Πανεπιστήμιο Πειραιώς

Τμήμα Πληροφορικής

Διδακτορική Διατριβή

Μέρμηγκας Δημήτρης

«Ποσοτικοποίηση της ασφάλειας συστημάτων πληροφορικής με τη χρήση στοχαστικών μεθόδων»

Πειραιάς, Σεπτέμβριος 2012

Συμβουλευτική επιτροπή

Επιβλέπων:

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη:

Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Θεμιστοκλής Παναγιωτόπουλος
Καθηγητής Πανεπιστημίου Πειραιώς

Πανεπιστήμιο Πειραιώς
Τμήμα Πληροφορικής

Διατριβή

για την απόκτηση Διδακτορικού Διπλώματος του Τμήματος Πληροφορικής

«*Ποσοτικοποίηση ασφάλειας συστημάτων πληροφορικής με τη χρήση στοχαστικών μεθόδων*»

Εξεταστική επιτροπή:

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Θεμιστοκλής Παναγιωτόπουλος
Καθηγητής Πανεπιστημίου Πειραιώς

Βασίλειος Χρυσικόπουλος
Καθηγητής Ιόνιου Πανεπιστημίου

Θεόδωρος Αρτίκης
Καθηγητής Πανεπιστημίου Πειραιώς

Γρηγόριος Χονδροκούκης
Καθηγητής Πανεπιστημίου Πειραιώς

Παναγιώτης Κοζανικολάου
Λέκτορας Πανεπιστημίου Πειραιώς

Πνευματικά δικαιώματα

Δημήτριος Χ. Μέρμηγκας

Μηχανικός λογισμικού Τ. Ε. Ι Αθηνών, MBA Leicester University

Αφιέρωση

Αφιερώνω την παρούσα διατριβή στους γονείς μου, που με στήριξαν σε κάθε βήμα της ζωής μου. Όχι μόνο με προέτρεψαν να σπουδάσω και να ακολουθήσω αυτό που μου άρεσε, αλλά μου παρείχαν κάθε είδους βοήθεια για να το πετύχω. Δυστυχώς, δεν πρόλαβα να δώσω και στους δύο τη χαρά να με δουν να καταφέρνω όλα όσα προσπάθησα, αλλά τους ευχαριστώ, τους αγαπώ και τους δίνω την υπόσχεση ότι θα θυμάμαι όλα όσα πέρασα τα τελευταία χρόνια και ότι θα προσπαθήσω να γίνω ένας άνθρωπος για τον οποίο θα είναι περήφανοι.

Ευχαριστίες

Η παρούσα διατριβή αποτελεί το αποτέλεσμα ερευνητικής εργασίας που πραγματοποιήθηκε τα τελευταία χρόνια στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς. Θα ήθελα να εκφράσω τις ευχαριστίες μου προς το Τμήμα Πληροφορικής, για την μεγάλη τιμή που μου έκανε, με το να με δεχθεί ανάμεσα στους υποψήφιους διδάκτορές του, καθώς και για την ευκαιρία που μου έδωσε να συνεργαστώ με καθηγητές υψηλού κύρους και αναγνώρισης.

Θέλω να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, κ. Νικόλαο Αλεξανδρή, για την επιστημονική του καθοδήγηση, την ανθρώπινη συμπεριφορά του και την απεριόριστη στήριξή του, σε όλη τη διάρκεια της δύσκολης, για εμένα, ερευνητικής προσπάθειας. Χωρίς αυτόν, δεν θα μπορούσα να ολοκληρώσω την προσπάθειά μου, και θα τον ευγνωμονώ για πάντα.

Θα ήθελα να ευχαριστήσω θερμά τους καθηγητές κ. Θεμιστοκλή Παναγιωτόπουλο και κ. Χρήστο Δουληγέρη, που με τίμησαν ως μέλη της Τριμελούς Επιτροπής Επίβλεψής μου. Οι οδηγίες τους, συνέβαλαν στην ολοκλήρωση αυτής της ερευνητικής προσπάθειας.

Επίσης, θα επιθυμούσα να ευχαριστήσω θερμά, τους καθηγητές κ.κ. Βασίλειο Χρυσικόπουλο, Θεόδωρο Αρτίκη, Γρηγόριο Χονδροκούκη καθώς και τον Λέκτορα κ. Παναγιώτη Κοζανικολάου, που μου έκαναν την τιμή να είναι μέλη της Εξεταστικής μου Επιτροπής, καθώς και για τις σημαντικές παρατηρήσεις που έκαναν για την έρευνά μου.

Ευχαριστώ, πολύ όλους τους φίλους μου στο Πανεπιστήμιο και ειδικότερα τον Δρ. Κωνσταντίνο Πατσάκη και τον υποψήφιο διδάκτορα Σωτήρη Πηρούνια, για τις ατελείωτες ώρες συζητήσεων και ανταλλαγής απόψεων στα διάφορα πεδία της παρούσας έρευνας. Η συμβολή τους ήταν ανεκτίμητη και χαίρομαι που εκτός από την ερευνητική εργασία, απέκτησα δύο πολύτιμους φίλους.

Δεν θα μπορούσα να ξεχάσω να ευχαριστήσω θερμά, τη μητέρα μου και τον αδελφό μου Γιώργο, για την απεριόριστη ηθική συμπαράσταση αλλά και υπο-

μονή (!!!), που έδειξαν αυτά τα τελευταία χρόνια. Η θετική τους στάση, έκανε εφικτή την ολοκλήρωση της προσπάθειά μου, με αποτέλεσμα να βρίσκομαι σε αυτήν την ευτυχή θέση αυτή τη στιγμή.

Τέλος, θέλω να ευχαριστήσω θερμά τη σύζυγό μου, για την υπομονή που έ-δειξε, τη στήριξη που μου έδωσε, και τον καλό της λόγο, σε κάθε δύσκολη για εμένα στιγμή. Χωρίς τη δική της συμβολή δεν θα είχα επιτύχει το στόχο μου.

Δημοσιεύσεις

Σε αυτές τις δημοσιεύσεις που παρουσιάζονται παρακάτω περιλαμβάνονται εργασίες που έχουν δημοσιευτεί σε διεθνή περιοδικά μετά από πλήρη κρίση, σε διεθνή συνέδρια μετά από πλήρη κρίση. Οι εργασίες αυτές σχετίζονται με την έρευνα που διεξήχθη στο πλαίσιο της παρούσης διατριβής.

1. Σε διεθνή Περιοδικά

- Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Gregory Chondrokoukis, «The role of weighted entropy in security quantification» in International Journal of Information and Electronics Engineering (IJIEE, ISSN: 2010-3719). Αναμένεται η δημοσίευση του άρθρου τον Σεπτέμβριο του 2012.

- Nikolaos Alexandris, Evangelos Fountas, Dimitrios Mermigas, Sotirios Pirounias, «Using time patterns to verify the utilization of stochastic calculus in security quantification» in International Journal of Information and Electronics Engineering (IJIEE, ISSN: 2010-3719). Αναμένεται η δημοσίευση του άρθρου τον Σεπτέμβριο του 2012.

- Sotirios Pirounias, Dimitrios Mermigas, Constantinos Patsakis, «The relation between information security events and firm market value, empirical evidence on recent disclosures», Journal of Information Systems Research, p. 21. Η δημοσίευση έχει κατατεθεί και αναμένεται η κρίση από το περιοδικό.

2. Σε Διεθνή Συνέδρια

- Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Nikolaos Alexandris, Evangelos Fountas, «Towards a formalistic measuring of

security using stochastic calculus» in 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010), Chengdu, China, July 9-11 2010, p. 4.

- Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Gregory Chondrokoukis, «The role of weighted entropy in security quantification» in 2010 IEEE International Conference on Information Security and Artificial Intelligence (ISAI 2010), Chengdu, China, Dec. 17-19 2010, p. 4.

- Nikolaos Alexandris, Evangelos Fountas, Dimitrios Mermigas, Sotirios Pirounias, «Using time patterns to verify the utilization of stochastic calculus in security quantification» in 2010 IEEE International Conference on Information Security and Artificial (ISAI 2010), Chengdu, China, Dec. 17-19, p. 5.

- Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Gregory Chondrokoukis, «The role of weighted entropy in security quantification» in 2011 Global Congress on Science and Engineering (GCSE 2011), Dubai, Dec. 28-30 2011, p. 4.

- Nikolaos Alexandris, Evangelos Fountas, Dimitrios Mermigas, Sotirios Pirounias, «Using time patterns to verify the utilization of stochastic calculus in security quantification» in 2011 Global Congress on Science and Engineering (GCSE 2011), Dubai, Dec. 28-30 2011, p. 5.

- Dimitrios Mermigas, Sotirios Pirounias, Nikolaos Alexandris, «A probabilistic method for the quantification of corporate losses due to security breaches» in 2012 International Congress on Mathematics (MICOM), Sarajevo, Bosnia, Sep. 19-23 2012.

- Dimitrios Mermigas, Constantinos Patsakis, Sotirios Pirounias, «A formalistic quantification of information systems security with stochastic calculus» in 8th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW 2012) also sponsored by National Nuclear Security Administration Cyber Sciences Laboratory, Oak Ridge, TN, USA — 30th Oct – 1st Nov, 2012. Τα proceedings του συνεδρίου που περιέχουν την έρευνα αυτή, θα δημοσιευτούν στο ACM Digital Library.

Περιεχόμενα

Πίνακες

Εικόνες

Διαγράμματα

Συντομογραφίες

Ξένος όρος	Επεξήγηση
BPEST	Business, Political, Economic, Social, Technological
CVRF	Common Vulnerability Reporting Framework
CVSS	Common Vulnerability Scoring System
FISMA	Federal Information Security Management Act
GPRA	Government Performance Act
HIPPA	Health Insurance Portability and Accountability Act
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
NVD	National Vulnerability Database
OSVDB	Open Source Vulnerability Database
PESTLE	Political, Economic, Social, Technical, Legal, Environmental
ROI	Return On Investment
SCADA	Supervisory Control And Data Acquisition
SWOT	Strengths, Weaknesses, Opportunities, and Threats

Πίνακας 1: Συντομογραφίες

Περίληψη

Ο κόσμος γύρω μας, έχει εισέλθει σε μία εντελώς νέα εποχή, αναφορικά με τη χρήση των συστημάτων πληροφορικής. Φυσικό αποτέλεσμα αυτού, είναι η ολοένα και μεγαλύτερη εξάρτηση, από τα διάφορα συστήματα πληροφορικής των επιχειρήσεων, που συχνά βασίζουν την επιτυχία τους, στην αδιάλειπτη (24x7) λειτουργία τους. Στο πλαίσιο αυτό, η αντιμετώπιση των κινδύνων που αντιμετωπίζει μία επιχείρηση, και ειδικότερα, εκείνων των κινδύνων που μπορούν δυνητικά να επηρεάσουν τα συστήματα πληροφορικής που διαθέτει, έχει γίνει επιτακτική. Όμως για να είναι δυνατή η αντιμετώπιση των κινδύνων, πρέπει πρώτα να μπορούμε να μετρήσουμε πόσο ασφαλές είναι το σύστημα πληροφορικής που διαθέτουμε.

Η παρούσα διατριβή, προσπαθεί να προσεγγίσει αυτό το πολύπλοκο πρόβλημα, να αναγνωρίσει πιθανά χρονικά πρότυπα επανάληψης κινδύνων, και, τέλος, να προτείνει μία νέα, αντικειμενική, ακριβή και αμερόληπτη μέθοδο υπολογισμού του επιπέδου της ασφάλειας ενός συστήματος πληροφορικής. Για το σκοπό αυτό, χρησιμοποιεί στοχαστικές μεθόδους, που από τη φύση τους μπορούν να διαχειριστούν τον παράγοντα χρόνο, και μπορούν να δώσουν ένα αριθμητικό, μη αμφισβητήσιμο και αμερόληπτο αποτέλεσμα.

Abstract

The world around us has already entered in a whole new era, regarding the use of Information Systems. The consequence of that is the increasing dependence of various corporations upon Information Systems, which frequently base their success on their continuous (24x7) operation. Within this context, the mitigation of risks that a corporation faces, and, especially, those that could potentially affect the corporation's Information Systems, has become more pressing than ever. However, in order to be able to mitigate the risks, we should first be able to measure how secure our Information System is.

This thesis makes an effort to address this complicated topic, identify any possible risk repeating time pattern as well as to suggest a new, objective, accurate and unbiased method for calculating the security level of an Information System. To this end, it explores the usage of stochastic calculus, which by definition can handle the time factor and produce a solid, objective and unbiased result.

ΚΕΦΑΛΑΙΟ 1: Στόχοι και κίνητρα της έρευνας

1. Εισαγωγή

Είναι γενικά αποδεκτό, ότι ο κόσμος των επιχειρήσεων έχει αλλάξει άρδην τα τελευταία χρόνια. Ο ανταγωνισμός μεταξύ τους έχει γίνει ιδιαίτερα σκληρός και η παγκοσμιοποίηση έχει εντείνει ακόμα περισσότερο την ανάγκη διαφοροποίησης μίας επιχείρησης από μία άλλη. Στο πλαίσιο αυτό, οι επιχειρήσεις χρειάστηκαν να χαράξουν νέες στρατηγικές, οι οποίες θα τους επέτρεπαν να αυξήσουν την πελατεία τους, απευθυνόμενες - αναγκαστικά - σε μία πολύ μεγαλύτερη –παγκόσμια- αγορά, μέσω της χρήσης του κυβερνοχώρου. Ο τεράστιος όγκος των χρηστών αλλά και των πληροφοριών που διακινούνται στο διαδίκτυο, αποτέλεσαν, αποτελούν αλλά και θα αποτελούν μία διαρκή πρόκληση αλλά και κίνδυνο για τις επιχειρήσεις που υιοθέτησαν αυτή τη στρατηγική.

1.1 Ηλεκτρονική διακυβέρνηση

Στη σύγχρονη εποχή των επιχειρήσεων όλο και συχνότερα συμβαίνει το πολυτιμότερο πλεονέκτημά τους να είναι οι πληροφορίες που έχουν στην κατοχή τους και τα συστήματα πληροφορικής που τις υποστηρίζουν. Το παράδοξο όμως είναι ότι αυτό γίνεται ελάχιστα κατανοητό από τις διοικήσεις τους. Οι επιτυχημένες επιχειρήσεις αναγνωρίζουν τα οφέλη των συστημάτων πληροφορικής και τα χρησιμοποιούν για να αυξήσουν την αξία και την ανταγωνιστικότητά τους. Αυτές οι επιχειρήσεις επίσης εντοπίζουν και διαχειρίζονται τους σχετικούς κινδύνους, όπως είναι η κρίσιμη εξάρτηση πολλών επιχειρησιακών διαδικασιών από τα συστήματα πληροφορικής και η αυξανόμενη πίεση για συμμόρφωση με ρυθμιστικά πλαίσια.

Η ανάγκη για την επιβεβαίωση της αξίας των συστημάτων πληροφορικής, η διαχείριση των κινδύνων που τα αφορούν και οι αυξανόμενες απαιτήσεις για έλεγχο των πληροφοριών γίνονται κατανοητές τώρα ως βασικά στοιχεία της επιχειρηματικής διακυβέρνησης. Η αξία, ο κίνδυνος και ο έλεγχος αποτελούν τον πυρήνα της

διακυβέρνησης των συστημάτων πληροφορικής (Information Technology Governance). Η διακυβέρνηση των συστημάτων πληροφορικής είναι ευθύνη των ανώτερων στελεχών και του διοικητικού συμβουλίου, και χωρίζεται στους τομείς της διοίκησης, των οργανωτικών δομών και τέλος, των διαδικασιών που εξασφαλίζουν ότι τα συστήματα πληροφορικής στηρίζουν και επεκτείνουν τις στρατηγικές καθώς και τους στόχους του οργανισμού.

1.2 Οφέλη της ηλεκτρονικής διακυβέρνησης

Η διακυβέρνηση των συστημάτων πληροφορικής ενσωματώνει αλλά και θεσμοθετεί ορθές πρακτικές που εξασφαλίζουν ότι τα συστήματα πληροφορικής υποστηρίζουν τους επιχειρησιακούς στόχους. Η διακυβέρνησή τους επιτρέπει έτσι στην επιχείρηση να εκμεταλλευθεί πλήρως τις πληροφορίες της, ώστε να μεγιστοποιήσει τα οφέλη, να αξιοποιήσει τις ευκαιρίες και να αποκομίσει ανταγωνιστικά πλεονεκτήματα.

Προκειμένου να πραγματοποιηθούν αυτά τα αποτελέσματα απαιτείται ένα πλαίσιο για τον έλεγχο των συστημάτων πληροφορικής που να ακολουθεί ευρέως αποδεκτά πλαίσια ελέγχου για την επιχειρηματική διακυβέρνηση και τη διαχείριση κινδύνων, όπως για παράδειγμα το πλαίσιο COSO (Committee of Sponsoring Organizations of the Tread way Commission, Internal Control—Integrated Framework) [1].

Οι επιχειρήσεις πρέπει να ικανοποιήσουν τις πιστωτικές απαιτήσεις και τις απαιτήσεις ασφάλειας και ποιότητας για τα συστήματα πληροφορικής, με τον ίδιο τρόπο που αυτό συμβαίνει για όλα τα υπόλοιπα πάγια. Η διοίκηση πρέπει επίσης να βελτιστοποιήσει τη χρήση των διαθέσιμων πόρων των συστημάτων πληροφορικής, συμπεριλαμβανομένων των εφαρμογών, των πληροφοριών, της υποδομής και του ανθρώπινου δυναμικού. Για να διαχειριστεί αυτές τις ευθύνες, καθώς επίσης και για να επιτύχει τους στόχους της, η διοίκηση πρέπει να γνωρίζει την κατάσταση των συστημάτων πληροφορικής της επιχείρησης και να αποφασίσει το είδος της διακυβέρνησης και τον έλεγχο που πρέπει να παρέχει.

1.3 Αποτελεσματική διαχείριση των συστημάτων πληροφορικής

Κρίσιμης λοιπόν σημασίας για την επιβίωση και την επιτυχία μίας επιχείρησης αποτελεί η αποτελεσματική διαχείριση των πληροφοριών και των σχετικών τεχνολογιών Πληροφορικής που χρησιμοποιεί. Στην παγκόσμια κοινωνία της πληροφορίας, όπου η πληροφορία ταξιδεύει μέσω του κυβερνοχώρου χωρίς τους περιορισμούς του χρόνου, απόστασης και ταχύτητας, αυτή η κρισιμότητα γίνεται εμφανής από μία σειρά γεγονότων ή / και καταστάσεων που διέπουν τη σύγχρονη καθημερινότητά μας αλλά και αυτής των επιχειρήσεων:

- Τα τελευταία χρόνια, η εξάρτησή μας από την πληροφορία και τα συστήματα που τη διαχειρίζονται, γίνεται ολοένα και μεγαλύτερη. Όλο και περισσότερες εργασίες διεκπεραιώνονται μέσω του κυβερνοχώρου και μάλιστα αποτελεί στρατηγικό στόχο η μεγαλύτερη χρησιμοποίησή του για την ολοκλήρωση μιας σειράς διεργασιών, όπως οι συναλλαγές μας με το Δημόσιο ή τις τράπεζες.
- Με την αυξανόμενη εξάρτησή μας από τα συστήματα πληροφορικής, εμφανίστηκαν και κάποιες παρενέργειες. Έτσι τα τελευταία χρόνια παρατηρούμε μία αυξητική τάση στην ανίχνευση ευπαθειών στα συστήματα πληροφορικής. Αυτό με την σειρά του προκύπτει, από το τεράστιο εύρος απειλών, όπως για παράδειγμα κυβερνο-απάτης και κυβερνο-επιθέσεων στα διάφορα συστήματα πληροφορικής με σκοπό την αποκόμιση ευαίσθητων αλλά και απόρρητων πληροφοριών. Ένα είδος πολέμου πληροφοριών ή καλύτερα πολέμου για την απόκτηση πληροφοριών, έχει ξεσπάσει τα τελευταία χρόνια ανάμεσα σε εταιρείες με την μορφή της εταιρικής κατασκοπίας, με σκοπό την αντιγραφή ή και την ενημέρωση για τα διάφορα

προϊόντα ή υπηρεσίες που παρέχουν, αλλά ακόμα και μεταξύ κρατών με την μορφή της κατασκοπίας.

- Γίνονται ολοένα και μεγαλύτερες επενδύσεις, τόσο σε μέγεθος όσο και σε κόστος, σε συστήματα πληροφορικής. Το κόστος των επενδύσεων αναμένεται να αυξηθεί τα επόμενα χρόνια αφού η εξάρτηση των επιχειρήσεων από τα συστήματα πληροφορικής όπως προαναφέρθηκε παρουσιάζει αυξητικές τάσεις.
- Υπάρχει μεγάλη πιθανότητα αλλά και προσμονή οι νέες τεχνολογίες να αλλάξουν ριζικά τις επιχειρήσεις καθώς και τις επιχειρηματικές πρακτικές του σήμερα, δημιουργώντας νέες ευκαιρίες αλλά και μειώνοντας τα κόστη των επενδύσεων.
- Για πάρα πολλές επιχειρήσεις, η πληροφορία, αλλά και τα συστήματα πληροφορικής που τη διαχειρίζονται, αποτελούν τα πιο πολύτιμα περιουσιακά τους στοιχεία.

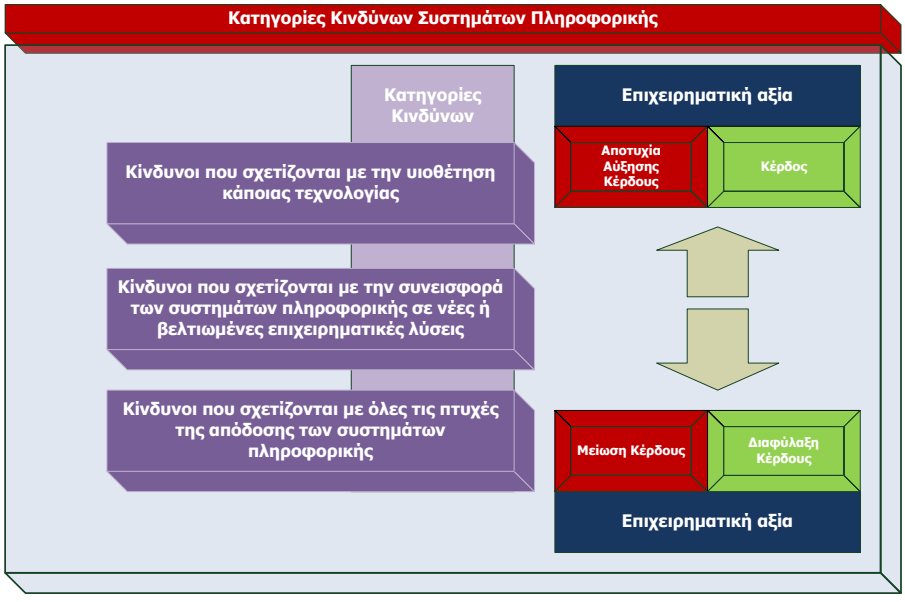
Επιπλέον, στο σημερινό ιδιαίτερα ανταγωνιστικό και συνεχώς μεταβαλλόμενο περιβάλλον των επιχειρήσεων, η διοίκηση έχει ιδιαίτερα αυξημένες απαιτήσεις όσον αφορά τις λειτουργίες των συστημάτων πληροφορικής: η διοίκηση απαιτεί αυξημένη ποιότητα, λειτουργικότητα αλλά ευκολία στη χρήση, μείωση του χρόνου παράδοσης και συνεχή βελτίωση των επιπέδων παροχής υπηρεσιών. Ενώ ταυτόχρονα, απαιτεί όλα τα προαναφερθέντα να ολοκληρωθούν με το χαμηλότερο δυνατόν κόστος.

Υπάρχουν μία σειρά από αλλαγές στα συστήματα πληροφορικής αλλά και το περιρρέον περιβάλλον λειτουργίας τους, που τονίζουν την ανάγκη για την καλύτερη διαχείριση των κινδύνων που έχουν να κάνουν με την Πληροφορική. Η εξάρτηση από την ηλεκτρονική πληροφόρηση και τα συστήματα πληροφορικής κρίνεται

απαραίτητη για την υποστήριξη κρίσιμων επιχειρηματικών διαδικασιών. Επιπλέον, το ρυθμιστικό περιβάλλον είναι η υποχρεωτική επιβολή αυστηρότερων ελέγχων στις διαθέσιμες πληροφορίες. Χαρακτηριστικό παράδειγμα είναι το ρυθμιστικό πλαίσιο των Sarbane-Oxley του 2002, όπου θεωρείται ίσως το πιο σκληρό ρυθμιστικό πλαίσιο που υπάρχει. Αυτό, με τη σειρά του, οφείλεται στις αυξημένες γνωστοποιήσεις των καταστροφών συστημάτων πληροφορικής και την αύξηση της ηλεκτρονικής απάτης.

1.4 Κίνδυνος συστημάτων πληροφορικής

Ο κίνδυνος συστημάτων πληροφορικής θεωρείται ως επιχειρηματικός κίνδυνος και ειδικότερα ως κίνδυνος που σχετίζεται με τη χρήση, την ιδιοκτησία, τη λειτουργία, τη συμμετοχή, την επιρροή και την έγκριση των συστημάτων πληροφορικής στην επιχείρηση. Αποτελείται από διάφορα γεγονότα που απορρέουν από τα συστήματα πληροφορικής και που θα μπορούσαν δυνητικά να έχουν βλαβερές επιπτώσεις στην επιχείρηση. Μπορεί να συμβεί με οποιαδήποτε συχνότητα και έκταση, και δημιουργεί προκλήσεις –μικρότερες ή μεγαλύτερες- στην επιχείρηση, για την επίτευξη του επιχειρηματικού στόχου και σκοπού. Οι κίνδυνοι συστημάτων πληροφορικής μπορούν να ταξινομηθούν σε διάφορες κατηγορίες, όπως φαίνεται στην Εικόνα 1:



Εικόνα 1: Κατηγοριοποίηση κινδύνων συστημάτων πληροφορικής

- Κίνδυνοι που σχετίζονται με τη μη υιοθέτηση κάποιας τεχνολογίας η οποία θα βελτιστοποιούσε την αποτελεσματικότητα και αποδοτικότητα των επιχειρηματικών διαδικασιών ή θα δρούσε ως καθοριστικός παράγοντας για την λήψη επιχειρηματικών πρωτοβουλιών.
- Κίνδυνοι που σχετίζονται με τη συνεισφορά των συστημάτων πληροφορικής σε νέες ή βελτιωμένες επιχειρηματικές λύσεις, συνήθως με τη μορφή νέων προγραμμάτων ή προϊόντων. Αυτό έχει άμεση επίδραση στο χαρτοφυλάκιο των επενδύσεων μίας επιχείρησης.
- Κίνδυνοι που σχετίζονται με όλες τις πτυχές της απόδοσης των συστημάτων πληροφορικής, οι οποίες μπορούν να επιφέρουν την καταστροφή ή την επιτυχία της αξίας μίας επιχείρησης.

Ως γενική παραδοχή μπορούμε να πούμε ότι οι κίνδυνοι συστημάτων πληροφορικής σε μία επιχείρηση υπάρχουν πάντα, ανεξαρτήτως αν αυτό ανιχνεύεται ή αναγνωρίζεται από αυτή.

1.5 Στόχοι της έρευνας

Η εμπειρία έχει δείξει ότι τα οφέλη από την ηλεκτρονική διακυβέρνηση είναι πολλά και σημαντικά. Όμως, η δημιουργία νέων ηλεκτρονικών διαδικασιών και η υιοθέτησή τους, υποκρύπτει και κάποιους κινδύνους, μερικοί από τους οποίους είναι εκείνοι των συστημάτων πληροφορικής. Οι κίνδυνοι από τα συστήματα πληροφορικής είναι κομμάτι του συνολικού κινδύνου που αντιμετωπίζει μία επιχείρηση. Έτσι λοιπόν, το πλαίσιο διαχείρισης κινδύνων είναι το καταλληλότερο εργαλείο για τη διαχείρισή τους από τις διοικήσεις των επιχειρήσεων. Το πλαίσιο αυτό μπορεί και πρέπει να εξειδικευτεί στη διαχείριση των κινδύνων συστημάτων πληροφορικής.

Αυτό είναι αναγκαίο γιατί πλέον η εξειδίκευση των συστημάτων πληροφορικής είναι πολύ μεγάλη και τα συστήματα έχουν γίνει πιο σύνθετα από ποτέ. Με τη σειρά του, αυτό μας οδηγεί στο να εστιάσουμε στους κινδύνους των συστημάτων πληροφορικής με τρόπο τέτοιο που να συνδυάζει τόσο τις γνώσεις μας από τη διαχείριση κινδύνων όσο και τις γνώσεις μας από τους κινδύνους συστημάτων πληροφορικής και ειδικότερα, στον τομέα της ασφάλειάς τους.

Έχοντας αναφερθεί στους κινδύνους των συστημάτων πληροφορικής και τη διαχείρισή τους, πρέπει να αναφέρουμε ότι ο σκοπός αυτής της έρευνας είναι να συμβάλει στη διεθνή βιβλιογραφία και να προτείνει ένα νέο τρόπο αποτίμησης κινδύνων συστημάτων πληροφορικής που θα μπορούσε να χρησιμοποιηθεί ως εργαλείο για την πρόβλεψη των κινδύνων των συστημάτων πληροφορικής μίας επιχείρησης.

1.6 Κίνητρα της έρευνας

Μια στρατηγική και μεγάλης σημασίας μονάδα σε μία επιχείρηση είναι αυτή της διαχείρισης κινδύνων. Υπάρχει τα τελευταία χρόνια έντονο ενδιαφέρον, τόσο από την πλευρά των επαγγελματιών του είδους όσο και από την πλευρά των ερευνητών, για τη βελτιστοποίηση των εργασιών της μονάδας αυτής. Πολλά μοντέλα διαχείρισης έχουν προταθεί και υιοθετηθεί και εκτεταμένες έρευνες έχουν γίνει σε αυτόν τον τομέα. Η έντονη λοιπόν ανάγκη αυτή, αποτέλεσε ένα ισχυρό κίνητρο για την εκπόνηση αυτής της διατριβής.

Ένα μεγάλο μέρος της διαχείρισης κινδύνων είναι αφιερωμένο στην αποτίμηση των κινδύνων. Μερικές από τις ερωτήσεις που καθημερινά καλούνται να αντιμετωπίσουν οι διοικήσεις των επιχειρήσεων είναι:

- Πόσο ασφαλές είναι ένα σύστημα πληροφορικής;
- Πρέπει να ενταχθεί στους κινδύνους συστημάτων πληροφορικής;
- Πρέπει να συμμετέχει στον συνολικό κίνδυνο που η επιχείρηση αντιμετωπίζει και ποιο θα είναι το αντίστοιχο κόστος;

Ένα λοιπόν από τα κίνητρα για τη διατριβή αυτή, είναι η βελτιστοποίηση της αποτίμησης των κινδύνων συστημάτων πληροφορικής, με την καθιέρωση ενός νέου αντικειμενικού μοντέλου που θα παρέχει τη δυνατότητα στις διοικήσεις των επιχειρήσεων να προβαίνουν σε αντικειμενικές αξιολογήσεις των κινδύνων που αντιμετωπίζουν. Με το νέο προτεινόμενο μοντέλο προσφέρεται η δυνατότητα στις επιχειρήσεις της καλύτερης διαχείρισης των πόρων της, τόσο σε επίπεδο ανθρώπινου δυναμικού όσο και σε οικονομικό επίπεδο που προέρχεται από την χρήση των συστημάτων πληροφορικής.

Είναι αδιαμφισβήτητο, ότι υπάρχει μια αυξανόμενη εξάρτηση των σύγχρονων επιχειρήσεων από τα συστήματα πληροφορικής που χρησιμοποιούν. Οι νέες τεχνολογίες που κατακλύζουν το χώρο της πληροφορικής αλλά και οι εξελίξεις στον τομέα των υλικών, παρέχουν καινούργιες ή και μεγαλύτερες ευκαιρίες στις επιχειρήσεις για να αυξήσουν τον κύκλο εργασιών τους, επεκτεινόμενες σε ολοένα και μεγαλύτερες αγορές αλλά με σημαντικά χαμηλότερο κόστος.

Ερευνητές εκτιμούν ότι μόνο στις Ηνωμένες Πολιτείες της Αμερικής ο ετήσιος μέσος όρος ζημιών από τα συστήματα πληροφορικής αγγίζει τα $15 δισεκατομμύρια δολάρια (USD), [2]. Αν σε αυτό το κόστος συνυπολογίσουμε και το κόστος από υπέρβαση προϋπολογισμών, υπερωριών και αποζημιώσεων από μηνύσεις τότε, ο μέσος όρος ζημιών από τα συστήματα πληροφορικής κυμαίνεται στο αστρονομικό ποσό μεταξύ των $60 με $70 δισεκατομμυρίων δολαρίων (USD), [3] .

Επιπλέον, το 2012 οργανισμοί και κυβερνήσεις παγκοσμίως αναμένεται να ξοδέψουν συνολικά κατά μέσο όρο πάνω από $3,75 τρισεκατομμύρια δολάρια (USD) ετησίως για επενδύσεις σε διάφορα συστήματα πληροφορικής, σύμφωνα με την εταιρεία Gartner [4], και το ποσό αυτό αναμένεται να αυξηθεί στα $4,44 τρισεκατομμύρια δολάρια (USD) το 2016. Όλα αυτά λοιπόν, αποτέλεσαν ισχυρά κίνητρα για την εκπόνηση αυτής της έρευνας, γιατί πιστεύουμε ότι με το προτεινόμενο εργαλείο αποτίμησης κινδύνων, το κόστος από τις πιθανές ζημιές είναι δυνατό να μειωθεί σημαντικά και να εξοικονομηθούν τεράστια ποσά, λόγω των καλύτερων και εστιασμένων επενδύσεων σε ασφαλέστερα συστήματα πληροφορικής.

1.7 Μεθοδολογία έρευνας

Στο πλαίσιο της έρευνας μελετήθηκε η δυνατότητα δημιουργίας ενός μοντέλου για την παρακολούθηση της συνολικής ασφάλειας μίας υπηρεσίας ή ενός σταθμού εργασίας ή ενός συστήματος πληροφορικής γενικότερα. Ο στόχος αυτού του μοντέλου θα ήταν να παρέχει τη δυνατότητα της αντικειμενικής μέτρησης της ασφάλειας του συστήματος.

Κατά τη διάρκεια της έρευνας, έγινε φανερό ότι οι κίνδυνοι που αντιμετωπίζουν τα συστήματα πληροφορικής είναι πολλοί και πολλές φορές δεν συνδέονται μεταξύ τους. Για το λόγο αυτό η έρευνα εστιάστηκε καθαρά στο τεχνικό κομμάτι των κινδύνων που αντιμετωπίζουν τα συστήματα πληροφορικής και, συγκεκριμένα, στις διάφορες μορφές ευπαθειών (vulnerabilities) που είναι δυνατό να επηρεάσουν την εύρυθμη λειτουργία τους.

Η χρήση μαθηματικών μεθοδολογιών και ειδικότερα των στοχαστικών μεθόδων ολοκλήρωσης, γνωστών ως κίνηση Brown, μας παρείχε το τεχνικό και αναγκαίο υπόβαθρο, για να εκφράσουμε το προτεινόμενο μοντέλο με τη μορφή ενός μαθηματικού τύπου. Σε αυτό, προσπαθήσαμε και ενσωματώσαμε τον τυχαίο παράγοντα της εμφάνισης μίας ευπάθειας σε ένα σύστημα, του οποίου μελετήσαμε την εξέλιξη μέσα στο χρόνο.

Δεν μελετήθηκαν άλλοι παράγοντες, όπως για παράδειγμα το ανθρώπινο προσωπικό και η συσχέτισή του με το επίπεδο ασφάλειας ενός συστήματος πληροφορικής καθώς και οι φυσικοί κίνδυνοι που είναι δυνατό να επηρεάσουν ή / και να θέσουν εκτός λειτουργίας σημαντικά τμήματα της υποδομής ασφάλειας ενός συστήματος.

Για τις ανάγκες της έρευνας χρησιμοποιήθηκαν ευρέως αναγνωρισμένες, μη αμφισβητήσιμες και αξιόπιστες –ως προς την ποιότητα της παρεχόμενης πληροφορίας- βάσεις δεδομένων. Στις βάσεις αυτές περιέχονται πληροφορίες για διάφορους κατασκευαστές λογισμικού καθώς και τις ευπάθειες που εμφανίζει το λογισμικό που έχουν κατασκευάσει. Επίσης, αναλυτική περιγραφή υπάρχει για την ημερομηνία εμφάνισης μιας ευπάθειας καθώς και την έκδοση του λογισμικού που

είναι ευάλωτο σε αυτή. Ο όγκος των παρεχόμενων πληροφοριών εκτείνεται μέχρι και 20 χρόνια πίσω.

1.8 Περίγραμμα έρευνας

Η παρούσα ερευνητική προσπάθεια έχει χωριστεί σε 7 κεφάλαια. Το πρώτο κεφάλαιο αποτελεί την εισαγωγή και την παρουσίαση του τομέα της ερευνητικής εργασίας που έχει γίνει. Στο δεύτερο κεφάλαιο παρουσιάζονται αναλυτικά οι ορισμοί των κινδύνων συστημάτων πληροφορικής και οι μεθοδολογίες αντιμετώπισής τους. Στο τρίτο κεφάλαιο γίνεται η αναφορά στο μαθηματικό υπόβαθρο που βασίστηκε η παρούσα έρευνα, δηλαδή στις στοχαστικές διαδικασίες και, συγκεκριμένα, στην κίνηση Brown, καθώς και τις ιδιότητές της. Επιπλέον, παρουσιάζεται η θεωρία της στοχαστικής ολοκλήρωσης και ειδικότερα το ολοκλήρωμα Itô, το οποίο χρησιμοποιήθηκε για να υπολογιστεί το στοχαστικό ολοκλήρωμα της προτεινόμενης μεθόδου. Στο τέταρτο κεφάλαιο, παρουσιάζονται διάφορες μελέτες και μεθοδολογίες και βέλτιστες πρακτικές, οι οποίες έχουν αναπτυχθεί από ερευνητές, κρατικές υπηρεσίες, ιδιωτικές εταιρίες και οργανισμούς, με θέμα τον τομέα της ποσοτικοποίησης της ασφάλειας των συστημάτων πληροφορικής. Στο πέμπτο κεφάλαιο της έρευνας, παρουσιάζεται αναλυτικά η προτεινόμενη μεθοδολογία καθώς και αριθμητικά παραδείγματα και μετρήσεις που έγιναν κατά τη διάρκειά της. Στο έκτο κεφάλαιο, παρουσιάζεται ένα πρότυπο πρόγραμμα υπολογισμού του επιπέδου ασφάλειας ενός προϊόντος λογισμικού ή ενός συστήματος πληροφορικής, που αναπτύχθηκε για να υποστηρίξει τη χρησιμότητα της προτεινόμενης μεθοδολογίας. Στο έβδομο κεφάλαιο, παρουσιάζονται τα συμπεράσματα της έρευνας καθώς και τομείς που πιστεύουμε πως μπορεί η παρούσα έρευνα να επεκταθεί αλλά και να χρησιμοποιηθεί. Τέλος, ακολουθεί ένα Παράρτημα, στο οποίο παρατίθεται ο πηγαίος κώδικας που χρησιμοποιήσαμε α) στο μαθηματικό πακέτο MatLab για την εξαγωγή των μετρήσεων και β) του πρότυπου προγράμματος υπολογισμού του επιπέδου ασφάλειας που αναπτύχθηκε.

ΚΕΦΑΛΑΙΟ 2: Ορισμός κινδύνων συστημάτων πληροφορικής

2. Η σημασία της ασφάλειας πληροφοριών από την πλευρά της διοίκησης

Η ασφάλεια των πληροφοριών είναι ευθύνη όλων των εργαζομένων σε μία επιχείρηση. Για να είναι όμως αποτελεσματική πρέπει να πηγάζει από τη διοίκηση της επιχείρησης. Ο τρόπος με τον οποίο επικοινωνεί η διοίκηση με τους υπαλλήλους της πρέπει να ενθαρρύνει την υλοποίηση δομών ασφαλείας και την υπακοή στις πολιτικές και τις διαδικασίες της επιχείρησης. Η προληπτική (proactive) δομή ασφάλειας είναι σημαντική στην ηλεκτρονική διακυβέρνηση και στην επιτυχή υλοποίηση των στόχων της επιχείρησης, αλλά και στην προστασία των ευαίσθητων πληροφοριών της επιχείρησης, όπως είναι τα στοιχεία πελατών - συνεργατών, τα πνευματικά δικαιώματα, τα οικονομικά δεδομένα και τέλος, τα στοιχεία πωλήσεων.

Για την επίτευξη μιας αποτελεσματικής ηλεκτρονικής διακυβέρνησης, η διοίκηση της επιχείρησης πρέπει να χρησιμοποιήσει την πολύτιμη εμπειρία της πληροφορικής [5], αλλά και της επιχείρησης στον τομέα της ασφάλειας. Η ασφάλεια των συστημάτων πληροφορικής είναι υψίστης σημασίας για την ασφαλή χρήση των τεχνολογιών στις διάφορες επιχειρηματικές διαδικασίες. Από αυτή θα προκύψουν μειώσεις στα επιμέρους κόστη [6], και αύξηση της παραγωγικότητας και των κερδών της επιχείρησης. Εν κατακλείδι, ένα καλά οργανωμένο πλαίσιο ασφάλειας μπορεί να αποτελέσει το θεμέλιο λίθο για την επίτευξη του στρατηγικού πλάνου της επιχείρησης.

Οι επιτυχημένες επιχειρήσεις, εκτός από το παράδειγμα της διοίκησης, προχωρούν στην επικοινωνία σε όλη την επιχείρηση του οράματος για τον καθορισμό της εταιρικής κουλτούρας σε θέματα ασφαλείας. Η ευθύνη για την υιοθέτηση και τη σωστή τήρηση της εταιρικής κουλτούρας ασφάλειας ανήκει στον εσωτερικό έλεγχο της επιχείρησης, ενώ η εναρμόνιση με τα ρυθμιστικά πλαίσια στους υπευθύνους στα διάφορα τμήματά της.

2.1 Η διακυβέρνηση ως διαδικασία

Πολλοί πιστεύουν ότι η διακυβέρνηση είναι καθαρά εσωτερική διαδικασία, η οποία είναι κυρίως στατική και δεν αλληλεπιδρά με το εσωτερικό ή / και εξωτερικό περιβάλλον της επιχείρησης. Είναι με άλλα λόγια, η διαδικασία κατά την οποία η διοίκηση θέτει τους στόχους της επιχείρησης και επιβλέπει την πρόοδο προς την επίτευξή τους. Το λάθος σε αυτή την πρόταση έγκειται στη λέξη «επιβλέπει». Η διακυβέρνηση απαιτεί την κατανόηση των κινήτρων και προσδοκιών των επιμέρους εμπλεκομένων στην επιχείρηση, όπως επενδυτές, συνεργάτες, κυβερνήσεις, το κοινό και φυσικά το ανθρώπινο δυναμικό της. Η επιτυχημένη διακυβέρνηση πρέπει να εξετάζει τόσο το εξωτερικό όσο και το εσωτερικό περιβάλλον στην επιχείρηση και πώς αυτά την επηρεάζουν.

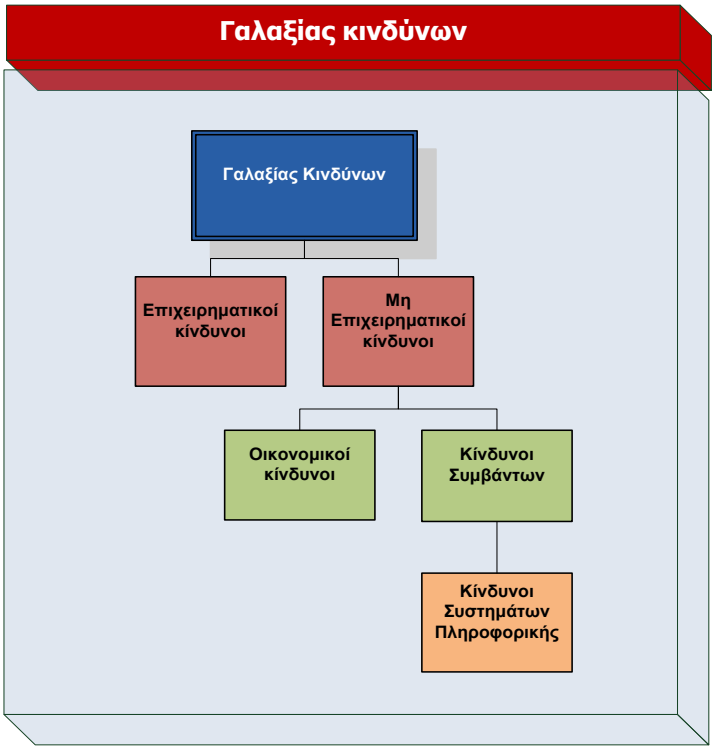
Από τη στιγμή που η διοίκηση θέσει τους στόχους της επιχείρησης πρέπει να ορίσει και τους υπευθύνους που θα επιβλέπουν την πορεία τους καθώς και να δημιουργήσει κατάλληλες διαδικασίες που να εξασφαλίζουν ότι η επιχείρηση θα καταφέρει να υλοποιήσει τους στόχους της αλληλεπιδρώντας με τα εμπλεκόμενα μέρη που προαναφέρθηκαν.

2.2 Η έννοια της διαχείρισης κινδύνων

Η έννοια της «Διαχείρισης Κινδύνων» μπορεί να ερμηνευτεί με πολλούς τρόπους ανάλογα με τον τομέα στον οποίο που αναφερόμαστε [7]. Μπορεί να σημαίνει αντιστάθμιση κινδύνων από επενδύσεις, συμβόλαια ασφάλειας, έλεγχο ποιότητας και πολλά άλλα. Το κοινό σε όλα αυτά είναι η ιδέα ότι η διαχείριση κινδύνων είναι ένα αναπόσπαστο κομμάτι της διαδικασίας λήψης αποφάσεων. Με άλλα λόγια, η διαχείριση κινδύνων υποστηρίζει τόσο την ανάληψη κινδύνου από την επιχείρηση όσο και την ανταγωνιστικότητά της. Για τα μέλη του διοικητικού συμβουλίου και τα ανώτερα στελέχη της επιχείρησης, η χρησιμότητα της διαχείρισης κινδύνων έχει γίνει πιο κατανοητή τα τελευταία χρόνια. Στο παρελθόν, η διαχείριση κινδύνων αποτελούσε μία διαδικασία χωρίς ιδιαίτερη βαρύτητα που συνήθως την αναλάμβανε το νομικό τμήμα κάθε επιχείρησης. Στις περιπτώσεις αυτές η διαχείριση

των κινδύνων ήταν κάτι που έπρεπε απλά να περιοριστεί και, εάν ήταν δυνατό, να εξαλειφθεί.

2.3 Ο Γαλαξίας των κινδύνων



Εικόνα 2: Γαλαξίας κινδύνων [8]

Στη βιβλιογραφία της διαχείρισης των κινδύνων ο όρος που έχει επικρατήσει για να περιγράψουμε όλους τους κινδύνους που αντιμετωπίζει μία επιχείρηση είναι αυτός του «Γαλαξία των κινδύνων», Εικόνα 2. Έτσι λοιπόν, ο γαλαξίας των κινδύνων σε μία επιχείρηση χωρίζεται σε δύο μεγάλες κατηγορίες, αυτή των επιχειρηματικών κινδύνων και αυτή των μη επιχειρηματικών κινδύνων.

Στην πρώτη κατηγορία σύμφωνα με την ετήσια αναφορά της Ernst & Young του 2010 [8], ανήκουν οι κίνδυνοι μη συμμόρφωσης σε ρυθμιστικά πλαίσια, κίνδυνοι αναδυόμενων αγορών, μείωσης κόστους και άλλοι κίνδυνοι. Η δεύτερη κατηγορία αναλύεται ακόμα περισσότερο σε δύο υποκατηγορίες, την κατηγορία των οικονομικών κινδύνων και την κατηγορία των κινδύνων συμβάντων.

Η κατηγορία των οικονομικών κινδύνων περιλαμβάνει κινδύνους από την μεταβολή των επιτοκίων, ισοτιμιών, μετοχικού κεφαλαίου, κινδύνους σχετικά με τα εμπορεύματα και άλλους. Η κατηγορία των κινδύνων συμβάντων περιέχει κινδύνους λειτουργίας μίας επιχείρησης, κινδύνους σχετικά με τη φήμη της επιχείρησης, κινδύνους συστημάτων πληροφορικής και άλλους κινδύνους. Η έρευνα αυτή θα επικεντρωθεί ειδικά στην τελευταία κατηγορία, δηλαδή αυτής των κινδύνων συστημάτων πληροφορικής.

2.4 Ορισμός κινδύνων

Ως ορισμό του κινδύνου μπορούμε να πούμε ότι είναι ο βαθμός της αβεβαιότητας που συνοδεύει μια συγκεκριμένη δράση. Οι ευαισθητοποιημένες διοικήσεις κάνουν ότι μπορούν για να περιορίσουν αυτόν τον κίνδυνο σε ανεκτά επίπεδα. Ωστόσο, η διοίκηση πρέπει να είναι έτοιμη να δεχθεί το ενδεχόμενο ότι αυτός ο στόχος της μπορεί να μην επιτευχθεί. Εν κατακλείδι, η ανάληψη κινδύνου αφορά στις καλά ενημερωμένες και πρόθυμες διοικήσεις που έχουν σκοπό να αποδεχθούν τον κίνδυνο.

Η θεώρηση ότι η ανάληψη κινδύνου είναι κάτι που πρέπει η επιχείρηση να αποδεχθεί και να διαχειριστεί, σηματοδοτεί την αλλαγή στάσης της διοίκησης μίας επιχείρησης, στο να χρησιμοποιήσει την ορολογία και τις τεχνικές διαχείρισης κινδύνων, σε ένα πιο ευρύ φάσμα επιχειρηματικών προβληματισμών.

2.5 Εννοιολογική θεμελίωση

Στη διεθνή βιβλιογραφία, οι μελέτες που ασχολούνται με τη διαχείριση των κινδύνων χρησιμοποιούν με μεγάλη συχνότητα τους όρους: αγαθό ή πληροφορικό στοιχείο (IT asset), απειλή (threat), ευπάθεια (vulnerability), επίπτωση (impact) και, τέλος, κίνδυνο (IT risk).

- Το ITILv3 στο [9], ορίζει ως «αγαθά ή περουσιακά στοιχεία» κάθε στοιχείο του οποίου οι απειλές και ευπάθειες μπορούν να υπολογιστούν έτσι ώστε να προβούμε στην αξιολόγηση του κινδύνου που αντιμετωπίζει.
- Η ENISA στο [10], ορίζει ως «απειλή» κάθε περίσταση ή συμβάν που είναι δυνατόν να επηρεάσουν δυσμενώς ένα περουσιακό στοιχείο μέσω της μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης των δεδομένων καθώς και της άρνησης υπηρεσίας ενός προγράμματος.
- Η «ευπάθεια» σύμφωνα με το ISO/IEC 27005:2008 [11], ορίζεται ως κάθε αδυναμία σε ένα αγαθό ή περιουσιακό στοιχείο που μπορεί να αξιοποιηθεί από μία ή περισσότερες απειλές.
- Στο ITILv3 στο [9], ορίζεται η «επίπτωση», ως το μέτρο της επίδρασης του συμβάντος ή προβλήματος ασφαλείας στην αλλαγή των επιχειρηματικών διαδικασιών.
- Σύμφωνα με την ISACA στο [12], «κίνδυνος» για τα συστήματα πληροφορικής ορίζεται ως ο επιχειρηματικός κίνδυνος που συνδέεται με τη χρήση τους, την ιδιοκτησία, τη λειτουργία, τη συμμετοχή, την επιρροή και την υιοθέτηση της πληροφορικής μέσα σε μια επιχείρηση.

2.6 Κατηγορίες κινδύνων

Έχουν γίνει πολλές συζητήσεις και διαμάχες για το θέμα της κατηγοριοποίησης των κινδύνων. Ακόμα και σήμερα δεν υπάρχει μια ευρέως αναγνωρισμένη κατηγοριοποίηση και αυτό έως ένα βαθμό είναι αναμενόμενο λόγω της μεγάλης πληθώρας επιχειρηματικών κινδύνων που παρουσιάζονται σε κάθε κλάδο επιχειρήσεων. Ένας κίνδυνος που μπορεί να θεωρηθεί ως λειτουργικός κίνδυνος για τον ένα κλάδο επιχειρήσεων αναγνωρίζεται ως οικονομικός κίνδυνος για κάποιον άλλο.

Φυσικά, υπάρχουν διάφορες κατηγορίες κινδύνου που η σύγχρονη επιχείρηση καλείται να αντιμετωπίσει. Μερικές από αυτές είναι: οι κίνδυνοι της αγοράς, οι στρατηγικοί κίνδυνοι, οι κίνδυνοι για το περιβάλλον, οι πιστωτικοί κίνδυνοι, οι λειτουργικοί κίνδυνοι και οι κίνδυνοι από μη συμμόρφωση σε κανονιστικά πλαίσια. Είναι φανερό ότι τα μέλη του διοικητικού συμβουλίου και τα ανώτερα στελέχη

της επιχείρησης χρειάζονται κάποιο τρόπο κατηγοριοποίησης αυτών των κινδύνων έτσι ώστε να μπορούν να τους διαχειριστούν.

Για να γίνει αυτό χρειάζεται να έχουμε υπόψη δύο πράγματα. Το πρώτο είναι ότι οι κίνδυνοι σχετίζονται με τους στόχους της επιχείρησης και για αυτό πρέπει να διαχωρίζονται ανάλογα με τις διαφορετικές κατηγορίες των στόχων της, για παράδειγμα στρατηγικοί κίνδυνοι και λειτουργικοί κίνδυνοι. Το δεύτερο είναι, ότι χρήσιμο θα ήταν να διαχωρίζονται οι κίνδυνοι, εκτός από την κατηγορία των στόχων της επιχείρησης που ανήκουν, και ανάλογα με τα εργαλεία που θα χρησιμοποιηθούν για την αντιμετώπισή τους. Για παράδειγμα, οι οικονομικοί κίνδυνοι παρόλο που θεωρητικά ανήκουν στην κατηγορία των λειτουργικών κινδύνων της επιχείρησης, συνετό θα ήταν να διαχειρίζονται ως κάτι το ξεχωριστό, γιατί τα εργαλεία και οι μεθοδολογίες για την αντιμετώπισή τους είναι ιδιαίτερα εξειδικευμένα και πολύ διαφορετικά από αυτά των λειτουργικών κινδύνων.

Έχοντας υπόψη όλα αυτά, μπορούμε να ξεχωρίσουμε τέσσερις μεγάλες κατηγορίες κινδύνων που συνήθως αντιμετωπίζει η διοίκηση.

2.6.1 Κίνδυνοι στρατηγικής

Οι κίνδυνοι στρατηγικής αφορούν στην μη επίτευξη των μακροπρόθεσμων στόχων της επιχείρησης. Μερικοί από τους στόχους αυτούς θα ήταν: Η επίτευξη καθορισμένου ποσοστού, για παράδειγμα 16%, ως απόδοση των επενδυμένων κεφαλαίων της επιχείρησης. Η ανάπτυξη νέων προϊόντων για την εξυπηρέτηση της αγοράς των επιχειρήσεων καθώς και ενός νέου καναλιού πωλήσεων για την εν λόγω αγορά.

2.6.2 Λειτουργικοί κίνδυνοι

Οι λειτουργικοί κίνδυνοι αφορούν στην αποδοτικότητα και την αποτελεσματικότητα της λειτουργίας της επιχείρησης, συμπεριλαμβανομένης και της κερδοφορίας και άλλων δεικτών απόδοσης. Τέτοιοι κίνδυνοι θεωρούνται οι καθυστερήσεις στην

αλυσίδα προμηθευτών ή η αποτυχία παράδοσης πρώτων υλών, οι δυσκολίες στην πρόσληψη ή η διατήρηση του ανθρώπινου δυναμικού της επιχείρησης, τα προβλήματα στα μηχανήματα της επιχείρησης, και η αύξηση των ελαττωματικών προϊόντων.

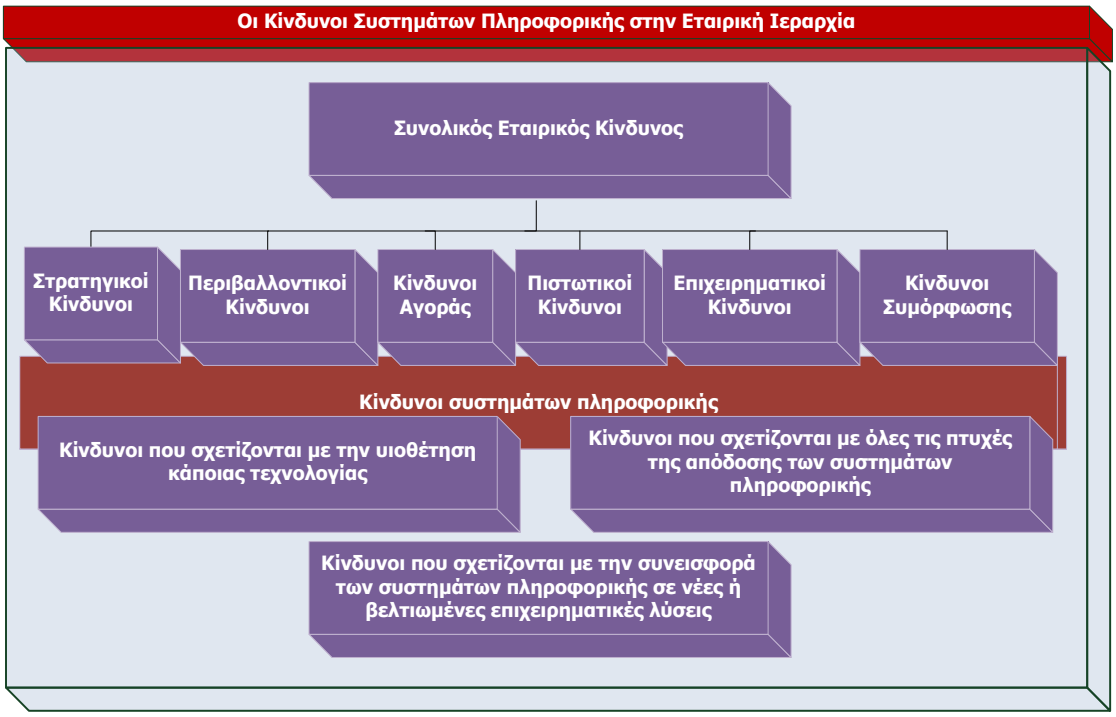
2.6.3 Οικονομικοί κίνδυνοι

Οι οικονομικοί κίνδυνοι αφορούν στις αλλαγές σε οικονομικά μεγέθη, όπως τα επιτόκια, οι τιμές μετοχών, οι ισοτιμίες συναλλάγματος, και οι μεταβολές μετοχικού κεφαλαίου. Τέλος, μεγάλο κομμάτι της κατηγορίας αυτής αφορούν οι πιστωτικοί κίνδυνοι που αντιμετωπίζει η επιχείρηση και που θα καθορίσουν σε μεγάλο βαθμό και τη στρατηγική των επενδύσεών της μεταξύ των τμημάτων της.

2.6.4 Νομικοί κίνδυνοι και κίνδυνοι μη συμμόρφωσης με ρυθμιστικά πλαίσια

Οι νομικοί κίνδυνοι και οι κίνδυνοι μη συμμόρφωσης με ρυθμιστικά πλαίσια αφορούν στη μη τήρηση κάποιων προτύπων όπως διαδικασίες ISO ή μη συμμόρφωση με ρυθμιστικά πλαίσια.

2.7 Συνολικοί κίνδυνοι μίας επιχείρησης



Εικόνα 3: Οι κίνδυνοι συστημάτων πληροφορικής στην εταιρική ιεραρχία [12]

Έχοντας περιγράψει ήδη τέσσερις κατηγορίες κινδύνων μπορούμε να ορίσουμε και τον όρο «Συνολικός Κίνδυνος μιας Επιχείρησης» - Εικόνα 3, ως τη διαδικασία που εφαρμόζεται σε ολόκληρη την επιχείρηση, η οποία ανήκει στον ευρύτερο σχεδιασμό για την επίτευξη των στόχων της, και προσπαθεί να εντοπίσει πιθανά γεγονότα που θα επηρεάζουν την επιχείρηση, τη διαχείριση των κινδύνων της εντός των καθορισμένων επιπέδων και η οποία παρέχει την εύλογη διαβεβαίωση για την επίτευξη των στόχων της.

Από τον ορισμό του «Συνολικού Κινδύνου μιας Επιχείρησης», μπορούμε να δούμε τα βασικά στοιχεία που είναι σημαντικά στη διαχείριση κινδύνων. Το διοικητικό συμβούλιο και τα διευθυντικά στελέχη, μετέχουν ενεργά στη διαχείριση κινδύνων. Οι κίνδυνοι είναι συσχετισμένοι με τους στόχους της επιχείρησης. Η διαχείριση κινδύνων αφορά σε ολόκληρη την επιχείρηση και αντικατοπτρίζει τη διάθεση της επιχείρησης για ανάληψη κινδύνων. Ο στόχος της διαχείρισης κινδύνων είναι η παροχή εύλογης διαβεβαίωσης και όχι βεβαιότητας και, τέλος, η διαχείριση κιν-

δύνων εστιάζεται κυρίως στους στόχους της επιχείρησης και όχι στις διαδικασίες της.

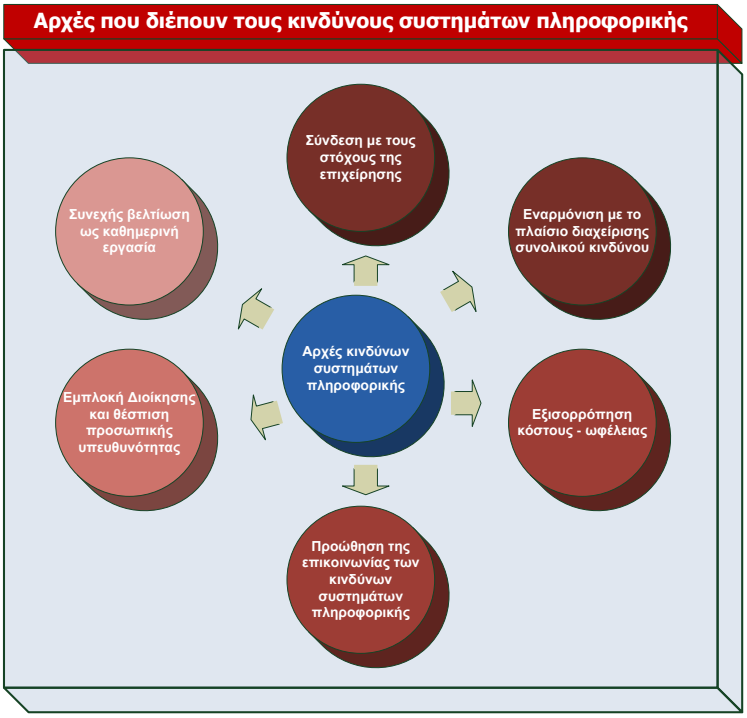
2.8 Διασύνδεση του κινδύνου πληροφοριακών συστημάτων με την ηλεκτρονική διακυβέρνηση μιας επιχείρησης

Η διαχείριση κινδύνων είναι μία από τις πέντε βασικές περιοχές της ηλεκτρονικής διακυβέρνησης, μαζί με την εναρμόνιση της στρατηγικής (strategic alignment), την παραγωγή προστιθέμενης αξίας (value delivery), τη μέτρηση των επιδόσεων (performance measurement) και της διαχείρισης των πόρων (resource management).

Η αποτελεσματική διακυβέρνηση ξεκινά με την ηγεσία, τη δέσμευση και τη στήριξη από την πλευρά της διοίκησης της επιχείρησης, ωστόσο δεν είναι αρκετή. Η διαχείριση κινδύνων συστημάτων πληροφορικής υποστηρίζει την ηγεσία παρέχοντας σαφή και συνεπή εφαρμογή των διαδικασιών, σαφή κατανόηση της εκτελεστικής εξουσίας και των επιχειρηματικών κανόνων αλλά και των ρόλων και των ευθυνών του τμήματος πληροφορικής.

