαμβάνουν μια ποικιλία μηχανισμών για να επιτεθούν στο

κεντρικό σύστημα (host), όπως να μολύνουν τον τομέα εκκίνησης (boot sector) ή τα έγγραφα εφαρμογής (application documents) και στη συνέχεια να εξαπλωθούν.

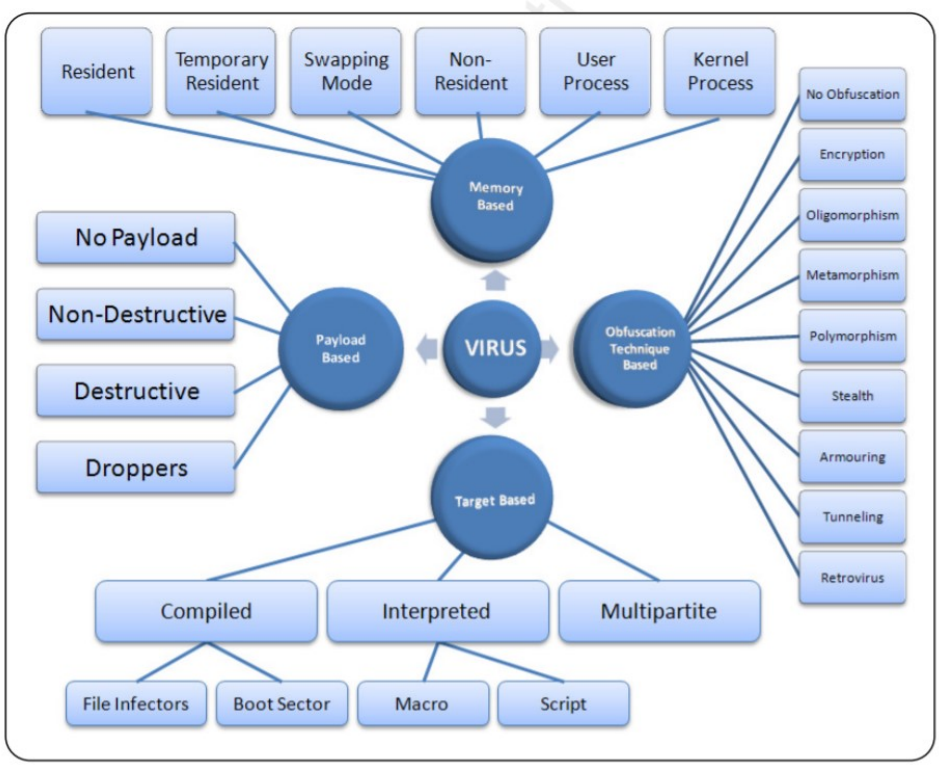
- Με βάση την τεχνική της συσκότισης (Obfuscation tehnique)

Αυτή η ταξινόμηση βασίζεται στην τεχνική που χρησιμοποιούν οι ιοί για να κρυφτούν από την ανίχνευση και την ανάλυση. Υπάρχουν διάφορες υποκατηγορίες, όπως Κρυπτογράφηση, Tunelling, No obfuscation, Oligomorphism, Metamorphisms, Stealth, Armoring, Retro.

- Με βάση το φορτίο

Αυτό αναφέρεται στο αποτέλεσμα της « μόλυνσης » από τον ιό. Ορισμένοι ιοί μπορεί να μην φέρουν τίποτα περισσότερο από τον κώδικα, ενώ άλλοι περιέχουν ένα μήνυμα ή ένα σχήμα που δεν επεκτείνει τη βλάβη. Αντιθέτως, υπάρχουν και άλλοι ιοί οι οποίοι θα μπορούσαν να καταστρέψουν ή να διαφθείρουν μεταδεδομένα αρχείων. Η υποκατηγορία της ταξινόμησης αυτής, στην οποία βασίζονται και οι περισσότεροι ιοί σύμφωνα με τους συγγραφείς, είναι οι ιοί Droppers, οι οποίοι βοηθούν τους εισβολείς να αποκτήσουν πρόσβαση στα προσωπικά δεδομένα των θυμάτων και συνεπώς να αποκτήσουν οικονομικό όφελος ή να βλάψουν τη λειτουργικότητα ενός οργανισμού. Παραδείγματα της τελευταίας υπο-κατηγορίας είναι τα εξής: κλοπή ταυτότητας, άρνηση εξυπηρέτησης (DDos), phishing, κλοπή άδειας χρήσης λογισμικού κλπ.

Η ολοκληρωμένη ταξονομία/κατηγοριοποίηση των ιών του Sans Institute παρουσιάζεται παρακάτω:



Σχήμα 41: Ταξονομία ιών Sans Institute

3.3 Σύγκριση Ταξονομιών

Όπως αναφέρθηκε παραπάνω στην εισαγωγή, υπάρχουν πολλοί τρόποι ταξινόμησης των απειλών και έχουν αναπτυχθεί πολλές ταξονομίες και καταλόγοι απειλών. Ορισμένες από τις ταξονομίες αυτές αναγνωρίζονται παγκοσμίως, μοντελοποιούνται και είναι διαθέσιμες για λήψη ή χρήση, ενώ άλλες βασίζονται σε εμπειρίες συγκεκριμένης ομάδας στη διαχείριση περιστατικών και εξυπηρετούν ειδικούς σκοπούς. Επιπλέον, ορισμένες ταξονομίες που παρουσιάστηκαν σε προηγούμενες ενότητες περιλαμβάνουν αμυντικούς μηχανισμούς ή αντίμετρα τα οποία αντιστοιχούν στις ταξονομίες απειλών.

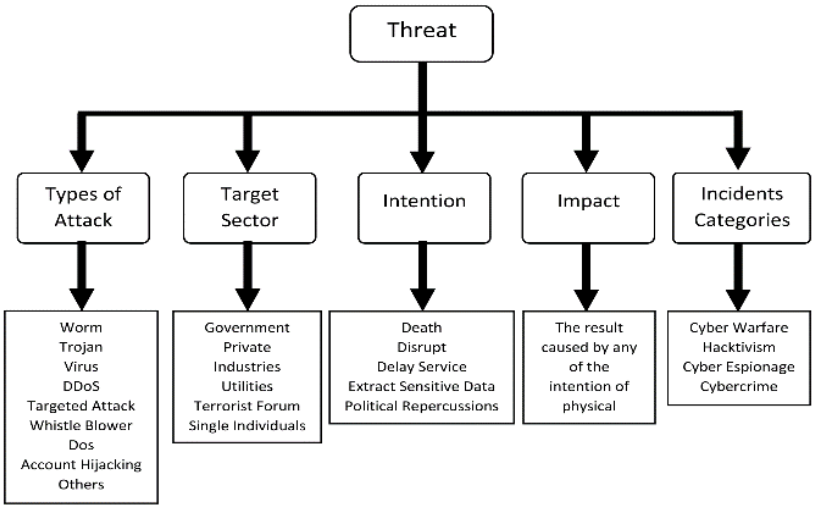
Οι ταξονομίες που περιγράφηκαν ποικίλλουν ανάλογα με το μέγεθος, το περιεχόμενο του πεδίου εφαρμογής τους, τον ορισμό των απειλών και με τις οντότητες που έχουν ως στόχο. Μερικές απο τις ταξονομίες αυτές περιέχουν πάνω από 500 απειλές, ενώ άλλες χρησιμοποιούν μόνο ένα μικρό σύνολο κατηγοριών που χρησιμοποιούνται σε περιπτώσεις χρήσης. Άλλες είναι κατάλληλες για επαγγελματίες ασφαλείας, ενώ υπάρχουν και ταξονομίες που ισχύουν περισσότερο για την ακαδημαϊκή κοινότητα. Επιπλέον, ορισμένες ταξονομίες περιέχουν τεχνικούς όρους, ενώ οι περισσότερες είναι λιγότερο εξειδικευμένες και επομένως, πιο κατανοητές από επαγγελματίες που δεν εμπλέκονται με την ασφάλεια των πληροφοριών. Για παράδειγμα, η ταξονομία WASC περιλαμβάνει ορισμένους όρους που μπορεί να μην ερμηνεύονται εύκολα από ανθρώπους χωρίς κάποιο τεχνικό υπόβαθρο, όπως για παράδειγμα το LDAP injection.

Στην ενότητα αυτή συγκρίνουμε τις παραπάνω ταξονομίες με βάση κάποια χαρακτηριστικά. Ορισμένες από τις έννοιες, όπως η απλή ταξινόμηση υψηλού επιπέδου, η κατάταξη των απειλών και άλλες όπως η ευκολία χρήσης, θεωρούνται από τον ENISA και από διάφορες CSIRT ως καλές πρακτικές. Μια ταξονομία που πρέπει να χρησιμοποιείται σε καθημερινή και σωστή βάση, θα πρέπει να περιέχει ένα μεγάλο σημασιολογικό λεξιλόγιο, το οποίο μπορεί να εμπλουτιστεί με όρους που αντλούνται από τα εθνικά και διεθνή πρότυπα και από τη συνεργασία άλλων CSIRT. Οι συμφωνημένες πρακτικές μπορεί να οδηγήσουν σε απλότητα, αφού γίνεται ευκολότερη η εξαγωγή μιας ταξονομίας σε άλλες, λόγω της ομοιότητας των γενικών τους όρων. Τα κριτήρια σύμφωνα με τα οποία πραγματοποίηθηκε η σύγκριση των ταξονομιών είναι τα εξής:

- **Οντολογία (Ontology - multi dimensional):** Μια οντολογία είναι ένα εργαλείο για την εκπροσώπηση της γνώσης ως ένα σύνολο διάφορων εννοιών. Σε σύγκριση με τις ταξονομίες, οι οντολογίες θεωρούνται τρισδιάστατες και, αν και δεν είναι πάντα πολύ σαφείς, δεν μπορούν να αναπαρασταθούν ως ένας ενιαίος πίνακας . Μια απλή ταξονομία είναι σαν ένα δέντρο, ενώ μια οντολογία μοιάζει με ένα δάσος. Όταν μια ταξονομία έχει τη μορφή μιας οντολογίας, αυτή η 3η διάσταση είναι συνήθως « η σχέση μεταξύ εννοιών ». Έτσι, η διαφορά ανάμεσα σε μια ταξονομία και μια οντολογία μπορεί να περιγραφεί με αυτό το παράδειγμα: « μία ταξονομία μπορεί να θεωρηθεί ως ένας παράγοντας απειλής που προκαλεί την απειλή και μια ονοντολογία ως η απειλή αυτή που οδηγεί σε επίθεση σε αγαθά του συστήματος ».
- **Τομέας προσανατολισμού (Sector oriented):** Ορισμένες ταξονομίες καλύπτουν το μεγαλύτερο μέρος των απειλών στον κυβερνοχώρο, ενώ άλλες επικεντρώνονται σε συγκεκριμένους τομείς ασφάλειας ή σε συγκεκριμένο τύπο απειλής, όπως για παράδειγμα, υπηρεσίες Cloud ή τοποθεσίες Web. Επιπλέον, μερικές ταξονομίες μπορεί να επικεντρωθούν σε συγκεκριμένες κατηγορίες απειλών όπως Επιθέσεις άρνησης εξυπηρέτησης ή ιούς.
- **Κατάταξη απειλών - Μέτρηση απόδοσης για την επίλυση ενός προβλήματος (Ranking threats – Performance Measurement in solving a problem):** Το χαρακτηριστικό αυτό αναφέρεται στην ύπαρξη οποιουδήποτε είδους βαθμού βαρύτητας της απειλής στην ταξονομία ή στη μέτρηση του χρόνου που χρειάζεται ένα περιστατικό για να κλείσει. Μάλιστα, η μέτρηση του χρόνου που χρειάζεται ένα περιστατικό για να κλείσει θεωρείται ότι αποτελεί καλή πρακτική από τον ENISA. Ο προκαθορισμένος χρόνος για μια απειλή βελτιώνει την κατανομή των πόρων ασφαλείας και τη διατήρηση στατιστικών στοιχείων.
- **Απλή ταξονομία ανώτατου επιπέδου (Simple top-level taxonomy):** Η απλή ταξονομία ανώτατου επιπέδου σχετίζεται με την πολυπλοκότητα της ταξονομίας, αλλά υποδηλώνει επίσης ότι μπορεί να υπάρχουν περισσότερα από ένα επίπεδα κατηγοριοποίησης. Με ένα σύστημα

κατηγοριοποίησης πολλαπλών επιπέδων, το επιθυμητό επίπεδο πολυπλοκότητας της ταξονομίας μπορεί εύκολα να επιλεγεί. Στην περίπτωση που απαιτείται μία αναφορά μη τεχνικού χαρακτήρα, τότε μπορεί να χρησιμοποιηθεί ένα υψηλότερο και γενικότερο επίπεδο κατηγοριοποίησης. Αντιθέτως, στην περίπτωση που απαιτείται μία τεχνική αναφορά, τότε η χρήση της κατώτερης κατηγορίας επιπέδου είναι απαραίτητη. Γενικά, ο καθορισμός των απλών κατηγοριών του ανώτερου επιπέδου συμβάλλει στην επιλογή του προτιμώμενου επιπέδου πολυπλοκότητας για μια ταξονομία, και έτσι γενικές και πιο τεχνικές αναφορές μπορούν εύκολα να αναπτυχθούν. Οι κατηγορίες υψηλού επιπέδου είναι ευκολότερο να ερμηνευτούν, ενώ οι βασικές κατηγορίες μπορεί να είναι πιο κατάλληλες για τεχνικές αναφορές.

- **Ιεραρχική ταξονομία (Hierarchical)** : Η διάκριση αυτή σημαίνει ότι οι κατηγορίες προκύπτουν από άλλες κατηγορίες με τη μορφή δέντρου. Γενικά, μια ταξονομία με τουλάχιστον 2-3 επίπεδα κατηγοριοποίησης παρέχει μεγάλη επεκτασιμότητα και ευελιξία, καθώς δίνει την επιλογή να προστεθεί ένα κλαδί σε ένα δέντρο ή να προστεθεί ένα φύλλο στο κλαδί.
- **Αμοιβαία αποκλειόμενες κατηγορίες (Mutually exclusive categories):** Ένα ζήτημα που έχει αναφερθεί από πολλούς CSIRTS είναι η αμοιβαία απόκλιση των κατηγοριών των απειλών. Θεωρείται καλή πρακτική, ειδικά αν χρησιμοποιείται machine reading, για τον καθορισμό αυστηρών όρων και περιορισμών, προκειμένου να αποφευχθεί η κατηγοριοποίηση ενός συμβάντος σε δύο ή περισσότερες διαφορετικές κλάσεις από διαφορετικούς αναλυτές. Μερικές φορές όμως αυτό δεν μπορεί να αποφευχθεί και ένα περιστατικό μπορεί να αλλάξει κατηγορίες κατά τη διάρκεια του κύκλου χειρισμού του. Αυτό οδηγεί σε διφορούμενες αναφορές που δεν μπορούν να ερμηνευθούν και να συνδυαστούν κατάλληλα.
- **Αναγνώσιμη από μηχανή (Machine Readable):** Όπως ένα περιστατικό μπορεί να αντιμετωπιστεί από ανθρώπους και μηχανές, είναι χρήσιμο για μια ταξονομία να είναι διαθέσιμη και σε μορφή αναγνώσιμο από τον άνθρωπο και σε μορφή αναγνώσιμη από μηχανή (JSON, XML κλπ).
- **Μέγεθος σημασιολογικού λεξιλογίου (Size of semantic vocabulary):** Το σημασιολογικό λεξιλόγιο περιγράφει στοιχεία γνώσης και πληροφορίας. Στη βιβλιογραφία, ορισμένες ταξονομίες που θεωρούνται δημοφιλείς μπορούν να καθορίσουν τα όρια και σε σύγκριση με αυτά μπορεί κανείς να εξετάσει εάν μια ταξονομία είναι μεγάλη, μεσαία ή μικρή.
- **Περιέχει φυσικές απειλές (Contains physical threats):** Υπάρχει διάκριση μεταξύ ταξονομιών που περιέχουν τουλάχιστον ορισμένες κατηγορίες φυσικών απειλών, σε σύγκριση με αυτές που περιέχουν μόνο απειλές σχετικές με τον κυβερνοχώρο.



Σχήμα 42: Ταξονομία απειλών

Όπως φαίνεται και στον πίνακα του παράρτηματος, όλες οι ταξινομίες χαρτογραφούνται στα προαναφερθέντα χαρακτηριστικά. Η τιμή του « Ναι » (Yes) υποδεικνύει ότι η ταξονομία πληρεί την έννοια του χαρακτηριστικού. Σε ορισμένες περιπτώσεις υπάρχει ένα επεξηγηματικό κείμενο ή ένας δείκτης κλίμακας. Επίσης, στον πίνακα αυτό περιλαμβάνονται συνολικά 20 ταξονομίες αλλά στις προηγούμενες ενότητες παρουσιάστηκαν 11 ταξονομίες για λόγους σπουδαιότητας, καθώς επιλέξαμε να περιγράψουμε πιο αναλυτικά τις πιο σημαντικές.

Ορισμένες ταξονομίες είναι υπό μορφή Οντολογίας ή περιέχουν πολλαπλές διαστάσεις. Για παράδειγμα, το πρότυπο ISO 28001 και η μεθοδολογία CYSM διαμορφώνουν κατά κάποιον τρόπο οντολογίες, δηλαδή συνδέουν τα αγαθά με τις απειλές (και τα αντίμετρα) χρησιμοποιώντας σενάρια. Η σχέση μεταξύ εννοιών υπάρχει επίσης στην ταξονομία των DDoS Attacks, συμπεριλαμβανομένων και των αμυντικών μηχανισμών στις κατηγορίες επίθεσης. Επίσης, στην ταξονομία *semantic social engineering attacks* κάθε τυπική επίθεση αντιστοιχεί σε συγκεκριμένες κατηγορίες και ιδιότητες, γεγονός που υποδηλώνει τις πολλάπλές διαστάσεις της, καθώς επίσης και η ταξονομία *Insider Threats in Cloud Computing* όπου εφαρμόζονται διαφορετικές έννοιες όπως η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα σε κατηγορίες cloud απειλών.

Επίσης, σύμφωνα με τον πίνακα σύγκρισης των ταξονομιών, ορισμένες ταξινομίες προορίζονται για συγκεκριμένους τομείς. Για παράδειγμα, το πρότυπο ISO 28001 επικεντρώνεται στα συστήματα ασφαλείας για την αλυσίδα εφοδιασμού, η ταξονομία WASC αναφέρεται στις απειλές που σχετίζονται με τους ιστότοπους, ενώ η ταξονομία *Hp Tipping Event Point* αφορά τις υπηρεσίες Web SMS. Επιπλέον, η ταξονομία *semantic social engineering attacks* εξηγεί τις απειλές στην Κοινωνική Μηχανική, ενώ οι ταξονομίες *Threat Taxonomies for Cloud* και *Insider Threats in Cloud Computing* παρουσιάζουν την κατηγοριοποίηση των απειλών που είναι κοινές στις υπηρεσίες Cloud. Τέλος, η ταξονομία *VoIP Security and Privacy Threat Taxonomy* ορίζει τις πιθανές απειλές για τις εφαρμογές VoIP.

Ακόμη, οι ταξονομίες αυτές μπορούν να επικεντρωθούν σε συγκεκριμένες κατηγορίες απειλών. Για παράδειγμα, η ταξονομία των μηχανισμών επίθεσης DDoS , περιγράφει απειλές (και αμυντικούς μηχανισμούς) που σχετίζονται με επιθέσεις DDoS (οι οποίες περιγράφονται επίσης στις ταξονομίες MISP), ενώ το Sans Institute αναλύει κυρίως τις κατηγορίες και τις υπο-κατηγορίες των ιών.

Αξίζει επίσης να αναφερθεί ότι οι περισσότερες ταξονομίες διατηρούν μια απλότητα στην επιλογή κατηγοριών υψηλού επιπέδου, οι οποίες, όπως προαναφέρθηκε, συμβάλλουν στην ενσωμάτωση και τη σύγκριση με άλλες κατηγοριοποιήσεις. Για παράδειγμα, οι ταξονομίες ENISA και CAPEC κατηγοριοποιούν τις απειλές με λίγα, σαφή, αμοιβαία αποκλειόμενα και εύκολα στην ερμηνεία τους ανώτατα επίπεδα και με πολλαπλές υποκατηγορίες σε δύο επιπλέον επίπεδα που ταιριάζουν τόσο σε τεχνικές όσο και σε μη τεχνικές αναφορές. Από την άλλη πλευρά, η ταξονομία WASC έχει μόνο δύο κατηγορίες υψηλού επιπέδου, επιθέσεις και αδυναμίες και πολύπλοκες υποκατηγορίες, καθιστώντας πιο δύσκολη την αντιστοίχηση σε κατηγορίες άλλων ταξονομιών ή τη δημιουργία ενός report που βασίζεται σε αυτές.

Τέλος, οι περισσότερες από τις ταξονομίες που παρουσιάστηκαν στην ενότητα αυτή καλύπτουν μόνο επιθέσεις στον κυβερνοχώρο. Υπάρχουν όμως και μερικές άλλες, όπως για παράδειγμα η ταξονομία ENISA που περιλαμβάνει κατηγορίες όπως φωτιά, φυσική επίθεση και μάλιστα, η συγκεκριμένη ταξονομία περιλαμβάνει και μια ολόκληρη κλάση με υποκατηγορίες όπως κλοπή, σαμποτάζ και τρομοκρατική επίθεση. Με την ίδια λογική, το πρότυπο ISO 28001, εστιάζοντας στην αλυσίδα εφοδιασμού, περιγράφει τις απειλές που σχετίζονται με τις υποδομές, τα αγαθά και το προσωπικό. Η ταξονομία IT Grundsutz περιέχει μια ποικιλία φυσικών απειλών, όπως φωτιά, δυσμενείς κλιματολογικές συνθήκες, νερό και άλλες. Οι περιβαλλοντικές απειλές είναι επίσης μια κατηγορία στην ταξονομία NIST, εστιάζοντας όμως στη μη διαθεσιμότητα της αιτίας στα συστήματα. Τέλος, η μεθοδολογία CYSM αφιερώνει επίσης μια κατηγορία ανώτατου επιπέδου σε φυσικές απειλές (σεισμός, πλημμύρα, τυφώνας κ.λπ.).

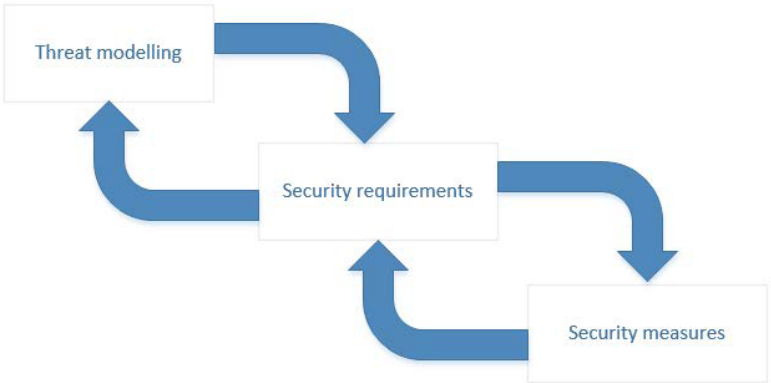
4 ΚΕΦΑΛΑΙΟ 4: Ανάλυση της Μοντελοποίησης των Απειλών

4.1 Τι είναι η μοντελοποίηση απειλών

Η αποτίμηση κινδύνου, όπως είδαμε σε προηγούμενη ενότητα, περιλαμβάνει την ανάλυση των απειλών του υπό μελέτη συστήματος. Για την ανάπτυξη ασφαλούς λογισμικού, είναι σημαντικό να έχουμε κατά νου την ασφάλεια κατά τη διάρκεια της φάσης σχεδιασμού του λογισμικού. Σε αντίθετη περίπτωση, ενδέχεται να προκύψουν πρόσθετα έξοδα, καθώς το κόστος της αναπροσαρμογής της ασφάλειας μετά την κυκλοφορία του λογισμικού εκτιμάται ότι είναι έως και 30 φορές υψηλότερο από ό, τι θα είχε κοστίσει για να διορθωθούν τα λάθη ασφαλείας κατά την αρχική φάση σχεδιασμού (Microsoft, 2009) . Ως εκ τούτου, συνίσταται να ανιχνευθούν τυχόν πιθανές απειλές ασφαλείας το συντομότερο δυνατό. Σε αυτό το σημείο εισάγεται η μοντελοποίηση απειλών, καθώς βοηθά τους αναλυτές ασφαλείας να αξιολογήσουν αρχικά την αρχιτεκτονική του συστήματος ή του λογισμικού και να εντοπίσουν τις απειλές κατά της ασφάλειας. Εξαιτίας αυτού, αναγνωρίστηκε ως ένα από τα πιο σημαντικά βήματα για τη δημιουργία ασφαλούς λογισμικού.'Ετσι, είναι σημαντικό να ενσωματωθεί η μοντελοποίηση απειλών όσο το δυνατόν νωρίτερα στον κύκλο ζωής ανάπτυξης του λογισμικού (SDLC).

Η μοντελοποίηση απειλών είναι, όπως ορίζεται από τους Oladimeji, Supakkul & Chung : « μια επίσημη διαδικασία εντοπισμού, τεκμηρίωσης και μετριασμού των απειλών ασφάλειας σε ένα σύστημα λογισμικού ». Μια απειλή για την ασφάλεια είναι η πιθανότητα να προκληθεί βλάβη σε ένα σύστημα ή μια εφαρμογή, επειδή υπάρχει ένα τρωτό σημείο στο σχεδιασμό. Όταν ένας εισβολέας βρίσκει αυτήν την ευπάθεια και την εκμεταλλεύεται, τότε αυτό οδηγεί σε επίθεση. Ως εκ τούτου, είναι σημαντικό να εφαρμοστούν μέτρα ασφαλείας για την εξάλειψη των τρωτών σημείων αλλά και για να μη μπορέσουν οι επιτιθέμενοι να βλάψουν το σύστημα.

Είναι σημαντικό να μην εφαρμόσουμε τυχαία τα μέτρα ασφαλείας. Επειδή ένα σύστημα έχει για παράδειγμα σύστημα ανίχνευσης εισβολών, δεν σημαίνει ότι είναι αυτόματα ασφαλές. Όλα εξαρτώνται από το πλαίσιο των λειτουργιών και του σχεδιασμού του συστήματος. Ο σχεδιαστής ασφάλειας του συστήματος πρέπει να εξετάσει ολόκληρο το σύστημα κατά την εξέταση των χαρακτηριστικών ασφαλείας που πρέπει να εφαρμόσει. Η δημιουργία ασφαλών συστημάτων δεν είναι μια εφάπαξ εργασία αλλά μια συνεχής διαδικασία βελτίωσης. Δεδομένου ότι η ασφάλεια είναι μια διαδικασία και όχι ένα προϊόν, επωφελείται σε μεγάλο βαθμό από μια συστηματική προσέγγιση. Η μοντελοποίηση των απειλών παρέχει αυτή τη δομημένη προσέγγιση για τον υπεύθυνο σχεδιασμού ασφάλειας του συστήματος να επιλέξει προσεκτικά τα μέτρα ασφάλειας που πραγματικά χρειάζεται το σύστημα.



Σχήμα 43: Η διαδικασία της ασφάλειας

Το παραπάνω σχήμα δείχνει πώς η μοντελοποίηση των απειλών διαδραματίζει κυρίαρχο ρόλο στη διαδικασία της ασφαλείας. Πιο συγκεκριμένα, η μοντελοποίηση των απειλών βοηθά τους σχεδιαστές ασφάλειας να κατανοήσουν την πολυπλοκότητα του συστήματος και να εντοπίσουν όλες τις απειλές, είτε αυτές μπορούν να αξιοποιηθούν είτε όχι. Αυτές οι απειλές προσδιορίζονται στη συνέχεια με βάση την πιθανότητα να συμβεί η επίθεση και τις πιθανές επιπτώσεις που θα μπορούσε να προκαλέσει μια τέτοια επίθεση. Στη συνέχεια, λαμβάνεται απόφαση για τον μετριασμό της απειλής με την εφαρμογή μέτρων ασφαλείας ή με την αποδοχή του σχετικού κινδύνου. Με άλλα λόγια, η μοντελοποίηση των απειλών παρέχει τη βάση για τις απαιτήσεις ασφαλείας και επομένως την ασφάλεια ολόκληρου του συστήματος. Βοηθά στην εστίαση των προσπαθειών της ομάδας ασφάλειας στην ανάπτυξη ουσιαστικών και χρήσιμων μέτρων ασφαλείας, παρέχοντας το θεμέλιο πάνω στο οποίο οικοδομείται η ασφάλεια του συστήματος. Διάφοροι τύποι συστημάτων μπορούν να επωφεληθούν από τη μοντελοποίηση των απειλών, από απλά έως πολύπλοκα συστήματα, ήδη αναπτυγμένα συστήματα ή ακόμη και συστήματα που υπάρχουν μόνο στο χαρτί μέχρι στιγμής. Ανεξάρτητα από το ποιο στάδιο της αναπτυξιακής διαδικασίας βρίσκεται το σύστημα, μπορεί να επωφεληθεί από τη μοντελοποίηση απειλών.

Σε γενικές γραμμές, θα πρέπει να βλέπουμε τη μοντελοποίηση απειλών ως μία σύνθετη διαδικασία αποτελούμενη από βήματα που επιτελούν κάποιους στόχους, και όχι ως μία μεμονωμένη δραστηριότητα. Τα βασικά ερωτήματα στα οποία πρέπει να απαντήσουμε προκειμένου να επιτευχθούν οι στόχοι αυτοί είναι τα ακόλουθα: Τι χτίζουμε/κατασκευάζουμε, τι μπορεί να πάει στραβά με αυτό όταν χτιστεί, τι πρέπει να κάνουμε για τα πράγματα που μπορεί να πάνε στραβά και αν έχουμε κάνει μια αξιοπρεπή εργασία ανάλυσης.

Προκειμένου να απαντήσουμε στα παραπάνω ερωτήματα, είναι σημαντικό να θεωρήσουμε τη διαδικασία της μοντελοποίησης απειλών ως ένα « πλαίσιο » το οποίο αποτελείται από τέσσερα βήματα, τα οποία απεικονίζονται γραφικά στο σχήμα 44. Τα βήματα αυτά είναι τα εξής:

1. Μοντελοποίηση του συστήματος που χτίζεται, αναπτύσσεται ή τροποποιείται.
2. Εύρεση των απειλών, χρησιμοποιώντας αυτό το μοντέλο.
3. Αντιμετώπιση των απειλών αυτών.
4. Επιβεβαίωση της εργασίας ως προς την πληρότητα και την αποτελεσματικότητα.

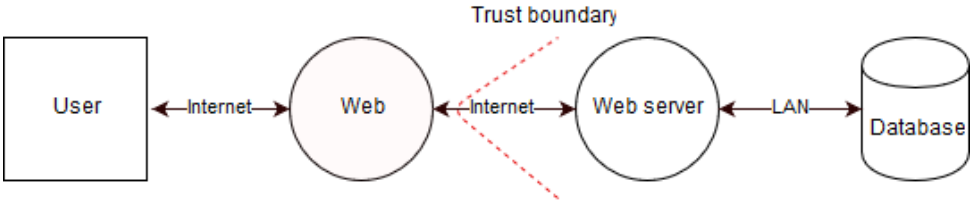
Σχήμα 44: Το πλαίσιο των τεσσάρων βημάτων

Η διαδικασία μοντελοποίησης των απειλών ποικίλλει ανάλογα με τον οργανισμό, τα εργαλεία που είναι διαθέσιμα, τις μεθοδολογίες και την προσέγγιση της μοντελοποίησης απειλών, κλπ. Εκτός από την παραπάνω προσέγγιση με το πλαίσιο των τεσσάρων βημάτων, υπάρχει και μια ακόμα πιο απλουστευμένη που αποτελείται από τρία βήματα. Υπάρχουν τρία βήματα τα οποία έχουν όλες οι διαδικασίες μοντελοποίησης απειλών, αν και η εκτέλεση και το όνομα κάθε βήματος μπορεί να διαφέρουν σε κάθε διαδικασία, και είναι τα παρακάτω:

1. Χαρακτηρισμός του συστήματος
2. Ταυτοποίηση των αγαθών
3. Εντοπισμός των απειλών

Το πρώτο βήμα κάθε διαδικασίας μοντελοποίησης απειλών είναι να εξοικειωθούμε με το σύστημα και τις συνιστώσες (components) του. Ο σχεδιαστής ασφάλειας πρέπει να γνωρίζει τις συνιστώσες του συστήματος, τον τρόπο που συνεργάζονται μεταξύ τους, τις εξαρτήσεις τους, τη ροή των πληροφοριών, τις περιπτώσεις χρήσης κλπ. Εξαρτάται από τον τύπο του συστήματος το πώς μπορούν να μοντελοποιηθούν οι διάφορες συνιστώσες του και οι εξαρτήσεις τους. Η πιο συνηθισμένη αναπαράσταση είναι ένα διάγραμμα ροής δεδομένων (DFD), το οποίο δείχνει τη ροή των πληροφοριών μέσω ενός συστήματος ή μιας εφαρμογής και όλων των συνιστωσών του.

Πιο αναλυτικά, το διάγραμμα DFD διευκολύνει την ανάλυση πιθανών απειλών, καθώς μπορεί να ακολουθηθεί η ροή δεδομένων μέσω των διαφόρων συνιστωσών και των αλληλεπιδράσεών τους. Η αλληλεπίδραση στοιχείων με διαφορετικά δικαιώματα ή προνόμια υποδεικνύεται με διακεκομμένες γραμμές, γνωστές ως *όρια εμπιστοσύνης* (trust boundaries). Αυτά τα όρια εμπιστοσύνης πρέπει να προειδοποιήσουν τον αναλυτή ασφαλείας να δώσει προσοχή, καθώς οι απειλές τείνουν να συσπειρώνονται γύρω από τα όρια εμπιστοσύνης σε ένα DFD. Για παράδειγμα, εάν δημιουργηθεί το DFD για ένα απλό ηλεκτρονικό κατάστημα, θα μοιάζει με το Σχήμα 45. Η κόκκινη διακεκομμένη γραμμή ανάμεσα στα στοιχεία του Web και του διακομιστή Web αντιπροσωπεύει ένα όριο εμπιστοσύνης. Αυτό το όριο εμπιστοσύνης τοποθετείται εδώ, επειδή ο χρήστης πρέπει να κάνει σύνδεση μέσω του διαδικτύου για να έχει πρόσβαση στο ηλεκτρονικό κατάστημα. Δεδομένου ότι η σύνδεση αυτή προέρχεται από το εξωτερικό του συστήματος, δεν είναι δυνατή η επαλήθευση της ακεραιότητας και της ποιότητας των δεδομένων. Ένας εισβολέας μπορεί να έχει αλλάξει τα εισερχόμενα δεδομένα ή να έχει στείλει κάποια κακόβουλα δεδομένα στο σύστημα. Αυτή η διακεκομμένη κόκκινη γραμμή αντιπροσωπεύει τη διαφορά στα επίπεδα εμπιστοσύνης των δεδομένων, δηλαδή τα δεδομένα από το εσωτερικό σύστημα που μπορούμε να παρακολουθούμε και να εμπιστευόμαστε και τα δεδομένα για τα οποία δεν έχουμε κανέναν έλεγχο και επομένως πρέπει να είμαστε επιφυλακτικοί. Αυτά τα όρια εμπιστοσύνης δεν εμφανίζονται μόνο σε DFDs όταν πραγματοποιείται σύνδεση με εξωτερικό δίκτυο (π.χ. Internet) αλλά και όταν υπάρχουν αλληλεπιδραστικά στοιχεία με διαφορετικά προνόμια ή μπορούν να χρησιμοποιηθούν για να υποδείξουν διαφορετικές ζώνες ασφαλείας (OWASP 2017).