2.9 Αρχές που διέπουν τη διαχείριση κινδύνων συστημάτων πληροφορικής

Οι κίνδυνοι συστημάτων πληροφορικής καθορίζουν αλλά και στηρίζονται σε ορισμένες αρχές που αποσκοπούν στην αποτελεσματική διαχείρισή τους. Οι αρχές αυτές βασίζονται πάνω στις ευρέως αποδεκτές αρχές της διαχείρισης του συνολικού κινδύνου μιας επιχείρησης, οι οποίες εφαρμόζονται στους κινδύνους των συστημάτων πληροφορικής. Το πλαίσιο διαχείρισης των κινδύνων συστημάτων πληροφορικής έχει σχεδιαστεί με σκοπό να καθοδηγήσει τις επιχειρήσεις που το χρησιμοποιούν, έτσι ώστε να είναι σε θέση να ελέγχουν την αποδοτικότητά τους βάσει των κανόνων που το διέπουν.



Εικόνα 4: Αρχές που διέπουν τους κινδύνους συστημάτων πληροφορικής [13]

2.9.1 Σύνδεση με επιχειρηματικούς στόχους

Έτσι λοιπόν, βασική αρχή είναι ότι τόσο η αποτελεσματική διακυβέρνηση των επιχειρήσεων όσο και η διαχείριση κινδύνων πληροφορικής συνδέονται πάντα με τους επιχειρηματικούς στόχους της επιχείρησης. Οι κίνδυνοι των συστημάτων πληροφορικής, σε αντίθεση με τα υπόλοιπα είδη κινδύνων, πρέπει πάντα να θεωρούνται ως επιχειρηματικοί κίνδυνοι και να αντιμετωπίζονται διεξοδικά και σε ολόκληρη την επιχείρηση. Ο προφανής στόχος είναι η επίτευξη του επιθυμητού αποτελέσματος της επιχείρησης.

Η ύπαρξη συστημάτων πληροφορικής υποστηρίζει και βοηθά στην επίτευξη των στόχων της επιχείρησης και για αυτό οι κίνδυνοι που διατρέχουν τα συστήματα πληροφορικής έχουν άμεσο αντίκτυπο στην επίτευξη των στόχων ή της στρατηγικής της επιχείρησης. Κάθε μελέτη για τους κινδύνους των συστημάτων πληροφορικής πρέπει να περιέχει και την αλληλεπίδραση των διεργασιών της επιχείρησης με τους πόρους της επιχείρησης που σχετίζονται με αυτά, όπως το ανθρώπινο δυναμικό, τα διαφορετικά λογισμικά που χρησιμοποιεί η επιχείρηση και την υποδομή - εξοπλισμό που διαθέτει. Η αποτελεσματική διαχείριση κινδύνων συ-

στημάτων πληροφορικής μπορεί να αποτελέσει τον μοχλό ανάπτυξης της εταιρείας και όχι ένα ακόμα εμπόδιο προς την επίτευξη των στόχων της επιχείρησης, [14].

2.9.2 Εναρμόνιση με τον συνολικό επιχειρηματικό κίνδυνο

Μία άλλη αρχή, είναι αυτή της εναρμόνισης της διαχείρισης κινδύνων συστημάτων πληροφορικής με τη διαχείριση του συνολικού κινδύνου της εταιρείας, που έτσι κι αλλιώς αποτελεί κομμάτι του. Οι στόχοι της επιχείρησης πρέπει να συσχετίζονται με καθορισμένο μέγεθος κινδύνου που η επιχείρηση προτίθεται να αναλάβει, προκειμένου να πετύχει το στόχο της. Η διοίκηση της επιχείρησης πρέπει να είναι σε θέση να υπολογίσει τα οφέλη αλλά και τις συνέπειες από την υιοθέτηση διαφόρων τεχνολογιών πληροφορικής και των κινδύνων που τις συνοδεύουν.

Η απόφαση για την ανάληψη συγκεκριμένου μεγέθους κινδύνου αποκαλύπτει και το είδος της διαχείρισης που κάθε διοίκηση ασκεί σε μία επιχείρηση. Έτσι έχουμε επιχειρήσεις που ακολουθούν ιδιαίτερα επιθετική στρατηγική και είναι διατεθειμένες να αναλάβουν μεγάλους κινδύνους προκειμένου να πετύχουν τους στόχους τους, ενώ υπάρχουν επιχειρήσεις με ιδιαίτερα συντηρητικό προφίλ διοίκησης που δεν αναλαμβάνουν κανένα κίνδυνο. Δεν υπάρχει τρόπος να αποφανθεί κανείς ποιος κάνει το σωστό, αφού ο κίνδυνος που αναλαμβάνει κάθε επιχείρηση είναι θέμα απόφασης των μετόχων της και του διοικητικού της συμβουλίου.

Αυτό που πραγματικά συμβαίνει είναι ότι οι κίνδυνοι αποτελούν μέρος της επιχείρησης και ότι κατανέμονται σε όλες τις διεργασίες της. Η εναρμόνιση με τη διαχείριση του συνολικού κινδύνου της επιχείρησης -για τους κινδύνους συστημάτων πληροφορικής- προσφέρει μία σειρά από μέτρα αποφυγής ή μείωσης κινδύνων, που σαφώς κάθε επιχείρηση πρέπει να έχει.

2.9.3 Εξισορρόπηση κόστους - ωφέλειας

Άλλη μία αρχή που διέπει τους κινδύνους συστημάτων πληροφορικής είναι ότι, η αποτελεσματική διαχείρισή τους προσπαθεί να βρει τη χρυσή τομή μεταξύ κόστους και ωφέλειας από τη χρήση τους, έτσι ώστε οι επενδύσεις σε τεχνολογίες πληροφορικής, να αποβαίνουν τελικά προς όφελος της επιχείρησης, [15].

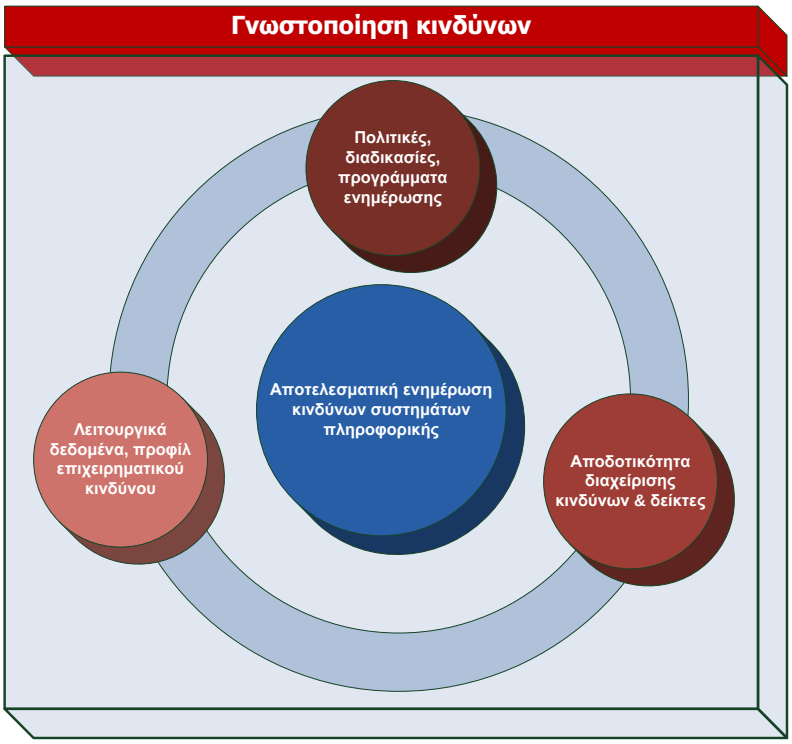
Πρέπει κάθε επιχείρηση να προβαίνει σε καθορισμό των προτεραιοτήτων της και πάντα σε συσχετισμό με το μέγεθος των κινδύνων που είναι διατεθειμένη να αναλάβει, αλλά και των καθορισμένων ορίων ζημιάς που δυνητικά μπορεί να έχει. Έτσι για παράδειγμα, κάθε αγορά πληροφοριακού συστήματος θα αντικατοπτρίζει τη διάθεση της επιχείρησης να αναλάβει το ρίσκο η επένδυση αυτή να μην της αποφέρει τα επιθυμητά αποτελέσματα αναλογικά με το κόστος που θα χρειαστεί να κάνει.

Για την αντιμετώπιση λοιπόν αυτών των κινδύνων, η επιχείρηση πρέπει να ορίσει μία σειρά σημείων ελέγχου, που θα περιορίζουν τους κινδύνους των συστημάτων πληροφορικής, παίρνοντας πάντα υπόψη της το κόστος των σημείων ελέγχου. Για παράδειγμα, αν υποθέσουμε ότι μία επιχείρηση θα έπρεπε να δαπανήσει πολλά χρήματα για την εξασφάλισή της από μία συγκεκριμένη βλάβη στα συστήματα πληροφορικής που έχει, ενώ η συγκεκριμένη βλάβη μπορεί να συμβεί κάτω από εντελώς απίθανες συνθήκες, τότε η επιχείρηση μπορεί να αποφασίσει να αναλάβει τον κίνδυνο και να μην προχωρήσει στην επένδυση αυτή. Η αναλογία κόστους – ωφέλειας θα είναι υπέρμετρα μεγάλη προς την πλευρά του κόστους και συνεπώς η επιχείρηση αποφασίζει να μην την υιοθετήσει. Αυτό θα πρέπει να γίνει για κάθε μία επένδυση που η επιχείρηση έχει ή σκέφτεται να κάνει σε συστήματα πληροφορικής έτσι ώστε να εξασφαλιστεί η αποτελεσματική διαχείριση των κινδύνων, [16].

2.9.4 Ενημέρωση των κινδύνων μέσα στην επιχείρηση

Μια πολύ βασική αρχή για τους κινδύνους πληροφορικής είναι και η γνωστοποίησή τους μέσα στην επιχείρηση. Δεν έχει νόημα η επιχείρηση να έχει δαπανήσει

τεράστια ποσά σε συστήματα πληροφορικής όταν οι κίνδυνοι από αυτά, αγνοούνται πλήρως από το ανθρώπινο δυναμικό της. Έτσι λοιπόν η ακριβής και επίκαιρη γνωστοποίησή τους μέσα στην επιχείρηση αποτελεί την αρχή για οποιαδήποτε επένδυση σε συστήματα πληροφορικής. Για να μεγιστοποιηθεί το όφελος της γνωστοποίησης από το προσωπικό της επιχείρησης πρέπει οι κίνδυνοι να παρουσιαστούν όχι με την καθαρά τεχνική τους μορφή αλλά με την μορφή πραγματικών παραδειγμάτων πάνω στη χρήση των διαφόρων τεχνολογιών πληροφορικής, έτσι ώστε οι κίνδυνοι να γίνουν κατανοητοί, αποδεκτοί, να εντυπωθούν στην μνήμη των υπαλλήλων και να αποτελέσουν την κουλτούρα σε θέματα διαχείρισης κινδύνων της επιχείρησης. Ποια στοιχεία όμως πρέπει να γνωστοποιηθούν;



Εικόνα 5: Γνωστοποίηση κινδύνων [12]

Η επιχείρηση πρέπει να γνωστοποιεί τις πολιτικές, τις διαδικασίες και να έχει διάφορα προγράμματα ενημέρωσης κινδύνων για τα συστήματα πληροφορικής. Αυτό το κομμάτι επικοινωνίας αποτελεί το βασικό στοιχείο που επιδεικνύει τη στάση της επιχείρησης προς τις τεχνολογίες πληροφορικής.

Επιπλέον, η επιχείρηση οφείλει να ενημερώνει για κάποια στοιχεία αναφορικά με την αποδοτικότητα της διαχείρισης κινδύνων αλλά και για τους δείκτες που να δείχνουν την αποτελεσματικότητα της διαχείρισης αυτής. Έτσι, ολόκληρη η επιχείρηση θα γνωρίζει κατά πόσο μπορεί να προστατευθεί από τυχόν κινδύνους, πράγμα που θα αυξήσει την εγρήγορση των εμπλεκομένων και θα διαμορφώσει την εταιρική κουλτούρα της επιχείρησης, μειώνοντας στο απώτερο μέλλον τους κινδύνους που αντιμετωπίζει.

Τέλος, η ενημέρωση θα πρέπει να περιέχει στοιχεία αναφορικά με τα λειτουργικά δεδομένα της επιχείρησης όπως το επιχειρηματικό προφίλ κινδύνων που αντιμετωπίζει, η αιτία που αντιμετωπίζει τέτοιους κινδύνους, τα επίπεδα ανοχής που υπάρχουν, περιπτώσεις απώλειας δεδομένων καθώς και παράγοντες κινδύνου που σηματοδοτούν την ύπαρξη των κινδύνων.

2.9.5 Ο σωστός ρόλος της διοίκησης και η προσωπική ευθύνη

Η αποτελεσματική διαχείριση κινδύνων συστημάτων πληροφορικής βασίζεται στην αρχή ότι η συμβολή της διοίκησης είναι καθοριστική και όχι τυπική. Οι αποφάσεις για την ανάληψη κινδύνου σε όλα τα επίπεδα πρέπει να προέρχονται κατόπιν ώριμης σκέψης και η συμβολή της διοίκησης σε αυτό είναι να δίνει το σωστό παράδειγμα, αλλά και να επιβάλλει την θέσπιση ανάλογων διαδικασιών, [17]. Στο πλαίσιο αυτό, είναι αναγκαία η θέσπιση του όρου της «προσωπικής ευθύνης» για κάθε εμπλεκόμενο. Πρέπει ο καθένας, ανεξαρτήτως σε ποιο επίπεδο της επιχείρησης εργάζεται, να αναλαμβάνει το μερίδιο ευθύνης που του αντιστοιχεί έτσι ώστε οι αποφάσεις να αποτελούν προϊόν συλλογικής ευθύνης και όχι μονομερών ανακοινώσεων.

Άτομα σε θέσεις κλειδιά που είναι ικανά να επηρεάσουν τη διοίκηση πρέπει να εμπλακούν στη διαχείριση των κινδύνων συστημάτων πληροφορικής. Για να εξασφαλιστεί αυτό, πρέπει να υπάρχουν διαδικασίες που θα τους αναθέτουν ξεκάθαρα την ευθύνη, την οποία θα κληθούν να αναλάβουν και να είναι υπόλογοι για τη εύρυθμη λειτουργία των συστημάτων πληροφορικής. Επιπλέον, η ανάληψη της ευθύνης, πέρα από την απόδοση ευθυνών πρέπει να συνδεθεί και με ένα σύστη-

μα ανταμοιβών έτσι ώστε να είναι αποδεκτή η ανάληψη της ευθύνης από τα εμπλεκόμενα άτομα.

Τέτοια άτομα μπορεί να είναι εκείνα που αποφασίζουν για επενδύσεις σε συστήματα πληροφορικής, για χρηματοδότηση έργων πληροφορικής, για ριζικές αλλαγές στην υποδομή – εξοπλισμό της επιχείρησης, για την εκτίμηση των κινδύνων και για την παρακολούθηση και τον έλεγχο των διαφόρων σημείων ελέγχου.

2.9.6 Η συνεχής βελτίωση ως καθημερινή λειτουργία

Η συνεχής και καθημερινή βελτίωση των διαδικασιών διαχείρισης κινδύνων αποτελεί την τελευταία και βασική αρχή της αποτελεσματικής διαχείρισης κινδύνων πληροφορικής. Επειδή η φύση των κινδύνων των συστημάτων πληροφορικής είναι δυναμική, η διαχείρισή τους πρέπει να είναι μία επαναλαμβανόμενη και αέναη διαδικασία. Δεν μπορεί η επιχείρηση σε κανένα σημείο της επιχειρηματικής της δραστηριότητας να αποφανθεί ότι πλέον δεν έχει να αντιμετωπίσει κινδύνους που σχετίζονται με τα πληροφοριακά της συστήματα. Οι κίνδυνοι είναι διαρκείς και εμπλουτίζονται με πρωτοφανείς ρυθμούς.

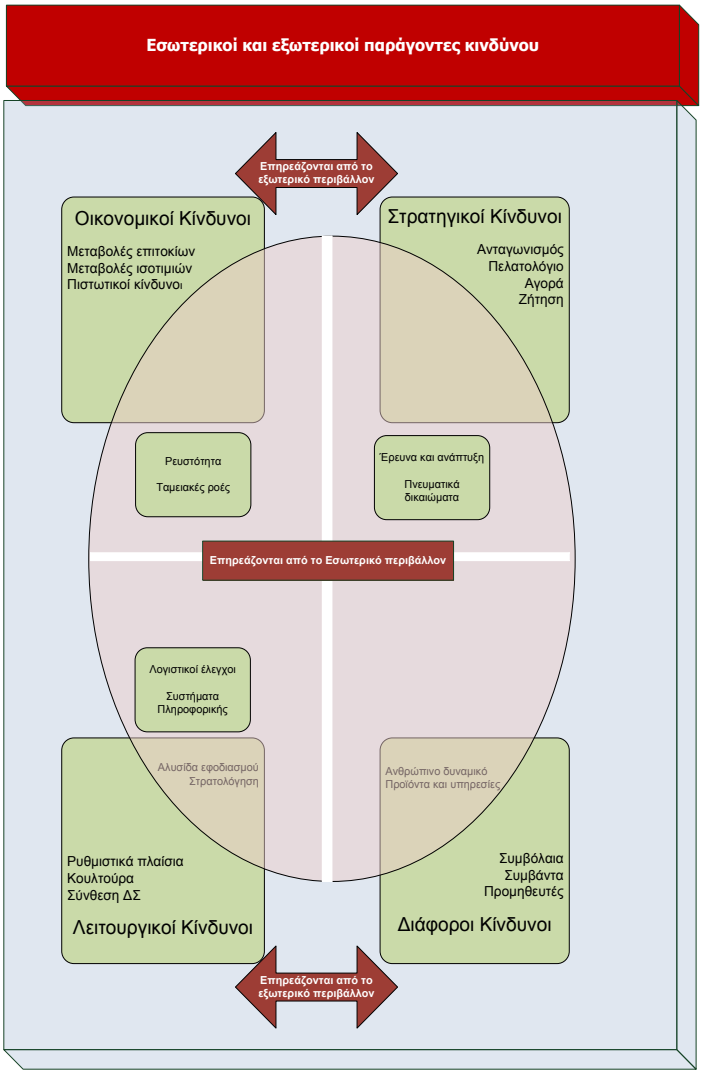
Η εμφάνιση νέων τεχνολογιών αποτελεί καθημερινό φαινόμενο ειδικά στις μέρες μας. Αυτό, αποτελεί δυνητικά μία ευκαιρία για την επιχείρηση, η οποία όμως υποκρύπτει και κάποιους κινδύνους. Πρέπει, λοιπόν, η διαχείριση των κινδύνων να είναι συνεχής γιατί μόνο έτσι θα έχει τη δυνατότητα η επιχείρηση να χρησιμοποιήσει τις δυνητικά νέες ευκαιρίες που τις παρουσιάζονται. Αλλαγές στο ρυθμιστικό πλαίσιο λειτουργίας μπορεί να επιφέρουν κάποιους νέους κινδύνους μη συμμόρφωσης, που πρέπει να αξιολογούνται σε καθημερινή βάση.

Ειδική αναφορά πρέπει να γίνει στις μεθόδους αποτίμησης κινδύνων, στην ύπαρξη ρόλων και αρμοδιοτήτων, στα εργαλεία, στις τεχνικές καθώς και στα κριτήρια κινδύνου που θέτει η επιχείρηση. Πρέπει, ειδικότερα, να εντοπιστούν οι διεργασίες της επιχείρησης που είναι συνδεδεμένες με τη ανάληψη κινδύνου, να εξεταστούν οι πιθανές επιπτώσεις των κινδύνων αυτών και, τέλος, να αναλυθούν οι

συνθήκες εκείνες που θα σηματοδοτήσουν ότι κάποιες αλλαγές πρέπει να γίνουν στο κύκλο της διαχείρισης κινδύνων.

2.10 Εξωτερικοί και εσωτερικοί παράγοντες κινδύνου

Οι κίνδυνοι που αντιμετωπίζει μια επιχείρηση μπορεί να οφείλονται σε εξωτερικούς ή εσωτερικούς παράγοντες. Όμως, υπάρχουν και κίνδυνοι που μπορούν να υπάρξουν τόσο στο εξωγενές περιβάλλον της επιχείρησης όσο και στο εσωτερικό της.



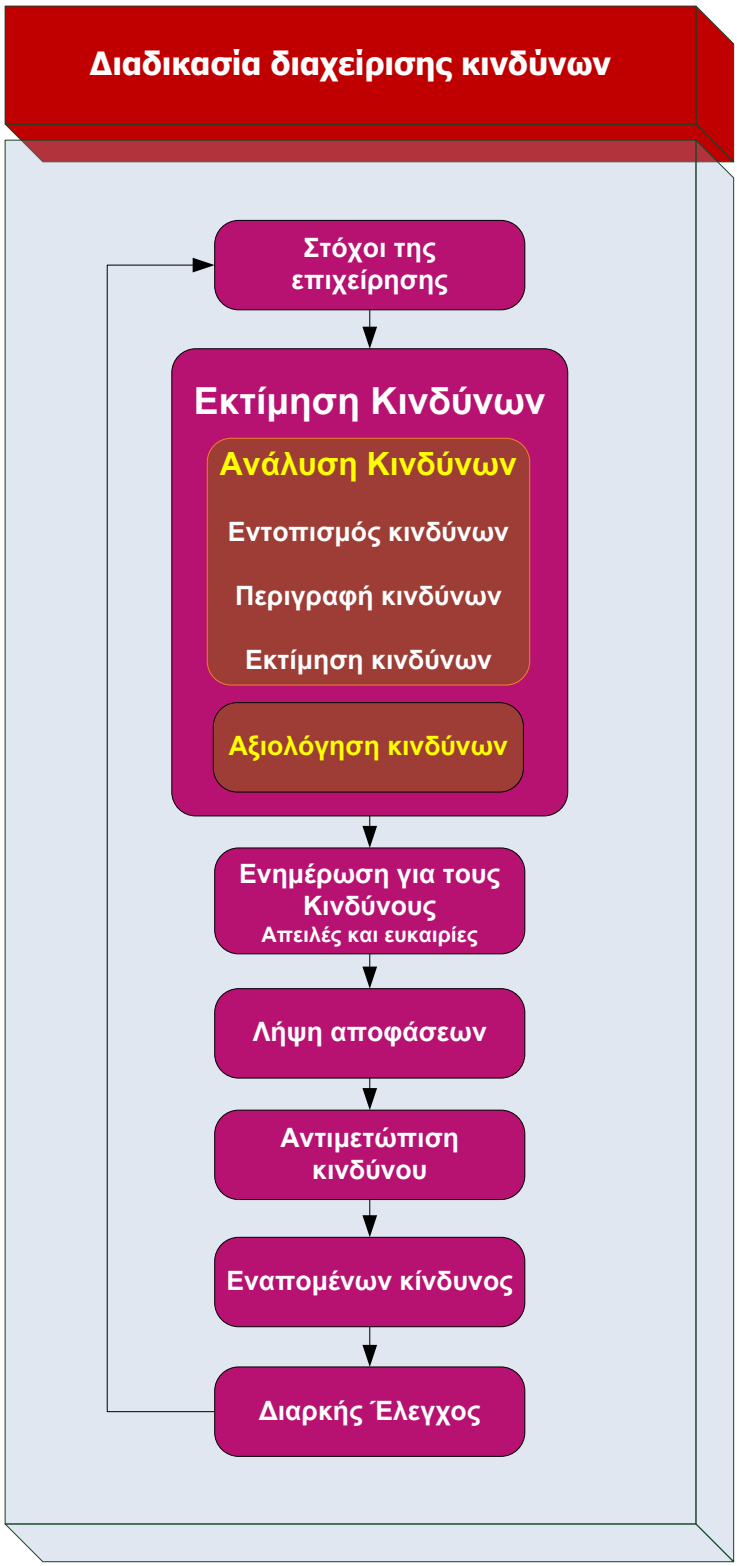
Εικόνα 6: Εσωτερικοί και εξωτερικοί παράγοντες κινδύνου [18]

Οι οικονομικοί κίνδυνοι, οι κίνδυνοι στρατηγικής, οι λειτουργικοί κίνδυνοι και οι λοιποί κίνδυνοι αλληεπιδρούν με το εξωτερικό περιβάλλον και επηρεάζονται άμεσα από αυτό. Όμως οι κίνδυνοι όπως η ρευστότητα και οι ταμειακές ροές, η έρευνα και ανάπτυξη για νέα προϊόντα, οι λογιστικοί έλεγχοι και τέλος τα συστήματα πληροφορικής επηρεάζονται τόσο από το εξωτερικό όσο και από το εσωτερικό περιβάλλον.

2.11 Η διαχείριση κινδύνων

Το πλαίσιο διαχείρισης κινδύνων έχει σχεδιαστεί με τέτοιο τρόπο ώστε να προσθέτει αξία στην επιχείρηση μέσω της υποστήριξης των επιμέρους στόχων της [18], με το να παρέχει ένα πλαίσιο διαδικασιών που επιτρέπει στην επιχείρηση να λειτουργήσει με ένα σταθερό και ελεγχόμενο τρόπο. Το πλαίσιο αυτό συμβάλλει στην αποδοτικότερη χρήση των πόρων της επιχείρησης, μειώνει την αστάθεια στις υποστηρικτικές λειτουργίες της, προστατεύει και ενισχύει τα περουσιακά της στοιχεία και ενισχύει την γενικότερη εικόνα της προς τον έξω κόσμο.

Επιπλέον, οι διαδικασίες που πηγάζουν από το πλαίσιο διαχείρισης κινδύνων βοηθούν στην υποστήριξη και ανάπτυξη του ανθρώπινου δυναμικού, στον εμπλουτισμό της εμπειρίας της επιχείρησης και στην αποτελεσματικότερη και αποδοτικότερη λειτουργία της.



Εικόνα 7: Διαδικασία διαχείρισης κινδύνων [18]

2.11.1 Εκτίμηση κινδύνου

Η εκτίμηση κινδύνου, σύμφωνα με το ISO/IEC Guide 73, ορίζεται ως η επαναλαμβανόμενη διαδικασία του υπολογισμού της πιθανότητας και των επιπτώσεων των κινδύνων, με τη χρήση ποιοτικών και ποσοτικών μεθόδων. Όπως υπονοεί και η λέξη «εκτίμηση», η διαδικασία αυτή είναι υποκειμενική, καθώς, κάτι που για κάποιον είναι σημαντικό, για κάποιον άλλον δεν είναι. Ομοίως, κάτι που θεωρείται μεγάλης σημασίας για μια επιχείρηση σε μία άλλη δεν έχει μεγάλη επίπτωση.

Σκοπός αυτής της έρευνας είναι να προτείνει μία νέα μέθοδο ποσοτικοποίησης των κινδύνων για τα συστήματα πληροφορικής η οποία δεν θα βασίζεται σε προσωπικές εκτιμήσεις αλλά σε αδιάσειστες μετρήσεις που θα υποδεικνύουν το βαθμό επικινδυνότητας ενός συστήματος, προϊόντος ή υπηρεσίας.

2.11.2 Ανάλυση κινδύνου

Η ανάλυση κινδύνων είναι η διαδικασία εντοπισμού και υπολογισμού της έκθεσης της επιχείρησης σε τυχαία –και ίσως καταστροφικά- συμβάντα. Αυτό απαιτεί την βαθιά γνώση της επιχείρησης, της αγοράς που απευθύνεται, του νομικού και κοινωνικοπολιτικού περιβάλλοντος μέσα στο οποίο ασκεί τις δραστηριότητές της, την πλήρη κατανόηση των στρατηγικών και λειτουργικών στόχων της καθώς και των κρίσιμων παραγόντων που θα συμβάλουν στην επίτευξή τους.

2.11.2.1 .Εντοπισμός κινδύνου

Ο εντοπισμός των κινδύνων είναι μια συνεχής διαδικασία που σκοπό έχει να εντοπίσει τις περιοχές κινδύνων της επιχείρησης. Ο εντοπισμός αυτός πρέπει να γίνεται με μεθοδικό τρόπο έτσι ώστε να εξασφαλιστεί ότι όλες οι λειτουργίες της επιχείρησης έχουν χαρτογραφηθεί, [19], καθώς και όλοι οι κίνδυνοι που απορρέουν από αυτές έχουν καταγραφεί και κατηγοριοποιηθεί σε μία από τις κατηγορίες που περιγράφτηκαν στην παράγραφο 2.5. Η διαδικασία του εντοπισμού των κινδύνων μίας επιχείρησης μπορεί να γίνει και από εξωτερικούς συμβούλους που ειδικεύονται σε αυτά τα θέματα. Όμως μία καλά οργανωμένη εσωτερικά της επι-

χείρησης προσπάθεια, την οποία θα γνωστοποιήσει η διοίκηση της επιχείρησης προς το ανθρώπινο δυναμικό της, θα είναι κατά κανόνα περισσότερο αποδοτική και ακριβής. Η αποδοχή της έννοιας του κινδύνου εσωτερικά σε μία επιχείρηση είναι ζωτικής σημασίας.

Μερικές από τις μεθόδους εντοπισμού κινδύνων είναι:

1. Η ανταλλαγή απόψεων (Brainstorming)
2. Η σύνθεση ερωτηματολογίων
3. Η ανάλυση αγοράς
4. Η διαμόρφωση σεναρίων για την πορεία της αγοράς
5. Οι ομάδες εργασίας αποτίμησης κινδύνων
6. Η έρευνα περιστατικών κινδύνων για την αναζήτηση αιτιών δημιουργίας τους
7. Η ύπαρξη εσωτερικής επιθεώρησης και διαδικασιών ελέγχου

2.11.2.2 .Περιγραφή κινδύνου

Ως φυσική συνέχεια της διαδικασίας εντοπισμού των κινδύνων μιας επιχείρησης είναι η ακριβής περιγραφή τους με τρόπο οργανωμένο, για παράδειγμα με τη χρήση πίνακα αποτύπωσης. Η χρήση ενός τέτοιου πίνακα είναι αναγκαία για να εξασφαλιστεί η ολοκληρωμένη και αναλυτική περιγραφή των αποτελεσμάτων της διαδικασίας εντοπισμού. Εξετάζοντας τόσο την πιθανή επίπτωση όσο και την πιθανότητα εμφάνισης καθενός από τους κινδύνους που αναφέρονται στο πίνακα αποτύπωσης κινδύνων της επιχείρησης, είναι δυνατό να καθοριστεί η προτεραιότητα στους βασικούς κινδύνους, οι οποίοι θα πρέπει να αναλυθούν με περισσότερη λεπτομέρεια. Οι κίνδυνοι που σχετίζονται με τις λειτουργικές εργασίες της επιχείρησης ή με τη λήψη αποφάσεων μπορούν να κατηγοριοποιηθούν τόσο ως κίνδυνοι στρατηγικής όσο και ως λειτουργικοί κίνδυνοι. Για αυτό είναι απαραίτητο να

ενσωματωθεί η έννοια του κινδύνου σε κάθε φάση όλων των έργων μιας επιχείρησης και να παρθούν τα αντίστοιχα μέτρα αποφυγής τους.

Ο Πίνακας 2, είναι ένας προτεινόμενος πίνακας αποτύπωσης των κινδύνων μιας επιχείρησης:

Πίνακας Αποτύπωσης Κινδύνων Επιχείρησης	
Κίνδυνος:	
Περιοχή κινδύνου	Ποιοτική περιγραφή του κινδύνου, του μεγέθους του, του τύπου του καθώς και των πιθανών εξαρτήσεων του.
Κατηγορία κινδύνου	Στρατηγικός, επιχειρησιακός, οικονομικός, νομικός, συμμόρφωσης σε ρυθμιστικό πλαίσιο κτλ.
Ενδιαφερόμενοι	Ποιους ενδιαφέρει και ποιες είναι οι προσδοκίες τους;
Ποσοτικοποίηση του κινδύνου	Σημασία και πιθανότητα
Ανοχή στον κίνδυνο	• Πιθανές απώλειες σε κέρδη και άλλες οικονομικές επιπτώσεις • Αποτίμηση του κινδύνου ζημιάς (Value at risk) • Πιθανότητα και έκταση πιθανών ζημιών • Στόχοι για τον έλεγχο του κινδύνου και επιθυμητά επίπεδα επιδόσεων
Αντιμετώπιση κινδύνου και μηχανισμοί ελέγχου	Διαδικασίες που θα χρησιμοποιηθούν στην περίπτωση εμφάνισης του κινδύνου και μηχανισμοί ελέγχου για την αποφυγή του κινδύνου
Πιθανές βελτιώσεις	Προτάσεις για την βελτίωση των διαδικασιών με σκοπό την μείωση των κινδύνων

Πίνακας 2: Πίνακας αποτύπωσης κινδύνων επιχείρησης

2.11.2.3 .Μέθοδοι εκτίμησης κινδύνου

Υπάρχουν διάφορες μέθοδοι για την εκτίμηση του κινδύνου. Οι μέθοδοι αυτοί κατηγοριοποιούνται σε ποσοτικές, μερικώς ποσοτικές ή ποιοτικές όσο αφορά στην πιθανότητα εμφάνισης και τις πιθανές επιπτώσεις. Η μέτρηση των πιθανοτήτων εμφάνισης αλλά και των επιπτώσεων του κινδύνου γίνεται με τη χρήση κλίμακας τριών διαβαθμίσεων: α) Υψηλή, β) Μεσαία και γ) Χαμηλή. Παρόλα αυτά, κάποιες επιχειρήσεις για την μέτρηση του κινδύνου και των επιπτώσεών του, χρησιμοποιούν διαφορετική κλίμακα, με περισσότερες διαβαθμίσεις οι οποίες εξυπηρετούν τις ανάγκες τους καλύτερα και τους δίνουν μια πιο ακριβή απεικόνιση των κινδύνων που διατρέχουν.

Στο σημείο αυτό προτείνονται ορισμένοι πίνακες (βλέπε πίνακες Πίνακας 3 καιΠίνακας 4: α) των επιπτώσεων κινδύνου και β) της πιθανότητας εμφάνισης του κινδύνου, σε συνδυασμό με τη χρήση της κλίμακας βαθμολόγησής τους.

Πίνακας επιπτώσεων κινδύνου	
Υψηλή	• Οι οικονομικές ζημιές προβλέπεται να ξεπεράσουν τα ... €. • Σημαντικές επιπτώσεις θα υπάρξουν στην επίτευξη των στρατηγικών στόχων και στη λειτουργία της επιχείρησης. • Σημαντική θα είναι η επίδραση του κινδύνου στους μετόχους της επιχείρησης
Μέτρια	• Οι οικονομικές ζημιές προβλέπεται να είναι μεταξύ των ... € και ... €. • Δεν θα υπάρξουν σημαντικές επιπτώσεις στην επίτευξη των στρατηγικών στόχων και στη λειτουργία της επιχείρησης. • Ο κίνδυνος θα ανησυχήσει μικρή μερίδα των μετόχων
Χαμηλή	• Οι οικονομικές ζημιές προβλέπεται να είναι λιγότερες από ... €.

Πίνακας επιπτώσεων κινδύνου	
	• Οι επιπτώσεις που θα υπάρξουν στην επίτευξη των στρατηγικών στόχων και στη λειτουργία της επιχείρησης θα είναι από μικρές έως μηδενικές. • Δεν θα έχει επίδραση ο κίνδυνος στους μετόχους της επιχείρησης

Πίνακας 3: Πίνακας επιπτώσεων κινδύνου

Πίνακας πιθανότητας εμφάνισης κινδύνου		
Εκτίμηση	Περιγραφή	Δείκτες
Υψηλή (Πιθανό να συμβεί)	Συμβαίνει κάθε χρόνο ή η πιθανότητα εμφάνισης να είναι πάνω από 25%	Πιθανότητα να συμβαίνει αρκετές φορές μέσα σε ένα καθορισμένο χρονικό πλαίσιο (π.χ. 2 ετών)
Χαμηλή (Ίσως να συμβεί)	Πιθανό να συμβαίνει σε μεγάλο χρονικό διάστημα (π.χ. 5 ετών) ή η πιθανότητα εμφάνισης να είναι μικρότερη από 25%	Θα μπορούσε να συμβεί μία φορά μέσα σε ένα καθορισμένο χρονικό διάστημα (π.χ. 2 ετών)
Χαμηλή (Απίθανο να συμβεί)	Δεν είναι πιθανό να συμβεί ή η πιθανότητα εμφάνισης να είναι μικρότερη από 2%	Δεν έχει συμβεί ποτέ και είναι απίθανο να συμβεί

Πίνακας 4: Πίνακα πιθανότητας εμφάνισης κινδύνου

Υπάρχουν και αρκετές μεθοδολογίες για την ανάλυση των κινδύνων [18]. Κάποιες από αυτές είναι:

1. Η έρευνα αγοράς

2. Η ανάλυση SWOT (Strength, Weaknesses, Opportunities, Threats)
3. Το σχέδιο επιχειρησιακής συνέχειας (Business Continuity Plan)
4. Η ανάλυση BPEST (Business, Political, Economic, Social, Technological)
5. Η ανάλυση PESTLE (Political, Economic, Social, Technical, Legal, Environmental)
6. Η συμπερασματική στατιστική ανάλυση (Statistical Inference Analysis).

Τα αποτελέσματα της ανάλυσης κινδύνων μπορούν και πρέπει να χρησιμοποιηθούν για τη δημιουργία του προφίλ των κινδύνων που αντιμετωπίζει η επιχείρηση. Έχοντας καταγράψει και βαθμολογήσει τους κινδύνους ανάλογα με την επικινδυνότητά τους η επιχείρηση μπορεί να προβεί στην κατάρτιση της λίστας προτεραιότητας αντιμετώπισης κινδύνων, δηλαδή από ποιους κινδύνους πρέπει να είναι έτοιμη να προστατευθεί αλλά και να αντιδράσει.

Αυτή η χαρτογράφηση των κινδύνων αναπόφευκτα υποδεικνύει τις επιχειρησιακές περιοχές που εκτιμούμε ότι θα συμβούν οι κίνδυνοι, περιγράφει τις αναγκαίες διαδικασίες ελέγχου που δυνητικά θα έπρεπε να υπάρχουν και, τέλος, αναδεικνύει την αναγκαιότητα της προσωπικής ευθύνης κάθε εμπλεκομένου ατόμου στις λειτουργίες της επιχείρησης.

2.11.3 Αξιολόγηση κινδύνου

Όταν πλέον ολοκληρωθεί η διαδικασία της ανάλυσης των κινδύνων της επιχείρησης, είναι αναγκαίο να χρησιμοποιηθούν τα ευρήματά της για την σύγκριση με τους κινδύνους που η επιχείρηση νόμιζε ότι θα αντιμετωπίζει όταν δημιουργήθηκε. Οι κίνδυνοι αυτοί μπορεί να είναι συσχετισμένοι με διάφορα κόστη και ποσοστά κερδών, νομικές υποχρεώσεις – προϋποθέσεις, κοινωνικοοικονομικούς παράγοντες, σύνθεση μετόχων και άλλα. Η διαδικασία της αξιολόγησης των κινδύνων βοηθά την επιχείρηση να αποφασίσει σχετικά με τη σημαντικότητα καθενός κινδύνου και, επιπλέον, αν θα πρέπει να γίνει αποδεκτή η ύπαρξη κάθε κινδύνου. Εάν ναι, τότε να καθορίσει τις διαδικασίες αντιμετώπισής του.

2.11.4 Ενημέρωση για τους Κινδύνους

Η σύγχρονη επιχείρηση αποτελείται από διαφορετικούς τομείς λειτουργίας και με τη σειρά τους αυτοί από πολλά τμήματα. Κάθε μία από αυτές τις υπηρεσιακές περιοχές έχει την ανάγκη διαφορετικής πληροφόρησης αναφορικά με τους κινδύνους που ενδέχεται να αντιμετωπίσει και οι οποίοι έχουν εντοπιστεί από τη διαδικασία ανάλυσης κινδύνων.

Έτσι, για παράδειγμα, το διοικητικό συμβούλιο πρέπει να γνωρίζει τους σημαντικότερους κινδύνους που αντιμετωπίζει η επιχείρηση, όπως επίσης και τις πιθανές επιπτώσεις που θα έχουν αυτοί στους μετόχους της επιχείρησης. Είναι απαραίτητο να γνωρίζει το επιχειρησιακό πλάνο που θα ακολουθήσει η επιχείρηση σε περίπτωση καθενός από τους σημαντικούς κινδύνους που αντιμετωπίζει.

Γνωρίζοντας τόσο τους κινδύνους όσο και τις διαδικασίες αντιμετώπισής τους, είναι ευθύνη του διοικητικού συμβουλίου να ενημερώσει για την κατάλληλη διαδικασία την ανάλογη υπηρεσιακή μονάδα, καθώς και να συντονίσει διαφορετικές υπηρεσιακές μονάδες μεταξύ τους σε περίπτωση σύνθετων κινδύνων. Επιπλέον, πρέπει να φροντίσει να εξασφαλίσει ότι οι καθορισμένες διαδικασίες θα αποφέρουν το επιθυμητό αποτέλεσμα και η επιχείρηση θα υποστεί τις λιγότερες δυνατές ή και καθόλου ζημιές, οποιασδήποτε φύσεως, σε περίπτωση που τελικά ο κίνδυνος συμβεί.

Αντίστοιχα, οι υπηρεσιακές μονάδες, πρέπει να γνωρίζουν ακριβώς τους κινδύνους που τις αφορούν μαζί με τις πιθανές επιπτώσεις σε αυτές ή σε άλλες υπηρεσιακές μονάδες. Για παράδειγμα, αν η Διεύθυνση Πληροφορικής σε έναν Οργανισμό, υποστεί ανεπανόρθωτη βλάβη από κάποιο φυσικό κίνδυνο, αυτό θα επηρεάσει και άλλες υπηρεσιακές μονάδες με αποτέλεσμα η συνολική επίπτωση να είναι αθροιστικά πολύ μεγαλύτερη από αυτή της Διεύθυνσης Πληροφορικής.

Ακριβώς για το λόγο αυτό είναι αναγκαία η ύπαρξη δεικτών απόδοσης που θα επιτρέπουν στις υπηρεσιακές μονάδες να παρακολουθούν τις πιθανές επιπτώσεις στις βασικές λειτουργίες της επιχείρησης, στα οικονομικά της στοιχεία, στα κέρδη και τις τιμές της μετοχής, και να κάνουν προβλέψεις για πιθανές βελτιώσεις ή/και

κόστη που θα χρειαστούν στη διάρκεια του χρόνου για την πρόληψη ή/και την αντιμετώπιση των κινδύνων.

Επίσης, σημαντικό είναι οι υπηρεσιακές μονάδες να αναφέρουν στη διοίκηση εγκαίρως και με οργανωμένο τρόπο, κάθε νέο κίνδυνο που είναι δυνατό να εμφανιστεί ή αστοχίες που έχουν συμβεί στις διαδικασίες ελέγχου κινδύνων, έτσι ώστε να υπάρχει αποτελεσματική και άμεση τροποποίηση των αναγκαίων διαδικασιών.

Φυσικά, ο ακρογωνιαίος λίθος κάθε επιχείρησης είναι το ανθρώπινο δυναμικό της. Έτσι και αυτοί με τη σειρά τους πρέπει να αποκτήσουν συνείδηση του κινδύνου αλλά και των ευθυνών τους, να βοηθούν στη διαρκή βελτίωση των διαδικασιών αντιμετώπισης κινδύνων και να αναφέρουν άμεσα και οργανωμένα στη διοίκηση κάθε πιθανό νέο κίνδυνο που αντιλαμβάνονται.

Κάθε επιχείρηση δεν έχει μόνο την ανάγκη να ενημερώνει εσωτερικά για τους κινδύνους, αλλά και προς τον έξω κόσμο. Για παράδειγμα, η διοίκηση πρέπει τακτικά να ενημερώνει τους μετόχους της επιχείρησης σχετικά με τις πολιτικές διαχείρισης των κινδύνων που υιοθετούνται. Οι μέτοχοι, με τη σειρά τους, απαιτούν όλο και περισσότερο ενδείξεις ότι η διοίκηση της επιχείρησης θεσπίζει διαδικασίες μείωσης των κινδύνων και των επιπτώσεών τους, πράγμα που σηματοδοτεί την ασφάλεια της επένδυσή τους.

2.11.5 Λήψη αποφάσεων

Από τη στιγμή που η διαδικασία ανάλυσης κινδύνων έχει εντοπίσει τους κινδύνους της επιχείρησης και αυτοί έχουν αξιολογηθεί ως προς τη συχνότητα εμφάνισής τους αλλά και ως προς τις επιπτώσεις τους στην επιχείρηση, και δεδομένου ότι έχει ενημερωθεί η διοίκηση, δεν μένει παρά να ακολουθήσει η διαδικασία λήψης αποφάσεων.

Κατά τη διάρκεια της διαδικασίας αυτής, τα διευθυντικά στελέχη της επιχείρησης έχουν στη διάθεσή τους όλα τα στοιχεία αναφορικά με τους κινδύνους που διατρέχει η επιχείρηση. Συχνότητα, επιπτώσεις, κόστη και διαδικασίες συνθέτουν ένα πολύ δύσκολο πρόβλημα που καλούνται να λύσουν. Θα πρέπει για κάθε κίνδυνο

που περιέχεται στην ανάλυση των κινδύνων, να αποφασίσουν αν θα πρέπει να αναλάβουν το ρίσκο να συμβεί ο κίνδυνος και σε περίπτωση που συμβεί, αν οι επιπτώσεις θα είναι τέτοιες που θα επιτρέψουν στην επιχείρηση να συνεχίσει τις λειτουργίες της αναλαμβάνοντας το κόστος της ζημιάς.

Έτσι για παράδειγμα, ας υποθέσουμε ότι έχουμε την περίπτωση να αποφασίσει η επιχείρηση εάν θα υιοθετήσει τη χρήση ιομορφικού λογισμικού (antivirus) για την αντιμετώπιση διαφόρων ιών και κακόβουλων επιθέσεων στο δίκτυό της. Στην περίπτωση αυτή τα διευθυντικά στελέχη θα πρέπει να αποφασίσουν αν θα πάρουν την απόφαση να πληρώνουν το κόστος για τη χρήση του λογισμικού προστασίας από ιούς ή αν σε περίπτωση ύπαρξης κάποιου κακόβουλου ιού αν η εταιρεία θα μπορεί να συνεχίσει τη λειτουργία της δίχως μηχανογραφική υποστήριξη. Διαδικασίες που θα επίλυαν το πρόβλημα είναι οι διαδικασίες ανάκαμψης συστημάτων πληροφορικής σε κάποιο εναλλακτικό χώρο (disaster recovery), που όμως με τη σειρά τους επισύρουν ένα σημαντικό κόστος για την επιχείρηση.

Παρατηρούμε λοιπόν ότι ίσως η πιο σημαντική λειτουργία στη διαχείριση κινδύνων είναι η λήψη αποφάσεων και για αυτό η διαδικασία της εκτίμησης κινδύνων πρέπει να είναι όσο το δυνατό επικαιροποιημένη και αναλυτική. Αυτό είναι ακριβώς και το στοιχείο που αναγκάζει τη διαχείριση των κινδύνων να είναι μια αέναη διαδικασία, αφού κάτι που μελετήθηκε πριν από ένα χρόνο, για παράδειγμα, μπορεί να μην ισχύει πλέον ή στο διάστημα αυτό να έχουν εμφανιστεί νέοι παράγοντες που επηρεάζουν –θετικά ή αρνητικά- την εκτίμηση.

2.11.6 Αντιμετώπιση κινδύνου

Η διαδικασία αντιμετώπισης κινδύνου είναι η διαδικασία της επιλογής και εφαρμογής μέτρων ελέγχου για τη μείωση του κινδύνου, [20]. Βασικά στάδια της διαδικασίας αυτής είναι η λήψη μέτρων ελέγχου και μείωσης του κινδύνου, η λήψη μέτρων για την αποφυγή του κινδύνου και η εξασφάλιση οικονομικών πόρων για την αντιμετώπιση των συνεπειών του κινδύνου.

Η διαδικασία ανάλυσης κινδύνων αναδεικνύει τους κινδύνους που αντιμετωπίζει η επιχείρηση και αυτό συμβάλλει στην αποτελεσματική και αποδοτική λειτουργία της επιχείρησης. Στη συνέχεια, η διοίκηση της επιχείρησης θα πρέπει να προχωρήσει στην ιεράρχηση των μέτρων ελέγχου των κινδύνων, [21], ανάλογα με το μέγεθος του πιθανού κέρδους από την υιοθέτησή τους.

Η αποδοτικότητα των μέτρων ελέγχου αντιστοιχεί στον βαθμό στον οποίο ο κίνδυνος θα μειωθεί ή θα εξαλειφθεί τελείως. Αντίστοιχα, η αποδοτικότητα για το κόστος της επένδυσης της εφαρμογής ενός μέτρου ελέγχου, σχετίζεται με το κόστος υλοποίησης του μέτρου αυτού σε σχέση με τη μείωση του κινδύνου που αναμένεται. Για παράδειγμα, αν θα πρέπει να δαπανηθεί ένα υπέρογκο ποσό για την προστασία από ένα κίνδυνο, για να υπάρξει μια μικρή σχετική μείωση της πιθανότητας να συμβεί ο κίνδυνος, τότε το μέτρο ελέγχου κρίνεται ανεπαρκές και μη αποδοτικό.

Η αρχή είναι ότι όλα τα μέτρα ελέγχου πρέπει να αξιολογούνται πάντα σε σχέση με το πιθανό οικονομικό αποτέλεσμα που θα έχει η επιχείρηση αν δεν τα λάβει. Έτσι για παράδειγμα, αν μία επιχείρηση διατηρεί ένα ηλεκτρονικό κατάστημα και στηρίζει το σύνολο των εργασιών της σε πωλήσεις μέσω του διαδικτύου, πρέπει να αξιολογήσει το κόστος που θα έχει η μη υιοθέτηση λογισμικού για προστασία από κακόβουλες επιθέσεις σε σχέση με αυτή της μη λειτουργίας του ηλεκτρονικού καταστήματός της όσο καιρό χρειάζεται για να επανέλθει αυτό, μετά από μία πιθανή επίθεση.

Αρχικά, λοιπόν, πρέπει να εκτιμηθεί το κόστος υλοποίησης ενός μέτρου με κάποια σχετική ακρίβεια γιατί από αυτό θα εξαρτηθεί η αποδοτικότητά του. Η ζημιά από τη μη υιοθέτηση του μέτρου πρέπει επίσης να εκτιμηθεί με αντίστοιχη ακρίβεια και τέλος η διοίκηση συγκρίνοντας τα δύο κόστη θα λάβει την απόφαση υιοθέτησης του μέτρου ή όχι. Δεν υπάρχει συγκεκριμένος κανόνας αν θα πρέπει να ληφθεί κάποιο μέτρο ή όχι καθώς αυτό εξαρτάται άμεσα από το προφίλ της επιχείρησης αναφορικά με τη αποδοχή κινδύνων. Κάποιες επιχειρήσεις είναι διατεθειμένες να αποδεχθούν κινδύνους και να μην επενδύσουν σε αντισταθμιστικά μέτρα λόγω κακών οικονομικών συγκυριών, με σκοπό την καλύτερη εικόνα των εξόδων τους.

Φυσικά την ίδια στιγμή κινδυνεύουν περισσότερο να μην επιτύχουν καθόλου κέρδη, αλλά μόνο ζημίες σε περίπτωση που ο κίνδυνος τελικά συμβεί.

Όμως υπάρχουν και κάποια μέτρα που δεν εξαρτάται από τη διοίκηση αν θα τα λάβει ή όχι, αλλά από τη νομοθεσία. Έτσι, για παράδειγμα, μπορεί η επιχείρηση να υποχρεούται να τηρεί κάποιο πρότυπο ISO για να εξασφαλίσει την άδεια λειτουργίας της, πράγμα που αυτόματα σηματοδοτεί τη λήψη αντισταθμιστικών -στους κινδύνους- μέτρων. Επιπλέον, η συμμόρφωση σε κάποιο νομικό πλαίσιο από την επιχείρηση, μπορεί να είναι επίσης αναγκαία και όχι θέμα επιλογής της διοίκησης.

Υπάρχει βέβαια και τρόπος η επιχείρηση να επιτύχει την προστασία της από κινδύνους που αντιμετωπίζει και ταυτόχρονα να επιτύχει την ελάφρυνση των οικονομικών ζημιών που πιθανών θα έχει. Αυτός είναι να ασφαλίσει τον κίνδυνο σε κάποια ασφαλιστική εταιρεία πράγμα που θα μειώσει σημαντικά τις πιθανές οικονομικές επιπτώσεις. Ωστόσο, υπάρχουν και κάποιες επιπτώσεις που επιδρούν στην φήμη της επιχείρησης ή στο ηθικό του ανθρώπινου δυναμικού της, που δεν είναι δυνατόν να αντιμετωπιστούν με αυτόν τον τρόπο.

2.11.7 Εναπομένων κίνδυνος

Η διαχείριση κινδύνων εντοπίζει τους κινδύνους που αντιμετωπίζει η επιχείρηση και τους αξιολογεί. Στη συνέχεια, για την προστασία της επιχείρησης, λαμβάνονται κάποια μέτρα ελέγχου για την μείωση του κινδύνου. Ωστόσο οι παράγοντες που μπορούν να προκαλέσουν ένα κίνδυνο να συμβεί είναι δυνητικά πολλοί, και η επιχείρηση μπορεί να επιλέξει να μην προστατευθεί από όλους, θεσπίζοντας κατάλληλες διαδικασίες ή λαμβάνοντας αντισταθμιστικά για τους κινδύνους μέτρα. Αυτό μπορεί να προέρχεται είτε από το δυσανάλογο ή / και υπέρογκο κόστος των μέτρων σε σχέση με τον κίνδυνο, είτε από τη μικρή πιθανότητα –σύμφωνα με την μελέτη ανάλυσης των κινδύνων που έχει προηγηθεί- να συμβεί ο κίνδυνος.

Όποιος και αν είναι ο λόγος που η διοίκηση αποφασίζει να μην προστατευθεί από έναν παράγοντα που μπορεί να προκαλέσει ένα κίνδυνο να συμβεί, αυτόματα θέ-

τει τη διοίκηση σε θέση να θεωρήσει ένα μέρος του κινδύνου ως αποδεκτό ή εντός των ορίων ανοχής. Αυτό το μέρος του κινδύνου που αποδέχεται και αναλαμβάνει ως ευθύνη η διοίκηση, ονομάζεται εναπομένων κίνδυνος.

Για παράδειγμα ο κίνδυνος να υπάρξει πλημμύρα σε ένα γεωγραφικό τόπο που επικρατούν συνθήκες ανομβρίας τα τελευταία εκατό χρόνια είναι πολύ ασήμαντος και, φυσικά, το κόστος για την κατασκευή εξαντλητικών αντιπλημμυρικών έργων θεωρείται ως μη αποδεκτό και απορρίπτεται. Σε αντίθεση φροντίζει να παρθούν κάποια αποδεκτά σε κόστος έργα για την μικρή πιθανότητα πλημμύρας. Στη περίπτωση αυτή η επιχείρηση αναλαμβάνει το ρίσκο ο κίνδυνος να συμβεί και να μην είναι ολικά προστατευμένη από αυτόν. Αυτό το μικρό ποσοστό που αποφάσισε η επιχείρηση να μην προστατευθεί είναι ο εναπομένων κίνδυνος.

Αυτή η διαδικασία πρέπει να γίνει για κάθε κίνδυνο που αντιμετωπίζει η επιχείρηση και αν θα προσπαθούσαμε να την αποτυπώσουμε με κάποια μαθηματική μορφή, αυτή θα ήταν:

Εναπομένων κίνδυνος = Συνολικός κίνδυνος – Μέτρα αποφυγής κινδύνου

2.11.8 Διαρκής έλεγχος

Η αποτελεσματική διαχείριση των κινδύνων προϋποθέτει τη αναφορά και την επαναξιολόγηση των κινδύνων και των μέτρων αποφυγής τους έτσι ώστε να εξασφαλιστεί ότι όλοι οι κίνδυνοι που τυχόν θα αντιμετωπίσει η επιχείρηση έχουν καλυφθεί με την ανάλογη διαδικασία αντιμετώπισής τους.

Για να επιτευχθεί αυτό, η επιχείρηση θα πρέπει να θεσπίσει πολιτικές συνεχούς ελέγχου για το σύνολο των κινδύνων που αντιμετωπίζει. Δεν θα πρέπει να ξεχνάμε ότι η σύγχρονη επιχείρηση δραστηριοποιείται σε ένα δυναμικό περιβάλλον και οφείλει να είναι και εκείνη δυναμικά τοποθετημένη απέναντι στους κινδύνους που αντιμετωπίζει γιατί αυτοί συνεχώς αλλάζουν, [22]. Κάθε αλλαγή στην αγορά που απευθύνεται η επιχείρηση μπορεί δυνητικά να δημιουργήσει νέους κινδύνους που σαφώς δεν πρέπει να αγνοηθούν. Ομοίως, κάθε εσωτερική αλλαγή στη δομή της επιχείρησης ή πιθανή επέκταση των δραστηριοτήτων της, πρέπει να ενεργοποιή-

σει την επαναξιολόγηση των κινδύνων και των μέτρων αντιμετώπισής τους μέσω της διαδικασίας ανάλυσης κινδύνων που αναλυτικά περιγράψαμε.

Οι πολιτικές ελέγχου που πρέπει να θεσπίσει η επιχείρηση έχουν σκοπό να παρέχουν εύλογη επιβεβαίωση στην επιχείρηση για τα μέτρα προστασίας και ανάκαμψης από τους κινδύνους που η επιχείρηση αντιμετωπίζει. Κάθε προσπάθεια διαδικασίας ελέγχου πρέπει να εξετάζει αν τα μέτρα που έχουν ληφθεί είναι αυτά που είχαν αποφασιστεί και, φυσικά, εάν εφαρμόζονται. Εν συνεχεία θα πρέπει να εξετάσει αν οι διαδικασίες που υιοθετήθηκαν για την ανάληψη του κινδύνου ήταν οι πρέπουσες, αν υπήρχαν πληροφορίες που θα οδηγούσαν σε διαφορετικό αποτέλεσμα, αναφορικά με την ανάληψη κινδύνου ή τη λήψη μέτρων αντιμετώπισής του, και δεν χρησιμοποιήθηκαν ή ανακοινώθηκαν και τέλος να κάνει προτάσεις προς τη διοίκηση για μελλοντική βελτίωση των μέτρων που εξετάζει.

2.12 Σύνοψη

Ο κίνδυνος συστημάτων πληροφορικής, θεωρείται ως επιχειρηματικός κίνδυνος και αποτελεί ένα κομμάτι του συνολικού κινδύνου μιας επιχείρησης. Άλλοι επιχειρηματικοί κίνδυνοι είναι: στρατηγικοί κίνδυνοι, κίνδυνοι για το περιβάλλον, κίνδυνοι αγοράς, πιστωτικοί κίνδυνοι, λειτουργικοί κίνδυνοι και κίνδυνοι από μη συμμόρφωση σε κανονιστικά πλαίσια. Σε πολλές επιχειρήσεις οι κίνδυνοι που σχετίζονται με τα συστήματα πληροφορικής, θεωρούνται ως κομμάτι του λειτουργικού κινδύνου, για παράδειγμα στον χρηματοπιστωτικό τομέα στο πλαίσιο της Βασιλείας ΙΙ [23]. Ωστόσο, ακόμη και ο στρατηγικός κίνδυνος μπορεί να έχει ένα σκέλος κινδύνου συστημάτων πληροφορικής, ειδικά όταν πρόκειται για το βασικό μοχλό για νέες επιχειρηματικές πρωτοβουλίες. Το ίδιο ισχύει και για τον πιστωτικό κίνδυνο, όπου η μη επαρκής ασφάλεια των συστημάτων πληροφορικής μπορεί να οδηγήσει σε χαμηλότερη πιστοληπτική φερεγγυότητα. Για το λόγο αυτό, είναι καλύτερα να μην θεωρείται ο κίνδυνος των συστημάτων πληροφορικής, ως μια ιεραρχική εξάρτηση από τις άλλες περιοχές κινδύνου.

Παρόλο που ο «Κίνδυνος Συστημάτων Πληροφορικής» είναι βασισμένος πάνω στα πρότυπα διαχείρισης «Συνολικού Επιχειρηματικού Κινδύνου», η ύπαρξη ενός

προτύπου διαχείρισης συνολικού επιχειρηματικού κινδύνου δεν αποτελεί προϋπόθεση για την υιοθέτηση ενός προτύπου για την αντιμετώπιση κινδύνων σχετικών με τα συστήματα πληροφορικής. Με την εφαρμογή του πλαισίου αρχών για τον κίνδυνο των συστημάτων πληροφορικής οι επιχειρήσεις αυτομάτως θα εφαρμόσουν και τις αρχές που διέπουν το πρότυπο διαχείρισης Συνολικού Επιχειρηματικού Κινδύνου.

Στις περιπτώσεις που υπάρχει ενεργό κάποιο πρότυπο διαχείρισης του Συνολικού Επιχειρηματικού Κινδύνου, είναι σημαντικό να αξιοποιηθούν τα πλεονεκτήματα του υπάρχοντος προτύπου, γιατί αυτό θα αυξήσει την αποδοχή του, θα διευκολύνει την υιοθέτηση του προτύπου διαχείρισης συστημάτων πληροφορικής, θα εξοικονομήσει χρόνο και χρήματα και θα βοηθήσει να αποφευχθούν παρανοήσεις σχετικά με συγκεκριμένους κινδύνους των συστημάτων πληροφορικής που μπορεί να είναι μέρος του συνολικού επιχειρηματικού κινδύνου.

Ο κίνδυνος των συστημάτων πληροφορικής, βασίζεται σε μια σειρά από κατευθυντήριες αρχές για την αποτελεσματική διαχείριση του συνολικού επιχειρηματικού κινδύνου. Οι αρχές αυτές βασίζονται σε ευρέως αποδεκτούς κανόνες, οι οποίοι έχουν εφαρμοστεί με επιτυχία στον τομέα της πληροφορικής. Το μοντέλο της διαχείρισης του κινδύνου συστημάτων πληροφορικής πρέπει να είναι έτσι σχεδιασμένο και δομημένο ώστε να επιτρέπει στις επιχειρήσεις να εφαρμόζουν τις αρχές στην πράξη και να συγκρίνουν τις επιδόσεις τους.

Ο κίνδυνος συστημάτων πληροφορικής έχει σχέση με τον κίνδυνο που σχετίζεται με τη χρήση της πληροφορικής. Η σύνδεση με τον συνολικό επιχειρηματικό κίνδυνο βασίζεται στις αρχές επί των οποίων το πλαίσιο είναι χτισμένο, δηλαδή, την αποτελεσματική διακυβέρνηση των επιχειρήσεων και τη διαχείριση των κινδύνων συστημάτων πληροφορικής.

Για την καλύτερη διαχείριση των κινδύνων των συστημάτων πληροφορικής, η παρούσα έρευνα προτείνει τη υιοθέτηση ενός νέου τρόπου ποσοτικοποίησης του επιπέδου της ασφάλειας των συστημάτων πληροφορικής που διαθέτει, με τη χρήση στοχαστικών μεθόδων. Με τον τρόπο αυτό θα είναι πλέον εφικτό να γνωρίζουμε ανά πάσα στιγμή ποιος είναι ο εναπομένων κίνδυνος που αναλαμβάνει η

επιχείρηση να καλύψει, στην περίπτωση που κάποιος από τους κινδύνους των συστημάτων πληροφορικής γίνει πραγματικότητα. Αυτή η σημαντική πληροφορία, είναι απολύτως απαραίτητη για την χάραξη μίας σωστής στρατηγικής από την πλευρά της Διοίκησης, τόσο σε επίπεδο διαχείρισης πόρων, ανθρώπινων και μη, όσο και για τη μείωση του κόστους για την αντιμετώπιση των κινδύνων που αντιμετωπίζει.

ΚΕΦΑΛΑΙΟ 3: Στοχαστικές διαδικασίες

3. Η κίνηση Brown

Η κίνηση Brown αποτελεί μία από τις πιο σημαντικές στοχαστικές διαδικασίες και πολλές φορές στην βιβλιογραφία αναφέρεται ως κίνηση Wiener. Έχει ιδιαίτερο ενδιαφέρον από θεωρητικής πλευράς και έχει χρησιμοποιηθεί σε πολλές πρακτικές εφαρμογές. Στο πλαίσιο της παρούσας έρευνας, η κίνηση Brown θα χρησιμοποιηθεί για να προσομοιώσουμε ένα τυχαίο περίπατο (random walk), στο χρονικό διάστημα μέσα στο οποίο θέλουμε να μετρήσουμε το επίπεδο ασφάλειας ενός συστήματος, και χρησιμοποιώντας την κίνηση αυτή θα υπολογίσουμε το κατά Itô στοχαστικό ολοκλήρωμα. Η στοχαστική αυτή διαδικασία, εφαρμόζεται στην θεωρία των στοχαστικών διαφορικών εξισώσεων και θεωρείται ως ο ακρογωνιαίος λίθος στα χρηματοοικονομικά μαθηματικά σχετικά με τα μοντέλα σε συνεχή χρόνο.