Σχήμα 45: Ένα απλοποιημένο παράδειγμα DFD για ένα ηλεκτρονικό κατάστημα

Το επόμενο βήμα στη διαδικασία μοντελοποίησης απειλών είναι η ταυτοποίηση των αγαθών, δηλαδή σε τι θα επιτεθεί ένας εισβολέας ή θα προσπαθήσει να θέσει σε κίνδυνο, τι πρέπει να υπερασπιστεί κλπ. Ο ορισμός που δίνεται σε ένα αγαθό σε αυτό το στάδιο εξαρτάται από την προσέγγιση της μοντελοποίησης απειλών που χρησιμοποιείται. ΄Ετσι. μπορεί να οριστεί από την οπτική γωνία του εισβολέα ή ως ένας πόρος του υπό μελέτη συστήματος. Με άλλα λόγια, σύμφωνα με τους Myagmar, Lee & Yurcik, « Ένα αγαθό

είναι ένας αφηρημένος ή συγκεκριμένος πόρος που ένα σύστημα πρέπει να προστατεύει από την κακή χρήση από έναν αντίπαλο. Τα αγαθά μπορούν να είναι απτά, όπως διαδικασίες και δεδομένα, ή πιο αφηρημένες έννοιες, όπως η συνέπεια των δεδομένων. Είναι αδύνατο να υπάρχει απειλή χωρίς ένα αντίστοιχο αγαθό, επειδή τα αγαθά είναι ουσιαστικά στόχοι απειλής ». Αυτός ο ευρύς ορισμός δείχνει ότι ένα αγαθό μπορεί να είναι πολλά πράγματα, τόσο απτά όσο και αφηρημένα, και ότι θέτει πιθανούς στόχους για κακόβουλους επιτιθέμενους. Επιπλέον, δείχνει ότι οι απειλές και τα αγαθά συσχετίζονται, καθώς χωρίς τα αγαθά είναι αδύνατο να υπάρξουν απειλές.

Το τελευταίο βήμα στη διαδικασία μοντελοποίησης των απειλών είναι να εντοπιστούν όλες οι πιθανές απειλές για το σύστημα που εξετάζουμε. Ο προσδιορισμός αυτών των απειλών βασίζεται στις πληροφορίες που συγκεντρώθηκαν στα προηγούμενα δύο βήματα. Μια απειλή μπορεί να οριστεί ως ο στόχος του εισβολέα ή ως ό, τι μπορεί να κερδίσει ο επιτιθέμενος όταν επιτίθεται στο σύστημα. Για να εντοπίσουμε όλες τις πιθανές απειλές και τα τρωτά σημεία, πρέπει να απαριθμήσουμε όλα τα αγαθά που ορίστηκαν στο προηγούμενο βήμα και να αναθεωρήσουμε μια λίστα πιθανών επιθέσεων για κάθε αγαθό. Το αποτέλεσμα είναι ένα προφίλ απειλών του συστήματος, το οποίο περιγράφει όλες τις πιθανές ευπάθειες και επιθέσεις. Για κάθε στοιχείο του προφίλ αυτού πρέπει να ληφθεί απόφαση για τον περιορισμό της απειλής με την εφαρμογή κάποιου είδους προστασίας στο σύστημα ή για τα αγαθά ή για την αποδοχή του κινδύνου. Αυτές οι επιλογές που γίνονται από τον σχεδιαστή ασφαλείας για να αποδεχθεί ή να μετριάσει τον κίνδυνο θα μετατραπούν στη συνέχεια σε απαιτήσεις ασφαλείας και τελικά θα εκδηλωθούν ως μέτρα ασφαλείας.

Συμπερασματικά, η εκτέλεση της διαδικασίας μοντελοποίησης των απειλών εξαρτάται από τη μεθοδολογία και την προσέγγιση της μοντελοποίησης των απειλών που χρησιμοποιείται, γεγονός που μπορεί να προσθέσει επιπλέον βήματα στη διαδικασία που περιγράφηκε παραπάνω. Πολλές διαφορετικές προσεγγίσεις και μεθοδολογίες μοντελοποίησης απειλών έχουν αναπτυχθεί για να ανταποκρίνονται καλύτερα στις ανάγκες των σχεδιαστών ασφάλειας. Οι επόμενες ενότητες παρέχουν μια επισκόπηση των διαφορετικών προσεγγίσεων και μεθοδολογιών μοντελοποίησης απειλών.

4.2 Διαφορετικές Προσεγγίσεις Μοντελοποίησης απειλών

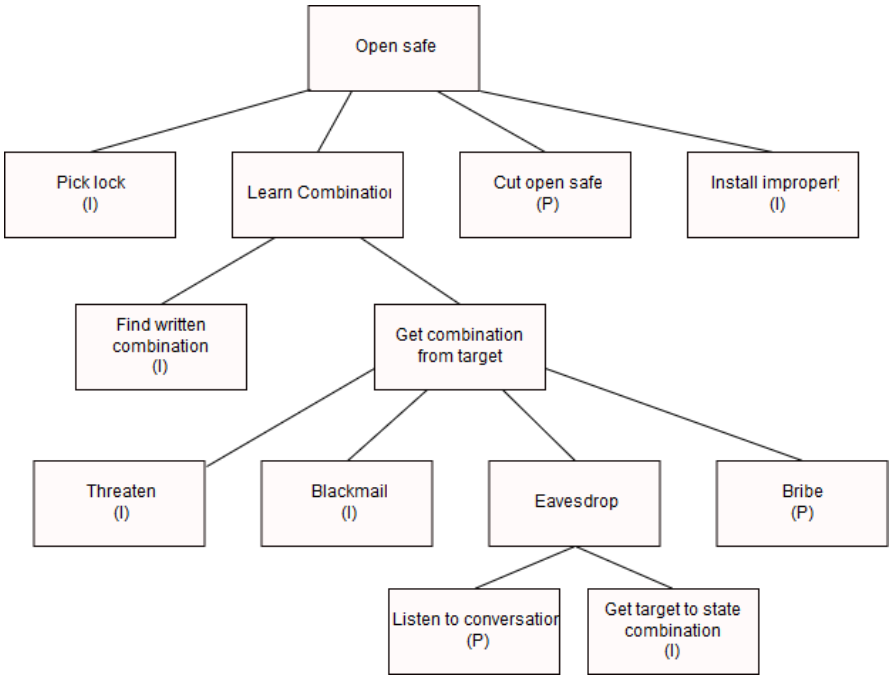
Η μοντελοποίηση των απειλών υλοποιείται συνήθως χρησιμοποιώντας μία από τις τρεις ανεξάρτητες προσεγγίσεις: attack centric, asset centric ή software centric. Η απόφαση του ποια προσέγγιση να χρησιμοποιήσει κάποιος εξαρτάται από τα εργαλεία και τις μεθόδους που χρησιμοποιούνται, τους περιορισμούς της επιλεγμένης προσέγγισης αλλά και τα πλεονεκτήματά της.

4.2.1 Attack centric

Η προσέγγιση μοντελοποίησης απειλών « Attack centric » επικεντρώνεται στην ασφάλεια του συστήματος από την άποψη των εισβολέων και στην αναγνώριση των σημείων πρόσβασης του συστήματος. Τα περισσότερα μοντέλα αυτού του τύπου αναγνωρίζουν τις αδυναμίες, συνοψίζοντας τις απειλές ως καταλόγους επιθέσεων ή ως δέντρα επίθεσης (Attack trees).Τα δέντρα επίθεσης παρέχουν μια δομημένη προσέγγιση για την περιγραφή της ασφάλειας ενός συστήματος. Η επίθεση που μπορεί να χρησιμοποιηθεί εναντίον του συστήματος παρουσιάζεται σε δομή δέντρου, όπου ο ριζικός κόμβος αντιπροσωπεύει το στόχο της επίθεσης και οι κόμβοι των φύλλων είναι οι διαφορετικοί τρόποι επίθεσης.

Ένα παράδειγμα ενός δέντρου επίθεσης απεικονίζεται στο Σχήμα 46, όπου φαίνονται οι πιθανές διαδρομές επίθεσης για να ανοίξει ένα χρηματοκιβώτιο. Αν και αυτό είναι ένα δέντρο επίθεσης που δεν σχετίζεται με την τεχνολογία πληροφοριών (IT), παρέχει μια καλή εικόνα για το πώς λειτουργεί ένα δέντρο επίθεσης. Ο ριζικός κόμβος δείχνει ποιος είναι ο σκοπός της επίθεσης και στην περίπτωση αυτή είναι το άνοιγμα ενός χρηματοκιβωτίου. Η πρώτη σειρά των κόμβων-παιδιών παρέχει όλους τους βιώσιμους τρόπους για το πώς ο εισβολέας μπορεί να ανοίξει το χρηματοκιβώτιο. Η επόμενη σειρά των κόμβων-παιδιών (3η σειρά) αντιπροσωπεύει τους δευτερεύοντες στόχους και τα παιδιά τους αντιπροσωπεύουν τους τρόπους για τον τρόπο επίτευξης αυτού του δευτερεύοντος στόχου.

Στο παρακάτω σχήμα αυτό σημαίνει ότι ο σκοπός της επίθεσης είναι να το άνοιγμα του χρηματοκιβωτίου. Ένας βιώσιμος τρόπος για να ανοίξει ένα χρηματοκιβώτιο από την άποψη του εισβολέα είναι να μάθουμε τον συνδυασμό, ο οποίος είναι κόμβος-παιδί του σκοπού (ή root / top κόμβος). Η τρίτη σειρά κόμβων δείχνει πώς ένας εισβολέας μπορεί να μάθει τον συνδυασμό του χρηματοκιβωτίου, για παράδειγμα με την υποκλοπή. Τα παιδιά του κόμβου αυτού δείχνουν δύο δυνατότητες για να ακούσουμε τον συνδυασμό του χρηματοκιβωτίου: να ακούσουμε τις συνομιλίες του θύματος ή να τον / την κάνουμε να αποκαλύψει τον συνδυασμό του χρηματοκιβωτίου. Δεδομένου ότι το να κάνουμε κάποιον να αποκαλύψει το συνδυασμό του χρηματοκιβωτίου δεν είναι εφικτό, η μόνη επιλογή που πρέπει να ληφθεί υπόψη για την εύρεση του συνδυασμού είναι η κατασκοπεία του θύματος και η ακρόαση όλων των συνομιλιών του. Σε περίπτωση που αυτό δεν είναι πάλι εφικτό, ο επιτιθέμενος μπορεί να πάει πίσω στο δέντρο και να αναζητήσει άλλες επιλογές επίθεσης που μπορεί να έχουν μεγαλύτερες πιθανότητες επιτυχίας.



Σχήμα 46: Ένα παράδειγμα δέντρου επίθεσης για το άνοιγμα ενός χρηματοκιβωτίου. Η τιμή μεταξύ των παρενθέσεων υποδεικνύει εάν η επιλογή επίθεσης είναι δυνατή (P) ή αδύνατη (I).

Συμπερασματικά, η προσέγγιση μοντελοποίησης απειλών « Attack centric » σε συνδυασμό με τη χρήση δέντρων επίθεσης ή καταλόγων επίθεσης είναι πολύ δημοφιλής μεταξύ των εμπειρογνωμόνων ασφαλείας, διότι είναι απλή στην ερμηνεία και στην κατανόηση, αλλά και παρέχει μια δομημένη προσέγγιση. Ωστόσο, υπάρχουν κάποια προβλήματα με αυτήν την προσέγγιση - επειδή οι ειδικοί ασφαλείας ακολουθούν έναν κατάλογο απειλών ή έναν δέντρο επίθεσης - δεν τους επιτρέπει να σκεφτούν τις απειλές που αντιπροσωπεύουν. Μπορεί να γίνουν πολύ σταθεροί με το δέντρο επίθεσης και να μην σκεφτούν κριτικά για οποιαδήποτε άλλη επιλογή επίθεσης που θα μπορούσε να έχει ο εισβολέας. Σύμφωνα με τη γνώμη κάποιων ειδικών ασφάλειας, δεν συνιστάται η χρήση της προσέγγισης αυτής ως μοντελοποίηση των απειλών, καθώς ο επιτιθέμενος έχει τα δικά του κίνητρα και ικανότητες, καθιστώντας έτσι δύσκολη την πρόβλεψη της προσέγγισης που μπορεί να χρησιμοποιήσει για να θέσει σε κίνδυνο το σύστημα.

4.2.2 Asset centric

Η προσέγγιση μοντελοποίησης απειλών « Asset centric » επικεντρώνεται στην προστασία της εσωτερικής υποδομής ενός συστήματος ή μιας εφαρμογής και στη διαχείριση του επιχειρηματικού κινδύνου. Η προσέγγιση αυτή χρησιμοποιείται συνήθως όταν πρέπει να προστατεύεται ένα αγαθό της πληροφορικής ή των επιχειρηματικών εφαρμογών - όπως δεδομένα, προσωπικές πληροφορίες κ.λπ. Όταν χρησιμοποιείται η συγκεκριμένη προσέγγιση μοντελοποίησης απειλών, οι επιχειρηματικοί στόχοι και τα πρότυπα ανάπτυξης του συστήματος ή της εφαρμογής θα είναι πιθανότατα γνωστά. Αυτό σημαίνει ότι οι έλεγχοι πρόσβασης και οι έλεγχοι των αγαθών θα γίνουν κατανοητοί, καθιστώντας έτσι μια ιδανική προσέγγιση για σαφώς διακεκριμένες επιχειρηματικές εφαρμογές με συγκεκριμένο στόχο.

Ωστόσο, υπάρχουν κάποιες ανησυχίες σχετικά με τη χρησιμότητα μιας προσέγγισης μοντελοποίησης απειλών τύπου« Asset centric » , λέγοντας ότι μόνο ένας μικρός αριθμός ανθρώπων θα επωφεληθεί από αυτήν. Σύμφωνα με τους εδικούς, υπάρχουν τρεις ερμηνείες του ορισμού ενός αγαθού: (1) τα πράγματα που θέλουν οι επιτιθέμενοι, (2) τα πράγματα που θέλουμε να προστατεύσουμε και (3)ο συνδυασμός αυτών των δύο. Εάν όλοι οι άνθρωποι που εμπλέκονται στη διαδικασία μοντελοποίησης απειλών δεν συμφωνούν για τον ορισμό ενός αγαθού, η όλη διαδικασία θα σταματήσει και θα γίνει πολύ περίπλοκη.

Κατά τα τελευταία έτη, διατέθηκαν αρκετοί κατάλογοι μέτρων ασφαλείας αλλά και εργαλεία για την καθοδήγηση για την προστασία των αγαθών μιας εταιρείας. Το Open Project Security Project (OWASP) - ένας παγκόσμιος μη κερδοσκοπικός οργανισμός που επικεντρώνεται στην ασφάλεια λογισμικού - διεξήγαγε έρευνα σε συσκευές IOT για να καταρτίσει έναν κατάλογο των κορυφαίων 10 τομέων επιθέσεων IOT και μετριασμών (OWASP, 2018). Αυτός ο κατάλογος μπορεί να χρησιμοποιηθεί για την προστασία των συσκευών IOT από τις πιο κοινές επιθέσεις και παρέχει σημαντικές πληροφορίες τεχνικού και επιχειρηματικού χαρακτήρα. Τέλος, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) έχει επίσης αναπτύξει ένα πλαίσιο ασφάλειας στον κυβερνοχώρο το οποίο επιτρέπει στις επιχειρήσεις να εξατομικεύουν τα μέτρα ασφαλείας και να τα κατηγοροποιούν σε ξεχωριστές κατηγορίες που συνδέονται με διάφορα είδη απειλών.

4.2.3 Software centric

Η προσέγγιση μοντελοποίησης απειλών « Software centric » είναι πιο κατάλληλη για συστήματα με άγνωστα πρότυπα ανάπτυξης και έχει σχεδιαστεί για να προστατεύει την ασφάλεια του κώδικα του λογισμικού. Η μοντελοποίηση αυτή επικεντρώνεται στο λογισμικό που κατασκευάζεται ή σχεδιάστηκε και αναζητά τις διάφορες επιθέσεις που μπορεί να εμφανιστούν στα διάφορα στοιχεία της εφαρμογής. Το πιο σημαντικό βήμα στη προσέγγιση αυτή είναι η κατανόηση του μοντέλου του λογισμικού που χρησιμοποιείται, είτε είναι απλό είτε είναι πολύπλοκο, και η διασφάλιση ότι όλοι οι συμμετέχοντες στο έργο έχουν καλή κατανόηση γι 'αυτό.

Αυτή η αμοιβαία κατανόηση του μοντέλου του λογισμικού μπορεί να προσφέρει σημαντική αξία και να οδηγήσει σε συνολική βελτίωση της ασφάλειας του λογισμικού. Ένα από τα βασικά πλεονεκτήματα αυτής της προσέγγισης μοντελοποίησης απειλών είναι ότι κάνει τους προγραμματιστές λογισμικού να συμμετέχουν στη διαδικασία μοντελοποίησης των απειλών και ότι το προκύπτον μοντέλο απειλών αλλά και το μοντέλο του λογισμικού μπορεί να χρησιμοποιηθεί από ολόκληρη την ομάδα. Αυτό θα οδηγήσει επίσης τους προγραμματιστές λογισμικού στην καλύτερη κατανόηση του οργανισμού καθώς και των αγαθών του οργανισμού.

4.3 Μεθοδολογίες Μοντελοποίησης απειλών

4.3.1 Μεθοδολογία STRIDE

Η μεθοδολογία STRIDE είναι μια δημοφιλής τεχνική μοντελοποίησης απειλών που δημιουργήθηκε από τη Microsoft, η οποία χρησιμοποιείται συνήθως στη βιομηχανία ασφάλειας και η Microsoft τη χρησιμοποιεί συνεχώς σε όλα τα προϊόντα της. Η μεθοδολογία STRIDE υποστηρίζεται από ορισμένες από τις πιο αναγνωρισμένες διαδικασίες ασφαλούς λογισμικού, όπως το Comprehensive, Lightweight, Application, Security Program (CLASP) και το SDL της Microsoft. Το STRIDE είναι ένα αρκτικόλεξο για τις διάφορες κατηγορίες απειλών που μπορεί να επηρεάσουν τα στοιχεία ενός συστήματος ή μιας εφαρμογής και αντιπροσωπεύει τα ακόλουθα:

- Πλαστογράφηση (Spoofing): Οι επιτιθέμενοι προσποιούνται ότι είναι κάποιος (ή κάτι άλλο).
- Αλλοίωση (Tampering): Οι εισβολείς αλλοιώνουν τα δεδομένα κατά τη μεταφορά τους ή και γενικά.
- Αποποίηση (Repudiation): Οι επιτιθέμενοι εκτελούν ενέργειες που δεν μπορούν να αναχθούν σε αυτούς.
- Αποκάλυψη πληροφοριών (Information disclosure): Οι εισβολείς κλέβουν τα δεδομένα κατά τη μεταφορά τους ή και γενικά.
- Άρνηση εξυπηρέτησης (Denial of service): Οι εισβολείς διακόπτουν τη νόμιμη λειτουργία του συστήματος.
- Αύξηση προνομίων (Elevation of privilege): Οι επιτιθέμενοι εκτελούν ενέργειες που δεν τους επιτρέπεται να εκτελέσουν.

Πιο αναλυτικά, η πλαστογράφηση (Spoofing) είναι όταν ο επιτιθέμενος προσποιείται ότι είναι κάτι ή κάποιος άλλος από τον εαυτό του. Για παράδειγμα, το να προσποιείται κάποιος ότι είναι το Google.com, συνεπάγεται την πλαστογράφηση της ταυτότητας μιας οντότητας σε ένα δίκτυο. Δεν υπάρχει αρχή διαμεσολάβησης που να αναλαμβάνει την ευθύνη να ενημερώσει τους χρήστες ότι το Google.com είναι ο ιστότοπος που όντως λέει οτί είναι. Αυτό διαφέρει από το δεύτερο παράδειγμα, καθώς τα Windows περιλαμβάνουν ένα αρχείο winsock.dll. Θα πρέπει να μπορούμε να ζητήσουμε από το λειτουργικό σύστημα να ενεργεί ως διαμεσολαβητική αρχή και να μας φέρει στο winsock. Εάν έχουμε τα δικά μας DLL, τότε πρέπει να βεβαιωθούμε ότι τα ανοίγουμε με την κατάλληλη διαδρομή (% installdir% \ dll). Διαφορετικά, κάποιος μπορεί να αντικαταστήσει κάποιον σε έναν κατάλογο εργασίας και να πάρει τον κώδικά μας για να κάνει ό, τι θέλει. (Παρόμοια ζητήματα υπάρχουν με τα UNIX και LD_PATH.) Τέλος, ένα παράδειγμα πλαστογράφησης μπορεί να θεωρηθεί και το spoofing Barack Obama, όπου προσποιούμαστε ότι είμαστε ένα συγκεκριμένο πρόσωπο.

Η αλλοίωση (Tampering) τροποποιεί κάτι, συνήθως σε δίσκο, σε δίκτυο ή στη μνήμη. Αυτό μπορεί να περιλαμβάνει την αλλαγή δεδομένων σε ένα υπολογιστικό φύλλο (χρησιμοποιώντας ένα πρόγραμμα όπως το Excel ή άλλο επεξεργαστή), την αλλαγή ενός δυαδικού αρχείου ή ενός αρχείου διαμόρφωσης στο δίσκο ή την τροποποίηση μιας πιο περίπλοκης δομής δεδομένων, όπως μια βάση δεδομένων στο δίσκο. Σε ένα δίκτυο, τα πακέτα μπορούν να προστεθούν, να τροποποιηθούν ή να καταργηθούν. Επιπλέον,οι επιτιθέμενοι μπορούν να τροποποιήσουν τα αρχεία όταν έχουν άδεια εγγραφής σε αυτά (write permission). Όταν ο κώδικας βασίζεται σε αρχεία που μπορούν να γράψουν οι άλλοι, υπάρχει πιθανότητα ότι το αρχείο αυτό να γράφτηκε κακόβουλα. Ενώ η πιο προφανής μορφή αλλοίωσης είναι σε έναν τοπικό δίσκο, υπάρχουν επίσης πολλοί τρόποι να το γίνει αυτό όταν το αρχείο περιλαμβάνεται εξ αποστάσεως, όπως το μεγαλύτερο μέρος της JavaScript στο Internet. Ο επιτιθέμενος μπορεί να παραβιάσει την ασφάλειά μας παραβιάζοντας τον ιστότοπο κάποιου άλλου. Μπορούν επίσης (εξαιτίας πλαστογράφησης ή αύξησης προνομίων) να τροποποιούν αρχεία που κατέχουμε. Τέλος, μπορούν να τροποποιήσουν συνδέσμους ή ανακατευθύνσεις διαφόρων ειδών.

Η αποποίηση (Repudiation) συμβαίνει όταν ο επιτιθέμενος ισχυρίζεται ότι δεν έκανε κάτι ή δεν ήταν υπεύθυνος για το τι συνέβη. Οι απειλές αυτού του τύπου είναι λίγο διαφορετικές από άλλες απειλές ασφαλείας, διότι συχνά εμφανίζονται στο επίπεδο επιχείρησης (business layer). Δηλαδή, πάνω από το

επίπεδο δικτύου, όπως το TCP / IP, πάνω από το επίπεδο εφαρμογής όπως το HTTP / HTML και όπου θα μπορούσε να εφαρμοστεί η επιχειρησιακή λογική της αγοράς προϊόντων. Οι απειλές που σχετίζονται με την αποποίηση συνδέονται επίσης με το σύστημα καταγραφής και τη διαδικασία καταγραφής. Εάν δεν υπάρχουν αρχεία καταγραφής, δεν διατηρούνται αρχεία καταγραφής ή δεν μπορούμε να αναλύσουμε αρχεία καταγραφής, οι απειλές αυτές είναι δύσκολο να εντοπιστούν. Υπάρχει επίσης μια κατηγορία επιθέσεων στις οποίες οι εισβολείς θα βάλουν δεδομένα στα αρχεία καταγραφής για να καταστήσουν δύσκολη την ανάλυση του αρχείου καταγραφής. Για παράδειγμα, εάν η εμφάνιση των αρχείων καταγραφής γίνεται σε HTML και ο εισβολέας στέλνει </ tr> ή </ html>, τότε η εμφάνιση του αρχείου καταγραφής πρέπει να τα αντιμετωπίζει ως δεδομένα και όχι ως κώδικα.

Η αποκάλυψη πληροφοριών (Information disclosure) σημαίνει ότι επιτρέπεται στους χρήστες να βλέπουν πληροφορίες τις οποίες δεν είναι εξουσιοδοτημένοι να βλέπουν. Πολλές περιπτώσεις στις οποίες μια διαδικασία θα αποκαλύψει πληροφορίες είναι αυτές που ενημερώνουν περαιτέρω επιθέσεις. Μια διαδικασία μπορεί να το κάνει αυτό διαγράφοντας διευθύνσεις μνήμης, εξάγοντας μυστικά από μηνύματα σφαλμάτων ή εξάγοντας λεπτομέρειες σχεδιασμού από μηνύματα σφαλμάτων. Οι διαρροές διευθύνσεων μνήμης μπορεί να βοηθήσει στην παράκαμψη του ASLR και παρόμοιων αμυντικών. Επιπλέον, δεδομένου ότι τα δεδομένα αποθηκεύονται, υπάρχει μια πληθώρα τρόπων που μπορούν να διαρρεύσουν. Η πρώτη αιτία είναι η αποτυχία για τη σωστή χρήση των μηχανισμών ασφαλείας. Για παράδειγμα, η μη κατάλληλη ρύθμιση των δικαιωμάτων ή η ελπίδα ότι κανείς δεν θα βρει ένα κρυμμένο αρχείο είναι συνηθισμένοι τρόποι με τους οποίους οι άνθρωποι αποτυγχάνουν να χρησιμοποιήσουν τους μηχανισμούς ασφαλείας. Τα κρυπτογραφικά κλειδιά είναι μια ειδική περίπτωση όπου η αποκάλυψη πληροφοριών επιτρέπει επιπρόσθετες επιθέσεις. Τα αρχεία που διαβάζονται από ένα χώρο αποθήκευσης δεδομένων μέσω του δικτύου συχνά διαβάζονται καθώς διέρχονται από το δίκτυο.

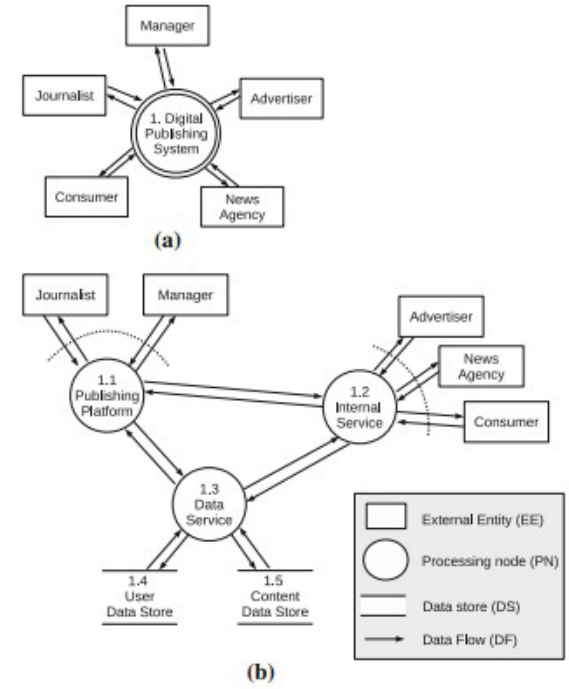
Οι επιθέσεις άρνησης εξυπηρέτησης (Denial of service) απορροφούν έναν πόρο που απαιτείται για την παροχή υπηρεσιών. Οι επιθέσεις άρνησης υπηρεσίας μπορούν να χωριστούν σε εκείνες που λειτουργούν ενώ ο επιτιθέμενος επιτίθεται (για παράδειγμα, γεμίζοντας το εύρος ζώνης) και σε εκείνες που επιμένουν. Οι επίμονες επιθέσεις (Persistent attacks) μπορούν να παραμείνουν σε ισχύ μέχρι την επανεκκίνηση (για παράδειγμα, while(1) {fork ();}), ή ακόμα και μετά την επανεκκίνηση (για παράδειγμα, γεμίζοντας ένα δίσκο). Οι επιθέσεις άρνησης εξυπηρέτησης μπορούν επίσης να χωριστούν σε ενισχυμένες και μη ενισχυμένες. Ενισχυμένες επιθέσεις (Amplified attacks) είναι εκείνες με τις οποίες η μικρή προσπάθεια ενός εισβολέα έχει μεγάλο αντίκτυπο στο σύστημα-στόχο.

Η αύξηση των προνομίων (Elevation of privilege) επιτρέπει σε κάποιον κακόβουλο να κάνει κάτι που δεν είναι εξουσιοδοτημένος να κάνει - για παράδειγμα, επιτρέποντας σε έναν κανονικό χρήστη να εκτελέσει κώδικα ως διαχειριστής (admin) ή επιτρέποντας σε ένα απομακρυσμένο άτομο (remote person) χωρίς δικαιώματα να εκτελεί κώδικα. Δύο σημαντικοί τρόποι για την αύξηση των προνομίων περιλαμβάνουν τη διαφθορά μιας διαδικασίας και τη λήψη προηγούμενων ελέγχων εξουσιοδότησης. Πιο αναλυτικά, η διαφθορά μιας διαδικασίας περιλαμβάνει τεχνικές όπως η κατάρρευση της στοίβας, η εκμετάλλευση δεδομένων στο σωρό και μια ολόκληρη ποικιλία τεχνικών εκμετάλλευσης. Η επίπτωση αυτών των τεχνικών είναι ότι ο επιτιθέμενος αποκτά επιρροή ή ελέγχει τη ροή ελέγχου ενός προγράμματος. Από την άλλη, υπάρχει επίσης μια σειρά από τρόπους για την ανύψωση των προνομίων μέσω αποτυχιών εξουσιοδότησης. Η απλούστερη αποτυχία είναι να μην ελέγχεται η εξουσιοδότηση σε κάθε διαδρομή. Τέλος, εάν ένα πρόγραμμα βασίζεται σε άλλα προγράμματα ή σύνολα δεδομένων που είναι αξιόπιστα, είναι σημαντικό να διασφαλιστεί ότι οι άδειες έχουν οριστεί έτσι ώστε κάθε μία από αυτές τις εξαρτήσεις να είναι σωστά εξασφαλισμένη.

Κατά την εφαρμογή της μεθοδολογίας STRIDE σε μια ανάλυση απειλών, ο αναλυτής ασφαλείας πρέπει να περάσει από αρκετά βήματα. Τα βήματα της μεθοδολογίας είναι τα εξής:

1. **Βήμα 1ο: Δημιουργία Διαγράμματος Ροής Δεδομένων (DFD)**

Στην καρδιά της μοντελοποίησης απειλών STRIDE βρίσκεται το διάγραμμα ροής δεδομένων DFD. Αυτή η γραφική αναπαράσταση βοηθά τον αναλυτή ασφαλείας να μελετήσει το σύστημα από την οπτική του εισβολέα και να αναλύσει τα επίπεδα εμπιστοσύνης που είναι διαθέσιμα στο σύστημα ή στην εφαρμογή. Τα διάφορα επίπεδα εμπιστοσύνης διαμορφώνονται στο DFD ως ένα όριο εμπιστοσύνης (trust boundary), όπου ένα αξιόπιστο στοιχείο και ένα αναξιόπιστο στοιχείο ανταλάσσουν δεδομένα. Τα διαφορετικά στοιχεία που έχουν διαμορφωθεί στο DFD παρέχουν τη δυνατότητα για την ανάλυση των απειλών. Το DFD μπορεί να μοντελοποιηθεί σε διάφορα επίπεδα λεπτομέρειας, γνωστό και ως λεπτομερειακό (granularity). Το υψηλότερο επίπεδο DFD, γνωστό ως DFD επιπέδου 1, δείχνει τον τρόπο ροής πληροφοριών μέσω του συστήματος ή της εφαρμογής από εξωτερικές οντότητες σε κόμβους επεξεργασίας και αποθήκες δεδομένων. Μάλιστα, το DFD επιπέδου 1 θα πρέπει να είναι απλό, εκτός εάν πρόκειται για πολύ περίπλοκα συστήματα. Το Σχήμα 47 δείχνει και ένα παράδειγμα ενός DFD επιπέδου 1 για ένα ψηφιακό σύστημα δημοσίευσης.



Σχήμα 47: Παράδειγμα DFD επιπέδου 1 για ένα ψηφιακό σύστημα δημοσίευσης

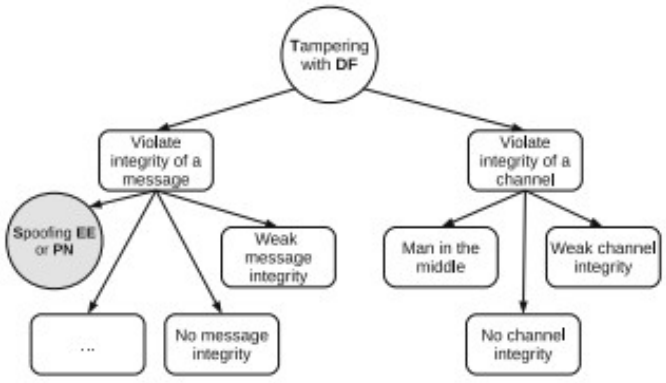
2. **Βήμα 2ο: Αντιστοίχιση των στοιχείων του διαγράμματος ροής δεδομένων στις κατηγορίες απειλών**

Αφού γίνει το διάγραμμα ροής δεδομένων, κάθε στοιχείο πρέπει να αναλυθεί σύμφωνα με τις κατηγορίες απειλών STRIDE. Οι διάφορες κατηγορίες απειλών μπορούν να βρεθούν στο ακρωνύμιο STRIDE που περιγράφηκε παρπάνω. Αυτός ο τρόπος χρήσης του STRIDE περιγράφεται από τον Shostack (2014) ως « STRIDE-ανά-στοιχείο » (STRIDE-per-Element). Αυτή η προσέγγιση μπορεί να διευκολύνει τον αναλυτή ασφαλείας να εντοπίσει τις απειλές εστιάζοντας στο σύνολο των απειλών κάθε στοιχείου. Συγκεκριμένα, αυτή η τεχνική μπορεί να βοηθήσει τους αναλυτές ασφαλείας να εντοπίσουν νέους τύπους αδυναμιών στα συστατικά μέρη του συστήματος αλλά και να εντοπίσουν κοινά προβλήματα. Ωστόσο, η προσέγγιση

« STRIDE-ανά-στοιχείο » έχει το μειονέκτημα ότι πολλά προβλήματα θα εμφανιστούν επανειλημμένα στο μοντέλο των απειλών. Ένας άλλος τρόπος ανάλυσης των απειλών είναι η ανάλυση όλων των διαφορετικών αλληλεπιδράσεων μεταξύ των συνιστωσώ του συστήματος, γνωστών και ως « STRIDE-per-Interaction ». Αυτή η μέθοδος αποδίδει ισοδύναμα αποτελέσματα με λιγότερα σημεία ανάλυσης.