Εκτός από τη σχετικότητα, ο Αϊνστάιν εξήγησε και την κίνηση Brown, το «χορό» των μικροσκοπικών σωματιδίων όταν αυτά αιωρούνται μέσα σε ρευστά, δείχνοντας ότι οι συγκρούσεις με περιβάλλοντα σωματίδια θα μπορούσαν να προκαλούν τέτοιες τυχαίες άτακτες κινήσεις. Οι θεωρητικοί φυσικοί ισχυρίζονταν ότι η κίνηση Brown μπορεί και να μην είναι εντελώς τυχαία όπως προέβλεπε ο Αϊνστάιν, και τώρα οι πειραματικοί το επιβεβαιώνουν. Με τη βοήθεια λέιζερ παρακολούθησαν πλαστικές και γυάλινες σφαίρες διαστάσεων μικρομέτρου μέσα σε νερό, ανά διαστήματα μικροδευτερολέπτου και σε νανομετρικές κλίμακες.

Τα αποτελέσματα επιβεβαιώνουν μια διορθωμένη μορφή της καθιερωμένης θεωρίας που περιγράφει την κίνηση Brown, σύμφωνα με την οποία η αδράνεια του ρευστού καθιστά τις τροχιές των σωματιδίων περισσότερο προβλέψιμες και για πολύ μεγαλύτερο χρονικό διάστημα από όσο αναμενόταν μέχρι τότε. Τα ευρήματα, τα οποία δημοσιεύονται και στην ιστοσελίδα του περιοδικού Physical Review Letters [24], έχουν θεμελιώδη σημασία για την κατανόηση της δυναμικής των ζωντανών κυττάρων, καθώς και για την κατασκευή δομών σε νανομετρική κλίμα-

κα, δηλώνει ο βιοφυσικός Ernst-Ludwig Florin, του Πανεπιστημίου τού Τέξας στο Ώστιν

3.1 Ορισμός της κίνησης Brown

Η κίνηση Brown είναι μια στοχαστική διαδικασία B_t η οποία παίρνει τιμές στον R και έχει τις ακόλουθες ιδιότητες:

i. Αν $t_0 < t_1 < \cdots < t_n$ τότε οι τυχαίες μεταβλητές B_{t_0}, $B_{t_1} - B_{t_0}$, $B_{t_n} - B_{t_{n-1}}$ είναι ανεξάρτητες (ανεξάρτητες μεταβολές).

ii. Αν $s, t \geq 0$, , τότε

$$P(B_{s+t} - B_s \in A) = \int_A \frac{1}{(2\pi t)^{1/2}} \exp\left(-\frac{|x|^2}{2t}\right),$$

όπου Α κάποιο σύνολο Borel. Δηλαδή οι μεταβολές της κίνησης Brown είναι κατανεμημένες με την κανονική κατανομή Gauss.

iii. Οι τροχιές της κίνησης Brown είναι συνεχείς, με πιθανότητα 1, δηλαδή η $t \to B_t$ είναι συνεχής συνάρτηση.

Οι τρείς αυτές ιδιότητες ορίζουν μία και μοναδική στοχαστική διαδικασία. Αποδεικνύεται με αυστηρά μαθηματικά η ύπαρξη μίας στοχαστικής διαδικασίας με τις παραπάνω ιδιότητες.

Από τις ιδιότητες της κίνησης Brown μπορούμε να οδηγηθούμε στις ιδιότητες του μέτρου μ που αυτή επάγει (μέτρο Wiener):

$$\mu_{t_1, t_2, \ldots, t_n}(A_1 \ x \ A_2 \ x \ \ldots \ x \ A_n) =$$

$$= \int_{A_1} dx_1 \int_{A_2} dx_2 \ldots \int_{A_n} dx_n \prod_{i=1}^{n} p(t_i - t_{i-1,} x_{i-1}, x_i),$$

όπου $x_0 = x, \ t_1 = 0$, και

$$p(t,x,y) = P(B_{s+t} - B_s \in A) =$$

$$= \frac{1}{(2\pi t)^{1/2}} \exp\left(-\frac{|y-x|^2}{2t}\right),$$

Η παραπάνω ποσότητα είναι η πιθανότητα να βρίσκεται η στοχαστική διαδικασία τις χρονικές στιγμές t_i στα υποσύνολα $A_i \in B(R)$. Μπορούμε να σκεφτούμε τα υποσύνολα αυτά ως διαστήματα του R οπότε και η παραπάνω ποσότητα είναι ουσιαστικά η πιθανότητα να βρίσκεται η κίνηση Brown τις χρονικές στιγμές t_i σε συγκεκριμένα διαστήματα του R. Η ποσότητα

$$\mu_{t_1, t_2, \dots, t_n}(A_1 \times A_2 \times \dots \times A_n) =$$
$$= P(B_{t_1} \in A_1, B_{t_2} \in A_2, \dots, B_{t_n} \in A_n)$$

ονομάζεται πεπερασμένης διάστασης κατανομή και η γνώση της είναι πολύ σημαντική στο να κατασκευάσουμε το μέτρο μ (θεώρημα επέκτασης του Kolmogorov).

Η κατανομή του B_t εξαρτάται από το αρχικό σημείο στο οποίο ξεκινάμε τη διαδικασία, δηλαδή το σημείο B_0. Αν $B_0 = x$ τότε η συνάρτηση κατανομής θα συμβολίζεται $P_x(B_t \in A)$ για κάποιο σύνολο Borel A. Η μέση τιμή ή υπό συνθήκη μέση τιμή ως προς το μέτρο αυτό, θα συμβολίζεται E_x ή $E_x[\cdot]$ αντιστοίχως.

Πρέπει να σημειωθεί ότι ακολουθούμε την σύμβαση να αφήνουμε την κίνηση Brown να ξεκινάει σε οποιοδήποτε σημείο x και όχι μόνο στο 0. Το σημείο που θα ξεκινάει η κίνηση Brown θα γίνεται σαφές στο μέτρο πιθανότητας που θα χρησιμοποιείται και αν δεν αναφέρεται τίποτα θα εννοείται ότι ξεκινάμε από το 0. Η κίνηση Brown που ξεκινάει στο 0 συνήθως αναφέρεται και ως τυπική (standard) κίνηση Brown.

Ένα βασικό σημείο που πρέπει να γνωρίζουμε είναι αν μία κίνηση που μελετάμε είναι κίνηση Brown ή όχι. Στο σημείο αυτό θα παρουσιάσουμε ένα τρόπο ελέγχου για να ελέγξουμε μία στοχαστική διαδικασία αν είναι κίνηση Brown ή όχι. Ο προτεινόμενος τρόπος βασίζεται σε ένα θεμελιώδες αποτέλεσμα που οφείλεται στον Paul Levy και χαρακτηρίζει την κίνηση Brown χρησιμοποιώντας ουσιαστικά τις

ιδιότητες *martingale* που αυτή έχει. Θα παραθέσουμε αυτό το θεώρημα ως έχει αφού η απόδειξή του κινείται εκτός των ορίων της παρούσης έρευνας.

3.2 Θεώρημα Paul Levy

Έστω $X_t, t \geq 0$ μία στοχαστική διαδικασία και $G_t = \sigma(X_s, s \leq t)$ η διήθηση που παράγεται από αυτή. Η X_t είναι μία κίνηση Brown αν και μόνο αν ισχύουν οι ακόλουθες συνθήκες:

i. $X_0 = 0$

ii. Οι τροχιές της στοχαστικής διαδικασίας X_t είναι συνεχείς συναρτήσεις χρόνου.

iii. Η X_t είναι μια στοχαστική διαδικασία τύπου martingale ως προς τη διήθηση $G_t = \sigma(X_s, s \leq t)$.

iv. Η $X_t^2 - t$ είναι μια στοχαστική διαδικασία τύπου martingale ως προς τη διήθηση $G_t = \sigma(X_s, s \leq t)$.

Το θεώρημα αυτό χαρακτηρίζει την κίνηση Brown ουσιαστικά από την μέση τιμή της και τη διακύμανση. Συγκεκριμένα μπορούμε να αντικαταστήσουμε τις συνθήκες (iii & iv) του παραπάνω θεωρήματος με τις ακόλουθες συνθήκες:

v. Η στοχαστική διαδικασία X_t έχει στάσιμες (stationary) και ανεξάρτητες μεταβολές.

vi. Οι μεταβολές της στοχαστικής διαδικασίας $X_t - X_s, s < t$ είναι κατανεμημένες με την κανονική κατανομή με μέσο 0 και διασπορά t – s.

Επίσης η συνθήκη (iv) μπορεί να αντικατασταθεί από μία συνθήκη σχετικά με την τετραγωνική μεταβολή της στοχαστικής διαδικασίας τύπου martingale X_t και συ-

γκεκριμένα από την $< X_t > = t$. Το θεώρημα αυτό είναι ιδιαίτερα χρήσιμο και θα το χρησιμοποιήσουμε στην έρευνά μας για να υπολογίσουμε το επίπεδο ασφάλειας ενός συστήματος πληροφορικής.

3.3 Ιδιότητες των τροχιών της κίνησης Brown

Οι τροχιές της κίνησης Brown έχουν μερικές χαρακτηριστικές ιδιότητες, η μελέτη των οποίων έχει απασχολήσει πολλούς ερευνητές της μαθηματικής κοινότητας. Στο σημείο αυτό θα παρουσιάσουμε μόνο τις πιο σημαντικές και χωρίς να τις συνοδεύουμε από την αντίστοιχη απόδειξή τους αφού κάτι τέτοιο ξεφεύγει από το πλαίσιο της παρούσας διατριβής.

Η κίνηση Brown έχει τις ακόλουθες ιδιότητες:

i. Η τετραγωνική μεταβολή της κίνησης Brown στο διάστημα $[0,\ t]$ είναι ίση με t.

ii. Η μεταβολή της κίνησης Brown είναι άπειρη.

Η (i) προκύπτει από το ότι η στοχαστική διαδικασία $B_t^2 - t$ είναι τύπου martingale. Αντίστοιχα η (ii) προκύπτει από το ότι η στοχαστική διαδικασία B_t είναι τύπου συνεχούς martingale.

Το γεγονός ότι η μεταβολή της κίνησης Brown είναι άπειρη είναι ιδιαίτερα σημαντικό. Λόγω της ιδιότητας αυτής δεν μπορούμε να ορίσουμε το ολοκλήρωμα μίας συνάρτησης f επάνω στην κίνηση Brown,

$$\int f(s,\omega)dB_s$$

σαν ένα ολοκλήρωμα Riemann – Stieljes αλλά θα πρέπει να βρούμε ένα εναλλακτικό τρόπο ορισμού του, έτσι ώστε το ολοκλήρωμα αυτό να έχει νόημα. Θα επανέλθουμε σε αυτό όταν θα παραθέσουμε την έννοια του στοχαστικού ολοκληρώματος Itô, παράγραφο § 3.5.

3.4 Πολυδιάστατη κίνηση Brown

Αφού έχουμε ορίσει την κίνηση Brown και τα θεωρήματα που τη διέπουν, μπορούμε πλέον να ορίσουμε και την πολυδιάστατη κίνηση Brown η οποία μπορεί να οριστεί με δύο τρόπους.

3.4.1 Πρώτος ορισμός της πολυδιάστατης κίνησης Brown

Η κίνηση Brown d-διαστάσεων είναι η σχετική στοχαστική διαδικασία $B_t = (B_{1,t}, B_{2,t}, \dots, B_{d,t})$ $όπου$ $B_{i,t}, i = 1,2, \dots, d$ είναι ανεξάρτητες μεταξύ τους κινήσεις Brown.

Οι ιδιότητες της πολυδιάστατης κίνησης Brown μπορεί να συναχθούν από τις ιδιότητες των επιμέρους μονοδιάστατων κινήσεων που την αποτελούν.

3.4.2 Δεύτερος ορισμός της πολυδιάστατης κίνησης Brown

Μια d-διάστατη κίνηση Brown είναι μια στοχαστική διαδικασία B_t η οποία παίρνει τιμές στον R^d και που έχει τις ακόλουθες ιδιότητες.

i. Αν το $t_0 < t_1 < \cdots < t_n$, τότε οι διανυσματικές τυχαίες μεταβλητές B_{t_0}, $B_{t_1} - B_{t_0}$, $B_{t_n} - B_{t_{n-1}}$, είναι ανεξάρτητες, (ανεξάρτητες αυξήσεις).

ii. Εάν $s, t \geq 0$, τότε

$$P(B_{s+t} - B_s \in A) = \int_A \frac{1}{(2\pi t)^{d/2}} \exp\left(-\frac{|x|^2}{2t}\right),$$

όπου $A \in B(R^d)$. Οι αυξήσεις της κίνησης Brown σε d-διαστάσεις είναι κατανεμημένες με την κανονική κατανομή σε d-διαστάσεις Gauss.

iii. Οι τροχιές της κίνησης Brown είναι συνεχείς με πιθανότητα 1, δηλαδή η συνάρτηση $t \rightarrow B_t$ είναι συνεχής.

Οι τρείς αυτές ιδιότητες ορίζουν μία και μοναδική στοχαστική διαδικασία. Η ύπαρξη της στοχαστικής διαδικασίας με τις παραπάνω ιδιότητες μπορεί να γίνει χρησιμοποιώντας γενικεύσεις των τρόπων απόδειξης της ύπαρξης της μονοδιάστατης κίνησης Brown.

Από τις ιδιότητες της κίνησης Brown μπορούμε να καταλήξουμε στις ιδιότητες του μέτρου που προέρχεται από την κίνηση Brown στις d-διαστάσεις:

$$\mu_{t_1,\, t_2,\ldots,t_n}(A_1 \times A_2 \times \ldots \times A_n) =$$

$$= \int_{A_1} dx_1 \int_{A_2} dx_2 \ldots \int_{A_n} dx_n \prod_{i=1}^{n} p\big(t_i - t_{i-1,}\, x_{i-1}, x_i\big),$$

όπου $x_0 = x \in R^d,\ t_1 = 0, A_i \in B(R^d),\ i = 1,2,\ldots,n$ και

$$p(t,x,y) = \frac{1}{(2\pi t)^{d/2}} \exp\left(-\frac{|y-x|^2}{2t}\right).$$

Με τον συμβολισμό |x| εννοούμε την Ευκλείδια νόρμα στον R^d. Η ποσότητα $\mu_{t_1,\, t_2,\ldots,t_n}(A_1 \times A_2 \times \ldots \times A_n)$ είναι η πιθανότητα να βρίσκεται η στοχαστική διαδικασία B_tτις χρονικές στιγμές t_i στα υποσύνολα A_i που ανήκουν στο σύνολο Borel που παράγεται από το R^d. Η ποσότητα αυτή ονομάζεται πεπερασμένης διάστασης κατανομή και η γνώση της είναι πολύ σημαντική στο να κατασκευάσουμε το μέτρο μ.

Η πολυδιάστατη κίνηση Brown έχει πολλές από τις ιδιότητες της μονοδιάστατης κίνησης Brown. Έτσι για παράδειγμα έχουμε την ιδιότητα Markov και την ισχυρή ιδιότητα Markov, τις ιδιότητες martingale της κίνησης Brown και των διαφόρων συναρτήσεών της. Πιο ειδικά μπορούμε να δούμε το θεώρημα Paul Levy για την κίνηση Brown σε περισσότερες της μίας διάστασης.

3.5 Το στοχαστικό ολοκλήρωμα Itô

Τα ολοκληρώματα πάνω στην κίνηση Brown είναι ιδιαίτερα χρήσιμα όταν χρειάζεται να μελετήσουμε την θεωρία των διαχύσεων ή τις στοχαστικές εξισώσεις, [25]. Στο σημείο αυτό θα παρουσιάσουμε πώς μπορούμε να ορίσουμε το ολοκλήρωμα πάνω στην κίνηση Brown χρησιμοποιώντας τον τρόπο που υπέδειξε τη δεκαετία του 1940 ο Ιάπωνας μαθηματικός Kyoshi Itô καθώς και άλλους εναλλακτικούς τρόπους ορισμού στοχαστικών ολοκληρωμάτων. Στο πλαίσιο της παρούσας ερευνητικής προσπάθειας, θα χρησιμοποιήσουμε το κατά Itô ολοκλήρωμα για να υπολογίσουμε το επίπεδο ασφάλειας ενός συστήματος πληροφορικής.

Ας θεωρήσουμε ότι έχουμε μια τυχαία συνάρτηση f η οποία εξαρτάται με κάποιο τρόπο από την έκβαση κάποιας κίνησης Brown και θέλουμε να ορίσουμε το ολοκλήρωμά της επάνω στις μεταβολές της κίνησης Brown. Αυτό σημαίνει ότι θέλουμε να ορίσουμε το ολοκλήρωμα

$$\int_a^b f(t,\omega)\, dB_t(\omega),$$

όπου $B_t(\omega)$ είναι μία μονοδιάστατη κίνηση Brown που ξεκινάει από το 0 και f μία συνάρτηση $f: (0,\infty) \times \Omega \rightarrow R$.

Θεωρούμε ότι ο (Ω, F, P) είναι ένας χώρος πιθανοτήτων. Η εξάρτηση της συνάρτησης από την τυχαία μεταβλητή και, συγκεκριμένα, από την κίνηση Brown υπάρχει λόγω του ω.

Ας θεωρήσουμε τη διαμέριση $a = t_0 < t_1 < \cdots < t_n = b$ του διαστήματος [a, b] και ότι προσεγγίζουμε την συνάρτηση $f(t,\omega)$ ως

$$f(t,\omega) \cong \sum_{i=1}^{n-1} f(t_i,\omega)\, 1_{[t_i,t_{i+1})}(t),$$

Το ολοκλήρωμα Itô μπορεί να ορισθεί ως το όριο στον L^2

$$\int_a^b f(t,\omega)\, dB_t(\omega) = \lim_{n\to\infty} \sum_{i=1}^{n} f(t_i,\omega)[B_{t_{i+1}} - B_{t_i}](\omega),$$

Η τιμή της συνάρτησης f την χρονική στιγμή t θα πρέπει να εξαρτάται από τις τιμές του $B_s\ \gamma\iota\alpha\ s \le t\ \alpha\lambda\lambda\acute{\alpha}\ \acute{o}\chi\iota\ \gamma\iota\alpha\ s\ \ge t$

Το όριο λαμβάνεται κατά την L^2 έννοια και όχι σημειακά δηλαδή για κάθε ω.

Τα δύο παραπάνω σημεία είναι ιδιαίτερα σημαντικά και διαφοροποιούν το ολοκλήρωμα Itô από άλλους ορισμούς στοχαστικών ή/και ντετερμινιστικών ολοκληρωμάτων.

Με παρόμοιο τρόπο μπορεί να οριστεί ολοκλήρωμα

$$\int_a^b f(t,\omega)\, dX_t,$$

Επάνω σε πιο γενικές στοχαστικές διαδικασίες X_t. Μία ιδιαίτερα ενδιαφέρουσα περίπτωση είναι η περίπτωση που η X_t είναι στοχαστική συνάρτηση τύπου martingale.

3.6 Ορισμός διαδικασίας βήματος

Μία στοχαστική διαδικασία f η οποία μπορεί να γραφτεί με την μορφή

$$f(t) = \sum_{j=1}^{n-1} n_j\, 1_{[t_j,t_{j+1})}(t),$$

για κάποια διαμέριση $a = t_0 < t_1 < \cdots < t_n = b$ του διαστήματος [a, b] όπου n_j τυχαίες μεταβλητές οι οποίες είναι F_{t_j} μετρήσιμες και $E\left[n_j^2\right] < \infty$ ονομάζεται διαδικασία βήματος. Θα συμβολίζουμε με $M_{step}([a,b])$ το σύνολο των διαδικασιών βήματος στο διάστημα [a, b].

3.7 Ιδιότητες του ολοκληρώματος του Itô

Το ολοκλήρωμα του Itô έχει τις ακόλουθες ιδιότητες:

1) Είναι γραμμικό, δηλαδή για δύο στοχαστικές διαδικασίες $f_1 και\, f_2$ ισχύει $I(\lambda_1 f_1 + \lambda_2 f_2) = \lambda_1 I(f_1) + \lambda_2 I(f_2)$, όπου $\lambda_1, \lambda_2 \in R$.

$$E\left[\int_a^b f\, dB_t\right] = 0$$

2)

$$E\left[\left|\int_a^b f(t,\omega) dB_t\right|^2\right] = E\left[\int_a^b |f(t,\omega)|^2\, dt\right]$$

Η ιδιότητα αυτή ονομάζεται ισομετρία του Itô.

Σε όλα τα παραπάνω θεωρούμε ότι η συνάρτηση την οποία ολοκληρώνουμε ανήκει στον κατάλληλο χώρο M^2.

3.8 Το ολοκλήρωμα Itô σαν στοχαστική διαδικασία

Στις προηγούμενες παραγράφους ορίσαμε και είδαμε τις ιδιότητες του στοχαστικού ολοκληρώματος κατά Itô όταν τα όρια της ολοκλήρωσης a και b ήταν δεδομένα. Αν θεωρήσουμε όμως ότι ενώ το κάτω όριο της ολοκλήρωσης παραμένει σταθερό, και χωρίς βλάβη της γενικότητας μπορούμε να το θέσουμε a=0, επιτρέπουμε το επάνω όριο της ολοκλήρωσης να μεταβάλλεται και να είναι b = t.

Μπορούμε λοιπόν να θεωρήσουμε το στοχαστικό ολοκλήρωμα

$$\int_0^t f(t)\, dB_t,$$

όπου $0 \leq t \leq T$. Για κάθε τιμή του t το ολοκλήρωμα ορίζεται όπως και παραπάνω αρκεί η στοχαστική διαδικασία $f \in M^2([0,T])$. Συνεπώς με την παραπάνω κατασκευή, για κάθε τιμή του t παίρνουμε μία τυχαία μεταβλητή η οποία είναι τετραγωνικά ολοκληρώσιμη και η τιμή της είναι ίση με το ολοκλήρωμα

$$\int_0^t f(t)\, dB_t.$$

Άρα κατασκευάζουμε μία στοχαστική διαδικασία

$$I_t := \int_0^t f(t)\, dB_t.$$

Η στοχαστική διαδικασία αυτή ονομάζεται το αόριστο ολοκλήρωμα του Itô. Η παραπάνω στοχαστική διαδικασία, ισοδύναμα μπορεί να οριστεί σαν το στοχαστικό ολοκλήρωμα από 0 έως το T της $f(t)1_{[0,t]}(s)dB_s$, δηλαδή

$$\int_0^t f(s)\, dB_s = \int_0^T f(s)\, 1_{[0,t]}(s) dB_s$$

Με βάση τις ιδιότητες του στοχαστικού ολοκληρώματος μπορούμε να δείξουμε τις παρακάτω ιδιότητες για την στοχαστική διαδικασία I_t:

1) Η στοχαστική διαδικασία I_t είναι μια τετραγωνικά ολοκληρώσιμη martingale.

2) Η διαδικασία τετραγωνικής μεταβολής της I_t είναι

$$< I >_t = \int_0^t |f(s)|^2\, ds$$

3.9 Διαδικασίες Itô

Κάνοντας χρήση του στοχαστικού ολοκληρώματος Itô μπορούμε να ορίσουμε μία νέα κατηγορία γενικότερων στοχαστικών διαδικασιών από την κίνηση Brown, τις διαδικασίες Itô.

3.9.1 Ορισμός διαδικασίας Itô

Μία διαδικασία Itô είναι μία στοχαστική διαδικασία X_t της μορφής

$$X_t = X_0 + \int_0^t u(s,\omega)ds + \int_0^t v(s,\omega)dB_{s,}$$

όπου *u* και *v* ικανοποιούν τις συνθήκες:

$$\int_0^t v^2(s,\omega)ds < \infty, \int_0^t u(s,\omega)ds < \infty.$$

Η διαδικασία αυτή μπορεί να γραφτεί και σε διαφορική μορφή

$$dX_t = udt + vdB_t$$

3.10 Χρησιμοποίηση της διαδικασίας Itô σε μονοδιάστατη κίνηση Brown

Μία μονοδιάστατη κίνηση Brown με ταχύτητα *m* είναι μία διαδικασία Itô. Πραγματικά, για τη διαδικασία αυτή έχουμε ότι $X_t = X_0 + mt + B_t$ η οποία μπορεί να γραφτεί ισοδύναμα

$$X_t = X_0 + \int_0^t mds + \int_0^t dB_s,$$

ή σε διαφορική μορφή

$$dX_t = mdt + dB_t$$

3.11 Ο τύπος του Itô

Ένα ενδιαφέρον ερώτημα, είναι τι μορφή έχει μία συνάρτηση μιας διαδικασίας Itô, δηλαδή αν θα είναι και αυτή με τη σειρά της μια διαδικασία Itô και αν ναι, ποια θα είναι η ακριβή της μορφή, σαν το άθροισμα ενός ολοκληρώματος Riemman και ενός ολοκληρώματος Itô.

Η απάντηση σε αυτό το ερώτημα δίνεται από το περίφημο Λήμμα του Itô, το οποίο μας προσφέρει έναν κανόνα αλλαγής μεταβλητών τροποποιημένο κατάλληλα ώστε να ισχύει για στοχαστικά ολοκληρώματα.

3.12 Το Λήμμα του Itô

Έχοντας μελετήσει αρκετά στοιχεία για το ολοκλήρωμα Itô, ήρθε η σειρά να παρουσιάσουμε μία νέα κατηγορία στοχαστικών διαδικασιών οι οποίες έχουν σημαντικές εφαρμογές στα χρηματοοικονομικά, τις διαδικασίες Itô, και να μελετήσουμε και τη σημαντικότερη ιδιότητα που τις χαρακτηρίζουν, δηλαδή το λήμμα του Itô [26], το οποίο χαρακτηρίζει τις ιδιότητες των διαδικασιών Itô κάτω από αλλαγή μεταβλητών.

Θεωρούμε ότι η X_t είναι μία στοχαστική διαδικασία Itô που μπορεί να εκφραστεί ως

$$X_t = X_0 + \int_0^t u(s,\omega)ds + \int_0^t v(s,\omega)dB_s$$

τότε οποιαδήποτε συνάρτηση της X_t της μορφής $g(t,x) \in C^{1,2}$ μπορεί να εκφραστεί επίσης ως ένα στοχαστικό ολοκλήρωμα της μορφής

$$g(t,X_t) = g(0,X_0) + \int_0^t \left(\frac{\partial g}{\partial s} + u\frac{\partial g}{\partial x} + \frac{1}{2}v^2\frac{\partial^2 g}{\partial x^2}\right)ds + \int_0^t v\frac{\partial g}{\partial x}\, dB_s$$

Το παραπάνω αποτέλεσμα μπορεί να γραφεί και σε ισοδύναμη διαφορική μορφή:

$$dg(t,X_t) = \left(\frac{\partial g}{\partial t} + u\frac{\partial g}{\partial x} + \frac{1}{2}v^2\frac{\partial^2 g}{\partial x^2}\right)dt + v\frac{\partial g}{\partial t}\, dB_t$$

Με $C^{1,2}$ συμβολίζουμε το χώρο των συναρτήσεων g(t, x) που έχουν συνεχή την πρώτη παράγωγο ως προς την πρώτη μεταβλητή και συνεχή δεύτερη παράγωγο ως προς τη δεύτερη μεταβλητή.

ΚΕΦΑΛΑΙΟ 4: Έρευνες στην ποσοτικοποίηση της ασφάλειας

4. Διασφάλιση της πληροφορίας και ποσοτικοποίηση της ασφάλειας

Η μεγάλη ανάπτυξη της ζήτησης για απομακρυσμένες συνδέσεις, η ανάγκη για πολύπλοκη επεξεργασία των πληροφοριών, ο όγκος των διακινούμενων πληροφοριών, η ανάπτυξη νέων τεχνολογιών δικτύωσης, η ραγδαία αύξηση των χρηστών και η παγκόσμια εξάρτηση από το διαδίκτυο είναι μερικοί από τους παράγοντες που έχουν οδηγήσει στην αύξηση των ευπαθειών των δομών των συστημάτων πληροφορικής (IT infrastructure), που με τη σειρά τους οδήγησαν στην εμφάνιση πιο εξελιγμένων και στοχευμένων επιθέσεων (attacks). Παρόλο που η χρηματοδότηση σε έργα έρευνας και ανάπτυξης μηχανισμών διασφάλισης της πληροφορίας (information assurance) και μέτρων άμυνας (counter measures) έναντι των επιθέσεων, έχει αυξηθεί τα τελευταία χρόνια, οι αναφορές για επιθέσεις και καταστροφές στα συστήματα πληροφορικής αυξάνονται με καταιγιστικούς ρυθμούς.

Τόσο για τη διασφάλιση της πληροφορίας όσο και για την προστασία των επενδύσεων στα συστήματα πληροφορικής έχουν αναπτυχθεί διάφορες στρατηγικές, μέθοδοι και εργαλεία από τη διεθνή κοινότητα των ερευνητών αλλά και των εταιριών. Παρόλα αυτά, δεν υπάρχουν κοινά αναγνωρισμένες, αξιόπιστες και επεκτάσιμες μέθοδοι για τη μέτρηση του επιπέδου ασφάλειας των συστημάτων πληροφορικής. Η επιτυχία των υπευθύνων ασφαλείας συστημάτων πληροφορικής εξαρτάται τόσο από την ικανότητά τους να αξιολογήσουν σε πραγματικό χρόνο (real time) την κατάσταση ασφαλείας των τοπικών υποδομών τους, όσο και από την κατανόηση που έχουν αναφορικά με την κατάσταση ασφαλείας στα εθνικά ή/και παγκόσμια δίκτυά τους.

Στο σημείο αυτό της παρούσης έρευνας, θα αναφερθούν διάφορες προσεγγίσεις που έχουν γίνει από τη διεθνή κοινότητα των ερευνητών, για την αντιμετώπιση του προβλήματος της μέτρησης του επιπέδου ασφαλείας ενός συστήματος πλη-

ροφορικής. Ενώ, έχουν γίνει κάποιες προσπάθειες προς την σωστή κατεύθυνση, έχουν ακόμα να γίνουν πολλά για να επιτευχθεί ο στόχος της μέτρησης –ποσοτικοποίησης- της ασφάλειας ενός συστήματος σε πραγματικό χρόνο. Εάν αυτό επιτευχθεί, θα βοηθήσει στην κατανόηση, βελτίωση και πρόβλεψη, του επιπέδου ασφαλείας των συστημάτων πληροφορικής.

Ο χώρος της διασφάλισης της πληροφορίας και της ποσοτικοποίησης της ασφάλειας καλύπτει διάφορους τομείς ενδιαφέροντος και συνεχώς εξελίσσεται. Παράδειγμα τέτοιων τομέων είναι η ασφάλεια των συστημάτων (system security), η διασφάλιση της ποιότητας του λογισμικού (software assurance) και η προστασία της ιδιωτικότητας (privacy). Το σημείο «εκκίνησης», από το οποίο ξεκίνησαν να εξελίσσονται οι διάφοροι τομείς, θα πρέπει να αναζητηθεί περίπου 10 χρόνια πίσω, στη δημοσίευση της τεχνικής αναφοράς [27] αναφορικά με την ανάπτυξη δεικτών που προορίζονταν για την ποσοτικοποίηση της ασφάλειας υπηρεσιών και συστημάτων πληροφορικής. Στην έρευνα αυτή παρουσιάζονταν οι βασικές έννοιες αναφορικά με τους δείκτες, η χρησιμότητά τους, ο τρόπος χρήσης τους, η διαδικασία ανάπτυξής τους και μερικές από τις αδυναμίες τους.

Αναγκαία για την επιτυχία σε αυτόν τον χώρο της έρευνας, είναι η ύπαρξη της συνεχούς ενημέρωσης όλων των εμπλεκομένων μερών, αναφορικά με το τι χρειάζεται για να δημιουργηθούν δείκτες χρήσιμοι για την ποσοτικοποίηση της ασφάλειας συστημάτων πληροφορικής, καθώς και τη βελτιστοποίηση των υπαρχόντων δεικτών, αλλά και την ενσωμάτωση αυτών στη διαδικασία λήψης αποφάσεων ενός οργανισμού.

4.1 Τεχνικοί όροι και ορισμοί

Στον χώρο της έρευνας που ασχολείται με την ποσοτικοποίηση της ασφάλειας συστημάτων πληροφορικής, υπάρχουν ορισμένοι τεχνικοί όροι και ορισμοί που χρησιμοποιούνται συνεχώς αλλά και που εμπεριέχουν τον κίνδυνο παρερμηνείας τους. Στη διεθνή βιβλιογραφία υπάρχουν οι όροι δείκτης (metric), μέτρο (measure) και μέτρηση (measurement). Οι όροι αυτοί χρησιμοποιούνται εναλλάξ πολλές φορές ανάλογα με το περιεχόμενο της δημοσίευσης. Αυτό γίνεται γιατί οι α-

ναγνώστες που θα χρησιμοποιήσουν την ερευνητική προσπάθεια στην οποία αναγράφονται αυτοί οι όροι, γνωρίζουν ακριβώς πού αναφέρεται ο ερευνητής και έτσι δεν δημιουργείται πρόβλημα κατανόησης. Παρόλα αυτά καλό θα ήταν να αποσαφηνιστούν οι έννοιες αυτές για να μη δημιουργούν σύγχυση.

4.1.1 Μέτρηση

Με το όρο μέτρηση (a measurement), εννοούμε τα δεδομένα που ποσοτικοποιούν μία διάσταση ενός αντικειμένου για παράδειγμα, των αριθμό των ευπαθειών σε μία εφαρμογή.

4.1.2 Δείκτης

Η συσχέτιση των δεδομένων από δύο ή περισσότερες μετρήσεις δημιουργούν μία σχέση μεταξύ τους για παράδειγμα, ο αριθμός των ευπαθειών (μέτρηση #1) και ο αριθμός των γραμμών πηγαίου κώδικα (μέτρηση #2). Ο δείκτης (metric) απεικονίζει αυτήν ακριβώς τη σχέση, μεταξύ του μεγέθους της εφαρμογής και των ευπαθειών που εμφανίζει. Οι δείκτες, συνεπώς, μπορεί να χρησιμοποιηθούν για να ποσοτικοποιήσουν το βαθμό που μία υπηρεσία, διεργασία ή ένα σύστημα πληροφορικής περιέχει μία συγκεκριμένη ιδιότητα ασφάλειας.

4.1.3 Μέτρο

Στη διεθνή βιβλιογραφία ο όρος «μέτρο» (measure), έρχεται να αντικαταστήσει τον προηγούμενο όρο «δείκτης» (metric). Απεικονίζει ακριβώς τα ίδια πράγματα και έχει υιοθετηθεί από τα διεθνή πρότυπα και τις σχετικές οδηγίες εφαρμογής τους. Έτσι, για παράδειγμα, η αρχική δημοσίευση του NIST SP 800-55 [28] χρησιμοποιούσε τον όρο «δείκτη» (metric), ενώ στην αναθεωρημένη δημοσίευση [29] χρησιμοποιεί τον όρο «μέτρο» (measure). Ομοίως τα διεθνή πρότυπα ISO 27004:2009 [30] και ISO 15939:2007 [31] χρησιμοποιούν τον όρο «μέτρο» (measure).

4.1.4 Μετρήσεις

Ο όρος «μετρήσεις» (measurements), χρησιμοποιείται στη διεθνή βιβλιογραφία για να απεικονίσει τη φυσική πράξη της λήψης τιμών για μία διάσταση ενός αντικειμένου.

4.2 Κατηγοριοποίηση μεθόδων

Σήμερα χωρίς καμία αμφιβολία και παρόλο που δεν υπάρχει μία κοινά αποδεκτή μέθοδος για την ποσοτικοποίηση της ασφάλειας ενός συστήματος πληροφορικής, υπάρχουν διάφορες προσεγγίσεις για την επίτευξη αυτού του στόχου. Οι διάφορες προσεγγίσεις μπορεί να κατηγοριοποιηθούν ανάλογα με το περιεχόμενό τους σε μεθοδολογίες και βέλτιστες πρακτικές, παραγωγή εργαλείων που συλλέγουν δεδομένα, κυβερνητικές προσπάθειες που είναι εστιασμένες σε συγκεκριμένες περιοχές, προσπάθειες από εταιρείες της αγοράς, εργαλεία και μεθοδολογίες που χρησιμοποιούνται από επιθεωρητές συστημάτων πληροφορικής, διάφορες προσεγγίσεις ταξινόμησης ευπαθειών, συστήματα αξιολόγησης και τέλος από το κανονιστικό, νομικό και ρυθμιστικό πλαίσιο λειτουργίας εταιρειών και οργανισμών.

Η κάθε μία από τις παραπάνω προσεγγίσεις προσπαθεί να μετρήσει το επίπεδο ασφάλειας ενός συστήματος πληροφορικής χρησιμοποιώντας τη δική της μεθοδολογία. Από το πλήθος των προσεγγίσεων που υπάρχουν μπορεί κανείς να κατανοήσει πόσο καίριο, επίκαιρο και αγωνιώδες είναι το ζήτημα της ποσοτικοποίησης της ασφάλειας για μία επιχείρηση ή έναν οργανισμό. Παρόλα αυτά, υπάρχουν και αρκετοί που βλέπουν με σκεπτικισμό αυτές τις μεθόδους και ενώ στη θεωρία συμφωνούν, στην πράξη αμφισβητούν κάθε προσέγγιση [32]. Οι απόψεις τους συγκλίνουν σε τρείς τομείς:

1. Αυτό που πρέπει να μετρηθεί είναι η ασφάλεια ή η διασφάλιση της τεχνικής ασφάλειας των συστημάτων (computer security controls).
2. Η μέτρηση της διασφάλισης της ασφάλειας ενός συστήματος πληροφορικής είναι μία αξιέπαινη προσπάθεια στη θεωρία.

3. Η σημερινή κατάσταση της ασφάλειας των συστημάτων πληροφορικής είναι τόσο φτωχή και μη ανεπτυγμένη, που κάθε προσπάθεια από κάποιον να την αξιολογήσει και να την ποσοτικοποιήσει, θα ήταν απλώς χάσιμο χρόνου.

4.3 Τομείς έρευνας στην ποσοτικοποίηση της ασφάλειας και της διασφάλισης των πληροφοριών

Ένα τόσο φλέγον θέμα, όπως η ποσοτικοποίηση της ασφάλειας (quantification of security) και η διασφάλιση της πληροφορίας (information assurance), δεν θα μπορούσε παρά να προσελκύσει το ενδιαφέρον των ερευνητών από πολλούς τομείς. Έτσι, σύμφωνα με το [33], οι τομείς έρευνας που ασχολούνται με αυτά τα θέματα είναι οι εξής:

- Ποσοτικοποίηση της οικονομικής αξίας της ασφάλειας και της διασφάλισης των πληροφοριών.
- Ποσοτικοποίηση της αποδοτικότητας των τεχνικών μέτρων ασφάλειας.
- Μέτρηση των μη τεχνικών μέτρων ασφάλειας, όπως η ασφάλεια των διαδικασιών.
- Μέτρηση της ασφάλειας ενός συστήματος πληροφορικής με τη χρήση τεχνικών αξιολόγησης κινδύνων (risk assessment).
- Μέτρηση της ασφάλειας ενός συστήματος πληροφορικής που εστιάζεται στις επιθέσεις (attacks) που δέχεται.
- Μετρήσεις ασφαλείας σχετικά με τις ευπάθειες (vulnerabilities) και τις αδυναμίες (weaknesses) που υπάρχουν στα διάφορα συστήματα πληροφορικής.

- Μετρήσεις σχετικά με τους δείκτες ασφάλειας των συστημάτων, όπως πιθανότητα έκθεσης σε επιθέσεις / αντίσταση σε αυτές.
- Μετρήσεις στα μέτρα αντιμετώπισης κινδύνων (security controls).
- Μετρήσεις της προστασίας της ιδιωτικότητας (privacy) στα συστήματα πληροφορικής.
- Μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας των συστημάτων πληροφορικής.

4.4 Μεθοδολογίες και βέλτιστες πρακτικές

Διάφορα πρότυπα, κανονισμοί και οδηγίες εφαρμογής τους, έχουν αναπτυχθεί τα τελευταία χρόνια, με σκοπό να αντιμετωπίσουν την πρόκληση που έχουν οι οργανισμοί και οι επιχειρήσεις στο να αναπτύξουν τεχνικές μέτρησης του επιπέδου της ασφάλειας ενός συστήματος αλλά και στη διασφάλιση της πληροφορίας που εμπεριέχουν. Σε γενικές γραμμές μπορούμε να εντάξουμε αυτά τα πρότυπα και τις οδηγίες εφαρμογής τους στις ακόλουθες ομάδες:

- Προσπάθειες για την ανάπτυξη μέτρων ασφάλειας των πληροφοριών με σκοπό την εκτίμηση της αποτελεσματικότητας των μέτρων αυτών σε επίπεδο ολόκληρου του οργανισμού ή απλά ενός συστήματος πληροφορικής και την εφαρμογή των μέτρων αυτών [34], [35].
- Μοντέλα ωρίμανσης τα οποία παρέχουν ένα πλαίσιο κανόνων λειτουργίας που μας βοηθούν στην εκτίμηση της ωριμότητας του επιπέδου ασφαλείας των διαδικασιών, βασισμένα σε συγκεκριμένα κριτήρια [36].
- Πλαίσιο αξιολόγησης προϊόντων βάσει συγκεκριμένων κριτηρίων. Η χρήση ενός τέτοιου πλαισίου μας βοηθά στο να εκτιμήσουμε το επίπεδο διασφά-

λισης που μας παρέχει ένα προϊόν με συγκεκριμένα χαρακτηριστικά ασφάλειας [36].

4.4.1 NIST SP 800-55 Rev 1: Οδηγός Μέτρησης της Απόδοσης για μέτρα ασφάλειας πληροφοριών

Η NIST τον Ιούλιο του 2008 δημοσίευσε έναν οδηγό, NIST SP 800-55 Rev 1 [29], για τη μέτρηση της απόδοσης των μέτρων ασφάλειας των πληροφοριών, σε αντικατάσταση παλαιοτέρων οδηγιών που είχε δημοσιεύσει τον Ιούλιο του 2003, NIST SP 800-55 [28]. Οι νέες οδηγίες ήταν σε συμφωνία με ένα άλλο έντυπο οδηγιών, NIST SP 800-53 [37], που αναφερόταν στα μέτρα ασφάλειας πληροφοριών που έπρεπε να έχουν όλες οι κυβερνητικές υπηρεσίες καλύπτοντας επίσης και τα προγράμματα ασφαλείας που υπήρχαν. Το NIST SP 800-55 Rev 1 [29] ήταν η συγχώνευση της αρχικής δημοσίευσης NIST SP 800-55 [28] και του Draft NIST SP 800-80 του Μαΐου 2006.

Οι διεργασίες και οι μεθοδολογίες που αναφέρονται στο NIST SP 800-55 Rev 1 [29], συνδέουν τη μέτρηση της απόδοσης των μέτρων ασφαλείας συστημάτων πληροφορικής τόσο με την απόδοση της ίδιας της υπηρεσίας όσο και με τη χρήση των στρατηγικών διεργασιών της τελευταίας. Με άλλα λόγια, η απόδοση μίας υπηρεσίας επηρεάζεται και από την απόδοσή της στο να μετρήσει το επίπεδο ασφαλείας των συστημάτων πληροφορικής που διαθέτει.

Τα μέτρα ασφαλείας που αναπτύσσονται στο NIST SP 800-55 Rev 1 [29] βοηθούν στην αύξηση της ικανότητας των υπηρεσιών στο να υιοθετήσουν μία σειρά από κυβερνητικές οδηγίες όπως η FISMA, η FEA καθώς και άλλες σχετικές με τον οργανισμό οδηγίες, με σκοπό την παραγωγή ποσοτικών αναφορών σχετικά με την μέτρηση της απόδοσης των μέτρων ασφαλείας που χρησιμοποιούν.

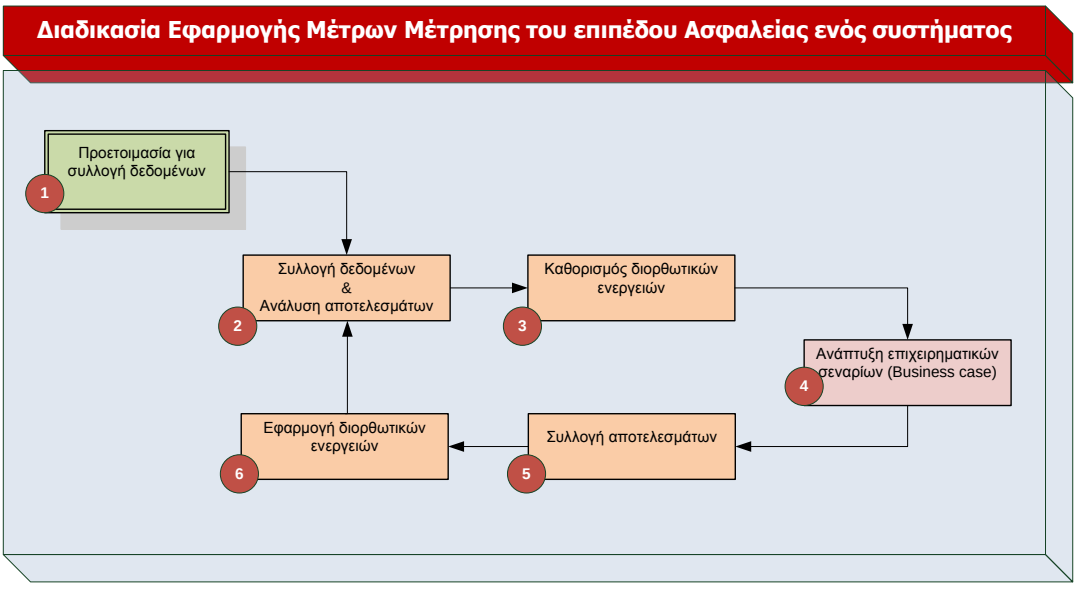
Η NIST SP 800-55 Rev 1 [29], εστιάζει σε τρείς βασικές κατηγορίες μετρήσεων:

1. Μέτρα υλοποίησης / εφαρμογής.

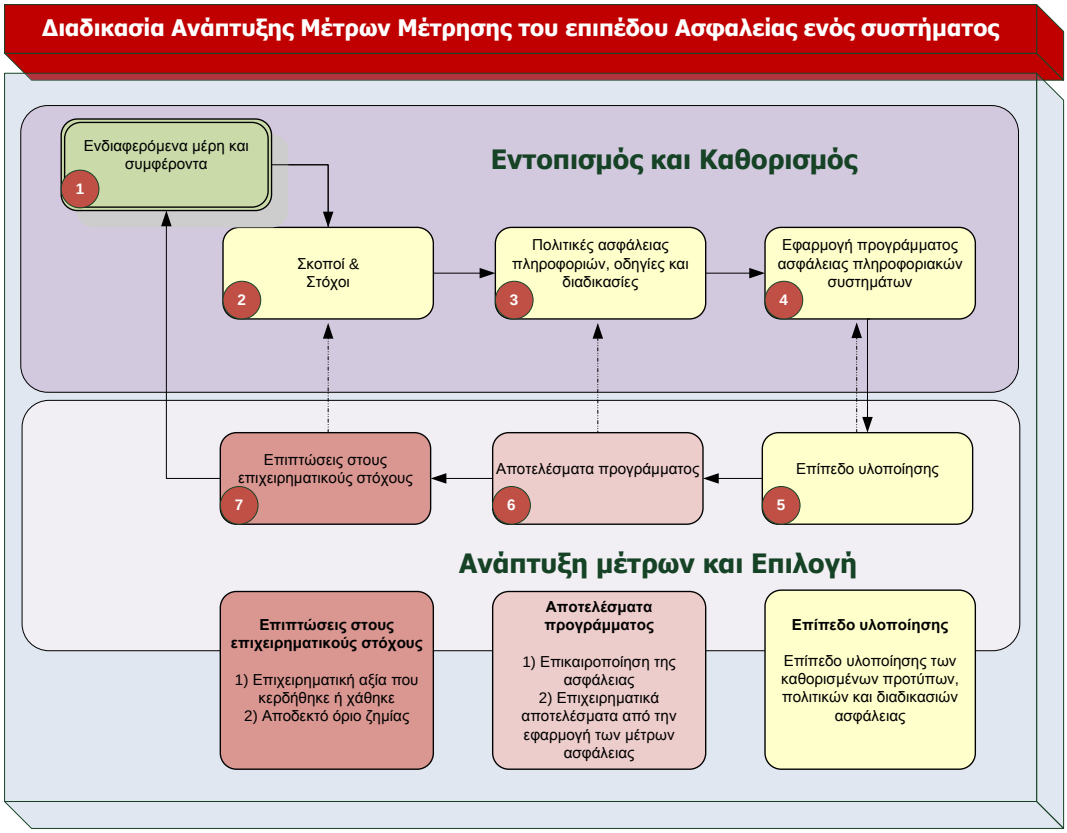
2. Μέτρα αποτελεσματικότητας και απόδοσης.
3. Επιπτώσεις των μέτρων.

Η NIST στην ειδική δημοσίευσή της (special publication) SP 800-55 Rev 1 [29], περιγράφει δύο πρωταρχικές διαδικασίες:

1. Τη διαδικασία εφαρμογής (implementation) των μέτρων μέτρησης του επιπέδου ασφαλείας ενός συστήματος (Εικόνα 8).
2. Τη διαδικασία ανάπτυξης (development) των μέτρων μέτρησης του επιπέδου ασφαλείας ενός συστήματος, η οποία αποτελεί και την πρώτη φάση της διαδικασίας εφαρμογής (implementation) που προαναφέρθηκε (Εικόνα 9).



Εικόνα 8: Διαδικασία Εφαρμογής Μέτρων Μέτρησης του επιπέδου Ασφαλείας ενός συστήματος, κατά [29]



Εικόνα 9: Διαδικασία Ανάπτυξης Μέτρων Μέτρησης του επιπέδου Ασφαλείας ενός συστήματος, σύμφωνα με [29]

Στην τρίτη ενότητα της δημοσίευσης από τη NIST, SP 800-55 Rev 1 [29], περιέχονται εκτενείς αναφορές για τα πλεονεκτήματα της χρήσης των μέτρων, τους διάφορους τύπους μέτρων και την συσχέτισή τους με την ωριμότητα του προγράμματος ασφαλείας (maturity of the information system program) που είναι υπό μέτρηση. Η NIST πιστεύει ότι η δυσκολία εφαρμογής των μέτρων ασφαλείας της πληροφορίας (information security measures) και το επίπεδο της πολυπλοκότητας (sophistication) που αναμένεται από τα μέτρα είναι άρρηκτα συνδεδεμένα με το επίπεδο ωριμότητας που παρουσιάζει το πρόγραμμα ασφάλειας.

Η NIST στο SP 800-55 Rev 1 [29], προτείνει ένα πρότυπο ανάπτυξης μέτρων παρέχοντας τις αναγκαίες λεπτομέρειες, τις οποίες απεικονίζει ο Πίνακας 5, για τον καθορισμό των επιμέρους μέτρων που θα απαιτηθούν για την υλοποίηση ενός τέτοιου προγράμματος.

Πεδίο	Περιγραφή
Κωδικός μέτρου (Measure ID)	Μοναδικός κωδικός που χρησιμοποιείται για την αναζήτηση και ταξινόμηση του μέτρου. Ο μοναδικός αυτός κωδικός μπορεί να ακολουθεί την τυχόν ειδική ονοματολογία που μπορεί να έχει ένας οργανισμός ή να αναφέρεται απευθείας σε κάποια άλλη πηγή.
Σκοπός (Goal)	Δήλωση του στρατηγικού σκοπού ή/και του σκοπού της ασφάλειας πληροφοριών που θα υλοποιεί αυτό το μέτρο. Για τα συστημικά μέτρα (system-level), ο στόχος θα καθορίζει και την εφαρμογή των μέτρων ασφάλειας για το συγκεκριμένο σύστημα πληροφορικής. Για τα μέτρα σε επίπεδο εφαρμογής (program-level), πρέπει να συμπεριλαμβάνονται τόσο ο στρατηγικός στόχος όσο και ο στόχος ασφάλειας πληροφοριών. Έτσι για παράδειγμα, οι στόχοι ασφάλειας πληροφοριών μπορούν να απορρέουν από τους εταιρικούς στόχους (enterprise goals), σε συνδυασμό με την αποστολή του οργανισμού (organization's mission). Αυτοί οι στόχοι συνήθως περιγράφονται σε στρατηγικά σχέδια και σχέδια αύξησης της απόδοσης ενός οργανισμού. Όταν είναι δυνατόν, πρέπει να περιλαμβάνονται τόσο ο στόχος σε εταιρικό επίπεδο, όσο και ο στόχος της ασφάλειας πληροφοριών.
Μέτρο (Measure)	Μία σύντομη περιγραφή του μέτρου. Καλό θα ήταν να χρησιμοποιηθούν αριθμητικά μέτρα που υποδηλώνονται από τις λέξεις: ποσοστό, νούμερο, συχνότητα, μέσος όρος ή άλλες παρεμφερείς λέξεις. Επίσης, εάν είναι δυνατόν, να χρησιμοποιηθούν τα μέτρα που περιέχονται από τη NIST στη ειδική δημοσίευση SP 800-53 [37]. Διαδικασίες ασφαλείας που εξασφαλίζουν την υποστήριξη των δεδομένων θα πρέπει να αναφέρονται σε στοιχεία εφαρμογής. Για παράδειγμα, εάν το μέτρο εφαρμόζεται σε μια συγκεκριμένη οδηγία FIPS 199 αναφορικά με επίπεδο επιπτώσεων (υψηλή, μέτρια ή χαμηλή), πρέπει να δηλωθεί και το επίπεδο μέσα στο μέτρο.
Τύπος μέτρου	Σύντομη περιγραφή για το εάν το μέτρο αναφέρεται στην:

Πεδίο	Περιγραφή
(Type)	α) εφαρμογή (implementation), β) αποδοτικότητα (effectiveness) / αποτελεσματικότητα (efficiency) ή γ) επιπτώσεις (impact)
Μαθηματικός τύπος υπολογισμού	Οι υπολογισμοί που πρέπει να γίνουν για να παραχθεί ένα αριθμητικό αποτέλεσμα.
Στόχος	Όρια για την ερμηνεία του αποτελέσματος, όπως ποσοστό ολοκλήρωσής ή κάποιο στατιστικό νούμερο. Ο στόχος μπορεί να εκφραστεί σε ποσοστά, ώρες, ευρώ ή οποιαδήποτε άλλη κατάλληλη μονάδα μέτρησης. Επίσης, ο στόχος μπορεί να συνδεθεί με ένα προαπαιτούμενο χρονικό πλαίσιο ολοκλήρωσης. Πρέπει να επιλέξουμε τελικό και ενδιάμεσο στόχο που να επιτρέπει την παρακολούθηση της προόδου προς την κατεύθυνση ολοκλήρωσής του.
Ενδείξεις εφαρμογής (Implementation Evidence)	Οι ενδείξεις εφαρμογής χρησιμοποιούνται: α) στον υπολογισμό του μέτρου, β) στην επαλήθευση της διαδικασίας που χρησιμοποιείται, και γ) στον εντοπισμό των πιθανών αιτίων για την ύπαρξη μη ικανοποιητικών αποτελεσμάτων για το συγκεκριμένο μέτρο. Για τη χειροκίνητη συλλογή δεδομένων, πρέπει να αναζητηθούν ερωτήσεις που θα χρησιμοποιηθούν: α) ως στοιχεία εισόδου στη μαθηματική εξίσωση υπολογισμού του μέτρου, β) στην αποδοχή του μέτρου και γ) στην αξιολόγηση της πληροφορίας που συλλέχθηκε. Για κάθε ερώτηση, αν είναι δυνατό, να αναγράφεται και η αναφορά στο σημείου ελέγχου ασφάλειας (security control) που περιέχεται στη λίστα της NIST SP 800-53 [37]. Για κάθε μέτρο στη λίστα οδηγιών FIPS 199, αναφορικά με το επίπεδο επίδρασης (impact level), οι ερωτήσεις θα πρέπει να αναγράφουν και το επίπεδο αυτό. Για την αυτοματοποιημένη συλλογή δεδομένων, πρέπει να καθορισθούν εκείνα τα δεδομένα τα οποία είναι αναγκαία:

Πεδίο	Περιγραφή
	α) στη μαθηματική εξίσωση υπολογισμού του μέτρου, β) στην αποδοχή του μέτρου και γ) στην αξιολόγηση της πληροφορίας που συλλέχθηκε.
Συχνότητα (Frequency)	Ένδειξη για τη συχνότητα συλλογής και επεξεργασίας των δεδομένων. Η επιλογή της συχνότητας συλλογής των δεδομένων, πρέπει να γίνει σύμφωνα με το ρυθμό αλλαγής του μέτρου ασφάλειας το οποίο αξιολογείται. Προς αυτή την κατεύθυνση, καλό θα ήταν να αναζητηθούν οι ανάγκες για πληροφόρηση εξωτερικών συνεργατών καθώς και ο εσωτερικός τρόπος λειτουργίας του οργανισμού.
Εμπλεκόμενα μέρη (Responsible parties)	Καθορισμός των ενδιαφερομένων μερών: Ιδιοκτήτης πληροφορίας (Information owner). Σύμφωνα με το οργανόγραμμα του οργανισμού αυτός που έχει στην ευθύνη του την πληροφορία που θέλουμε να συλλέξουμε. Ανθρώπινο δυναμικό που θα συλλέξει την πληροφορία (Information collector). Θα πρέπει να είναι διαφορετικό από τον ιδιοκτήτη της πληροφορίας, για την αποφυγή της σύγκρουσης συμφερόντων αλλά και για την εξασφάλιση του διαχωρισμού των ρόλων και των αρμοδιοτήτων. Τελικός χρήστης της πληροφορίας (Information customer). Αποτελεί τον τελικό χρήστη στον οργανισμό και είναι αυτός που χρησιμοποιεί την πληροφορία που θέλουμε να συλλέξουμε.
Πηγή πληροφοριών (Data source)	Το σημείο που υπάρχουν οι πληροφορίες που θέλουμε να συλλέξουμε για να υπολογίσουμε το μέτρο ασφάλειας. Τέτοια σημεία μπορεί να είναι οι βάσεις δεδομένων του οργανισμού, διάφορα ημερολόγια ηλεκτρονικά ή όχι, καθώς και άτομα που ανήκουν σε συγκεκριμένους ρόλους μέσα στον οργανισμό που είναι σε θέση να γνωρίζουν τις πληροφορίες που χρειαζόμαστε.
Μορφοποίηση Αναφο-	Λεπτομέρειες για τον τρόπο παρουσίασης του μέτρου, όπως

Πεδίο	Περιγραφή
ρών ***(Reporting format)***	για παράδειγμα ο τύπος γραφικών pie chart, line chart, bar chart κτλ. Πρέπει να δοθεί ένα παράδειγμα του τρόπου παρουσίασης που επιθυμούμε.

Πίνακας 5: Πρότυπος πίνακας αποτύπωσης μέτρων και οδηγίες

4.4.2 Πρακτικό πλαίσιο μετρήσεων για τη διασφάλιση της ποιότητας του λογισμικού και της ασφάλειας των πληροφοριών

Το πρακτικό πλαίσιο διασφάλισης της ποιότητας λογισμικού και της ασφάλειας των πληροφοριών αναπτύχθηκε από το Software Assurance (SwA) Measurement Working Group [36] υπό την αιγίδα του SwA Forum. Το SwA Forum καθώς και το SwA Measurement Working Group χρηματοδοτούνται από: το Υπουργείο Εσωτερικής Ασφάλειας (Department of Homeland Security – DHS) των ΗΠΑ, το Υπουργείο Αμύνης (Department of Defense – DoD) των ΗΠΑ και το National Institute of Standards and Technology (NIST). Όλοι μαζί συμμετέχουν σε μία κοινή προσπάθεια που την απαρτίζουν μέλη της αγοράς, της κυβέρνησης και των επιστημόνων της ακαδημαϊκής κοινότητας, με σκοπό να δώσουν λύση στο δύσκολο πρόβλημα που αντιμετωπίζουν αναφορικά με το λογισμικό, αυτό της μέτρησης της κυβερνοασφάλειας και της διασφάλιση της ασφάλειας και των πληροφοριών. Το πλαίσιο που προτείνουν, δημοσιεύθηκε στο Practical Software and the Systems Measurement (PSM) Support Center σύμφωνα με το [36].

Σύμφωνα με την ιστοσελίδα του SwA Measurement WG στο [36], το πλαίσιο «… αποτελεί μία προσέγγιση για τη μέτρηση της αποτελεσματικότητας της προσπάθειας επίτευξης των στόχων και των σκοπών, της διασφάλισης ποιοτικού λογισμικού (SwA) μέσα σε ένα οργανισμό ή σε ένα έργο πληροφορικής. Δίνει απαντήσεις στο πώς μπορεί να εκτιμηθεί ο βαθμός της διασφάλισης της ποιότητας του λογισμικού, με τη χρήση ποσοτικών και ποιοτικών μεθοδολογιών και τεχνικών. Το πλαίσιο λαμβάνει υπόψη του τις υπάρχουσες μεθοδολογίες στον τομέα αυτό, και στοχεύει να βοηθήσει τους οργανισμούς στο να ενσωματώσουν τις μεθοδολογίες

μέτρησης διασφάλισης ποιοτικού λογισμικού στα ήδη υπάρχοντα έργα πληροφορικής που έχουν.»

Το πλαίσιο δεν προτείνει νέες μεθόδους για τη δημιουργία μέτρων εφαρμογής προγραμμάτων διασφάλισης ποιότητας λογισμικού. Αυτό που κάνει, είναι να εξισορροπεί τις υπάρχουσες προσεγγίσεις στη διασφάλιση της ασφάλειας και των πληροφορικών και στον τομέα των συστημάτων πληροφορικής και λογισμικού. Τέλος, προτείνει μία αρμονική προσέγγιση που να μπορεί να χρησιμοποιηθεί τόσο από τους χρήστες του τομέα της ασφάλειας πληροφοριών, όσο και από τους χρήστες του τομέα ανάπτυξης συστημάτων πληροφορικής και λογισμικού. Οι ακόλουθες προσεγγίσεις αποτέλεσαν την βάση στην οποία στηρίχθηκε η ανάπτυξη αυτού του πλαισίου:

- Ο οδηγός της NIST που αναφέρθηκε στην παράγραφο § 4.4.1.
- Το πρότυπο ISO/IEC 27004:2009 [30].
- Το πρότυπο ISO/IEC 15939:2007 [31].
- Το πρότυπο Capability Maturity Model Integration (CMMI) Measurement and Analysis (MA) [38].
- Η μεθοδολογία CMMI Goal, Question, Indicator, Measure (GQIM) [39].

Κατά τη διαδικασία ανάπτυξης του πλαισίου, το SwA Measurement WG κατέγραψε τις ομοιότητες καθώς και τις διαφορές μεταξύ πέντε μεθοδολογιών και, τελικά, δημιούργησε μία αρμονική προσέγγιση για μετρήσεις. Η προσέγγιση αυτή συνοψίζει τις μεθοδολογίες που μελετήθηκαν και προτείνει μία υψηλού επιπέδου διαδικασία, η οποία μπορεί να εφαρμοστεί σε διαφορετικές επιχειρησιακές περιοχές του τομέα της διασφάλισης της ασφάλειας και των πληροφοριών. Το πλαίσιο επίσης συμβουλεύει εκείνους που θα προσπαθήσουν να το υιοθετήσουν, στο πώς μπορούν να ξεκινήσουν τη διαδικασία ενσωμάτωσης της διασφάλισης της ποιότητας του λογισμικού και των μέτρων μέτρησης της ασφάλειας, σε έναν οργανισμό, σε έργα που βρίσκονται σε εξέλιξη ή ακόμα σε άλλα προγράμματα μέτρησης, το οποία μπορεί να μην καλύπτουν αυτούς τους τομείς.

4.5 Εργαλεία συλλογής δεδομένων

Στον τομέα των μεθοδολογιών μέτρησης της διασφάλισης της πληροφορίας, πραγματικών περιπτώσεων, πρακτικών ασφαλών μετρήσεων και διάφορων άλλων παραδειγμάτων έχει αναρτηθεί στο διαδίκτυο ένας μεγάλος όγκος πληροφοριών. Ωστόσο, υπάρχει πολύ μικρός όγκος δεδομένων ή/και δημοσιεύσεων, σχετικά με εργαλεία που μπορούν να χρησιμοποιηθούν για την κυβερνοασφάλεια και τη διασφάλιση της πληροφορίας.

Υπάρχουν προϊόντα λογισμικού (εμπορικές εφαρμογές), που παρουσιάζονται ως εργαλεία για την επίτευξη της ασφάλειας στον κυβερνοχώρο ή/και της διασφάλισης της πληροφορίας. Παραδείγματα τέτοιων προϊόντων, είναι εκείνα που βοηθούν στη επίτευξη της συμμόρφωσης σε κάποιο πρότυπο, όπως ISO ή άλλα που παρέχουν τη δυνατότητα ανάλυσης των συστημάτων πληροφορικής που διαθέτει μία επιχείρηση, Plumtree Portal [40] και Symbiot Security [41]. Και οι δύο αυτές κατηγορίες προτρέπουν τον χρήστη να συμπληρώσει ένα αρκετά εκτενές ερωτηματολόγιο και, στη συνέχεια, παράγουν μία αναλυτική εκτύπωση με τα ευρήματά τους, αξιολογώντας έτσι την κατάσταση των υποδομών πληροφορικής του οργανισμού ή της εταιρείας.

Ωστόσο, μόνο μερικά από αυτά καταφέρνουν να παρουσιάσουν την ασφάλεια στον κυβερνοχώρο και τη διασφάλιση της πληροφορίας ως βασικά συστατικά της λειτουργικότητάς τους. Τα περισσότερα εργαλεία που έχουν φτιαχτεί για το σκοπό αυτό, χαρακτηρίζονται με μια συνήθη έκφραση του μάρκετινγκ για τις εμπορικές εφαρμογές, ως «κυβερνητικές εφαρμογές από το ράφι» (government off-the-shelf - GOTS). Οι εφαρμογές αυτές χρησιμοποιούν υπάρχουσες τεχνολογίες κατασκευαστών, που έχουν δημιουργηθεί σύμφωνα με τις ανάγκες των οργανισμών για συμμόρφωση σε κανονιστικά πλαίσια, όπως το FISMA, καθώς και άλλες οδηγίες ή κανονισμούς.

Συνήθως, τα εργαλεία της ασφάλειας του κυβερνοχώρου και της διασφάλισης της πληροφορίας, μπορούν να ταξινομηθούν στις ακόλουθες κατηγορίες:

- Ολοκληρωμένα πλαίσια ή πλατφόρμες.

- Εργαλεία συλλογής / αποθήκευσης στοιχείων.
- Εργαλεία ανάλυσης και εκτιμήσεων.
- Εργαλεία παραγωγής αναφορών.

Κατά τη διαδικασία διαμόρφωσης ή επιλογής ενός από τα παραπάνω εργαλεία μέτρησης, είναι σημαντικό να γίνεται πρώτα η συλλογή των απαιτήσεων, μετά η εύρεση των ελλείψεων και τελικά η επιλογή του εργαλείου. Αυτό γίνεται, έτσι ώστε ο οργανισμός να καταλάβει ποιο εργαλείο καλύπτει καλύτερα τις ανάγκες του ή ακόμα να αναζητηθεί αν κάποιο παρόμοιο εργαλείο μπορεί να χρησιμοποιηθεί για την επίτευξη του σκοπού του οργανισμού.

Εδώ θα πρέπει να αναφερθεί, ότι για να είναι ένα εργαλείο μέτρησης της ασφάλειας του κυβερνοχώρου ή διασφάλισης της πληροφορίας επιτυχημένο, πρέπει να εφαρμόζονται οι ακόλουθες σαφείς πρακτικές μέτρησης:

- Πρέπει να υποβληθούν εργαλεία και πίνακες αποφάσεων στα κατάλληλα διοικητικά επίπεδα προς έγκριση.
- Οι πολιτικές, οι διαδικασίες και η ιεράρχηση των κινδύνων πρέπει να χρησιμοποιούν μετρήσιμους στόχους, πριν την επιλογή και την εφαρμογή κάποιου από τα διαθέσιμα εργαλεία.
- Τα εργαλεία θα πρέπει να επιτρέπουν στα μέτρα διασφάλισης της πληροφορίας να είναι περισσότερο ποσοτικά και εστιασμένα στην αντικειμενικότητα και εγκυρότητα των δεδομένων.
- Τα εργαλεία θα πρέπει να βοηθούν τα μέτρα διασφάλισης της πληροφορίας:
  - ✓ στην εύκολη συλλογή δεδομένων μετρήσεων,
  - ✓ στην απρόσκοπτη προσπέλασή τους,
  - ✓ στην εύκολη αποθήκευσή τους.

- Τα εργαλεία και οι διαδικασίες θα πρέπει να μπορούν να επαναληφθούν, με σκοπό την παραγωγή στατιστικών τάσεων (trends) σε βάθος χρόνου.
- Τα εργαλεία θα πρέπει να είναι σε θέση να παράγουν αποτελέσματα σε τέτοια μορφή ανάλογα με το επίπεδο των ενδιαφερομένων χρηστών (Διοίκηση, προϊστάμενοι κτλ).
- Τα εργαλεία θα πρέπει να καθιστούν τα αποτελέσματα χρήσιμα στα διάφορα ενδιαφερόμενα μέρη και να αναδεικνύουν πληροφορίες χρήσιμες στη διαδικασία λήψης αποφάσεων.

4.5.1 Εργαλεία συλλογής / αποθήκευσης στοιχείων

Είναι σύνηθες σε διάφορους οργανισμούς να χρησιμοποιούνται τα προγράμματα Microsoft Excel® ή Access® για τη συλλογή και αποθήκευση στοιχείων για την μέτρηση της ασφάλειας και της διασφάλισης της πληροφορίας. Όμως, περίπου το 2000, κάποια προϊόντα λογισμικού έκαναν την εμφάνισή τους, αυτοματοποιώντας έτσι τις προσπάθειες των οργανισμών, σε μία σειρά από δραστηριότητες συλλογής στοιχείων, με σκοπό τη διασφάλιση της ασφάλειας των πληροφοριών. Ο παρακάτω Πίνακας 6 εμφανίζει μερικά από αυτά.

Όνομα	Περιγραφή
CSAM και ASSERT OMB Security Line of Business **[42]**	Επιτρέπει στους χρήστες να βλέπουν τον κατάλογο με τα διαθέσιμα μέτρα ασφάλειας, και να εξάγουν τις πληροφορίες από τη βάση δεδομένων σε διάφορες μορφές που χρησιμοποιούν γνωστά εργαλεία υποστήριξης.
Trusted Agent (FISMA) **[43]**	Επιτρέπει στους χρήστες να αυτοματοποιήσουν την παραγωγή αναφορών απόδοσης των μέτρων ασφάλειας με τη χρήση σχεσιακής βάσης δεδομένων για την επίτευξη της συμμόρφωσης στο πλαίσιο αρχών FISMA.
Splunk **[44]**	Βοηθά στην επίτευξη της συμμόρφωσης σε κανονιστικό πλαίσιο, με το να παρακολουθεί, ανασκοπεί και αποθηκεύει ηλεκτρονικά ίχνη (audit trails). Μπορεί να χρησιμοποιηθεί σε όλα τα μέτρα ασφάλειας της πληροφορίας και αποθηκεύει τα δεδομένα για μεγάλο χρονικό διάστημα, σύμφωνα με τα πρότυπα και τις οδηγίες της NIST.

Πίνακας 6: Εργαλεία συλλογής / αποθήκευσης στοιχείων

4.5.2 Εργαλεία ανάλυσης και εκτιμήσεων

Τα εργαλεία ανάλυσης και εκτιμήσεων έχουν πολλές δυνατότητες, συμπεριλαμβανομένων και της εύρεσης ευπαθειών (vulnerabilities) σε δίκτυα, της ανάλυσης πηγαίου κώδικα, της ανάλυσης διάφορων ημερολογίων, της εκτίμησης της συνολικής εικόνας της ασφάλειας ενός συστήματος πληροφορικής, της εκτίμησης κινδύνων που σχετίζονται με τη διασφάλιση της πληροφορίας και, τέλος, της συμμόρφωσης σε κανονιστικά πλαίσια ή πρότυπα. Μερικά από αυτά περιγράφονται στον παρακάτω, Πίνακας 7:

Όνομα	Περιγραφή
Klocwork Insight **[45]**	Το εργαλείο «Klockwork Insight» μπορεί να αναλύσει τον πηγαίο κώδικα ενός λογισμικού, με σκοπό να αναγνωρίσει ευπάθειες σε αυτόν. Το εργαλείο προσφέρει τη δυνατότητα παραγωγής αναφορών, οι οποίες δίνουν εκτιμήσεις ανάλογα με τα δεδομένα που έχουν συλλεχθεί. Μερικά από αυτά είναι ο αριθμός των ευπαθειών που αναγνωρίστηκαν και επιδιορθώθηκαν στην επιφάνεια εργασίας των προγραμματιστών, και συγκρίσεις των ελαττωμάτων σε σχέση με το χρόνο.
Ounce Suite **[46]**	Η σουίτα αυτή μας παρέχει ένα σύνολο εργαλείων, για την ανίχνευση του πηγαίου κώδικα εφαρμογών και την παροχή στατιστικών μέτρων, τα οποία βασίζονται στον αριθμό και τη σοβαρότητα των ευπαθειών που ανιχνεύτηκαν. Με το την έκδοση Ounce Portfolio Manager, μπορούμε να πάρουμε συγκεντρωτικά αποτελέσματα σε επίπεδο οργανισμού.
Fortify Suite **[47]**	Το εργαλείο αυτό ανιχνεύει τον πηγαίο κώδικα μίας εφαρμογής και αυτομάτως αναλύει τα αποτελέσματα που βρίσκει. Με αυτό τον τρόπο ένας οργανισμός μπορεί να παρακολουθεί την εξέλιξη των ευρημάτων στις εφαρμογές του μέσα στο χρόνο και να αποκτά λεπτομερή εικόνα αναφορικά με την ασφάλεια που του παρέχουν.

Πίνακας 7: Εργαλεία ανάλυσης και εκτιμήσεων

4.5.3 Εργαλεία παραγωγής αναφορών

Τα στοιχεία που έχουν συλλεχθεί και αποθηκευτεί αναφορικά με την ασφάλεια των πληροφοριών από τα παραπάνω εργαλεία παρέχουν την αναγκαία πληροφόρηση για τον σχηματισμό ηλεκτρονικών ταμπλό (dashboard) και άλλων αναφο-

ρών, που εμφανίζουν σε σχεδόν πραγματικό χρόνο την εικόνα ασφάλειας ενός οργανισμού. Σε περίπτωση που ένας οργανισμός, έχει επιλέξει τη λύση ενός ηλεκτρονικού ταμπλό, θα πρέπει να έχει εξασφαλίσει την α) πρόσβαση, β) την επαναχρησιμοποίηση, γ) την εμφάνιση και δ) την ανανέωση των δεδομένων ασφαλείας από το χώρο που αποθηκεύονται, για παράδειγμα τη βάση δεδομένων, με γρήγορο και αποδοτικό τρόπο.

Όνομα	Περιγραφή
IBM Cognos **[48]**	Το εργαλείο αυτό παράγει αναφορές που αντλούνται από μεγάλο όγκο δεδομένων. Μπορεί να εκτελέσει ad-hoc ερωτήσεις, να τις διανείμει σε όλο το δίκτυο ενός οργανισμού και να ελέγξει κεντρικά την ροή των αναφορών, με τη δημιουργία επιμέρους αναφορών προσαρμοσμένες στις ανάγκες κάθε χρήστη.
Corda **[49]**	Το εργαλείο αυτό μας παρέχει τη δυνατότητα της πρόσβασης σε εταιρικά δεδομένα ασφάλειας σε πραγματικό χρόνο, με τη χρήση ηλεκτρονικών ταμπλό, από οποιαδήποτε τοποθεσία.
Clear Point Metrics **[50]**	Το ολοκληρωμένο αυτό εργαλείο συνδυάζει τον έλεγχο της απόδοσης και τη συμμόρφωση με τις βέλτιστες πρακτικές, και επιτρέπει την επιτυχημένη μέτρηση, παρακολούθηση, και επικοινωνία της κατάστασης ασφάλειας, της ποιότητας και της αποδοτικότητας των μέτρων ασφάλειας που έχει πάρει ο οργανισμός.

Πίνακας 8: Εργαλεία παραγωγής αναφορών

4.6 Κυβερνητικές προσπάθειες

Παίρνοντας για παράδειγμα τις ΗΠΑ, όπου θεωρείται ως η πιο ενεργή και ευαισθητοποιημένη χώρα στον τομέα της διασφάλισης της πληροφορίας και των επιθέσεων στον κυβερνοχώρο, μπορούμε να αντλήσουμε χρήσιμα συμπεράσματα. Τα τελευταία χρόνια, στην προσπάθεια των ΗΠΑ να διασφαλίσουν την ασφάλεια των πληροφοριών και να περιορίσουν το φαινόμενο των επιθέσεων στον κυβερνοχώρο, οι προσπάθειες των κυβερνητικών της υπηρεσιών, έχουν αξιοσημείωτα ενταθεί.

Για αυτό τον λόγο, έχει ξεκινήσει μία σειρά από προγράμματα που σκοπό έχουν να λειτουργήσουν ως οδηγός εφαρμογής κυβερνητικών προγραμμάτων διασφάλισης της πληροφορίας και προστασίας από κυβερνοεπιθέσεις. Επιπλέον, έχει αυξήσει τις ερευνητικές της προσπάθειες, με σκοπό την εύρεση νέων μέτρων που μπορούν να χρησιμοποιηθούν σε μελλοντικά προγράμματα, και, τέλος, ασκεί υψηλή εποπτεία, με το να μετράει τις επιδόσεις των κυβερνητικών της υπηρεσιών στον τομέα της ασφάλειας. Αξιοσημείωτες κυβερνητικές προσπάθειες στον τομέα αυτό είναι του Υπουργείου Αμύνης (Department of Defense – DoD), του National Institute of Standards and Technology (NIST) και της Υπηρεσίας Ασφαλείας (National Security Agency – NSA).

4.6.1 Υπουργείο Αμύνης των ΗΠΑ (Department of Defense – DoD)

Διάφορα μέτρα πού αποσκοπούν στη διασφάλιση της πληροφορίας και άλλα σχετικά προγράμματα υπάρχουν σε όλα τα επίπεδα Διοίκησης μέσα στο Υπουργείο Αμύνης. Κάθε οργανωτική μονάδα μπορεί να υιοθετεί τα δικά της μέτρα, εργαλεία και διαδικασίες για το σκοπό αυτό. Όλες όμως οι μονάδες, έχουν επιλέξει, να επικεντρωθούν στον εντοπισμό και την ανάπτυξη μέτρων που θα χρησιμοποιηθούν στην αξιολόγηση της απόδοσης επιλεγμένων προγραμμάτων μέσα στο υπουργείο. Οι κοινοί στόχοι και προκλήσεις που αντιμετώπισαν, μπορούν να κατηγοριοποιηθούν σε:

- Δυσκολίες στην εκτίμηση της αποδοτικότητας (performance) και αποτελεσματικότητας (effectiveness) των μέτρων προστασίας της πληροφορίας.
- Ύπαρξη ανάγκης καθορισμού του κόστους των μέτρων διασφάλισης της πληροφορίας, με σκοπό την εξασφάλιση οικονομικών κονδυλίων για την κάλυψή τους.
- Προσδιορισμός του τομέα που θα ανήκει το κόστος (κέντρο κόστους).
- Υψηλό κόστος συμμόρφωσης σε πρότυπα και οδηγίες.
- Ανάγκη να αναπτυχθεί μια αποτελεσματική στρατηγική για την επίτευξη και διατήρηση της συμμόρφωσης σε πρότυπα και οδηγίες.
- Καθορισμός σχεδίου δράσης και ορόσημων (Plan Of Action and Milestones – POA&M) για την αναγνώριση και τον μετριασμό των κινδύνων.

Οι επιμέρους υπηρεσίες του υπουργείου αναφέρουν το βαθμό συμμόρφωσής τους σε πρότυπα, οδηγίες και άλλους κανονισμούς, με την παραγωγή αναφορών σε προκαθορισμένες κοινές –μεταξύ των κυβερνητικών υπηρεσιών- φόρμες. Παρόλα αυτά, ο τρόπος μέτρησης των δεδομένων που απεικονίζονται στις φόρμες, καθορίζεται αποκλειστικά από την κάθε μία υπηρεσία που παράγει την αναφορά.

4.6.2 DHS / DoD / National Institute of Standards and Technology (NIST) και Software Assurance Measurement Working Group

Το Υπουργείο Εσωτερικής Ασφάλειας (Department of Homeland Security – DHS) των ΗΠΑ, το Υπουργείο Αμύνης (Department of Defense – DoD) των ΗΠΑ, το National Institute of Standards and Technology (NIST) και το Software Assurance (SwA) Measurement Working Group (WG) που αναφέρθηκε στην παράγραφο § 4.4.2, δραστηριοποιούνται από το 2005. Το SwA WG, συνέρχεται αρκετές φορές μέσα στο χρόνο, για να εργαστεί σε κοινά παραδοτέα έργα και να παρέχει τη δυ-

νατότητα διαμοιρασμού της γνώσης που έχει αποκτηθεί. Οι στόχοι του σύμφωνα με το [51] είναι:

- Να παρέχει ένα πρακτικό πλαίσιο διασφάλισης της ποιότητας του λογισμικού και διάφορες άλλες πηγές στην επιστημονική κοινότητα.
- Να ενθαρρύνει την ενσωμάτωση πρακτικών διασφάλισης της ποιότητας του λογισμικού στους τομείς ανάπτυξης λογισμικού και συστημάτων πληροφορικής, με την υιοθέτηση ολοκληρωμένων προσεγγίσεων μέτρησης.
- Να κάνει γνωστό στην επιστημονική κοινότητα όλο το υλικό που διαθέτει, σχετικά με τον τομέα διασφάλισης της ποιότητας του λογισμικού, συμπεριλαμβανομένων πρότυπων σεναρίων, άρθρων, μεθόδων και παραδειγμάτων μέτρων που χρησιμοποίησαν.
- Να δημιουργήσει μία κοινότητα επιστημόνων, με θέμα τη διασφάλιση της ποιότητας λογισμικού, που να μοιράζεται τις γνώσεις της και τις τεχνικές της.
- Να συνεργάζεται με άλλες ομάδες, με σκοπό την ενσωμάτωση των μέτρων διασφάλισης ποιότητας λογισμικού, μέσα στις δραστηριότητές τους.

Μέχρι πρόσφατα, το SwA WG, επικεντρώνονταν στην ανάπτυξη και δημοσίευση πρακτικού πλαισίου για τη διασφάλιση της ποιότητας του λογισμικού και την ασφάλεια της πληροφορίας. Τελευταία, οι προσπάθειες του SwA WG έχουν εστιαστεί στο να παράγουν μία σειρά από μελέτες μετρήσεων, που οι διάφοροι οργανισμοί και επιχειρήσεις θα μπορούσαν να χρησιμοποιήσουν, με σκοπό να δημιουργήσουν χρήσιμα για αυτούς μέτρα και να αυξήσουν το επίπεδο της ασφάλειας και της ποιότητας του λογισμικού τους.

Το SwA WG βρίσκεται στη διαδικασία δημιουργίας μίας διαδικτυακής κοινότητας (Web-base community), με σκοπό την καταγραφή μέτρων και άλλων πηγών, αναφορικά με τον τομέα διασφάλισης της ποιότητας λογισμικού. Αυτή η διαδικτυ-

ακή κοινότητα οραματίζεται ότι θα αποτελέσει το χώρο, όπου αυτοί που ασχολούνται με τα θέματα της διασφάλισης θα μπορούν να ανταλλάσουν ιδέες, να ανακοινώνουν γενικής χρήσης μέτρα, να βρίσκουν χρήσιμες πληροφορίες και φυσικά, να βρίσκουν νέα μέτρα για την επίτευξη του σκοπού τους. Οι διαθέσιμες πληροφορίες στην ιστοσελίδα του SwA WG στο [52], περιλαμβάνουν κατευθυντήριες γραμμές σε πρότυπα, οδηγούς, σχετική βιβλιογραφία, άρθρα και παραδείγματα που έχουν δημοσιεύσει μέλη του.

4.6.3 Υπηρεσία Ασφαλείας των ΗΠΑ (National Security Agency- NSA)

Η υπηρεσία ασφαλείας των ΗΠΑ έχει αναπτύξει μία μεθοδολογία για το Υπουργείο Άμυνας σε συνεργασία με το εργαστήριο εφαρμοσμένης φυσικής του πανεπιστημίου «Johns Hopkins», η οποία ονομάζεται «Mission Oriented Risk and Design Analysis – MORDA» [53]. Ο σκοπός της μεθοδολογίας αυτής είναι έχει να παρέχει μία ποσοτική μέθοδο υπολογισμού και διαχείρισης των κινδύνων, χρησιμοποιώντας σύγχρονα μοντέλα ασφάλειας, ανάλυση δεδομένων και τεχνικές μέτρησης. Για το σκοπό αυτό, το MORDA χρησιμοποιεί μία μεγάλη γκάμα εργαλείων, συμπεριλαμβανομένων των δέντρων επίθεσης (attack trees) αλλά και άλλων μοντέλων διασφάλισης της πληροφορίας (information assurance), καθώς και τεχνικές ανάλυσης αποφάσεων πολλαπλών στόχων (multiple objective decision analysis).

Κάθε μοντέλο παράγει μαθηματικά αποτελέσματα τα οποία εκφράζονται σε μέτρα, όπως εκτιμώμενες ζημιές από τις επιθέσεις, προβλεπόμενη συχνότητα επιθέσεων και αποτελεσματικότητα των αντιμέτρων, δηλαδή των μέτρων που έχουν υλοποιηθεί για την αντιμετώπιση ή/και πρόληψη των επιθέσεων. Συλλογικά, αυτά τα ποσοτικά αποτελέσματα σκοπεύουν στο να βοηθήσουν στη λήψη αποφάσεων επένδυσης που σχετίζονται με τις βελτιώσεις στις υποδομές της ασφάλειας και στον επανασχεδιασμό, την αναβάθμιση ή την υποβάθμιση των υπαρχόντων μέτρων και συστημάτων.

Η διαδικασία MORDA έχει υλοποιηθεί σύμφωνα με το μοντέλο «Security Optimization Countermeasure Risk and Threat Evaluation System - SOCRATES», που επίσης έχει αναπτυχθεί από το εργαστήριο εφαρμοσμένης φυσικής του πανεπι-

στημίου «Johns Hopkins». Το μοντέλο, το οποίο υποστηρίζεται από το εργαλείο SOCRATES, επιτρέπει σε ομάδες ειδικών σε αυτά τα θέματα, αλλά και σε αναλυτές, να καθορίσουν παραδοχές ή παραμέτρους, σύμφωνα με τις οποίες τα τρία μοντέλα του MORDA, δηλαδή α) το μοντέλο αντιπάλου (adversary model), β) το μοντέλο χρήστη (user model) και το μοντέλο παροχέα υπηρεσιών (service provider), θα υλοποιηθούν και στη συνέχεια θα αναγνωρίσουν και θα εισάγουν τα δεδομένα για την παραγωγή αυτών των τριών μοντέλων.

Για το μοντέλο αντιπάλου, τα δεδομένα περιλαμβάνουν ήδη γνωστούς αντιπάλους και τις προτιμήσεις τους αναφορικά με τους τρόπους επίθεσης καθώς και τις τεχνικές που χρησιμοποιούν. Για το μοντέλο του παροχέα υπηρεσιών, τα δεδομένα περιλαμβάνουν ορισμούς των αντιμέτρων, δηλαδή των μέτρων προστασίας ή πρόληψης, εναλλακτικά σενάρια που χρησιμοποιούνται για την προστασία των συστημάτων πληροφορικής από τις συγκεκριμένες επιθέσεις και, τέλος, λεπτομερείς περιγραφές των προδιαγραφών ασφαλείας για κάθε εναλλακτικό σενάριο.

Επίσης, θα πρέπει να ληφθούν υπόψη οι προβληματισμοί των χρηστών και των παροχέων υπηρεσιών, όπως η λειτουργικότητα, η διασυνδεσιμότητα και η χρηστικότητα, που μπορούν να επηρεαστούν από πιθανές επιθέσεις, αντίμετρα ή εναλλακτικά σενάρια. Βασισμένο στα τρία μοντέλα του MORDA, το εργαλείο SOCRATES επιτρέπει στους αναλυτές:

- Να κατηγοριοποιήσουν ποιοτικά τις επιθέσεις και να χρησιμοποιήσουν μία ποσοτική κλίμακα για να εκτιμήσουν τον πιθανό αντίκτυπο, αναφορικά με τη μείωση της αξίας.
- Να καταγράψουν και να ποσοτικοποιήσουν την ικανότητα κάθε αντίμετρου στο να ενισχύσει την ασφάλεια των υποδομών ή του συστήματος πληροφορικής που εξετάζουν.
- Να ποσοτικοποιήσουν την αξία της ζημίας από την επίθεση στις υποδομές του οργανισμού, η οποία προκύπτει από τη μείωση των λειτουργιών των

συστημάτων, που προέρχεται από πιθανή αποτυχία των υπαρχόντων συστημάτων ασφαλείας.

Ως αποτέλεσμα της ποσοτικής εκτίμησης της αποτελεσματικότητας των αντιμέτρων, χρησιμοποιώντας βελτιστοποιήσεις και αναλύσεις κόστους-οφέλους, οι υπεύθυνοι λήψης αποφάσεων μπορούν πιο αποδοτικά να χρησιμοποιήσουν τους διαθέσιμους πόρους τους και να πετύχουν μειώσεις σε κόστη. Σύμφωνα με τους δημιουργούς του MORDA στο [54], οι κυριότερες αδυναμίες του είναι η εξάρτησή του από την εκτενή πρόσβαση σε ειδικούς θεμάτων και τα μεγάλα σύνολα δεδομένων που χρειάζονται για την παραγωγή των τριών μοντέλων του. Αυτές οι δύσκολες απαιτήσεις συλλογής δεδομένων κάνουν το MORDA ικανό να χρησιμοποιηθεί μόνο σε κρίσιμης σημασίας πληροφοριακά συστήματα που απαιτούν λεπτομερή και ακριβή ανάλυση κινδύνου.

4.7 Πρωτοβουλίες από εταιρείες της βιομηχανίας της πληροφορικής

Σε αυτό το σημείο της διατριβής, θα παρουσιαστούν πρωτοβουλίες της βιομηχανίας της πληροφορικής, για τη δημιουργία μέτρων διασφάλισης της ασφάλειας του κυβερνοχώρου και της ασφάλειας των πληροφοριών. Τέτοιες πρωτοβουλίες έχουν γίνει τόσο από εταιρείες που δραστηριοποιούνται στη βιομηχανία της πληροφορικής, όπως η CIS και η securitymetrics.org, που ασχολούνται με τον τομέα της ασφάλειας, όσο και από εταιρείες που δραστηριοποιούνται σε άλλους τομείς, όπως η ISACA, που δραστηριοποιείται στο χώρο του ελέγχου των συστημάτων πληροφορικής. Όπως οι προσπάθειες που έχουμε περιγράψει μέχρι τώρα, έτσι και ο στόχος των εταιρειών της αγοράς είναι να βελτιστοποιήσουν τα προγράμματα μέτρησης της ασφάλειας σε όλους τους τομείς, είτε αυτοί είναι κυβερνητικοί, είτε όχι.

4.7.1 Πρωτοβουλία από την εταιρεία CIS για μέτρα ασφάλειας

Η πρωτοβουλία της CIS παρουσιάστηκε στο [55], και η υλοποίησή της αναλήφθηκε από μία ομάδα ατόμων -μελών της-, συμπεριλαμβανομένων μελών από:

i. το Fortune 500 αλλά και άλλες μικρότερους εμπορικούς μη κερδοσκοπικούς οργανισμούς, που ενεργοποιούνται στον τραπεζικό και οικονομικό τομέα,
ii. κυβερνητικές υπηρεσίες,
iii. κατασκευαστές λογισμικού ασφάλειας,
iv. ειδικούς της πληροφορικής στον τομέα της ασφάλειας,
v. πανεπιστήμια,
vi. ανεξάρτητους ερευνητές,
vii. μαθηματικούς, στατιστικολόγους, αναλογιστές,
viii. υπεύθυνους τμημάτων ασφαλείας οργανισμών, και
ix. άλλα ινστιτούτα και πρόσωπα που ασχολούνται με τον τομέα της ασφάλειας των συστημάτων πληροφορικής.

Οι στόχοι αυτής της πρωτοβουλίας, είναι η επίτευξη της συναίνεσης σε αρχικά μικρό σύνολο (10 ή λιγότερες) σαφείς μετρήσεις ασφάλειας. Επιπλέον, η πρωτοβουλία επιδιώκει να καθιερώσει μια επιχειρησιακή υπηρεσία συγκριτικής αξιολόγησης για τη διευκόλυνση:

- της επικοινωνίας της εσωτερικής κατάστασης ασφαλείας με την πάροδο του χρόνου,
- της ενδοεπιχειρησιακής συγκριτικής αξιολόγησης της κατάστασης ασφαλείας, και

- της ανάπτυξης μίας βάσης δεδομένων από την οποία μπορούν να αναζητηθούν συσχετίσεις αναφορικά με τις τεχνικές ασφάλειας και τα αποτελέσματά τους.

Η πρωτοβουλία αυτή σκόπευε, μέχρι το τέλος του 2008, να είχε επιτύχει την συναίνεση για τον τελικό ορισμό των μέτρων και α) να συμπληρώσει τον χάρτη των μέτρων που ανέπτυσσε, και β) να υλοποιήσει την πλατφόρμα αξιολόγησης που θα επέτρεπε στην CIS, να ξεκινήσει τις υπηρεσίες της αναφορικά με τα μέτρα ασφάλειας και την αξιολόγηση αυτών.

Την άνοιξη του 2009, η CIS δημοσίευσε το «*CIS Security Metrics*» [56], στο οποίο περιέχονταν 21 ορισμοί μέτρων ασφαλείας για έξι επιχειρησιακές περιοχές. Τα μέτρα που παρουσιάστηκαν σε αυτή τη δημοσίευση αναπτύχθηκαν μέσα από μία συναινετική διαδικασία μεταξύ των ενδιαφερομένων και τα οποία παρουσιάζει ο Πίνακας 9:

Επιχειρησιακή περιοχή	Συναινετικά μέτρα ασφαλείας
Διαχείριση περιστατικών ασφαλείας (Incident management)	• Χρόνος μέχρι την ανακάλυψη ενός περιστατικού ασφαλείας. • Αριθμός περιστατικών ασφαλείας. • Ποσοστό περιστατικών ασφαλείας που ανιχνεύτηκαν από τα ήδη ανεπτυγμένα μέτρα ασφάλειας. • Χρόνος ανάμεσα σε δύο συνεχόμενα περιστατικά ασφαλείας. • Χρόνος μεταξύ της ανακάλυψης και περιορισμού ενός περιστατικού ασφαλείας. • Χρόνος μέχρι την τελική ανάκαμψη των

Επιχειρησιακή περιοχή	Συναινετικά μέτρα ασφαλείας
	συστημάτων πληροφορικής, από ένα περιστατικό ασφαλείας.
Διαχείριση ευπαθειών (Vulnerability Management)	• Εύρος περιοχής ανίχνευσης για ευπάθειες. • Ποσοστό συστημάτων πληροφορικής με κανένα γνωστό τύπο ευπάθειας υψηλού κινδύνου. • Αριθμός γνωστών ευπαθειών που έχουν βρεθεί.
Πολιτική εφαρμογής διορθώσεων ευπαθειών (Patch Management)	• Συμμόρφωση της πολιτικής εφαρμογής διορθώσεων στα πρότυπα. • Χρόνος μέχρι την εφαρμογή της διόρθωσης της ευπάθειας. • Χρόνος μέχρι την εφαρμογή (εγκατάσταση) κρίσιμων διορθώσεων.
Ασφάλεια εφαρμογών (Application Security)	• Αριθμός εφαρμογών • Ποσοστό εφαρμογών που θεωρούνται επιχειρησιακά κρίσιμες. • Εύρος περιοχής εκτίμησης κινδύνου. • Εύρος περιοχής ελέγχου για ευπάθειες ασφαλείας.
Διαχείριση διαμόρφωσης συστημάτων (Configuration Management)	• Χρόνος που χρειάζεται για την ολοκλήρωση αλλαγών. • Ποσοστό αλλαγών με αναφορές σε ευ-

Επιχειρησιακή περιοχή	Συναινετικά μέτρα ασφαλείας
	πάθειες ασφαλείας. • Ποσοστό αλλαγών με εξαιρέσεις από το πλαίσιο ασφαλείας που χρησιμοποιείται.
Οικονομικά (Finance)	• Ποσοστό εξόδων για τα συστήματα πληροφορικής, σε σχέση με το ποσό του προϋπολογισμού για αυτά. • Ποσό εξόδων στα συστήματα πληροφορικής που αφορούν θέματα ασφαλείας.

Πίνακας 9: Συναινετικά μέτρα ασφάλειας κατά CIS [56]

Τα μέτρα και οι ορισμοί τους καθορίστηκαν από τη συναίνεση μίας ομάδας ειδικών σε μια σειρά από θέματα, που ανήκουν σε διάφορες επιχειρησιακές περιοχές. Η ομάδα αυτή συγκροτήθηκε από:

- Συμβούλους.
- Προγραμματιστές.
- Ελεγκτές και ειδικούς για τη συμμόρφωση σε πρότυπα.
- Ερευνητές σε θέματα ασφάλειας πληροφοριακών συστημάτων.
- Εμπειρογνώμονες σε θέματα επιχειρησιακής ασφάλειας.
- Κυβερνητικούς εκπροσώπους.
- Νομικούς συμβούλους.

Ο στόχος της συναίνεσης ήταν να αναγνωριστούν μια σειρά από μέτρα ασφαλείας, τα οποία θα μπορούσαν να χρησιμοποιηθούν σε ένα ευρύ σύνολο οργανισμών και επιχειρήσεων, για τη μέτρηση της αποτελεσματικότητας και της αξίας των λειτουργιών και των εννοιών της ασφάλειας, όπως της διαθεσιμότητας των δεδο-

μένων (data availability), της διαχείρισης των μέτρων ασφάλειας (security management), και της απόδοσης των μέτρων ασφάλειας (security performance).

Επιπλέον από των μέτρων ασφαλείας, η ομάδα αναγνώρισε ένα σύνολο ιδιοτήτων των δεδομένων σχετικά με τα περιστατικά ασφάλειας, τα οποία πρέπει να συλλεχθούν έτσι ώστε να δοθεί η δυνατότητα να καθορίσουμε τις τιμές για πολλά από τα μέτρα που προτείνονται. Σύμφωνα με την CIS, επιπλέον μέτρα ασφάλειας θα καθοριστούν για αυτές αλλά και για άλλες επιχειρησιακές περιοχές, οι οποίες θα περιλαμβάνουν:

- Μέτρα ασφαλείας κακόβουλου λογισμικού (Anti-malware controls).
- Μέτρα για την επαλήθευση ταυτότητας και την αδειοδότηση (Authentication, authorization).
- Μέτρα για την ασφάλεια των δεδομένων και του δικτύου.
- Μέτρα για την μεθοδολογία ανάπτυξης λογισμικού Software Development Life Cycle - SDLC.
- Μέτρα για τις προσπάθειες ανάκαμψης από περιστατικά ασφαλείας.
- Διαχείριση κινδύνων από εξωτερικούς προς την επιχείρηση ελεγκτές – συνεργάτες.

4.7.2 Information Systems Audit and Control Association (ISACA)

Η ISACA είναι μία διεθνής ένωση του κλάδου των ελεγκτών συστημάτων πληροφορικής που απαριθμεί περισσότερα από 85.000 μέλη. Τα μέλη της απασχολούνται σε διάφορες θέσεις στον κλάδο της Πληροφορικής, συμπεριλαμβανομένων συμβούλων, εκπαιδευτικών, επαγγελματιών του χώρου της ασφάλειας συστημάτων πληροφορικής, υπαλλήλων σε ρυθμιστικές αρχές, διευθυντών πληροφορικής και ως εσωτερικοί ελεγκτές.

Τα τελευταία χρόνια, η ISACA έχει δημοσιεύσει πολλά άρθρα που ασχολούνται αποκλειστικά με το θέμα της ασφάλειας και των κερδών μιας επιχείρησης από τις επενδύσεις της σε αυτή, (Return On Security Investment – ROSI), καθώς επίσης και μελέτες που έχουν ως κεντρικό θέμα τη μέτρηση της ασφάλειας. Μία τέτοια μελέτη είναι η «*Information Security Governance: Guidance for Boards and Executive Management*» [57]. Η μελέτη αυτή αποτελεί ένα έργο αναφορικά με τα μέτρα ασφάλειας της πληροφορίας, το οποίο σκοπεύει να αποτελέσει τον οδηγό για τους διευθυντές ασφάλειας πληροφοριών, στο πώς να αναπτύξουν επιχειρησιακά και αποδοτικά προγράμματα μέτρησης της ασφάλειας.

Στο έκτο κεφάλαιο της μελέτης αυτής, παρέχεται μία χρήσιμη σύνοψη των θεμάτων και των προκλήσεων, που είναι συσχετισμένα με την υλοποίηση ενός προγράμματος μέτρησης της ασφάλειας και παρακολούθησης της ικανότητας να υποστηριχθεί η διακυβέρνηση (governance) της ασφάλειας των πληροφοριών. Στο κεφάλαιο αυτό αναφέρεται ότι η μέτρηση είναι αναγκαία για την αποδοτική διακυβέρνηση, και επεξηγεί μία σειρά θεμάτων που σχετίζονται με τη μέτρηση της ασφάλειας πληροφοριών, συμπεριλαμβανομένου του γεγονότος ότι τα παραδοσιακά μέτρα, όπως η ετήσια αναμενόμενη ζημία (Annual Loss of Expectancy - ALE), ο χρόνος που τα συστήματα πληροφορικής δεν λειτουργούσαν λόγω κάποιου περιστατικού ασφαλείας και ο αριθμός των εξυπηρετητών (servers) που έχουν εγκατεστημένες διορθώσεις ασφαλείας (patches), έχουν μικρή χρησιμότητα στο να παρέχουν μία συνολική εικόνα αναφορικά με το πόσο ασφαλής είναι μία επιχείρηση ή ένας οργανισμός.

Περαιτέρω, συνεχίζει και αναφέρει ότι η απουσία μιας ανεπιθύμητης ενέργειας δεν είναι χρήσιμος δείκτης του κατά πόσον ένας οργανισμός είναι ασφαλής, και ότι η χρήση ασκήσεων «προσομοίωσης», όπως δοκιμές διείσδυσης (penetration testing), έχουν περιορισμένη χρήση. Η μελέτη συμπεραίνει ότι:

- Κάποιοι οργανισμοί δέχονται επιθέσεις ή / και θα υποστούν ζημίες πιο συχνά από κάποιους άλλους.

- Υπάρχει μία στενή συσχέτιση μεταξύ της καλής διαχείρισης (management) της ασφάλειας των πληροφοριών και βέλτιστων πρακτικών, και των σχετικά λιγότερων περιστατικών ασφαλείας και ζημιών.

Η μελέτη της ISACA αναφέρεται στο γεγονός ότι, ενώ η διαχείριση (governance) των μετρήσεων αποτελεί εξίσου πρόκληση με τη μέτρηση της ασφάλειας είναι παρόλα αυτά αναγκαίο για τους οργανισμούς να προσπαθήσουν να αξιολογήσουν και τη διαδικασία διαχείρισης της ασφάλειας, με σκοπό την παρακολούθηση της προόδου των προγραμμάτων ασφάλειας, με απώτερο σκοπό την μείωση των κινδύνων ασφαλείας του οργανισμού. Στη μελέτη αναφέρεται ότι ενώ δεν υπάρχει ένας κοινά αποδεκτός τρόπος για τη μέτρηση της διακυβέρνησης της ασφάλειας των πληροφοριών, κάθε οργανισμός πρέπει να καθιερώσει τη δική του μέθοδο και κλίμακα βασιζόμενος στις δικές του ανάγκες. Στη συνέχεια προτείνει αρκετούς τρόπους αναφορικά με τη μέτρηση της διακυβέρνησης της ασφάλειας των πληροφοριών, συμπεριλαμβανομένων των παρακάτω:

- Εφαρμογή των διαδικασιών διακυβέρνησης για την παρακολούθηση της προόδου του πλαισίου διακυβέρνησης. Η μελέτη αναφέρει ότι ενώ η ασφάλεια πληροφοριών απέχει πολύ από τη διακυβέρνηση, δείκτες βασικών στόχων (Key Goal Indicators – KGIs) και δείκτες απόδοσης (Key Performance Indicators – KPIs) μπορούν να χρησιμοποιηθούν για να μας δώσουν πληροφορίες αναφορικά με την επίτευξη των διαδικασιών και των στόχων.
- Ευθυγράμμιση της στρατηγικής για την ασφάλεια των πληροφοριών με τη στρατηγική για την επίτευξη των επιχειρησιακών και οργανωτικών στόχων.
- Διαδικασίες διαχείρισης των κινδύνων (Risk Management) και παρακολούθηση της αποτελεσματικότητάς τους σε καθορισμένους στόχους.

- Αξιολόγηση για το κατά πόσον η αποδοχή κινδύνων πετυχαίνεται στο δυνατό χαμηλότερο κόστος για τον οργανισμό.
- Διαδικασία διαχείρισης πόρων, που να αξιολογεί εάν ο οργανισμός έχει αποτελεσματικά διαθέσει τους πόρους του αναφορικά με την ασφάλεια των πληροφοριών.
- Διαδικασία διαχείρισης της απόδοσης που να παρακολουθεί εάν ο οργανισμός έχει επιτύχει τους καθορισμένους στόχους του.
- Ενσωμάτωση διαδικασιών που να αξιολογούν την πρόοδο των διαδικασιών διασφάλισης.

Άλλες παρόμοιες μελέτες της ISACA είναι:

- «*Developing Metrics for Effective Information Security Governance*» στο [58], στο οποίο ο Pironti δηλώνει ότι η δημιουργία ενός πλαισίου για τη διαχείριση της ασφάλειας πληροφοριών, είναι καθοριστικός παράγοντας επιτυχίας. Συνεχίζει και προτείνει τη δημιουργία ενός μέτρου βασισμένου στις επιχειρησιακές ανάγκες του οργανισμού, το οποίο θα μετρά τη διακυβέρνηση της ασφάλειας α) στο ανθρώπινο δυναμικό, β) στις διαδικασίες, γ) στον τεχνολογικό τομέα και δ) στον τομέα της συμμόρφωσης σε κανονιστικά πλαίσια.
- «How can security be measured?» στο [59], στο οποίο ο David Chapin και Steven Akridge προτείνουν ένα πρόγραμμα ασφαλείας βασισμένο σε μοντέλα ωριμότητας, με σκοπό να παρακολουθήσουν την πρόοδο προς την επίτευξη ωριμότητας του προγράμματος ασφαλείας του οργανισμού.

4.7.3 Securitymetrics.org

Η Securitymetrics.org είναι μία διαδικτυακή κοινότητα που ιδρύθηκε από τον Andrew Jawuith το 2004. Ο σκοπός της κοινότητας αυτής είναι να φιλοξενήσει τους επαγγελματίες στον χώρο της μέτρησης της ασφάλειας. Για το σκοπό αυτό προσφέρει μία σειρά από υπηρεσίες στα μέλη της, όπως:

- Μία λίστα με τα emails των μελών της, μέσω της οποίας όλοι όσοι ασχολούνται με τον κλάδο της μέτρησης της ασφάλειας να μπορούν να επικοινωνήσουν μεταξύ τους και να ανταλλάξουν πληροφορίες.
- Συμμετοχή σε ομάδες εργασίες σχετικά με τη μέτρηση της ασφάλειας (Workshop on Security Metrics – MetriCon [56]) και σε συνέδρια της USENIX και RSA.
- Ανακοινώσεις για άρθρα που έχουν δημοσιευτεί από τα μέλη της.
- Εναλλακτικό τρόπο για τα μέλη της, για τη δημοσίευση της ερευνητικής τους προσπάθειας.

Πολλά από τα έργα που φιλοξενήθηκαν από τη securitymetrics.org αποτελούν σημείο αναφοράς για την κοινότητα που ασχολείται με την μέτρηση της ασφάλειας συστημάτων πληροφορικής. Ένα παράδειγμα τέτοιου έργου είναι το συνέδριο MetriCon, που έγινε το 2006, το οποίο αποτέλεσε το σημείο στο οποίο συγκεντρώθηκαν όλοι οι ειδικοί στον τομέα της ασφάλειας πληροφοριών και αντάλλαξαν τη γνώση και τις εμπειρίες τους.

Ένα άλλο μεγάλο έργο από την securitymetrics.org είναι σε εξέλιξη, το «*Metrics Catalog Project*», το οποίο είναι ένας χώρος για την αποθήκευση, οργάνωση και διαμοιρασμό των μέτρων ασφαλείας. Το έργο επίσης περιλαμβάνει μία βάση δεδομένων για τον ορισμό των μέτρων, διορθωτές (editors) για την υποβολή των μέτρων από τα μέλη της κοινότητας, ιστορικότητα εκδόσεων των μέτρων (versioning), αξιολογήσεις των μέτρων και άδειες χρήσης αυτών. Ο σκοπός αυτού του έργου είναι να παρέχει ένα κοινό και εύκολα προσβάσιμο χώρο, όπου όλοι οι

επαγγελματίες του χώρου καθώς και οι ερευνητές, θα μπορούν να εντοπίσουν, καθορίσουν, και επιλέξουν ένα μέτρο ασφάλειας για τον δικό τους οργανισμό ή επιχείρηση. Στην παρούσα φάση το έργο παρέχει πληροφορίες σχετικά με:

- Δεδομένα ασφαλείας σύμφωνα με το πρότυπο PCI [60].
- Μέτρα ασφαλείας που έχουν προταθεί από τη NIST [37].
- Μέτρα ασφαλείας που έχουν δημοσιευτεί στο [29] από τη NIST.
- Μέτρα ασφαλείας σύμφωνα με το πρότυπο ISO / IEC 27002:2005 [61].
- Μέτρα ασφαλείας που προτείνει η ομάδα εργασίας CIS WG [56].

Είναι φανερό ότι η υπάρχουσα λίστα είναι περιορισμένη, αλλά το *Metrics Catalog Project* [56] από την securitymetrics.org έχει τη δυναμική να αποτελέσει μία σημαντική πηγή πληροφοριών αναφορικά με τα διαθέσιμα προς τους ενδιαφερόμενους οργανισμούς μέτρα ασφαλείας των συστημάτων πληροφορικής.

4.8 Εργαλεία και μεθοδολογίες για Επιθεωρητές συστημάτων πληροφορικής

Όπως είναι φυσικό, η ύπαρξη ενός μέτρου υποδηλώνει ένα σύστημα αξιολόγησης των μετρήσεων. Οι Juneja, Arora και Duggal [62], μελέτησαν διεξοδικά τα χαρακτηριστικά ενός μέτρου για ένα σύστημα αξιολόγησης, καθώς και τις κατηγορίες που μπορεί αυτό να ανήκει. Σύμφωνα με την έρευνά τους, ένα ποιοτικό μέτρο πρέπει να τηρεί τις ακόλουθες συνθήκες:

i. Να είναι συγκεκριμένο (specific).
ii. Να είναι μετρήσιμο (measurable).
iii. Να μπορεί να ανιχνευθεί για να μετρηθεί (achievable).
iv. Η μέτρησή του να μπορεί να επιβεβαιωθεί και από κάποιον τρίτο ανεξάρτητο ερευνητή (repeatable).
v. Πρέπει να είναι εξαρτώμενο από τον παράγοντα του χρόνου (time-dependent).

Συνεχίζοντας την έρευνά τους, επιχειρηματολογούν ότι οποιοδήποτε μέτρο ανήκει και μπορεί να κατηγοριοποιηθεί σε μία από τις τέσσερις μεγάλες κατηγορίες, οι οποίες είναι:

1. Μέτρα διαχείρισης κινδύνων (risk management metrics).
2. Μέτρα δημοσιονομικής διαχείρισης (budget management metrics).
3. Μέτρα αξιολόγησης και συμμόρφωσης (audit and compliance metrics).
4. Μέτρα διαδικασιών ασφάλειας (security operation metrics).

Επιπλέον, ανεξαρτήτως της κατηγορίας στην οποία ανήκει ένα μέτρο, υπάρχουν μερικές σημαντικές πτυχές που πρέπει κάποιος να λαμβάνει υπόψη του, όταν προτείνει τη δημιουργία νέων μέτρων. Για το λόγο αυτό λοιπόν προτείνουν ότι κάθε μέτρο πρέπει:

- Να διασφαλίζει την ορθότητα και την αποτελεσματικότητα.
- Να διακρίνεται ως «πριν» ή «μετά» δείκτης, ο οποίος αντικατοπτρίζει τις συνθήκες ασφάλειας οι οποίες υπάρχουν πριν ή μετά αντίστοιχα, από τη αλλαγή στο πλαίσιο ασφάλειας.
- Να λαμβάνει υπόψη του κάθε επιχειρησιακό στόχο αναφορικά με την ασφάλεια των συστημάτων πληροφορικής.
- Να έχει ποσοτικά ή ποιοτικά χαρακτηριστικά.
- Να χρησιμοποιείται σε μετρήσεις σε σχετικά μικρές περιοχές αξιολόγησης, διότι οι μεγάλες και πολύπλοκες περιοχές προς αξιολόγηση χρειάζονται περισσότερο και διεξοδικότερο έλεγχο για να αξιολογηθούν.

Η προσέγγισή τους, χωρίς αμφιβολία, χρειάζεται για τον καθορισμό των χαρακτηριστικών μέτρων και συστημάτων αξιολόγησης, αλλά στοχεύει στην κατηγοριοποίηση των μέτρων που υπάρχουν –ή που θα δημιουργηθούν- και όχι στη δη-

μιουργία μιας μεθόδου μέτρησης του επιπέδου ασφάλειας ενός συστήματος πληροφορικής.

4.9 Διάφορες ταξινομήσεις ευπαθειών

Μια μεγάλη κατηγορία ερευνητών στην προσπάθειά τους να μετρήσουν το επίπεδο ασφάλειας ενός συστήματος προχώρησαν στη δημιουργία ταξινομήσεων των ευπαθειών που εμφανίζονται στα συστήματα πληροφορικής, βάσει των οποίων θα μπορεί κάποιος να τα αξιολογήσει.

4.9.1 Ταξινόμηση κατά NIST

Στην ειδική δημοσίευση της NIST, SP 800-55 Rev 1 [29], παρουσιάζονται οι τύποι των μέτρων ασφάλειας που μπορεί να έχει ένα σύστημα πληροφορικής. Πρόκειται για μία κατηγοριοποίηση των μέτρων ασφάλειας σε τρείς τομείς: α) των μέτρων εφαρμογής, β) των μέτρων μέτρησης της απόδοσης / αποτελεσματικότητας και γ) των μέτρων μέτρησης των επιπτώσεων που έχουν τα μέτρα στον οργανισμό που τα εφαρμόζει.

4.9.1.1 Μέτρα Εφαρμογής

Τα μέτρα που ανήκουν στην κατηγορία αυτή, χρησιμοποιούνται για να αναδείξουν την εξέλιξη: α) της εφαρμογής των προγραμμάτων ασφαλείας ενός οργανισμού, β) των ειδικών ελέγχων ασφαλείας (security controls), γ) της ασφάλειας σε επίπεδο του συστήματος, καθώς και δ) των πολιτικών, διαδικασιών που σχετίζονται με τα προαναφερθέντα.

Ενδεικτικά τέτοια μέτρα **ασφάλειας** (security controls) είναι:

1. Ποσοστό συστημάτων πληροφορικής που έχουν εγκεκριμένο πλάνο ασφάλειας.

2. Ποσοστό συστημάτων πληροφορικής που έχουν την πρέπουσα πολιτική διαχείρισης συνθηματικών (passwords).
3. Ποσοστό εξυπηρετητών στον οργανισμό που έχουν φτιαχτεί να ακολουθούν ένα προκαθορισμένο προφίλ ρυθμίσεων.
4. Ποσοστό συστημάτων πληροφορικής που έχουν αναγνωριστεί και αξιολογηθεί ως κρίσιμα συστήματα.
5. Ύπαρξη καταγεγραμμένων στόχων διασφάλισης (assurance objectives) των συστημάτων πληροφορικής.

4.9.1.2 Μέτρα μέτρησης της αποτελεσματικότητας / απόδοσης

Τα μέτρα που ανήκουν στην κατηγορία αυτή χρησιμοποιούνται για να καθορίσουν εάν οι διαδικασίες των εφαρμογών και οι έλεγχοι ασφαλείας σε επίπεδο συστήματος έχουν εφαρμοστεί σωστά, λειτουργούν όπως αναμενόταν, και έχουν επιτύχει το σκοπό τους. Τα μέτρα της αποτελεσματικότητας / απόδοσης αντικατοπτρίζουν δύο πτυχές της εφαρμογής των ελέγχων ασφαλείας (security control implementation): α) το ίδιο το αποτέλεσμα, δηλαδή πόσο αποτελεσματικό είναι και β) πόσο αποδοτικό είναι.

Ενδεικτικά τέτοια μέτρα **αποτελεσματικότητας** (effectiveness) είναι:

1. Ποσοστό συμβάντων παραβίασης της ασφάλειας των πληροφοριών (information security incidents), που συνέβησαν λόγω κακής ρύθμισης των ελέγχων πρόσβασης (access control).
2. Ποσοστό αναπάντεχων και ανεπιθύμητων συμβάντων ασφαλείας που έχουν καταγραφεί.

Ενδεικτικά τέτοια μέτρα **αποδοτικότητας** (efficiency) είναι:

1. Ποσοστό από τα μέρη ενός συστήματος (system components) που συντηρούνται σύμφωνα με το καθορισμένο πρόγραμμα.
2. Πόσος χρόνος χρειάστηκε για να υπάρξει αντίδραση σε ένα συμβάν ασφαλείας;
3. Πόσος χρόνος χρειάστηκε για να ανακάμψουν πλήρως τα συστήματα πληροφορικής μετά από μία απρόσμενη διακοπή τους;

4.9.1.3 Μέτρα μέτρησης των επιπτώσεων

Το μέτρα που ανήκουν στην κατηγορία αυτή χρησιμοποιούνται για να καθορίσουν τον αντίκτυπο (στην επιχείρηση ή στους επιχειρηματικούς στόχους) της ασφάλειας των πληροφοριών αναφορικά με την ικανότητα της επιχείρησης να εκπληρώσει το σκοπό της. Ανάλογα με τον σκοπό της επιχείρησης, τα μέτρα αυτά είναι δυνατό να ποσοτικοποιήσουν παράγοντες όπως:

1. Μειώσεις σε κόστη που προέρχονται από την εφαρμογή μέτρων ασφάλειας των πληροφοριών.
2. Κόστος για κάθε συμβάν αναφορικά με την ασφάλεια των πληροφοριών.
3. Κόστη που δημιουργήθηκαν κατά την αντιμετώπιση συμβάντων σχετικών με την ασφάλεια των πληροφοριών.
4. Βαθμός δημόσιας αποδοχής που κερδήθηκε ή διατηρήθηκε λόγω της εφαρμογής του προγράμματος ασφάλειας των πληροφοριών.
5. Διαφορές μεταξύ των προϋπολογισθέντων και των πραγματοποιηθέντων δαπανών για την εκπαίδευση σε θέματα ασφάλειας των πληροφοριών.
6. Return On Investment (ROI) από κόστη που σχετίζονται με τα μέτρα ασφάλειας σε σχέση με τις αναμενόμενες ζημίες (expected losses), από πι-

θανές παραβιάσεις ασφαλείας που θα συνέβαιναν αν οι συγκεκριμένοι στόχοι (συστήματα πληροφορικής) δεν προστατεύονταν.

7. Κάθε άλλη επίπτωση που σχετίζεται με τους στόχους της επιχείρησης και προέρχεται από την ασφάλεια των πληροφοριών.

Ενδεικτικά τέτοια μέτρα **μέτρησης των επιπτώσεων** είναι:

1. Ποσοστό από τον προϋπολογισμό της επιχείρησης που αφιερώνεται σε μέτρα ασφάλειας.
2. Αριθμός από επενδύσεις σε μέτρα ασφάλειας των πληροφοριών.

4.9.2 Ταξινόμηση Rejo Savola

Ο Reijo Savola στο [63], αναζητεί ενδείξεις που μπορούν να παρέχουν αποδεικτικά στοιχεία για το πόσο αποτελεσματικά είναι τα μέτρα ασφαλείας στο να μειώσουν τους κινδύνους, καθώς και το βαθμό μείωσης του επιπέδου του ρίσκου που αναμένουμε από τα μέτρα αυτά. Για το σκοπό αυτό, προτείνει μία νέου τύπου ταξινόμηση των μέτρων ασφάλειας για προϊόντα νέας τεχνολογίας, πληροφορικής και επικοινωνιών (Information Communication Technology products), η οποία βασίζεται στην εκτενή μελέτη του στη διεθνή βιβλιογραφία. Όπως αναφέρθηκαν στην παράγραφο § 4.1 και εκείνος κάνει τον διαχωρισμό μεταξύ «μέτρου» και «μέτρησης» και συνεχίζει τονίζοντας την αναγκαιότητα χρήσης δεικτών ασφαλείας για τη μέτρηση του επιπέδου ασφάλειας ενός συστήματος πληροφορικής.

Το προτεινόμενο μοντέλο ταξινόμησης, είναι μία ταξινόμηση υψηλού επιπέδου των μέτρων ασφάλειας που προέρχεται από τις περιοχές της οργάνωσης και διαχείρισης της πληροφορίας μιας επιχείρησης (organizational information security management) αλλά και της ανάπτυξης / κατασκευής των προϊόντων (product development).

Το βασικό επιχείρημά του είναι ότι το θέμα «ασφάλεια» είναι άρρηκτα συνδεδεμένο με τους ανθρώπους μίας επιχείρησης. Για αυτό, ο ένας πρέπει να μπορεί και να ωφελείται από την εμπειρία του άλλου και όχι να προσπαθεί να ξαναεφεύρει τον τροχό –όπως χαρακτηριστικά αναφέρει-. Παρόλο που η ταξινόμηση που προτείνει μας παρέχει μία εικόνα της επιχείρησης, δεν καταφέρνει να μας δώσει την τεχνική για να δημιουργήσουμε ένα καθαρό αριθμό για τη μέτρηση του επιπέδου της ασφάλειας μίας υπηρεσίας ή ενός συστήματος πληροφορικής.

4.9.3 Ταξινόμηση κατά Institute Information Protection (I3P)

Το Ινστιτούτο I3P είναι μια εθνική κοινοπραξία κορυφαίων ακαδημαϊκών ιδρυμάτων, ομοσπονδιακών χρηματοδοτούμενων εργαστηρίων, και μη κερδοσκοπικών οργανώσεων που ασχολούνται με την ενίσχυση της υποδομής στον κυβερνοχώρο των Ηνωμένων Πολιτειών [64]. Ο σκοπός του Ινστιτούτου I3P είναι να κατηγοριοποιήσει τη μέτρηση της ασφάλειας των συστημάτων ελέγχου διαδικασιών (process control systems), όπως για παράδειγμα τα συστήματα Supervisory Control And Data Acquisition (SCADA).

Από τη στιγμή που δεν υπάρχει ένας παγκόσμια αποδεκτός τρόπος ή μέθοδος για τη μέτρηση των κινδύνων στον κυβερνοχώρο από τις προσπάθειες για παραβίαση της ασφάλειας, το I3P προτείνει έναν πολύ-παραγοντικό τρόπο κατάταξης ή ταξινόμησης, ο οποίος θα βοηθά στη λήψη των αποφάσεων στα διάφορα επίπεδα διοίκησης μέσα σε μία επιχείρηση. Πιο απλά, πιστεύουν ότι αν μία επιχείρηση μπορεί να αντιμετωπίσει τους κινδύνους που προέρχονται από τα συστήματα πληροφορικής που διαθέτει σε διοικητικό επίπεδο, τότε θα έχει αντιμετωπίσει και τα τεχνικά θέματα που πιθανώς θα προέκυπταν. Το πρόβλημα λοιπόν εστιάζεται σε διοικητικό και όχι σε τεχνικό επίπεδο.

Οι εμπνευστές αυτού του τύπου ταξινόμησης, χρησιμοποίησαν ως σημείο έναρξης / αναφοράς, τρείς ταξινομήσεις για τη διασφάλιση της ασφάλειας της πληροφορίας:

- Την κατηγοριοποίηση των μέτρων διασφάλισης της πληροφορίας που περιγράφονται στο WISSSR [65].
- Τους στόχους ελέγχου στα πρότυπα ISO / IEC 17799:2005 [66] και ISO / IEC 27001:2005 [67].
- Τις κατηγορίες τεχνολογιών σύμφωνα με το American National Standards Institute (ANSI) / International Society of Automation (ISA) [68].

Η ταξινόμηση κατά I3P χωρίζει τα μέτρα ασφάλειας σε τρείς κατηγορίες:

1. Οργανωτική (Organizational).
2. Επιχειρησιακή (Operational).
3. Τεχνική (Technical).

Στη συνέχεια προσθέτει άλλες δύο κατηγορίες για να περιλάβει και τα μέτρα ασφάλειας που περιγράφονται τόσο στο ISO / IEC 1799:2005 [66], όσο και στο ANSI / ISA – TR 99.00.01-2004 [68]. Αυτοί που κάνουν τις ταξινομήσεις θεωρούν ότι τα ακόλουθα μετρήσιμα στοιχεία της ασφάλειας των πληροφοριών ή ενός συστήματος πληροφορικής μπορούν να συσχετισθούν με μία ή και περισσότερες κατηγορίες. Ο Πίνακας 10 περιγράφει τιςκατηγορίες αυτές.

Μετρήσιμα στοιχεία	ISO/IEC 1799:2005	ISA TR99.1	Metrics		
			Οργανωτική (Organizational)	Επιχειρησιακή (Operational)	Τεχνικής (Technical)
Πολιτική ασφάλειας (Security Policy)	✓		✓	✓	
Εκτίμηση ευπαθειών και κινδύνων (Vulnerability and Risk Assessment)		✓		✓	
Οργανωτική Ασφάλεια (Organizational Security)	✓		✓		
Προσδιορισμός και έλεγχος των περιουσιακών στοιχείων (Asset clarification and control)	✓		✓		✓
Ασφάλεια προσωπικού (Personnel Security)	✓	✓	✓		
Φυσική και περιβαλλοντική ασφάλεια (Physical and Environmental Security)	✓	✓	✓		
Οργανωτική Διαχείριση και Διαχείριση επικοινωνιών (Communications and Operations Management)	✓			✓	
Έλεγχος πρόσβασης (Access Control)	✓	✓		✓	
Ανάπτυξη και συντήρηση των συστημάτων (Systems Development and Maintenance)	✓			✓	✓

Μετρήσιμα στοιχεία	ISO/IEC 1799:2005	ISA TR99.1	Metrics		
			Οργανωτική (Organizational)	Επιχειρησιακή (Operational)	Τεχνικής (Technical)
Διαχείριση Επιχειρησιακής Συνέχειας (Business Continuity Management)	✓		✓	✓	
Συμμόρφωση σε κανονιστικό πλαίσιο (Compliance)	✓		✓		

Πίνακας 10: Αντιστοίχιση μετρήσιμων στοιχείων ασφάλειας με τις κατηγορίες μέτρων ασφάλειας

4.9.4 Ταξινόμηση κατά Nabil Seddigh et. al.

Οι Seddigh et. al. στο [69] ασχολήθηκαν στον τομέα μέτρων διασφάλισης της πληροφορίας, με τις υποδομές των συστημάτων πληροφορικής και ειδικότερα με τα δίκτυα πληροφορικής. Αυτό που προτείνουν είναι μία νέα ταξινόμηση για τη διασφάλιση της πληροφορίας η οποία λαμβάνει υπόψη της τρία βασικά στοιχεία: α) την ασφάλεια, β) την ποιότητα των υπηρεσιών των δικτύων και γ) τη διαθεσιμότητα των δικτύων. Υποστηρίζουν ότι απαιτείται ένα ολοκληρωμένο και τυποποιημένο σύνολο μετρήσεων της ποιότητας και των δεικτών, παρόμοιο με αυτά που υπάρχουν ήδη στη χρηματοοικονομική αγορά ή αγορά εμπορευμάτων.