3. Βήμα 3ο: Ανάλυση των απειλών

Στη συνέχεια, για κάθε κατηγορία απειλών που αντιστοιχεί σε ένα στοιχείο του διαγράμματος DFD, το STRIDE παρέχει μια λίστα ελέγχου των απειλών που πρέπει να εξεταστούν. Αυτή η λίστα ελέγχου απειλών παρουσιάζεται με τη μορφή ενός δέντρου επίθεσης και το βιβλίο αναφοράς για το STRIDE παρέχει συνολικά δώδεκα δέντρα επίθεσης (Σχήμα 48). Το επόμενο βήμα είναι να αναλύσουμε τον κίνδυνο της απειλής που εντοπίζεται στην εφαρμογή ή στο σύστημα. Για παράδειγμα, η μεθοδολογία *DREAD* (Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability) μπορεί να χρησιμοποιηθεί για να δώσει προτεραιότητα στις διάφορες απειλές. Για κάθε απειλή που προσδιορίζεται στα προηγούμενα βήματα δίνεται μια τιμή για κάθε κατηγορία DREAD. Όλες οι τιμές γι 'αυτή την απειλή προστίθενται στη συνέχεια μαζί για να υπολογιστεί το αντίκτυπου της απειλής. Η μεθοδολογία DREAD ήταν μέρος της μεθοδολογίας STRIDE μέχρι το 2010, αλλά είναι υποκειμενική στην κατάταξη των απειλών και μπορεί να οδηγήσει σε απρόβλεπτα και ποικίλα αποτελέσματα Η Microsoft τώρα συνιστά τη χρήση του συστήματος «Security Update Severity Rating ». Αυτό το νέο σύστημα ταξινομεί απειλές σε μία από τις 4 κατηγορίες με βάση την πιθανότητα εκμετάλλευσης μιας απειλής: χαμηλή, μέτρια, σημαντική και κρίσιμη. Στην παρούσα εργασία, θα γίνει στη συνέχεια χρήση της μεθοδολογίας DREAD για τη μοντελοποίηση των απειλών μιας διαδικτυακής εφαρμογής.



Σχήμα 48: Ένα παράδειγμα δέντρου επίθεσης που δείχνει πώς μπορεί να συμβεί παραβίαση της ροής δεδομένων. (DF = ροή δεδομένων, EE = εξωτερική οντότητα, PN = εσωτερική υπηρεσία).

4. Βήμα 4ο: Καταγραφή των απειλών

Στο τελευταίο βήμα της μεθοδολογίας STRIDE, όλες οι απειλές που ανακαλύπτονται πρέπει να καταγράφονται. Δεν υπάρχει υποχρεωτική ή συγκεκριμένη μορφή αυτού του βήματος. Η τεκμηρίωση των απειλών που εντοπίστηκαν κατά την εφαρμογή της μεθοδολογίας STRIDE στο υπό μελέτη σύστημα ή εφαρμογή είναι πολύ σημαντική από την οπτική της ασφάλειας, καθώς αποτελεί το τεκμήριο για όλα τα ευρήματα του αναλυτή και μάλιστα, μπορεί να αποτελέσει βοηθητικό εργαλείο σε παρόμοια εργασία κάποιου άλλου αναλυτή.

4.3.2 Μεθοδολογία LINDUNN: STRIDE ανάλυση για την προστασία του απορρήτου

Η ιδιωτικότητα παραβλέπεται τακτικά στη διαδικασία της μηχανικής λογισμικού και συχνά αποτελεί μόνο μια ανησυχία στο τέλος του κύκλου SDLC, γεγονός που καθιστά πιο δύσκολη και δαπανηρή τη διόρθωσή της. Ωστόσο, τα τελευταία χρόνια υπήρξε η εμφάνιση μιας νέας στάσης απέναντι στο απόρρητο, την οποία οι Cavoukian et al. (2010) αποκαλούν « ιδιωτικό απόρρητο ». Αυτή η προσέγγιση προωθεί δραστηριότητες που εστιάζονται στην προστασία της ιδιωτικής ζωής στα αρχικά στάδια του κύκλου ανάπτυξης του λογισμικού. Η μοντελοποίηση απειλών συμβάλλει στην εξάλειψη πιθανών απειλών για το σύστημα, αλλά μια μεθοδολογία όπως η STRIDE δεν γίνεται να εξαλείψει πιθανές απειλές για την προστασία του απορρήτου. Επομένως, δημιουργήθηκε μια τεχνική μοντελοποίησης απειλών που βασίζεται στην έννοια του απορρήτου, η LINDUNN. Η μεθοδολογία LINDUNN είναι μια τεχνική μοντελοποίησης απειλών, η οποία είναι συμπληρωματική της μεθοδολογίας STRIDE. Και οι δύο τεχνικές οδηγούνται από το μοντέλο, βασίζουν την ανάλυσή τους στο διάγραμμα ροής δεδομένων DFD της εφαρμογής ή του συστήματος και ακολουθούν τα ίδια βήματα για να ολοκληρώσουν την ανάλυσή τους. Όπως και η μεθοδολογία STRIDE, η LINDUNN είναι ένα ακρωνύμιο όπου κάθε γράμμα αναφέρεται σε πιθανή απειλή της ιδιωτικότητας για τις συνιστώσες του συστήματος ή της εφαρμογής. Οι Wuyts, Scandariato & Joosen (2014) ορίζουν το ακρωνύμιο LINDUNN ως εξής:

- Συνδεσιμότητα (L) - Linkability: συμβαίνει όταν κάποιος μπορεί να διακρίνει επαρκώς εάν σχετίζονται δύο στοιχεία ενδιαφέροντος (IOI) όπως τα αιτήματα ενός χρήστη.
- Αναγνωσιμότητα (I) - Identifiability: συμβαίνει όταν είναι δυνατό να εντοπιστεί η ταυτότητα ενός υποκειμένου (π.χ. ενός χρήστη).
- Μη αποποίηση (Nr) - Non-repudiation: συμβαίνει όταν είναι δυνατή η συγκέντρωση αποδεικτικών στοιχείων έτσι ώστε ένα μέρος να μην μπορεί να αρνηθεί την εκτέλεση μιας ενέργειας.
- Ανιχνευσιμότητα (D) - Detectability: συμβαίνει όταν κάποιος μπορεί να διακρίνει επαρκώς εάν υπάρχουν δύο στοιχεία ενδιαφέροντος (IOI) π.χ. σε ένα σύστημα.
- Αποκάλυψη πληροφοριών (Di) - Disclosure of information: είναι η έκθεση πληροφοριών σε άτομα που υποτίθεται ότι δεν έχουν πρόσβαση σε αυτήν.
- ‘Ελλειψη γνώσης (U) - Unawareness: συμβαίνει όταν ο χρήστης δεν γνωρίζει τις πληροφορίες που παρέχει στο σύστημα και τις συνέπειες της πράξης του.
- Μη συμμόρφωση (Nc) - Non-compliance: συμβαίνει όταν το σύστημα δεν συμμορφώνεται με τη νομοθεσία (προστασία δεδομένων), τις υπάρχουσες πολιτικές και τις συγκατθέσεις των χρηστών.

Οι Wuyts, Scandariato & Joosen εντόπισαν στην έρευνά τους ότι παρόλο που η μεθοδολογία LINDUNN χρειάζεται ορισμένες βελτιώσεις σε ορισμένους τομείς, θεωρήθηκε εύκολη στη χρήση και χρήσιμη από τους εμπειρογνώμονες σε θέματα απορρήτου. Αυτή η μεθοδολογία μπορεί να αποδειχθεί πολύ χρήσιμη για τους εμπειρογνώμονες στον τομέα της προστασίας της ιδιωτικής ζωής, καθώς ο γενικός κανονισμός για την προστασία των προσωπικών δεδομένων GDPR τέθηκε σε ισχύ στις 25 Μαΐου 2018 (GDPR EU, 2018). Αυτός ο ευρωπαϊκός κανονισμός ρυθμίζει τη συλλογή και την αποθήκευση των προσωπικών στοιχείων (Personally Identifiable Information - PII) των ευρωπαίων πολιτών. Επίσης, διέπει τον τρόπο με τον οποίο οι εταιρείες πρέπει να αντιμετωπίζουν τυχόν παραβιάσεις δεδομένων που ενδέχεται να προκύψουν. Βλέποντας τον τρόπο με τον οποίο ο κανονισμός GDPR δίδει έμφαση στην προστασία της ιδιωτικής ζωής και των δεδομένων, η μοντελοποίηση των απειλών θα μπορούσε να διαδραματίσει σημαντικό ρόλο στην προετοιμασία των εταιρειών για αυτόν τον κανονισμό. Δεδομένου ότι τα πρόστιμα για μη συμμόρφωση με τον κανονισμό GDPR έχουν καθοριστεί σε 20 εκατομμύρια ευρώ ή 4% ετήσιο συνολικό κύκλο εργασιών, οι εταιρείες έχουν κίνητρο να συμμορφωθούν με τον νέο κανονισμό.

4.3.3 Μεθοδολογία Trike

Η μεθοδολογία μοντελοποίησης απειλών Trike είναι ένα πλαίσιο ανοιχτού κώδικα για τη μοντελοποίηση απειλών που επικεντρώνεται σε μια προσέγγιση βασισμένη στον κίνδυνο (risk-based approach) που είναι παρόμοια με τη μεθοδολογία STRIDE της Microsoft. Τα μοντέλα απειλών Trike επικεντρώνονται στην επίδραση πάνω στους ενδιαφερόμενους του συστήματος, ενώ τα μοντέλα τύπου STRIDE επικεντρώνονται περισσότερο στην αναπαράσταση των απειλών και των επιθέσεων. Ο στόχος της μεθοδολογίας Trike είναι ότι ο κίνδυνος ασφάλειας για τα αγαθά του συστήματος είναι αποδεκτός για όλους τους ενδιαφερόμενους (OWASP, 2017). Το εργαλείο Trike, το οποίο είναι επίσης διαθέσιμο με το έγγραφο Trike που διευκρινίζει τη μεθοδολογία, ενσωματώνει μια προσέγγιση attack centric και software centric. Ωστόσο, το εργαλείο Trike δεν έχει ενημερωθεί από το 2012 και το έγγραφο Trike κυκλοφόρησε μόνο ως πρόχειρη έκδοση. Επομένως, είναι δύσκολο να εκτιμηθεί πόσο ευρέως χρησιμοποιείται αυτή η μεθοδολογία και το εργαλείο αυτό.

4.3.4 Μεθοδολογία VAST

Η μεθοδολογία μοντελοποίησης απειλών VAST (Visual, Agile και Simple Threat modeling) επικεντρώνεται στην επεκτασιμότητα της διαδικασίας μοντελοποίησης των απειλών και στην ενσωμάτωση σε περιβάλλον ανάπτυξης λογισμικού της Agile. Επιδιώκει να αποδώσει αποτελέσματα για όλους τους ενδιαφερόμενους σε έναν οργανισμό: από προγραμματιστές και αρχιτέκτονες συστημάτων έως αναλυτές ασφαλείας και στελέχη επιχειρήσεων. Η μεθοδολογία αυτή παρέχει έναν μοναδικό και απλό τρόπο για την απεικόνιση των αρχιτεκτονικών συστημάτων και εφαρμογών και δεν απαιτεί εκτεταμένη τεχνογνωσία ασφάλειας, καθιστώντας έτσι δυνατή την πρόσβαση σε ένα ευρύτερο κοινό. Από όσο γνωρίζουμε, δεν έχει κυκλοφορήσει κανένα επίσημο έγγραφο μεθοδολογίας από τους δημιουργούς καθώς παραμένει ακόμα σε πρόχειρο στάδιο.

4.3.5 Μεθοδολογία PASTA

Η διαδικασία προσομοίωσης επίθεσης και ανάλυσης απειλών (Process for Attack Simulation and Threat Analysis - PASTA) είναι μια μεθοδολογία μοντελοποίησης απειλών που επικεντρώνεται στους κινδύνους (risk centric). Συγκεκριμένα, η μεθοδολογία PASTA ενσωματώνει την ανάλυση των απειλών ενός συστήματος ή μιας εφαρμογής με επιχειρηματικούς στόχους, με επιχειρηματική ανάλυση και με συμμόρφωση. Εφαρμόζει μια διαδικασία επτά βημάτων η οποία αρχίζει με τον καθορισμό των επιχειρηματικών στόχων, συνεχίζει με την αποσύνθεση της εφαρμογής ή του συστήματος και την ανάλυση των απειλών και τελειώνει με την ανάλυση του πιθανού αντίκτυπου στον οργανισμό. Αυτή η εστίαση στον αντίκτυπο των απειλών για την ασφάλεια των μετόχων και του οργανισμού είναι αυτό που κάνει τη μεθοδολογία PASTA να ξεχωρίζει από άλλες μεθοδολογίες μοντελοποίησης απειλών.

4.4 Εργαλεία μοντελοποίησης απειλών και επιστημονική συμβολή

Η επιλογή των εργαλείων μοντελοποίησης των απειλών είναι εξίσου σημαντική με τη μεθοδολογία επιλογής της μοντελοποίησης των απειλών. Η μοντελοποίηση των απειλών μπορεί να γίνει χωρίς τη χρήση εργαλείων, αλλά οι περισσότεροι χρήστες θα επωφεληθούν από μια πιο δομημένη και καθοδηγούμενη προσέγγιση. Υπάρχει μια ευρεία ποικιλία διαφορετικών διαθέσιμων εργαλείων, τα οποία διαφέρουν μεταξύ τους στις λειτουργίες τους, στην πολυπλοκότητα τους και στην εξειδίκευση τους. Το ευρύ φάσμα των διαθέσιμων εργαλείων μπορεί να κυμαίνεται από μη δομημένα έγγραφα κειμένου ή λογισμικό χαρτογράφησης που εξειδικεύεται στην ανάλυση απειλών, μέχρι και εξειδικευμένα εργαλεία που αυτοματοποιούν ολόκληρη τη διαδικασία μοντελοποίησης των απειλών. Συγκεκριμένα, το φάσμα των διαθέσιμων εργαλείων μοντελοποίησης των απειλών έχει δύο άκρα: (1) χρειάζεται ένα συγκεκριμένο μοντέλο δεδομένων για τη δημιουργία της ανάλυσης των απειλών και (2) χρειάζεται συγκεκριμένα εργαλεία που αναγκάζουν τα δεδομένα να συμμορφώνονται με μια συγκεκριμένη δομή.

Τα γενικά εργαλεία έχουν το πλεονέκτημα ότι είναι ευέλικτα, καθώς υπάρχουν ελάχιστοι περιορισμοί ως προς τον τρόπο δομής των δεδομένων. Ωστόσο, το μειονέκτημα των γενικών εργαλείων είναι ότι είναι δύσκολο να επαναχρησιμοποιηθούν τα δεδομένα του μοντέλου απειλής για συγκρίσιμα μοντέλα απειλών. Από την άλλη πλευρά, τα εξειδικευμένα εργαλεία μπορούν να αυτοματοποιήσουν τη διαδικασία μοντελοποίησης των απειλών, δεδομένου ότι τα δεδομένα πρέπει να ταιριάζουν σε μια συγκεκριμένη μορφή. Ωστόσο, αυτός ο περιορισμός στα δεδομένα εισόδου καθιστά τις εφαρμογές αυτών των εργαλείων περιορισμένες. Σήμερα, υπάρχουν διαθέσιμα στο κοινό εργαλεία μοντελοποίησης απειλών, τα οποία παράγουν πιο αξιόπιστα και συνεπή αποτελέσματα, δημιουργώντας αυτόματα καταλόγους πιθανών απειλών. Ωστόσο, μέχρι σήμερα έχουν πραγματοποιηθεί λίγες εμπειρικές μελέτες για την ποσοτικοποίηση της αποτελεσματικότητας τέτοιων αυτοματοποιημένων εργαλείων μοντελοποίησης απειλών.

Οι Möckel & Abdallah (2010) μελέτησαν την αποδοτικότητα δύο εργαλείων μοντελοποίησης απειλών της Microsoft για την ασφάλεια μιας εφαρμογής e-banking: το εργαλείο ανάλυσης και μοντελοποίησης απειλών (Threat Analysis & Modelling Tool - TAM) και το εργαλείο μοντελοποίησης απειλών κατά τον κύκλο ζωής της ασφάλειας (Security Development Lifecycle Threat Modelling tool). Κατέληξαν στο συμπέρασμα ότι το πλεονέκτημα της ύπαρξης διαδικασίας μοντελοποίησης των απειλών με τη βοήθεια λογισμικού καθίσταται εμφανές, όταν το εργαλείο δημιουργεί έναν εκτεταμένο κατάλογο πιθανών απειλών, ακόμη και αν αυτές είναι μικρότερης σημασίας. Αυτό αναγκάζει τον χρήστη να σκεφτεί κριτικά όλες τις πιθανές απειλές που παρουσιάζονται, ακόμα κι αν είναι απίθανες. Ωστόσο, αυτό το πολύ χρήσιμο χαρακτηριστικό των εργαλείων έχει το μειονέκτημα ότι ο χρήστης πρέπει ακόμα να παρέχει λογική συμβολή και να ερμηνεύει σωστά τα αποτελέσματα με βάση την εμπειρία του.

Επίσης, οι Möckel & Abdallah κατέληξαν στο συμπέρασμα ότι τα πλεονεκτήματα μιας διαδικασίας μοντελοποίησης απειλών με τη βοήθεια λογισμικού θα έχουν νόημα μόνο στην περίπτωση που το αποτέλεσμα της διαδικασίας θα χρησιμοποιηθεί για τη βελτίωση της ασφάλειας του συστήματος. Έτσι, παρόλο που τα εργαλεία μοντελοποίησης των απειλών μπορούν να προσφέρουν καθοδήγηση και βοήθεια στον χρήστη, εναπόκειται στα άτομα με άφθονη γνώση και εμπειρογνωμοσύνη να μετατρέψουν το αποτέλεσμα της διαδικασίας σε ένα σχέδιο που μπορεί να εκτελεστεί. Τα δύο εργαλεία μοντελοποίησης της απειλής της Microsoft, τα οποία μελέτησαν οι Möckel & Abdallah (2010), έχουν συγχωνευθεί από τότε σε ένα εργαλείο: το *Microsoft Threat Modeling Tool*. Μια μελέτη σχετικά με την αποτελεσματικότητα του εργαλείου Microsoft Threat Modeling Tool πραγματοποιήθηκε από τους Williams & Yuan (2015). Στη μελέτη αυτή, υπολόγισαν την αποτελεσματικότητα του εργαλείου Microsoft Threat Modeling Tool συγκρίνοντας τα αποτελέσματα μιας manual threat modelling exercise (χωρίς εξειδικευμένα εργαλεία μοντελοποίησης απειλών) με τα αποτελέσματα της ίδιας άσκησης που πραγματοποιήθηκε με το εργαλείο Microsoft Threat Modeling Tool. Με βάση τη μελέτη αυτή, η οποία διεξήχθη σε είκοσι προπτυχιακούς φοιτητές υπολογιστών, διαπιστώθηκε ότι με τη χρήση του Microsoft Threat Modeling Tool τα συνολικά αποτελέσματα ήταν καλύτερα και οι περισσότερες απειλές έχουν εντοπιστεί σωστά. Οι Williams & Yuan (2015) σημειώνουν ότι τα αποτελέσματα ποικίλλουν από φοιτητή σε φοιτητή και εξαρτώνται από την πληρότητα του διαγράμματος ροής δεδομένων DFD που παρήγαγε ο φοιτητής.

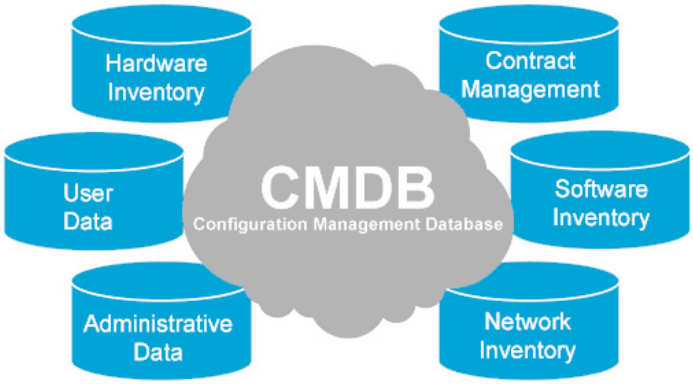
Οι αποκλίσεις στα διαγράμματα ροής δεδομένων DFD και των στοιχείων τους προκάλεσαν διακυμάνσεις στις απειλές που εντοπίστηκαν. Αυτή η απόκλιση μπορεί να ερμηνευθεί από την έλλειψη εμπειρίας ή γνώσης σχετικά με τη μοντελοποίηση απειλών. Τέλος, οι Williams και Yuan (2015) κατέληξαν στο συμπέρασμα ότι το Microsoft Threat Modeling Tool βοήθησε όντως τα αποτελέσματα μοντελοποίησης απειλών από τους φοιτητές. Άλλη έρευνα σχετικά με τα εργαλεία μοντελοποίησης των απειλών έχει επικεντρωθεί στην ανάπτυξη και στην επικύρωση ενός νέου εργαλείου ή πλαισίου μοντελοποίηση των απειλών. Οι περισσότερες μελέτες επικεντρώνονται στα εργαλεία που αναπτύσσουν οι ερευνητές και λίγες μελέτες επικεντρώνονται στη μέτρηση της αποτελεσματικότητας των διαθέσιμων στο κοινό εργαλείων της μοντελοποίησης των απειλών. Συμπερασματικά, η αποτελεσματικότητα των εργαλείων θα δοκιμαστεί χρησιμοποιώντας επαγγελματίες ασφαλείας, οι οποίοι θα επιλέξουν τα κατάλληλα εργαλεία μοντελοποίησης απειλών και αυτό με τη σειρά του θα αποτελέσει ένα βήμα για περαιτέρω έρευνα σχετικά με την αποτελεσματικότητα των εργαλείων μοντελοποίησης απειλών.

5 ΚΕΦΑΛΑΙΟ 5: Διαδικτυακή εφαρμογή uCMDB και μοντελοποίηση των απειλών μέσω του εργαλείου Microsoft Threat Modelling Tool

5.1 Περιγραφή της εφαρμογής uCMDB

Μια CMDB (configuration management database) είναι μια βάση δεδομένων που περιέχει όλες τις σχετικές πληροφορίες σχετικά με τα στοιχεία υλικού και λογισμικού που χρησιμοποιούνται στις υπηρεσίες IT ενός οργανισμού και τις σχέσεις μεταξύ αυτών των στοιχείων. Μια βάση CMDB παρέχει μια οργανωμένη οπτική των δεδομένων διαμόρφωσης και ένα μέσο για την εξέταση αυτών των δεδομένων από οποιαδήποτε επιθυμητή προοπτική.

Καθώς η IT υποδομή γίνεται όλο και πιο σύνθετη, η σημασία της παρακολούθησης και κατανόησης των πληροφοριών στο περιβάλλον IT αυξάνεται. Η χρήση των CMDB είναι μια βέλτιστη πρακτική που διευκολύνει τους ενδιαφερόμενους να εντοπίσουν και να ελέγξουν κάθε στοιχείο της υποδομής τους για καλύτερη διαχείριση και βελτίωση. Στο πλαίσιο μιας βάσης CMDB, τα στοιχεία ενός συστήματος πληροφοριών αναφέρονται ως στοιχεία διαμόρφωσης (CI- configuration item). Ένα στοιχείο διαμόρφωσης CI μπορεί να είναι οποιαδήποτε πιθανή IT συνιστώσα, συμπεριλαμβανομένου λογισμικού, υλικού, τεκμηρίωσης και προσωπικού, καθώς και οποιουδήποτε συνδυασμού αυτών ή εξαρτήσεων μεταξύ τους. Οι διαδικασίες διαμόρφωσης της διαχείρισης (configuration management) επιδιώκουν να καθορίσουν, να ελέγξουν και να παρακολουθήσουν τα στοιχεία διαμόρφωσης και τις τυχόν αλλαγές που γίνονται σ 'αυτές με ολοκληρωμένο και συστηματικό τρόπο.



Σχήμα 49: CMDB - Configuration Management Database

Για την εργασία αυτή, έγινε επιλογή του λογισμικού uCMDB. Η uCMDB, ένα προϊόν της Hewlett Packard, είναι ένα λογισμικό που συνδυάζει μια κλασσική CMDB μαζί με δυνατότητες IT infrastructure discovery. Επίσης, υποστηρίζει ITIL Configuration Management με την λειτουργία μιας Configuration Management Database. Η πιο σημαντική λειτουργία όμως είναι η διαδικασία του discovery IT infrastructure components. Ανάμεσα σε αυτά βρίσκονται δικτυακές συσκευές, φυσικοί και virtual servers καθώς και οι αντίστοιχες σχέσεις που υπάρχουν μεταξύ τους.

Πιο αναλυτικά, τα βασικά components της εφαρμογής ώστε να υλοποιηθεί μια ολοκληρωμένη CMDB λύση είναι τα εξής:

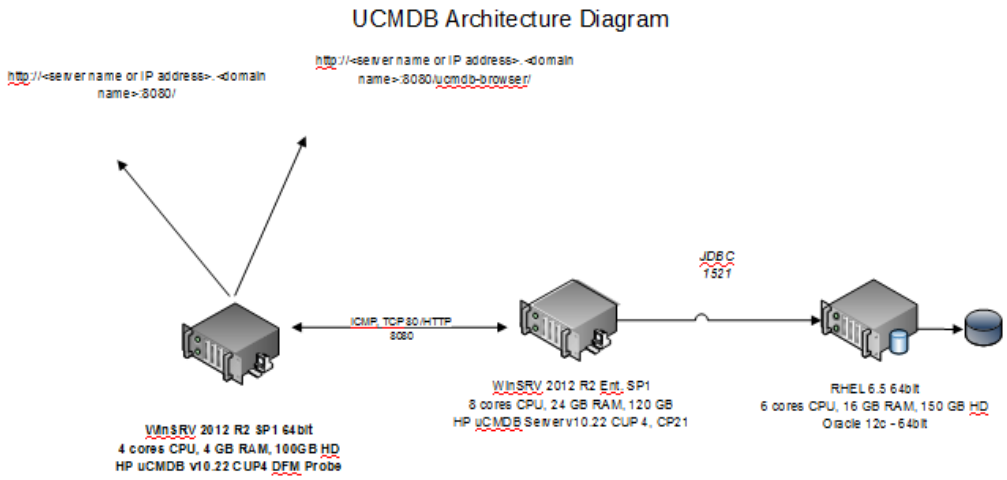
- **uCMDB Admin UI**: Σε αυτό το interface μπορεί ο εκάστοτε admin να συνδεθεί για να εκτελέσει τα διάφορα uCMDB tasks. Το συγκεκριμένο UI « ακούει » στην πόρτα 8080 και μπορεί να υποστηρίξει http, https και μπορεί να βρίσκεται είτε μόνο σε ένα intranet είτε και στο internet ανάλογα με τις ανάγκες του οργανισμού. Επίσης είναι συνδεδεμένο με τον web server.

- **uCMDB Browser:** Σε αυτό το UI συνδέονται οι τελικοί χρήστες της uCMDB. Αυτό το UI δεν εξυπηρετεί για administration αλλά περισσότερο για users που είναι καταναλωτές και όχι implementers. Δηλαδή εδώ οι χρήστες μπορούν να δούνε reports και πληροφορίες για infrastructure assets με μικρή δυνατότητα αλλαγής των πληροφοριών αυτών. Το συγκεκριμένο UI « ακούει » στην πόρτα 8080 και μπορεί να υποστηρίξει http, https και μπορεί να βρίσκεται σε ένα intranet μόνο ή και στο internet ανάλογα με τις ανάγκες του οργανισμού. Επίσης, εδώ μπορεί να δημιουργηθούν διάφορα widgets τα οποία προσφέρουν προσαρμοσμένες στον τελικό χρήστη λύσεις.
- **DF Probe – Probe DB:** Αυτό το component χρησιμεύει στο discovery όλων των infrastructure assets του οργανισμού. Αυτή η διαδικασία γίνεται triggered από ένα module του application sever μέσω της χρήσης πολλών σε αλληλουχία python scripts στα οποία έχουν οριστεί τα πρωτόκολλα επικοινωνίας και οι αντίστοιχες πόρτες. Στην συνέχεια, κανονικοποιεί τα αποτελέσματα και μέσω της λειτουργίας integration, στέλνει τα αποτελέσματα δηλαδή τα Configuration items (CIs) μέσω του web server στην βάση της uCMDB. Επικοινωνία γίνεται μέσω της πόρτας http/https 8080 από το server του probe στον web server και αντίστροφα στην πόρτα 80.
- **uCMDB Web server:** Στον web server εκτελούνται όλες οι σημαντικές λειτουργίες, όπως η αποστολή queries στην βάση του db server. Οι εφαρμογές που μπορεί κάποιος να χρησιμοποιήσει μέσω του admin UI και uCMDB browser είναι ενδεικτικά: impact analysis, reporting, reconciliation, enrichment, modeling, security, federation, TQL/UDM, resources. Η επικοινωνία με την βάση μέσω του database server γίνεται με JDBC driver στην πόρτα 1521 (για oracle σχήμα). Ο web server και ο database server πρέπει να είναι στο ίδιο lan χωρίς firewall και proxy ανάμεσα**.**
- **uCMDB Database Server:** Ο database server φιλοξενεί την βάση της uCMDB. Μπορεί να φιλοξενήσει Microsoft SQL server, Oracle ή PostgreSQL. Στην βάση γίνεται όλη η επεξεργασία των δεδομένων που γράφει ο web server. Όταν ο web server στέλνει query στην βάση, εκεί γίνεται ο υπολογισμός και το αποτέλεσμα στέλνεται πίσω μέσω του JDBC driver.

5.2 Αρχιτεκτονική της εφαρμογής uCMDB

Στην ενότητα αυτή παρουσιάζεται η ενδεικτική αρχιτεκτονική διασύνδεσης των βασικών components για την version του software 10.22 CUP 4, CP21. Θεωρούμε ότι η όλη διασύνδεση βρίσκεται σε ένα εταιρικό intranet και local IPs χωρίς την δυνατότητα να μπορεί να βγει στο internet. Επίσης, θεωρούμε ότι έχουμε έναν administrator user για τα windows server machines και πρόσβαση στη θύρα 3389, όπως και έναν user root για το redhat μηχάνημα. Αυτοί οι χρήστες έχουν δοθεί για την διαδικασία εγκατάστασης και συντήρησης/patching της υποδομής.

Το παρακάτω διάγραμμα απεικονίζει την αρχιτεκτονική της εφαρμογής uCMDB μαζί με τα dependencies των βασικών components:



Σχήμα 50: Διάγραμμα Αρχιτεκτονικής της εφαρμογής uCMDB

Στον πίνακα που ακολουθεί περιγράφεται αναλυτικά για κάθε component της εφαρμογής uCMDB που είδαμε στην προηγούμενη ενότητα τι αρχιτεκτονική ακολουθεί:

Component	Architecture
uCMDB Admin UI	web-based μέσω http 8080 http://<server name or IP address>.<domain name>:8080/
uCMDB Browser	web-based μέσω http 8080 http://<server name or IP address>.<domain name>:8080/ucmdb-browser/
DF Probe – Probe DB	http 8080 WinSRV 2012 R2 SP1 64bit 4 cores CPU, 4 GB RAM, 100GB HD HP uCMDB v10.22 CUP4 DFM Probe
uCMDB Web server	web server http 8080 WinSRV 2012 R2 Ent. SP1 8 cores CPU, 24 GB RAM, 120 GB HP uCMDB Server v10.22 CUP 4, CP21
uCMDB Database Server	JDBC 1521 RHEL 6.5 64bit

	6 cores CPU, 16 GB RAM, 150 GB HD Oracle 12c - 64bit

Σχήμα 51: Πίνακας Component - Architecture της εφαρμογής uCMDB

Στην εφαρμογή uCMDB οι χρήστες που μπορεί να υπάρξουν είναι οι εξής (Trust levels):

1. Admin με έγκυρα στοιχεία αυθεντικοποίησης (login credentials): Ο χρήστης αυτός έχει διακαίωμα πρόσβασης στον στον web server, uCMDB UI, uCMDB browser και πλήρη δικαιώματα implementation.
2. Χρήστης (όχι admin) με λανθασμένα στοιχεία αυεθντικοποίησης: Πρόκειται για χρήστη του οργανισμού ο οποίος έχει πρόσβαση στο url της εφαρμογής αλλά δεν έχει valid credentials.
3. Installation user: Ο συγκεκριμένος χρήστης διαθέτει admin credentials αλλά και δικαιώματα εγκατάστασης.
4. Integration user: Χρήση για integration μεταξύ των components της εφαρμογής καθώς και δικαίωμα read/write στην βάση.
5. Τελικός χρήστης (End user): Ο χρήστης αυτός έχει δικαίωμα πρόσβασης στο uCMDB UI και στον uCMDB browser αλλά με δικαιώματα read only.
6. Implementation user: Ο συγκεκριμένος χρήστης μπορεί να δημιουργεί queries, discovery IT data, views, enrichments, credentials (encrypted), integration points αλλά και να διαχερίζεται την εφαρμογή και να αλλάζει ορισμένες ρυθμίσεις της π.χ. infrastructure settings.

Τα επίπεδα εμπιστοσύνης (Trust levels) έχουν εκχωρηθεί σε σημεία εισόδου / εξόδου για να καθορίσουν τα προνόμια που πρέπει να έχει μια εξωτερική οντότητα προκειμένου να έχει πρόσβαση στο σύστημα αλλά και να το επηρεάσει. Τα επίπεδα εμπιστοσύνης κατηγοριοποιούνται σύμφωνα με τα προνόμια που έχουν εκχωρηθεί και διασταυρώνονται με σημεία εισόδου / εξόδου και προστατευόμενους πόρους.

Στη συνέχεια, θα ορίσουμε τα entry points της εφαρμογής uCMDB. Ένα σημείο εισαγωγής (entry point) της εφαρμογής προσδιορίζει έναν πόρο που είναι ουσιαστικά ένα σημείο πρόσβασης σε μια εφαρμογή. Τα σημεία εισαγωγής εφαρμογών χρησιμοποιούνται για τον έλεγχο της πρόσβασης των χρηστών σε διαφορετικές εκδόσεις μιας εφαρμογής που αναπτύσσεται σε μια πλατφόρμα. Χρησιμοποιούνται επίσης για τη δημιουργία πλαισίου εφαρμογών με σκοπό την παρακολούθηση της χρήσης των πόρων των εφαρμογών αυτών, αλλά και για τον προσδιορισμό μιας εφαρμογής που εκτελείται.