Προς αυτή την κατεύθυνση, μελέτησαν παρόμοιες ταξινομήσεις που έχουν κατά καιρούς προταθεί από διάφορους ερευνητές ή οργανισμούς, όπως η ταξινόμηση κατά NIST [29] που αναφέρθηκε στην παράγραφο § 4.9.1, ή η ταξινόμηση κατά Vaughn et al. [70] και τελικά πρότειναν μία δική τους. Η ταξινόμηση που προτείνουν κατηγοριοποιεί τα μέτρα σε τρείς κατηγορίες αυτές της: α) ασφάλειας, β) της ποιότητας παρεχομένων υπηρεσιών και γ) της διαθεσιμότητας, οι οποίες με τη σειρά τους χωρίζονται σε άλλες τρείς υποκατηγορίες μέτρων: α) τα οργανωτι-

κά, β) τα τεχνικά και γ) τα επιχειρησιακά. Με την κατηγοριοποίηση κάθε μέτρου σύμφωνα με τη δική τους ταξινόμηση, υλοποιούν τα μέτρα διασφάλισης της πληροφορίας (Information Assurance Metrics). Παρόλα αυτά, όπως και εκείνοι παραδέχονται, σύμφωνα με τη δική τους μεθοδολογία ταξινόμησης, κάποια μέτρα μπορεί να κατηγοριοποιηθούν σε περισσότερες από μία κατηγορίες. Για αυτό, η προτεινόμενη μεθοδολογία τους ενώ προσφέρει ένα πλαίσιο για τη διασφάλιση της πληροφορίας, δεν είναι ούτε αντικειμενική, ούτε παρέχει ένα αριθμητικό αποτέλεσμα βάσει του οποίου μπορούμε να μετρήσουμε το επίπεδο ασφάλειας ενός συστήματος πληροφορικής.

4.9.5 Ταξινόμηση κατά Pratyusa K. et. al.

Διαφορετική προσέγγιση είχαν οι ερευνητές Pratyusa K., Manadhata και Jeannette M. Wing στο [71]. Αυτό που προτείνουν, είναι να δημιουργηθεί ένα νέο μέτρο, το οποίο θα ονομάζεται «επιφάνεια επίθεσης» (attack surface). Το μέτρο της «επιφάνειας επίθεσης» θα μπορούσε, δυνητικά, να χρησιμοποιηθεί τόσο από τη βιομηχανία όσο και από μεμονωμένους χρήστες. Αυτό που οραματίζονται είναι όλοι οι προγραμματιστές εφαρμογών καθώς και οι μεμονωμένοι χρήστες να χρησιμοποιούν αυτό το νέο εργαλείο, για να μετρούν σε τακτά χρονικά διαστήματα την «επιφάνεια επίθεσης» στα συστήματά τους.

Ακόμα παραπέρα, θα μπορούν μόνοι τους να αντιπαραβάλλουν τα αποτελέσματα της μέτρησής τους με προηγούμενες μετρήσεις που πιθανώς θα έχουν κάνει, δίνοντάς τους έτσι τη δυνατότητα να παρακολουθούν την πορεία του επιπέδου ασφάλειας του συστήματός τους. Ο ορισμός που δίνουν στον όρο «επιφάνεια επίθεσης» είναι «*το σύνολο των μεθόδων / τρόπων που μπορεί να χρησιμοποιήσει ένας κακόβουλος χρήστης για να επιτεθεί στο σύστημα πληροφορικής που διαθέτουμε*». Ένα τέτοιο παράδειγμα θα ήταν η εκμετάλλευση της υπερχείλισης μίας ενδιάμεσης μνήμης, ευρέως γνωστή με τον όρο «buffer overflow».

Προκειμένου να μετρηθεί η «επιφάνεια επίθεσης» έχουν προτείνει την εισαγωγή δύο νέων εννοιών, της πιθανής ζημιάς και της προσπάθειας. Όσο η δυνητική ζημία ενός πόρου του συστήματος από επίθεση γίνεται μεγαλύτερη, τόσο μεγαλύ-

τερη θεωρούν ότι είναι και η επιφάνεια επίθεσης του εν λόγω συστήματος. Από την άλλη πλευρά, όσο μεγαλύτερη είναι η προσπάθεια ενός πιθανού εισβολέα προκειμένου να αποκτήσει παράνομη πρόσβαση στο σύστημα, τόσο μικρότερη θεωρούν ότι είναι και η επιφάνεια επίθεσης του συστήματος. Είναι πράγματι ένας τρόπος για να παραχθεί ένα μέτρο για την ποσοτικοποίηση του επιπέδου ασφάλειας ενός συστήματος πληροφορικής, αλλά η έννοια «προσπάθεια» είναι ανοικτή σε διάφορες ερμηνείες ανάλογα με το άτομο που χρησιμοποιεί τη μέθοδο και τα διαθέσιμα εργαλεία και πόρους. Οι hackers, πλέον, χρησιμοποιούν αρκετά αυτοματοποιημένα εργαλεία (automated tools) καθώς και ελεγχόμενα από αυτούς δίκτυα (botnets), οπότε μπορούν να κάνουν κατανεμημένες επιθέσεις μεγάλου μεγέθους. Ως εκ τούτου, η προτεινόμενη ταξινόμηση δεν μπορεί να χρησιμοποιηθεί προκειμένου να παρασχεθεί μία αριθμητική και αμερόληπτη μέτρηση για το επίπεδο ασφάλειας ενός συστήματος.

4.10 Συστήματα αξιολόγησης

Μία από τις πολλές προσεγγίσεις που ακολούθησαν αρκετοί ερευνητές στην προσπάθειά τους να μετρήσουν το επίπεδο ασφάλειας ενός συστήματος πληροφορικής, ήταν να αναπτύξουν διάφορες μεθοδολογίες ή συστήματα αξιολόγησης. Η κεντρική ιδέα των συστημάτων αυτών, είναι η παραγωγή ενός αμερόληπτου αριθμητικού αποτελέσματος που θα οδηγήσει στην αναμενόμενη ποσοτικοποίηση της ασφάλειας ενός συστήματος πληροφορικής. Για το σκοπό αυτό, έχουν αναπτύχθει αρκετά μοντέλα και τρόποι βαθμολόγησης, βασιζόμενοι σε κάποια ιδιότητα των συστημάτων πληροφορικής.

4.10.1 Πυκνότητα ευπαθειών

Η ύπαρξη ευπαθειών στο λογισμικό ενός συστήματος, καθώς και η χρήση της έννοιας της «πυκνότητας των ευπαθειών» (vulnerability density) για την μέτρηση της αξιοπιστίας του λογισμικού, αποτελούν την προσέγγιση του Alhazmi et al. στο [72]. Μετρώντας την «πυκνότητα των ευπαθειών», ή αλλιώς την «πυκνότη-

τα ελαττωμάτων» (defect density) ενός λογισμικού, σύμφωνα με τον ερευνητή, μας δίνει τη δυνατότητα να αποφασίσουμε αν υπάρχει ανάγκη για περαιτέρω δοκιμές ή διαδικασίες βελτίωσης. Οι Alhazmi et al. υποστηρίζουν, ότι ενώ η «πυκνότητα ελαττωμάτων» χρησιμοποιείται ως παράγοντας για την κυκλοφορία ενός λογισμικού στην αγορά, δεν υπάρχει παρόμοια διαδικασία αναφορικά με τις ευπάθειες ασφάλειας ενός συστήματος πληροφορικής. Συνεχίζει την έρευνά του, δίνοντας ένα ορισμό για τον όρο «πυκνότητα ευπαθειών», ως τον αριθμό των ευπαθειών που εμφανίζονται για κάθε μονάδα μεγέθους πηγαίου κώδικα (1000 γραμμές πηγαίου κώδικα). Έτσι, ένα σύστημα με υψηλό βαθμό ελαττωμάτων ή υψηλή «πυκνότητα ευπαθειών» είναι πιθανό να δεχθεί μία επίθεση με μεγαλύτερη συχνότητα σε σχέση με κάποιο άλλο που έχει χαμηλή «πυκνότητα ευπαθειών».

Υποστηρίζουν ότι η υιοθέτηση του μέτρου της «πυκνότητας ευπαθειών», στη διαδικασία ανάπτυξης λογισμικού (Software Development Life Cycle), θα μπορούσε αδιαμφισβήτητα να ωφελήσει τους κατασκευαστές λογισμικού, αφού, αφενός θα μείωνε σημαντικά τους κινδύνους από τα ελαττώματα του λογισμικού και αφετέρου τα κόστη που σχετίζονται με αυτά. Το μειονέκτημα αυτής της μεθοδολογίας είναι ότι χρησιμοποιεί είτε τον αριθμό των γραμμών πηγαίου κώδικα που χρειάζεται ένα σύστημα πληροφορικής, είτε το μέγεθος των εκτελέσιμων αρχείων του. Επιπλέον, στις ημέρες μας, που η τάση για τη χρησιμοποίηση του υπολογιστικού νέφους (cloud computing) συνεχώς αυξάνεται, και που η χρήση των διαδικτυακών υπηρεσιών (web-services) είναι ήδη αναπόσπαστο μέρος της καθημερινής διαδικασίας ανάπτυξης λογισμικού, η υιοθέτηση τέτοιων μεθοδολογιών σίγουρα δεν θα μπορούσε να πετύχει τα επιθυμητά αποτελέσματα.

4.10.2 Συντελεστής Ευπάθειας Προγράμματος

Στον τομέα της αξιοπιστίας του λογισμικού, οι Sridharan και Kaeli στο [73] προτείνουν ένα νέο μέτρο για τη μέτρηση των ευπαθειών του λογισμικού, που ονόμασαν «συντελεστή ευπάθειας προγράμματος» (Program Vulnerability Factor). Η μελέτη τους βασίστηκε στην ανάλυση ACE, η οποία επιτρέπει στους ερευνητές να ποσοτικοποιήσουν το «συντελεστή ευπαθειών της αρχιτεκτονικής του υλικού

(hardware)» (Architectural Vulnerability Factor), με τη χρήση προσομοιωτών για παράδειγμα. Ο «συντελεστής ευπαθειών της αρχιτεκτονικής του υλικού», ενός επεξεργαστή, ορίζεται ως η πιθανότητα ύπαρξης λάθους στην αρχιτεκτονική που θα μπορούσε να οδηγήσει σε εμφανές λάθος στις διαδικασίες εξόδου (output) ενός προγράμματος.

Η δουλειά τους επικεντρώνεται κυρίως στα πιθανά ελαττώματα των μικροεπεξεργαστών, και γίνεται μία προσπάθεια να επεκτείνουν αυτή τη θεωρία στο χώρο της αξιοπιστίας του λογισμικού. Δεδομένου ότι κάθε επεξεργαστής έχει κάποιο ρυθμό μικρών λαθών (soft errors rate - SER), αυτό σημαίνει, όπως υποστηρίζουν, ότι τα προγράμματα που εκτελούνται στον συγκεκριμένο επεξεργαστή πιθανότατα θα εμφανίσουν κάποια εμφανή λάθη. Σίγουρα αυτό μπορεί να θεωρηθεί ως ένα σημείο έναρξης για την προσέγγιση του τομέα της αξιοπιστίας του λογισμικού, όμως, όσον αφορά την ποσοτικοποίηση της ασφάλειας ενός συστήματος πληροφορικής, αυτή η τεχνική δεν μπορεί να βρει τομέα εφαρμογής. Αυτό γίνεται για τους εξής λόγους: α) λόγω της πολυπλοκότητας των προγραμμάτων που χρησιμοποιούνται στα σύγχρονα συστήματα πληροφορικής, β) λόγω της κυριαρχίας των διαδικτυακών υπηρεσιών (web-services), και γ) λόγω της ολοένα και αυξανόμενης τάσης χρησιμοποίησης του υπολογιστικού νέφους (cloud computing).

4.10.3 Ποσοτικοποίηση του κινδύνου για αποτελεσματικές στρατηγικές επενδύσεων

Μία πολύ ενδιαφέρουσα έρευνα έγινε από τους Carin, Cybenko και Huges στο [74]. Αυτό που προτείνουν είναι μία νέα ποσοτική μέθοδος εκτίμησης των κινδύνων (quantitative risk assessment), η οποία είναι βασισμένη σε ένα συνδυασμό της θεωρίας της επιστήμης των υπολογιστών, της οικονομικής θεωρίας, της θεωρίας παιγνίων και της θεωρίας ελέγχου. Η προτεινόμενη μεθοδολογία ονομάζεται «ποσοτικοποίηση του κινδύνου για αποτελεσματικές στρατηγικές επενδύσεων» (*Quantitative Evaluation of Risk for Investment Efficient Strategies «QuERIES»*), και περιέχει α) το σχηματισμό ενός οικονομικού μοντέλου επίθεσης / άμυνας, προσαρμοσμένη ως ένα θεωρητικό παιχνίδι, β) το σχηματισμό ενός μοντέλου

επίθεσης και, τελικά, γ) την ποσοτική σύγκριση των αποτελεσμάτων των δύο μοντέλων. Για την ποσοτικοποίηση των αποτελεσμάτων των πρώτων δύο μοντέλων χρησιμοποίησαν τις διεργασίες λήψης αποφάσεων κατά Markov (Markov's decision processes), και, συγκεκριμένα, τις πεπερασμένες αλυσίδες κατά Markov (finite Markov's chain), οι οποίες υπάρχουν ορισμένες στο πλαίσιο της θεωρίας ελέγχου, της επιστήμης της επιχειρησιακής έρευνας και της επιστήμης των οικονομικών, εδώ και πολλά χρόνια.

Τέλος, χρησιμοποίησαν τη θεωρία της πληροφορίας των αγορών (*Information –or Decision- Markets Theory)*, από τον χώρο των οικονομικών, με σκοπό να προβάλουν τα ευρήματά τους στο μέλλον και να δημιουργήσουν μία πρόβλεψη της πιθανότητας και του κόστους των επιτυχημένων επιθέσεων σε σχέση με τα προτεινόμενα και τα εγκατεστημένα μέτρα ασφάλειας. Το θεωρητικό υπόβαθρο που χρησιμοποιήθηκε σε καμία περίπτωση δεν αμφισβητείται καθώς είναι βασισμένο σε μεγάλο όγκο ιστορικών δεδομένων από τους χώρους της οικονομικής και ασφαλιστικής βιομηχανίας. Παρόλα αυτά, όπως και οι ίδιο παραδέχονται, λόγω α) της έλλειψης ενός θεωρητικού πλαισίου και β) αναλογιστικών στοιχείων από τον ασφαλιστικό κλάδο, τα δεδομένα που χρησιμοποιήθηκαν στο προτεινόμενο μοντέλο, προέρχονται από μοντέλα προσομοίωσης επιθέσεων και ως εκ τούτου δεν είναι αμερόληπτα αλλά υποκειμενικά. Εδώ πρέπει να σημειωθεί, ότι αυτή η ερευνητική προσπάθεια χρησιμοποιεί στοιχεία του μαθηματικού υπόβαθρου της παρούσης έρευνας, εντούτοις δεν έχει σχέση με την παρούσα έρευνα.

4.10.4 Κοινό πλαίσιο αξιολόγησης ευπαθειών CVSS

Μία γενική παρουσίαση των μέτρων ασφάλειας για τα συστήματα πληροφορικής καθώς και μια εξήγηση για την ύπαρξή τους επιχειρούν οι Patriciu, Priescu και Nicolaescu στο [75]. Σύμφωνα με τη μελέτη τους, μία στροφή προς την ασφάλεια έχει γίνει κατά τη διάρκεια των τελευταίων ετών και αρκετοί κυβερνητικοί κανονισμοί έχουν εισαχθεί, όπως του πλαισίου αρχών κατά GLBA (Gramm-Leach-Bliley Act), του πλαισίου αρχών κατά HIPAA (Health Insurance Portability and Accountability Act), του πλαισίου αρχών κατά FISMA (Federal Information Securi-

ty Management Act) του 2002– για τις ΗΠΑ, και της κοινοτικής οδηγίας για την προστασία των δεδομένων (The Data Protection Directive 95/46/EC) του Ευρωπαϊκού Κοινοβουλίου– για την Ευρωπαϊκή Ένωση.

Η έρευνα παρουσιάζει με λεπτομέρεια το κοινό πλαίσιο αξιολόγησης ευπαθειών CVSS (Common Vulnerability Scoring System), το οποίο είναι ένα σύστημα μέτρων για την αξιολόγηση των ευπαθειών ασφάλειας καθώς και μέτρων σχετικά με την ακεραιότητα και αξιοπιστία των δικτυακών υποδομών και συστημάτων. Το σύνολο των μέτρων αυτών χρησιμοποιούνται για την αξιολόγηση των μέτρων ασφαλείας των πληροφοριών. Για την ποσοτικοποίηση της ακεραιότητας των δικτυακών υποδομών και των υποδομών των συστημάτων, οι ερευνητές προτείνουν την υιοθέτηση συστημάτων συνεχούς παρακολούθησης των δικτύων και των συστημάτων (monitoring systems), τα οποία θα βοηθήσουν στην εξάλειψη των λαθών μέτρησης ή/και της υποκειμενικής ερμηνείας τους.

Η έρευνά τους παρουσιάζει τη μεθοδολογία CVSS με σκοπό την ταξινόμηση των ευπαθειών και των μέτρων ασφάλειας που έχουν εγκατασταθεί, με ένα συνεπή τρόπο. Ενώ αυτή η εργασία σίγουρα χρειάζεται να υπάρχει σε μία σύγχρονη επιχείρηση ή οργανισμό, δεν μας παρέχει τα απαραίτητα εργαλεία μέτρησης του επιπέδου ασφάλειας ενός συστήματος πληροφορικής με ένα αμερόληπτο τρόπο που να λαμβάνει υπόψη του και τον παράγοντα του χρόνου.

4.10.5 Ενιαίος τρόπος απεικόνισης των αναφορών για ευπάθειες στα συστήματα πληροφορικής

Ενώ κάποιοι ερευνητές προσπαθούν να δημιουργήσουν νέους δείκτες ή νέα πλαίσια για την εκτίμηση αλλά και την ποσοτικοποίηση του επιπέδου ασφάλειας ενός συστήματος πληροφορικής, ο Schiffman στο [76] είχε μία διαφορετική ιδέα. Υποστηρίζει ότι δεν υπάρχει ένας κοινός τρόπος για την παραγωγή αναφορών ευπάθειας στα συστήματα πληροφορικής. Για το λόγο αυτό, κάθε μεγάλη εταιρεία όπως η Cisco, η Microsoft, η CERT ή η Secunia, χρησιμοποιεί ένα μοναδικό δικό της τρόπο απεικόνισης αναφορών ευπάθειας, ο οποίος δεν συμβαδίζει με την αντίστοιχη αναφορά ευπαθειών κάποιας άλλης εταιρείας. Αυτό έχει ως αποτέλε-

σμα, ο τελικός χρήστης –μία εταιρεία για παράδειγμα-, να πρέπει χειροκίνητα να συνθέσει την πληροφορία που χρειάζεται από τις επιμέρους αναφορές ευπαθειών, για να καταλήξει στην εκτίμηση του επιπέδου ασφάλειας των συστημάτων πληροφορικής που διαθέτει.

Όπως υποστηρίζουν, αυτό, όχι μόνο είναι χρονοβόρο αλλά συγχρόνως εμπεριέχει τον κίνδυνο κάποιο εύρημα κατά τη διαδικασία της εκτίμησης του επιπέδου της ασφάλειας ενός συστήματος πληροφορικής α) να ερμηνευτεί με λάθος τρόπο ή/και β) να παραληφθεί εντελώς. Με την υιοθέτηση ενός κοινά αποδεκτού τρόπου για την παραγωγή αναφορών ευπάθειας (vulnerability reports), οποιοσδήποτε θα μπορούσε να επεξεργαστεί αυτές τις αναφορές με ηλεκτρονικό τρόπο, γρήγορα και εύκολα και να ανακαλύψει το συνολικό επίπεδο ασφάλειας των συστημάτων πληροφορικής που διαθέτει η επιχείρηση ή ο οργανισμός.

Η προτεινόμενη λύση, που ονομάζεται «Κοινό πλαίσιο αναφορών ευπάθειας» (Common Vulnerability Reporting Framework - CVRF), είναι ένα αρχείο τύπου XML το οποίο έχει ένα αρκετά μεγάλο αριθμό πεδίων στη δομή του. Επειδή η χρήση της τεχνολογίας των αρχείων αυτών είναι αρκετά διαδεδομένη, θα ήταν πολύ εύκολο για κάθε μεγάλη εταιρεία να παράγει το ίδιο αρχείο, αφού τα πεδία που περιέχει το αρχείο θα ήταν κοινά τόσο στην ονοματολογία τους όσο και στον τύπο τους. Αυτό είναι ένα επιθυμητό χαρακτηριστικό για το πλήθος των αναφορών ευπάθειας στα διάφορα συστήματα προστασίας μιας επιχείρησης και θα ωφελούσε τα τμήματα πληροφορικής, βοηθώντας τα να έχουν μία γρηγορότερη απόκριση σε οποιοδήποτε περιστατικό ασφάλειας.

Παρόλα αυτά, η συλλογή όλων των ιχνών και των δεδομένων ασφάλειας με ένα κοινά αποδεκτό τρόπο που θα βοηθούσε στην εύκολη επεξεργασία τους, δεν είναι ακριβώς ένας τρόπος μέτρησης του επιπέδου της ασφάλειας ενός συστήματος πληροφορικής. Είναι περισσότερο ένας οδηγός για τα τμήματα πληροφορικής και αποσκοπεί στην άμεση ανταπόκρισή τους σε περίπτωση περιστατικού ασφάλειας στα συστήματα μιας επιχείρησης. Ο τρόπος που όλα τα συλλεγόμενα δεδομένα θα εκτιμηθούν από τον υπεύθυνο ασφαλείας είναι κάτι που η έρευνα αυτή δεν προσεγγίζει.

4.10.6 Διαχείριση κρίσιμων πληροφοριακών υποδομών με τη χρήση μεθόδων ποσοτικοποίηση της ασφάλειας

Στη διδακτορική του μελέτη ο Σερέλης στο [77], προσέγγισε το θέμα της μέτρησης της ασφάλειας των συστημάτων πληροφορικής με ένα άλλο τρόπο. Προτείνει ότι η μέτρηση της ασφάλειας μίας υπηρεσίας ή ενός συστήματος πληροφορικής μπορεί να αποτυπωθεί με μαθηματικό τρόπο και να εκφραστεί ως συνάρτηση των παραγόντων οι οποίες είναι μεταβλητές της συνάρτησης. Ο μαθηματικός τύπος που προτείνει είναι ο ακόλουθος:

$$Sec_s = \frac{C}{C_T} x \frac{A}{A_T} x \frac{R-L}{R_T} x \frac{S}{S_T} \quad (\mathbf{1})$$

Όπου:	
SEC_s	Το επίπεδο ασφάλειας μίας συγκεκριμένης υπηρεσίας ή συστήματος πληροφορικής s
C	Το τρέχον επίπεδο συμμόρφωσης το οποίο παίρνει τιμές 1 ή 0.
C_T	Το Επίπεδο – Στόχος της συμμόρφωσης το οποίο παίρνει τιμές 1 ή 0.
A	Το τρέχον επίπεδο διαθεσιμότητας το οποίο παίρνει τιμές από 0 έως 1.
A_T	Το Επίπεδο – Στόχος της διαθεσιμότητας το οποίο παίρνει τιμές 1 ή 0.
R	Η τρέχουσα απόδοση της υπηρεσίας (σε νόμισμα).
R_T	Το Επίπεδο – Στόχος της απόδοσης της υπηρεσίας (σε νόμισμα).
L	Το τρέχον παθητικό της υπηρεσίας σε (νόμισμα).
S	Η τρέχουσα τιμή της μετοχής της εταιρείας (σε νόμισμα).
S_T	Το Επίπεδο – Στόχος της τιμής της μετοχής της εταιρείας (σε νόμισμα).

Έχοντας εκφράσει το επίπεδο της ασφάλειας με τον παραπάνω μαθηματικό τύπο, επιδιώκει να ισορροπήσει τις επενδύσεις στην ασφάλεια κάθε υπηρεσίας ή συστήματος πληροφορικής, ώστε να μεγιστοποιηθούν τα κέρδη του οργανισμού, τα οποία εκφράζονται ως Return On Investment – ROI της συγκεκριμένης υπηρεσίας, ως εξής:

$$\max ROI(Sec_1, Sec_2, \dots, Sec_n)$$

Υπό τον όρο ότι:

$$\sum_{i=1}^{n} (R_i - I_i - L_i) > 0$$

4.10.7 OpenVAS, MS BSA και Nessus Vulnerability Scanners

Μία ενδιαφέρουσα προσέγγιση για την αξιολόγηση του επιπέδου ασφάλειας ενός συστήματος πληροφορικής είναι η ανίχνευση των ευπαθειών που έχει. Υπάρχουν διάφορα προϊόντα λογισμικού που κάνουν ανίχνευση ευπαθειών (vulnerability scanners) αλλά τα περισσότερο γνωστά είναι το OpenVAS (Open Vulnerability Assessment System) [78], το MSBSA (Microsoft Baseline Security Analyzer) [79] και το Nessus [80]. Τα εργαλεία αυτά ανιχνεύουν ένα σύστημα πληροφορικής μεταξύ άλλων για ευπάθειες:

- που θα επέτρεπαν σε έναν hacker να αποκτήσει απομακρυσμένη πρόσβαση σε αυτό,
- για τυχόν διορθωτικά πακέτα λογισμικού (patches) που λείπουν,
- για αστοχίες στην παραμετροποίηση του συστήματος,
- για ύπαρξη κωδικών ασφαλείας (passwords) που δεν τηρούν συγκεκριμένη πολυπλοκότητα,
- για τη μη ύπαρξη ή κενών κωδικών ασφαλείας (blank passwords),
- για τυχόν επιθέσεις με σκοπό την άρνηση υπηρεσιών (denial of service), κτλ.

Τα προϊόντα αυτά λογισμικού αποτελούν εργαλεία στα χέρια των διαχειριστών ασφαλείας ενός συστήματος πληροφορικής. Από τα στοιχεία που συλλέγουν, είτε με απευθείας ανίχνευση του συστήματος είτε μέσω της συμπλήρωσης ερωτηματολογίων, είναι σε θέση να δώσουν στοιχεία αναφορικά με την κατάσταση του συστήματος πληροφορικής που μελέτησαν σε διάφορες μορφές όπως XML, HTML και LaTex. Ωστόσο, η χρησιμοποίησή τους σε μεγάλες επιχειρήσεις ή / και οργα-

νισμούς θέτει κάποια θέματα αποδοτικότητας, αφού η λειτουργία τέτοιων εργαλείων θα θέσει σε σοβαρή δοκιμασία την απόδοση τόσο των σταθμών εργασίας όσο και του δικτύου της επιχείρησης.

4.11 Κανονιστικό, νομικό και ρυθμιστικό πλαίσιο

Υπάρχουν διάφοροι νόμοι, οδηγίες και κανονισμοί οι οποίοι εμπεριέχουν απαιτήσεις για την μέτρηση της απόδοσης των μέτρων προστασίας των πληροφοριών. Μερικές επιχειρήσεις όμως επιλέγουν, πέρα από τις υποχρεώσεις τους αυτές, να σχεδιάσουν και να εφαρμόσουν δικές τους τεχνικές και κανόνες για τα θέματα ασφάλειας των συστημάτων πληροφορικής που διαθέτουν. Η υιοθέτηση τέτοιων κανόνων βελτιώνει ιδιαίτερα την ποιότητα μέτρησης των μέτρων ασφάλειας ενός οργανισμού και επιτρέπει σε αυτόν, να διαχειρίζεται καλύτερα αλλά ταυτοχρόνως και να βελτιώνει το επίπεδο ασφάλειας των συστημάτων πληροφορικής στα οποία εφαρμόζονται οι κανόνες αυτοί.

Στην αγορά είναι διαθέσιμα διάφορα εργαλεία και μεθοδολογίες που πιστοποιούν την συμμόρφωση των συστημάτων πληροφορικής σε αντίστοιχες νομοθεσίες και νόρμες. Τα εργαλεία και οι μεθοδολογίες αυτές παρέχουν μετρήσιμους δείκτες συμμόρφωσης στο κανονιστικό πλαίσιο που πιστοποιούν. Έτσι για παράδειγμα, υπάρχει μια μεγάλη γκάμα εργαλείων αφιερωμένα στην πιστοποίηση της συμμόρφωσης μίας επιχείρησης όπως το πλαίσιο αρχών κατά Sarbanes-Oxley, το πλαίσιο αρχών κατά FISMA (Federal Information Security Management Act) και το πλαίσιο αρχών κατά HIPPA (Health Insurance Portability and Accountability Act).

4.11.1 Πλαίσιο αρχών κατά FISMA

Το FISMA είναι ένα εκτεταμένο πλαίσιο αρχών που στοχεύει στην εξασφάλιση των ομοσπονδιακών κυβερνητικών συστημάτων πληροφορικής των ΗΠΑ. Για την επίτευξη του στόχου αυτού, καθορίζει μία σειρά από ρόλους και αρμοδιότητες μεταξύ των ομοσπονδιακών κυβερνητικών υπηρεσιών, απαιτώντας από αυτές να

ενσωματώσουν την ασφάλεια των πληροφοριών, τόσο στους οικονομικούς σχεδιασμούς τους όσο και στις αρχιτεκτονική των διαδικασιών των συστημάτων τους. Επιπλέον, απαιτεί από τις εμπλεκόμενες υπηρεσίες να προβαίνουν σε ετήσια αξιολόγηση του επιπέδου ασφάλειας όλων των συστημάτων πληροφορικής που διαθέτουν και να αποστέλλουν τις εκθέσεις τους στο Κογκρέσο [81].

Το Κογκρέσο εκδίδει ένα ετήσιο οδηγό αναφορικά με το πλαίσιο αρχών FISMA, ο οποίος περιέχει συγκεκριμένους και μετρήσιμους δείκτες απόδοσης, οι οποίοι πρέπει να εμπεριέχονται σε όλες τις τριμηνιαίες και ετήσιες αναφορές των εμπλεκομένων υπηρεσιών. Ειδικότερα το 2008, το κογκρέσο ζήτησε από τις κυβερνητικές υπηρεσίες να περιλάβουν στις αναφορές τους τρείς δείκτες απόδοσης που χρησιμοποιούν για να μετρήσουν την απόδοση και την αποτελεσματικότητα των μέτρων ασφάλειας που έχουν υιοθετήσει. Οι δείκτες αυτοί θα έπρεπε να ήταν διαφορετικοί από αυτούς που ήδη χρησιμοποιούσαν στο πλαίσιο αρχών FISMA και τους πρότεινε να απευθυνθούν στην ειδική δημοσίευση για τα θέματα αυτά από τη NIST [29].

Είναι φανερό λοιπόν, πόσο μεγάλη σημασία στη μέτρηση του επιπέδου της ασφάλειας των συστημάτων πληροφορικής δίνουν οι ΗΠΑ, αφού έχουν οργανώσει μία σειρά από κυβερνητικές υπηρεσίες, τόσο για τη διαμόρφωση προτύπων, όσο και για την παρακολούθηση της εφαρμογής αυτών.

4.11.2 Πλαίσιο αρχών κατά GPRA και Αναφορές Ασφαλείας

Το πλαίσιο αρχών κατά GPRA (Government Performance Result Act) είναι άλλο ένα παράδειγμα έμμεσης, αυτή τη φορά, υποχρέωσης μέτρησης της ασφάλειας των συστημάτων πληροφορικής ενός οργανισμού. Το GPRA δεν υποχρεώνει άμεσα κάποιον οργανισμό να εφαρμόσει κάποιο σχέδιο προστασίας, μέτρησης ή δημιουργίας αναφορών της ασφάλειας των συστημάτων πληροφορικής αλλά αναφέρει ότι είναι θεμιτό όλες οι κυβερνητικές υπηρεσίες των ΗΠΑ, να συνδέσουν τις στρατηγικές ασφάλειας που εφαρμόζουν, με τους στρατηγικούς στόχους και δείκτες απόδοσης που έχουν υιοθετήσει.

Με άλλα λόγια, αφού οι στρατηγικοί στόχοι των υπηρεσιών είναι σαφώς μετρήσιμοι, το ίδιο πρέπει να είναι και οι στόχοι για την ασφάλεια των συστημάτων πληροφορικής. Η NIST στο [29] προτείνει ακριβώς το ίδιο, δηλαδή ότι οι υπηρεσίες πρέπει να συνδέσουν, ή καλύτερα να ευθυγραμμίσουν, τους στόχους τους για την ασφάλεια των συστημάτων πληροφορικής και των πληροφοριών με τη συνολική στρατηγική που διέπει όλες τις υπηρεσίες και στη συνέχεια να προβούν στη μέτρηση της απόδοσης των μέτρων ασφάλειας που έχουν θεσμοθετήσει. Επιπλέον θα πρέπει να κρατούν μητρώο στο οποίο να φαίνεται πόσο επιτυχημένα ή όχι ήταν τα μέτρα που επιλέχθηκαν.

4.12 Μεθοδολογίες ανάλυσης και διαχείρισης της επικινδυνότητας

Κλείνοντας την αναφορά στις προσπάθειες ποσοτικοποίησης της ασφάλειας των συστημάτων πληροφορικής, πρέπει να αναφερθούν μερικές από τις ολοκληρωμένες μεθοδολογίες ανάλυσης και διαχείρισης επικινδυνότητας που υπάρχουν. Οι μεθοδολογίες αυτές εντοπίζουν τις απειλές και τις ευπάθειες αλλά και βοηθούν στο να μετριαστούν οι πιθανές επιπτώσεις από ένα συμβάν ασφαλείας. Ο τελικός σκοπός αυτών των μεθολογιών είναι να συμβάλλουν στον ακριβή προσδιορισμό, αξιολόγηση και αντιμετώπιση των κινδύνων που αντιμετωπίζουν τα συστήματα πληροφορικής.

4.12.1 CRAMM

Η CRAMM (CCTA Risk Assessment and Management Methodology) [82] αναπτύχθηκε για να υποστηρίξει μεγάλους οργανισμούς και επιχειρήσεις. Είναι συμβατή με το πρότυπο ISO/IEC 17799:2005 [66] και καλύπτει τις φάσεις της ασφάλειας πληροφοριών, δηλαδή, του σχεδιασμού, της ανάπτυξης – υλοποίησης και, τέλος, της αναβάθμισης. Η CRAMM προτείνει τη χρησιμοποίηση τριών φάσεων για την ανάλυση της επικινδυνότητας , α) του προσδιορισμού και αποτίμησης αγαθών (asset identification), β) της ανάλυσης επικινδυνότητας (risk assessment) και, τέλος, γ) της διαχείρισης του κινδύνου (risk management). Η μεθοδολογία αυτή

βασίζεται και στηρίζει τα αποτελέσματά της στην ποιοτική προσέγγιση αφού η εκτίμηση των κινδύνων και των κατάλληλων μέτρων προστασίας γίνετα από το προσωπικό του οργανισμού που μπορεί να παρέχει τέτοιου είδους πληροφόρηση.

4.12.2 OCTAVE

Μία παρόμοια μεθοδολογία για την ανάλυση και διαχείριση της επικινδυνότητας των συστημάτων πληροφορικής είναι η OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [83]. Ο μέθοδος αυτή προτείνει τη χρήση ομάδων εργασίας στις φάσεις που χρησιμοποιεί. Οι φάσεις αυτές είναι: α) της δημιουργίας προφίλ απειλών σε συνάρτηση με τα αγαθά του οργανισμού, β) του εντοπισμού των ευπαθειών και, τέλος, γ) της ανάπτυξης στρατηγικής και σχεδίων προστασίας. Η OCTAVE βασίζεται στη λήψη των πληροφοριών από ερωτηματολόγια και συνεπώς ακολουθεί την ποιοτική προσέγγιση στον προδιορισμό του επιπέδου της ασφάλειας.

4.12.3 MAGERIT

Η MAGERIT [84], [85], [86] είναι μία μεθοδολογία η οποία αναπτύχθηκε από το Ισπανικό Ανώτατο Συμβούλιο για την Ηλεκτρονική Διακυβέρνηση και είναι συμβατή με τα πρότυπα ISO/IEC 27001:2005 [67] και ISO/IEC 27005:2008 [11]. Η μεθοδολογία αυτή, προτείνει μία σειρά από φάσεις για: α) τον προσδιορισμό των περιουσιακών στοιχείων, β) τον εντοπισμό απειλών και ευπαθειών, γ) τον προσδιορισμό των επιπτώσεων και, τέλος, δ) τον προσδιορισμό και μετριασμό των κινδύνων. Ωστόσο, η διαφορά της με τις προηγούμενες μεθοδολογίες είναι ότι ο προσδιορισμός του κινδύνου γίνεται βάση του αντίκτυπου που έχει μία απειλή πάνω σε ένα αγαθό καθώς και τη μέτρηση της συχνότητας εμφάνισης τέτοιων απειλών. Η MAGERIT μπορεί να χρησιμοποιηθεί μόνο από χρήστες με υψηλή τεχνογνωσία σε συστήματα πληροφορικής, οι οποίοι θα αναλάβουν και την ευθύνη για την ανάλυση του κινδύνου στα συστήματα του οργανισμού μέσω της διαδι-

κασίας συνεντεύξεων και συμπλήρωσης ερωτηματολογίων από εκπροσώπους του οργανισμού.

4.12.4 EBIOS

Η EBIOS (Expression des Besoins et Identification des Objectifs de Securite) [87] έχει αναπτυχθεί από τη Γαλλική Γενική Γραμματεία Εθνικής Άμυνας με σκοπό την αξιολόγηση και την αντιμετώπιση των κινδύνων συστημάτων πληροφορικής. Προτείνει τη χρήση πέντε φάσεων στη διαδικασία της αξιολόγησης: α) του προσδιορισμού των αλληλοεξαρτήσεων των αγαθών, β) και γ) του προσδιορισμού και της αξιολόγησης των απειλών του υπό εξέταση συστήματος πληροφορικής, δ) της αξιολόγησης της επικινδυνότητας και, τέλος, ε) του προσδιορισμού και επιλογής των μέτρων προστασίας για το σύστημα πληροφορικής που εξετάζεται. Η EBIOS στηρίζεται στην ποιοτική προσέγγιση ωστόσο η έλλειψη τρόπου υπολογισμού για τον προσδιορισμό του επιπέδου ασφάλειας ενός συστήματος πληροφορικής αποτελεί βασικό μειονέκτημα για την υιοθέτηση αυτής της μεθοδολογίας.

4.12.5 MEHARI

Άλλη μία μεθοδολογία που υιοθετεί την ποιοτική προσέγγιση στη διαδικασία ανάλυσης και διαχείρισης της επικινδυνότητας είναι η MEHARI [88], η οποία καλύπτει πλήρως τις απαιτήσεις του προτύπου ISO/IEC 27001:2005 [67]. Η μεθοδολογία απευθύνεται σε όσους εμπλέκονται στη διαχείριση της ασφάλειας ενός οργανισμού (διαχειριστές, ελεγκτές, ομάδα ασφάλειας) καθώς και σε χρήστες με διοικητικές και τεχνικές αρμοδιότητες. Οι εταιρικοί χρήστες εμπλέκονται μόνο στις φάσεις της μεθοδολογίας που έχουν να κάνουν με τον προσδιορισμό των αγαθών και των ευπαθειών τους. Η MEHARI είναι κατάλληλη για επιχειρήσεις ή / και οργανισμούς μεσαίας και μεγάλης κλίμακας.

4.13 Γενικά συμπεράσματα από τις διάφορες έρευνες

Είναι εμφανές ότι ο τομέας της ποσοτικοποίησης της ασφάλειας ενός συστήματος πληροφορικής προβληματίζει ιδιαίτερα τους ερευνητές ανά τον κόσμο τα τελευταία χρόνια. Απόδειξη για αυτό, είναι το πλήθος των δημοσιεύσεων και οι προσπάθειες που έχουν γίνει στον τομέα αυτόν. Όλοι οι ερευνητές ανά τον κόσμο συμφωνούν ότι δεν έχει ακόμα βρεθεί, ένας κοινά αντικειμενικός τρόπος για τη μέτρηση του επιπέδου της ασφάλειας στον τομέα της πληροφορικής. Σε αντίθεση, σε άλλους τομείς, όπως ο χρηματοοικονομικός ή ο ασφαλιστικός, έχει σημειωθεί ιδιαίτερα μεγάλη πρόοδος, και ήδη υπάρχουν κάποια πρότυπα.

Η ύπαρξη μέτρων παίζει ένα σημαντικό ρόλο στην κοινότητα των ερευνητών και ο καθένας προσπαθεί να προτείνει κάποιο μέτρο το οποίο, πρώτον θα παράγει το επιθυμητό αποτέλεσμα και δεύτερον θα είναι παγκοσμίως αποδεκτό. Παρόλα αυτά, λόγω της πολυπλοκότητας της βιομηχανίας της πληροφορικής, τις συνεχείς τεχνολογικές εξελίξεις, του τρόπου που καθημερινά λειτουργούμε και της συνεχούς πίεσης για συμμόρφωση σε πρότυπα από κυβερνήσεις, ινστιτούτα και εταιρείες, δεν έχει υιοθετηθεί μία ακριβής και αμερόληπτη μέθοδος για τη μέτρηση του επιπέδου της ασφάλειας ενός συστήματος πληροφορικής, αλλά επειγόντως αναζητείται.

Οι διάφορες προσεγγίσεις που υπάρχουν, όπως αναφέρθηκε, μπορούν να κατηγοριοποιηθούν ανάλογα με το περιεχόμενό τους. Έτσι, έχουμε διάφορες μεθοδολογίες και βέλτιστες πρακτικές, που περισσότερο έχουν ως σκοπό, την αύξηση ή / και τη βελτίωση του επιπέδου ασφάλειας των συστημάτων πληροφορικής σε έναν οργανισμό, καθώς και την ενσωμάτωση ασφαλιστικών δικλείδων για τη διατήρηση αποτελεσματικών ελέγχων που θα σηματοδοτούσαν μία πιθανή παραβίαση ασφάλειας, παρά την ποσοτικοποίηση του επιπέδου ασφάλειας με τη παραγωγή ενός καθαρού αριθμητικού μέτρου.

Μια άλλη προσέγγιση, είναι η παραγωγή εργαλείων που συλλέγουν δεδομένα, με σκοπό την ανάλυσή τους (risk assessment), με διάφορους τρόπους και από διαφορετικές ομάδες ατόμων μέσα στην εταιρεία, για παράδειγμα από τους Εσωτερικούς Επιθεωρητές, που αποσκοπούν στη βελτίωση των διαδικασιών αντιμετώ-

πισης κινδύνων και κατ' επέκταση, κινδύνων από τα συστήματα πληροφορικής. Η προσέγγιση αυτή, έχει προτείνει διάφορα μέτρα ποσοτικοποίησης της ασφάλειας, αλλά κανένα από αυτά δεν έχει κοινά γίνει αποδεκτό από την επιστημονική κοινότητα.

Μία άλλη προσέγγιση, είναι διάφορες κυβερνητικές προσπάθειες που είναι εστιασμένες σε συγκεκριμένες περιοχές της ηλεκτρονικής διακυβέρνησης. Η NIST έχει, ίσως, την πιο ολοκληρωμένη προσπάθεια στον τομέα της αντιμετώπισης των κινδύνων των συστημάτων πληροφορικής και αρκετές έρευνές της χρησιμοποιούνται από κυβερνητικές υπηρεσίες των Ηνωμένων Πολιτειών ως εσωτερικοί κανονισμοί ή ως οδηγίες για την ασφάλεια των συστημάτων τους. Ανάμεσα στις οδηγίες αυτές υπάρχουν και δείκτες αξιολόγησης της απόδοσης των εφαρμοζόμενων διαδικασιών, που κατά κάποιο τρόπο, παράγουν ένα δείκτη ποσοτικοποίησης της ασφάλειας. Παρόλα αυτά, η προσέγγιση αυτή, ίσως και λόγω της δυσκολίας εφαρμογής της δεν έχει την καθολική αποδοχή τόσο από την επιστημονική όσο και από την επιχειρηματική κοινότητα, ως το μέσο για την ποσοτικοποίηση της ασφάλειας.

Άλλες προσεγγίσεις περιλαμβάνουν προσπάθειες από εταιρείες της αγοράς, διάφορες ταξινομήσεις ευπαθειών και συστήματα αξιολόγησης. Όλα τα παραπάνω, αποσκοπούν στη μέτρηση του επιπέδου της ασφάλειας μέσω της ποσοτικοποίησης των ευπαθειών αλλά και της πρόβλεψής τους. Έτσι, υπάρχουν εργαλεία για την εύρεση ευπαθειών σε δίκτυα ή ακόμα και σε πηγαίο κώδικα που μας παρέχουν μία εκτίμηση της συνολικής εικόνας της ασφάλειας ενός συστήματος πληροφορικής. Οι διάφορες προσπάθειες ταξινόμησης των ευπαθειών αλλά και αξιολόγησής τους αποσκοπούν στη μέτρηση της επίπτωσης μίας ευπάθειας στον οργανισμό και την ενεργοποίηση εκείνου του μηχανισμού από τα μέτρα αντιμετώπισης του συνολικού κινδύνου μίας επιχείρησης (Enterprise Risk Management), έτσι ώστε να μειωθούν οι πιθανές ζημίες.

Σημαντικές προσπάθεις έχουν γίνει στον τομέα δημιουργίας προτύπων καθώς και κανονιστικού, νομικού και ρυθμιστικού πλαισίου λειτουργίας εταιρειών και οργανισμών. Υπάρχουν εταιρείες που είναι υποχρεωμένες από το νόμο να εφαρμόσουν κάποιο πρότυπο, πέρα από το νομικό και ρυθμιστικό πλαίσιο λειτουργίας

τους. Έτσι, για παράδειγμα, υπάρχει μια μεγάλη γκάμα εργαλείων αφιερωμένα στην πιστοποίηση της συμμόρφωσης μίας επιχείρησης όπως το πλαίσιο αρχών κατά Sarbanes-Oxley, το πλαίσιο αρχών κατά FISMA και πλαίσιο αρχών κατά HIPPA (Health Insurance Portability and Accountability Act. Όλα τα προαναφερθέντα, αποσκοπούν στην αύξηση και τη διατήρηση ενός υψηλού επιπέδου ασφάλειας σε ένα οργανισμό αλλά δεν παρέχουν εκείνο το μέτρο το οποίο θα μπορούσε να χρησιμοποιηθεί για να αποτυπώσει το επίπεδο ασφάλειας ενός συστήματος πληροφορικής.

Τέλος, προσπάθειες για την ποσοτικοποίηση του επιπέδου της ασφάλειας ενός συστήματος πληροφορικής, έχουν γίνει με τη χρήση μεθοδολογιών ανάλυσης και διαχείρισης της επικινδυνότητας. Οι μεθοδολογίες αυτές επικεντρώνονται στον προσδιορισμό των περουσιακών στοιχείων, τον εντοπισμό απειλών και ευπαθειών, τον προσδιορισμό των επιπτώσεων και, τέλος, τον προσδιορισμό και μετριασμό των κινδύνων. Οι περισσότερες στηρίζουν τα αποτελέσματά τους στη λήψη πληροφοριών με τη χρήση ποιοτικών μεθόδων, συνήθως με τη συμπλήρωση ερωτηματολογίων από τα εμπλεκόμενα στη διαδικασία μέρη, γεγονός που υποδεικνύει το μεγάλο βαθμό υποκειμενικότητάς τους. Επιπλέον, μερικές από αυτές δεν προτείνουν καθόλου κάποιο τρόπο υπολογισμού του επιπέδου της ασφάλειας. Παρόλα αυτά, οι μεθοδολογίες αυτές χρησιμοποιούνται για την πιστοποίηση σε κάποιο πρότυπο, αφού υλοποιούν σχεδόν όλες τις προϋποθέσεις που τα γνωστά πρότυπα ασφάλειας θέτουν.

Η παρούσα έρευνα, προτείνει μία νέα μεθοδολογία, που είναι βασισμένη στην μελέτη των ευπαθειών (vulnerability-driven) που ένα σύστημα πληροφορικής μπορεί να έχει. Τα στοιχεία για τη μελέτη αυτή, προέρχονται από δύο πολύ γνωστές βάσεις δεδομένων που περιέχουν στοιχεία ευπαθειών, και, περιγράφονται αναλυτικά στις παραγράφους § 5.6 και § 5.7.1 αντίστοιχα. Ο συνδυασμός της ποσοτικής προσέγγισης στη μελέτη των ευπαθειών, με τη χρήση μη αμφισβητούμενων στοιχείων για τις ευπάθειες των προϊόντων λογισμικού, βοηθούν την προτεινόμενη μεθοδολογία και πετυχαίνει υψηλό βαθμό αντικειμενικότητας. Πρέπει να σημειωθεί ότι στην προτεινόμενη μεθοδολογία γίνεται η μελέτη του επιπέδου της ασφάλειας που έχει ένα σύστημα πληροφορικής, χωρίς να ληφθούν υπόψη τα

διάφορα μέτρα προστασίας που μπορεί να έχει λάβει η επιχείρηση όπως: vulnerability scanners, firewall, προϊόντα λογισμικού για την προστασία από ιούς κτλ.

Προς την κατεύθυνση αυτή, για την ποσοτικοποίηση της ασφάλειας ενός προϊόντος, μίας υπηρεσίας ή ενός συστήματος πληροφορικής, προτείνουμε τη χρήση στοχαστικών μεθόδων. Οι μέθοδοι αυτές μπορούν να μελετήσουν το επίπεδο ασφάλειας ενός συστήματος πληροφορικής στην εξέλιξή του σε βάθος χρόνου, αφού μπορούν να ενσωματώσουν τον παράγοντα του «χρόνου». Ο τελικός σκοπός είναι να παραχθεί ένα αμερόληπτο και καθαρό αριθμητικό αποτέλεσμα, το οποίο θα υποδηλώνει το ζητούμενο επίπεδο ασφάλειας.

ΚΕΦΑΛΑΙΟ 5: Παρουσίαση μεθοδολογίας ποσοτικοποίησης της ασφάλειας

5. Εισαγωγή

Για να μπορέσουμε να διατηρήσουμε τον «γεμάτο από πληροφορική» τρόπο ζωής μας, οφείλουμε να διαφυλάξουμε και να εξασφαλίσουμε τη διαθεσιμότητα των συστημάτων πληροφορικής που χρησιμοποιούμε. Ο ολοένα και μεγαλύτερος αριθμός επιχειρήσεων, που κυριολεκτικά στηρίζονται στην αδιάλειπτη λειτουργία (24x7) και διαθεσιμότητα των συστημάτων πληροφορικής που διαθέτουν, με σκοπό να εξασφαλίσουν την ακεραιότητα αλλά και την επιχειρησιακή συνέχειά τους, υποδεικνύει τον πολύ υψηλό κίνδυνο που αναλαμβάνουμε, λόγω της αυξανόμενης εξάρτησής μας από τα συστήματα πληροφορικής.

Η διατήρηση της υψηλής διαθεσιμότητας των συστημάτων πληροφορικής όμως, απαιτεί δυσβάσταχτα υψηλές επενδύσεις και αυξάνει το κόστος λειτουργίας μιας επιχείρησης. Αυτό με τη σειρά του δημιουργεί ένα άλλο πρόβλημα, αφού η εποχή που ζούμε, απαιτεί από τις επιχειρήσεις δραστικές μειώσεις κόστους, αν θέλουν να είναι ανταγωνιστικές και να έχουν ικανοποιητικό αριθμό πελατών. Οι διοικήσεις των επιχειρήσεων προσπαθούν να μειώσουν τα λειτουργικά κόστη που έχουν και ταυτόχρονα, να διατηρήσουν ένα υψηλό βαθμό απόδοσης, στην αντιμετώπιση των προβλημάτων των συστημάτων πληροφορικής σχετικά με την ασφάλεια των πληροφοριών. Η εξισορρόπηση αυτών των δυο εκ διαμέτρου αντίθετων δυνάμεων, είναι μία σοβαρή και πολύπλοκη διαδικασία και ως ένα βαθμό κρίνει την επιτυχία της επιχείρησης στο κλάδο που δραστηριοποιείται.

Υψηλές επενδύσεις στον τομέα της ασφάλειας θα σημαίνουν για την επιχείρηση μεγάλο κόστος και μειωμένη κερδοφορία. Από την άλλη πλευρά, χαμηλές επενδύσεις στον τομέα της ασφάλειας μπορεί να μειώσουν το κόστος της επιχείρησης αλλά με την ταυτόχρονη ανάληψη υψηλών κινδύνων που θα μπορούσαν, εάν συμβούν, να καταστρέψουν όχι μόνο την φήμη της επιχείρησης αλλά και τη βιωσιμότητα της επιχείρησης. Οι εταιρείες προσεγγίζουν αυτό το ευαίσθητο σημείο εταιρικής διακυβέρνησης, με την πρόσληψη ειδικών σε θέματα ασφάλειας, για να

τους καθοδηγήσουν με τον καλύτερο δυνατό τρόπο. Για το λόγο αυτό, είναι πάρα πολύ σημαντικό για μία επιχείρηση να είναι σε θέση με αντικειμενικό, σαφή και αμερόληπτο τρόπο σε οποιαδήποτε χρονική στιγμή να γνωρίζει πόσο ασφαλή είναι τα κρίσιμα συστήματα πληροφορικής που διαθέτει.

5.1 Παράγοντες κινδύνου

Όπως αναφέρθηκε, οι επιχειρήσεις είναι αναγκασμένες να αναλάβουν κάποιους κινδύνους αναφορικά με τα συστήματα πληροφορικής που διαθέτουν. Όσο μεγαλύτερες είναι οι επενδύσεις της επιχείρησης σε μέτρα ασφάλειας, τόσο πιο μικροί γίνονται οι κίνδυνοι αλλά και λιγότερα αποδοτικά τα συστήματα πληροφορικής, γιατί τα μέτρα ασφάλειας σίγουρα θα έχουν κάποια επίδραση στην απόκρισή τους. Σε αντίθεση, όσο μικρότερες είναι οι επενδύσεις σε μέτρα ασφάλειας, τόσο μεγαλύτεροι είναι οι κίνδυνοι που δέχεται να αναλάβει η επιχείρηση και κατά συνέπεια η απόκριση των συστημάτων πληροφορικής που διαθέτει θα είναι καλύτερη.

Υπάρχουν όμως κάποιες περιπτώσεις, που το κόστος μιας επιχείρησης για να διορθώσει ένα κενό ασφαλείας μπορεί να είναι δυσανάλογο με την πιθανότητα αυτός ο κίνδυνος πραγματικά να συμβεί. Ένα παράδειγμα αυτού, θα ήταν μια επιχείρηση να πληρώσει υπέρογκα ποσά για την προστασία της από πλημύρες ενώ τα γραφεία της και ο χώρος με τα συστήματα πληροφορικής, βρίσκονται στον 40^{o} όροφο ενός ουρανοξύστη. Ενώ το παράδειγμα είναι πραγματικά ακραίο, δεν παύει να απεικονίζει μία πραγματικότητα, ότι όλες οι επιχειρήσεις θα αποφασίσουν, για δικούς τους, κυρίως οικονομικούς λόγους, να μην πάρουν μέτρα προστασίας για κάποιους από τους κινδύνους που διατρέχουν.

Η παρούσα έρευνα, επικεντρώνεται αποκλειστικά, στην τεχνική πλευρά του επιπέδου ασφάλειας των συστημάτων πληροφορικής μιας επιχείρησης. Η συνολική ανάλυση των κινδύνων ενός συστήματος πληροφορικής περιλαμβάνει τρείς βασικές διαστάσεις:

- Της επιχειρησιακής λειτουργίας.

- Της φυσικής ασφάλειας.
- Της τεχνικής ασφάλειας.z

Κάθε μία από αυτές τις διαστάσεις περιέχει συγκεκριμένους παράγοντες κινδύνου που μπορούν να επηρεάσουν τη συνολική ασφάλεια ενός συστήματος πληροφορικής. Το μοντέλο εκτίμησης του κινδύνου (risk assessment) που προτείνει αυτή η έρευνα, μπορεί να χρησιμοποιηθεί για την αντικειμενική, αμερόληπτη και ακριβή μέτρηση των τεχνικών παραγόντων που επηρεάζουν το επίπεδο ασφάλειας ενός συστήματος πληροφορικής, δηλαδή της τρίτης διάστασης από αυτές που αναφέρθηκαν.

5.1.1 Ορισμός τεχνικού παράγοντα κινδύνου

Βασική παραδοχή της έρευνας αυτής, είναι η υιοθέτηση του όρου «τεχνικός παράγοντας κινδύνου (technical risk factor)», ο οποίος όπως αναφέρθηκε και στο [89], ορίζεται ως «*κάθε διακριτό στοιχείο που αποτελεί το σύστημα πληροφορικής, του οποίου γίνεται η εκτίμηση των κινδύνων (risk assessment)».* Με αυτό τον τρόπο, κάθε ένα στοιχείο που συμπεριλαμβάνεται σε ένα σύστημα πληροφορικής, π.χ. το λειτουργικό του σύστημα, μία εφαρμογή, ή ένα πακέτο του εμπορίου που βρίσκονται εγκατεστημένα σε αυτό, αποτελούν και ένα διακριτό τεχνικό παράγοντα κινδύνου (technical risk factor), που δυνητικά μπορεί να επηρεάσει το επίπεδο ασφάλειάς του.

5.1.2 Πλεονεκτήματα από τον ορισμό τεχνικού παράγοντα κινδύνου

Η υιοθέτηση αυτού του ορισμού, παρέχει στην προτεινόμενη μεθοδολογία, τα ακόλουθα οφέλη:

- Ο τεράστιος όγκος των ευπαθειών (vulnerabilities) των συστημάτων πληροφορικής που υπάρχουν κατηγοριοποιείται με ένα εύκολο τρόπο, που βοηθά στην εξοικονόμηση χρόνου κατά τη διάρκεια της ανάλυσης. Ο κλάδος

των ταξινομήσεων των ευπαθειών, είτε κατά τύπο (type), είτε κατά σπουδαιότητα (severity), είναι ακόμα σε συζήτηση μεταξύ της κοινότητας των ερευνητών όπως αναφέρεται και στο [90]. Αυτό επιβεβαιώνεται και από το γεγονός ότι ακόμα και η πιο διαδεδομένη και αποδεκτή ταξινόμηση ευπαθειών που αναφέρθηκε στην παράγραφο § 4.9.1, έχει προβλήματα και δεν μπορεί να θεωρηθεί σαφής. Ο παράγοντας αυτός έπαιξε καθοριστικό ρόλο στην έρευνα αυτή, καθώς επιχειρήθηκε η αποφυγή της ανάλυσης των παραγόντων κινδύνου των συστημάτων πληροφορικής, που είναι βασισμένη στην ταξινόμηση των ευπαθειών, και, έγινε προσπάθεια δημιουργίας ενός πιο γενικευμένου μοντέλου εκτίμησης κινδύνων, το οποίο θα προσπερνούσε τα προβλήματα αυτά.

- Η ιεράρχηση των παραγόντων κινδύνου από τη διοίκηση μιας επιχείρησης, εστιάζεται στα συγκεκριμένα στοιχεία του συστήματος πληροφορικής και όχι σε συγκεκριμένες ευπάθειες.
- Η συσχέτιση του κινδύνου με συγκεκριμένο στοιχείο του συστήματος πληροφορικής ταυτόχρονα λαμβάνει υπόψη της και τον παράγοντα του χρόνου. Με αυτόν τον τρόπο, η εκτίμηση του κινδύνου από έναν υπάλληλο μπορεί να γίνει με μεγαλύτερη ακρίβεια, να είναι αντικειμενική, αμερόληπτη και, όπως θα εξηγήσουμε παρακάτω, να είναι σταθμισμένη (risk-weighted).

5.2 Ανάγκη χρήσης στοχαστικών μεθόδων

Στο σύγχρονο κόσμο των επιχειρήσεων, ο όρος «κίνδυνος» (risk), είναι ίσως ο περισσότερο χρησιμοποιούμενος όρος ανάμεσα στα διάφορα επίπεδα διοίκησης

μίας επιχείρησης. Παίζει εξαιρετικά σημαντικό ρόλο στο σχηματισμό των αποφάσεων και του στρατηγικού πλάνου της επιχείρησης. Για να υιοθετηθούν στρατηγικά μέτρα ή αντίμετρα (counter measures) για τη μείωση των κινδύνων, πρέπει πρώτα η επιχείρηση να γνωρίζει πόσος είναι ο εναπομένων κίνδυνος (residual risk), δηλαδή το βαθμό του κινδύνου που αναλαμβάνει.

Ο παράγοντας του χρόνου παίζει καθοριστικό ρόλο στη διαδικασία αυτή και μέχρι τώρα δεν έχει χρησιμοποιηθεί σε προτεινόμενες μεθοδολογίες ποσοτικοποίησης της ασφάλειας. Για το λόγο αυτό, η παρούσα έρευνα προτείνει τη χρησιμοποίηση των στοχαστικών μεθόδων, οι οποίες μπορούν να διαχειριστούν τον παράγοντα «χρόνο» μαζί με άλλα τυχαία φαινόμενα με γνωστές κατανομές. Η προσέγγιση αυτή, δεν είναι τόσο θεωρητική όσο φαίνεται. Αποτελεί μία πρακτική προσέγγιση που χρησιμοποιεί κυριολεκτικά όλες τις γνωστές ευπάθειες των γνωστών οίκων κατασκευής λογισμικού και των προϊόντων τους, όπως η Microsoft, η Oracle κ.α. Η προτεινόμενη μεθοδολογία έχει ως σκοπό να δημιουργήσει ένα αξιόπιστο, αριθμητικό, αμερόληπτο και αντικειμενικό αποτέλεσμα που θα αποτελεί την ποσοτικοποίηση του επιπέδου της ασφάλειας (ή του κινδύνου) ενός συστήματος πληροφορικής, χρησιμοποιώντας μαθηματικά μοντέλα από τον κλάδο των οικονομικών.

5.2.1 Πλεονεκτήματα της χρήσης στοχαστικών μεθόδων

Τόσο η εμφάνιση μίας ευπάθειας όσο και η αντίστοιχη εκμετάλλευσή της είναι ένα φαινόμενο το οποίο, αν και ακολουθεί κάποια πρότυπα, εξακολουθεί να αποτελεί ένα τυχαίο γεγονός ως προς τη μέτρηση του δείκτη ασφάλειας. Αυτό με τη σειρά του, δημιουργεί την ανάγκη χρησιμοποίησης στον τρόπο υπολογισμού των στοχαστικών διαδικασιών. Στο πλαίσιο αυτό, για να εμπλακεί η τυχαιότητα (randomness), χρησιμοποιούμε στοχαστική αντί για κατά Riemann ολοκλήρωση. Έτσι λοιπόν, δημιουργούμε μία κίνηση Brown, προσομοιώνοντας ένα τυχαίο περίπατο (random walk), στο χρονικό διάστημα στο οποίο θέλουμε να μετρήσουμε την ασφάλεια ενός συστήματος πληροφορικής, και χρησιμοποιώντας αυτή την κίνηση υπολογίζουμε το κατά Itô στοχαστικό ολοκλήρωμα. Η τυχαιότητα που το χαρα-

κτηρίζει, σε συνδυασμό με την αντικειμενικότητα των μετρήσεων της προτεινόμενης μεθοδολογίας, δημιουργεί ένα ιδιαίτερα χρήσιμο μέτρο.