Έτσι, τα σημεία εισαγωγής (entry points) της εφαρμογής uCMDB είναι τα παρακάτω:

1. Μη εξουσιοδοτημένη πρόσβαση στον web server port 3389
2. Παραποίηση του JDBC driver port 1521
3. Από το admin UI στην 8080 http
4. Από το browser UI στην 8080 http
5. Μη εξουσιοδοτημένη πρόσβαση στον database server ssh port 22
6. Μη εξουσιοδοτημένη πρόσβαση στον server του DF probe port 3389
7. Υποκλοπή του installation χρήστη ports 22,3389

Για παράδειγμα, για το entry point 1 το trust level είναι ο admin με έγκυρα credentials ή ο Installation user ενώ για το entry point 3 είναι ο admin με έγκυρα credentials ή ο τελικός χρήστης ή και ο Integration user. Σε επόμενη ενότητα, θα παρουσιαστούν σε μορφή πίνακα όλα τα entry points της εφαρμογής uCMDB μαζί με τα αντίστοιχα trust levels.

Όσον αφορά στα αγαθά της εφαρμογής uCMDB, παρακάτω παρατίθεται η αρχιτεκτονική της εφαρμογής, ώστε να γίνει κατανοητή η ανταλλαγή πληροφορίας σε κάθε σελίδα της. Τα αγαθά είναι ο λόγος για τον οποίο υπάρχουν οι απειλές. Ο στόχος ενός αντιπάλου είναι να αποκτήσει πρόσβαση σε ένα αγαθό. Η ομάδα ασφαλείας πρέπει να προσδιορίσει ποια στοιχεία πρέπει να προστατεύονται από μη εξουσιοδοτημένους χρήστες. Επιπλέον, τα αγαθά μπορούν να αλληλεπιδράσουν με άλλα αγαθά και, ως εκ τούτου, μπορούν να λειτουργήσουν ως σημείο διέλευσης για έναν αντίπαλο.

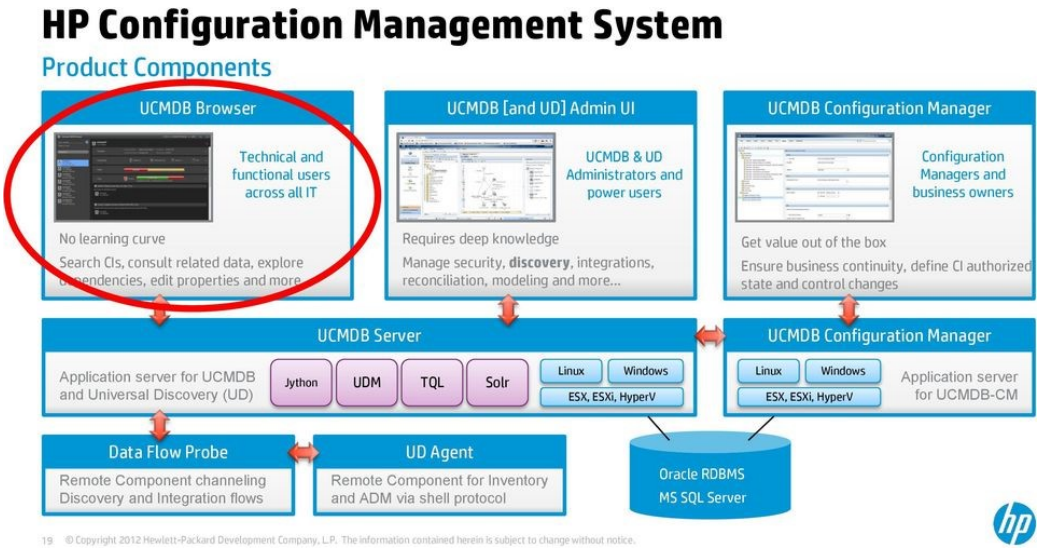
Έτσι, οι βασικές σελίδες της εφαρμογής uCMDB είναι τρεις και υπάρχουν στο Admin UI. Στο Admin UI, ο χρήστης ανάλογα με τα δικαιώματα που έχει (read/write) μπορεί να χειριστεί όλες τις λειτουργίες της uCMDB. Πρόσβαση έχουν οι implementation user (admin) και end user. Οι βασικές σελίδες είναι οι εξής:

1. **Discovery Control panel:** Εδώ μπορεί να κάνει trigger λειτουργίες στον web server, πρόσβαση στα resources να χειριστεί το federation και να προβεί σε UDM/TQL. Μπορεί σε αυτή την σελίδα να χειριστεί και το df probe. Από εδώ οι πληροφορίες καταχωρούνται στην βάση μέσω web server.

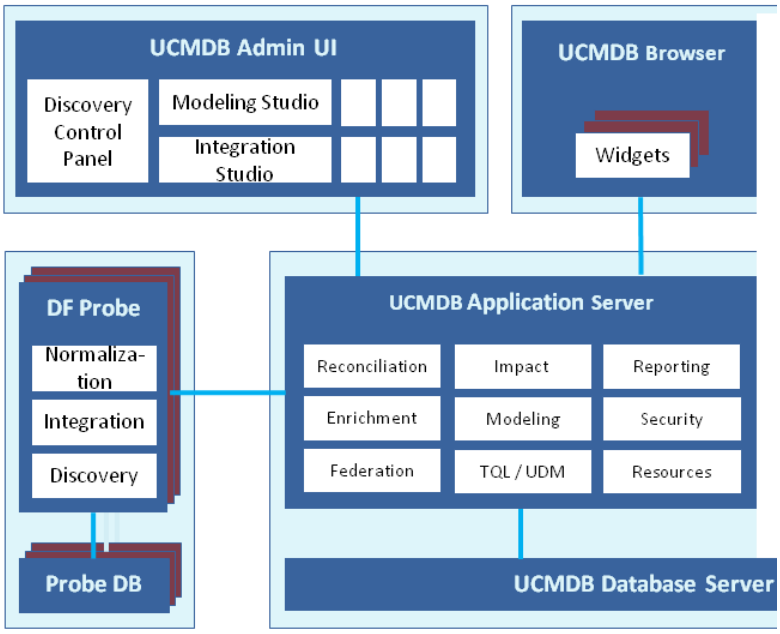
2. **Modeling studio:** Μπορεί ο χρήστης να κάνει enrichment των infra αποτελεσμάτων του discovery, μοντελοποίηση και να ασχοληθεί με security settings. Από εδώ οι πληροφορίες καταχωρούνται στην βάση μέσω web server**.**

3. **Integration studio:** Εδώ γίνεται το reconciliation των CIs , impact analysis και reporting. Μπορεί σε αυτή την σελίδα να χειριστεί και το df probe. Από εδώ οι πληροφορίες καταχωρούνται στην βάση μέσω web server. Από εδώ οι πληροφορίες καταχωρούνται στην βάση μέσω web server.

Στην εικόνα που ακολουθεί, παρουσιάζεται σχηματικά η εφαρμογή uCMDB καθώς και όλα τα αγαθά που εμπλέκονται σε αυτήν. Στο σχήμα 53, παρουσιάζονται ακόμα πιο αναλυτικά όλες οι λιτουργίες της εφαρμογής uCMDB. Για παράδειγμα, στον uCMDB Browser έχουν πρόσβαση οι implementation user (admin) και end user. Μπορούν ανάλογα τα δικαιώματα με πιο εύκολο στην χρήση UI να κάνουν συγκεκριμένες ενέργειες στο modeling studio και να παράγουν reports.



Σχήμα 52: Configuration Management uCMDB

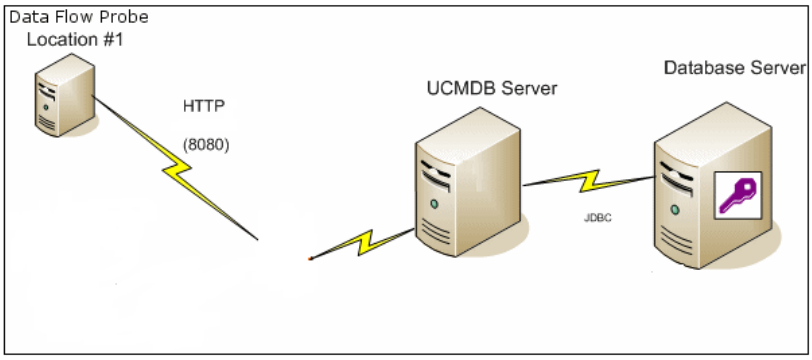


Σχήμα 53: Configuration Management uCMDB

Το authentication process από την χρήση του security γίνεται στο modeling studio. Κατά την εγκατάσταση, by default δημιουργείται ο admin user. Στην συνέχεια, ο χρήστης αυτός δημιουργεί τους υπόλοιπους ρόλους και χρήστες στο admin UI.

Σχήμα 54: Admin UI uCMDB

Στο διάγραμμα ροής δεδομένων (data flow diagram) που ακολουθεί, φαίνεται η πληροφορία που βρίσκει στον infrastructure κόσμο του οργανισμού το data flow probe και την διοχετεύει διαμέσου της πόρτας 8080 http στον web server και μετά από normalization γράφεται η πληροφορία στην βάση από τον web server.



Σχήμα 55: Data flow probe της uCMDB

5.3 Μοντελοποίηση απειλών της εφαρμογής uCMDB

5.3.1 Threat Model Information

Στην ενότητα αυτή πραγματοποιείται μοντελοποίηση των απειλών της εφαρμογής uCMDB και παρουσιάζονται όλα τα βήματα αναλυτικά. Η μεθοδολογία που χρησιμοποιείται είναι το template "Application Threat Modelling - Indicative Template" του κ.Ντούσκα.

Σε πρώτη φάση, στον πίνακα που ακολουθεί παρουσίαζονται κάποια βασικά στοιχεία της εφαρμογής uCMDB όπως είναι για παράδειγμα η τρέχουσα έκδοση, η περιγραφή της εφαρμογής κ.α.

Threat Model Information

Application version:	10.22 CUP 4 CP22			
Description	UCMDB is a CMDB and discovery (combining DDMA and DDMI technique) software product produced by Hewlett Packard supporting ITIL Configuration Management and which features a Configuration Management Database, as well as a mechanism for the automatic discovery of IT infrastructure components, such as computers, network devices and composing relationships between them.			
Document Owner:	ITSM Team			
Participants:	ITSM Team			
Reviewer:	ITSM Manager			

Στη συνέχεια, αναφέρονται οι εξωτερικές εξαρτήσεις (External Dependencies) της εφαρμογής όπως για παράδειγμα sso, ldap, κλπ. Οι εξωτερικές εξαρτήσεις ορίζουν την εξάρτηση του συστήματος από εξωτερικούς πόρους και την πολιτική ασφάλειας έξω από το μοντέλο του συστήματος. Εάν δεν ληφθεί υπόψη μια απειλή από εξωτερική εξάρτηση, μπορεί να γίνει μία έγκυρη ευπάθεια. Στα συστήματα λογισμικού, οι εξωτερικές εξαρτήσεις συχνά περιγράφουν λειτουργίες ευρείας διάταξης του συστήματος, όπως η ασυνέπεια των αλγορίθμων.

Στη συγκεκριμένη εφαμογή, οι εξωτερικές εξαρτήσεις είναι για παράδειγμα το λογισμικό του webserver που είναι windows 2012 R2 Ent SP1, όπως περιγράφεται στον ακόλουθο πίνακα:

External Dependencies

ID	Description
1	The uCMDB 10.22 is installed in webservice with Jetty, version 9.2.10. The webserver software has windows 2012 R2 Ent SP1. This includes the application of the latest operating system and application security patches.
2	The admin UI link is on the port 8080, http://<server name or IP address>.<domain name>:8080/
3	uCMDB browser mostly for end user is on the port 8080, http://<server name or IP address>.<domain name>:8080/ucmdb-browser/
4	The data flow probe server which is used for feeding the uCMDB database with Cis data, it has WinSRV 2012 R2 SP1 64bit and Jetty, version 9.2.10. The server will be hardened as per HP instructions. This includes the application of the latest operating system and application security patches.

5	The uCMDB database server's software has RHEL 6.5 64bit and Oracle 12c - 64bit
6	All the servers will be inside intranet on the same Vlan with low latency
7	The webserver connects with dataflow probe bidirectionaly with ports 80,8080 and with database server with JDBC driver port 1521 open from webserver to db server port 80,8080 will be open from bd server to webserver

Στο επόμενο βήμα, γίνεται περιγραφή των κύριων σημείων εισόδου (entry points) της εφαρμογής καθώς και τα αντίστοιχα επίπεδα εμπιστοσύνης (trust levels) που έχουν πρόσβαση σε κάθε ένα από τα σημεία εισόδου.

Entry Points

ID	Name	Description	Trust Level
1	RDP to 3389	Not authorized RDP login to webserver , dataflow probe server	(1) Admin with valid login credentials (2) user (no admin) with invalid login credentials (3) Installation user
2	JDBC driver port 1521	Not authorized use of JDBC driver connectivity	(1) Admin with valid login credentials (2) user (no admin) with invalid login credentials (3) Integration user
3	Admin UI main login page port 8080	All users can access the application main page	(1) Admin with valid login credentials (2) user (no admin) with invalid login credentials (3) Integration user (4) End user
4	uCMDB browser UI port 8080	All users can access the uCMDB browser UI main page	(1) Admin with valid login credentials (2) user (no admin) with invalid login credentials (3) Integration user (4) End user
5	Login Function	The login function accepts user credentials that created in the installation process and compares them with those in the Oracle db	(1) Admin with valid login credentials (2) user (no admin) with invalid login credentials (3) Integration user (4) End user
6	Login to database server port 22	Not authorized SSH login to db sever	(1) Admin with valid login credentials (2) user (no admin) with invalid login credentials (3) Installation user

Μετά την περιγραφή των σημείων εισόδου της εφαρμογής, γίνεται καταγραφή των αγαθών της (asset register), όπως για παράδειγμα το Discovery Control panel (Admin UI) και άλλα που είδαμε στην προηγούμενη ενότητα:

Assets

ID	Name	Description	Trust Level
1	Discovery Control panel (Admin UI)	Εδώ μπορεί να κάνει trigger λειτουργίες στον application server, πρόσβαση στα resources να χειριστεί το federation και να προβεί σε UDM/TQL. Μπορεί σε αυτή την σελίδα να χειριστεί και το df probe. Από εδώ οι πληροφορίες καταχωρούνται στην βάση μέσω application server.	(1) Implementation user (admin) (2) end user
2	Modeling studio (Admin UI)	Μπορεί ο χρήστης να κάνει enrichment των infra αποτελεσμάτων του discovery, μοντελοποίηση και να ασχοληθεί με security settings. Από εδώ οι πληροφορίες καταχωρούνται στην βάση μέσω web server.	(1) Implementation user (admin) (2) end user
3	Integration studio (Admin UI)	Εδώ γίνεται το reconciliation των CIs , impact analysis και reporting. Μπορεί σε αυτή την σελίδα να χειριστεί και το df probe. Από εδώ οι πληροφορίες καταχωρούνται στην βάση μέσω web server	(1) Implementation user (admin) (2) end user
4	uCMDB Browser	Μπορούν ανάλογα τα δικαιώματα με πιο εύκολο στην χρήση UI να να κάνουν συγκεκριμένες ενέργειες στο modeling studio και να παράγουν reports.	(1) Implementation user (admin) (2) end user
5	Login sessions	Οι χρήστες κάνουν login στο admin UI, uCMDB browser	(1) Implementation user (admin) (2) end user
6	Access to Database server	Για διαχείριση προβλημάτων στην βάση	(1) Admin
7	User creation roles	Δημιουργία ρόλων και Users	(1) Implementation user (admin)
8	Access to Dataflow server	Για διαχείριση προβλημάτων στην βάση	(1) Admin
9	Access to Webserver server	Για διαχείριση προβλημάτων στην βάση	(1) Admin
10	Access to Audit μεσω Admin UI	Για διαχείριση όλων των log file	(1) Implementation user (admin)
11	Organization data	Όλα τα δεδομένα που δημιουργούνται queries, discovery IT data, views, enrichments, credentials (encrypted), integration points κ.α	(1) Implementation user (admin) (2) end user

Το επόμενο βήμα, είναι η περιγραφή των επιπέδων εμπιστοσύνης (trust levels) της εφαρμογής όπως είναι για παράδειγμα ο τελικός χρήστης που έχει δικαίωμα πρόσβασης στο uCMDB UI και στον uCMDB browser αλλά με δικαιώματα read only.

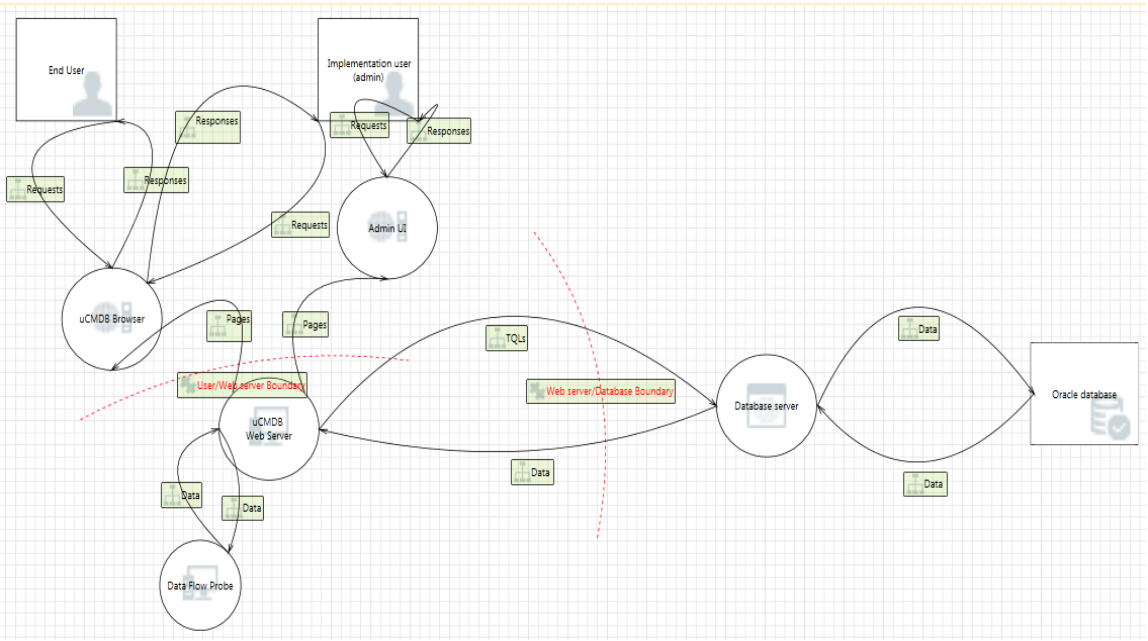
Trust Levels

ID	Name	Description
1	Admin with valid login credentials	Δικαίωμα πρόσβασης στον application server, ucmdb UI, uCMDB browser και πλήρη δικαιώματα implementation.
2	user (no admin) with invalid login credentials	Χρήστης του οργανισμού με πρόσβαση στα url της εφαρμογής αλλά χωρίς valid credentials.
3	Installation user	Χρήστης με admin credentials αλλά με δικαίωματα εγκατάστασης.
4	Integration user	Χρήση για integration μεταξύ των components. Δικαίωμα read/write στην βάση.
5	End user	Δικαίωμα πρόσβασης στο uCMDB UI και στον uCMDB browser αλλά με δικαιώματα read only.
6	Implementation user (admin)	Χρήστης που μπορεί να δημιουργεί queries, discovery IT data, views, enrichments, credentials (encrypted), integration points και να διαχειρίζεται την εφαρμογή αλλά και να αλλάζει infrastructure settings.

5.3.2 Διάγραμμα Ροής Δεδομένων (DFD)

Στην ενότητα αυτή παρουσιάζονται τα διαγράμματα ροής δεδομένων της εφαρμογής uCMDB. Για να δημιουργηθεί ένα χρήσιμο μοντέλο, πρέπει να εξετάσουμε την εφαρμογή μέσω των ματιών του αντιπάλου. Τα διαγράμματα μοντελοποίησης είναι μια οπτική αναπαράσταση του τρόπου λειτουργίας και συνεργασίας των υποσυστημάτων μιας εφαρμογής. Ο σχεδιασμός του διαγράμματος ροής δεδομένων αποτελεί απαραίτητο βήμα για τη μοντελοποίηση απειλών, γεγονός που είχαμε δει και στο προηγούμενο κεφάλαιο.

Τα διαγράμματα ροής δεδομένων (DFD) είναι ένας τρόπος υψηλού επιπέδου επικέντρωσης στα δεδομένα ενός συστήματος αλλά και ένας τρόπος ροής των δεδομένων μέσα στο σύστημα. Τα DFD είναι επαναληπτικά και πρέπει να οργανώνονται σε μια ιεραρχία που αντικατοπτρίζει με ακρίβεια το σύστημα. Έτσι, στο παρακάτω διάγραμμα ροής δεδομένων απεικονίζεται η αναταλλαγή δεδομένων στα components και στους χρήστες της εφαρμογής uCMDB.

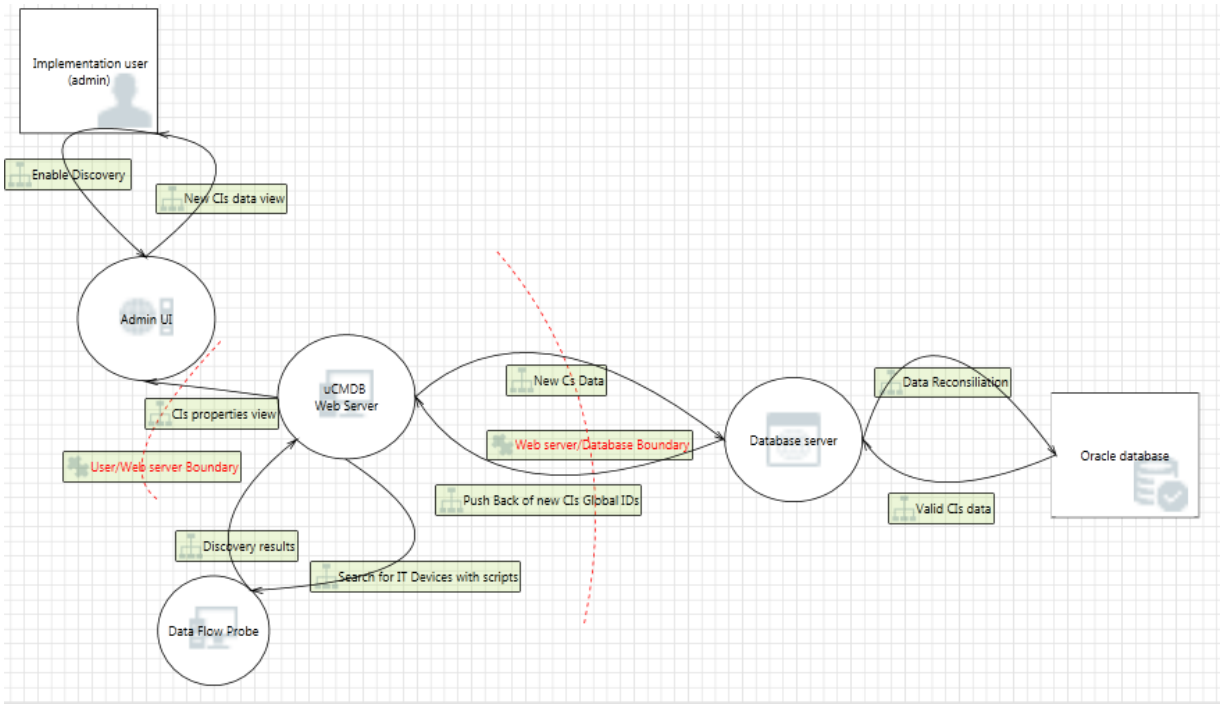


Σχήμα 56: Διάγραμμα Ροής Δεδομένων της εφαρμογής uCMDB

Για παράδειγμα, ο τελικός χρήστης (end user) στέλνει κάποιο request στον uCMDB browser (π.χ. Search CIs) και αντίστοιχα, ο uCMDB browser στέλνει στον τελικό χρήστη το response στο αίτημά του με αποτέλεσμα ο χρήστης να βλέπει τα δεδομένα που θέλει. Ο uCMDB browser με τη σειρά του, λαμβάνει τις σελίδες (δεδομένα) που θα « δείξει » στον τελικό χρήστη από τον uCMDB Web Server. Στο σημείο αυτό, είναι απαραίτητο να ορίσουμε τα λεγόμενα *trust boundaries* (όρια εμπιστοσύνης), όπου ένα αξιόπιστο στοιχείο και ένα αναξιόπιστο στοιχείο ανταλάσσουν δεδομένα. Τα διαφορετικά στοιχεία που έχουν διαμορφωθεί στο DFD παρέχουν τη δυνατότητα για την ανάλυση των απειλών. Στο παραπάνω διάγραμμα, τα *trust boundaries* έχουν σχεδιαστεί με κόκκινη διακεκομμένη γραμμή.

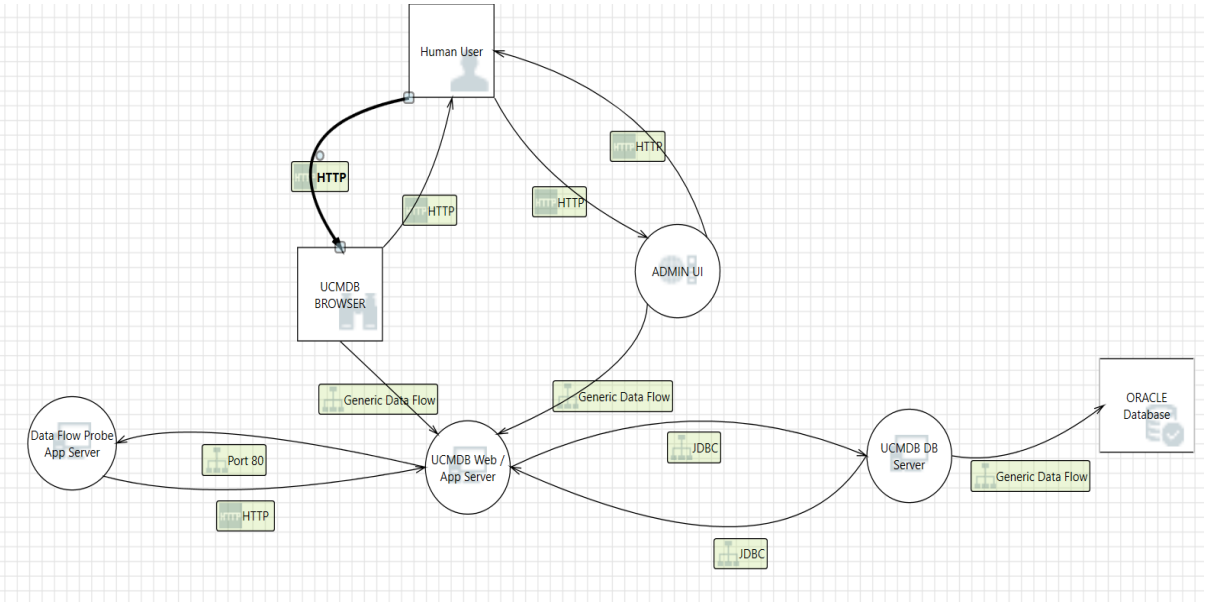
Επίσης, το παρακάτω διάγραμμα απεικονίζει σχηματικά μια διαδικασία που προσφέρει η εφαρμογή uCMDB, την *Discovery process*. Συγκεκριμένα, το διάγραμμα αυτό δείχνει πως ο Implementation user (admin) πραγματοποιεί discovery IT data μέσω του Discovery Control panel (Admin UI). Εδώ, τη διαδικασία *Discovery process* ξεκινά ο Implementation user επιλέγοντας να δει τα νέα CIs data στο Admin UI. Το Admin

UI με τη σειρά του λαμβάνει τα CIs properties view από τον Web Server της εφαρμογής uCMDB, ο οποίος δέχεται και στέλνει νέα CIs δεδομένα από τον Database Server.



Σχήμα 57: Διάγραμμα Ροής Δεδομένων uCMDB Discovery Process

Μέσω του εργαλείου « Microsoft Threat Modelling Tool 2016 » έγινε η γραφική αναπαράσταση της επικοινωνίας της web εφαρμογής uCMDB.



Σχήμα 58: Διάγραμμα Ροής Δεδομένων επικοινωνίας της uCMDB

5.3.3 Εντοπισμός και Κατηγοριοποίηση Απειλών

Μόλις δημιουργηθεί το διάγραμμα ροής δεδομένων, χρησιμοποιείται για να καθορίσει ποια δεδομένα παρέχονται σε έναν κόμβο και τους στόχους που έχει ο αντίπαλος για την εφαρμογή - ένας αντίπαλος πρέπει να παρέχει δεδομένα για να ξεκινήσει μια επίθεση. Οι στόχοι χρησιμοποιούνται στη συνέχεια στο DFD για να προσδιοριστούν οι διαδρομές απειλών (threat paths), να εντοπιστούν τα σημεία εισόδου / εξόδου και να ακολουθηθούν τα δεδομένα μέσω του συστήματος. Η διαδρομή απειλής (threat path) ορίζεται ως η ακολουθία οποιωνδήποτε κόμβων διεργασίας που εκτελούν security-critical processing. Όλες οι περιοχές όπου υπάρχει αλλαγή ή ενέργεια για λογαριασμό των δεδομένων είναι ευαίσθητες σε απειλές, δηλαδή κόμβους διεργασίας.

Ο εντοπισμός των απειλών αποτελεί το κλειδί για ένα ασφαλές σύστημα. Ο εντοπισμός των απειλών συνίσταται στην ανάλυση κάθε σημείου εισόδου / εξόδου, καθορίζοντας ποια κρίσιμη security processing λαμβάνει χώρα στο σημείο εισόδου / εξόδου και πώς μπορεί να γίνει αντικείμενο επίθεσης. Οι απειλές είναι οι στόχοι του αντιπάλου και για να υπάρξει μια απειλή πρέπει να έχει ένα αγαθό ως στόχο.

Το επόμενο βήμα στον εντοπισμό των απειλών είναι η ταξινόμηση των απειλών χρησιμοποιώντας το μοντέλο STRIDE, το οποίο αναλύσαμε στο κεφάλαιο 4.3.1. Μέσω του εργαλείου « Analysis View » απεικονίζεται η λίστα ευπαθειών της επικοινωνίας του σχήματος 58. Οι ευπάθειες / πιθανές απειλές που εντοπίστηκαν είναι οι παρακάτω:

- Cross Site Scripting το οποίο αλληλοεπιδρά στην HTTP σύνδεση. Ο web server « UCMDB Web / App Server » θα μπορούσε να είναι ένα θέμα σε μια cross-site scripting επίθεση, διότι δεν αποκλείει μία μη αξιόπιστη είσοδο.

- Elevation Using Impersonation το οποίο αλληλοεπιδρά στην HTTP σύνδεση. Η UCMDB App στο διακομιστή μπορεί να είναι σε θέση να μιμηθεί το πλαίσιο των Data Flow Probe App Server για να κερδίσει επιπλέον προνόμια.

- Spoofing the Human User External Entity το οποίο αλληλοεπιδρά στην HTTP σύνδεση. Ο χρήστης μπορεί να πλαστογραφηθεί από έναν εισβολέα και αυτό μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση σε ADMIN UI. Εδώ, θα μπορούσαμε να χρησιμοποιήσουμε ένα πρότυπο μηχανισμό ελέγχου ταυτότητας για τον προσδιορισμό της εξωτερικής οντότητας.

- Cross Site Scripting το οποίο αλληλοεπιδρά στην JDBC σύνδεση. Ο web server « UCMDB DB Server » θα μπορούσε να είναι ένα θέμα σε μια cross-site scripting επίθεση διότι δεν αποκλείει μία μη αξιόπιστη είσοδο.

- Elevation Using Impersonation το οποίο αλληλοεπιδρά στην JDBC σύνδεση. Η UCMDB DB Server ενδέχεται να είναι σε θέση να μιμηθεί το πλαίσιο της UCMDB App στο διακομιστή, προκειμένου να αποκτήσει επιπλέον προνόμια.

- Cross Site Scripting το οποίο αλληλοεπιδρά στην JDBC σύνδεση. Ο web server « UCMDB Web / App Server » θα μπορούσε να είναι ένα θέμα σε μια cross-site scripting επίθεση διότι δεν αποκλείει μία μη αξιόπιστη είσοδο.

- Elevation Using Impersonation το οποίο αλληλοεπιδρά στην JDBC σύνδεση. Η UCMDB App στο διακομιστή μπορεί να είναι σε θέση να μιμηθεί το πλαίσιο της UCMDB DB στο διακομιστή, προκειμένου να αποκτήσει επιπλέον προνόμια.

- Spoofing of Destination Data Store SQL Database το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Η Oracle Database μπορεί να πλαστογραφηθεί από έναν εισβολέα και αυτό μπορεί να οδηγήσει σε δεδομένα που εγγράφονται στο στόχο του εισβολέα, αντί της Oracle Database. Εδώ,

θα μπορούσαμε να χρησιμοποιήσουμε ένα πρότυπο μηχανισμό ελέγχου ταυτότητας για τον προσδιορισμό του χώρου αποθήκευσης δεδομένων προορισμού.

- Risks from Logging το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Απλοί αναγνώστες μπορεί να έρθουν αντιμέτωποι με μία επίθεση με τα αρχεία καταγραφής. Εδώ, θα μπορούσαμε να χρησιμοποιήσουμε τρόπους για να γίνει canonicalize δεδομένων σε όλα τα αρχεία καταγραφής. Η εφαρμογή ενός ενιαίου αναγνώστη για τα αρχεία καταγραφής είναι απαραίτητη προκειμένου να μειωθεί η επιφάνεια επίθεσης.

- Potential SQL Injection Vulnerability for SQL Database το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Η SQL injection είναι μια επίθεση στην οποία κακόβουλος κώδικα εισάγεται σε strings που αργότερα θα περάσει σε μια παρουσία του SQL Server για την ανάλυση και την εκτέλεση. Κάθε διαδικασία που κατασκευάζει δηλώσεις SQL θα πρέπει να αναθεωρηθεί για τα τρωτά σημεία, επειδή ο SQL Server θα εκτελέσει όλα τα συντακτικά έγκυρα ερωτήματα που λαμβάνει. Ακόμη και τα παραμετροποιημένα δεδομένα μπορούν να χειραγωγηθούν από έναν έμπειρο και αποφασιστικό εισβολέα.

- Lower Trusted Subject Updates Logs το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Υπάρχουν επίπεδα εμπιστοσύνης και κάποιος άλλος έξω από το υψηλότερο επίπεδο εμπιστοσύνης μπορεί να συνδεθεί. Αφήνοντας όλους να γράψουν στα αρχεία μας, μπορεί να οδηγήσει σε προβλήματα πιστοποίησης. Εδώ, θα μπορούσαμε να επιτρέπουμε μόνο αξιόπιστους χρήστες με κωδικό να συνδεθούν.

- Data Logs from an Unknown Source το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Στην περίπτωση που δεχόμαστε αρχεία καταγραφής από άγνωστο ή ασθενώς πιστοποιημένους χρήστες ή συστήματα, είναι απαραίτητη η ταυτοποίηση και η αυθεντικοποίηση της πηγής των αρχείων καταγραφής πριν από την αποδοχή τους.

- Potential Weak Protections for Audit Data το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Σκεφτείτε τι συμβαίνει όταν ο μηχανισμός ελέγχου δέχεται επιθέσεις, συμπεριλαμβανομένων των προσπαθειών να καταστρέψουν τα αρχεία καταγραφής, ή προγράμματα ανάλυσης ης επίθεσης καταγραφής. Πρέπει να γίνετε διασφάλιση της πρόσβασης στο αρχείο καταγραφής μέσα από μια οθόνη αναφοράς, η οποία ελέγχει ποιός διαβάζει και ποιος γράφει χωριστά. Αναφέρετε ποια φίλτρα, εάν υπάρχουν, οι αναγνώστες μπορούν να επικαλεστούν, ή συγγραφείς θα πρέπει να αναμένουν.

- Weak Credential Storage το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Οι κωδικοί που αποθηκεύονται στο διακομιστή μπορούν πολλές φορές να παραποιηθούν και οι πιστοποιήσεις που αποθηκεύονται στον υπολογιστή-πελάτη μπορούν να κλαπούν. Για την πλευρά του διακομιστή, μπορεί να αποθηκεύει ένα Hash των κωδικών αντί για την αποθήκευση των ίδιων των κωδικών. Αν αυτό δεν είναι δυνατό λόγω των απαιτήσεων των επιχειρήσεων, να είστε βέβαιος να κρυπτογραφήσετε τα διαπιστευτήρια πριν από την αποθήκευση, τη χρήση ενός SDL-εγκεκριμένο μηχανισμό. Για την πλευρά του πελάτη, εάν η αποθήκευση των κωδικών απαιτείται, πρέπει να τα κρυπτογραφήσει και να προστατεύσει το μέσο αποθήκευσης στο οποίο είναι αποθηκευμένο.

- Potential Excessive Resource Consumption for UCMDB DB Server or SQL Database το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Μήπως ο UCMDB DB Server ή η Oracle Database έχει λάβει ρητά μέτρα για τον έλεγχο της κατανάλωσης των πόρων; Επιθέσεις τύπου κατανάλωσης πόρων μπορεί να είναι δύσκολο να τις αντιμετωπίσει κανείς, και υπάρχουν φορές

που είναι λογικό να αφήσει το λειτουργικό σύστημα να κάνει αυτή τη δουλειά. Πρέπει να είμαστε προσεκτικοί στα αιτήματα των πόρων μας, έτσι ώστε να μην οδηγούν σε αδιέξοδο και να μην κάνουν χρήση του χρονικού ορίου.

- Cross Site Scripting το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Ο web server « UCMDB Web / App Server » θα μπορούσε να είναι ένα θέμα σε μια cross-site scripting επίθεση, διότι δεν αποκλείει μία μη αξιόπιστη είσοδο.

- Elevation Using Impersonation το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Η UCMDB App μπορεί να είναι σε θέση να μιμηθεί το πλαίσιο του ADMIN UI, προκειμένου να αποκτήσει επιπλέον προνόμια.

- Spoofing the UCMDB BROWSER External Entity το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Ο UCMDB περιηγητής μπορεί να πλαστογραφηθεί από έναν εισβολέα και αυτό μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση στο UCMDB Web / App Server. Εδώ, θα μπορούσαμε να χρησιμοποιήσουμε ένα πρότυπο μηχανισμό ελέγχου ταυτότητας για τον προσδιορισμό της εξωτερικής οντότητας.

- Cross Site Scripting το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Ο web server « UCMDB Web / App Server » θα μπορούσε να είναι ένα θέμα σε μια cross-site scripting επίθεση, διότι δεν αποκλείει μία μη αξιόπιστη είσοδο.

- Elevation Using Impersonation το οποίο αλληλοεπιδρά στη Generic Data Flow σύνδεση. Η UCMDB Web / App Server μπορεί να είναι σε θέση να μιμηθεί το πλαίσιο του UCMDB browser, προκειμένου να αποκτήσει επιπλέον προνόμια.

- Cross Site Scripting το οποίο αλληλοεπιδρά στη Port 80. Ο web server « Data Flow Probe App Server » θα μπορούσε να είναι ένα θέμα σε μια cross-site scripting επίθεση, διότι δεν αποκλείει μία μη αξιόπιστη είσοδο.

Cross Site Scripting	Tampering	HTTP
Elevation Using Impersonation	Elevation Of Privilege	HTTP
Spoofing the Human User External Entity	Spoofing	HTTP
Elevation Using Impersonation	Elevation Of Privilege	HTTP
Spoofing of Destination Data Store SQ...	Spoofing	Generic Data Flow
Risks from Logging	Tampering	Generic Data Flow
Potential SQL Injection Vulnerability fo...	Tampering	Generic Data Flow
Lower Trusted Subject Updates Logs	Repudiation	Generic Data Flow
Data Logs from an Unknown Source	Repudiation	Generic Data Flow
Insufficient Auditing	Repudiation	Generic Data Flow
Potential Weak Protections for Audit D...	Repudiation	Generic Data Flow
Weak Credential Storage	Information Disclosure	Generic Data Flow
Potential Excessive Resource Consump...	Denial Of Service	Generic Data Flow
Cross Site Scripting	Tampering	Generic Data Flow
Elevation Using Impersonation	Elevation Of Privilege	Generic Data Flow
Spoofing the UCMDB BROWSER Exter...	Spoofing	Generic Data Flow
Cross Site Scripting	Tampering	Generic Data Flow
Elevation Using Impersonation	Elevation Of Privilege	Generic Data Flow
Cross Site Scripting	Tampering	JDBC
Elevation Using Impersonation	Elevation Of Privilege	JDBC
Cross Site Scripting	Tampering	JDBC
Elevation Using Impersonation	Elevation Of Privilege	JDBC
Cross Site Scripting	Tampering	Port 80
Elevation Using Impersonation	Elevation Of Privilege	Port 80

Σχήμα 59: Κατηγοριοποίηση των απειλών στην εφαρμογή uCMDB σύμφωνα με τη μεθοδολογία STRIDE

Το επόμενο βήμα στην ανάλυση των απειλών είναι ο προσδιορισμός του κίνδυνο της απειλής και των συνθηκών της απειλής χρησιμοποιώντας το μοντέλο DREAD. Όταν χρησιμοποιείται το μοντέλο DREAD, μια ομάδα μοντελοποίησης απειλών υπολογίζει τους κινδύνους ασφαλείας ως έναν μέσο όρο των αριθμητικών τιμών που αποδίδονται σε καθεμία από τις πέντε κατηγορίες. Πιο συγκεκριμένα, το DREAD είναι ένα σύστημα ταξινόμησης για τον ποσοτικό προσδιορισμό, τη σύγκριση και την ιεράρχηση του κινδύνου που παρουσιάζει κάθε αξιολογούμενη απειλή. Το ακρωνύμιο DREAD σχηματίζεται από το πρώτο γράμμα κάθε κατηγορίας που χρησιμοποιείται για την αξιολόγηση.

Η μοντελοποίηση αυτή επηρεάζει το σκεπτικό πίσω από τη ρύθμιση και την άμεση αξιολόγηση των κινδύνων. Ο αλγόριθμος DREAD, όπως παρουσιάζεται παρακάτω, χρησιμοποιείται για να υπολογίσει την τιμή ενός κινδύνου, η οποία είναι ο μέσος όρος των πέντε επιμέρους κατηγοριών.

Risk_DREAD = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5

Ο υπολογισμός παράγει πάντα έναν αριθμό μεταξύ 0 και 10, ενώ όσο υψηλότερος είναι ο αριθμός, τόσο πιο σοβαρός είναι ο κίνδυνος. Αναλυτικά, το ακρωνύμιο DREAD περιλαμβάνει τα παρακάτω:

- Damage: Αναγνωρίζει την έκταση της βλάβης που προκύπτει εάν η ευπάθεια αξιοποιείται. Με άλλα λόγια, αν μια απειλή γίνει εκμεταλλεύσιμη, πόση ζημιά θα προκληθεί; Ο τρόπος βαθμολόγησης του κινδύνου γίνεται ως εξής: 0: Μηδενική ζημιά, 5: Τα δεδομένα του χρήστη είναι σε κίνδυνο ή επηρεάζονται, 10: Πλήρης καταστροφή του συστήματος ή των δεδομένων.

- Reproducability: Αναγνωρίζει το πόσο συχνά επιχειρείται η προσπάθεια εκμετάλλευσης ενός τρωτού σημείου. Δηλαδή, το πόσο εύκολη είναι η αναπαραγωγή ή η εκμετάλλευση της ευπάθειας. Ο τρόπος βαθμολόγησης του κινδύνου γίνεται ως εξής: 0: Πολύ δύσκολο ή αδύνατο, ακόμα και για τους διαχειριστές της εφαρμογής, 5: Ένα ή δύο βήματα απαιτούνται, μπορεί να χρειαστεί να υπάρχουν δικαιώματα εξουσιοδοτημένου χρήστη και 10: Δε χρειάζεται χρήση αυθεντικοποίησης.

- Exploitability: Αναθέτει έναν αριθμό στην προσπάθεια που απαιτείται για την εκμετάλλευση της ευπάθειας. Επιπροσθέτως, το exploitability έχει κάποιες προϋποθέσεις όπως το εάν ο χρήστης πρέπει να αυθεντικοποιηθεί. Ουσιαστικά, προσδιορίζει το τι χρειάζεται για την εκμετάλλευση της απειλής. Ο τρόπος βαθμολόγησης του κινδύνου γίνεται ως εξής: 0: Προχωρημένες γνώσεις προγραμματισμού και δικτύων, με προσαρμοσμένα ή προηγμένα εργαλεία επίθεσης, 5: Κάποιο malware που υπάρχει στο διαδίκτυο ή με χρήση διαθέσιμων εργαλείων επίθεσης και 10: Μόνο ένας web browser.

- Affected users: Μια τιμή που χαρακτηρίζει τον αριθμό των installed instances (πόσοι χρήστες θα επηρεαστούν) του συστήματος που θα επηρεαστεί εάν ένα exploit έγινε ευρέως διαθέσιμο. Ο τρόπος βαθμολόγησης του κινδύνου γίνεται ως εξής: 0: Κανένας, 5: Ορισμένοι χρήστες, αλλά όχι όλοι, 10: Όλοι οι χρήστες.

- Discoverability: Μέτρηση της πιθανότητας ότι, εάν δεν παραληφθεί, θα εντοπιστεί ευπάθεια από ερευνητές εξωτερικής ασφάλειας, χάκερς κλπ, δηλαδή το πόσο εύκολο είναι να ανακαλυφθεί η συγκεκριμένη απειλή. Ο τρόπος βαθμολόγησης του κινδύνου γίνεται ως εξής: 0: Πολύ δύσκολο εώς αδύνατο, καθώς απαιτεί τον πηγαίο κώδικα ή πρόσβαση διαχειριστή, 5: Μπορεί να ανακαλυφθεί τυχαία ή παρακολουθώντας την κίνηση του δικτύου, 9: Λεπτομέρειες σφαλμάτων μπορούν να ανακαλυφθούν εύκολα χρησιμοποιώντας μια μηχανή αναζήτησης και 10: Οι πληροφορίες είναι ορατές στη γραμμή διευθύνσεων του web browser ή σε μια φόρμα.

Υλοποιώντας αυτή τη λογική δημιουργούμε τον πίνακα για τον υπολογισμό του συνολικού ρίσκου για κάθε απειλή. Οι απειλές είναι αυτές που βρέθηκαν με χρήση του εργαλείου Threat Modeling Tool καθώς επίσης και αυτές που καταγράφονται στο OWASP Top Ten Project, με τις πιο διαδεδομένες ευπάθειες σε διαδικτυακές εφαρμογές. Επιπλέον. παρατίθενται προτεινόμενα μέτρα ασφαλείας με βάση τις παραγράφους του Application Security Verification Standard (Version 3.0.1) του OWASP.

ID	Threat	Vulnerability	Countermeasures	DREAD	
1	Cross Site Scripting το οποίο αλληλεπιδρά στην HTTP σύνδεση	Cross-Site Scripting (XSS), Information Disclosure, Spoofing	V5: Malicious input handling verification requirements V11: HTTP security configuration verification requirements	Damage	9
				Reproducibility	8
				Exploitability	8
				Affected Users	10
				Discoverability	8
				OVERALL RISK	**8.6**
2	Elevation Using Impersonation το οποίο αλληλεπιδρά στην HTTP σύνδεση	Λανθασμένη διαδικασία ταυτοποίησης χρήστη/ ελέγχου προνομίων, Repudiation, Information Disclosure	V2: Authentication Verification Requirements, V3: Session Management Verification Requirements, V10: Communications security verification requirements	Damage	9
				Reproducibility	7
				Exploitability	8
				Affected Users	9
				Discoverability	8
				OVERALL RISK	**8.2**
3	Spoofing the Human User External Entity	Μη ασφαλής έλεγχος ταυτότητας, Repudiation, Information Disclosure	V2: Authentication Verification Requirements	Damage	10
				Reproducibility	7
				Exploitability	8
				Affected Users	10
				Discoverability	9
				OVERALL RISK	**8.8**
4	Cross Site Scripting το οποίο αλληλεπιδρά στην JDBC σύνδεση	Cross-Site Scripting (XSS), Tampering, Information Disclosure	V5: Malicious input handling verification requirements V9: Data protection verification requirements	Damage	10
				Reproducibility	9
				Exploitability	9
				Affected Users	10
				Discoverability	10
				OVERALL RISK	**9.6**
5	Elevation Using Impersonation το οποίο αλληλεπιδρά στην JDBC σύνδεση	Ελλιπής έλεγχος προνομίων χρήστη από την βάση δεδομένων, Tampering, Information Disclosure	V2: Authentication Verification Requirements, V9: Data protection verification requirements	Damage	10
				Reproducibility	7
				Exploitability	8
				Affected Users	10
				Discoverability	10
				OVERALL RISK	**9**
6	Spoofing of Destination Data Store SQL Database το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Tampering, Information Disclosure	V9: Data protection verification requirements	Damage	10
				Reproducibility	7
				Exploitability	8
				Affected Users	10
				Discoverability	10
				OVERALL RISK	**9**
7	Risks from Logging το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Ανεπαρκής μηχανισμός ελέγχου ταυτότητας για τον προσδιορισμό του χώρου αποθήκευσης δεδομένων προορισμού, Repudiation, Denial of Service	V8: Error handling and logging verification requirements, V16: Files and resources verification requirements	Damage	8
				Reproducibility	7
				Exploitability	8
				Affected Users	8
				Discoverability	7
				OVERALL RISK	**7.6**
8	Potential SQL Injection Vulnerability for SQL Database το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Injection, Tampering, Information Disclosure	V9: Data protection verification requirements	Damage	10
				Reproducibility	9
				Exploitability	8
				Affected Users	10
				Discoverability	9
				OVERALL RISK	**9.2**
9	Lower Trusted Subject Updates Logs το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Λανθασμένη διαδικασία ταυτοποίησης χρήστη/ ελέγχου προνομίων, Repudiation, Information Disclosure	V2: Authentication Verification Requirements, V4: Access Control Verification Requirements, V8: Error handling and logging verification requirements	Damage	10
				Reproducibility	7
				Exploitability	8
				Affected Users	10
				Discoverability	10
				OVERALL RISK	**9**

10	Data Logs from an Unknown Source το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Data Logs from an Unknown Source το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	V8: Error handling and logging verification requirements, V16: Files and resources verification requirements	Damage	6
				Reproducibility	7
				Exploitability	8
				Affected Users	8
				Discoverability	7
				OVERALL RISK	**7.2**
11	Insufficient Auditing το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Έλλειψη ταυτοποίησης/αυθεντικοποίησης χρηστών, Spoofing, Tampering, Information Disclosure	V2: Authentication Verification Requirements	Damage	6
				Reproducibility	8
				Exploitability	8
				Affected Users	7
				Discoverability	8
				OVERALL RISK	**7.4**
12	Potential Weak Protections for Audit Data το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Λανθασμένα δικαιώματα ανάγνωσης/εγγραφής, Spoofing, Tampering, Information Disclosure	V4: Access Control Verification Requirements	Damage	6
				Reproducibility	7
				Exploitability	8
				Affected Users	7
				Discoverability	8
				OVERALL RISK	**7.2**
13	Weak Credential Storage το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Απουσία μεθόδων κρυπτογράφησης δεδομένων, Information Disclosure	V7: Cryptography at rest verification requirements	Damage	10
				Reproducibility	8
				Exploitability	8
				Affected Users	10
				Discoverability	9
				OVERALL RISK	**9**
14	Potential Excessive Resource Consumption for UCMDB DB Server or SQL Database το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Απουσία ελέγχου κατανάλωσης πόρων του συστήματος, Denial of Service	V16: Files and resources verification requirements	Damage	9
				Reproducibility	7
				Exploitability	8
				Affected Users	9
				Discoverability	8
				OVERALL RISK	**8.2**
15	Spoofing the UCMDB BROWSER External Entity το οποίο αλληλεπιδρά στη Generic Data Flow σύνδεση	Έλλειψη πρότυπου μηχανισμού ελέγχου ταυτότητας για τον προσδιορισμό της εξωτερικής οντότητας, Spoofing, Elevation of Privilege	V2: Authentication Verification Requirements, V4: Access Control Verification Requirements	Damage	9
				Reproducibility	7
				Exploitability	8
				Affected Users	8
				Discoverability	10
				OVERALL RISK	**8.4**
16	Cross Site Scripting το οποίο αλληλεπιδρά στη Port 80 σύνδεση	Cross-Site Scripting (XSS)	V5: Malicious input handling verification requirements, V11: HTTP security configuration verification requirements	Damage	9
				Reproducibility	7
				Exploitability	8
				Affected Users	9
				Discoverability	8
				OVERALL RISK	**8.2**
17	Elevation Using Impersonation το οποίο αλληλεπιδρά στη Port 80 σύνδεση	Έλλειψη ταυτοποίησης/αυθεντικοποίησης χρηστών	V2: Authentication Verification Requirements	Damage	8
				Reproducibility	7
				Exploitability	7
				Affected Users	8
				Discoverability	7
				OVERALL RISK	**7.4**
18	Αλλοίωση δεδομένων	Injection, Information Disclosure	V9: Data protection verification requirements, V7: Cryptography at rest verification requirements, V4: Access Control Verification Requirements	Damage	10
				Reproducibility	9
				Exploitability	9
				Affected Users	10
				Discoverability	10
				OVERALL RISK	**9.6**
19	Η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	Security Misconfiguration, Tampering, Information Disclosure	V4: Access Control Verification Requirements, V9: Data protection verification requirements	Damage	10
				Reproducibility	8
				Exploitability	8
				Affected Users	10
				Discoverability	10
				OVERALL RISK	**9.2**
20	Οι κωδικοί πρόσβασης, τα αναγνωριστικά περιόδου και άλλα διαπιστευτήρια αποστέλλονται μέσω μη κρυπτογραφημένης σύνδεσης	Broken Authentication and Session Management, Spoofing, Tampering, Information Disclosure	V2: Authentication Verification Requirements, V7: Cryptography at rest verification requirements, V9: Data protection verification requirements	Damage	10
				Reproducibility	7
				Exploitability	8
				Affected Users	10
				Discoverability	10
				OVERALL RISK	**9**

Σχήμα 60: Ταξινόμηση των απειλών στην εφαρμογή uCMDB σύμφωνα με τη μεθοδολογία DREAD

5.3.4 Security controls ASVS και Στρατηγικές μετριασμού

Οι απειλές που αφορούν την εφαρμογή αυτή μπορούν να αντιμετωπιστούν ακολουθώντας τις απαιτήσεις ασφάλειας που προτείνει το Πρότυπο Ελέγχου Ασφάλειας Εφαρμογών (**ASVS**). Πρόκειται για μια λίστα των απαιτήσεων ασφάλειας των εφαρμογών για να καθορίσουμε τι είναι μια ασφαλής εφαρμογή που ορίζει τρία επίπεδα ελέγχου ασφαλείας, με κάθε επίπεδο να αυξάνεται σε βάθος. Εδώ, θα χρησιμοποιήσουμε το Επίπεδο 1 το οποίο θεωρείται το ελάχιστο που απαιτείται για όλες τις εφαρμογές. Συγκεκριμένα, στην πρώτη στήλη καταγράφονται οι απαιτήσεις ασφαλείας που ήδη ικανοποιούνται στην εφαρμογή μας, ενώ στη δεύτερη οι απαιτήσεις που αν υπήρχαν θα είχαμε μια πιο secure εφαρμογή.

TYPE	*SECURITY CONTROL*
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-Repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

REQUIREMENTS	*EXAMPLES (στήλη 1)*	*(στήλη 2)*
Authentication Verification (Authentication)	1. Επιβεβαίωση ότι όλοι οι έλεγχοι ταυτότητας επιβάλλονται από την πλευρά του διακομιστή.	1. Επιβεβαιώστε ότι τα password entry fields επιτρέπουν ή ενθαρρύνουν τη χρήση φράσεων πρόσβασης, και δεν αποτρέπουν συνθηματικές φράσεις ή εξαιρετικά σύνθετους κωδικούς πρόσβασης.
	2. Βεβαιωθείτε ότι όλοι οι έλεγχοι αυθεντικοποίησης δεν αποτύγχάνουν να εξασφαλίσουν ότι οι επιτιθέμενοι δεν μπορούν να συνδεθούν.	2. Επιβεβαιώστε ότι όλες οι λειτουργίες πιστοποίησης ταυτότητας λογαριασμού (όπως το προφίλ ενημέρωση, ξέχασα κωδικό πρόσβασης ή IVR), που θα μπορούσαν να ανακτήσουν την πρόσβαση στους λογαριασμούς είναι τουλάχιστον εξίσου ανθεκτικοί στην επίθεση ως ο κύριος μηχανισμός ελέγχου ταυτότητας.

	3. Επιβεβαιώστε όλες τις λειτουργίες πιστοποίησης ταυτότητας λογαριασμού (όπως το προφίλ ενημέρωση, ξέχασα τον κωδικό πρόσβασης, άτομα με ειδικές ανάγκες ,γραφείο βοήθειας ή IVR), που θα μπορούσε να ανακτήσει την πρόσβαση στο λογαριασμό είναι τουλάχιστον εξίσου ανθεκτικά στην επίθεση ως ο κύριος μηχανισμός ελέγχου ταυτότητας.	3. Βεβαιωθείτε ότι όλες οι ύποπτες αποφάσεις ταυτότητας γίνονται logged. Αυτό θα πρέπει να περιλαμβάνει τις αιτήσεις με τα σχετικά metadata που απαιτούνται για τις έρευνες ασφαλείας.
	4. Βεβαιωθείτε ότι αν η εφαρμογή επιτρέπει στους χρήστες τον έλεγχο ταυτότητας, αυτοί χρησιμοποιούν έναν αποδεδειγμένα ασφαλή μηχανισμό ελέγχου ταυτότητας.	4. Βεβαιωθείτε ότι οι κωδικοί πρόσβασης του λογαριασμού κάνουν χρήση της ρουτίνας κρυπτογράφησης επαρκή και ότι αντέχουν στην brute force attack εναντίον της ρουτίνας κρυπτογράφησης.
	5. Επιβεβαίωση ότι τα administrative interfaces δεν είναι προσιτά σε μη αξιόπιστα μέρη.	5. Βεβαιωθείτε ότι όλα τα διαπιστευτήρια ελέγχου ταυτότητας για την πρόσβαση σε υπηρεσίες εκτός της εφαρμογή κρυπτογραφούνται και αποθηκεύονται σε μια προστατευμένη θέση.
Session Management Verification (Authentication)	1. Βεβαιωθείτε ότι οι συνεδρίες ακυρώνονται όταν ο χρήστης αποσυνδεθεί.	1. Βεβαιωθείτε ότι μόνο τα αναγνωριστικά περιόδου που παράγονται από το πλαίσιο εφαρμογής αναγνωρίζεται ως ενεργά από την εφαρμογή.
	2. Βεβαιωθείτε ότι συνεδρίες σταματούν μετά από μια ορισμένη περίοδο αδράνειας.	2. Βεβαιωθείτε ότι τα αναγνωριστικά περιόδου που αποθηκεύονται στα cookies έχουν την πορεία τους σε κατάλληλα περιοριστική αξία για την εφαρμογή, και τα authentication session tokens ορίζουν τα «HttpOnly» και «ασφαλείς» ιδιότητες.
	3. Βεβαιωθείτε ότι όλες οι σελίδες που απαιτούν έλεγχο ταυτότητας έχουν εύκολη και ορατή πρόσβαση στη λειτουργικότητα logout.	3. Βεβαιωθείτε ότι η εφαρμογή περιορίζει τον αριθμό των ενεργών ταυτόχρονων συνεδριών.
	4. Βεβαιωθείτε ότι όλες οι επιτυχημένες ταυτοποιήσεις και η εκ νέου πιστοποίηση δημιουργεί μια νέα σύνοδο και id συνόδου.	4. Βεβαιωθείτε ότι το αναγνωριστικό περιόδου δεν αποκαλύπτεται σε διευθύνσεις URL, μηνύματα λάθους, ή αρχεία καταγραφής. Αυτό περιλαμβάνει την επαλήθευση ότι η εφαρμογή δεν υποστηρίζει URL ξαναγράφοντας τα session cookies.
Access Control Verification (Authentication, Integrity)	1. Βεβαιωθείτε ότι οι ίδιοι κανόνες ελέγχου πρόσβασης που συνάγονται από το στρώμα παρουσίασης επιβάλλονται από την πλευρά του διακομιστή.	1. Βεβαιωθείτε ότι όλα τα δεδομένα του χρήστη και τα τα χαρακτηριστικά του που χρησιμοποιούνται από τους ελέγχους πρόσβασης, δεν μπορούν να χειραγωγηθούν από τους τελικούς χρήστες χωρίς τη ρητή άδεια.

	2. Βεβαιωθείτε ότι η εφαρμογή ή το πλαίσιο χρησιμοποιεί ισχυρά αντι-CSRF tokens ή έχει άλλο μηχανισμό προστασίας των συναλλαγών.	2. Βεβαιωθείτε ότι υπάρχει ένας κεντρικός μηχανισμός (συμπεριλαμβανομένων των βιβλιοθηκών που απαιτούν εξωτερικά authorization services) για την προστασία της πρόσβασης σε κάθε είδος protected resource.
	3. Βεβαιωθείτε ότι η εφαρμογή εφαρμόζει σωστά context-sensitive authorisation, έτσι ώστε να μην επιτρέπεται η μη εξουσιοδοτημένη χειραγώγηση μέσω της παραμέτρου αλλοίωσης (tampering).	3. Βεβαιωθείτε ότι όλες οι αποφάσεις ελέγχου πρόσβασης μπορεί να γίνουν logged και όλες οι failed decisions το ίδιο.
Malicious input handling verification (Availability)	1. Βεβαιωθείτε ότι το περιβάλλον χρόνου εκτέλεσης δεν είναι επιρρεπές σε υπερχειλίσεις μνήμης, ή ότι οι έλεγχοι ασφαλείας εμποδίζουν υπερχειλίσεις μνήμης.	1. Βεβαιωθείτε ότι υπάρχει μόνον ένα χειριστήριο επικύρωσης είσοδου που χρησιμοποιείται από την εφαρμογή για κάθε τύπο δεδομένων που είναι αποδεκτός.
		2. Βεβαιωθείτε ότι η εφαρμογή δεν ευπαθής σε LDAP Injection, ή ότι η έλεγχοι ασφάλειας αποτρέπουν την LDAP Injection. 3. Βεβαιωθείτε ότι όλα τα ερωτήματα SQL, HQL, OSQL, NoSQL είναι αποθηκευμένες διαδικασίες, ζητώντας του αποθηκευμένες διαδικασίες που προστατεύονται από τη χρήση των έτοιμων προτάσεων ή ερώτηματα παραμετροποίησης, και ως εκ τούτου δεν είναι ευπαθή σε SQL injection.
Error handling and logging verification (Non-Repudiation)	1.Βεβαιωθείτε ότι η εφαρμογή δεν εξάγει τα μηνύματα λάθους ή ίχνη στοίβας που περιέχει ευαίσθητα δεδομένα που θα μπορούσαν να βοηθήσουν έναν εισβολέα, συμπεριλαμβανομένων την id συνεδρία, το λογισμικό και τις προσωπικές πληροφορίες.	1. Βεβαιωθείτε ότι η λογική αντιμετώπιση των λαθών στους ελέγχους ασφαλείας αρνείται την πρόσβαση από προεπιλογή. 2. Βεβαιωθείτε ότι κάθε log event περιλαμβάνει τις απαραίτητες πληροφορίες που θα επιτρέπουν την λεπτομερή διερεύνηση του χρονοδιαγράμματος όταν συμβαίνει ένα γεγονός.
Data protection verification (Integrity)	1. Βεβαιωθείτε ότι όλα τα ευαίσθητα δεδομένα αποστέλλονται στο διακομιστή στο σώμα του μηνύματος HTTP ή στις κεφαλίδες (δηλαδή, οι παράμετροι URL δεν χρησιμοποιούνται για την αποστολή ευαίσθητων δεδομένων).	1. Βεβαιωθείτε ότι ο κατάλογος των ευαίσθητων δεδομένων που επεξεργάζεται την αίτηση αναγνωρίζεται, και ότι υπάρχει μια σαφής πολιτική για το πώς θα πρέπει να ελέγχεται η πρόσβαση σε αυτά τα δεδομένα, να είναι κρυπτογραφημένα και ναεκτελούνται σύμφωνα με τις σχετικές οδηγίες για την προστασία των δεδομένων.

Communications security verification (Authentication)	1. Βεβαιωθείτε ότι η διαδρομή μπορεί να κατασκευαστεί από μια αξιόπιστη CA σε κάθε πιστοποιητικό διακομιστή Transport Layer Security (TLS), και ότι κάθε πιστοποιητικό του διακομιστή είναι έγκυρο.	1. Βεβαιωθείτε ότι τα μονοπάτια πιστοποιητικών έχουνκατασκευαστεί και επαληθεύονται για όλα τα πιστοποιητικά πελάτη χρησιμοποιώντας configured trust anchors και revocation information.
		2. Βεβαιωθείτε ότι μόνο ισχυροί αλγόριθμοι, αλγόριθμους κρυπτογράφησης και πρωτόκολλα χρησιμοποιούνται, μέσα από όλη την ιεραρχία πιστοποιητικού, συμπεριλαμβανομένων των ριζών και ενδιάμεσων πιστοποιητικών της επιλεγμένης αρχής πιστοποίησης σας.
HTTP security configuration (Availability)	1. Βεβαιωθείτε ότι η εφαρμογή δέχεται μόνο ένα καθορισμένο σύνολο των απαιτούμενων μεθόδων αίτησης HTTP, όπως GET και POST γίνονται δεκτές, και αχρησιμοποίητες μεθοδοι (π.χ. TRACE, που, και διαγραφή) είναι ρητά μπλοκαρισμένες.	1. Βεβαιωθείτε ότι κεφαλίδες HTTP προστίθενται από ένα trusted proxy ή SSO, όπως ένα bearer token και επικυρώνονται από την εφαρμογή.
	2. Βεβαιωθείτε ότι κάθε απόκριση HTTP περιέχει μια κεφαλίδα τύπου περιεχομένου καθορίζοντας, ένα ασφαλές σύνολο χαρακτήρων (π.χ., UTF-8, ISO 8859-1).	2. Βεβαιωθείτε ότι το περιεχόμενο της πολιτικής V2 Ασφαλείας (CSP) είναι σε χρήση για τοποθεσίες όπου το περιεχόμενο δεν θα πρέπει να εξεταστεί σε ένα 3rd-party X-Frame.
	3. Βεβαιωθείτε ότι οι κεφαλίδες HTTP ή οποιοδήποτε μέρος της απάντησης HTTP δεν εκθέτουν λεπτομερείς πληροφορίες για την έκδοση των στοιχείων του συστήματος.	3. Βεβαιωθείτε ότι το περιεχόμενο της πολιτικής V2 Ασφαλείας (CSP) είναι σε χρήση κατά τρόπο που είτε αapενεργοποιεί το inline JavaScript ή παρέχει έναν έλεγχο ακεραιότητας στο εσωτερικό JavaScript με CSP noncing ή κατακερματισμού.
Malicious controls verification		1. Βεβαιωθείτε ότι όλες οι κακόβουλες δραστηριότητες είναι κατάλληλα sandboxed, containerized ή isolated για να καθυστερήουν και να αποτρέψουν τους εισβολείς από το να επιτεθούν σε άλλες εφαρμογές.

Business logic verification		1. Βεβαιωθείτε ότι η εφαρμογή θα είναι μόνο η διαδικασία της επιχειρηματικής λογικής flow σε διαδοχικά βήματα ώστε, με όλα τα βήματα να υποβάλλονται σε ρεαλιστικό ανθρώπινο χρόνο και να μην επεξεργάζονται εκτός λειτουργίας, αλλά και να μην παραλείπονται βήματα της διαδικασίας. 2. Βεβαιωθείτε ότι η εφαρμογή διαθέτει επιχειρηματικά όρια και σωστά επιβάλλει σε κάθε χρήστη με βάση τη δυνατότητα ρύθμισης συναγερμού και τις αυτοματοποιημένες αντιδράσεις σε αυτοματοποιημένη ή ασυνήθιστη επίθεση.
Files and resources verification (Authentication, Integrity)	1. Βεβαιωθείτε ότι οι ανακατευθύνσεις διευθύνσεων URL επιτρέπουν μόνο τους επιτρεπόμενους προορισμούς της λίστας, ή να δείχνουν μια προειδοποίηση όταν γίνεται ανακατεύθυνση σε δυνητικά μη αξιόπιστο περιεχόμενο.	1. Βεβαιωθείτε ότι τα αρχεία που προέρχονται από μη αξιόπιστες πηγές αποθηκεύονται έξω από το Webroot, με περιορισμένα δικαιώματα, κατά προτίμηση με ισχυρή επικύρωση.
	2. Βεβαιωθείτε ότι τα μη αξιόπιστα αρχείο δεδομένων που υποβάλλονται στην εφαρμογή δεν χρησιμοποιούνται άμεσα με το αρχείο I/O, ιδιαίτερα για την προστασία του OS command injection vulnerabilities.	2. Βεβαιωθείτε ότι το web ή application server έχει ρυθμιστεί από προεπιλογή να αρνηθεί την πρόσβαση σε απομακρυσμένους πόρους ή συστήματα έξω από το web ή application server.
	3. Βεβαιωθείτε ότι τα αρχεία που προέρχονται από μη αξιόπιστες πηγές επικυρώνονται να είναι αναμενόμενοι τύποι και σαρώνονται από σαρωτές ιών για την πρόληψη της αποστολής των γνωστού κακόβουλου περιεχόμενου.	3. Μην χρησιμοποιείτε Flash, Active-X, Silverlight, NaCl, client-side Java ή άλλη client side τεχνολογία που δεν υποστηρίζεταιεγγενώς με τα πρότυπα του προγράμματος περιήγησης W3C.
	4. Επιβεβαιώστε τον κώδικα της εφαρμογής ότι δεν εκτελεί uploaded data που προκύπτουν από μη αξιόπιστες πηγές.	
Web services verification (Integrity)	1 .Βεβαιωθείτε ότι η ίδια κωδικοποίηση χρησιμοποιείται μεταξύ του πελάτη και του διακομιστή.	1. Βεβαιωθείτε ότι η REST service προστατεύεται από Cross-Site Request Forgery.