Η χρήση των στοχαστικών μεθόδων εκτός του ότι, σύμφωνα με την παρούσα έρευνα, είναι αναγκαία, μας παρέχει και μία σειρά από πλεονεκτήματα τα οποία παρουσιάζονται παρακάτω:

- Η εκτίμηση του κινδύνου ή η ποσοτικοποίηση της ασφάλειας για ένα σύστημα πληροφορικής παρουσιάζεται με ένα εύκολα κατανοητό αριθμητικό αποτέλεσμα, και όχι μέσω επιστημονικών εργασιών ή/και θέσεων που, θα μπορούσαν να εκτιμηθούν και να κατανοηθούν από τα μέλη της επιχείρησης που ανήκουν στη Διεύθυνση Πληροφορικής και όχι από ανώτερα στελέχη της διοίκησης, τα οποία γνωρίζουν ελάχιστα, στην καλύτερη των περιπτώσεων, ή πιθανότερα καθόλου από τεχνικά θέματα.
- Τα ανώτερα στελέχη της διοίκησης, τα οποία έχουν την ευθύνη τόσο του καθορισμού, όσο και της εφαρμογής της επιχειρησιακής στρατηγικής, θα έχουν στη διάθεσή τους χειροπιαστές και συγκεκριμένες μετρήσεις, που θα αποδεικνύουν την έκθεση στο κίνδυνο των συστημάτων πληροφορικής. Έτσι, η στάση της επιχείρησης απέναντι στον κίνδυνο μπορεί να καθοριστεί με μεγαλύτερη ακρίβεια, αποφεύγοντας περιπτώσεις διακοπής της επιχειρησιακής συνέχειας, που θα είχαν σοβαρές επιπτώσεις τόσο στην επιχείρηση και τη φήμη της, όσο και στους μετόχους της.
- Επιπλέον, η χρήση στοχαστικών μεθόδων αυξάνει τις πιθανότητες να πειστεί η διοίκηση της επιχείρησης, για την αναγκαιότητα μιας επένδυσης σε εξειδικευμένα συστήματα παρακολούθησης (monitoring) και διαχείρισης των κινδύνων σχετικά με τα συστήματα πληροφορικής που διαθέτει. Αυτό γίνεται, απλά και μόνο επειδή τα αποτελέσματα των στοχαστικών μεθόδων είναι ένας αριθμός

που μπορεί να κατανοηθεί από όλα τα επίπεδα διοίκησης ανεξαρτήτως των τεχνικών γνώσεων που διαθέτουν.

- Η χρήση ποιοτικών μεθόδων ανάλυσης, σε αντίθεση με τη χρήση ποσοτικών μεθόδων όπως η στοχαστική ανάλυση, οδηγεί περισσότερο στην εύρεση πιθανών ευρημάτων με πολύ χαμηλό δείκτη αντικειμενικότητας, τα οποία μπορούν κυρίως να χρησιμοποιηθούν για να πειστούν τα στελέχη της Διεύθυνσης Πληροφορικής παρά η διοίκηση της επιχείρησης. Επιπλέον, η διοίκηση δεν θα μπορούσε να κατανοήσει πλήρως τέτοιου είδους ευρήματα, γεγονός που θα οδηγούσε σε καθυστερήσεις των εγκρίσεων για τα απαραίτητα κονδύλια που χρειάζονται, τόσο για την υλοποίηση, όσο και για την εφαρμογή τους. Αυτό, θα οδηγούσε με τη σειρά του, στην επιμήκυνση του χρόνου που η επιχείρηση θα ήταν εκτεθειμένη σε κίνδυνο, επειδή δεν είχε χρησιμοποιηθεί η σωστή επιχειρηματολογία, συνήθως ιδιαίτερα εμπλουτισμένη με τεχνικούς όρους, κατά τη διάρκεια παρουσίασης των ευρημάτων στη διοίκηση.
- Η χρήση των στοχαστικών μεθόδων βοηθά τη διοίκηση μιας επιχείρησης στη καλύτερη κατανόηση των εξής παραμέτρων:
    - ✓ Της αξίας των συστημάτων πληροφορικής που διαθέτει.
    - ✓ Του εντοπισμού διαφόρων κινδύνων ασφάλειας σε όλα τα επίπεδα διοίκησης μέσα στην επιχείρηση.
    - ✓ Της μέτρησης της ευαισθησίας που έχουν τα συστήματα πληροφορικής σε συνδυασμό με τον συνολικό επιχειρηματικό κίνδυνο της επιχείρησης.
- Οι υπάρχουσες μέθοδοι εκτίμησης κινδύνων δεν παράγουν ικανοποιητικά αποτελέσματα αναφορικά με το ειδικό βάρος, σύμφωνα με το οποίο κάθε παρά-

γοντας κινδύνου συμμετέχει στο συνολικό κίνδυνο της επιχείρησης. Με τη χρήση των στοχαστικών μεθόδων είναι δυνατή η χαρτογράφηση των κινδύνων ενός συστήματος πληροφορικής ανάλογα με το ειδικό βάρος που διαθέτει. Για παράδειγμα μία εφαρμογή που δεν θεωρείται κρίσιμη και σπανίως χρησιμοποιείται, δεν μπορεί να συμμετέχει στο συνολικό κίνδυνο με την ίδια βαρύτητα όπως μια άλλη εφαρμογή που χρησιμοποιείται καθημερινά.

5.3 Μέτρηση της ασφάλειας ενός συστήματος πληροφορικής με τη χρήση στοχαστικών διαδικασιών

Είναι γενικά αποδεκτό πως δεν μπορούμε να βρίσκουμε μία καινούργια ευπάθεια σε ένα λειτουργικό σύστημα κάθε μέρα. Επίσης, κάθε ευπάθεια δεν μπορεί να έχει την ίδια σπουδαιότητα ή/και επίδραση στα συστήματα πληροφορικής, και η διόρθωση της ευπάθειας αυτής, μπορεί να χρειαστεί περισσότερο χρόνο από ότι αναμένουμε. Συνεπώς, δεν μπορούμε ακριβώς να προβλέψουμε πότε θα έχουμε κάποιο πρόβλημα στην ασφάλεια των πληροφοριακών μας υποδομών και για αυτό, θα έπρεπε να θεωρούμε την ασφάλεια περισσότερο ως δυναμική και λιγότερο ως στατική.

Φυσικά τις περισσότερες φορές είμαστε σε θέση να καθορίσουμε τους παράγοντες που επηρεάζουν την ασφάλεια ενός συστήματος πληροφορικής, μίας υπηρεσίας ή ακόμα ενός οργανισμού. Παρόλα αυτά όμως, χρειάζεται να είμαστε σε θέση να παρακολουθήσουμε, και πολύ περισσότερο να ποσοτικοποιήσουμε, αυτούς τους παράγοντες σε σχέση με το χρόνο.

Μία προσπάθεια για τη μέτρηση της ασφάλειας μίας υπηρεσίας έχει γίνει στο [91], αλλά αυτή η προσπάθεια δεν λάμβανε υπόψη της, τον παράγοντα του χρόνου. Ακριβώς για το λόγο αυτό, χρησιμοποιήσαμε στοχαστικές διαδικασίες που μπορούν να διαχειριστούν τον παράγοντα του χρόνου και προτείνουμε το παρακάτω μαθηματικό μοντέλο για την παρακολούθηση και ποσοτικοποίηση του επιπέδου της ασφάλειας μίας υπηρεσίας ή ενός συστήματος πληροφορικής:

$$\text{Security } Status(t) = \int_0^t \prod_{i=1}^{k} f_i(x)\, dx \quad (2)$$

Όπου:	
f_i	Είναι η στοχαστική συνάρτηση που περιγράφει τον τεχνικό παράγοντα κινδύνου i.
K	Είναι ο αριθμός των τεχνικών παραγόντων κινδύνου.
t	Είναι ο χρόνος μέσα στον οποίο θέλουμε να γνωρίζουμε πόσο ασφαλές είναι ένα σύστημα πληροφορικής.

5.3.1 Επεξήγηση μαθηματικού μοντέλου

Ιδιαίτερη έμφαση σε αυτό το σημείο πρέπει να δοθεί στον τρόπο υπολογισμού του επιπέδου ασφαλείας, σύμφωνα με το προτεινόμενο μαθηματικό μοντέλο. Έτσι λοιπόν, βλέπουμε ότι το επίπεδο ασφάλειας ενός συστήματος πληροφορικής, υπολογίζεται από το γινόμενο του επιπέδου της ασφάλειας των επιμέρους στοιχείων που το αποτελούν. Αυτό είναι ιδιαίτερα σημαντικό, γιατί το προτεινόμενο μαθηματικό μοντέλο, λαμβάνει υπόψη του και υλοποιεί μια συγκεκριμένη αλήθεια, ότι εάν ένα από τα στοιχεία του συστήματος πληροφορικής αποτελέσει στόχο μιας επιτυχημένης επίθεσης, τότε όλο το σύστημα πληροφορικής θα θεωρηθεί ότι έχει υποστεί παραβίαση ασφαλείας. Πιο απλά, όταν ένα από τα στοιχεία του συστήματος πληροφορικής υποστεί επιτυχημένη επίθεση, τότε το επίπεδο ασφαλείας του θα είναι μηδέν. Συνεπώς, το γινόμενο του επιπέδου ασφάλειας των στοιχείων του συστήματος πληροφορικής θα γίνει επίσης μηδέν. Αντιθέτως, όταν τα επιμέρους στοιχεία του συστήματος πληροφορικής τείνουν στην μονάδα, τότε και το συνολικό επίπεδο του συστήματος πληροφορικής θα τείνει στην μονάδα, δηλαδή θα θεωρείται ασφαλές.

5.4 Παράγοντες συστημάτων πληροφορικής

Πολλοί θα υποστήριζαν ότι οι κυριότεροι παράγοντες για ένα σύστημα πληροφορικής είναι:

- ✓ Η αξιοπιστία (reliability).
- ✓ Η ασφάλεια (safety).
- ✓ Η συντηρησιμότητα (maintainability).
- ✓ Η διαθεσιμότητα (availability).
- ✓ Η ακεραιότητα (integrity).
- ✓ Η εμπιστευτικότητα (confidentiality).

Όμως, εάν έχουμε να κάνουμε με ένα σύστημα πληροφορικής ή μία υπηρεσία, μπορούμε εύκολα να μετρήσουμε τις παραβιάσεις ασφαλείας (security breaches) όπου και εάν αυτές οφείλονται, όπως: α) σε υπάρχουσες διαδικασίες, β) σε τεχνικά προβλήματα, γ) σε προβλήματα στο εγκατεστημένο λογισμικό, και δ) προέρχονται από ανθρώπινο λάθος. Για το λόγο αυτό, πρέπει να αναλύσουμε το σύστημα πληροφορικής στα επιμέρους μέρη που το αποτελούν.

5.5 Επεξήγηση της προτεινόμενης μεθοδολογίας

Για να γίνει περισσότερο κατανοητή η προσέγγιση αυτή, ας δούμε ένα παράδειγμα υπολογισμού του επιπέδου ασφάλειας μίας διαδικτυακής υπηρεσίας (web service). Έστω, λοιπόν, ότι έχουμε ως παράδειγμα μια διαδικτυακή υπηρεσία που λειτουργεί σε ένα καθορισμένο πλαίσιο διαδικασιών, υλοποιημένη σε μία γνωστή γλώσσα προγραμματισμού, η οποία είναι εγκατεστημένη σε ένα γνωστό εξυπηρετητή. Ο εξυπηρετητής αυτός έχει εγκατεστημένο ένα γνωστό λειτουργικό σύστημα και το υλικό του είναι επίσης καθορισμένο. Επιπλέον, ο εξυπηρετητής συντηρείται από μία μικρή και γνωστή ομάδα διαχειριστών και έχουν πρόσβαση σε αυτόν καθορισμένος και γνωστός αριθμός χρηστών.

Για όλες τις παραπάνω παραμέτρους της διαδικτυακής υπηρεσίας του παραδείγματός μας, είμαστε σε θέση να μετρήσουμε τις ευπάθειες που παρουσιάστηκαν καθώς και τη συχνότητά τους. Η γνώση της συχνότητας εμφάνισης των ευπαθειών, μας επιτρέπει να ανιχνεύσουμε μοτίβα επανάληψης στο χρόνο και συνεπώς να καθορίσουμε τις συναρτήσεις πυκνότητας πιθανότητας (probability density functions) όλων των παραπάνω παραμέτρων. Από τις συναρτήσεις πυκνότητας που βρίσκουμε, είμαστε σε θέση να καθορίσουμε τις συναρτήσεις f_i και, συνεπώς, να μετρήσουμε το τρέχον επίπεδο ασφαλείας της διαδικτυακής υπηρεσίας μας.

Είναι φανερό ότι αυτός ο τρόπος μέτρησης, δεν μπορεί να εφαρμοστεί μόνο στη διαδικτυακή υπηρεσία μας, αλλά και σε ένα σύστημα πληροφορικής. Το μόνο πρόβλημα που φαίνεται ότι υπάρχει, είναι ο καθορισμός των συναρτήσεων πυκνότητας πιθανότητας των επιμέρους στοιχείων (παραμέτρων) του συστήματος πληροφορικής. Θα πρέπει να τονιστεί, ότι η προτεινόμενη μεθοδολογία λαμβάνει υπόψη της τους τεχνικούς παράγοντες κινδύνου και μόνο. Συνεπώς, παραβιάσεις ασφαλείας που έγιναν από ανθρώπινο λάθος δεν αποτελούν μέρος αυτής της ερευνητικής προσπάθειας.

5.6 Open Source Vulnerability Database

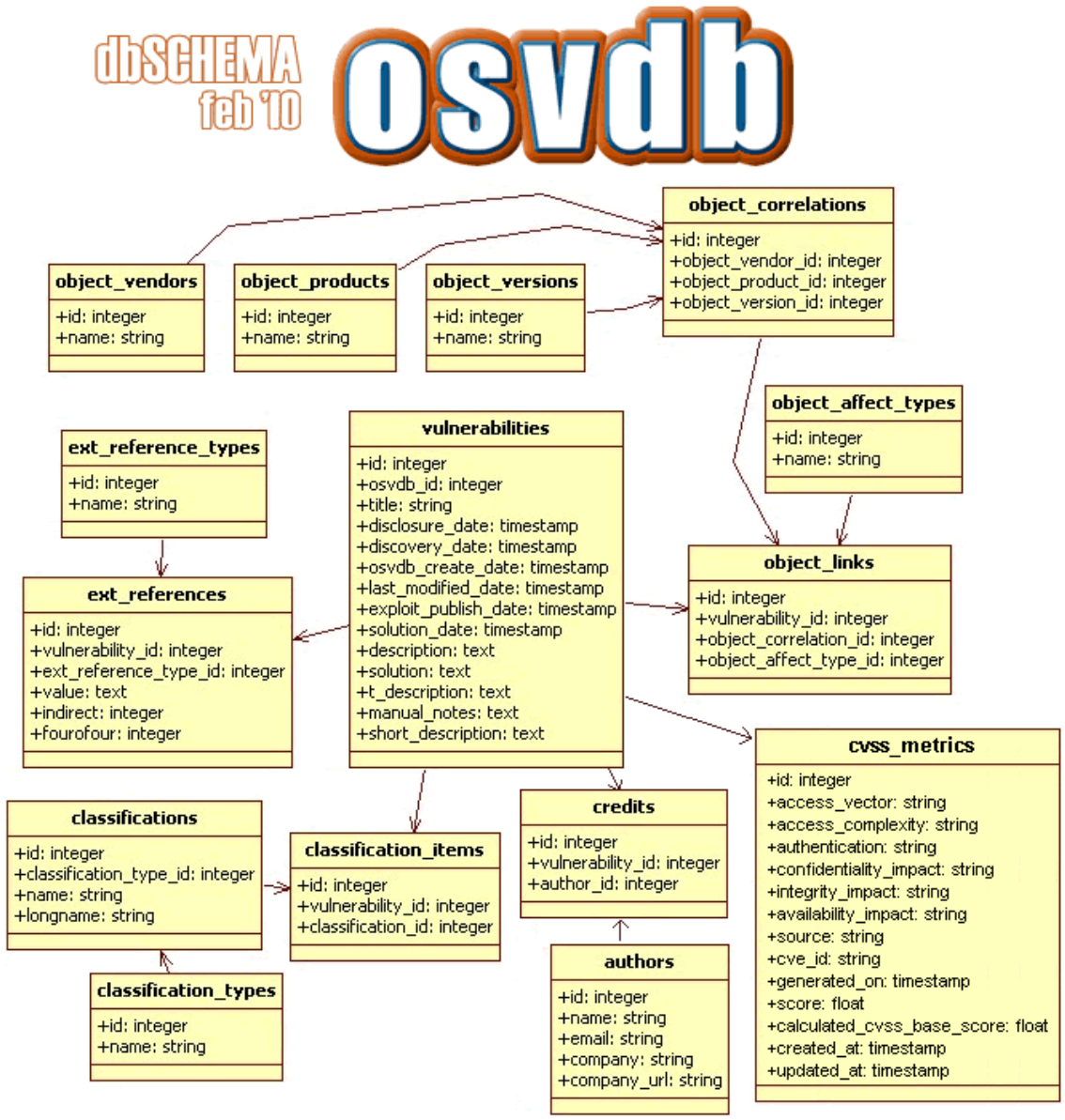
Στο διαδίκτυο υπάρχει ένας ικανός αριθμός από ανοικτού κώδικα (open source) βάσεις δεδομένων, όπως η Open Source Vulnerability Database (OSVDB) [92]. Η OSVDB είναι μία ανεξάρτητη και ανοικτού κώδικα βάση δεδομένων, η οποία δημιουργήθηκε από την κοινότητα των χρηστών, με σκοπό να την εξυπηρετήσει. Στόχος της είναι να παρέχει ακριβή, αναλυτικά, επίκαιρα και αμερόληπτα τεχνικά δεδομένα. Η βάση δεδομένων, την ώρα συγγραφής της παρούσας διατριβής, καλύπτει 80.866 ευπάθειες, που αφορούν 41.677 προϊόντα, έχει ενημερωθεί από 4.735 ερευνητές και εκτείνεται σε μία χρονική περίοδο μεγαλύτερη των 47 ετών.

Στη παρούσα έρευνα, μία από τις βάσεις δεδομένων που χρησιμοποιήθηκε, ήταν η OSVDB, με σκοπό την εξαγωγή στοιχείων αναφορικά με τις ευπάθειες των προϊόντων που μελετήθηκαν. Τέτοια στοιχεία είναι η συχνότητα των ευπαθειών, η

σπουδαιότητά τους, ο αριθμός και ημερομηνία ανακοίνωσής τους (disclosure date). Αυτό μας επέτρεψε, να υπολογίσουμε τα μοτίβα που εμφανίζουν, αναφορικά με την προσφερόμενη ασφάλεια ενός συγκεκριμένου προϊόντος, στη διάρκεια του χρόνου. Οι ευπάθειες αυτές, έχουν αναγνωριστεί από τους κατασκευαστές λογισμικού των προϊόντων που αφορούν, και δεν επιδέχονται καμία αμφισβήτηση. Τα στοιχεία που μελετήθηκαν, εκτείνονται σε μία χρονική περίοδο μεγαλύτερη των είκοσι ετών. Με τον τρόπο αυτό εξασφαλίστηκε η αντικειμενικότητα και η αμεροληψία των αποτελεσμάτων της παρούσας έρευνας.

5.6.1 Σχήμα της βάσης δεδομένων OSVB

Στην Εικόνα 10 αποτυπώνεται το σχήμα της βάσης δεδομένων (πίνακες, σχέσεις και πεδία). Στη συνέχεια θα γίνει μία μικρή αναφορά σχετικά με τα περιεχόμενα κάθε πίνακα.



Εικόνα 10: Σχηματική απεικόνιση της βάσης δεδομένων OSVDB

Όπου:

Πεδίο	Περιγραφή
External Reference	Τα external reference, είναι πληροφορίες σχετικά με τις ευπάθειες, που προέρχονται εκτός της βάσης δεδομένων, για παράδειγμα έναν υπερσύνδεσμο (link) στην ιστοσελίδα της κατασκευάστριας εταιρείας λογισμικού.
Vulnerabilities	Είναι ο κυρίως πίνακας της βάσης αυτής. Σε αυτόν αποθηκεύονται οι κωδικοί (OSVDB ID) καθώς και οι περιγραφές και οι ημερομηνίες κάθε ευπάθειας.
Authors	Σε αυτόν τον πίνακα αποθηκεύονται οι ερευνητές που καταχώρησαν κάποια ευπάθεια στην βάση δεδομένων.
Ext_References	Αυτός ο πίνακας συσχετίζει τις εξωτερικές αναφορές με κάποια από τις ευπάθειες της βάσης δεδομένων (OSVDB ID). Η σχέση αυτή είναι τύπου 1→N.
Ext_references_Types	Ο πίνακας αυτός περιέχει τους τύπους των εξωτερικών αναφορών με μία μικρή περιγραφή για την καλύτερη επεξεργασία τους.
Classification_Items	Ο πίνακας αυτός συσχετίζει τις ευπάθειες με τους τύπους κατηγοριοποίησης των ευπαθειών.
Classifications	Ο πίνακας αυτός περιέχει τις διάφορες κατηγοριοποιήσεις των ευπαθειών.
Classification_Types	Ο πίνακας αυτός ομαδοποιεί τις διάφορες κατηγοριοποιήσεις των ευπαθειών.
Object_Links	Ο πίνακας αυτός περιέχει πληροφορίες σχετικά με τα διάφορα προϊόντα και συνδέεται με τα osvbd_id. Αναφέρεται στα προϊόντα που βρέθηκαν οι ευπάθειες.
Object_Correlations	Αυτός ο πίνακας συσχετίζει τους κατασκευαστές λογισμικού με τις εκδόσεις των προϊόντων και τις ευπάθειές τους.
Object_Affect_Types	Αυτός ο πίνακας αποθηκεύει τις πιθανές τιμές επηρεασμού ενός συστήματος.

Πεδίο	Περιγραφή
Object_Products	Αυτός ο πίνακας περιέχει την πλήρη περιγραφή των προϊόντων, π.χ. Windows Exchange.
Object_Vendors	Αυτός ο πίνακας περιέχει τα ονόματα των κατασκευαστών λογισμικού, π.χ. Sun Microsystems.
Object_Versions	Αυτός ο πίνακας περιέχει τις περιγραφές των εκδόσεων των διαφόρων προϊόντων, π.χ. XP, 2000 κτλ.
Credits	Αυτός ο πίνακας βοηθά στην αναγνώριση των ερευνητών. Αντί να αποθηκεύονται οι πληροφορίες του κάθε ερευνητή, γίνεται αναφορά στον πίνακα των ερευνητών (Authors).

Πίνακας 11: Επεξήγηση του σχήματος της βάσης δεδομένων OSVDB.

5.7 National Vulnerability Database

Άλλη μία ανοιχτή προς το κοινό, βάση δεδομένων, που χρησιμοποιήθηκε στη παρούσα έρευνα και περιέχει ευπάθειες συστημάτων πληροφορικής είναι η National Vulnerability Database (NVD) [93]. Στη βάση αυτή περιέχονται 50.291 ευπάθειες, που καλύπτουν ένα διάστημα μεγαλύτερο των 20 ετών.

Η βάση NVD, είναι ένα προϊόν του Τμήματος Ασφάλειας Συστημάτων Πληροφορικής της NIST [93] και υποστηρίζεται από το Τμήμα Εθνικής Ασφάλειας Κυβερνοχώρου, του Υπουργείου Εθνικής Αμύνης των Ηνωμένων Πολιτειών [94]. Το προϊόν αυτό έχει δημιουργηθεί για να υποστηρίξει διάφορες υπηρεσίες των Ηνωμένων Πολιτειών και αποτελεί ένα κυβερνητικό χώρο αποτύπωσης εκείνων των προτύπων ασφάλειας, που βασίζονται στις ευπάθειες συστημάτων πληροφορικής, όπως για παράδειγμα το FISMA, § 4.11.1.

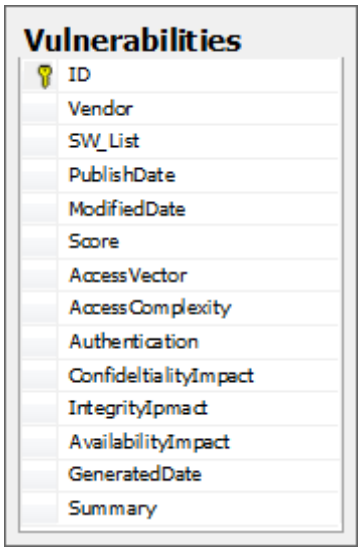
Η χρησιμοποίηση της NVD μας έδωσε τη δυνατότητα να μελετήσουμε τη συχνότητα των ευπαθειών, την κατηγοριοποίησή τους ανάλογα με το CVSS Score που έχουν, τον αριθμό και την ημερομηνία ανακοίνωσής τους (Publish date). Αυτό μας επέτρεψε, να υπολογίσουμε τα μοτίβα που εμφανίζουν, αναφορικά με την προσφερόμενη ασφάλεια ενός συγκεκριμένου προϊόντος, στη διάρκεια του χρό-

νου. Οι ευπάθειες αυτές, έχουν αναγνωριστεί από τους κατασκευαστές λογισμικού των προϊόντων που αφορούν, και δεν επιδέχονται καμία αμφισβήτηση. Τα στοιχεία που μελετήθηκαν, εκτείνονται σε μία χρονική περίοδο μεγαλύτερη των είκοσι ετών. Με τον τρόπο αυτό εξασφαλίστηκε η αντικειμενικότητα και η αμεροληψία των αποτελεσμάτων της παρούσας έρευνας.

5.7.1 Σχήμα της βάσης δεδομένων NVD

Η NVD παρέχει ένα σύνολο από xml αρχεία στα οποία περιέχονται οι πληροφορίες για τις ευπάθειες που έχουν βρεθεί και για κάθε ένα έτος υπάρχει και ένα xml αρχείο. Δυστυχώς όμως, η έκδοση του σχήματος που περιγράφει κάθε ένα xml αρχείο δεν είναι η ίδια. Για να μπορέσουμε να μελετήσουμε τα δεδομένα αναφορικά με τις ευπάθειες που περιέχονται στα αρχεία αυτά, ως σύνολο, και να ξεπεράσουμε το πρόβλημα των διαφορετικών εκδόσεων σχήματος των xml, δημιουργήθηκε ένα πρόγραμμα σε γλώσσα προγραμματισμού VB.Net, το οποίο διάβαζε τα διάφορα αρχεία από την NVD και καταχωρούσε τα στοιχεία που χρειαζόμασταν, σε μία βάση δεδομένων SQL Server.

Ο τελικός πίνακας αποθήκευσης με την ονομασία «Vulnerabilities», αποτυπώνεται στο σχήμα της βάσης δεδομένων που ακολουθεί. Στη συνέχεια θα γίνει μία μικρή αναφορά σχετικά με τα περιεχόμενα του πίνακα.



Εικόνα 11: Σχηματική απεικόνιση της βάσης δεδομένων NVD

Όπου:

Πεδίο	Περιγραφή
ID	Είναι ο κωδικός της ευπάθειας σύμφωνα με την NVD.
Vendor	Είναι ο κατασκευαστής λογισμικού.
SW List	Είναι μία λίστα από τα προϊόντα που επηρεάστηκαν από τη συγκεκριμένη ευπάθεια.
Publish Date	Είναι η ημερομηνία ανακοίνωσης της ευπάθειας.
Modified Date	Είναι η ημερομηνία που έγινε η τελευταία ενημέρωση της εγγραφής.
Score	Είναι η τιμή που αποδόθηκε στην ευπάθεια αυτή, βάση της CVSS μεθοδολογίας, § 4.10.4.
Access Vector	Στη στήλη αυτή αναγράφεται ο τύπος επίδρασης που είχε η ευπάθεια, για παράδειγμα δικτυακή (Network) / τοπική (Local).
Access Complexity	Η πολυπλοκότητα της ευπάθειας. Οι τιμές που μπορεί να έχει αυτή η στήλη είναι Υψηλή, Μέτρια και Χαμηλή.
Authentication	Αναφέρονται οι περιπτώσεις εμφάνισης της ευπάθειας. Πιθανές τιμές είναι Single Instance ή None.
Confidentiality Impact	Η επίπτωση της ευπάθειας στον τομέα της εμπιστευτικότητας των δεδομένων. Οι τιμές που μπορεί να έχει αυτή η στήλη είναι Υψηλή, Μέτρια και Χαμηλή.
Integrity Impact	Η επίπτωση της ευπάθειας στον τομέα της ακεραιότητας των δεδομένων. Οι τιμές που μπορεί να έχει αυτή η στήλη είναι Υψηλή, Μέτρια και Χαμηλή.
Availability Impact	Η επίπτωση της ευπάθειας στον τομέα της διαθεσιμότητας των δεδομένων. Οι τιμές που μπορεί να έχει αυτή η στήλη είναι Υψηλή, Μέτρια και Χαμηλή.
Generated Date	Η ημερομηνία δημιουργία της εγγραφής.

Πεδίο	Περιγραφή
Summary	Μία μικρή περιγραφή της ευπάθειας και των συνεπειών της.

Πίνακας 12: Επεξήγηση του σχήματος της βάσης δεδομένων NVD

5.8 Σταθμισμένη εντροπία

Είναι γενικά αποδεκτό, ότι η ασφάλεια των συστημάτων πληροφορικής δεν μπορεί να διαχειριστεί αν δεν μπορεί να μετρηθεί επαρκώς με αντικειμενικότητα και αμεροληψία, όπως αναφέρεται και στο [75]. Η αντικειμενικότητα κατά τη διαδικασία μέτρησης των κινδύνων, μπορεί να μας δώσει απαντήσεις σε ερωτήσεις όπως:

1. Ποιο μπορούμε να θεωρήσουμε ότι είναι το τρέχον επίπεδο ασφάλειας της εταιρείας ή του οργανισμού;
2. Ποιά είναι η κατάσταση ασφάλειας ενός συστήματος πληροφορικής της εταιρείας ή του οργανισμού;
3. Ποιά είναι η χρονική στιγμή κατά την οποία ένα σύστημα πληροφορικής θεωρείται ως περισσότερο ευάλωτο;

Η παρούσα έρευνα επικεντρώνεται περισσότερο στο να δώσει απαντήσεις σχετικά με τη δεύτερη ερώτηση η οποία θα δημιουργήσει το κατάλληλο θεωρητικό υπόβαθρο για να απαντήσουμε την πρώτη και την πιο καίρια.

Έχοντας λοιπόν υπόψη την μέγιστη επίτευξη της αντικειμενικότητας, χρησιμοποιήσαμε την μεθοδολογία της σταθμισμένης εντροπίας ως μέσον για την εκτίμηση κινδύνου ενός συστήματος πληροφορικής. Στην παρούσα έρευνα αποτυπώνεται μια εκτεταμένη στατιστική ανάλυση «κυριολεκτικά όλων», των τεχνικών παραγόντων κινδύνου, οι οποίοι έχουν προκαλέσει ζημιά ή κατέστησαν μη λειτουργικά συστήματα πληροφορικής, κατά τη διάρκεια των τελευταίων είκοσι ετών.

Ο Shannon [95] εισήγαγε τον όρο «εντροπία της πληροφορίας», με σκοπό να μετρήσει την αβεβαιότητα που είναι συσχετισμένη με τυχαίους παράγοντες. Ακολουθώντας λοιπόν τη θεωρία του, μετρήσαμε την εντροπία σε σχέση με τον «τυχαίο παράγοντα», δηλαδή την «εμφάνιση των ευπαθειών» για σύστημα πληροφορικής. Ο ορισμός της εντροπίας H(X) όμως, είναι αρκετά γενικός και εκφράζεται σε διακεκριμένες ομάδες πιθανοτήτων p_i :

$$H(X) = -\sum_{i=1}^{n} p_i \log(p_i) \quad (\mathbf{3})$$

Όπου:	
i	Είναι ο δείκτης της κλίμακας των επιπτώσεων (None, Complete, Partial) που βρέθηκαν στην βάση δεδομένων (OSVDB), με όλες τις ευπάθειες τα τελευταία είκοσι χρόνια, για τα προϊόντα που μελετήθηκαν.
p_i	Η πιθανότητα να συμβεί μια ευπάθεια επίπτωσης i.

5.8.1 Υπολογισμός των πιθανοτήτων p_i

Η παρούσα έρευνα επικεντρώθηκε κυρίως σε κατασκευαστές λογισμικού όπως η Microsoft και Oracle, λόγω του μεγάλου αριθμού προϊόντων τους, καθώς και των διαφορετικών εκδόσεων αυτών, σε βάθος χρόνου. Ο μεγάλος αριθμός προϊόντων λογισμικού και των εκδόσεών τους, έχουν σωρευτικά, εμφανίσει ένα ιδιαίτερα μεγάλο αριθμό ευπαθειών τα τελευταία είκοσι χρόνια. Μετρώντας λοιπόν, τον αριθμό των ευπαθειών για κάθε προϊόν καταφέραμε να υπολογίσουμε την πιθανότητα p_i, χρησιμοποιώντας τον παρακάτω τύπο:

$$p_i = \frac{Αριθμός\ ευπαθειών\ επίπτωσης\ i}{\text{Συνολικός αριθμός ευπαθειών}} \quad (\mathbf{4})$$

Όπου:	
I	Είναι ο δείκτης της κλίμακας των επιπτώσεων για όλες τις ευπάθειες των τελευταίων είκοσι ετών, για τα προϊόντα που μελετήθηκαν: α) (None, Complete, Partial) από τα στοιχεία που βρέθηκαν στην βάση δεδομένων (OSVDB), ή β) (CVSS Score) από τα στοιχεία που βρέθηκαν στην (NVD)

5.8.2 Χρήση ειδικών βαρών στον υπολογισμό της εντροπίας

Χρησιμοποιώντας μια ανοικτού κώδικα βάση δεδομένων, όπως την OSVDB ή / και NVD, βρέθηκε λύση στο πρόβλημα της ανεύρεσης των συμβάντων. Αυτό που όμως παρέμενε, ήταν ότι για όλα τα συμβάντα – ευπάθειες, που βρέθηκαν στις βάσεις δεδομένων των είκοσι και πλέον ετών, είχε υπολογιστεί η ίδια τιμή για την πιθανότητα να συμβούν, γεγονός που δεν θα μας οδηγούσε σε ακριβή αποτελέσματα. Εάν παραβλέπαμε αυτό το γεγονός, θα είχαμε παραλείψει μία πολύ σημαντική πληροφορία, αυτή της ποιότητας κάθε τεχνικού παράγοντα κινδύνου (technical risk factor).

Με άλλα λόγια, κάθε παράγοντας κινδύνου δεν αναμένεται να προκαλέσει την ίδια ζημιά και να εκθέσει ένα σύστημα πληροφορικής στον ίδιο βαθμό. Για το λόγο αυτό, μελετήθηκε η επίπτωση (impact) κάθε παράγοντα κινδύνου στις βάσεις δεδομένων που είχαμε. Ο σκοπός μας ήταν, να καθορίσουμε ένα «ειδικό βάρος» για κάθε παράγοντα κινδύνου, όχι βάσει των συνολικών ευπαθειών που βρέθηκαν στο βάθος του χρόνου, αλλά σε σχέση με τη σοβαρότητα (severity) αυτών στο ίδιο χρονικό διάστημα.

Ήταν αναμενόμενο, ότι τα μεγάλα λειτουργικά συστήματα, θα ήταν περισσότερο επιρρεπή σε επιθέσεις και για αυτό θα υπήρχαν πολλές πολλαπλάσιες περιπτώσεις ευπαθειών καταγεγραμμένες για αυτά, στις βάσεις δεδομένων που διαθέταμε. Αυτό όμως, δεν θα έπρεπε να αλλάξει το «ειδικό βάρος» του παράγοντα κινδύνου, εκτός φυσικά αν οι περισσότεροι από αυτούς ήταν κατηγοριοποιημένοι ως πολύ σοβαροί (severe).

Έτσι λοιπόν, για να διακρίνουμε τους παράγοντες κινδύνους σε σχέση με την επίπτωσή τους σε ένα σύστημα πληροφορικής, ανάλογα με τη βάση δεδομένων που χρησιμοποιήσαμε, ακολουθήσαμε την εξής μεθοδολογία:

- Στην βάση δεδομένων OSVDB, υπάρχουν τρείς πιθανές επιπτώσεις που μπορεί ένας παράγοντας κινδύνου να επιφέρει σε ένα σύστημα πληροφορικής: α) Καμία (None), β) Μεσαία (Partial) και γ) Υψηλή (Complete). Χρησιμοποιώντας την ποιοτική διάκριση (qualitative distinction), αναθέσαμε διαφορετικά «ειδικά βάρη» ανάλογα με την επίπτωση που θα είχαν σε ένα σύστημα πληροφορικής: α) 1, β) 3 και γ) 10, αντίστοιχα.
- Στην βάση δεδομένων NVD, υπάρχει ειδική στήλη, «CVSS Score», που απεικονίζει το βαθμό της επίπτωσης της ευπάθειας σε ένα σύστημα πληροφορικής, βάσει του συστήματος αξιολόγησης των επιπτώσεων Common Vulnerability Scoring System (CVSS). Η μεθοδολογία CVSS είναι ευρέως αποδεκτή και τη χρησιμοποιούν πολύ γνωστές εταιρείες του κλάδου της Πληροφορικής, όπως η McAfee, Symantec, Microsoft, Cisco κ.α. Με τη χρήση ενός τέτοιου μέτρου η μεθοδολογία μας εξασφαλίζει ακόμα μεγαλύτερο βαθμό αμεροληψίας στην ανάθεση ειδικών βαρών στους τεχνικούς παράγοντες κινδύνου.

Χρησιμοποιήσαμε τα προτεινόμενα βάρη στον υπολογισμό της εντροπίας της πληροφορίας καταλήξαμε στην ακόλουθη εξίσωση:

$$W(X) = W(w_1, w_2, \dots w_n; p_1, p_2, \dots p_n) = -\sum_{i=1}^{n} w_i p_i \log(p_i) \quad (\mathbf{5})$$

Όπου:	
w_i	Είναι το ειδικό βάρος για κάθε πιθανή κατηγορία επίπτωσης ενός παράγοντα κινδύνου.

Συνεπώς, ας υποθέσουμε ότι έχουμε ένα σύστημα πληροφορικής, για το οποίο έχουμε αναγνωρίσει όλους τους παράγοντες κινδύνου του. Για να μπορέσουμε να υπολογίσουμε το επίπεδο ασφάλειάς του, χρησιμοποιώντας την εξίσωση 2, θα πρέπει να καθορίσουμε καλύτερα την στοχαστική συνάρτηση f_i, και να καθορίσουμε τα ειδικά βάρη σε κάθε ένα παράγοντα και να τα θέσουμε ως εκθέτη. Φυσικά υποθέτουμε, ότι αν ένας από τους παράγοντες κινδύνου μηδενιστεί, τότε το συνολικό επίπεδο ασφάλειας του συστήματος πληροφορικής πρέπει να θεωρηθεί και αυτό μηδέν. Αυτό από μόνο του μας οδηγεί στη δημιουργία ενός γινομένου. Εάν υποθέσουμε, ότι κάθε παράγοντας κινδύνου, είναι ανεξάρτητος από τους υπόλοιπους, τότε για να ενσωματώσουμε τα ειδικά βάρη στον υπολογισμό του επιπέδου της ασφάλειας ενός συστήματος πληροφορικής, η εξίσωση 2 μετασχηματίζεται στην ακόλουθη εξίσωση:

$$Security\ Status = \int \prod f_i^{\frac{1}{c_i}}(t)dt \quad (\mathbf{6})$$

Όπου:	
c_i	Είναι το ειδικό βάρος για κάθε παράγοντα κινδύνου.

Με τον τρόπο υπολογισμού που προτείνεται, πετυχαίνουμε ότι εάν έχουμε ένα συμβάν υψηλής επίπτωσης – επικινδυνότητας (high impact), να υπολογίζεται και υψηλή τιμή της εντροπίας και αντίστροφα.

Θέτουμε το c_i ως την υπολογιζόμενη σταθμισμένη εντροπία για κάθε παράγοντα κινδύνου όπως εμφανίζεται στην ακόλουθη εξίσωση 7:

$$c_i = -\sum_{j=1}^{n} w_j p_j \log(p_j) \quad (7)$$

Όπου:	
n	Είναι ίσο με τον αριθμό των διαφορετικών κατηγοριών επιπτώσεων, που μπορεί ένας παράγοντας κινδύνου να επιφέρει σε ένα σύστημα πληροφορικής.
w_j	Είναι το ειδικό βάρος του παράγοντα κινδύνου.

Με τον τρόπο αυτό, είμαστε σε θέση να μετρήσουμε πόσο επηρεάζεται το γινόμενο από τους παράγοντες αυτούς, χρησιμοποιώντας ως μέτρο τη σταθμισμένη εντροπία της σοβαρότητας της εκάστοτε ευπάθειας, γεγονός που κάνει τους υπολογισμούς μας, αμερόληπτους.

Επιπλέον, επειδή οι συναρτήσεις f_i, επηρεάζονται μόνο από τον παράγοντα του χρόνου και αφού $0 \leq f_i \leq 1$, μπορούμε να συμπεράνουμε ότι αν η τιμή της συνάρτησης αυξηθεί, τότε θα αυξηθεί και το ειδικό βάρος και αντιστρόφως.

5.8.3 Χρήση του παράγοντα χρόνου στον υπολογισμό του ειδικού βάρους

Χρησιμοποιώντας την παραπάνω μεθοδολογία, θεωρήσαμε ότι το ειδικό βάρος για κάθε παράγοντα κινδύνου είναι σταθερό και συμμετέχει στους υπολογισμούς. Όμως εδώ γεννάται το ερώτημα, «Είναι σωστό ένας παράγοντας κινδύνου που εμφανίστηκε σε παλαιότερα έτη, να επηρεάζει το συνολικό επίπεδο ασφαλείας ενός συστήματος πληροφορικής το ίδιο, με ένα νέο παράγοντα κινδύνου που εμφανίστηκε πολύ κοντά στην σημερινή ημερομηνία»; Υποστηρίζουμε πως όχι. Ορισμένοι από τους παράγοντες κινδύνου, ειδικά όταν αναφερόμαστε σε ευπάθειες, είναι αναμενόμενο να εμφανιστούν στα πρώτα χρόνια κυκλοφορίας ενός λειτουργικού λογισμικού για παράδειγμα, ενώ είναι μη αποδεκτό η μακροχρόνια ύπαρξή τους. Έτσι, λαμβάνοντας υπόψη και την εξέλιξη της κοινότητας των προ-

γραμματιστών, εφαρμόζουμε ενός είδους ποινής (penalty) σε αυτά τα προϊόντα που ενώ είναι καιρό στην αγορά είναι ακόμη ευάλωτα σε ευπάθειες.

Για να το αποτυπώσουμε αυτό στη μεθοδολογία υπολογισμού μας, εισάγουμε ένα τρόπο μεταβολής των ειδικών βαρών c_i για κάθε παράγοντα κινδύνου του συστήματος πληροφορικής που μελετάμε. Για να εξισορροπήσουμε την υπολογιζόμενη ποσότητα την υψώνουμε στη δύναμη k. Με το σκεπτικό αυτό, προτείνεται η ακόλουθη εξίσωση:

$$c_i = -\sum_{j=1}^{n}\sum_{k=0}^{m} e^{-k} w_j p_{jk} \log\left(p_{jk}\right) \quad (\mathbf{8})$$

Όπου:	
i	Είναι το προϊόν λογισμικού.
n	Είναι ίσο με τον αριθμό των διαφορετικών κατηγοριών επιπτώσεων, που μπορεί ένας παράγοντας κινδύνου να επιφέρει σε ένα σύστημα πληροφορικής.
w_j	Είναι το ειδικό βάρος του παράγοντα κινδύνου.
m	Είναι ο αριθμός των ετών που το προϊόν λογισμικού i, βρίσκεται στην αγορά.
j	Είναι οι κατηγορίες επιπτώσεων (impact) των κινδύνων.
k	Είναι ο αριθμός των ετών που ένα προϊόν λογισμικού βρίσκεται στην αγορά.
p_{jk}	Είναι η πιθανότητα το προϊόν λογισμικού i, να ανήκει σε μία κατηγορία επίπτωσης (impact) κινδύνου j, και να βρίσκεται στην αγορά k έτη.

5.8.4 Χρήση του «ποσοστού χρήσης» στον υπολογισμό του βάρους

Ο υπολογισμός του ειδικού βάρους μπορεί περαιτέρω να βελτιωθεί με την εισαγωγή της έννοιας «ποσοστό χρήσης». Για να πετύχουμε ακόμη περισσότερη ακρίβεια και αντικειμενικότητα στις μετρήσεις του συνολικού επιπέδου ασφάλειας

του συστήματος πληροφορικής, θα πρέπει να εξετάσουμε την περίπτωση μία συγκεκριμένη εφαρμογή να είναι επιρρεπής σε ευπάθειες, αλλά να μην χρησιμοποιείται τόσο συχνά. Συνεπώς, ενσωματώσαμε και την παράμετρο αυτή στην εξίσωση υπολογισμού και έτσι προτείνεται η ακόλουθη εξίσωση:

$$c_i = -\sum_{j=1}^{n}\sum_{k=1}^{m} t_{ik} e^{-k} w_j p_{ijk} \log\left(p_{ijk}\right) \quad (\mathbf{9})$$

Όπου:	
i	Είναι το προϊόν λογισμικού.
n	Είναι ο αριθμός διαφορετικών κατηγοριών επιπτώσεων (impact), που υπάρχουν για το προϊόν i.
w_j	Είναι το ειδικό βάρος του παράγοντα κινδύνου για κάθε n.
m	Είναι ο αριθμός των ετών που το προϊόν λογισμικού i βρίσκεται στην αγορά.
p_{ijk}	Η πιθανότητα που ένα προϊόν λογισμικού i να έχει μία ευπάθεια j και να βρίσκεται στην αγορά για k χρόνια.
k	Είναι ο αριθμός των ετών που ένα προϊόν λογισμικού βρίσκεται στην αγορά.
t_{ik}	Είναι το ποσοστό της χρήσης του προϊόντος λογισμικού i, που βρίσκεται στην αγορά k έτη.

5.9 Υπολογισμός της εντροπίας

Έχοντας καθορίσει τα βάρη σε κάθε κατηγορία επίπτωσης, προχωρήσαμε και υπολογίσαμε την εντροπία της πληροφορίας για όλους του παράγοντες κινδύνου και για όλους τους κατασκευαστές λογισμικού που υπήρχαν στη βάση δεδομένων μας. Αυτό μας έδωσε μία αμερόληπτη και ακριβή εικόνα για όλους τους κατασκευαστές και τα προϊόντα τους. Μερικά από τα αποτελέσματα παρουσιάζονται παρακάτω:

Κατασκευαστής (Vendor)	*Προϊόν (Product)*	*Σύνολο ευπαθειών (Total Vulnerabilities)*	*Επιπτώσεις (Impact)*			*Σύνολο εντροπίας (Total Entropy) Log base 10*
			Καμία (None)	*Μεσαία (Partial)*	*Υψηλή (Complete)*	
Microsoft	Windows XP	3836	616	1520	1700	2,172
Microsoft	Windows 2003	2496	300	890	1306	2,062
Microsoft	Office XP	210	9	90	111	2,000

Πίνακας 13: Πίνακας με τις τιμές εντροπίας γνωστών προϊόντων λογισμικού, της κατασκευάστριας εταιρείας Microsoft (Τα στοιχεία προέρχονται από την OSVDB)

Κατασκευαστής (Vendor)	*Προϊόν (Product)*	*Σύνολο ευπαθειών (Total Vulnerabilities)*	*Επιπτώσεις (Impact)*			*Εντροπία με τη χρήση του παράγοντα χρόνου (Taking into account the time factor)*
			Καμία (None)	*Μεσαία (Partial)*	*Υψηλή (Complete)*	
Microsoft	Windows XP	3836	616	1520	1700	0,22
Microsoft	Windows 2003	2496	300	890	1306	0,35
Microsoft	Office XP	210	9	90	111	0,13

Πίνακας 14: Πίνακας με τις τιμές εντροπίας γνωστών προϊόντων λογισμικού χρησιμοποιώντας και τον παράγοντα του χρόνου (Τα στοιχεία προέρχονται από την OSVDB)

Κατασκευαστής (Vendor)	*Προϊόν (Product)*	*Σύνολο ευπαθειών (Total Vulnerabilities)*	*Εντροπία με τη χρήση του παράγοντα χρόνου (Taking into account the time factor)*
Microsoft	Windows XP	638	3,072
Microsoft	Windows 2003	565	3,375
Microsoft	Office XP	110	1,2015

Πίνακας 15 Πίνακας με τις τιμές εντροπίας γνωστών προϊόντων λογισμικού, της κατασκευάστριας εταιρείας Microsoft (Τα στοιχεία προέρχονται από την NVD)

Είναι φανερό ότι ενώ το σύνολο των ευπαθειών και η κατηγοριοποίηση των επιπτώσεων για τα προϊόντα του πίνακα διαφέρουν κατά πολύ, η χρήση της σταθμισμένης εντροπίας, μας δίνει τη δυνατότητα να έχουμε ένα κοινό μέτρο και να κάνουμε την σύγκριση μεταξύ αυτών.

Από τη στιγμή που υπολογίσαμε τη δύναμη $\frac{1}{c_i}$ μικρές διαφορές παράγουν αντιληπτά αποτελέσματα στο σύνολο των μετρήσεων. Οι μετρήσεις έγιναν με την παραδοχή ότι ποσοστό χρήσης των προϊόντων που μελετήθηκαν, ήταν 100%. Παρόλο που οι μετρήσεις προέρχονται από δύο διαφορετικές βάσεις δεδομένων, βλέπουμε ότι τα αποτελέσματα μας οδηγούν στο ίδιο συμπέρασμα σχετικά με την εντροπία.

5.10 Προσέγγιση της στοχαστικής συνάρτησης

Έχοντας υπολογίσει τα βάρη με οποιαδήποτε από τις παραπάνω μεθόδους, αυτό που μας λείπει για τον υπολογισμό του επιπέδου της ασφάλειας ενός συστήματος πληροφορικής είναι, να προσεγγίσουμε τις στοχαστικές συναρτήσεις που θα πρέπει να χρησιμοποιήσουμε στην εξίσωση υπολογισμού.

Για την επίτευξη του σκοπού αυτού, επιλέξαμε την εμπειρική προσέγγιση στον μεγάλο όγκο δεδομένων που διαθέταμε. Η ιδέα ήταν, ότι έπρεπε να μελετηθούν αν υπήρχαν ενδείξεις ύπαρξης χρονικών προτύπων [96], τα οποία χαρακτήριζαν τους παράγοντες κινδύνου που επηρεάζουν τα συστήματα πληροφορικής. Αυτό, θα αρκούσε ώστε να οδηγηθούμε στην εμπειρική επαλήθευση του προτεινόμενου μοντέλου, εξίσωση 2.

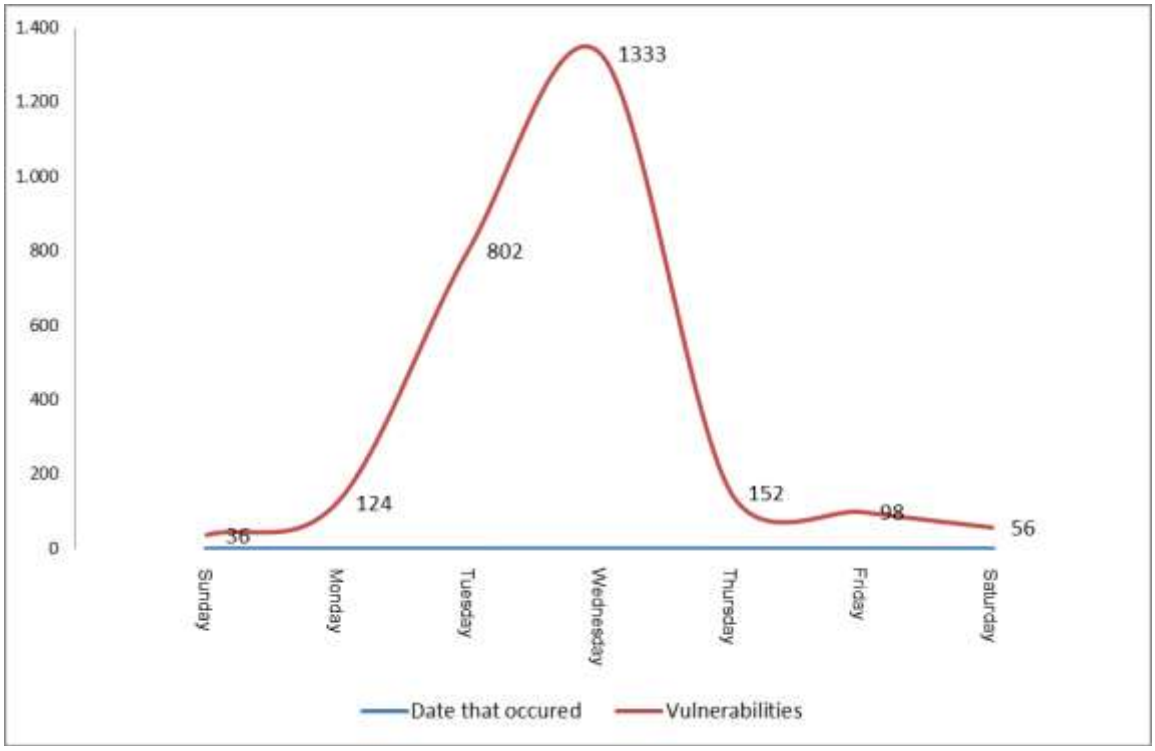
Η εμπεριστατωμένη μελέτη των χρονικών μοτίβων στα δεδομένα που διαθέταμε, αποκάλυψε τις κατανομές των πιθανοτήτων, που ακολουθεί κάθε παράγοντας κινδύνου. Έτσι λοιπόν, η επιθυμητή στοχαστική συνάρτηση, η οποία αναπαριστά κάθε παράγοντα κινδύνου, μπορεί πλέον, να προσεγγιστεί με την ακρίβεια και την αντικειμενικότητα που αναζητούσαμε.

5.11 Ανάλυση χρονικών προτύπων

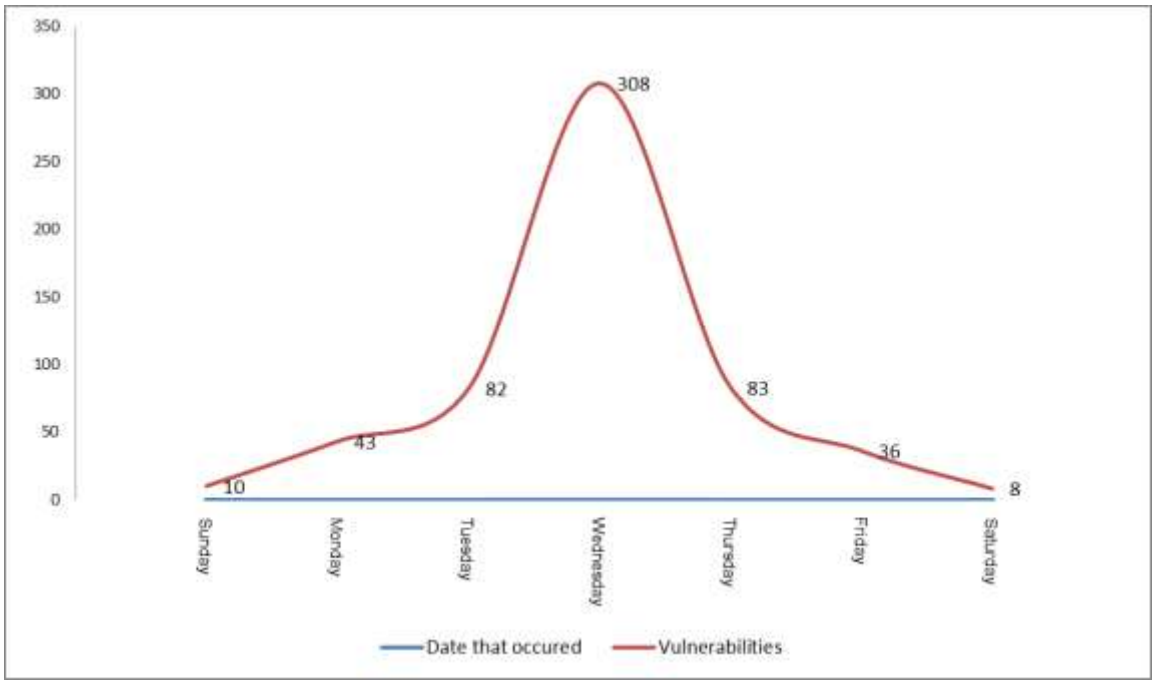
Είναι χωρίς αμφιβολία, πάρα πολύ ενδιαφέρουσα, η έρευνα σχετικά με τις ευπάθειες που τα τελευταία χρόνια έχουν προκαλέσει ζημία στα συστήματα πληροφορικής. Με τη χρήση κατάλληλων ερωτημάτων στις βάσεις δεδομένων OSVDB και NVD, καταφέραμε να ανακαλύψουμε όχι μόνο τις κατανομές πιθανοτήτων των παραγόντων κινδύνου, αλλά και άλλες πολύ χρήσιμες πληροφορίες. Μία από τις πιο ενδιαφέρουσες πληροφορίες είναι, η πολιτική που υλοποιούν οι διάφοροι μεγάλοι κατασκευαστές λογισμικού, αναφορικά με τη δημιουργία και αποστολή, διορθωτικών πακέτων λογισμικού για τα προϊόντα τους. Αυτό, με τη σειρά του μας έδωσε απαντήσεις σε καίρια ερωτήματα που θα εξηγήσουμε παρακάτω.

5.11.1 Κατανομή ευπαθειών για Windows 2003

Ξεκινώντας την έρευνά μας, αναλύσαμε τη κατανομή ευπαθειών ενός προϊόντος του κατασκευαστή λογισμικού Microsoft, και συγκεκριμένα για τα Windows 2003. Βρήκαμε τον αριθμό των ευπαθειών που ανακοινώθηκαν και τον κατηγοριοποιήσαμε ανάλογα με την ημέρα της εβδομάδας. Έτσι λοιπόν το Διάγραμμα 1 και το Διάγραμμα 2, αποτυπώνουν την κατανομή αυτή. Βλέπουμε ότι είναι τύπου καμπάνας και ότι η κορύφωση της ανακοίνωσης των ευπαθειών συμβαίνει περίπου την Τετάρτη. Επίσης, μπορούμε να δούμε ότι ο αριθμός αυτός περίπου αγγίζει τις 1.333 σύμφωνα με την OSVDB και 308 σύμφωνα με την NVD, ευπάθειες. Τα διαγράμματα για το προϊόν αυτό αποτυπώνουν ξεκάθαρα το χρονικό πρότυπο που αναζητούσαμε.



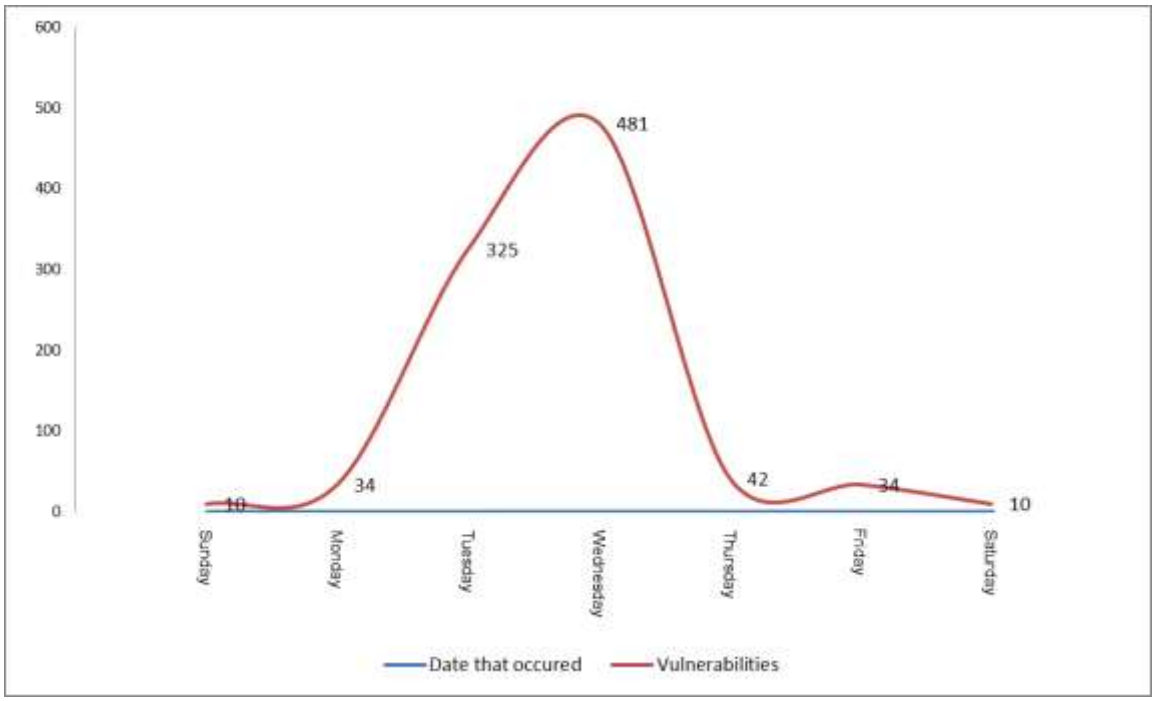
Διάγραμμα 1: Κατανομή ευπαθειών για το προϊόν Windows 2003 του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την OSVDB)



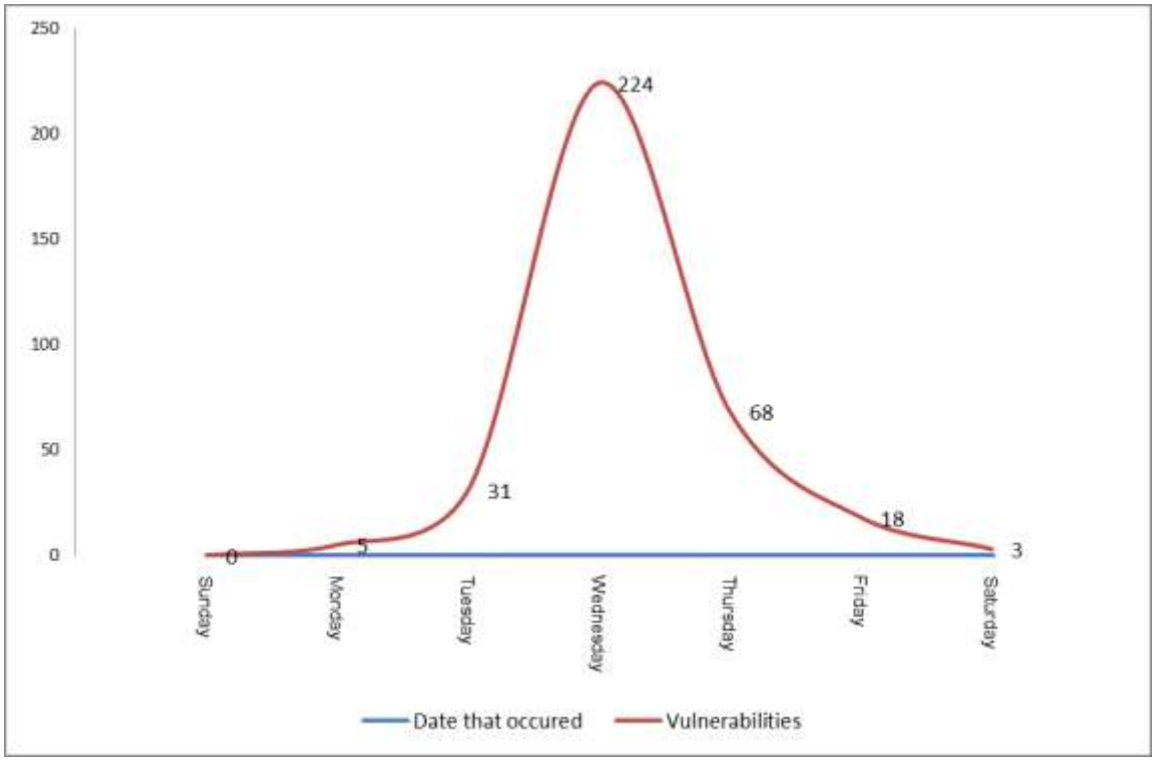
Διάγραμμα 2: Κατανομή ευπαθειών για το προϊόν Windows 2003 του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την NVD)

5.11.2 Κατανομή ευπαθειών για Windows Vista

Συνεχίζοντας την έρευνά μας, αναλύσαμε τη κατανομή ευπαθειών ενός προϊόντος του κατασκευαστή λογισμικού Microsoft, και συγκεκριμένα του Windows Vista. Το Διάγραμμα 3 και το Διάγραμμα 4, αποτυπώνουν την κατανομή αυτή. Βλέπουμε ότι πάλι είναι τύπου καμπάνας και ότι η κορύφωση της ανακοίνωσης των ευπαθειών συμβαίνει την Τετάρτη. Επίσης, μπορούμε να δούμε ότι ο αριθμός αυτός περίπου αγγίζει τις 481 σύμφωνα με την OSVDB και 224 σύμφωνα με την NVD, ευπάθειες. Τα διαγράμματα για το προϊόν αυτό, επίσης αποτυπώνουν ξεκάθαρα το χρονικό πρότυπο που αναζητούσαμε.