	2. Βεβαιωθείτε ότι η πρόσβαση στην διοίκηση και τη διαχείριση των λειτουργιών εντός της υπηρεσίας Web Application περιορίζεται στους διαχειριστές των υπηρεσιών web.	2. Επιβεβαιώστε την υπηρεσία REST και ελέγξετε ρητά την εισερχόμενη Content-Type για να είναι τη αναμενόμενη, όπως η εφαρμογή / XML ή application / JSON.
		3. Βεβαιωθείτε ότι η εναλλακτική λύση και λιγότερο ασφαλείς διαδρομές πρόσβασης δεν υπάρχουν.
Configuration	1. Όλα τα εξαρτήματα θα πρέπει να είναι ενημερωμένα με τη σωστή ρύθμιση παραμέτρων ασφαλείας (ες) και έκδοση (ες). Αυτό θα πρέπει να περιλαμβάνει την αφαίρεση των περιττών διατάξεων και φακέλων, όπως δείγματα εφαρμογών, τεκμηρίωση πλατφόρμας, και default or example users.	1. Επικοινωνίες μεταξύ των συνιστωσών, όπως είναι μεταξύ του διακομιστή εφαρμογών και ο διακομιστής της βάσης δεδομένων, θα πρέπει να κρυπτογραφηθεί, ιδιαίτερα όταν τα στοιχεία είναι σε διαφορετικά containers ή σε διαφορετικά συστήματα.
		2. Βεβαιωθείτε ότι τα application deployments είναι κατάλληλα sandboxed, containerized ή isolated, για να να καθυστερήσει και να αποτρέψει τους εισβολείς από το να επιτεθούν σε άλλες εφαρμογές.
		3. Βεβαιωθείτε ότι οι εξουσιοδοτημένοι διαχειριστές έχουν τη δυνατότητα να επαληθεύσουν την ακεραιότητα όλων των security-relevant configurations για να διασφαλιστεί ότι δεν έχουν αλλοιωθεί.
		4. Βεβαιωθείτε ότι όλα τα εξαρτήματα εφαρμογής είναι signed.

Έως τώρα, εντοπίστηκαν και αναλύθηκαν οι απειλές. Εάν η απειλή δεν έχει επιλυθεί, θα γίνει μια ευπάθεια. Υπάρχει μια ευπάθεια όταν υπάρχει απειλή και δεν έχουν εφαρμοστεί τα μέτρα για τον μετριασμό της. Για να μειωθεί ο κίνδυνος από απειλές, η ομάδα πρέπει να αναλύσει τις συνθήκες κάθε απειλής, χρησιμοποιώντας το DREAD για να καθορίσει ένα επίπεδο κινδύνου και να προσδιορίσει μια στρατηγική μετριασμού για κάθε κατάσταση.

Ο σκοπός της στρατηγικής μετριασμού είναι να μειωθούν οι επιπτώσεις που θα έχει μία ενδεχόμενη εκμετάλλευση μιας απειλής για την εφαρμογή. Παρακάτω καταγράφονται οι έξι πιθανές ενέργειες που είναι δυνατόν να υλοποιηθούν για κάθε απειλή:

- Καμία ενέργεια
- Ενημέρωση σχετικά με τον κίνδυνο: για παράδειγμα, με την προειδοποίηση των χρηστών σχετικά με τον κίνδυνο
- Μετριασμός του κινδύνου: για παράδειγμα, με την υλοποίηση αντίμετρων
- Αποδοχή του κινδύνου: μετά από αξιολόγηση των επιπτώσεων της εκμετάλλευσης (των επιπτώσεων στην επιχείρηση)
- Μεταφορά του κινδύνου: μέσω συμβατικών συμφωνιών με άλλες οντότητες
- Τερματισμός του κινδύνου: με την αποσύνδεση ή τον τερματισμό χρήσης ενός asset

Χρησιμοποιώντας τη λίστα των κινδύνων που καταγράφηκε στην προηγούμενη παράγραφο, θεωρούμε ότι οι απειλές με συνολικό βαθμό της κλίμακας DREAD μεγαλύτερο ή ίσο του 8, είναι αυτές που χρήζουν άμεσης αντιμετώπισης, συνήθως μέσω της υλοποίησης πρόσθετων μέτρων ασφαλείας ή τη μεταφορά του ρίσκου σε άλλες οντότητες. Ένα παράδειγμα για τη στρατηγική μετριασμού που ακολουθείται παρουσιάζεται στον παρακάτω πίνακα:

Threat	Mitigation Techniques	Mitigation Strategies
Η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα	1) Authorization 2) Τεχνικές Προστασίας Κωδικού Πρόσβασης (salt, hash)	Μετριασμός του κινδύνου
Repudiation	1) Ψηφιακή υπογραφή 2) Timestamp	Μετριασμός του κινδύνου
Denial of Service	1) Έλεγχος χρήσης δικτύου 2) Φιλτράρισμα δεδομένων που εισάγει ο χρήστης 3) Χρήση Intrusion Detection Systems (IDS) και Intrusion Protection Systems (IPS	Μετριασμός του κινδύνου
Αλλοίωση δεδομένων	1) Τεχνικές Προστασίας Κωδικού Πρόσβασης (salt, hash) 2) Προστασία ευαίσθητων δεδομένων 3) Sanitize user input 4) Ορθή διαδικασία αυθεντικοποίησης	Μετριασμός του κινδύνου
Elevation of Privilege	1) Ύπαρξη αυστηρής πολιτικής προνομίων	Μετριασμός του κινδύνου
Οι κωδικοί πρόσβασης, τα αναγνωριστικά περιόδου και άλλα διαπιστευτήρια αποστέλλονται μέσω μη κρυπτογραφημένης σύνδεσης	1) Χρήση κρυπτογραφημένης σύνδεσης (SSL)	Μετριασμός του κινδύνου
Elevation Using Impersonation το οποίο αλληλεπιδρά στη Port 80 σύνδεση	-	Καμία ενέργεια

Σχήμα 61: Mitigation Stretegies για την εφαρμογή uCMDB

6 ΚΕΦΑΛΑΙΟ 6: Διεξαγωγή Αποτίμησης Κινδύνου για την εφαρμογή uCMDB

‘Οπως είδαμε και στο πρώτο κεφάλαιο, η η διαδικασία της αποτίμησης του κινδύνου ενός ΠΣ ορίζεται ως το αποτέλεσμα της ανάλυσης του κινδύνου (Risk Analysis) και της αξιολόγησης του κινδύνου (Risk Evaluation) και υπάρχουν διάφορες μεθοδολογίες που μπορεί να ακολουθήσει κάποιος ενδιαφερόμενος. Για τη web εφαρμογή uCMDB, επιλέξαμε να πραγματοποίησουμε την αποτίμηση των κινδύνων (risk assessment) χρησιμοποιώντας το πρότυπο **ISO 27005**, το οποίο παρουσιάσαμε και αναλύσαμε στην ενότητα 2.7.

6.1 Asset Model και Asset Register της εφαρμογής uCMDB

Στην ενότητα αυτή θα καταγράψουμε όλα τα αγαθά ανά υπηρεσία ώστε να δημιουργηθεί το asset model αλλά και όλα τα αγαθά του υπό εξέταση οργανισμού και θα τα ταξινομήσουμε ανάλογα με τις κατηγορίες αγαθών που θα ορίσουμε. Αρχικά, για το asset model έχουμε τους παρακάτω πίνακες:

#	SERVICE	NAME:	Web Application uCMDB
1	DESCRIPTION	Πρόκειται για την διαδικτυακή εφαρμογή που συνδυάζει μια κλασσική CMDB μαζί με δυνατότητες IT infrastructure discovery. Επίσης, υποστηρίζει ITIL Configuration Management με την λειτουργία μιας Configuration Management Database. Η πιο σημαντική λειτουργία όμως είναι η διαδικασία του discovery IT infrastructure components. Ανάμεσα σε αυτά βρίσκονται δικτυακές συσκευές, φυσικοί και virtual servers καθώς και οι αντίστοιχες σχέσεις που υπάρχουν μεταξύ τους.	

#	DATA				
1	NAME:	Πηγαίος κώδικας της ιστοσελίδας	CATEGORY:	Δεδομένα παραμετροποίησης	
2	NAME:	Configuration Αρχεία της ιστοσελίδας	CATEGORY:	Δεδομένα παραμετροποίησης	
3	NAME:	Στοιχεία αυθεντικοποίησης χρηστών	CATEGORY:	Δεδομένα Αυθεντικοποίησης	
4	NAME:	Login Session	CATEGORY:	Δεδομένα Αυθεντικοποίησης	
5	NAME:	User creation roles	CATEGORY:	Δεδομένα παραμετροποίησης	
6	NAME:	Organization data π.χ. δεδομένα που δημιουργούνται queries, discovery IT data, views, enrichments, credentials (encrypted), integration points κ.α	CATEGORY:	Δεδομένα παραμετροποίησης	

SYSTEMS

#	SYSTEM NAME:	Web Server	**CATEGORY:**	Computer System	
1	**DESCRIPTION**	Στον web server εκτελούνται όλες οι σημαντικές λειτουργίες, όπως η αποστολή queries στην βάση του db server. Οι εφαρμογές που μπορεί κάποιος να χρησιμοποιήσει μέσω του admin UI και uCMDB browser είναι ενδεικτικά: impact analysis, reporting, reconciliation, enrichment, modeling, security, federation, TQL/UDM, resources.			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A1	HP uCMDB Server v10.22	H/W	Server Computer	C/R
	A2	WinSRV 2012	S/W	Operating System	
	A3	Apache	S/W	Web Server SW	

SYSTEMS

#	**SYSTEM NAME:**	Database Server	**CATEGORY:**	Computer System	
2	**DESCRIPTION**	Ο database server φιλοξενεί την βάση της uCMDB. Μπορεί να φιλοξενήσει Microsoft SQL server, Oracle ή PostgreSQL. Στην βάση γίνεται όλη η επεξεργασία των δεδομένων που γράφει ο web server. Όταν ο web server στέλνει query στην βάση, εκεί γίνεται ο υπολογισμός και το αποτέλεσμα στέλνεται πίσω μέσω του JDBC driver.			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A4	RHEL 6.5	H/W	Server Computer	C/R
	A5	Ubuntu 12.04	S/W	Operating System	
	A6	Oracle 12c	S/W	Database SW	

SYSTEMS

#	**SYSTEM NAME:**	DF Probe – Probe DB	**CATEGORY:**	Computer System	
3	**DESCRIPTION**	Αυτό το component χρησιμεύει στο discovery όλων των infrastructure assets του οργανισμού. Αυτή η διαδικασία γίνεται triggered από ένα module του application sever μέσω της χρήσης πολλών σε αλληλουχία python scripts στα οποία έχουν οριστεί τα πρωτόκολλα επικοινωνίας και οι αντίστοιχες πόρτες. Στην συνέχεια κανονικοποιεί τα αποτελέσματα και μέσω της λειτουργίας integration, στέλνει τα αποτελέσματα δηλαδή τα Configuration items (CIs) μέσω του web server στην βάση της uCMDB			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A7	HP uCMDB v10.22	H/W	Server Computer	C/R
	A8	WinSRV 2012	S/W	Operating System	

SYSTEMS

#	**SYSTEM NAME:**	Workstation 1	**CATEGORY:**	Computer System	
4	**DESCRIPTION**	Πρόκειται για το workstation του διαχειριστή (admin) της εφαρμογής uCMDB			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A9		H/W	Server Computer	C/R
	A10		S/W	Operating System	

SYSTEMS

#	SYSTEM NAME:	main network	CATEGORY:	Network	
5	DESCRIPTION	Το βασικό δίκτυο των servers όπου φιλοξενείται η web εφαρμογή uCMDB			
	ASSET	**NAME**	**Category**	**Subcategory**	**LOCATION**
	A10	Βασικό router του CR	H/W	Router	C/R
	A11	Βασικό switch του CR	H/W	Switch	
	A12	Βασικό firewall του CR	H/W	Firewall	

Έτσι, σύμφωνα με τους παραπάνω πίνακες οι κατηγορίες των αγαθών που ορίσαμε είναι οι εξής:

1. Data Category: Δεδομένα Αυθεντικοποίησης, Δεδομένα παραμετροποίησης
2. System Category: Computer System, Network
3. S/W - H/W Category: DF Probe – Probe DB , Operating System, Database SW, Web Server SW, Server Computer, Router, Switch, Firewall, Workstation
4. Physical Asset: Computer room, Κτήρια – Εγκαταστάσεις
5. Χρήστες (USERS): Admin, Installation user, Integration user, End user

Στη συνέχεια, θα καθορίσουμε το Asset Register της εφαρμογής στο οποίο καταγράφουμε όλα τα αγαθά του υπό εξέταση οργανισμού και τα ταξινομούμε ανάλογα με τις κατηγορίες αγαθών που εντοπίσαμε (εδώ είναι πέντε οι κατηγορίες). Πιο αναλυτικά, ο παρακάτω πίνακας αποτελεί το Asset Register της εφαρμογής uCMDB:

#	‘Ονομα Αγαθού	Περιγραφή	Κατηγορία	Ιδιοκτήτης
1	Κτήρια-Εγκαταστάσεις	Το κτήριο όπου στεγάζεται η εφαρμογή uCMDB	Φυσικά Αγαθά (Physical Asset)	Ιδιοκτήτης κτηρίου
2	Computer room (CR)	Το δωμάτιο στο οποίο στεγάζεται το βασικό δίκτυο των servers και γενικά όλο το H/W - S/W της εφαρμογής	Φυσικά Αγαθά (Physical Asset)	Ιδιοκτήτης κτηρίου
3	Server Computer	Ο server HP uCMDB Server v10.22 του web server της εφαρμογής	Υλικά αγαθά (H/W)	ITSM Team
4	Cabling	Τα διάφορα cables μεταξύ των components της εφαρμογής	Υλικά αγαθά (H/W)	ITSM Team
5	Βασικό router του CR	Το βασικό router του CR	Υλικά αγαθά (H/W)	ITSM Team
6	Βασικό switch του CR	Το βασικό switch του CR	Υλικά αγαθά (H/W)	ITSM Team
7	Βασικό firewall του CR	Το βασικό firewall του CR	Υλικά αγαθά (H/W)	ITSM Team
8	Λειτουργικό Σύστημα	Το λειτουργικό σύστημα του Web Server, του Database Server, κλπ.	Αγαθά Λογισμικού (S/W)	ITSM Team
9	Web Server	Στον web server εκτελούνται όλες οι σημαντικές λειτουργίες της εφαρμογής, όπως η αποστολή queries στην βάση του db server.	Αγαθά Λογισμικού (S/W)	ITSM Team

10	Database Server	Ο database server φιλοξενεί την βάση της uCMDB.	Αγαθά Λογισμικού (S/W)	ITSM Team
11	DF Probe – Probe DB	Αυτό το component χρησιμεύει στο discovery όλων των infrastructure assets του οργανισμού.	Αγαθά Λογισμικού (S/W)	ITSM Team
12	Δικτυακό Λογισμικό	Το λογισμικό του βασικού δικτύου των servers όπου φιλοξενείται η web εφαρμογή uCMDB	Αγαθά Λογισμικού (S/W)	ITSM Team
13	Δεδομένα Αυθεντικοποίησης	Στην κατηγορία αυτή ανήκουν τα στοιχεία αυθεντικοποίησης των χρηστών, το Login Session, κλπ.	Αγαθά Δεδομένων (DATA)	ITSM Team
14	Δεδομένα παραμετροποίησης	Στην κατηγορία αυτή ανήκει ο πηγαίος κώδικας της ιστοσελίδας, τα Configuration Αρχεία της ιστοσελίδας και τα Organization data π.χ., discovery IT data, views, enrichments, credentials (encrypted), integration points κ.α	Αγαθά Δεδομένων (DATA)	ITSM Team
15	Admin	Ο χρήστης που χρήστης που διαχειρίζεται την εφαρμογή και μπορεί να δημιουργεί queries, discovery IT data, views, enrichments, credentials (encrypted), integration points και να τα αλλάζει infrastructure settings.	Χρήστες (USERS)	
16	Installation user	Ο χρήστης με admin credentials αλλά και με δικαίωματα εγκατάστασης.	Χρήστες (USERS)	
17	Integration user	Χρήση για integration μεταξύ των components. Δικαίωμα read/write στην βάση.	Χρήστες (USERS)	
18	End user	Χρήστης με δικαίωμα πρόσβασης στο uCMDB UI, uCMDB browser αλλά με δικαιώματα read only.	Χρήστες (USERS)	
19	Workstation	Πρόκειται για το workstation του διαχειριστή (admin) της εφαρμογής uCMDB.	Υλικά αγαθά (H/W)	Admin

6.2 Αποτίμηση επιπτώσεων της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας της εφαρμογής uCMDB

Σύμφωνα με το πρότυπο ISO 27005, στην ενότητα αυτή θα πραγματοποιήσουμε αποτίμηση επιπτώσεων της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των αγαθών της εφαρμογής uCMDB. Για να γίνει αυτό, ορίζουμε την παρακάτω κλίμακα για τα τρία μεγέθη (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) και με βάση την οποία θα προκύψει η αποτίμηση των επιπτώσεων.

Απώλεια Διαθεσιμότητας	**15 Λ**	Απώλεια Διαθεσιμότητας μέχρι 15 λεπτά
	1 Ω	Απώλεια Διαθεσιμότητας μέχρι 1 ώρα
	3 Ω	Απώλεια Διαθεσιμότητας μέχρι 3ώρες
	12 Ω	Απώλεια Διαθεσιμότητας μέχρι 12 ώρες
	1 Η	Απώλεια Διαθεσιμότητας μέχρι 1 ημέρα
	2 Η	Απώλεια Διαθεσιμότητας μέχρι 2 ημέρες
	1 Ε	Απώλεια Διαθεσιμότητας μέχρι 1 εβδομάδα
Απώλεια Ακεραιότητας	**ΟΚ**	Ολική καταστροφή δεδομένων (και των backup)
	ΜΚ	Μερική Καταστροφή των δεδομένων
	ΣΑ	Σκόπιμη αλλοίωση δεδομένων
	ΑΑ	Ακούσια Αλλοίωση δεδομένων
Απώλεια Εμπιστευτικότητας	**ΑΕΣ**	Αποκάλυψη δεδομένων σε χρήστες εντός της εταιρίας
	ΑΣΥΝ	Αποκάλυψη δεδομένων σε συνεργάτες της εταιρίας
	ΑΕΞ	Αποκάλυψη δεδομένων σε εξωτερικούς χρήστες

Οι κατηγορίες των επιπτώσεων που λαμβάνουμε υπόψη είναι οι εξής:

1. **Εξωτερικό περιβάλλον**: Επιπτώσεις στις πολιτικές σχέσεις, Διαταραχή πολιτικής απόφασης, Επιπτώσεις στη φήμη / εικόνα του Οργανισμού, Επιπτώσεις στη δημόσια τάξη, Επιπτώσεις στην άμυνα και την εθνική ασφάλεια
2. **Διαδικασίες και Συστήματα**: Διαταραχή ελέγχου διαχείρισης, Απρόβλεπτες ή πρόσθετες δαπάνες, Απώλεια αγαθών, Υπέρβαση προϋπολογισμού, Υποβάθμιση υπηρεσιών.
3. **Επιπτώσεις σε πελάτες / υπαλλήλους**: Υγεία και ασφάλεια, Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων, Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού, Κατάχρηση προσωπικών δεδομένων.
4. **Οικονομικές απώλειες**: Άμεσες οικονομικές συνέπειες, Έμμεσες / μακροπρόθεσμες οικονομικές συνέπειες
5. **Νομικές και κανονιστικές επιπτώσεις**: Παραβίαση της ιδιωτικότητας, Αποκάλυψη ευαίσθητων προσωπικών δεδομένων, Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements), Παρεμπόδιση εφαρμογής νόμου ή κανονισμών

Αρχικά, για την απώλεια της εμπιστευτικότητας (Confidentiality) θα πρέπει να αποτυπώσουμε για κάθε αγαθό ΔΕΔΟΜΕΝΩΝ και για κάθε σενάριο την αποτίμηση επιπτώσεων απώλειας εμπιστευτικότητας. Στον πίνακα που ακολουθεί γίνεται η αποτίμηση της απώλειας της εμπιστευτικότητας, λαμβάνοντας

υπόψη τα παραπάνω. Ενδεικτικά παρουσιάζουμε την αποτίμηση της απώλειας της εμπιστευτικότητας για τα αγαθά 1) Δεδομένα Αυθεντικοποίησης και 2) Δεδομένα Παραμετροποίησης, αλλά η διαδικασία έγινε για όλα τα αγαθά του οργανισμού (Asset Register της εφαρμογής uCMDB) :

#	1	ΑΓΑΘΟ	Δεδομένα Αυθεντικοποίησης	
ΑΠΩΛΕΙΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ				
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)** **0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ**			**Σχόλια**
	ΑΕΣ	**ΑΣΥΝ**	**ΑΕΞ**	
Εξωτερικό περιβάλλον				
Επιπτώσεις στις πολιτικές σχέσεις	0	0	0	
Διαταραχή πολιτικής απόφασης	0	0	0	
Επιπτώσεις στην άμυνα και την εθνική ασφάλεια	0	0	0	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	3	3	3	
Ειπτώσεις στη δημόσια τάξη	0	0	0	
Διαδικασίες και Συστήματα				
Διαταραχή ελέγχου διαχείρισης	3	3	3	
Υποβάθμιση υπηρεσιών	2	3	3	
Απρόβλεπτες ή πρόσθετες δαπάνες	2	2	2	
Απώλεια αγαθών	3	3	3	
Υπέρβαση προϋπολογισμού	2	2	2	
Επιπτώσεις σε πελάτες / υπαλλήλους				
Υγεία και ασφάλεια	1	1	1	
Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων	0	0	0	
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	2	1	2	
Κατάχρηση προσωπικών δεδομένων	3	3	3	
Νομικές και κανονιστικές επιπτώσεις				
Παραβίαση της ιδιωτικότητας	3	3	3	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων	3	3	3	
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)	1	3	2	

Παρεμπόδιση εφαρμογής νόμου ή κανονισμών	3	3	3	Λόγω GDPR
Summary of ratings	**ΑΕΣ**	**ΑΣΥΝ**	**ΑΕΞ**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	3	3	3	
Τελικός Βαθμός Αποτίμησης Αγαθού	**3**			**Μέγιστος βαθμός αποτίμησης όλων των σεναρίων**
Επίπεδο Επίπτωσης	**ΥΨΗΛΟ**			

#	**2**	**ΑΓΑΘΟ**	**Δεδομένα Παραμετροποίησης**
ΑΠΩΛΕΙΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ			
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)** **0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ**		**Σχόλια**
	ΑΕΣ	**ΑΣΥΝ**	**ΑΕΞ**	
Εξωτερικό περιβάλλον				
Επιπτώσεις στις πολιτικές σχέσεις	0	0	0	
Διαταραχή πολιτικής απόφασης	0	0	0	
Επιπτώσεις στην άμυνα και την εθνική ασφάλεια	0	0	0	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	1	2	2	
Ειπτώσεις στη δημόσια τάξη	0	0	0	
Διαδικασίες και Συστήματα				
Διαταραχή ελέγχου διαχείρισης	2	2	2	
Υποβάθμιση υπηρεσιών	2	2	2	
Απρόβλεπτες ή πρόσθετες δαπάνες	2	2	2	
Απώλεια αγαθών	2	2	2	
Υπέρβαση προϋπολογισμού	2	2	2	
Επιπτώσεις σε πελάτες / υπαλλήλους				
Υγεία και ασφάλεια	1	1	1	
Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων	0	0	0	
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	2	1	2	

Κατάχρηση προσωπικών δεδομένων	1	1	1	
Νομικές και κανονιστικές επιπτώσεις				
Παραβίαση της ιδιωτικότητας	1	1	1	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων	1	1	1	
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)	1	2	2	
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών	1	1	1	Λόγω GDPR
Summary of ratings	**ΑΕΣ**	**ΑΣΥΝ**	**ΑΕΞ**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	2	2	2	
Τελικός Βαθμός Αποτίμησης Αγαθού	**2**			**Μέγιστος βαθμός αποτίμησης όλων των σεναρίων**
Επίπεδο Επίπτωσης	**ΜΕΤΡΙΟ**			

Στη συνέχεια, θα εφαρμόσουμε την ίδια ακριβώς μεθοδολογία για την αποτίμηση της ακεραιότητας των επιλεγμένων αγαθών με τις ίδιες επιπτώσεις αλλά με διαφορετική κλίμακα:

#	1	ΑΓΑΘΟ	Δεδομένα Αυθεντικοποίησης

ΑΠΩΛΕΙΑ ΑΚΕΡΑΙΟΤΗΤΑΣ					
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**				**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ				
	ΜΚ	**ΟΚ**	**ΣΑ**	**ΑΑ**	
Εξωτερικό περιβάλλον					
Επιπτώσεις στις πολιτικές σχέσεις	0	0	2	1	
Διαταραχή πολιτικής απόφασης	0	0	2	2	
Επιπτώσεις στην άμυνα και την εθνική ασφάλεια	0	0	1	1	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	3	3	3	3	
Ειπτώσεις στη δημόσια τάξη	0	0	1	1	
Διαδικασίες και Συστήματα					
Διαταραχή ελέγχου διαχείρισης	3	3	3	3	

Υποβάθμιση υπηρεσιών	3	3	3	3	
Απρόβλεπτες ή πρόσθετες δαπάνες	1	3	3	3	
Απώλεια αγαθών	3	3	3	2	
Υπέρβαση προϋπολογισμού	2	3	3	2	
Επιπτώσεις σε πελάτες / υπαλλήλους					
Υγεία και ασφάλεια	1	2	2	2	
Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων	0	0	0	0	
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	1	2	2	2	
Κατάχρηση προσωπικών δεδομένων	2	2	3	2	
Νομικές και κανονιστικές επιπτώσεις					
Παραβίαση της ιδιωτικότητας	2	3	3	2	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων	2	3	3	3	
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)	2	3	3	2	
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών	2	3	3	2	
Συνολικοί βαθμοί	**ΜΚ**	**ΟΚ**	**ΣΑ**	**ΑΑ**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**3**	**3**	**3**	**3**	
Τελικός Βαθμός Αποτίμησης Αγαθού	3				**Μέγιστος βαθμός αποτίμησης όλων των σεναρίων**
Επίπεδο Επίπτωσης	**ΥΨΗΛΟ**				

#	2	ΑΓΑΘΟ	Δεδομένα Παραμετροποίησης

ΑΠΩΛΕΙΑ ΑΚΕΡΑΙΟΤΗΤΑΣ					
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης (ISO 27005)**				**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ				
	ΜΚ	**ΟΚ**	**ΣΑ**	**ΑΑ**	

Εξωτερικό περιβάλλον					
Επιπτώσεις στις πολιτικές σχέσεις	0	0	2	1	
Διαταραχή πολιτικής απόφασης	0	0	2	2	
Επιπτώσεις στην άμυνα και την εθνική ασφάλεια	0	0	1	1	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	2	2	2	2	
Ειπτώσεις στη δημόσια τάξη	0	0	1	1	
Διαδικασίες και Συστήματα					
Διαταραχή ελέγχου διαχείρισης	2	2	2	2	
Υποβάθμιση υπηρεσιών	2	2	2	2	
Απρόβλεπτες ή πρόσθετες δαπάνες	1	2	2	2	
Απώλεια αγαθών	2	2	2	2	
Υπέρβαση προϋπολογισμού	2	2	2	2	
Επιπτώσεις σε πελάτες / υπαλλήλους					
Υγεία και ασφάλεια	1	1	2	1	
Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων	0	0	0	0	
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	1	1	2	1	
Κατάχρηση προσωπικών δεδομένων	1	1	1	1	
Νομικές και κανονιστικές επιπτώσεις					
Παραβίαση της ιδιωτικότητας	1	2	2	2	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων	2	2	2	2	
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)	1	2	2	1	
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών	1	2	2	1	
Συνολικοί βαθμοί	**ΜΚ**	**ΟΚ**	**ΣΑ**	**ΑΑ**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**2**	**2**	**2**	**2**	
Τελικός Βαθμός Αποτίμησης Αγαθού	2				**Μέγιστος βαθμός αποτίμησης όλων των σεναρίων**
Επίπεδο Επίπτωσης	**ΜΕΤΡΙΟ**				

Στον πίνακα που ακολουθεί πραγματοποιούμε αποτίμηση της διαθεσιμότητας των αγαθών δεδομένων, χρησιμοποιώντας τις ίδιες επιπτώσεις αλλά διαφορετική κλίμακα η οποία παρουσιάστηκε στην αρχή της ενότητας αυτή. Έτσι, έχουμε:

Business impact levels (ISO 27005)

0	1	2	3	4
Very Low	**Low**	**Medium**	**High**	**Very High**

#	**1**	**ΑΓΑΘΟ**	**Δεδομένα Αυθεντικοποίησης**			
ΑΠΩΛΕΙΑ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ						
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης**					**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ					
	Διάρκεια Διακοπής					
	2 ώρες (μη εργάσιμες)	**8 ώρες (μη εργάσιμες)**	**2 ώρες**	**8 ώρες**	**1 ημέρα**	
Εξωτερικό περιβάλλον						
Επιπτώσεις στις πολιτικές σχέσεις	0	0	0	0	1	
Διαταραχή πολιτικής απόφασης	0	0	0	0	1	
Επιπτώσεις στην άμυνα και την εθνική ασφάλεια	0	0	0	0	1	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	0	0	1	2	3	
Επιπτώσεις στη δημόσια τάξη	0	0	0	0	0	
Διαδικασίες και Συστήματα						
Διαταραχή ελέγχου διαχείρισης	0	0	1	3	4	
Υποβάθμιση υπηρεσιών	0	0	1	1	2	
Απρόβλεπτες ή πρόσθετες δαπάνες	0	0	1	1	2	
Απώλεια αγαθών	0	0	1	2	3	
Υπέρβαση προϋπολογισμού	0	0	1	1	2	
Επιπτώσεις σε πελάτες / υπαλλήλους						
Υγεία και ασφάλεια	1	1	1	2	3	
Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων	0	0	0	0	0	
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	1	1	1	2	3	
Κατάχρηση προσωπικών δεδομένων	0	0	0	0	0	
Νομικές και κανονιστικές επιπτώσεις						
Παραβίαση της ιδιωτικότητας	0	0	1	2	3	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων	0	0	1	2	3	
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)	0	0	1	2	3	

Παρεμπόδιση εφαρμογής νόμου ή κανονισμών	0	0	1	2	3	
ΣΥΝΟΛΙΚΟΙ ΒΑΘΜΟΙ	**2 ώρες (μη εργάσιμες)**	**8 ώρες (μη εργάσιμες)**	**2 ώρες**	**8 ώρες**	**1 ημέρα**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**1**	**1**	**3**	**4**	
Τελικός Βαθμός Αποτίμησης Αγαθού	**4**					**Μέγιστος βαθμός αποτίμησης όλων των σεναρίων**
Επίπεδο Επίπτωσης	**ΠΟΛΥ ΥΨΗΛΟ**					

#	**2**	**ΑΓΑΘΟ**	**Δεδομένα Παραμετροποίησης**			
ΑΠΩΛΕΙΑ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ						
Επιπτώσεις κάθε σεναρίου (λαμβάνεται υπόψη το χειρότερο σενάριο (worst case)	**Επίπεδο Επίπτωσης**					**Σχόλια**
	0=ΠΧ, 1=Χ, 2=Μ, 3=Υ, 4=ΠΥ					
	Διάρκεια Διακοπής					
	2 ώρες (μη εργάσιμες)	**8 ώρες (μη εργάσιμες)**	**2 ώρες**	**8 ώρες**	**1 ημέρα**	
Εξωτερικό περιβάλλον						
Επιπτώσεις στις πολιτικές σχέσεις	0	0	0	0	1	
Διαταραχή πολιτικής απόφασης	0	0	0	0	1	
Επιπτώσεις στην άμυνα και την εθνική ασφάλεια	0	0	0	0	1	
Επιπτώσεις στη φήμη / εικόνα του Οργανισμού	0	0	1	2	3	
Επιπτώσεις στη δημόσια τάξη	0	0	0	0	0	
Διαδικασίες και Συστήματα						
Διαταραχή ελέγχου διαχείρισης	0	0	1	2	3	
Υποβάθμιση υπηρεσιών	0	0	1	1	2	
Απρόβλεπτες ή πρόσθετες δαπάνες	0	0	1	1	2	
Απώλεια αγαθών	0	0	1	2	3	
Υπέρβαση προϋπολογισμού	0	0	1	1	2	
Επιπτώσεις σε πελάτες / υπαλλήλους						
Υγεία και ασφάλεια	1	1	1	2	2	
Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων	0	0	0	0	0	
Επιπτώσεις στο ηθικό ή την παραγωγικότητα του προσωπικού	1	1	1	2	3	

Κατάχρηση προσωπικών δεδομένων	0	0	0	0	0	
Νομικές και κανονιστικές επιπτώσεις						
Παραβίαση της ιδιωτικότητας	0	0	1	2	3	
Αποκάλυψη ευαίσθητων προσωπικών δεδομένων	0	0	1	2	3	
Παραβίαση συμφωνητικών μη αποκάλυψης (Non disclosure agreements)	0	0	1	2	3	
Παρεμπόδιση εφαρμογής νόμου ή κανονισμών	0	0	1	2	3	
ΣΥΝΟΛΙΚΟΙ ΒΑΘΜΟΙ	**2 ώρες (μη εργάσιμες)**	**8 ώρες (μη εργάσιμες)**	**2 ώρες**	**8 ώρες**	**1 ημέρα**	
Ο συνολικός βαθμός προκύπτει ως ο μέγιστος βαθμός της συγκεκριμένης στήλης	**0**	**1**	**1**	**2**	**3**	
Τελικός Βαθμός Αποτίμησης Αγαθού	**3**					**Μέγιστος βαθμός αποτίμησης όλων των σεναρίων**
Επίπεδο Επίπτωσης	**ΥΨΗΛΟ**					

Αφού οκλοκληρώσαμε την αποτίμηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των αγαθών (εδώ είδαμε τα Δεδομένα Αυθεντικοποίησης και Δεδομένα Παραμετροποίησης), θα πρέπει να καταγράψουμε την συνολική αποτίμηση επιπτώσεων ασφάλειας (Εμπιστευτικότητας-Ακεραιότητας-Διαθεσιμότητας) για όλα τα αγαθά του οργανισμού. Η κλίμακα που χρησιμοποιούμε είναι η εξής:

Κλίμακα Αποτίμησης Επιπτώσεων Ασφάλειας

ΒΑΘΜΟΣ ΕΠΙΠΤΩΣΗΣ	Περιγραφή
0	**VERY LOW (VL)**
1	**LOW (L)**
2	**MEDIUM (M)**
3	**HIGH (H)**
4	**VERY HIGH (VH)**

						ΒΑΘΜΟΣ ΕΠΙΠΤΩΣΗΣ			4
#	Όνομα Αγαθού	Περιγραφή	Κατηγορία	Τοποθεσία	Ιδιοκτήτης	C	I	A	MAX
1	Κτήρια-Εγκαταστάσεις	Το κτήριο όπου στεγάζεται η εφαρμογή uCMDB	Φυσικά Αγαθά (Physical Asset)	Κτήρια-Εγκαταστάσεις	Ιδιοκτήτης κτηρίου	**4**	**4**	**4**	**4**
2	Computer room (CR)	Το δωμάτιο στο οποίο στεγάζεται το βασικό δίκτυο των servers και γενικά όλο το H/W - S/W της εφαρμογής	Φυσικά Αγαθά (Physical Asset)	Computer room (CR)	Ιδιοκτήτης κτηρίου	**4**	**4**	**4**	**4**
3	Server Computer	Ο server HP uCMDB Server v10.22 του web server της εφαρμογής	Υλικά αγαθά (H/W)	Computer room (CR)	ITSM Team	**4**	**4**	**4**	**4**
4	Cabling	Τα διάφορα cables μεταξύ των components της εφαρμογής	Υλικά αγαθά (H/W)	Computer room (CR)	ITSM Team	**3**	**3**	**3**	**3**
5	Βασικό router του CR	Το βασικό router του CR	Υλικά αγαθά (H/W)	Computer room (CR)	ITSM Team	**3**	**3**	**3**	**3**
6	Βασικό switch του CR	Το βασικό switch του CR	Υλικά αγαθά (H/W)	Computer room (CR)	ITSM Team	**3**	**3**	**3**	**3**
7	Βασικό firewall του CR	Το βασικό firewall του CR	Υλικά αγαθά (H/W)	Computer room (CR)	ITSM Team	**3**	**3**	**3**	**3**
8	Λειτουργικό Σύστημα	Το λειτουργικό σύστημα του Web Server, του Database Server, κλπ.	Αγαθά Λογισμικού (S/W)	Computer room (CR)	ITSM Team	**3**	**3**	**3**	**3**
9	Web Server	Στον web server εκτελούνται όλες οι σημαντικές λειτουργίες της εφαρμογής, όπως η αποστολή queries στην βάση του db server.	Αγαθά Λογισμικού (S/W)	Computer room (CR)	ITSM Team	**4**	**4**	**4**	**4**
10	Database Server	Ο database server φιλοξενεί την βάση της uCMDB.	Αγαθά Λογισμικού (S/W)	Computer room (CR)	ITSM Team	**4**	**3**	**4**	**4**
11	DF Probe – Probe DB	Αυτό το component χρησιμεύει στο discovery όλων των infrastructure assets του οργανισμού.	Αγαθά Λογισμικού (S/W)	Computer room (CR)	ITSM Team	**3**	**3**	**3**	**3**

12	Δικτυακό Λογισμικό	Το λογισμικό του βασικού δικτύου των servers όπου φιλοξενείται η web εφαρμογή uCMDB	Αγαθά Λογισμικού (S/W)	Computer room (CR)	ITSM Team	**3**	**3**	**3**	**3**
13	Δεδομένα Αυθεντικοποίησης	Στην κατηγορία αυτή ανήκουν τα στοιχεία αυθεντικοποίησης των χρηστών, το Login Session, κλπ.	Αγαθά Δεδομένων (DATA)	Computer room (CR)	ITSM Team	**3**	**3**	**4**	**4**
14	Δεδομένα παραμετροποίησης	Στην κατηγορία αυτή ανήκει ο πηγαίος κώδικας της ιστοσελίδας, τα Configuration Αρχεία της ιστοσελίδας και τα Organization data π.χ., discovery IT data, views, enrichments, credentials (encrypted), integration points κ.α	Αγαθά Δεδομένων (DATA)	Computer room (CR)	ITSM Team	**2**	**2**	**3**	**3**
15	Admin	Ο χρήστης που χρήστης που διαχειρίζεται την εφαρμογή και μπορεί να δημιουργεί queries, discovery IT data, views, enrichments, credentials (encrypted), integration points και να τα αλλάζει infrastructure settings.	Χρήστες (USERS)						
16	Installation user	Ο χρήστης με admin credentials αλλά και με δικαίωματα εγκατάστασης.	Χρήστες (USERS)						
17	Integration user	Χρήση για integration μεταξύ των components. Δικαίωμα read/write στην βάση.	Χρήστες (USERS)						
18	End user	Χρήστης με δικαίωμα	Χρήστες (USERS)						

		πρόσβασης στο uCMDB UI, uCMDB browser αλλά με δικαιώματα read only.							
19	Workstation	Πρόκειται για το workstation του διαχειριστή (admin) της εφαρμογής uCMDB.	Υλικά αγαθά (H/W)	Computer room (CR)	Admin	**3**	**3**	**3**	**3**

Σημείωση: Για τα αγαθα τύπου « ΧΡΗΣΤΕΣ » δεν υποστηρίζεται η αποτίμηση επιπτώσεων ασφάλειας (Εμπιστευτικότητας-Ακεραιότητας-Διαθεσιμότητας) σύμφωνα με το πρότυπο ISO 27005, γι’αυτό και οι συγκεκριμένες στήλες είναι κενές στον παραπάνω πίνακα.

6.3 Αποτίμηση των αδυναμιών και των απειλών της εφαρμογής uCMDB

Αφού ολοκληρώσουμε την αποτίμηση των αδυναμιών και των απειλών για την εφαρμογή uCMDB, σειρά έχει η αποτίμηση απειλών και αδυναμιών της εφαρμογής έτσι ώστε να προκύψει ο τελικός πίνακας της αποτίμησης κινδύνου ο οποίος θα περιέχει τον αντίστοιχο κίνδυνο για κάθε συνδυασμό Αγαθού-Απειλής-Αδυναμίας. Συγκεκριμένα, για κάθε κατηγορία αγαθού που ορίσαμε σε προήγουμενη ενότητα θα γίνει καταγραφή μιας λίστας ενδεικτικών Απειλών – Αδυναμιών. Έτσι, έχουμε τους παρακάτω πίνακες ανά κατηγορία αγαθού:

1. **Physical Asset: Κτήρια – Εγκαταστάσεις (συγκαταλέγεται και το Computer Room)**

Απειλές	Αδυναμίες
Μη έγκαιρη αποκατάσταση πληροφοριακών συστημάτων	Έλλειψη σχεδίου Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan)
	Έλλειψη εφεδρικού υπολογιστικού κέντρου ή σύμβασης με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών
	Τα συστήματα που περιλαμβάνονται στο Σχέδιο Ανάκαμψης από Καταστροφή δεν καλύπτουν πλήρως τα κρίσιμα πληροφοριακά συστήματα, όπως προκύπτουν από από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας
	Το Σχέδιο Ανάκαμψης από Καταστροφή δεν δοκιμάζεται και δεν ανανεώνεται σε τακτά χρονικά διαστήματα
	Δεν είναι διαθέσιμη σε όλο το προσωπικό, λίστα με χρήσιμα τηλέφωνα επικοινωνίας για περίπτωση καταστροφής
	Έλλειψη ελέγχου φυσικής πρόσβασης στο εναλλακτικό κέντρο λειτουργίας
Πυρκαγιά	Ακαταλληλότητα υλικών κατασκευής (π.χ. μη πυράντοχες πόρτες, πάτωμα, ξύλινη επικάλυψη στον τοίχο κλπ.)
	Έλλειψη κατάλληλων μέσων πυρόσβεσης
	Έλλειψη κατάλληλων μηχανισμών ανίχνευσης φωτιάς
	Ύπαρξη εύφλεκτων υλικών και ελλιπής καθαριότητα
	Ανεπαρκής συντήρηση πυροσβεστικών μέσων
	Απουσία πλάνου εκκένωσης
	Ελλειπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας
	Η εγκατάσταση βρίσκεται κοντά σε χώρους με αυξημένο κίνδυνο πυρκαγίας (π.χ. πρατήριο καυσίμων, δασική εκταση κλπ.)
Σεισμός	Ακατάλληλες κτιριακές υποδομές
	Απουσία πλάνου εκκένωσης

Πλημμύρα	Απουσία εξοπλισμού ανίχνευσης διεισδυσης νερού / υγρασίας
	Κρίσιμος εξοπλισμός τοποθετημένος σε τοποθεσία με πηγές ύδατος (σωληνώσεις κτλ)
	Κρίσιμος εξοπλισμός δεν είναι καλυμένος με αδιάβροχα καλύματα
	Απουσία αντλιών νερού με ανεξάρτητη παροχή ενέργειας
Καιρικά φαινόμενα / Ακραίες συνθήκες	Οι εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα είναι ευάλωτες σε παλιρροϊκό κύμα
	Οι εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα είναι ευάλωτες σε ακραίες συνθήκες θερμοκρασίας και υγρασίας
	Ελλιπής συντήρηση των εγκαταστάσεων που φιλοξενούν κρίσιμα συστήματα
Ανεπάρκεια Κλιματισμού	Ακαταλληλότητα κλιματισμού στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα
	Παλαιότητα κλιματισμού στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα
	Ελλιπής συντήρηση κλιματισμού στις εγκαταστάσεις που φιλοξενούν κρίσιμα συστήματα
Διακυμάνσεις ηλεκτρικής ισχύος / Διακοπή ηλεκτροδότησης	Απουσία εξοπλισμού Αδιάληπτης Παροχής Τροφοδοσίας Ηλεκτρικού Ρεύματος (UPS)
	Έλλειψη εναλλακτικών μεθόδων παροχής ηλεκτρικής ενέργειας
	Έλλειψη προστασίας των κτιρίων από αστραπές
	Οι εξωτερικές γραμμές παροχής είναι εκτεθειμένες σε φυσικές καταστροφές ή σε τρίτους
Δολιοφθορά (Sabotage)	Έλλειψη πολιτικών και διαδικασιών (φυσικής) διαχείρισης πρόσβασης
	Οι κτηριακές υποδομές δεν παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack)
	Οι πόρτες δεν είναι ανθεκτικές σε επίθεση / δεν έχουν θωράκιση
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού
	Στους χώρους όπου υπάρχει κρίσιμος εξοπλισμος επιτρέπεται η πρόσβαση στο κοινό

2. H/W : Εξυπηρετητές – Servers

Απειλές	**Αδυναμίες**
Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένων εξυπηρετητών
	Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή

	Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου
	Ανεπαρκής εποπτεία της λειτουργίας των εξυπηρετητών
	Δεν εφαρμόζεται πολιτική απαγόρευσης χρήσης φαγητού, ποτών και καπνίσματος στους χώρους όπου φιλοξενούνται εξυπηρετητές
	Έλλειψη συμβολαίων συντήρησης ή εγγυήσης των εξυπηρετητών
	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων
	Ελλιπής συντήρηση των εξυπηρετητών
Σφάλμα χειρισμού και διαχείρησης	Ανεπαρκής επαγγελματική εμπειρία - εξειδίκευση των διαχειριστών
	Έλλειψη εκπαίδευσης των διαχειριστών
	Έλλειψη αξιολόγησης διαχειριστών
	Ανεπαρκής έγγραφη τεκμηρίωση χρήσης και διαχείρισης των εξυπηρετητών
	Μη διατήρηση αρχείων με τις μετατροπές και επισκευές στους εξυπηρετητές
	Απουσία μηχανισμών ελέγχου
Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Ελλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)
	Χρήση εξυπηρετητή για περισσότερες από μία υπηρεσίες
	Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές
Κλοπή	Ο εξυπηρετητής δεν βρίσκεται εντός υπολογιστικού κέντρου (data center) με ελεγχόμενη πρόσβαση
	Στους χώρους όπου φιλοξενούνται εξυπηρετητές επιτρέπεται η πρόσβαση στο κοινό
	Έλλειψη πολιτικών και διαδικασιών φυσικής πρόσβασης στο χώρο που φιλοξενείται ο εξυπηρετητής
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας

3. H/W : Σταθμός Εργασίας – Workstation

Απειλές	Αδυναμίες
Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένου εξοπλισμού

	Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή
	Λειτουργία εξοπλισμού σε ακραίες συνθήκες φόρτου
	Έλλειψη συμβολαίων συντήρησης ή εγγυήσης;
	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων
	Ελλιπής συντήρηση του εξοπλισμού
Σφάλμα χειρισμού	Ανεπαρκής επαγγελματική εμπειρία - εξειδίκευση των χρηστών
	Έλλειψη εκπαίδευσης των χρηστων
	Έλλειψη αξιολόγησης χρηστών
	Ανεπαρκής έγγραφη τεκμηρίωση χρήσης και διαχείρισης του εξοπλισμού
	Απουσία μηχανισμών ελέγχου
Κλοπή	Έλλειψη πολιτικών και διαδικασιών φυσικής πρόσβασης στο χώρο που φιλοξενείται ο εξυπηρετητής
	Οι κτηριακές υποδομές δεν παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack)
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού
	Στους χώρους όπου φιλοξενούνται σταθμοί εργασίας επιτρέπεται η πρόσβαση στο κοινό

4. H/W : Δικτυακός Εξοπλισμός – Network

Απειλές	**Αδυναμίες**
Τεχνικές Βλάβες και Αστοχίες	Ύπαρξη πεπαλαιωμένου εξοπλισμού
	Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή
	Λειτουργία δικτυακού εξοπλισμού σε ακραίες συνθήκες φόρτου
	Υπερφόρτωση δικτύου
	Ανεπαρκής εποπτεία της λειτουργίας του εξοπλισμού και του δικτύου
	Έλλειψη συμβολαίων συντήρησης ή εγγυήσης

	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων
	Ελλιπής συντήρηση του δικτυακού εξοπλισμού
Σφάλμα χειρισμού και συντήρησης	Ανεπαρκής επαγγελματική εμπειρία των διαχειριστών
	Έλλειψη εκπαίδευσης των διαχειριστών
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας
	Έλλειψη αξιολόγησης χρηστών / διαχειριστών
	Μη διατήρηση αρχείων με τις μετατροπές και επισκευές στον δικτυακό εξοπλισμό
	Απουσία μηχανισμών ελέγχου
Άρνηση Υπηρεσίας (Denial of Service)	Ελλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)
	Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές
Ηλεκτρονικές Παρεμβολές	Η περιοχή είναι ευάλωτη σε ηλεκτρονικές παρεμβολές
	Έλλειψη προστασίας/θωράκισης των δικτυακών υποδομών από Η/Μ παρεμβολές
Παρακολούθηση επικοινωνιών	Στους χώρους όπου βρίσκεται ο δικτυακός εξοπλισμός επιτρέπεται η πρόσβαση στο κοινό
	Ανεπαρκής διαδικασία διαχείρισης αλλαγών για τις υποδομές δικτύου.
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού
Κλοπή	Έλλειψη πολιτικών και διαδικασιών διαχείρισης φυσικής πρόσβασης
	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού
	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού
	Στους χώρους όπου φιλοξενείται ο δικτυακός εξοπλισμός επιτρέπεται η πρόσβαση στο κοινό

5. S/W: Λειτουργικό Σύστημα (OS)

Απειλές	Αδυναμίες
Κακόβουλο Λογισμικό (Malicious Code)	Απουσία λογισμικού ανίχνευσης κακόβουλου λογισμικού (antivirus) ή ελλειπής διαχείριση του antivirus (π.χ. δεν ανανεώνεται αυτόματα)
	Απουσία ή ανεπαρκής παραμετροποίηση του λογισμικού αναχώματος ασφαλείας (personal firewall)
	Οι απλοί χρήστες έχουν διαχειριστικά δικαιώματα (π.χ. δικαίωμα εγκατάστασης λογισμικού)
	Οι χρήστες έχουν δικαιώματα χρήσης εξωτερικών μέσων αποθήκευσης (cd, usb κτλ)
	Έλλειψη πολιτικής αυτόματου ελέγχου επισυναπτόμενων αρχείων του ηλεκτρονικού ταχυδρομείου
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα ασφαλείας
	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)
	Έλλειψη διαδικασίας ελέγχου αξιοπιστίας του λογισμικού πριν την εγκατάστασή του
	Έλλειψη διαδικασίας αναφοράς ή/και αντιμετώπισης περιστατικών ασφαλειάς
	Ανεπαρκείς μηχανισμοί καταγραφής πρόσβασης και ενεργειών στο σύστημα (audit logs)
	Ανεπαρκής έλεγχος και επισκόπιση των αρχείων καταγραφής.
	Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)
Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	Υπάρχει πολιτική για την υποχρεωτική χρήση αυθεντικού λογισμικού;
	Έλλειψη επισκόπησης (audit) λογισμικού
	Δυνατότητα εγκατάστασης λογισμικού από τους χρήστες
Μη εξουσιοδοτημένη πρόσβαση χρηστών (unauthorized access / weak authentication)	Η πρόσβαση στο σύστημα είναι δυνατή χωρίς κανένα έλεγχο (π.χ. δεν απαιτείται η χρήση κάποιου κωδικού πρόσβασης ή βιομετρικού χαρακτηριστικού ή/και έξυπνης κάρτας)
	Η ισχύς (πολυπλοκότητα) των κωδικών δεν ελέγχονται αυτόματα πριν την έκδοσή τους (π.χ. δεν υπάρχει εγκατεστημένη πολιτική κωδικών)
	Οι κωδικοί πρόσβασης, αποθηκεύονται σε απλή και όχι σε κρυπτογραφημένη μορφή στο σύστημα (π.χ. hashed passwords)
	Είναι ενεργοποιημένη η απομακρυσμένη πρόσβαση των χρηστών στο σύστημα (remote login)
	Το σύστημα περιέχει τους αρχικούς λογαριασμούς ή/και κωδικούς πρόσβασης (default accounts, default passwords)

	Το σύστημα επιτρέπει τη χρήση του ίδιου συνθηματικού για περισσότερο από 1 χρόνο
	Ανεπαρκείς μηχανισμοί καταγραφής πρόσβασης και ενεργειών στο σύστημα (audit logs)
	Δεν πραγματοποιούνται συστηματικά έλεγχοι αποτίμησης αδυναμιών (Vulnerability Assessments) και δοκιμές διείσδυσης (penetration tests)
Δικτυακή εισβολή (network intrusion)	Επιτρέπεται η απομακρυσμένη διαχείριση του συστήματος χωρίς ασφαλή σύνδεση
	Το σύστημα είναι εγκατεστημένο σε δίκτυο μη προστατευμένο δίκτυο (π.χ. απουσία αναχώματος ασφαλείας - firwewall)
	Η δικτυακή πρόσβαση στο σύστημα δεν ελέγχεται από σύστημα ανίχνευσης παρείσφρησης (Intrusion Detection/ Prevention System)
	Έλλειψη διαδικασίας τακτικού ελέγχου των συστημάτων περιμετρικής προστασίας του δικτύου (π.χ. Firewall, IDS κτλ)
	Το σύστημα δεν διαχωρίζεται από άλλα δίκτυα με τη χρήση αρχιτεκτονικών δικτύων (π.χ. VLAN, LAN, switches κτλ)
Εσφαλμένος χειρισμός/χρήση συστήματος (System missuse)	Ανεπαρκής επαγγελματική εμπειρία των χρηστών
	Έλλειψη εκπαίδευσης χρηστών
	Οι απλοί χρήστες έχουν διαχειριστικά δικαιώματα (π.χ. δικαίωμα εγκατάστασης λογισμικού)
Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration missuse)	Ανεπαρκής επαγγελματική εμπειρία /εξειδίκευση των διαχειριστών
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης των διαχειριστώνσε ζητήματα ασφαλείας
	Ανεπαρκής έγγραφη τεκμηρίωση διαχείρισης του λογισμικού
	Το Λειτουργικό Σύστημα δεν είναι ενημερωμένο με τις πιο πρόσφατες διορθώσεις αδυναμιών (patches)
	Έλλειψη αντιγράφων επαναφοράς του συστήματος

6. S/W: Database Server

Απειλές	Αδυναμίες
Επίθεση κλοπής/ αλλοίωσης δεδομένων	Μη χρήση μηχανισμών κρυπτογράφησης των ευαίσθητων δεδομένων

	Μη χρήση μηχανισμών ελέγχου ακεραιότητας των ευαίσθητων δεδομένων
	Έλλειψη διαδικασίας ελέγχου πρόσβασης και καταγραφής ενεργειών σε επίπεδο βάσης δεδομένων
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών
Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ και στη βάση να περνούν μόνο έγκυρα πεδία….)
	Έλλειψη ελέγχου ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.
	Έλλειψη ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών
Εσφαλμένη διαχείριση εφαρμογής	Ανεπαρκής επαγγελματική εμπειρία των διαχειριστών εφαρμογής
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης των διαχειριστών σε ζητήματα ασφαλείας
	Ανεπαρκής έγγραφη τεκμηρίωση διαχείρισης του λογισμικού
	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)
	Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της
	Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)
	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)
Απώλεια δεδομένων	Μη διαθεσιμότητα αντιγράφων ασφαλείας
	Έλλειψη διαδικασίας λήψης αντιγράφων ασφαλείας
	Μη διαθεσιμότητα αντιγράφων ασφαλείας για κρίσιμα δεδομένα
	Έλλειψη διαδικασίας ανάκαμψης αντιγράφων ασφαλείας

7. S/W: Application Server

Απειλές	Αδυναμίες

Επίθεση XSS	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation)
	Μη χρήση συναρτήσεων μετατροπής ειδικών χαρακτήτων σε απλή html
	Μη χρήση τεχνικών αφαίρεσης μη έγκυρων ετικετών html
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών
Επίθεση sql injection	Έλλειψη ελέγχων της εγκυρότητας των δεδομένων εισόδου (input validation), ώστε να επιτρέπονται μόνο έγκυροι τύποι δεδομένων στις φόρμες, πεδία κτλ και στη βάση να περνούν μόνο έγκυρα πεδία)
	Έλλειψη ελέγχου ώστε να μην γίνεται επιστροφή αναλυτικών μηνυμάτων σφάλματος για τη βάση.
	Έλλειψη ελέγχου ώστε ο web server να μην παρέχει πληροφορίες διαμόρφωσης (configuration), π.χ. μέσω banner
	Έλλειψη ελέγχου λειτουργίας ανεπιθύμητων υπηρεσιών - θυρών
Εσφαλμένη διαχείριση εφαρμογής	Ανεπαρκής επαγγελματική εμπειρία των διαχειριστών εφαρμογής
	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης των διαχειριστών σε ζητήματα ασφαλείας
	Ανεπαρκής έγγραφη τεκμηρίωση διαχείρισης του λογισμικού
	Έλλειψη διαδικασίας διαχείρισης αλλαγών (change management process)
	Έλλειψη αντιγράφων ασφαλείας της εφαρμογής και των δεδομένων της
	Ανεπαρκής / μη έγκαιρη ενημέρωση εφαρμογής (sw update)
	Μη επαρκής διαχωρισμός αρμοδιοτήτων διαχειριστών και τελικών χρηστών (π.χ. οι χρήστες της εφαρμογής μπορούν να δημιουργήσουν νέο λογαριασμό χρήστη)

8. S/W: Δικτυακό λογισμικό (net)

Απειλές	**Αδυναμίες**
Παρακολούθηση επικοινωνιών (Traffic Monitoring)	Μετάδοση δεδομένων μέσω μη ασφαλών διαύλων

	Χρήση δημόσιων δικτύων
	Μετάδοση διαβαθμισμένων δεδομένων στο δίκτυο
	Μη υλοποίηση μεταπηδησης συχνοτήτων σε ευρύ φάσμα (frequency hopping spread spectrum)
	Μη χρήση κρυπτογραφίας για τη μετάδοση κρίσιμων δεδομένων
	Μη ορθή παραμετροποίηση δικτυακού εξοπλισμου
Εξαπάτηση διεύθυνσης δικτύου (IP Spoofing)	Η αυθεντικοποίηση πραγματοποιείται μόνο βάση της διεύθυνσης δικτύου (IP address)
	Έλλειψη ιχνών ασφαλείας (audit logs)
	Έλλειψη Συστήματος Ανίχνευσης Παρείσφρησης (Intrusion Detection System - IDS)
Εξαπάτηση φυσικής διεύθυνσης (MAC spoofing)	Η αυθεντικοποίηση πραγματοποιείται μόνο βάση της φυσικής διεύθυνσης (MAC address)
	Έλλειψη Συστήματος Ανίχνευσης Παρείσφρησης (Intrusion Detection System - IDS)
	Ανεπαρκείς μηχανισμοί παρακολούθησης
Μη ορθή δρομολόγηση επικοινωνιών	Απουσία κεντρικού συστήματος ελέγχου και εποπτείας του δικτύου
	Κατάχρηση των θυρών απομακρυσμένης πρόσβασης (remote maintenance ports)
	Μη ορθή παραμετροποίηση δικτυακού εξοπλισμου

Στη συνέχεια, αφού καταγράψαμε για κάθε κατηγορία αγαθού το ζεύγος « Απειλή – Αδυναμία », θα πραγματοποίησουμε την αποτίμηση των απειλών και αδυναμιών συνολικά για όλα τα αγαθά. Για κάθε αγαθό προφανώς θα έχουμε πολλες εγγραφές, ανάλογα με το πόσες απειλές θα εξετάσουμε. Η αποτίμηση αυτή θα γίνει σύμφωνα με τις παρακάτω κλίμακες:

Κλίμακα Αποτίμησης Απειλών

Επίπεδο Απειλής	Βαθμός Απειλής	Περιγραφή
LOW (L)	**0**	**αναμένεται να συμβούν το πολύ μέχρι μία φορά κάθε 10 χρόνια**
MEDIUM (M)	**1**	**αναμένεται να συμβούν κατά μέσο όρο μία φορά τα 3 χρόνια.**
HIGH (H)	**2**	**αναμένεται να συμβούν κατά μέσο όρο μία φορά το χρόνο**

Κλίμακα Αποτίμησης Αδυναμιών

Επίπεδο Αδυναμίας	Βαθμός Αδυναμίας	Περιγραφή
LOW (L)	**0**	**Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι < 33%**
MEDIUM (M)	**1**	**Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι 33% - 66%**
HIGH (H)	**2**	**Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι > 66%**

'Ονομα Αγαθού	Όνομα Απειλής	Επίπεδο Απειλής	Επίπεδο Αδυναμίας
server 1	Τεχνικές Βλάβες και Αστοχίες	Μέτριο (M)	Χαμηλό (X)
server 1	Σφάλμα χειρισμού και διαχείρησης	Μέτριο (M)	Χαμηλό (X)
server 1	Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού	Υψηλό (Y)	Μέτριο (M)
server 1	Κλοπή	Μέτριο (M)	Χαμηλό (X)
Κτήριο – Εγκαταστάσεις 1	Μη έγκαιρη αποκατάσταση πληροφοριακών συστημάτων	Μέτριο (M)	Μέτριο (M)
Κτήριο – Εγκαταστάσεις 1	Πυρκαγιά	Χαμηλό (X)	Μέτριο (M)
Κτήριο – Εγκαταστάσεις 1	Σεισμός	Χαμηλό (X)	Χαμηλό (X)
Κτήριο – Εγκαταστάσεις 1	Πλημμύρα	Χαμηλό (X)	Χαμηλό (X)
Κτήριο – Εγκαταστάσεις 1	Καιρικά φαινόμενα / Ακραίες συνθήκες	Χαμηλό (X)	Χαμηλό (X)
Κτήριο – Εγκαταστάσεις 1	Ανεπάρκεια Κλιματισμού	Χαμηλό (X)	Χαμηλό (X)
Κτήριο – Εγκαταστάσεις 1	Διακυμάνσεις ηλεκτρικής ισχύος / Διακοπή ηλεκτροδότησης	Χαμηλό (X)	Χαμηλό (X)
Κτήριο – Εγκαταστάσεις 1	Δολιοφθορά (Sabotage)	Χαμηλό (X)	Χαμηλό (X)
Σταθμός εργασίας 1	Τεχνικές Βλάβες και Αστοχίες	Μέτριο (M)	Μέτριο (M)
Σταθμός εργασίας 1	Σφάλμα χειρισμού	Υψηλό (Y)	Υψηλό (Y)
Σταθμός εργασίας 1	Κλοπή	Χαμηλό (X)	Χαμηλό (X)
Δικτυακός εξοπλισμός 1	Τεχνικές Βλάβες και Αστοχίες	Υψηλό (Y)	Μέτριο (M)
Δικτυακός εξοπλισμός 1	Σφάλμα χειρισμού και συντήρησης	Υψηλό (Y)	Μέτριο (M)

Δικτυακός εξοπλισμός 1	Άρνηση Υπηρεσίας (Denial of Service)	Υψηλό (Υ)	Μέτριο (Μ)
Δικτυακός εξοπλισμός 1	Ηλεκτρονικές Παρεμβολές	Χαμηλό (Χ)	Χαμηλό (Χ)
Δικτυακός εξοπλισμός 1	Παρακολούθηση επικοινωνιών	Χαμηλό (Χ)	Χαμηλό (Χ)
Δικτυακός εξοπλισμός 1	Κλοπή	Χαμηλό (Χ)	Χαμηλό (Χ)
Λειτουργικό Σύστημα 1	Κακόβουλο Λογισμικό (Malicious Code)	Υψηλό (Υ)	Μέτριο (Μ)
Λειτουργικό Σύστημα 1	Εγκατάσταση και χρήση "πειρατικού" λογισμικού (pirate software)	Μέτριο (Μ)	Χαμηλό (Χ)
Λειτουργικό Σύστημα 1	Μη εξουσιοδοτημένη πρόσβαση χρηστών (unauthorized access / weak authentication)	Μέτριο (Μ)	Χαμηλό (Χ)
Λειτουργικό Σύστημα 1	Δικτυακή εισβολή (network intrusion)	Μέτριο (Μ)	Μέτριο (Μ)
Λειτουργικό Σύστημα 1	Εσφαλμένος χειρισμός/χρήση συστήματος (System missuse)	Μέτριο (Μ)	Υψηλό (Υ)
Λειτουργικό Σύστημα 1	Ελλιπής / εσφαλμένη διαχείριση λειτουργικού συστήματος (Administration missuse)	Μέτριο (Μ)	Μέτριο (Μ)
Database Server 1	Επίθεση κλοπής/ αλλοίωσης δεδομένων	Υψηλό (Υ)	Υψηλό (Υ)
Database Server 1	Επίθεση sql injection	Υψηλό (Υ)	Υψηλό (Υ)
Database Server 1	Εσφαλμένη διαχείριση εφαρμογής	Μέτριο (Μ)	Χαμηλό (Χ)
Database Server 1	Απώλεια δεδομένων	Μέτριο (Μ)	Χαμηλό (Χ)
Application Server 1	Επίθεση XSS	Υψηλό (Υ)	Υψηλό (Υ)
Application Server 1	Επίθεση sql injection	Υψηλό (Υ)	Υψηλό (Υ)
Application Server 1	Εσφαλμένη διαχείριση εφαρμογής	Μέτριο (Μ)	Χαμηλό (Χ)
Δικτυακό λογισμικό (net) 1	Παρακολούθηση επικοινωνιών (Traffic Monitoring)	Μέτριο (Μ)	Χαμηλό (Χ)
Δικτυακό λογισμικό (net) 1	Εξαπάτηση διεύθυνσης δικτύου (IP Spoofing)	Μέτριο (Μ)	Χαμηλό (Χ)
Δικτυακό λογισμικό (net) 1	Εξαπάτηση φυσικής διεύθυνσης (MAC spoofing)	Μέτριο (Μ)	Χαμηλό (Χ)
Δικτυακό λογισμικό (net) 1	Μη ορθή δρομολόγηση επικοινωνιών	Χαμηλό (Χ)	Χαμηλό (Χ)

6.4 Αποτίμηση κινδύνου της εφαρμογής uCMDB (Συνολικός Πίνακας)

Στο τελευταίο στάδιο της διαδικασίας πραγματοποιείται ουσιαστικά η αποτίμηση κινδύνου για την εφαρμογή και προκύπτει ο συνολικός πίνακας, όπου συγκεντρώνονται οι τιμές για το Impact, Threat, Vulnerability και προκύπτει ο αντίστοιχος Κίνδυνος για κάθε συνδυασμό Αγαθού-Απειλής-Αδυναμίας. Στο συνολικό πίνακα περιλαμβάνεται επιπλέον και η λίστα με τα αντίμετρα για κάθε απειλή – αδυναμία που εντοπίστηκε στην προηγούμενη ενότητα, καθώς και τι στρατηγική πρέπει να ακολουθήσουμε σε κάθε περίπτωση. Συγκεκριμένα, οι δυνατές στρατηγικές αντιμετώπισης του κινδύνου είναι τέσσερις: 1. Μετριασμός, 2. Μεταφορά, 3. Αποδοχή, 4. Αποφυγή. Επίσης, στη στήλη « ΧΡΟΝΟΣ ΥΛΟΠΟΙΗΣΗΣ » οι δυνατές τιμές είναι: 1. ΑΜΕΣΑ, 2. ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ και 3. ΤΟΝ ΕΠΟΜΕΝΟ ΧΡΟΝΟ, οι οποίες δείχνουν το πόσο γρήγορα πρέπει να εφαρμοστεί το προτεινόμενο μέτρο ασφαλείας, πάντα σε σχέση με το επίπεδο του κινδύνου (στήλη Μ) που προέκυψε. Τέλος, στη στήλη « ΕΝΑΠΟΜΕΙΝΩΝ ΚΙΝΔΥΝΟΣ » (Residual Risk) περιγράφεται το επίπεδο κινδύνου που απομένει μετά την υλοποίηση των μέτρων προστασίας. Πιο αναλυτικά, αν στην στρατηγική επιλέξουμε « ΜΕΤΡΙΑΣΜΟΣ » τότε τότε το επίπεδο του Residual Risk θα είναι ΧΑΜΗΛΟ (LOW), αν στην στρατηγική επιλέξουμε « ΑΠΟΔΟΧΗ » τότε το επίπεδο του Residual Risk θα είναι το ίδιο με τον Τελικό Κίνδυνο και αν στην στρατηγική επιλέξουμε « ΜΕΤΑΦΟΡΑ » τότε το επίπεδο του Residual Risk θα είναι το ίδιο πάλι ΧΑΜΗΛΟ (LOW) γιατί μεταφέρεται σε κάποιον συνεργάτη ή προμηθευτή με τις απαραίτητες συμβατικές δεσμεύσεις.

‘Ετσι, ο συνολικός πίνακας που προκύπτει είναι ο εξής: Οι κλίμακες του προτύπου που χρησιμοποιήθηκαν για την αποτίμηση του κινδύνου παρουσιάζονται αναλυτικά στο παράρτημα 2. Ενδεικτικά για λόγους χωρητικότητας, παρουσιάζουμε στον παρακάτω συνολικό πίνακα την αποτίμηση κινδύνων για τα αγαθά server, κτήριο – εγκαταστάσεις.