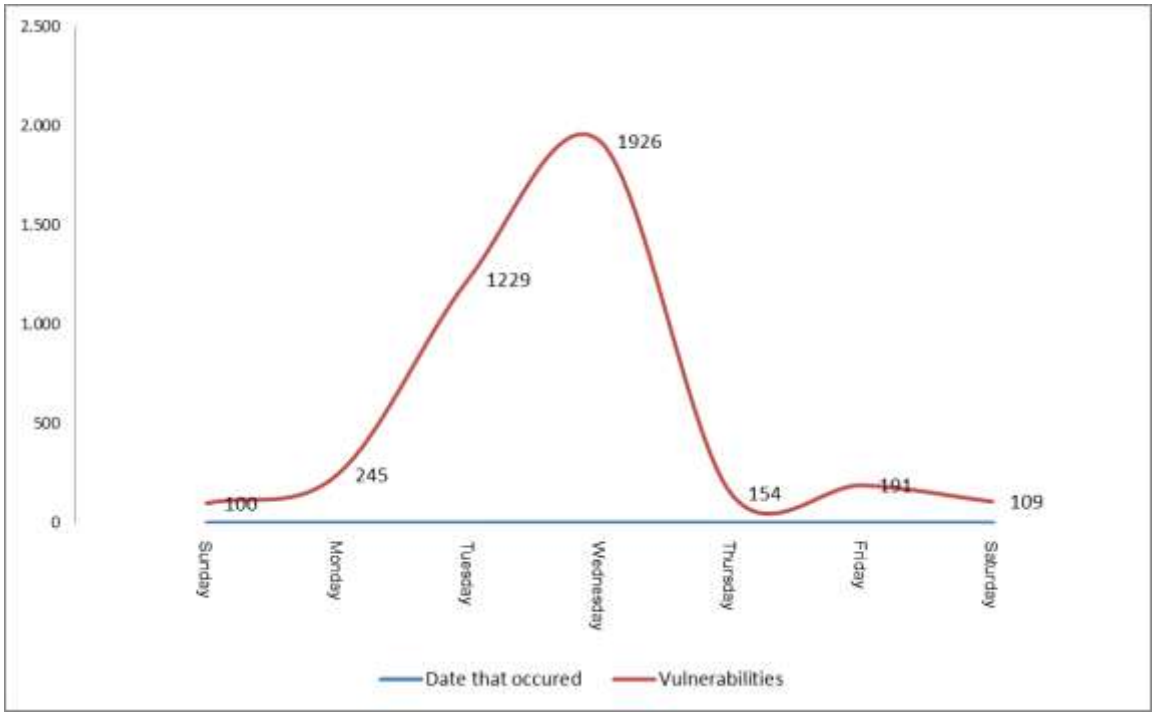
Διάγραμμα 3: Κατανομή ευπαθειών για το προϊόν Windows Vista του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την OSVBD)



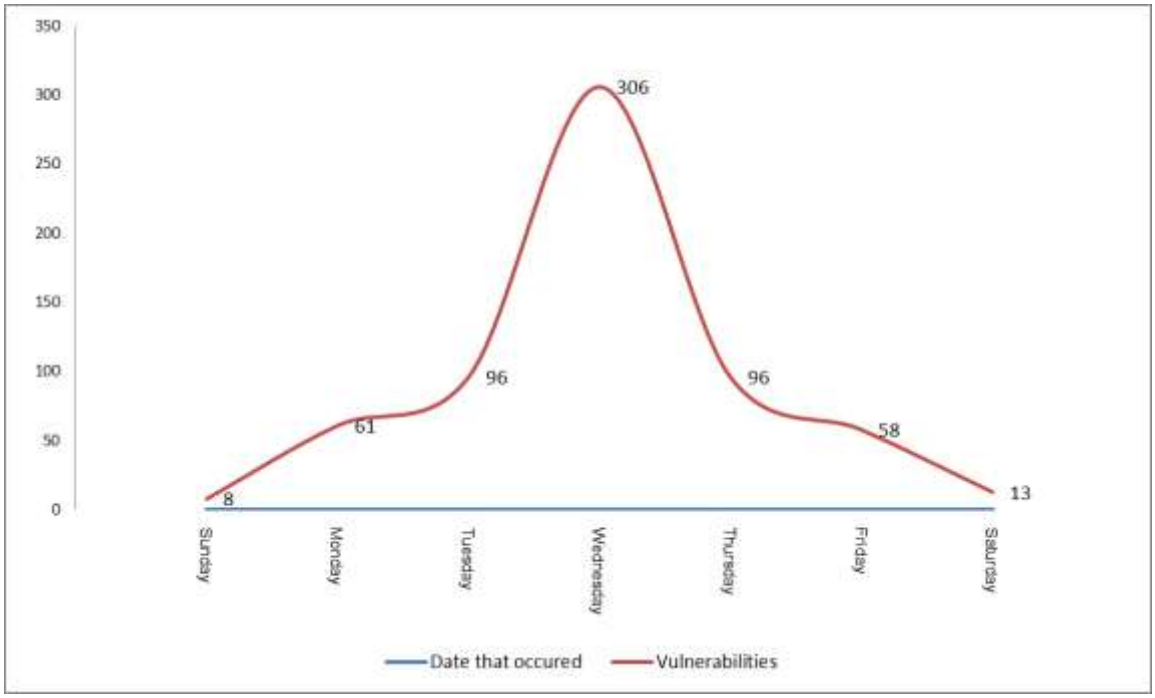
Διάγραμμα 4: Κατανομή ευπαθειών για το προϊόν Windows Vista του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την NVD)

5.11.3 Κατανομή ευπαθειών για Windows XP

Συνεχίζοντας την έρευνά μας, αναλύσαμε τη κατανομή ευπαθειών ενός προϊόντος του κατασκευαστή λογισμικού Microsoft, και συγκεκριμένα για τα Windows XP. Το Διάγραμμα 5 και Διάγραμμα 6 αποτυπώνουν την κατανομή αυτή. Βλέπουμε ότι πάλι είναι τύπου καμπάνας και ότι η κορύφωση της ανακοίνωσης των ευπαθειών συμβαίνει την Τετάρτη. Επίσης, μπορούμε να δούμε ότι ο αριθμός αυτός περίπου αγγίζει τις 1.926 σύμφωνα με την OSVDB και 306 σύμφωνα με την NVD, ευπάθειες. Για μία ακόμη φορά τα διαγράμματα για το προϊόν αυτό αποτυπώνουν ξεκάθαρα το χρονικό πρότυπο που αναζητούσαμε.



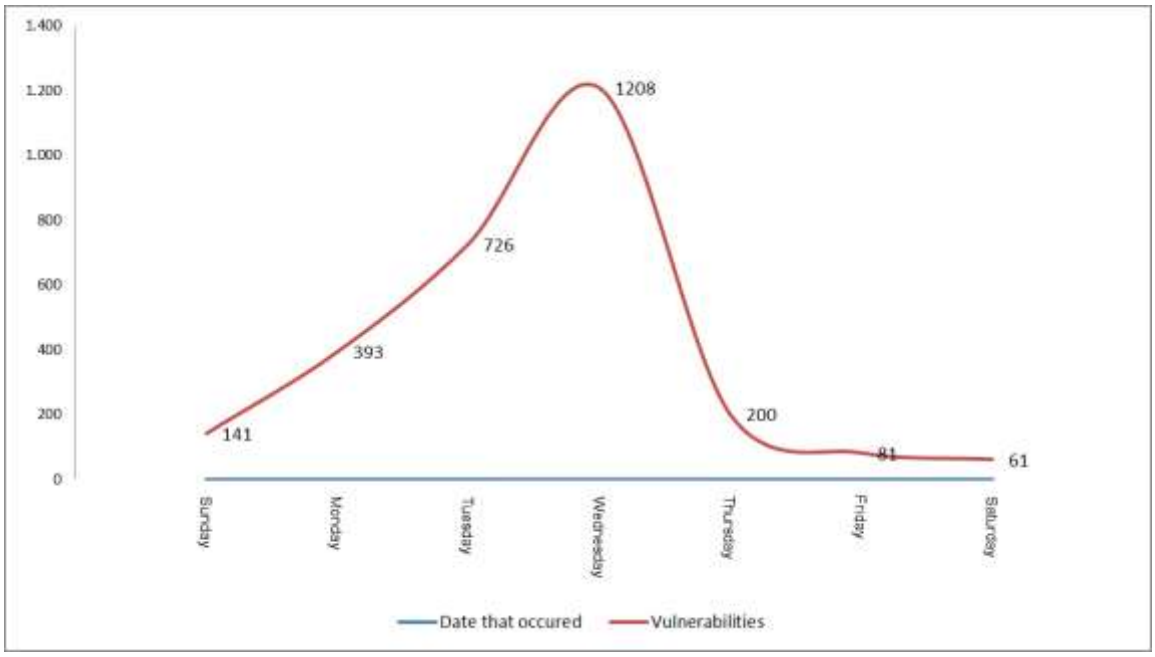
Διάγραμμα 5: Κατανομή ευπαθειών για το προϊόν Windows XP του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την OSVDB)



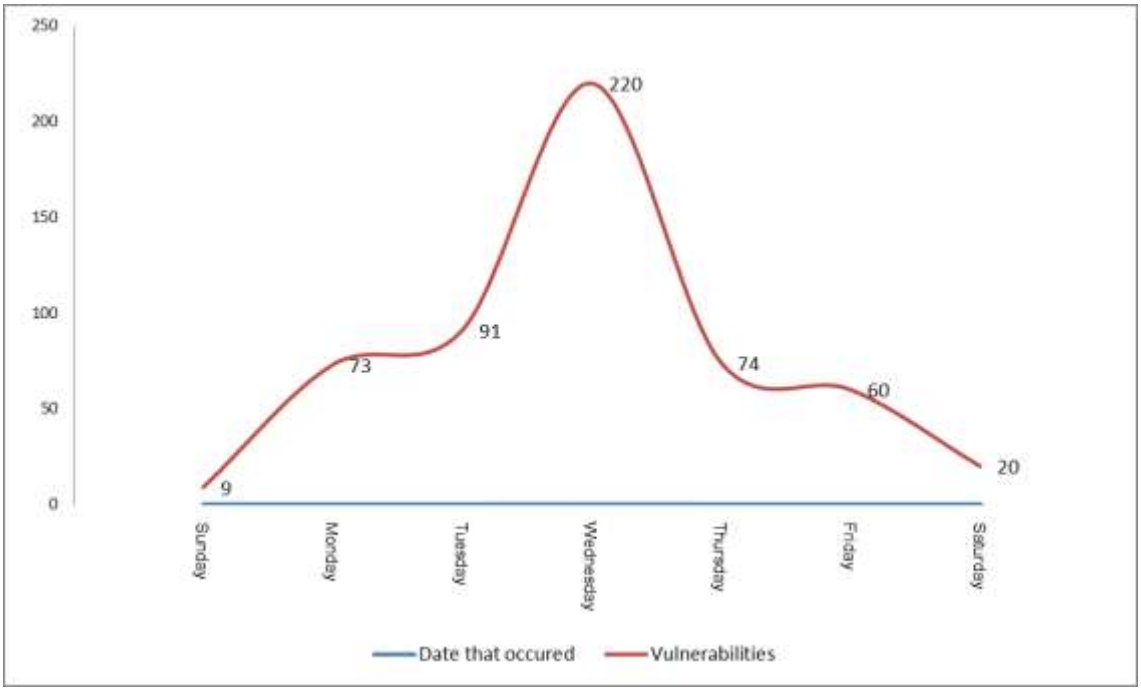
Διάγραμμα 6: Κατανομή ευπαθειών για το προϊόν Windows XP του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την NVD)

5.11.4 Κατανομή ευπαθειών για Windows 2000

Συνεχίζοντας την έρευνά μας, αναλύσαμε τη κατανομή ευπαθειών ενός προϊόντος του κατασκευαστή λογισμικού Microsoft, και συγκεκριμένα για τα Windows 2000. Έτσι λοιπόν το Διάγραμμα 7 και Διάγραμμα 8, αποτυπώνουν την κατανομή αυτή. Βλέπουμε ότι πάλι είναι τύπου καμπάνας και ότι η κορύφωση της ανακοίνωσης των ευπαθειών συμβαίνει περίπου την Τετάρτη. Επίσης, μπορούμε να δούμε ότι ο αριθμός αυτός περίπου αγγίζει τις 1.208 σύμφωνα με την OSVDB και 220 σύμφωνα με την NVD, ευπάθειες. Για μία ακόμη φορά, τα διαγράμματα για το προϊόν αυτό, αποτυπώνουν ξεκάθαρα το χρονικό πρότυπο που αναζητούσαμε.



Διάγραμμα 7: Κατανομή ευπαθειών για το προϊόν Windows 2000 του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την OSVDB)

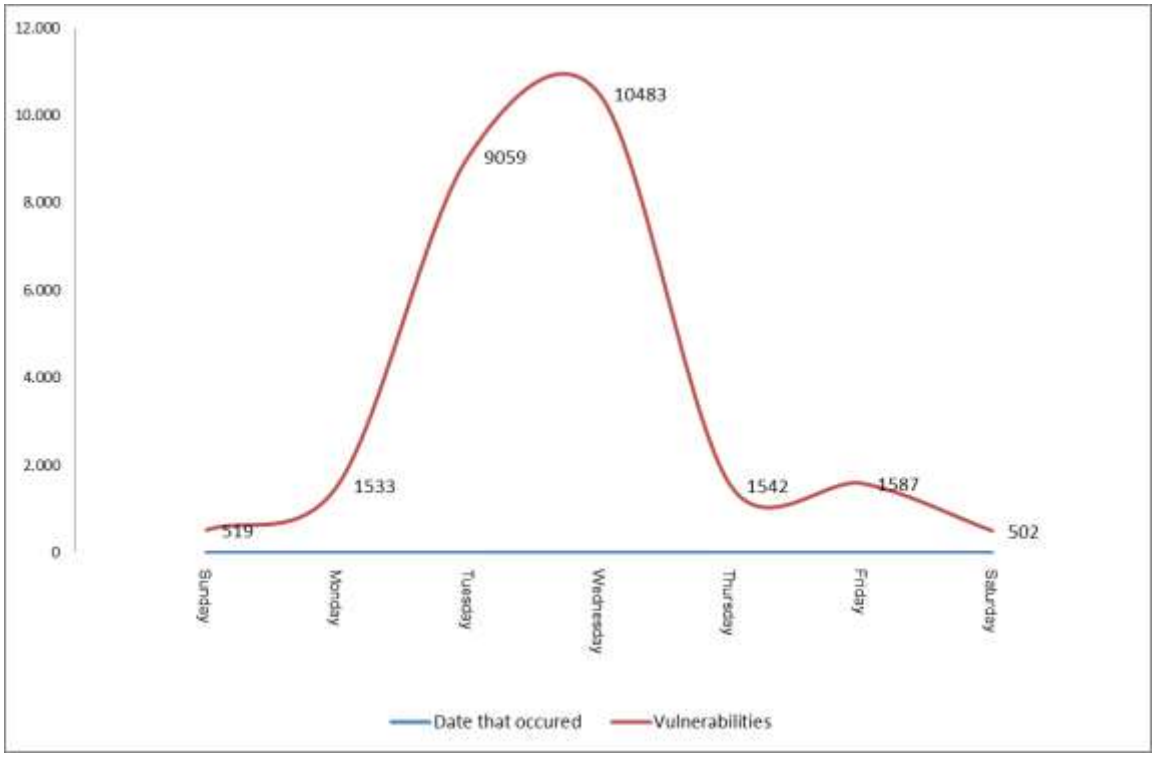


Διάγραμμα 8: Κατανομή ευπαθειών για το προϊόν Windows 2000 του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την NVD)

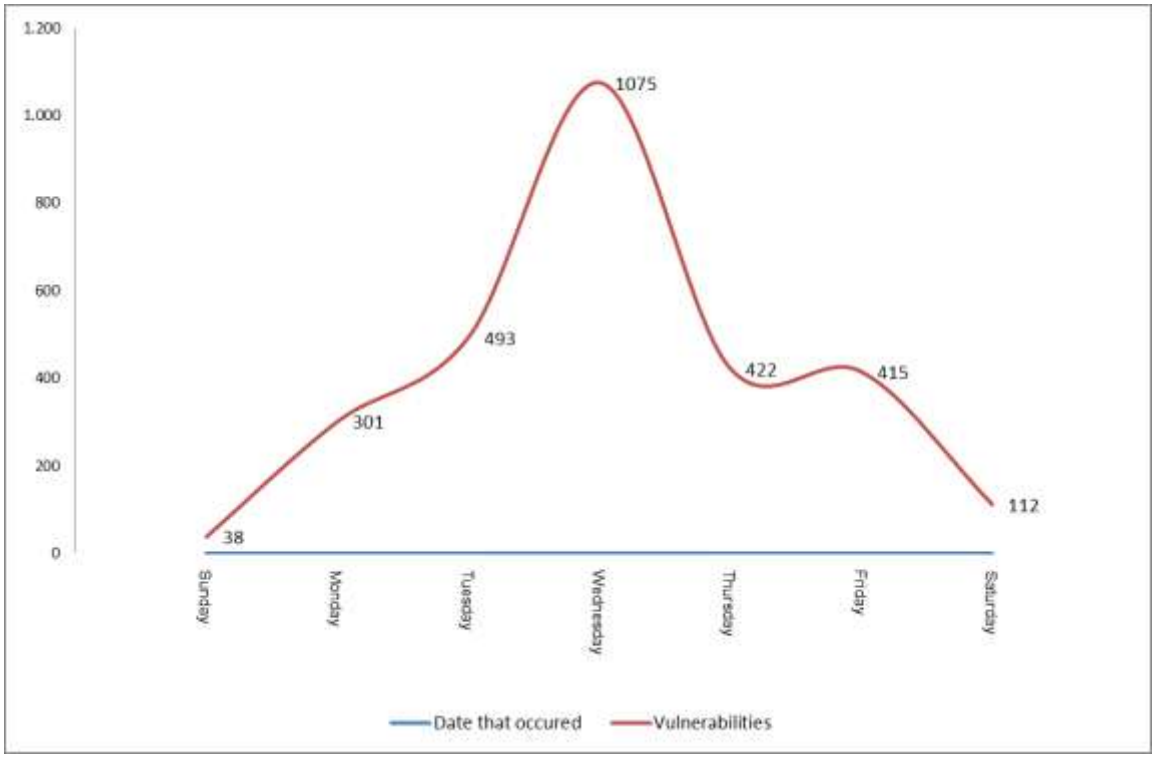
5.11.5 Κατανομή ευπαθειών για τον κατασκευαστή λογισμικού Microsoft

Έχοντας ήδη μελετήσει και αποτυπώσει, τις κατανομές ευπαθειών για τέσσερα (4) από τα πιο γνωστά προϊόντα της κατασκευάστριας εταιρείας, αποφασίσαμε να επεκτείνουμε την έρευνά μας. Έτσι, μελετήσαμε την κατανομή για τις ευπάθειες που έχουν να κάνουν με την κατασκευάστρια εταιρεία λογισμικού Microsoft, συνολικά, αγνοώντας το προϊόν. Προσπαθήσαμε, να τις κατανείμουμε για μία ακόμη φορά σε ημέρες της εβδομάδας και τις αποτυπώσαμε στο Διάγραμμα 9 και Διάγραμμα 10.

Τα διαγράμματα αυτά, είναι τύπου καμπάνας και βλέπουμε ότι η κορύφωση της ανακοίνωσης των ευπαθειών συμβαίνει περίπου την Τετάρτη. Επίσης, μπορούμε να δούμε ότι ο αριθμός αυτός περίπου αγγίζει τις 10.483 σύμφωνα με την OSVDB και 1.075 σύμφωνα με την NVD, ευπάθειες. Για μία ακόμη φορά, τα διαγράμματα για το προϊόν αυτό, αποτυπώνουν ξεκάθαρα το χρονικό πρότυπο που αναζητούσαμε. Συνεπώς, τα προϊόντα της κατασκευάστριας εταιρείας Microsoft ως σύνολο, είναι περισσότερο επιρρεπή γύρω στην Τετάρτη, και για αυτό υπάρχει και ορός «Exploit Wednesday» [97], [98].



Διάγραμμα 9: Κατανομή ευπαθειών του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την OSVDB)



Διάγραμμα 10: Κατανομή ευπαθειών του κατασκευαστή λογισμικού Microsoft, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την NVD)

5.12 Πολιτική διορθωτικών πακέτων λογισμικού της Microsoft

Όπως αναφέρθηκε στην παράγραφο § 5.11, η μελέτη των ευπαθειών που έβλαψαν τα συστήματα πληροφορικής τα προηγούμενα χρόνια μας αποκάλυψε χρήσιμες πληροφορίες. Μία από αυτές, είναι και η πολιτική που ακολουθούν οι κατασκευάστριες εταιρείες λογισμικού, αναφορικά με τη δημιουργία και αποστολή διορθωτικών πακέτων λογισμικού.

Στην περίπτωση της κατασκευάστριας εταιρείας λογισμικού Microsoft, επαληθεύτηκε, ο όρος που ήταν γνωστός για χρόνια, «Patch Tuesday». Ο όρος αυτός, υποδήλωνε ότι κάθε Τρίτη η εταιρεία έβγαζε σε κυκλοφορία για την κοινότητα των χρηστών, διορθωτικά πακέτα λογισμικού. Αυτό ήταν ιδιαίτερα γνωστό, στην κοινότητα των διαχειριστών των διαφόρων εξυπηρετητών που χρησιμοποιούσαν προϊόντα της Microsoft.

5.12.1 Windows Update Tool

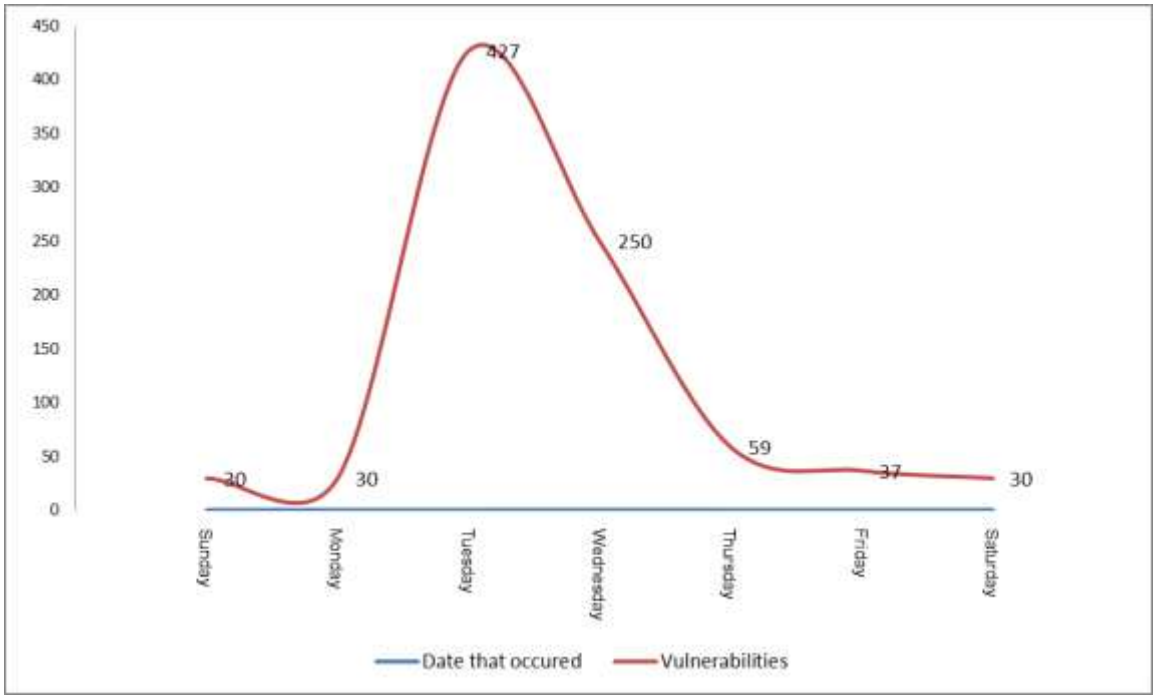
Σύμφωνα λοιπόν με την πολιτική της Microsoft, κάθε δεύτερη Τρίτη του μήνα, η εταιρεία έδινε προς χρήση τα διορθωτικά πακέτα λογισμικού για τα προϊόντα της και τις διάφορες εκδόσεις τους. Από την αρχή του προϊόντος «Windows 98», μέχρι και σήμερα, ένα νέο εργαλείο συμπεριλαμβάνονταν σε κάθε λειτουργικό σύστημα της Microsoft, το «Windows Update». Κάθε ένα σύστημα, που είχε το συγκεκριμένο εργαλείο ενεργοποιημένο έλεγχε αυτόματα το διαδικτυακό τόπο της εταιρείας, για να βρει εάν υπήρχαν καινούργια διορθωτικά πακέτα λογισμικού. Σε περίπτωση που υπήρχαν, τα κατέβαζε αυτόματα στο σύστημα και τα εγκαθιστούσε. Φυσικά, με την ίδια διαδικασία, το συγκεκριμένο εργαλείο, έλεγχε και εγκαθιστούσε, διορθώσεις για όλα τα εγκατεστημένα, στο εκάστοτε σύστημα, προϊόντα της Microsoft, όπως SQL Server, Microsoft Office ή ακόμα και εργαλεία ανάπτυξης σαν το Visual Studio.

Φυσικά, αυτό που επαληθεύσαμε με τα προηγούμενα διαγράμματα, αποτελεί μία λογική εξήγηση, για την κορύφωση της ύπαρξης ευπαθειών σε συγκεκριμένη ημέρα της εβδομάδας. Παρόλα αυτά όμως, το πρόβλημα παραμένει. Η συγκεκρι-

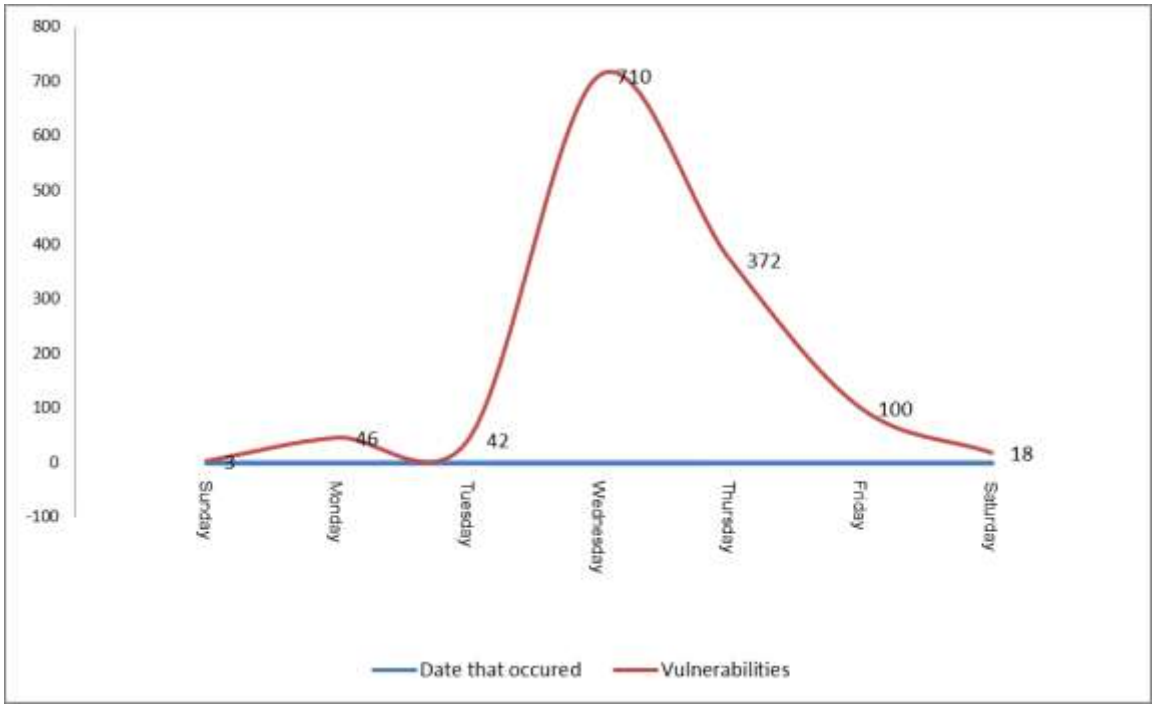
μένη εταιρεία, είναι περισσότερο ευάλωτη σε επιθέσεις ασφαλείας τη Τετάρτη, ακριβώς για τον ίδιο λόγο, δηλαδή της μη εγκατάστασης των διορθωτικών πακέτων.

5.13 Πολιτική διορθωτικών πακέτων λογισμικού της Oracle

Συνεχίζοντας την έρευνα στις βάσεις δεδομένων OSVB και NVD, ανακαλύψαμε ότι δεν είναι μόνο η κατασκευάστρια εταιρεία λογισμικού Microsoft που επιδεικνύει αυτή τη συμπεριφορά, αναφορικά με τις ευπάθειες. Στο Διάγραμμα 11 και στο Διάγραμμα 12, αποτυπώνεται ένα από τα πιο γνωστά και ευρέως χρησιμοποιούμενα προϊόντα της κατασκευάστριας εταιρείας λογισμικού Oracle, το Oracle Database 10g. Όπως και πριν, και σε αυτήν την περίπτωση έχουμε δύο διαγράμματα τύπου καμπάνας, τα οποία αποτυπώνουν τον αριθμό των ευπαθειών ανά ημέρα της εβδομάδας, με μέγιστο αριθμό ευπαθειών, 427 σύμφωνα με την OSVDB και 710 σύμφωνα με την NVD. Η μοναδική διαφορά που υπάρχει, είναι ότι η ημέρα της κορύφωσης της καμπύλης αλλάζει και είναι πλέον η Τρίτη σύμφωνα με την OSVDB και παραμένει Τετάρτη σύμφωνα με την NVD.



Διάγραμμα 11: Κατανομή ευπαθειών για το προϊόν Oracle Database 10g, του κατασκευαστή λογισμικού Oracle, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την OSVDB)



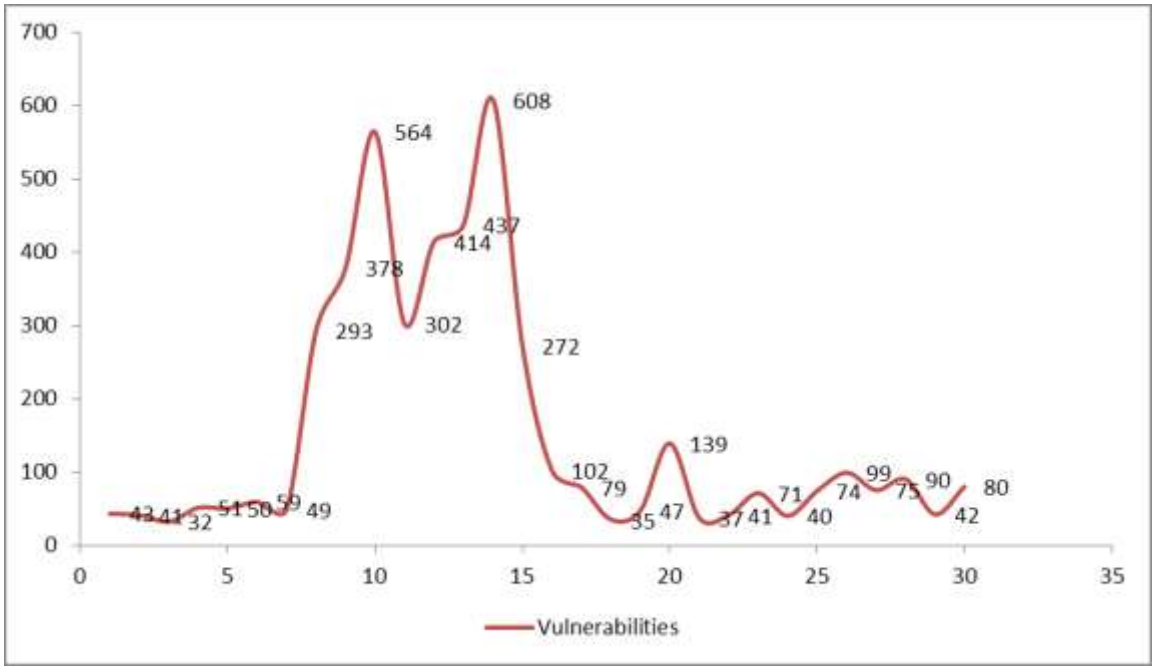
Διάγραμμα 12: Κατανομή ευπαθειών για το προϊόν Oracle Database 10g, του κατασκευαστή λογισμικού Oracle, ανά ημέρα της εβδομάδας (Τα στοιχεία προέρχονται από την NVD)

5.14 Μηνιαίες κατανομές ευπαθειών

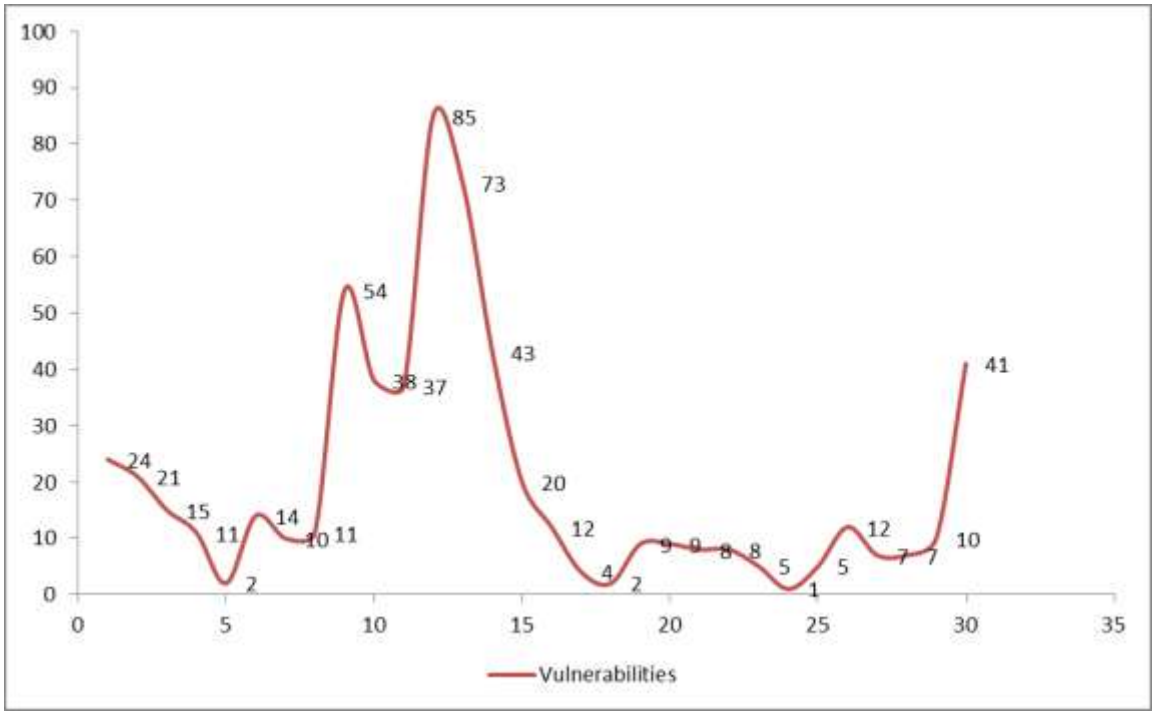
Στην παρούσα έρευνα, έγινε προσπάθεια περαιτέρω κατανόησης της κατανομής των ευπαθειών, και για αυτό το λόγο, μελετήσαμε τις ευπάθειες προϊόντων κατά τη διάρκεια ενός μήνα. Αυτό που κάναμε, ήταν να αθροίσουμε όλες τις ευπάθειες ενός προϊόντος από τα διαθέσιμα στοιχεία των βάσεων δεδομένων OSVDB και NVD, σύμφωνα με την ημερολογιακή ημέρα ανακοίνωσης της ευπάθειας και να τις προβάλουμε σε ένα παρόμοιο, με τα παραπάνω, διάγραμμα.

5.14.1 Μηνιαία κατανομή ευπαθειών του προϊόντος λογισμικού, «Windows XP»

Στο Διάγραμμα 13 και Διάγραμμα 14, αποτυπώνεται η μηνιαία κατανομή των ευπαθειών του προϊόντος «Windows XP», της κατασκευάστριας εταιρείας λογισμικού Microsoft. Αυτό που φαίνεται καθαρά από τα διαγράμματα, είναι ότι ο αριθμός των ευπαθειών κορυφώνεται κάποια στιγμή του μήνα και εν συνεχεία, φθίνει απότομα.



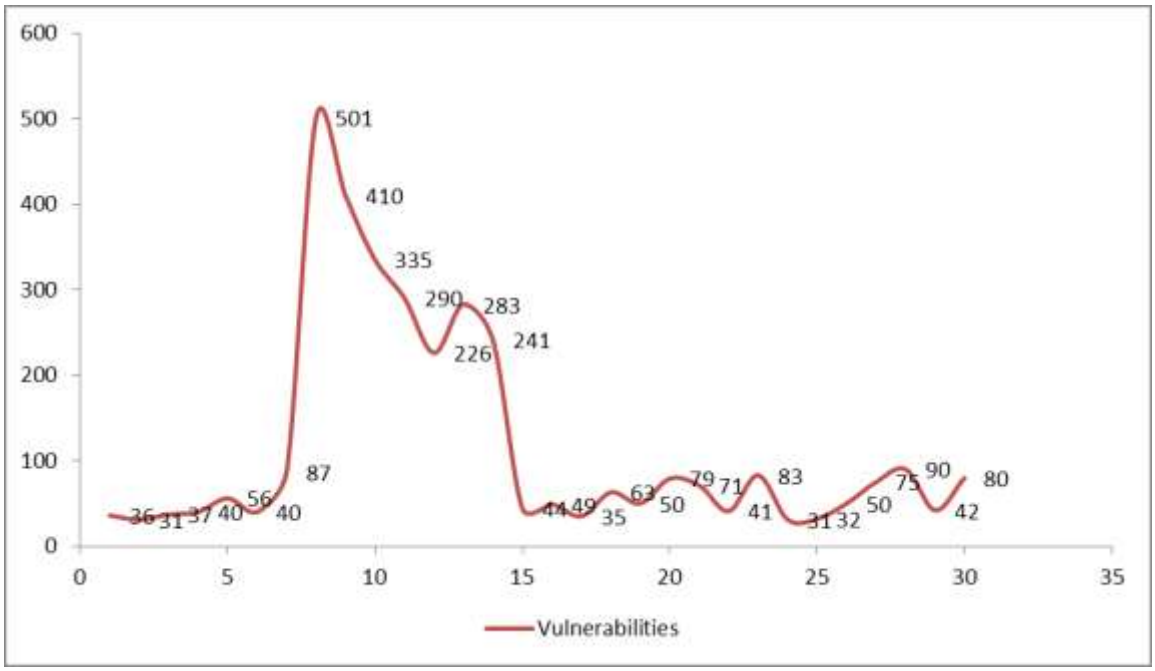
Διάγραμμα 13: Μηνιαία κατανομή ευπαθειών για το προϊόν Windows XP, του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την OSVDB)



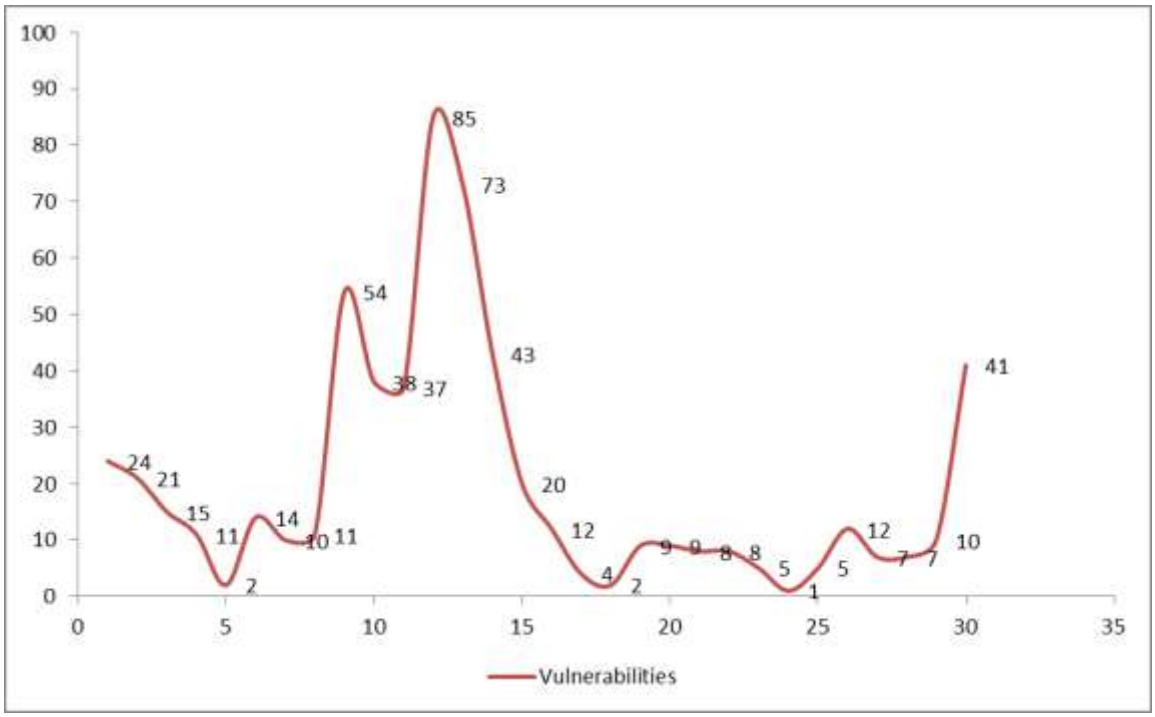
Διάγραμμα 14: Μηνιαία κατανομή ευπαθειών για το προϊόν Windows XP, του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την NVD)

5.14.2 Μηνιαία κατανομή ευπαθειών του προϊόντος λογισμικού, «Windows 2003»

Στο Διάγραμμα 15 και Διάγραμμα 16, αποτυπώνεται η μηνιαία κατανομή των ευπαθειών του προϊόντος «Windows 2003», της κατασκευάστριας εταιρείας λογισμικού Microsoft. Αυτό που επίσης φαίνεται καθαρά από τα διαγράμματα, είναι ότι ο αριθμός των ευπαθειών κορυφώνεται κάποια στιγμή του μήνα και εν συνεχεία, φθίνει απότομα.



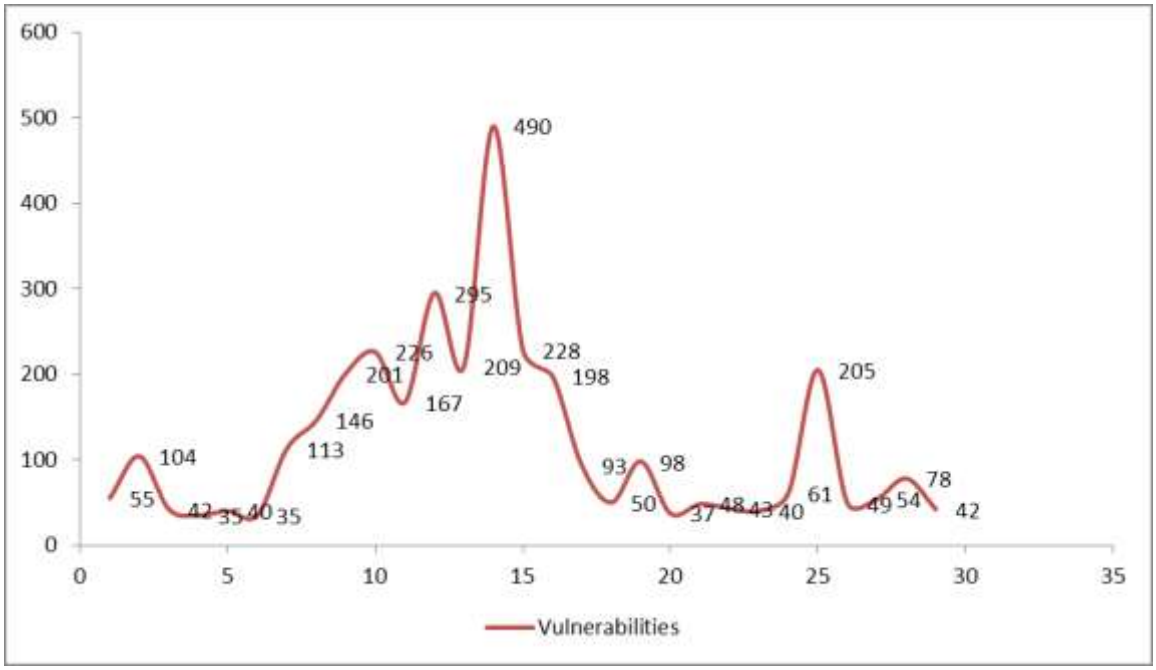
Διάγραμμα 15: Μηνιαία κατανομή ευπαθειών για το προϊόν Windows 2003, του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την OSVDB)



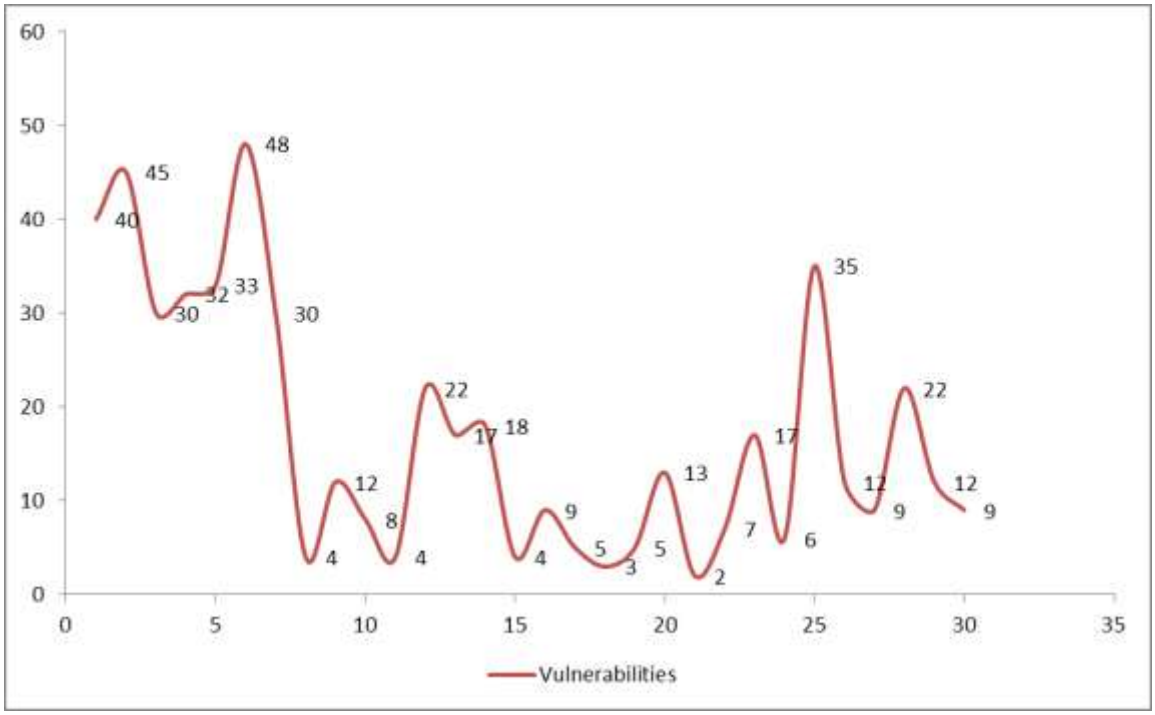
Διάγραμμα 16: Μηνιαία κατανομή ευπαθειών για το προϊόν Windows 2003, του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την NVD)

5.14.3 Μηνιαία κατανομή ευπαθειών του προϊόντος λογισμικού, «Windows 2000»

Στο Διάγραμμα 17 και Διάγραμμα 18, αποτυπώνεται η μηνιαία κατανομή των ευπαθειών του προϊόντος «Windows 2000», της κατασκευάστριας εταιρείας λογισμικού Microsoft. Για άλλη μία φορά, αυτό που φαίνεται καθαρά από τα διαγράμματα, είναι ότι ο αριθμός των ευπαθειών κορυφώνεται κάποια στιγμή του μήνα και εν συνεχεία, φθίνει απότομα.



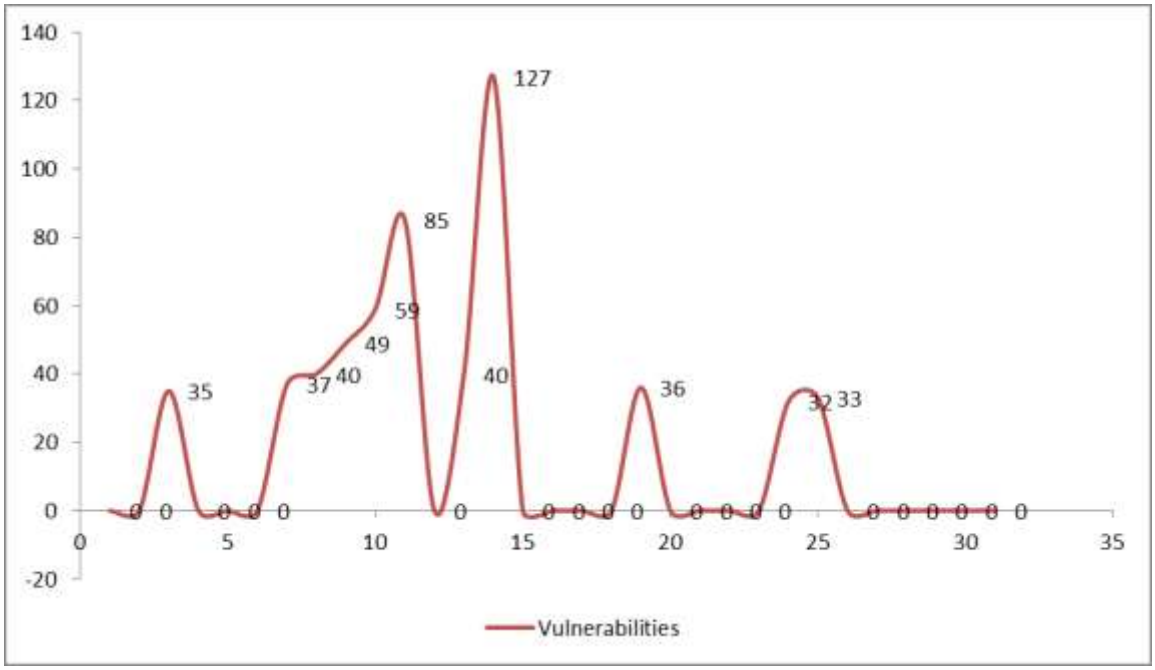
Διάγραμμα 17: Μηνιαία κατανομή ευπαθειών για το προϊόν Windows 2000, του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την OSVDB)



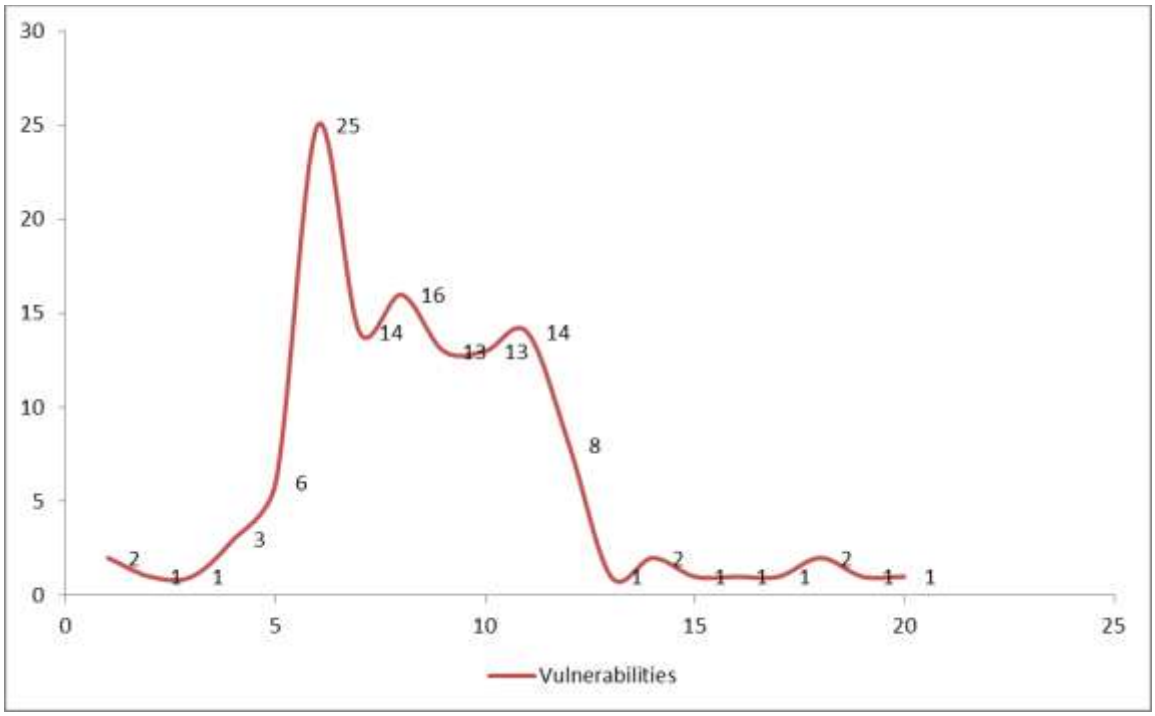
Διάγραμμα 18: Μηνιαία κατανομή ευπαθειών για το προϊόν Windows 2000, του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την NVD)

5.14.4 Μηνιαία κατανομή ευπαθειών του προϊόντος λογισμικού, «Office XP»

Στο Διάγραμμα 19 και Διάγραμμα 20, αποτυπώνεται η μηνιαία κατανομή των ευπαθειών του προϊόντος «Office XP», της κατασκευάστριας εταιρείας λογισμικού Microsoft. Για άλλη μία φορά, αυτό που φαίνεται καθαρά από τα διαγράμματα, είναι ότι ο αριθμός των ευπαθειών κορυφώνεται κάποια στιγμή του μήνα και εν συνεχεία, φθίνει απότομα.



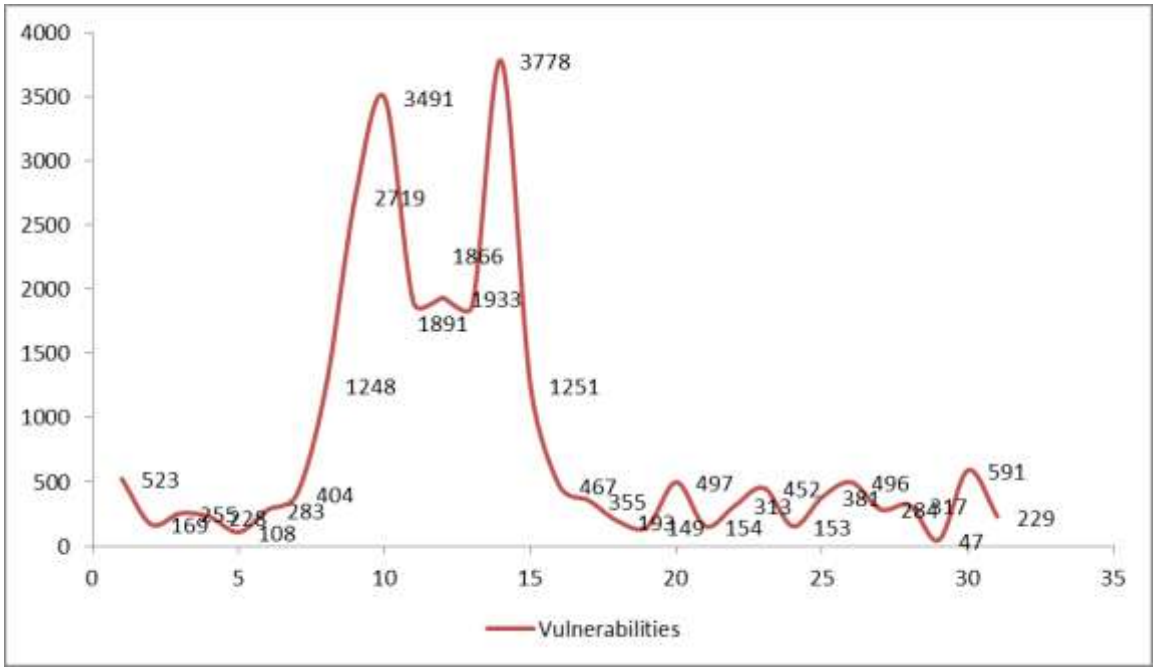
Διάγραμμα 19: Μηνιαία κατανομή ευπαθειών για το προϊόν Office XP, του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την OSVDB)



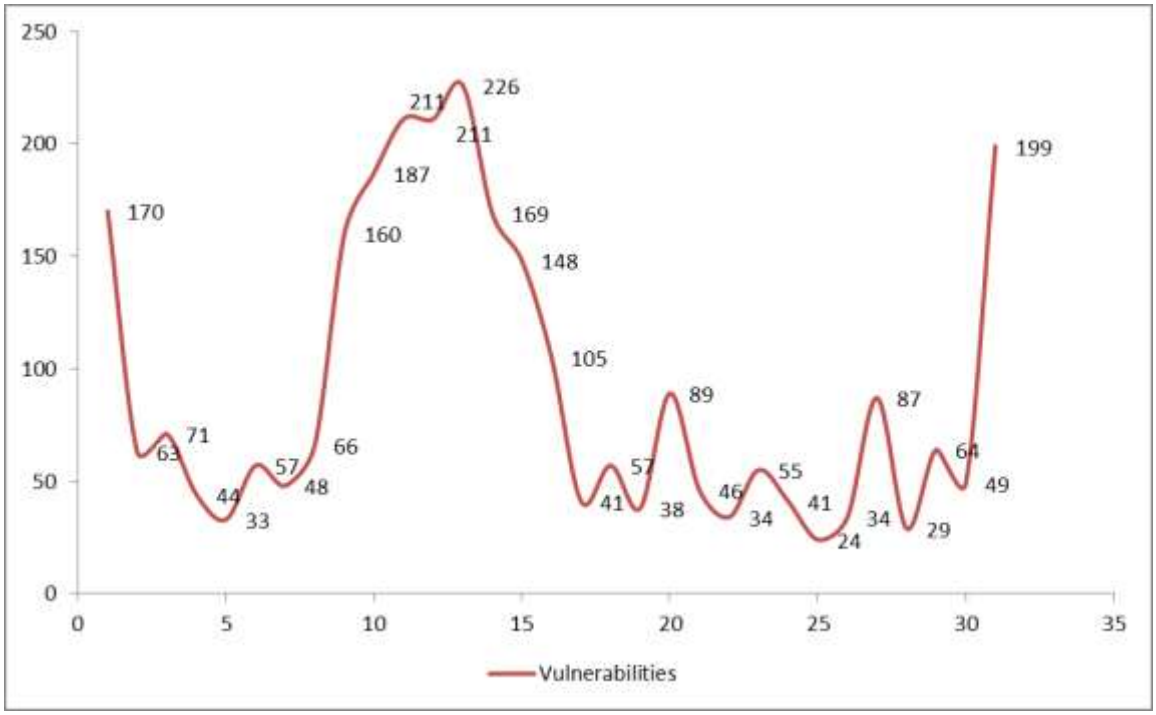
Διάγραμμα 20: Μηνιαία κατανομή ευπαθειών για το προϊόν Office XP, του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την NVD)

5.14.5 Μηνιαία κατανομή ευπαθειών της κατασκευάστρια εταιρείας λογισμικού, Microsoft

Στο Διάγραμμα 21 και Διάγραμμα 22, αποτυπώνεται η μηνιαία κατανομή των ευπαθειών της κατασκευάστριας εταιρείας λογισμικού, Microsoft. Για άλλη μία φορά, αυτό που φαίνεται καθαρά από τα διαγράμματα, είναι ότι ο αριθμός των ευπαθειών κορυφώνεται γύρω στις 15 του μήνα και εν συνεχεία, φθίνει απότομα.



Διάγραμμα 21: Μηνιαία κατανομή ευπαθειών του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την OSVDB)



Διάγραμμα 22: Μηνιαία κατανομή ευπαθειών του κατασκευαστή λογισμικού Microsoft (Τα στοιχεία προέρχονται από την NVD)

Από την έρευνα αυτή, είναι φανερό ότι μπορεί η διοίκηση μιας εταιρείας ή ενός οργανισμού να ωφεληθεί. Μελετώντας με προσοχή τα παραπάνω διαγράμματα, μπορεί κάποιος να αντλήσει χρήσιμες πληροφορίες και να κατανέμει καλύτερα τους πόρους που διαθέτει, έτσι ώστε να πετύχει τη μέγιστη δυνατή αποτελεσματικότητα, ενάντια στις επιθέσεις ασφαλείας που έχουν τη μεγαλύτερη πιθανότητα να συμβούν, στα μέσα του εκάστοτε μήνα.

5.15 Καθορισμός της στοχαστικής συνάρτησης

Η εμπειρική προσέγγιση της παρούσας έρευνας, έχει αναμφισβήτητα επιδείξει μέχρι τώρα, ότι διαφορετικές εταιρείες κατασκευής λογισμικού, επιδεικνύουν παρόμοια συμπεριφορά σχετικά με τις ευπάθειες και την κατανομή τους. Μελετώντας τα διαγράμματα που δείχνουν αυτή τη συμπεριφορά, μπορούμε να πούμε ότι αυτή αποτυπώνεται (ή προσεγγίζεται) από μία συνάρτηση Gauss, όπως φαίνεται στην ακόλουθη εξίσωση:

$$f(x) = ae^{-\frac{(x-b)^2}{2c^2}} \quad (\mathbf{10})$$

Όπου:	
a	Καθορίζει την κορύφωση του σχήματος της καμπάνας.
b	Καθορίζει τη θέση της κορύφωση του σχήματος της καμπάνας.
c	Καθορίζει το πλάτος του σχήματος της καμπάνας.

Έτσι λοιπόν, στην πλήρη ανάπτυξη το προτεινόμενο μοντέλο όπως αναφέρθηκε και στο [99], έχει την παρακάτω μορφή:

$$\sec\_status(t) = \int_0^t \prod_{i=1}^{k} f_i^{\frac{1}{c_i}}(t)\, dt \quad (\mathbf{11})$$

$$\text{όπου } f_i(t) = a_i e^{-\frac{(t-b_i)^2}{2c_i^2}} \quad (\mathbf{12})$$

$$\text{και } c_i = -\sum_{j=1}^{n}\sum_{k=1}^{m} t_{ik} e^{-k} w_j p_{ijk} \log\left(p_{ijk}\right) \quad (\mathbf{13})$$

Συνεπώς, αν ανατρέξουμε στις προτεινόμενες εξισώσεις υπολογισμού, εξίσωση 11, εξίσωση 12 καθώς και εξίσωση 13, για να ποσοτικοποιήσουμε το επίπεδο ασφάλειας ενός συστήματος πληροφορικής, αυτό που μένει να κάνουμε, είναι να προσεγγίσουμε τις παραμέτρους a, b, c για κάθε παράγοντα κινδύνου. Από τη στιγμή που θα το κάνουμε αυτό, μπορούμε να έχουμε μια αξιόπιστη, αλλά και αμερόληπτη μέτρηση του επιπέδου ασφάλειας του συστήματος πληροφορικής που μελετάμε.

Στην προσπάθειά μας, να προσεγγίσουμε τις παραμέτρους a, b, c για μία καμπύλη διαπιστώσαμε:

- Ότι δεν ήταν καθόλου εύκολη διαδικασία
- Ότι η δυσκολία που είχαμε στον προσδιορισμό των παραμέτρων, είχε το κίνδυνο να καταστήσει όλη τη μεθοδολογία μας δύσχρηστη και, συνεπώς, όχι πιθανά ευρέως αποδεκτή.

Για τους παραπάνω λόγους, αποφασίσαμε να χρησιμοποιήσουμε ένα από τα πιο αξιόπιστα μαθηματικά πακέτα που υπάρχουν στην αγορά λογισμικού, το MatLab R2012a, της εταιρείας MathWorks Inc. Ο σκοπός της χρησιμοποίησης του εν λόγω μαθηματικού πακέτου, ήταν η εύρεση εκείνης της μαθηματικής συνάρτησης, που θα προσέγγιζε καλύτερα την καμπύλη ανακοινώσεων των ευπαθειών, που είχαμε ήδη υπολογίσει.