	Αποτίμηση Επίπτωσης				Απειλές	Επίπεδο Απειλής	Αδυναμίες	ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ	Είπεδο Κινδύνου	Μέτρο Ασφάλειας	ΣΤΡΑΤΗΓΙΚΗ	ΧΡΟΝΟΣ ΥΛΟΠΟΙΗΣΗΣ	ΕΝΑΠΟΜΕΙΝΩΝ ΚΙΝΔΥΝΟΣ RESIDUAL RISK
Αγαθό	C	I	A	MAX									
server 1	2	1	2	**2**	**Τεχνικές Βλάβες και Αστοχίες**	**ΜΕΤΡΙΟ**	Ύπαρξη πεπαλαιωμένων εξυπηρετητών	**ΧΑΜΗΛΟ**	Medium	Η ηλικία των εξυπηρετητών θα πρέπει να είναι μικρότερη από 5 έτη.	ΜΕΤΡΙΑΣΜΟΣ	ΑΜΕΣΑ	**ΧΑΜΗΛΟ**
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Μη τήρηση των προδιαγραφών λειτουργίας και συντήρησης όπως αυτές παρέχονται από τον κατασκευαστή	**ΧΑΜΗΛΟ**	Low	Πρέπει να τηρούνται οι προδιαγραφές του κατασκευαστή κατά την εγκατάσταση, λειτουργία και συντήρηση των εξυπηρετητών.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Λειτουργία εξυπηρετητών σε ακραίες συνθήκες φόρτου	**ΧΑΜΗΛΟ**	Low	Θα πρέπει να αποφεύγεται η χρήση του εξυπηρετητή στο μέγιστο των δυνατοτήτων του, από απόψη χωρητικότητας, φόρτου κλπ.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Ανεπαρκής εποπτεία της λειτουργίας των εξυπηρετητών	**ΧΑΜΗΛΟ**	Low	Θα πρέπει να υπάρχουν διαδικασίες εποπτείας της λειτουργίας των εξυπηρετητών.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**

server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Δεν εφαρμόζεται πολιτική απαγόρευσης χρήσης φαγητού, ποτών και καπνίσματος στους χώρους όπου φιλοξενούνται εξυπηρετητές	**ΧΑΜΗΛΟ**	Low	Πρέπει να εφαρμόζεται πολιτική απαγόρευσης χρήσης φαγητού, ποτών και καπνίσματος στους χώρους όπου φιλοξενούνται εξυπηρετητές.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	1	1	1	**1**		**ΜΕΤΡΙΟ**	Έλλειψη συμβολαίων συντήρησης ή εγγυήσης των εξυπηρετητών	**ΧΑΜΗΛΟ**	Low	Πρέπει να υπάρχει συμβόλαιο συντήρησης για τον συγκεκριμένο εξοπλισμό και να ελέγχεται εάν είναι εντός εγγύησης.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Έλλειψη πόρων και τεχνογνωσίας για αντιμετώπιση τεχνικών αστοχιών και βλαβων	**ΧΑΜΗΛΟ**	Low	Πρέπει να υπάρχουν διαθέσιμοι πόροι και τεχνογνωσία για την επιδιόρθωση τεχνικών αστοχιών και βλαβών στους εξυπηρετητές.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Ελλιπής συντήρηση των εξυπηρετητών	**ΧΑΜΗΛΟ**	Low	Οι εξυπηρετητές θα πρέπει να συντηρούνται ανά τακτά χρονικά διαστήματα.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**

server 1	2	1	2	**2**	**Σφάλμα χειρισμού και διαχείρησης**	**ΜΕΤΡΙΟ**	Ανεπαρκής επαγγελματική εμπειρία - εξειδίκευση των διαχειριστών	**ΧΑΜΗΛΟ**	Low	Κατά τη διαδικασία πρόσληψης προσωπικού να λαμβάνεται υπόψη η επαγγελματική εμπειρία και η εξειδίκευση των διαχειριστών.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	1	1	1	1		**ΜΕΤΡΙΟ**	Έλλειψη εκπαίδευσης των διαχειριστών	**ΧΑΜΗΛΟ**	Low	Πρέπει να υπαρχεί πλάνο εκπαίδευσης για τους διαχειριστές.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	1	1	1	1		**ΜΕΤΡΙΟ**	Έλλειψη αξιολόγησης διαχειριστών	**ΧΑΜΗΛΟ**	Low	Πρέπει να υπάρχει πρόγραμμα αξιολόγησης των διαχειριστών.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	1	1	1	1		**ΜΕΤΡΙΟ**	Ανεπαρκής έγγραφη τεκμηρίωση χρήσης και διαχείρισης των εξυπηρετητών	**ΧΑΜΗΛΟ**	Low	Πρέπει να υπάρχει έγγραφη τεκμηρίωση χρήσης και διαχείρισης των εξυπηρετητών.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	1	1	1	1		**ΜΕΤΡΙΟ**	Μη διατήρηση αρχείων με τις μετατροπές και επισκευές στους εξυπηρετητές	**ΧΑΜΗΛΟ**	Low	Πρέπει να διατηρούνται αρχεία με τις μετατροπές και επισκευές στους εξυπηρετητές.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**

server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Απουσία μηχανισμών ελέγχου	**ΜΕΤΡΙΟ**	Medium	Πρέπει να υπάρχουν μηχανισμοί ελέγχου ώστε να εντοπίζονται τυχόν λάθη χειρισμού.	ΜΕΤΡΙΑΣΜΟΣ	ΑΜΕΣΑ	**ΧΑΜΗΛΟ**
server 1	2	2	3	**3**	**Άρνηση Υπηρεσίας (Denial of Service) λόγω διακοπής λειτουργίας του υλικού**	**ΥΨΗΛΟ**	'Ελλειψη πλεονάζοντος ή εφεδρικού εξοπλισμού (redundant equipment)	**ΥΨΗΛΟ**	High	Για τους εξυπηρετητές που χρησιμοποιούνται για κρίσιμες υπηρεσίες, θα πρέπει να υπάρχει πλεονάζον ή εφεδρικός εξυπηρετητής.	ΑΠΟΔΟΧΗ	ΑΜΕΣΑ	**ΥΨΗΛΟ**
server 1	2	2	3	**3**		**ΥΨΗΛΟ**	Χρήση εξυπηρετητή για περισσότερες από μία υπηρεσίες	**ΥΨΗΛΟ**	High	Θα πρέπει να αποφεύγεται να χρησιμοποιείται ο εξυπηρετητής για την λειτουργία πολλών υπηρεσιών.	ΜΕΤΡΙΑΣΜΟΣ	ΑΜΕΣΑ	**ΧΑΜΗΛΟ**
server 1	2	2	3	**3**		**ΥΨΗΛΟ**	Μη συμμόρφωση με πρότυπα και βέλτιστες πρακτικές	**ΜΕΤΡΙΟ**	Medium	Πρέπει να χρησιμοποιούνται διεθνή πρότυπα και βέλτιστες πρακτικές κατά την παραμετροποιήση και χρήση των εξυπηρετητών.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΜΕΤΡΙΟ**

server 1	2	1	2	**2**	**Κλοπή**	**ΜΕΤΡΙΟ**	Ο εξυπηρετητής δεν βρίσκεται εντός υπολογιστικού κέντρου (data center) με ελεγχόμενη πρόσβαση	**ΧΑΜΗΛΟ**	Low	Η πρόσβαση στους χώρους που βρίσκονται οι εξυπηρετητές, θα πρέπει να ελέγχεται.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Στους χώρους όπου φιλοξενούνται εξυπηρετητές επιτρέπεται η πρόσβαση στο κοινό)	**ΧΑΜΗΛΟ**	Low	Πρέπει να γίνεται έλεγχος της πρόσβασης του κοινού στους χώρους που βρίσκονται εξυπηρετητές και κρίσιμος εξοπλισμός.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Έλλειψη πολιτικών και διαδικασιών φυσικής πρόσβασης στο χώρο που φιλοξενείται ο εξυπηρετητής	**ΧΑΜΗΛΟ**	Low	Πρέπει να υπαρχουν πολιτικές και διαδικασίες για την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις που βρίσκονται οι εξυπηρετητές.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Ανεπαρκής παρακολούθηση των εγκαταστάσεων του οργανισμού	**ΧΑΜΗΛΟ**	Low	Πρέπει να χρησιμοποιούνται κατάλληλα μέσα παρακολούθησης (monitoring) της πρόσβασης στις εγκαταστάσεις που	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**

										φιλοξενούνται εξυπηρετητές.			
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Έλλειψη πολιτικών και διαδικασιών καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού	**ΧΑΜΗΛΟ**	Low	Πρέπει να υπάρχουν πολιτικές και διαδικασιές καθορισμού και επισκόπησης των δικαιωμάτων πρόσβασης του προσωπικου στις εγκαταστάσεις του οργανισμού όπου φιλοξενούνται εξυπηρετητές.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
server 1	2	1	2	**2**		**ΜΕΤΡΙΟ**	Έλλειψη προγράμματος ενημέρωσης και εκπαίδευσης του προσωπικού σε ζητήματα φυσικής ασφαλείας	**ΧΑΜΗΛΟ**	Low	Πρέπει να υπάρχει σχέδιο για την ενημέρωση και εκπαίδευση του προσωπικού σε ζητήματα φυσικής ασφαλείας.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
κτήριο 1	3	3	3	**3**	**Μη έγκαιρη αποκατάσταση πληροφοριακών συστημάτων**	**ΜΕΤΡΙΟ**	Έλλειψη σχεδίου Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan)	**ΜΕΤΡΙΟ**	Medium	Πρέπει να διατηρείται Σχέδιο Ανάκαμψης από Καταστροφή (DRP Disaster Recovery Plan).	ΜΕΤΡΙΑΣΜΟΣ	ΑΜΕΣΑ	**ΧΑΜΗΛΟ**
κτήριο 1	3	3	3	**3**		**ΜΕΤΡΙΟ**	Έλλειψη εφεδρικού υπολογιστικού κέντρου ή	**ΜΕΤΡΙΟ**	Medium	Θα πρέπει να υπάρχει εφεδρικό υπολογιστικό κέντρο ή	ΜΕΤΑΦΟΡΑ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6	**ΜΕΤΡΙΟ**

							σύμβασης με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών			σύμβαση με εξωτερικό συνεργάτη για παροχή παρόμοιων υπηρεσιών.		ΜΗΝΕΣ	
κτήριο 1	3	3	3	**3**		**ΜΕΤΡΙΟ**	Τα συστήματα που περιλαμβάνονται στο Σχέδιο Ανάκαμψης από Καταστροφή δεν καλύπτουν πλήρως τα κρίσιμα πληροφοριακά συστήματα, όπως προκύπτουν από από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας	**ΜΕΤΡΙΟ**	Medium	Το Σχέδιο Ανάκαμψης από Καταστροφή πρέπει να περιλαμβάνει όλα τα κρίσιμα πληροφοριακά συστήματα του οργανισμού, όπως αυτά προκύπτουν από την ανάλυση επιπτώσεων και την ανάλυση επικινδυνότητας.	ΜΕΤΡΙΑΣΜΟΣ	ΑΜΕΣΑ	**ΧΑΜΗΛΟ**
κτήριο 1	3	3	3	**3**		**ΜΕΤΡΙΟ**	Το Σχέδιο Ανάκαμψης από Καταστροφή δεν δοκιμάζεται και δεν ανανεώνεται σε τακτά χρονικά διαστήματα	**ΜΕΤΡΙΟ**	Medium	Το Σχέδιο Ανάκαμψης από Καταστροφή θα πρέπει να δοκιμάζεται και να ανανεώνεται συχνά, ώστε να καλύπτει τις πιθανές μεταβολές στις υποδομές του οργανισμού.	ΜΕΤΡΙΑΣΜΟΣ	ΑΜΕΣΑ	**ΧΑΜΗΛΟ**

κτήριο 1	3	3	3	**3**		**ΜΕΤΡΙΟ**	Δεν είναι διαθέσιμη σε όλο το προσωπικό, λίστα με χρήσιμα τηλέφωνα επικοινωνίας για περίπτωση καταστροφής	**ΜΕΤΡΙΟ**	Medium	Θα πρέπει να είναι διαθέσιμη σε όλο το προσωπικό, λίστα με χρήσιμα τηλέφωνα επικοινωνίας για περίπτωση καταστροφής.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΜΕΤΡΙΟ**
κτήριο 1	3	3	3	**3**		**ΜΕΤΡΙΟ**	Έλλειψη ελέγχου φυσικής πρόσβασης στο εναλλακτικό κέντρο λειτουργίας	**ΜΕΤΡΙΟ**	Medium	Η φυσική πρόσβαση στο εναλλακτικό κέντρο λειτουργίας θα πρέπει να ελέγχεται σύμφωνα με καταγεγραμμένη διαδικασία.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΜΕΤΡΙΟ**
κτήριο 1	3	3	3	3	**Πυρκαγιά**	**ΧΑΜΗΛΟ**	Ακαταλληλότητα υλικών κατασκευής (π.χ. μη πυράντοχες πόρτες, πάτωμα, ξύλινη επικάλυψη στον τοίχο κλπ.)	**ΜΕΤΡΙΟ**	Medium	Οι χώροι που φυλοξενούν κρίσιμο εξοπλισμό θα πρέπει να είναι κατασκευασμένοι με πυράντοχα υλικά.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΜΕΤΡΙΟ**
κτήριο 1	3	3	3	3		**ΧΑΜΗΛΟ**	Έλλειψη κατάλληλων μέσων πυρόσβεσης	**ΜΕΤΡΙΟ**	Medium	Θα πρέπει να υπάρχουν εγκατεστημένα κατάλληλα μέσα πυρόσβεσης στις εγκαταστάσεις που φιλοξενούν κρίσιμο εξοπλισμό.	ΜΕΤΡΙΑΣΜΟΣ	ΑΜΕΣΑ	**ΧΑΜΗΛΟ**

κτήριο 1	3	3	3	3		**ΧΑΜΗΛΟ**	Έλλειψη κατάλληλων μηχανισμών ανίχνευσης φωτιάς	**ΜΕΤΡΙΟ**	Medium	Θα πρέπει να είναι εγκατεστημένος μηχανισμός ανίχνευσης φωτιάς/καπνού, στις εγκαταστάσεις που φιλοξενούν κρίσιμο εξοπλισμό	ΜΕΤΡΙΑΣΜΟΣ	ΑΜΕΣΑ	**ΧΑΜΗΛΟ**
κτήριο 1	3	3	3	3		**ΧΑΜΗΛΟ**	Ύπαρξη εύφλεκτων υλικών και ελλιπής καθαριότητα	**ΜΕΤΡΙΟ**	Medium	Δεν επιτρέπεται η αποθήκευση εύφλεκτων υλικών σε χώρους όπου φυλάσσεται κρίσιμος εξοπλισμός. Ο καθαρισμός αυτώντων χώρων θα πρέπει να γίνεται σε τακτά χρονικά διαστήματα.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΜΕΤΡΙΟ**
κτήριο 1	3	3	3	3		**ΧΑΜΗΛΟ**	Ανεπαρκής συντήρηση πυροσβεστικών μέσων	**ΜΕΤΡΙΟ**	Medium	Θα πρέπει να πραγματοποιείται περιοδίκη συντήρηση των πυροσβεστικών μέσων.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΜΕΤΡΙΟ**
κτήριο 1	3	3	3	3		**ΧΑΜΗΛΟ**	Απουσία πλάνου εκκένωσης	**ΜΕΤΡΙΟ**	Medium	Θα πρέπει να διατηρείται πλάνο εκκένωσης των εγκαταστάσεων σε περίπτωση έκτακτης	ΜΕΤΡΙΑΣΜΟΣ	ΑΜΕΣΑ	**ΧΑΜΗΛΟ**

										ανάγκης. Στους χώρους εργασίας θα πρέπει να υπάρχει κατάλληλη σήμανση ενδείξεων εκκένωσης.			
κτήριο 1	3	3	3	3		**ΧΑΜΗΛΟ**	Ελλειπής εκπαίδευση προσωπικού σε ζητήματα πυρόσβεσης και πυροπροστασίας	**ΜΕΤΡΙΟ**	Medium	Θα πρέπει να πραγματοποιείται τακτική εκπαίδευση / ενημέρωση του προσωπικού σε ζητημάτα πυρόσβεσης και πυροπροστασίας.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΜΕΤΡΙΟ**
κτήριο 1	3	3	3	3	**Σεισμός**	**ΧΑΜΗΛΟ**	Ακατάλληλες κτιριακές υποδομές	**ΧΑΜΗΛΟ**	Low	Οι εγκαταστάσεις θα πρέπει να πληρούν τις αντισεισμηκές προδιαγραφές.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
κτήριο 1	3	3	3	3		**ΧΑΜΗΛΟ**	Απουσία πλάνου εκκένωσης	**ΧΑΜΗΛΟ**	Low	Θα πρέπει να διατηρείται πλάνο εκκένωσης των εγκαταστάσεων σε περίπτωση έκτακτης ανάγκης. Στους χώρους εργασίας θα πρέπει να υπάρχει κατάλληλη σήμανση ενδείξεων εκκένωσης.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**

κτήριο 1	2	2	2	**2**	**Δολιοφθορά (Sabotage)**	**ΧΑΜΗΛΟ**	Έλλειψη πολιτικών και διαδικασιών (φυσικής) διαχείρισης πρόσβασης	**ΧΑΜΗΛΟ**	Low	Θα πρέπει να υπάρχουν καταγεγραμμένες πολιτικές και διαδικασίες για την διαχείριση πρόσβασης του προσωπικού και τρίτων στις εγκαταστάσεις οπου φιλοξενούνται κρίσιμες υποδομές πληροφοριακών συστημάτων.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
κτήριο 1	1	1	1	**1**		**ΧΑΜΗΛΟ**	Οι κτιριακές υποδομές δεν παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack)	**ΧΑΜΗΛΟ**	Low	Οι κτιριακές υποδομές θα πρέπει να παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (forced attack).	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
κτήριο 1	2	2	2	**2**		**ΧΑΜΗΛΟ**	Οι πόρτες δεν είναι ανθεκτικές σε επίθεση / δεν έχουν θωράκιση	**ΧΑΜΗΛΟ**	Low	Θα πρέπει στους χώρους που φιλοξενούνται κρίσιμα συστήματα, οι πόρτες είναι ανθεκτικές σε επίθεση.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**
κτήριο 1	2	2	2	**2**		**ΧΑΜΗΛΟ**	Ανεπαρκής παρακολούθηση των	**ΧΑΜΗΛΟ**	Low	Θα πρέπει να υπάρχουν διαδικασίες ή/και μηχανισμοί	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6	**ΧΑΜΗΛΟ**

							εγκαταστάσεων του οργανισμού			παρακολούθησης της πρόσβασης, στις εγκαταστάσεις οπου φιλοξενούνται κρίσιμα συστήματα.		ΜΗΝΕΣ	
κτήριο 1	3	3	3	**3**		**ΧΑΜΗΛΟ**	Στους χώρους όπου υπάρχει κρίσιμος εξοπλισμος επιτρέπεται η πρόσβαση στο κοινό	**ΧΑΜΗΛΟ**	Low	Θα πρέπει να απαγορεύεται η πρόσβαση στο κοινό, σε χώρους με κρίσιμο εξοπλισμό.	ΑΠΟΔΟΧΗ	ΤΟΥΣ ΕΠΟΜΕΝΟΥΣ 6 ΜΗΝΕΣ	**ΧΑΜΗΛΟ**

7 ΚΕΦΑΛΑΙΟ 7: Συμπεράσματα

Ο ρόλος και η λειτουργία των δραστηριοτήτων αποτίμησης κινδύνου και ο τρόπος με τον οποίο εντάσσονται στις πρακτικές διαχείρισης κινδύνου απαιτεί λεπτομερή διευκρίνιση. Η αποτίμηση του κινδύνου είναι πάντοτε μια αξιολόγηση σε βάθος χρόνου. Έχει ελάχιστη σχέση με την πραγματική διαχείριση κινδύνου. Η διαχείριση κινδύνου είναι σταθερή. Ενώ οι περιοδικές αξιολογήσεις είναι απαραίτητες προκειμένου ένας οργανισμός να κατανοήσει πώς να κάνει ευρείες προσαρμογές, η αληθινή διαχείριση κινδύνου ενημερώνεται καλύτερα μέσω των μεθοδολογιών μοντελοποίησης απειλών που παρουσιάζονται σε αυτό το έγγραφο. Εάν η διαχείριση κινδύνου είναι η συνεχής αξιολόγηση της επίπτωσης και της πιθανότητας εμφάνισης τυχόν ανεπιθύμητων συνθηκών (π.χ. απειλής), τότε τα υψηλής ποιότητας στοιχεία ανάλυσης απειλών και οι τρέχουσες πληροφορίες απειλών είναι τα πιο ακριβή στοιχεία δεδομένων για την καθοδήγηση των συζητήσεων και των αποφάσεων της διαδικασίας αποτίμησης του κινδύνου. Η πρόκληση - όπως ήταν πάντα στην ασφάλεια του κυβερνοχώρου / των πληροφοριών - είναι να αρθρωθούν και να αξιολογηθούν οι μεταβλητές της πιθανότητας και των επιπτώσεων με επαναλαμβανόμενο και αξιόπιστο τρόπο για την αποτελεσματική διαχείριση και μείωση του κινδύνου.

Είναι πιο αποτελεσματικό να χρησιμοποιούμε τα τεχνικά στοιχεία της μοντελοποίησης απειλών και τις πληροφορίες για την απειλή προκειμένου να λάβουμε ενημερωμένες αποφάσεις για τη διαχείριση του κινδύνου. Η ανάλυση των απειλών παρέχει εγγενώς στους υπεύθυνους λήψης αποφάσεων τα απαραίτητα σημεία δεδομένων, την ιστορική ανάλυση και τις πιθανές αξιολογήσεις των επιπτώσεων. Ένα κοινό πρόβλημα στην ασφάλεια του κυβερνοχώρου / των πληροφοριών είναι η νοοτροπία « must prevent », δηλαδή η λογική ότι όλες οι επιθέσεις πρέπει να αποτρέπονται. Αυτή η περιορισμένη άποψη δεν λαμβάνει υπόψη την αποζημίωση των ελέγχων και παραβλέπει την έννοια της προστασίας από τα αντίμετρα (βλ. ενότητα 6.4). Οι αξιόπιστες αρχιτεκτονικές και οι αντισταθμιστικοί έλεγχοι επιτρέπουν τη διαχείριση του κινδύνου και τον μετριασμό του κινδύνου.

Πολύ σημαντική έννοια στη διαδικασία αποτίμησης του κινδύνου είναι και η έννοια της αποδοχής του κινδύνου. Η επιχειρηματική δραστηριότητα περιλαμβάνει και την αποδοχή κινδύνου - από το μικρότερο γραφείο μέχρι και τους μεγαλύτερους οργανισμούς. Ο κυβερνητικός κίνδυνος είναι μια άλλη πτυχή που οι ειδικοί ασφάλειας, οι διευθυντές και τα στελέχη πρέπει να διαχειριστούν. Τα κριτήρια αποδοχής κινδύνου και διαχείρισης κινδύνου πρέπει να καθορίζονται ανά εκάστοτε σενάριο και να μεταβάλλονται κατάλληλα καθώς οι στόχοι, τα αγαθά, οι απειλές και οι μεταβλητές κινδύνου διαφέρουν ανάλογα με το χρόνο. Οι εξουσιοδοτημένοι υπεύθυνοι λήψης αποφάσεων πρέπει να διαθέτουν τις καλύτερες διαθέσιμες πληροφορίες για να λαμβάνουν αποφάσεις σχετικά με την αποδοχή και τη διαχείριση των κινδύνων. Από την άποψη της ασφάλειας των πληροφοριών, οι πιο σχετικές και επίκαιρες πληροφορίες παράγονται από το συνδυασμό των μεθοδολογιών μοντελοποίησης απειλών (π.χ. STRIDE) και των μεθοδολογιών αποτίμησης κινδύνων (π.χ. ISO 27005), όπως περιγράφονται στο παρόν έγγραφο.

Έτσι, με τη δημιουργία πλήρων μοντέλων απειλών όπως αυτά προκύπτουν από τα διαγράμματα ροής δεδομένων, καθώς και με την αποτίμηση του κινδύνου των ανιχνευόμενων απειλών σε αυτά τα μοντέλα, μπορεί κανείς να καθορίσει τις καλύτερες απαιτήσεις ασφαλείας για ένα πληροφοριακό σύστημα αλλά και για ολόκληρο τον οργανισμό.

Βιβλιογραφία

[1] **Δημήτρης Γκρίτζαλης**, *Αυτονομία και Πολιτική Ανυπακοή στον Κυβερνοχώρο*, Παπασωτηρίου, Αθήνα 2004

[2] **ISO/IEC 27001**, *Information Technology-Security Techniques-Information Security management systems*, First edition, Switzerland 2005

[3] *Παρακολούθηση και επιτυχής πιστοποίηση στο **σεμινάριο ISO 27001: 2013**,* 08/01-12/01/2019 στο Πανεπιστήμιο Πειραιά

[4] Εργασίες ατομικές και ομαδικές στο μάθημα «Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων» στο πλαίσιο του ΠΜΣ Προηγμένα Συστήματα Πληροφορικής, 2016-2017

[5] **ENISA**, *Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)*, Deliverable 2 Final version 1.0, 30/03/2006

[6] **Οικονομικό Πανεπιστήμιο Αθηνών**, Διάλεξη μαθήματος Ασφάλειας : *Διαχείριση Επικινδυνότητας Πληροφοριακών Συστημάτων & Κρίσιμων Υποδομών*, 2013

[7] **Πανεπιστήμιο Πειραιά**, Διάλεξη μαθήματος Διοίκησης Ασφάλειας: *Ανάλυση και Διαχείριση Επικινδυνότητας,* 2017

[8] **Carnegie Mellon Software Engineering Institute**, *Introduction to the OCTAVE® Approach,* Christopher Alberts, Audree Dorofee, James Stevens, Carol Woody, August 2003

[9] ***ISO/IEC 27005,** Information Technology-Security Techniques-Information Security risk management*, Third edition, 2018

[10] **ISO 28001: 2007,** *Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance,* 2007

[11] **CYSM,** *Risk Management Methodology,* http://www.cysm.eu/index.php/en/

[12] **ENISA,** *Threat Taxonomy A tool for structuring threat information,* Initial Version 1.0, January 2016

[13] **WASC- Web Application Security Consortium,** *Threat Classification,* Version 2.00, 01/01/2010

[14] **BSI,** *IT Grundschutz-Catalogues,* Version 14, 2014

[15] **FORWARD Consortium**, *Whitebook: Managing Emerging Threats in ICT Infrastructures*, Deliverable D3.1, 17/01/2010

[16] **Jelena Mirkovic-Peter Reiher,** *A Taxonomy of DDoS attack and DDoS defence mechanisms*, April 2004

[17] **NIST,** *Guide for conducting Risk Assessment,* Computer Security Division, September 2012

[18] **Microsoft,** *STRIDE Threat Model,* https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

[19] **OWASP,** *Taxonomy of web application vulnerabilities,* 2017

[20] **SANS,** *Evaluation of Comprehensive Taxonomies for Information Technology Threats*, March 2018

[21] **Adam Shostack,** *Threat Modeling-Designing for Security*, Wiley, 2014

[22] **Lorenz Verheyden,** *Effectiveness of Threat Modeling Tools*, University of Gent, 2018

[23] **Agarwa**l, A.*VAST Methodology: Visual, Agile, and Simple Threat Modeling,* Various Interviews. Prescott Valley: Transformational Opportunities,2016

[24] **Continuum Security. Vries**, *Threat Modeling and SDLC Security tools,* March 25, 2018, https://www.continuumsecurity.net/

[25] **GDPR EU,** *WAT IS GDPR*. Retrieved February 28, 2018, https://gdpr-eu.be/wat-is-gdpr/

[26] **Hernan, S., Lambert, S., & Ostwald,** *Uncover Security Design Flaws using The STRIDE Approach*, March 25, 2018, https://msdn.microsoft.com/en-gb/msdnmag/issues/06/11/ThreatModeling/default.aspx

[27] **Möckel, C., & Abdallah**, *Threat modeling approaches and tools for securing architectural designs of an e-banking application,*2010, 6th International Conference on Information Assurance and Security, IAS 2010 (pp. 149–154), https://doi.org/10.1109/ISIAS.2010.5604049

[28] **Dr. Theodoros Ntouskas,** *Application Threat Modeling – Indicative Template,* University of Piraeus

[29] **Steven Burns,** *Threat Modeling: A Process To Ensure Application Security,* SANS Institute 2005, http://www.sans.org/reading-room/whitepapers/securecode/threat-modeling-process-ensure-application-security-1646

[30] **Frank Swiderski, *Window Snyder***, *Threat Modeling*, 2004, Microsoft Press

[31] **Jan Steffan, Markus Schumaker,** *Collaborative Attack Modeling***,** 2002, http://www.ito.tu-darmstadt.de/publs/pdf/sac2002.pdf

[32] Dana Epp's Weblog, *Why Threat Modeling Matters*, http://silverstr.ufies.org/blog/archives/000700.html

[33] **ISO/IEC 27005,** *Risk Assessment template-example,* Πανεπιστήμιο Πειραιά, Διάλεξη μαθήματος Διοίκησης Ασφάλειας: *Ανάλυση και Διαχείριση Επικινδυνότητας,* 2017

[34] **Sathya Prakash Kadhirvelan, Andrew Söderberg-Rivkin,** *Threat Modelling and Risk Assessment Within Vehicular Systems*, Chalmers University of Technology, August 2014

[35] **Myagmar, Suvda, Adam J. Lee, and William Yurcik.**, *Threat modeling as a basis for security requirements*, Symposium on requirements engineering for information security (SREIS), 2005

[36] **Michael Muckin, Scott C. Fitch, Lockheed Martin Corporation,** *A Threat-Driven Approach to Cyber Security*

Παράρτημα 1

Methodology	Ontology (multi dimentional)	Sector oriented	Ranking threats - Performance measurement in problem solving	Simple top level taxonomy	Machine readable	Mutually exclusive categories	Size of semantic vocabulary	Hierarchical	Contains physical threats
Forward-whitebook	No	No	No	Yes	No	Yes	Medium	Yes	Yes
Enisa	No	No	No	Yes	Yes	Yes	Large	Yes	Yes
Wasc	No	Yes - Web Sites	No	No	No	Yes	Medium	No	No
ISO 28001: 2007	Yes	Yes - Supply Chain	No	Yes	No	No	Medium	No	Yes
IT Grundsutz	No	No	No	Yes	No	No	Medium	No	Yes
CYSM	Yes	Yes - Port Security	No	Yes	No	Yes	Large	Yes	Yes
Taxonomy of DDoS Attack and DDoS Defense Mechanisms Jelena Mircovic	Yes	Yes - DDoS Attacks	No	No	No	No	Medium	No	No
Nist Guide for conducting Risk Assesment	Yes	No	Yes	Yes	No	No	Medium	No	Yes
Ecsirt.net Incident Classification	No	No	No	Yes	No	Yes	Medium	Yes	No
OWASP Threat Categories	No	No	Yes	Yes	No	Yes	Large	Yes	No
Stride Threat Model	No	No	No	Yes	No	Yes	Small	No	No
HP Tipping Point Event Taxonomy V 2.2	No	Yes - SMS Web Services	No	Yes	No	Yes	Medium	Yes	No
Threat Taxonomy for Cloud Of Things	No	Yes - Cloud Services	No	Yes	No	Yes	Medium	Yes	No
A Multidimension Taxonomy of Insider Threats in Cloud Computing	Yes	Yes - Cloud Services	No	Yes	No	No	Small	Yes	No
A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks	Yes	Yes - Social Engineering	No	Yes	No	No	Medium	No	No

VoIP Security and Privacy Threat Taxonomy	No	Yes - VoIP	No	Yes	No	Yes	Medium	Yes	No
Cssa taxonomies	No	Yes - MISP Database	No	Yes	Yes	Yes	Small	No	No
Csirt Incident Classification	Yes	No	Yes	Yes	Yes	Yes	Small	No	No
Europol Incident Class	Yes	Yes - MISP Database	No	Yes	Yes	Yes	Medium	Yes	No
Sans Institute Taxonomy	No	Yes - Viruses	No	Yes	No	Yes	Medium	Yes	No

Σχήμα 62: Σύγκριση Ταξονομιών

Παράρτημα 2

Στο παράρτημα αυτό παρουσιάζονται όλες οι κλίμακες του προτύπου ISO 27005 που χρησιμοποιήθηκαν για την αποτίμηση του κινδύνου της εφαρμογής uCMDB:

Κλίμακα Αποτίμησης Επιπτώσεων Ασφάλειας

ΒΑΘΜΟΣ ΕΠΙΠΤΩΣΗΣ	Περιγραφή
0	VERY LOW (VL)
1	LOW (L)
2	MEDIUM (M)
3	HIGH (H)
4	VERY HIGH (VH)

Κλίμακα Αποτίμησης Απειλών

Επίπεδο Απειλής	Βαθμός Απειλής	Περιγραφή
LOW (L)	0	αναμένεται να συμβούν το πολύ μέχρι μία φορά κάθε 10 χρόνια
MEDIUM (M)	1	αναμένεται να συμβούν κατά μέσο όρο μία φορά τα 3 χρόνια.
HIGH (H)	2	αναμένεται να συμβούν κατά μέσο όρο μία φορά το χρόνο

Κλίμακα Αποτίμησης Αδυναμιών

Επίπεδο Αδυναμίας	Βαθμός Αδυναμίας	Περιγραφή
LOW (L)	0	Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι < 33%
MEDIUM (M)	1	Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι 33% - 66%
HIGH (H)	2	Η πιθανότητα να συμβεί το χειρότερο σενάριο είναι > 66%

Κλίμακα Επικινδυνότητας	
Risk Level	**Risk Value**
Low	0 - 2
Medium	3 - 5
High	6 - 8

Likelihood Matrix									
Likelihood of Threat	Low			Medium			High		
	0	0	0	1	1	1	2	2	2
Vulnerability Level	L	M	H	L	M	H	L	M	H
	0	1	2	0	1	2	0	1	2
Likelihood Value of an incident scenario	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**

	Risk Scale Matrix									
	Likelihood of Threat –Threat Level	**Low**			**Medium**			**High**		
		0	**0**	**0**	**1**	**1**	**1**	**2**	**2**	**2**
	Vulnerability Level	L	M	H	L	M	H	L	M	H
		0	**1**	**2**	**0**	**1**	**2**	**0**	**1**	**2**
	Likelihood Value of an incident scenario	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**
Asset Value	**0**	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Likelihood Level	Likelihood Value
Very Low (Very Unlikely)	0
Low (Unlikely)	1
Medium (Possible)	2
High (Likely)	3
Very High (Frequent)	4

Risk Scale Matrix						
Likelihood Value of an incident scenario		0	1	2	3	4
Likelihood Level		Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Very Low Business Impact	0	0	1	2	3	4
Low Business Impact	1	1	2	3	4	5
Medium Business Impact	2	2	3	4	5	6
High Business Impact	3	3	4	5	6	7
Very High Business Impact	4	4	5	6	7	8

Risk Level Evaluation Matrix						
Likelihood Value of an incident scenario		0	1	2	3	4
Likelihood Level		Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Very Low Business Impact	0	Low	Low	Low	Medium	Medium
Low Business Impact	1	Low	Low	Medium	Medium	Medium

Medium Business Impact	**2**	Low	Medium	Medium	Medium	High
High Business Impact	**3**	Medium	Medium	Medium	High	High
Very High Business Impact	**4**	Medium	Mium	High	High	High