Το MatLab R2012a, έχει ένα ειδικό εργαλείο, το «curve fitting tool», που μας δίνει αυτή ακριβώς τη δυνατότητα. Έτσι λοιπόν, χρησιμοποιήσαμε το εργαλείο και διαπιστώσαμε ότι η προσέγγιση κατά Fourier με οκτώ βαθμούς ελευθερίας, είχε τα καλύτερα αποτελέσματα. Ο πηγαίος κώδικας της εφαρμογής που δημιουργήθηκε στο MatLab R2012a, παρατίθεται στο Παράρτημα. Η μαθηματική εξίσωση της προσέγγισης αυτής, ακολουθεί:

$$f(x) = a_0 + \alpha_1 \cos(wx) + b_1 \sin(wx) + \alpha_2 \cos(2wx) + b_2 \sin(2wx) + \alpha_3 \cos(3wx) + b_3 \sin(3wx) + \alpha_4 \cos(4wx) + b_4 \sin(4wx) + \alpha_5 \cos(5wx) + b_5 \sin(5wx) + \alpha_6 \cos(6wx) + b_6 \sin(6wx) + \alpha_7 \cos(7x) + b_7 \sin(7wx) + \alpha_8 \cos(8wx) + b_8 \sin(8wx) \quad (11)$$

Όπου:	
a0, a1, a2, a3, a4, a5, a6, a7, a8, b0, b1, b2, b3, b4, b5, b6, b7, b8, w	Υπολογίζονται από το μαθηματικό πακέτο MatLab κατά τη διαδικασία της καλύτερης προσέγγισης της καμπύλης.

Τέλος υπολογίζουμε το στοχαστικό ολοκλήρωμα τύπου Itô:

$$\int_1^{31} \theta(t)dW(t) \ (\mathbf{12})$$

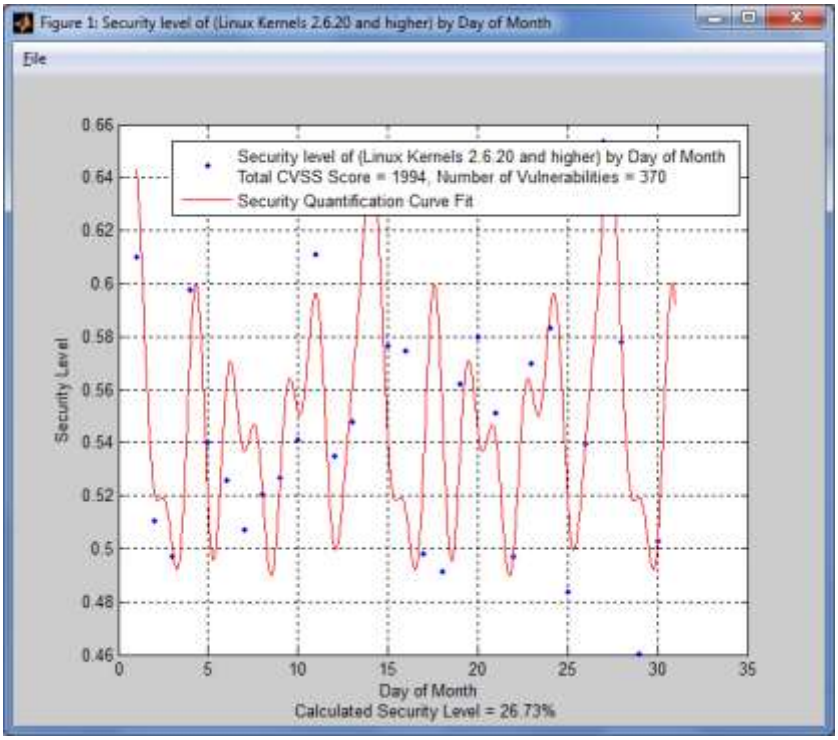
Όπου:	
Θ(t)	*Θέτουμε το* $\theta(t) = \frac{f(t)}{30}$

Ο μέσος όρος αυτού του στοχαστικού ολοκληρώματος, θα μας δώσει το ζητούμενο επίπεδο ασφάλειας του συστήματος πληροφορικής που μελετάμε.

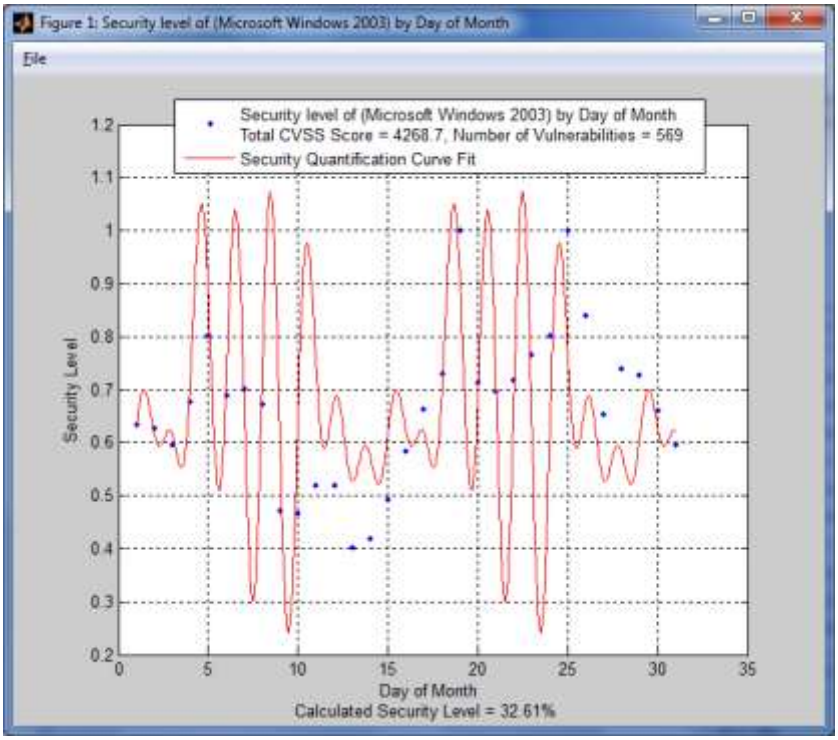
5.16 Εύρεση του επίπεδου ασφάλειας γνωστών προϊόντων

Χρησιμοποιώντας τη μεθοδολογία που περιγράψαμε και το μαθηματικό πακέτο MatLab, υπολογίσαμε το επίπεδο ασφαλείας κατά τη διάρκεια ενός μήνα, γνωστών προϊόντων και κατασκευαστών λογισμικού, των οποίων και παραθέτουμε τα σχετικά διαγράμματα που το αποτυπώνουν. Για να το πετύχουμε αυτό, αθροίσαμε όλες τις ευπάθειες από τη βάση δεδομένων NVD, και τις προβάλαμε στη διάρκεια ενός μήνα. Τα προϊόντα για τα οποία επιλέξαμε να βρούμε το επίπεδο ασφαλείας είναι:

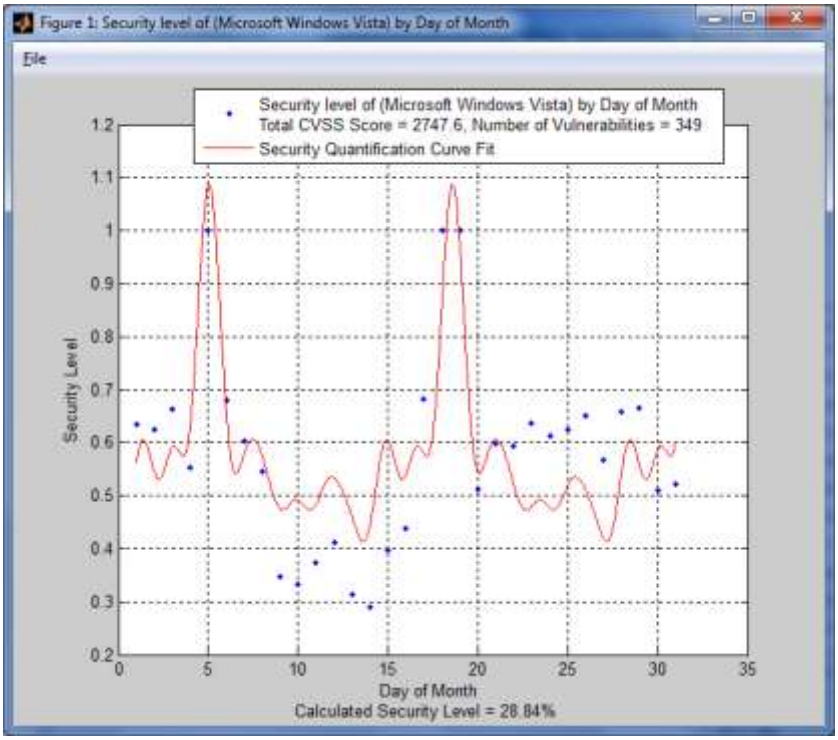
1. Λειτουργικό σύστημα Linux kernels 2.6.20 και μετά.
2. Λειτουργικό σύστημα Windows 2003.
3. Λειτουργικό σύστημα Windows Vista.
4. Λειτουργικό σύστημα Windows XP.
5. Λειτουργικό σύστημα Windows 2000.
6. Windows Office XP.
7. Βάση δεδομένων Microsoft SQL Server 2000.
8. Βάση δεδομένων Oracle 10g.
9. Web Server Microsoft IIS 7.
10. Web Server Apache 2.
11. Κατασκευαστής λογισμικού Microsoft.
12. Κατασκευαστής λογισμικού Oracle.



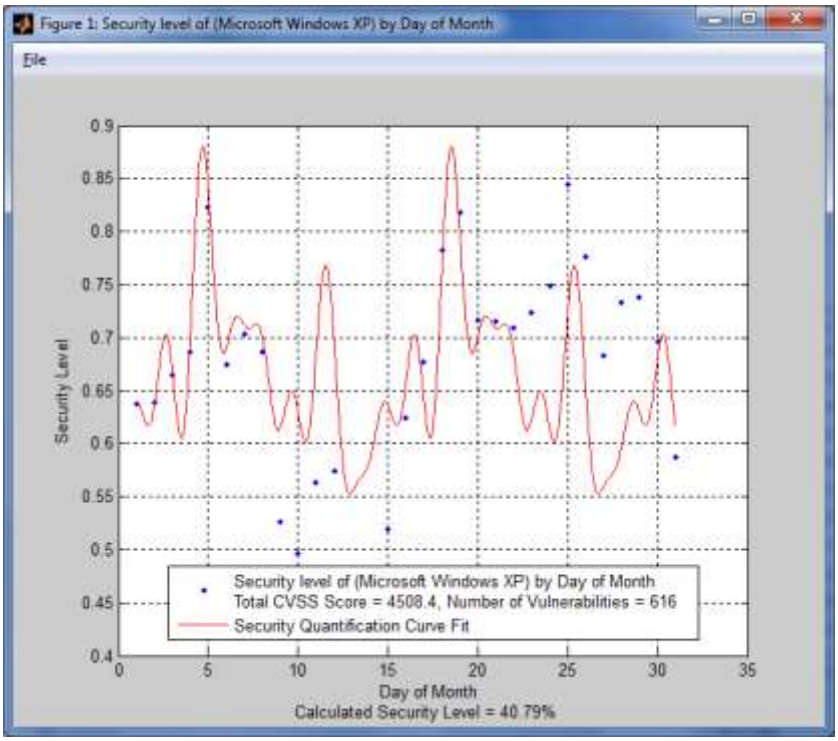
Διάγραμμα 23: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Linux kernels 2.6.20 και μετά



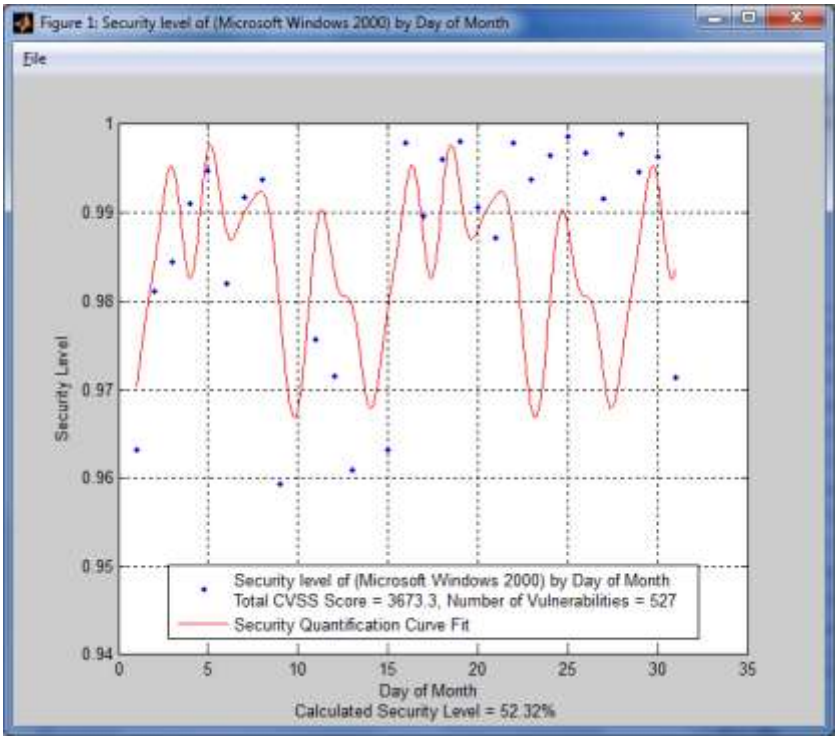
Διάγραμμα 24: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Microsoft Windows 2003



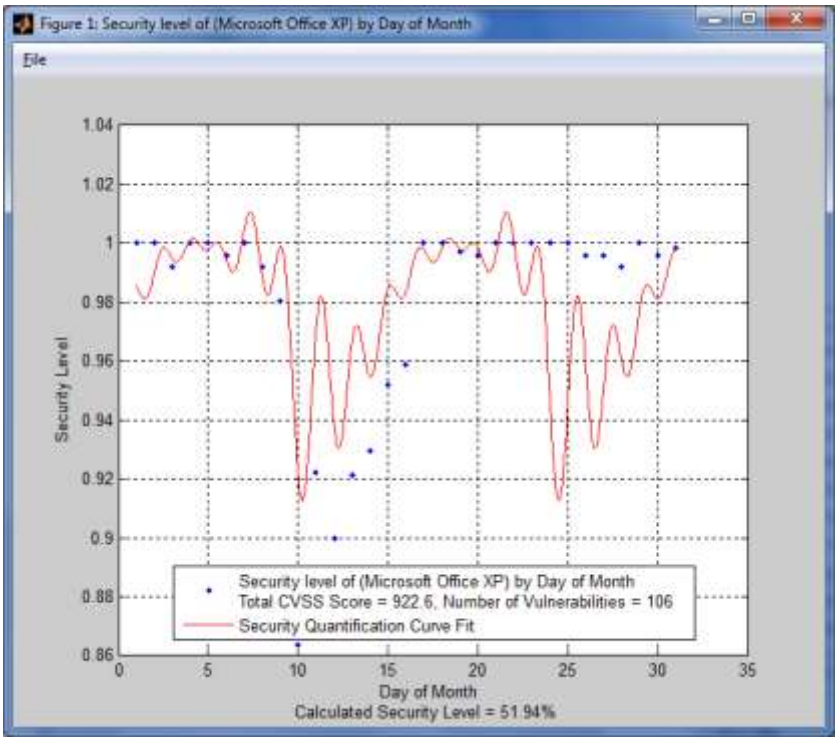
Διάγραμμα 25: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Microsoft Windows Vista



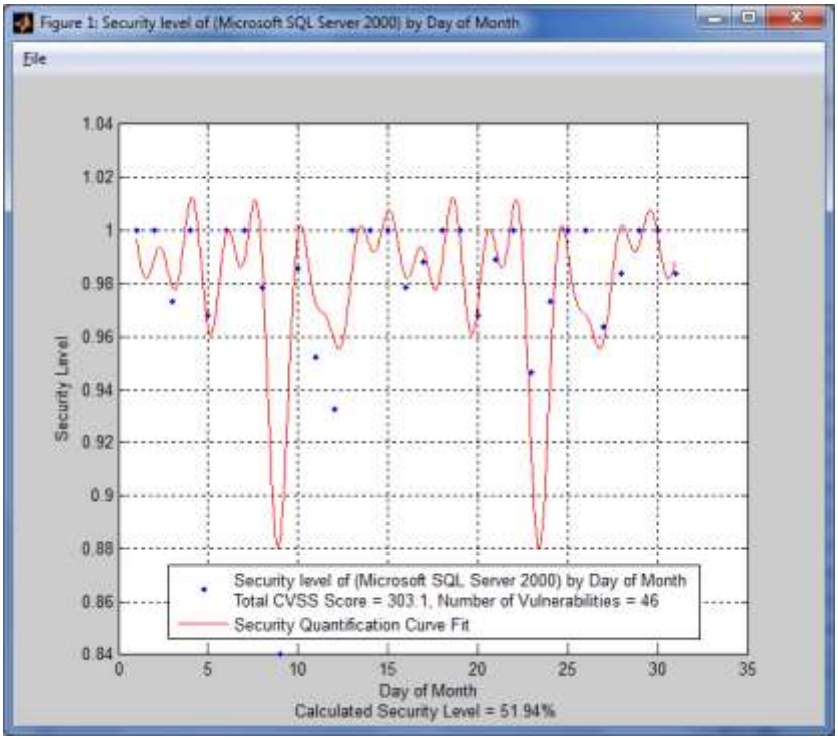
Διάγραμμα 26: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Microsoft Windows XP



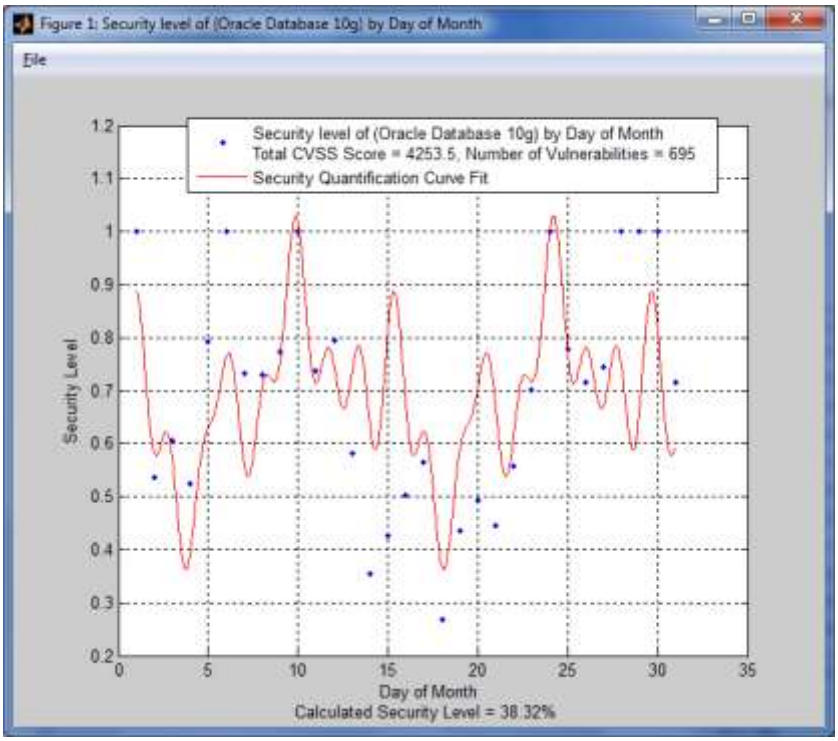
Διάγραμμα 27: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Microsoft Windows 2000



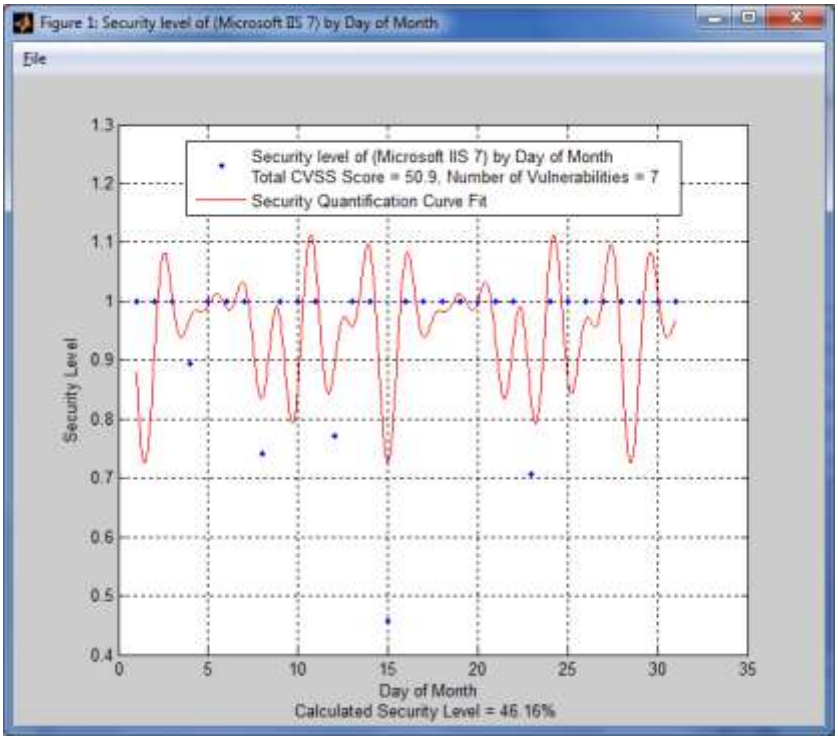
Διάγραμμα 28: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Windows Office XP



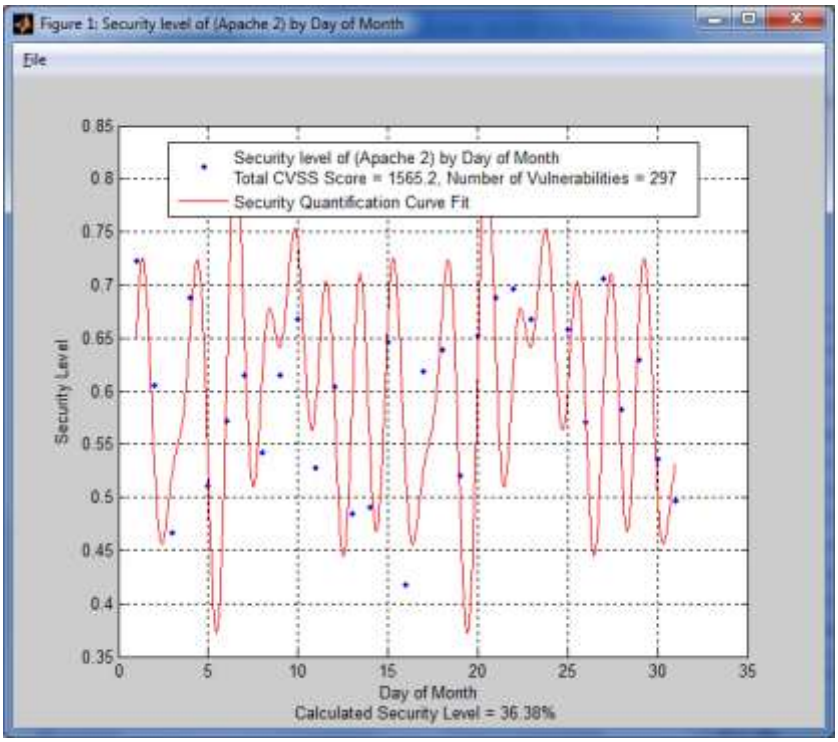
Διάγραμμα 29: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Microsoft SQL Server 2000



Διάγραμμα 30: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Oracle 10g

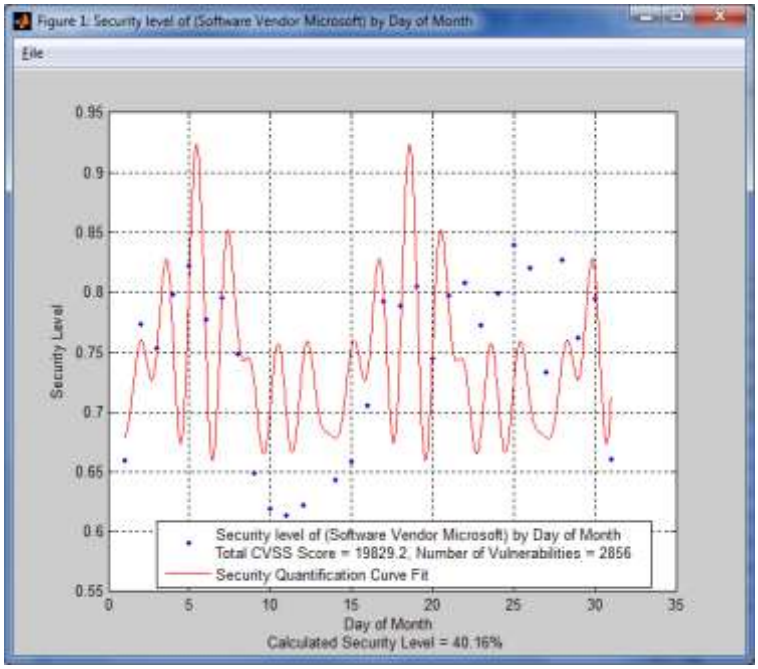


Διάγραμμα 31: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Microsoft IIS 7

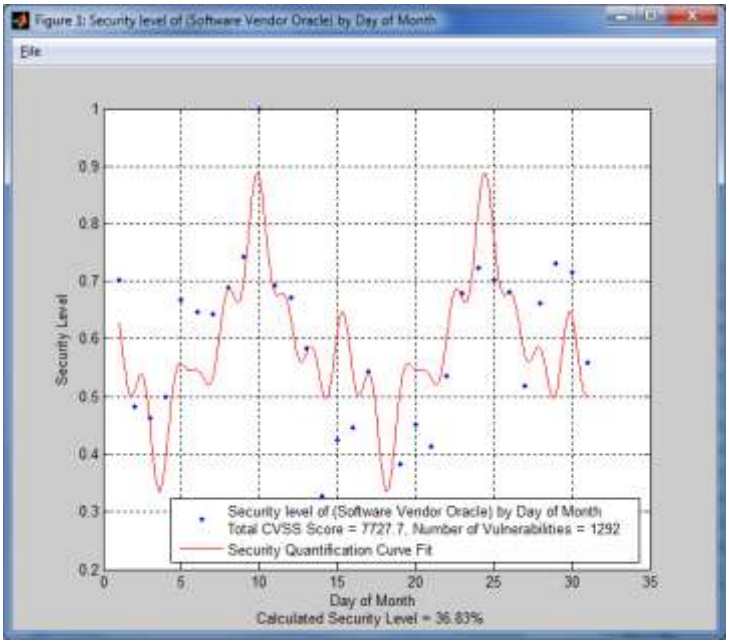


Διάγραμμα 32: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για το προϊόν Apache 2

Τέλος, υπολογίσαμε και παραθέτουμε το επίπεδο ασφάλειας των προϊόντων των κατασκευαστών λογισμικού Microsoft και Oracle. Τα διαγράμματα ακολουθούν:



Διάγραμμα 33: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για τον κατασκευαστή λογισμικού Microsoft



Διάγραμμα 34: Επίπεδο ασφαλείας κατά τη διάρκεια του μήνα, για τον κατασκευαστή λογισμικού Oracle

Από όλα τα παραπάνω διαγράμματα, επιβεβαιώνεται και εμπειρικά, ότι τόσο τα προϊόντα λογισμικού όσο και οι κατασκευαστές λογισμικού που μελετήθηκαν, εμφανίζουν ένα σημείο καμπής γύρω στα μέσα του μήνα, με συνέπεια τα προϊόντα τους και τα επέκταση, τα συστήματα πληροφορικής που βασίζονται σε αυτά, να είναι περισσότερο επιρρεπή σε επιθέσεις ασφαλείας.

5.17 Παράδειγμα σύγκρισης δύο συστημάτων πληροφορικής

Έχοντας αναλύσει το τεχνικό υπόβαθρο της έρευνάς μας, αυτό που πρέπει να κάνουμε είναι να δούμε μία πρακτική εφαρμογή της μεθόδου μας. Έστω λοιπόν, ότι θέλουμε να συγκρίνουμε το επίπεδο ασφάλειας δύο συστημάτων πληροφορικής στη διάρκεια ενός μήνα. Όπως έχουμε αναφέρει, κάθε λογισμικό που είναι εγκατεστημένο στο σύστημα πληροφορικής που μελετάμε, αποτελεί δυνητικά και ένα παράγοντα κινδύνου. Έτσι λοιπόν, στους παρακάτω πίνακες Πίνακας 16 και Πίνακας 17, αποτυπώνονται οι τιμές της εντροπίας για κάθε παράγοντα κινδύνου των συστημάτων A & B.

5.17.1 Σύστημα A

Το πρώτο σύστημα, που εφεξής θα αναφέρεται ως «Σύστημα A», είναι ένα σύστημα βασισμένο στο λειτουργικό Linux, που έχει εγκατεστημένο ένα web server Apache 2, και τέλος μία βάση δεδομένων Oracle 10g. Εάν εφαρμόσουμε την προτεινόμενη μέθοδο υπολογισμού της εντροπίας (c_i), εξίσωση 7 και εξίσωση 8, παίρνουμε τα αποτελέσματα που φαίνονται στον παρακάτω πίνακα:

Προϊόν	***Σύνολο ευπαθειών***	***Εντροπία με τη χρήση του παράγοντα χρόνου (εξίσωση 9)***
Σύστημα A		
Linux kernels 2.6.20 και μετά	826	1,530205
Apache 2	96	1,988656
Oracle 10g	89	0,364065

Πίνακας 16: Τιμές εντροπίας παραγόντων κινδύνου για το Σύστημα A (Τα στοιχεία προέρχονται από την NVD)

5.17.2 Σύστημα B

Το δεύτερο σύστημα, που εφεξής θα αναφέρεται ως «Σύστημα B», είναι βασισμένο στο λειτουργικό σύστημα Windows 2003, που έχει εγκατεστημένο έναν web server της Microsoft, τον Internet Information Server 7 (IIS), και τέλος μία βάση δεδομένων SQL Server 2000. Εάν εφαρμόσουμε την προτεινόμενη μέθοδο υπολογισμού της εντροπίας (c_i), εξίσωση 7 και εξίσωση 8, παίρνουμε τα αποτελέσματα που φαίνονται στον παρακάτω πίνακα:

Προϊόν	***Σύνολο ευπαθειών***	***Εντροπία με τη χρήση του παράγοντα χρόνου (εξίσωση 9)***
Σύστημα B		
Windows 2003	565	3,374999
IIS 7	7	2,977185
SQL Server 2005	46	0,828787

Πίνακας 17: Τιμές εντροπίας παραγόντων κινδύνου για το Σύστημα B (Τα στοιχεία προέρχονται από την NVD)

5.17.3 Υπολογισμός της συνολικής ασφάλειας των Συστημάτων A & B

Σε αυτό το παράδειγμά, επικεντρωνόμαστε μόνο στους τεχνικούς παράγοντες κινδύνου, όπως τους έχουμε εξηγήσει στην παράγραφο § 5.1.1, και θεωρούμε ότι αυτοί χρησιμοποιούνται συνεχώς από το σύστημα πληροφορικής που εξετάζουμε σε ποσοστό 100%. Επίσης, θεωρούμε ότι όποια εφαρμογή είναι εγκατεστημένη στο σύστημα δεν έχει παρουσιάσει καμία ευπάθεια ακόμη, έτσι ώστε να μην επηρεάζει τους υπολογισμούς μας.

Θα εξετάσουμε το επίπεδο ασφάλειας των Συστημάτων A & B στη διάρκεια ενός μήνα, χρησιμοποιώντας τα δεδομένα από την βάση δεδομένων NVD. Για να το κάνουμε αυτό προβάλλαμε όλα τα δεδομένα της βάσης δεδομένων, για τον κάθε παράγοντα κινδύνου, στο διάστημα των 31 ημερών. Οι υπολογιζόμενες τιμές της εντροπίας κάθε τεχνικού παράγοντα κινδύνου φαίνονται στον Πίνακας 16 για το «Σύστημα A» και στον Πίνακας 17 για το «Σύστημα B». Για κάθε ημέρα και για

κάθε παράγοντα υπολογίσαμε το ημερήσιο άθροισμα του CVSS Score που υπήρχε στη βάση NVD. Στη συνέχεια το διαιρέσαμε με το συνολικό CVSS Score του παράγοντα αυτού. Οι τιμές που πήραμε κυμαίνονται από 0 έως 1. Στη συνέχεια τις υψώσαμε στη δύναμη $1/c_i$. Το αποτέλεσμα αυτής της διαδικασίας μας δίνει το πόσο ευάλωτο είναι ένα σύστημα. Έτσι λοιπόν αφαιρώντας την τιμή που βρήκαμε από τη μονάδα, που αποτελεί το 100% ασφαλές σύστημα πληροφορικής, υπολογίσαμε το επίπεδο ασφάλειας του συστήματος πληροφορικής που μελετούσαμε.

Προϊόν	Πίνακας υπολογισμού
Linux kernels 2.6.20 και μετά	Πίνακας 18
Apache 2	Πίνακας 19
Oracle 10g	Πίνακας 20
Windows 2003	Πίνακας 21
IIS 7	Πίνακας 22
SQL Server 2005	Πίνακας 23

Linux kernel 2.6.20 και μετά			Ci = 1,530205		
Ημέρα Μήνα	**Αριθμός ευπαθειών ημέρας**	**Άθροισμα CVSS Score ημέρας**	**Πιθανότητα (p_i)**	**Υπολογισμός Δ^{1/c_i}**	**Μετατροπή σε % ασφάλειας**
(Α)	**(Β)**	**(Γ)**	**(Δ)**	**(Ε)**	**(Ζ)**
1	35	165,20	0,0405	0,1229	0,8771
2	45	210,50	0,0515	0,1440	0,8560
3	33	164,50	0,0403	0,1226	0,8774
4	12	63,20	0,0155	0,0656	0,9344
5	20	109,90	0,0269	0,0942	0,9058
6	27	133,70	0,0327	0,1071	0,8929
7	32	165,20	0,0405	0,1229	0,8771
8	24	128,70	0,0315	0,1044	0,8956
9	26	146,80	0,0359	0,1138	0,8862
10	31	164,50	0,0403	0,1226	0,8774
11	14	80,00	0,0196	0,0765	0,9235
12	34	148,50	0,0364	0,1147	0,8853
13	16	89,20	0,0218	0,0822	0,9178
14	19	85,90	0,0210	0,0802	0,9198
15	25	121,30	0,0297	0,1005	0,8995
16	14	74,60	0,0183	0,0731	0,9269
17	27	119,00	0,0291	0,0992	0,9008
18	34	186,30	0,0456	0,1330	0,8670
19	25	127,30	0,0312	0,1037	0,8963
20	18	103,00	0,0252	0,0903	0,9097
21	26	116,70	0,0286	0,0980	0,9020
22	36	191,50	0,0469	0,1354	0,8646
23	36	150,90	0,0370	0,1159	0,8841
24	17	101,60	0,0249	0,0895	0,9105
25	15	82,90	0,0203	0,0783	0,9217
26	24	122,60	0,0300	0,1012	0,8988
27	36	160,40	0,0393	0,1206	0,8794
28	12	63,70	0,0156	0,0659	0,9341
29	33	144,70	0,0354	0,1127	0,8873
30	27	128,00	0,0313	0,1040	0,8960
31	53	233,20	0,0571	0,1540	0,8460
Σύνολα	**826**	**4.083,50**			

Πίνακας 18: Υπολογισμός τιμών εντροπίας για τεχνικό παράγοντα κινδύνου Linux kernel 2.6.20 και μετά (Τα στοιχεία προέρχονται από την NVD)

Όπου:

Η στήλη Δ = Γ / Άθροισμα CVSS Score, η στήλη Ε = Δ^{1/c_i} και η στήλη Ζ = 1 - Δ

Apache 2			Ci = 1,988656		
Ημέρα Μήνα	**Αριθμός ευπαθειών ημέρας**	**Άθροισμα CVSS Score ημέρας**	**Πιθανότητα (p_i)**	**Υπολογισμός Δ^{1/c_i}**	**Μετατροπή σε % ασφάλειας**
(Α)	**(Β)**	**(Γ)**	**(Δ)**	**(Ε)**	**(Ζ)**
1	0	0,00	0,0000	0,0000	1,0000
2	2	12,50	0,0254	0,1578	0,8422
3	4	32,20	0,0655	0,2539	0,7461
4	2	9,30	0,0189	0,1360	0,8640
5	8	45,70	0,0930	0,3028	0,6972
6	5	21,20	0,0431	0,2058	0,7942
7	2	12,50	0,0254	0,1578	0,8422
8	6	20,00	0,0407	0,1999	0,8001
9	3	15,00	0,0305	0,1729	0,8271
10	1	7,10	0,0144	0,1187	0,8813
11	3	15,00	0,0305	0,1729	0,8271
12	4	23,90	0,0486	0,2186	0,7814
13	7	32,90	0,0669	0,2567	0,7433
14	3	12,90	0,0262	0,1603	0,8397
15	0	0,00	0,0000	0,0000	1,0000
16	2	11,10	0,0226	0,1486	0,8514
17	0	0,00	0,0000	0,0000	1,0000
18	6	32,90	0,0669	0,2567	0,7433
19	1	5,00	0,0102	0,0995	0,9005
20	6	26,00	0,0529	0,2281	0,7719
21	3	17,10	0,0348	0,1847	0,8153
22	1	4,30	0,0087	0,0923	0,9077
23	1	5,00	0,0102	0,0995	0,9005
24	1	5,00	0,0102	0,0995	0,9005
25	5	21,20	0,0431	0,2058	0,7942
26	0	0,00	0,0000	0,0000	1,0000
27	2	9,30	0,0189	0,1360	0,8640
28	6	28,70	0,0584	0,2397	0,7603
29	4	22,80	0,0464	0,2135	0,7865
30	3	13,60	0,0277	0,1646	0,8354
31	5	29,40	0,0598	0,2426	0,7574
Σύνολα	**96**	**491,60**			

Πίνακας 19: Υπολογισμός τιμών εντροπίας για τεχνικό παράγοντα κινδύνου Apache 2 και μετά (Τα στοιχεία προέρχονται από την NVD)

Όπου:

Η στήλη Δ = Γ / Άθροισμα CVSS Score, η στήλη Ε = Δ^{1/c_i} και η στήλη Ζ = 1 - Δ

Oracle 10g			Ci = 0,364065		
Ημέρα Μήνα	**Αριθμός ευπαθειών ημέρας**	**Άθροισμα CVSS Score ημέρας**	**Πιθανότητα (p_i)**	**Υπολογισμός Δ^{1/c_i}**	**Μετατροπή σε % ασφάλειας**
(Α)	**(Β)**	**(Γ)**	**(Δ)**	**(Ε)**	**(Ζ)**
1	0	0,00	0,0000	0,0000	1,0000
2	3	21,80	0,0420	0,0002	0,9998
3	0	0,00	0,0000	0,0000	1,0000
4	11	73,60	0,1418	0,0047	0,9953
5	0	0,00	0,0000	0,0000	1,0000
6	0	0,00	0,0000	0,0000	1,0000
7	0	0,00	0,0000	0,0000	1,0000
8	1	7,50	0,0145	0,0000	1,0000
9	0	0,00	0,0000	0,0000	1,0000
10	0	0,00	0,0000	0,0000	1,0000
11	3	14,20	0,0274	0,0001	0,9999
12	1	5,00	0,0096	0,0000	1,0000
13	0	0,00	0,0000	0,0000	1,0000
14	16	75,40	0,1453	0,0050	0,9950
15	34	180,50	0,3478	0,0550	0,9450
16	8	48,80	0,0940	0,0015	0,9985
17	0	0,00	0,0000	0,0000	1,0000
18	5	41,00	0,0790	0,0009	0,9991
19	0	0,00	0,0000	0,0000	1,0000
20	1	10,00	0,0193	0,0000	1,0000
21	0	0,00	0,0000	0,0000	1,0000
22	1	7,50	0,0145	0,0000	1,0000
23	1	6,80	0,0131	0,0000	1,0000
24	0	0,00	0,0000	0,0000	1,0000
25	0	0,00	0,0000	0,0000	1,0000
26	2	12,20	0,0235	0,0000	1,0000
27	0	0,00	0,0000	0,0000	1,0000
28	0	0,00	0,0000	0,0000	1,0000
29	0	0,00	0,0000	0,0000	1,0000
30	0	0,00	0,0000	0,0000	1,0000
31	2	14,70	0,0283	0,0001	0,9999
Σύνολα	**89**	**519,00**			

Πίνακας 20: Υπολογισμός τιμών εντροπίας για τεχνικό παράγοντα κινδύνου Oracle 10g και μετά (Τα στοιχεία προέρχονται από την NVD)

Όπου:

Η στήλη Δ = Γ / Άθροισμα CVSS Score, η στήλη Ε = Δ^{1/c_i} και η στήλη Ζ = 1 - Δ

Windows 2003			Ci = 3,374999		
Ημέρα Μήνα	**Αριθμός ευπαθειών ημέρας**	**Άθροισμα CVSS Score ημέρας**	**Πιθανότητα (p_i)**	**Υπολογισμός Δ^{1/c_i}**	**Μετατροπή σε % ασφάλειας**
(Α)	**(Β)**	**(Γ)**	**(Δ)**	**(Ε)**	**(Ζ)**
1	16	99,40	0,0235	0,3290	0,6710
2	17	107,80	0,0255	0,3371	0,6629
3	21	144,50	0,0341	0,3676	0,6324
4	9	63,00	0,0149	0,2875	0,7125
5	2	10,00	0,0024	0,1666	0,8334
6	9	54,50	0,0129	0,2754	0,7246
7	7	47,40	0,0112	0,2642	0,7358
8	8	65,90	0,0156	0,2913	0,7087
9	44	357,00	0,0843	0,4806	0,5194
10	53	405,60	0,0958	0,4991	0,5009
11	36	278,90	0,0659	0,4467	0,5533
12	38	279,70	0,0661	0,4471	0,5529
13	80	622,50	0,1471	0,5667	0,4333
14	73	563,30	0,1331	0,5501	0,4499
15	41	337,30	0,0797	0,4726	0,5274
16	22	163,20	0,0386	0,3811	0,6189
17	10	74,00	0,0175	0,3015	0,6985
18	6	32,50	0,0077	0,2363	0,7637
19	0	0,00	0,0000	0,0000	1,0000
20	6	40,10	0,0095	0,2514	0,7486
21	8	49,80	0,0118	0,2681	0,7319
22	5	38,00	0,0090	0,2475	0,7525
23	3	18,90	0,0045	0,2012	0,7988
24	1	10,00	0,0024	0,1666	0,8334
25	0	0,00	0,0000	0,0000	1,0000
26	1	4,70	0,0011	0,1332	0,8668
27	11	82,20	0,0194	0,3110	0,6890
28	4	28,30	0,0067	0,2268	0,7732
29	4	33,70	0,0080	0,2388	0,7612
30	9	75,30	0,0178	0,3031	0,6969
31	21	145,40	0,0343	0,3683	0,6317
Σύνολα	**565**	**4.232,90**			

Πίνακας 21: Υπολογισμός τιμών εντροπίας για τεχνικό παράγοντα κινδύνου Windows 2003 και μετά (Τα στοιχεία προέρχονται από την NVD)

Όπου:

Η στήλη Δ = Γ / Άθροισμα CVSS Score, η στήλη Ε = Δ^{1/c_i} και η στήλη Ζ = 1 - Δ

	IIS 7		Ci = 2,977186		
Ημέρα Μήνα	**Αριθμός ευπαθειών ημέρας**	**Άθροισμα CVSS Score ημέρας**	**Πιθανότητα (p_i)**	**Υπολογισμός Δ^{1/c_i}**	**Μετατροπή σε % ασφάλειας**
(Α)	**(Β)**	**(Γ)**	**(Δ)**	**(Ε)**	**(Ζ)**
1	0	0,00	0,0000	0,0000	1,0000
2	0	0,00	0,0000	0,0000	1,0000
3	0	0,00	0,0000	0,0000	1,0000
4	1	2,60	0,0511	0,3682	0,6318
5	0	0,00	0,0000	0,0000	1,0000
6	0	0,00	0,0000	0,0000	1,0000
7	0	0,00	0,0000	0,0000	1,0000
8	1	8,50	0,1670	0,5482	0,4518
9	0	0,00	0,0000	0,0000	1,0000
10	0	0,00	0,0000	0,0000	1,0000
11	0	0,00	0,0000	0,0000	1,0000
12	1	7,20	0,1415	0,5184	0,4816
13	0	0,00	0,0000	0,0000	1,0000
14	0	0,00	0,0000	0,0000	1,0000
15	3	22,60	0,4440	0,7613	0,2387
16	0	0,00	0,0000	0,0000	1,0000
17	0	0,00	0,0000	0,0000	1,0000
18	0	0,00	0,0000	0,0000	1,0000
19	0	0,00	0,0000	0,0000	1,0000
20	0	0,00	0,0000	0,0000	1,0000
21	0	0,00	0,0000	0,0000	1,0000
22	0	0,00	0,0000	0,0000	1,0000
23	1	10,00	0,1965	0,5789	0,4211
24	0	0,00	0,0000	0,0000	1,0000
25	0	0,00	0,0000	0,0000	1,0000
26	0	0,00	0,0000	0,0000	1,0000
27	0	0,00	0,0000	0,0000	1,0000
28	0	0,00	0,0000	0,0000	1,0000
29	0	0,00	0,0000	0,0000	1,0000
30	0	0,00	0,0000	0,0000	1,0000
31	0	0,00	0,0000	0,0000	1,0000
Σύνολα	**7**	**50,90**			

Πίνακας 22: Υπολογισμός τιμών εντροπίας για τεχνικό παράγοντα κινδύνου IIS 7 και μετά (Τα στοιχεία προέρχονται από την NVD)

Όπου:

Η στήλη Δ = Γ / Άθροισμα CVSS Score, η στήλη Ε = Δ^{1/c_i} και η στήλη Ζ = 1 - Δ

SQL Server 2005			Ci = 1,878724		
Ημέρα Μήνα	**Αριθμός ευπαθειών ημέρας**	**Άθροισμα CVSS Score ημέρας**	**Πιθανότητα (p_i)**	**Υπολογισμός Δ^{1/c_i}**	**Μετατροπή σε % ασφάλειας**
(Α)	**(Β)**	**(Γ)**	**(Δ)**	**(Ε)**	**(Ζ)**
1	0	0,00	0,0000	0,0000	1,0000
2	0	0,00	0,0000	0,0000	1,0000
3	0	0,00	0,0000	0,0000	1,0000
4	0	0,00	0,0000	0,0000	1,0000
5	0	0,00	0,0000	0,0000	1,0000
6	0	0,00	0,0000	0,0000	1,0000
7	0	0,00	0,0000	0,0000	1,0000
8	0	0,00	0,0000	0,0000	1,0000
9	4	32,00	0,1749	0,3953	0,6047
10	1	9,00	0,0492	0,2012	0,7988
11	7	63,30	0,3459	0,5683	0,4317
12	0	0,00	0,0000	0,0000	1,0000
13	0	0,00	0,0000	0,0000	1,0000
14	8	74,40	0,4066	0,6194	0,3806
15	0	0,00	0,0000	0,0000	1,0000
16	1	4,30	0,0235	0,1358	0,8642
17	0	0,00	0,0000	0,0000	1,0000
18	0	0,00	0,0000	0,0000	1,0000
19	0	0,00	0,0000	0,0000	1,0000
20	0	0,00	0,0000	0,0000	1,0000
21	0	0,00	0,0000	0,0000	1,0000
22	0	0,00	0,0000	0,0000	1,0000
23	0	0,00	0,0000	0,0000	1,0000
24	0	0,00	0,0000	0,0000	1,0000
25	0	0,00	0,0000	0,0000	1,0000
26	0	0,00	0,0000	0,0000	1,0000
27	0	0,00	0,0000	0,0000	1,0000
28	0	0,00	0,0000	0,0000	1,0000
29	0	0,00	0,0000	0,0000	1,0000
30	0	0,00	0,0000	0,0000	1,0000
31	0	0,00	0,0000	0,0000	1,0000
Σύνολα	**217**	**183,00**			

Πίνακας 23: Υπολογισμός τιμών εντροπίας για τεχνικό παράγοντα κινδύνου SQL Server 2005 και μετά (Τα στοιχεία προέρχονται από την NVD)

Όπου:

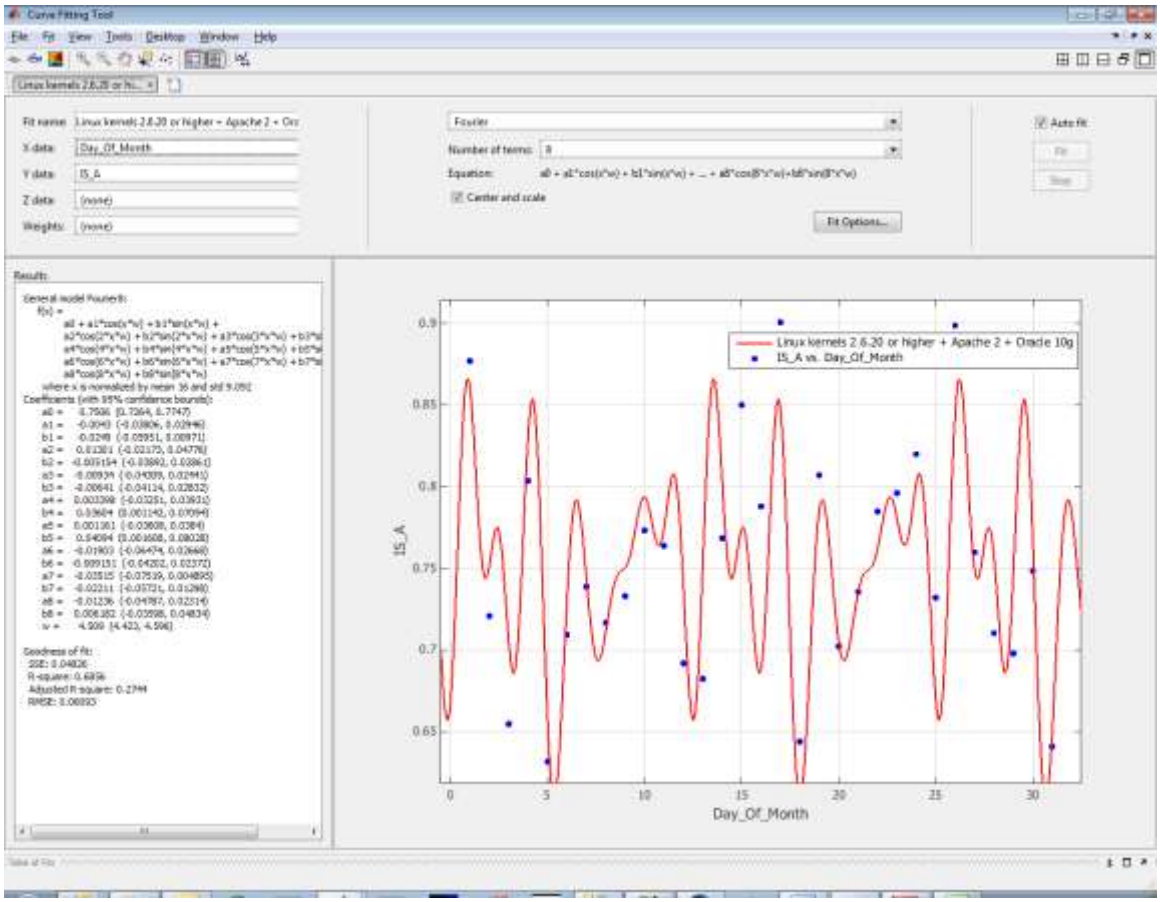
Η στήλη Δ = Γ / Άθροισμα CVSS Score, η στήλη Ε = Δ^{1/c_i} και η στήλη Ζ = 1 - Δ

Τέλος, έχοντας υπολογίσει τις τιμές εντροπίας για κάθε έναν από τους παράγοντες κινδύνου, υπολογίζουμε το γινόμενό τους, στήλη Ζ, από κάθε παράγοντα κινδύνου, για να βρούμε το συνολική τιμή της εντροπίας του συστήματος του οποίου αναζητούμε το επίπεδο ασφάλειας, Πίνακας 24.

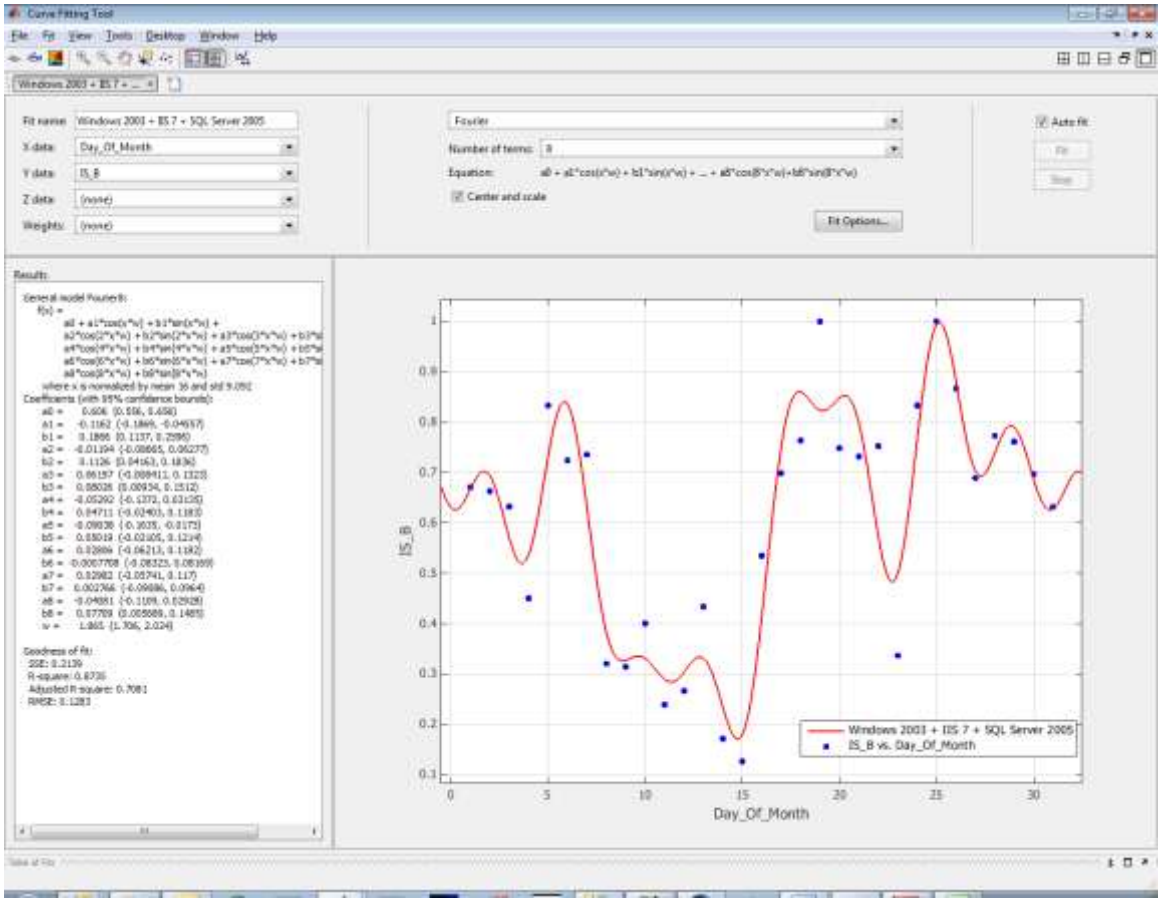
Ημερήσια Συνολική Εντροπία Συστημάτων Α & Β		
Ημέρα Μήνα	**Γινόμενο Ζ στήλης τεχνικών παραγόντων του Συστήματος Α**	**Γινόμενο Ζ στήλης τεχνικών παραγόντων του Συστήματος Β**
(Α)	**(Β)**	**(Γ)**
1	0,8771	0,6710
2	0,7208	0,6629
3	0,6546	0,6324
4	0,8035	0,4502
5	0,6315	0,8334
6	0,7092	0,7246
7	0,7387	0,7358
8	0,7166	0,3202
9	0,7329	0,3141
10	0,7732	0,4001
11	0,7637	0,2388
12	0,6918	0,2663
13	0,6822	0,4333
14	0,7685	0,1712
15	0,8501	0,1259
16	0,7879	0,5348
17	0,9008	0,6985
18	0,6438	0,7637
19	0,8071	1,0000
20	0,7022	0,7486
21	0,7354	0,7319
22	0,7848	0,7525
23	0,7961	0,3364
24	0,8199	0,8334
25	0,7320	1,0000
26	0,8988	0,8668
27	0,7598	0,6890
28	0,7102	0,7732
29	0,6979	0,7612
30	0,7484	0,6969
31	0,6407	0,6317

Πίνακας 24: Ημερήσια συνολική εντροπία συστημάτων Α & Β

Αν εισάγουμε τις τιμές αυτές στο MatLab, θα σχηματιστεί μία καμπύλη, η οποία σχηματίζεται από την στοχαστική συνάρτηση που χρειαζόμαστε, έτσι ώστε να υπολογίσουμε το επίπεδο ασφάλειας του συστήματος πληροφορικής που μελετάμε. Την στοχαστική συνάρτηση αυτή την προσεγγίσουμε με το Curve Fitting Tool του MatLab και με την βοήθεια της ανάλυσης κατά Fourier με οκτώ βαθμούς ελευθερίας, εξίσωση 14.



Εικόνα 12: Χρήση του Curve Fitting Tool, του MatLab, για την προσέγγιση της στοχαστικής συνάρτησης του «Συστήματος Α», κατά Fourier



Εικόνα 13: Χρήση του Curve Fitting Tool, του MatLab, για την προσέγγιση της στοχαστικής συνάρτησης του «Συστήματος Β», κατά Fourier

Όπως είχαμε αναφέρει, το MatLab, κάνοντας την προσέγγιση της καμπύλης, υπολογίζει και όλες τις μεταβλητές από την **Error! Reference source not found.**εξίσωση 14,

$$f(x) = a_0 + \alpha_1 \cos(wx) + b_1 \sin(wx) + \alpha_2 \cos(2wx) + b_2 \sin(2wx) + \alpha_3 \cos(3wx) + b_3 \sin(3wx) + \alpha_4 \cos(4wx) + b_4 \sin(4wx) + \alpha_5 \cos(5wx) + b_5 \sin(5wx) + \alpha_6 \cos(6wx) + b_6 \sin(6wx) + \alpha_7 \cos(7x) + b_7 \sin(7wx) + \alpha_8 \cos(8wx) + b_8 \sin(8wx) \quad (11)$$

οι οποίες εμφανίζονται στους ακόλουθους πίνακες, Πίνακας 25 και Πίνακας 26:

Όπου:			
a0	0.7506	**a5**	0.001161
a1	-0.0043	**b5**	0.04094
b1	-0.0249	**a6**	-0.01903
a2	0.01301	**b6**	-0.009151
b2	-0.005154	**a7**	-0.03515
a3	-0.00934	**b7**	-0.02211
b3	-0.00641	**a8**	-0.01236
a4	0.003398	**b8**	0.006182
b4	0.03604	**W**	0.4509

Πίνακας 25: Υπολογισμός μεταβλητών Fourier για το Σύστημα Α

Όπου:			
a0	0.606	**a5**	0.090038
a1	-0.1162	**b5**	0.05019
b1	-0.1866	**a6**	0.02806
a2	-0.01194	**b6**	0.0007708
b2	0.1126	**a7**	-0.02982
a3	-0.06197	**b7**	-0.002766
b3	-0.08026	**a8**	-0.04081
a4	-0.05292	**b8**	0.07709
b4	0.04711	**w**	1.865

Πίνακας 26: Υπολογισμός μεταβλητών Fourier για το Σύστημα Β

Στη συνέχεια δημιουργήσαμε ένα πρόγραμμα στο MatLab, το οποίο επισυνάπτεται στο Παράρτημα, και επιλύσαμε μέσω του MatLab, αυτή τη συνάρτηση, για κάθε μία ημέρα και τέλος, υπολογίσαμε το μέσο όρο των αποτελεσμάτων. Πρέπει να σημειωθεί εδώ, ότι η λύση της συνάρτησης αυτής, με τους παραπάνω όρους, αποτελεί και το ζητούμενο επίπεδο ασφάλειας τους συστήματος πληροφορικής που μελετάμε. Επειδή όμως, όπως έχει ήδη αναφερθεί, η ασφάλεια είναι δυναμική και μεταβάλλεται με το χρόνο, ζητάμε το μέσο όρο του μήνα έτσι ώστε να έχουμε όσο το δυνατόν, καλύτερη προσέγγιση του επιπέδου ασφαλείας του συστήματος πληροφορικής που μελετάμε.

Επιλύοντας, λοιπόν στο MatLab, την παραπάνω εξίσωση με τους όρους που προσεγγίσαμε, έχουμε τα εξής αποτελέσματα:

Σύστημα Α	
Linux kernels 2.6.20 και μετά	Επίπεδο Ασφάλειας 35,96%
Apache 2	Σύνολο ευπαθειών: 1.011
Oracle 10g	Σύνολο CVSS Score: 5.094,10
Σύστημα Β	
Windows 2003	Επίπεδο Ασφάλειας 50,94%
IIS 7	Σύνολο ευπαθειών: 593
SQL Server 2005	Σύνολο CVSS Score: 4.466,80

Πίνακας 27: Συνολικό επίπεδο ασφάλειας συστημάτων Α & Β

Παρατηρούμε λοιπόν, ότι το Σύστημα Α, έχει μικρότερο επίπεδο ασφάλειας (35,96%) συγκριτικά με Σύστημα Β (50,94%) και για το λόγο αυτό θεωρείται περισσότερο επιρρεπή σε επιθέσεις ασφαλείας. Αυτό μπορεί να εξηγηθεί, αφού το Σύστημα Α έχει μεγαλύτερο αριθμό ευπαθειών, 1.011 έναντι 593 του Συστήματος Β, αλλά και υψηλότερο συνολικά CVSS Score, 5.094,10 του Συστήματος Α, έναντι 4.466,80 του Συστήματος Β. Συνεπώς, η προτεινόμενη μεθοδολογία για τη μέτρηση του επιπέδου ασφάλειας ενός συστήματος πληροφορικής, επιβεβαιώνεται και εμπειρικά.

Είναι κατανοητό από το παράδειγμα αυτό, ότι έχουμε δημιουργήσει ένα νέο μέτρο για την ποσοτικοποίηση της ασφάλειας, το οποίο μπορεί να χρησιμοποιηθεί για την σύγκριση δύο εντελώς διαφορετικών συστημάτων πληροφορικής. Επιπλέον, ανάλογα με την ανάγκη της σύγκρισης, δύο ή περισσοτέρων συστημάτων πληροφορικής, η χρονική περίοδος μπορεί να μεταβληθεί σε μήνες, χρόνια ή ακόμα και να μειωθεί σε επίπεδο εβδομάδας.

Για το σκοπό αυτό, έχουμε υλοποιήσει ένα πρότυπο πρόγραμμα μέτρησης του επιπέδου της ασφάλειας ενός προϊόντος (Security Quantification Tool - SQT), χρησιμοποιώντας την προτεινόμενη μεθοδολογία και αξιοποιώντας τα δεδομένα της βάσης NVD. Το SQT, έχει αναρτηθεί στο internet ως ανοικτού κώδικα πρόγραμμα, για όποιον επιθυμεί και θέλει να το κατεβάσει και να το δοκιμάσει, στην ιστοσελίδα www.sourceforge.net/projects/sqt [100]. Το SQT παρουσιάζεται ανα-

λυτικά, τόσο ως προς τον τρόπο λειτουργίας του όσο και ως προς τα εργαλεία υλοποίησής του, στο επόμενο κεφάλαιο.

Επιπλέον, έχει υλοποιηθεί και μία λίγο διαφορετική έκδοση αυτού [101] και την έχουμε αναρτήσει στο διαδίκτυο για όποιον θέλει να το δοκιμάσει. Η έκδοση αυτή, για την εύρεση του επιπέδου ασφάλειας ενός προϊόντος ή συστήματος πληροφορικής χρησιμοποιεί απλή ολοκλήρωση τη στιγμή που το SQT χρησιμοποιεί στοχαστική ολοκλήρωση. Η διεύθυνση που μπορεί να το βρει και να το κατεβάσει κάποιος από το internet, είναι: http://sourceforge.net/projects/secqua/.

Κεφάλαιο 6: Πρότυπο πρόγραμμα υπολογισμού επιπέδου ασφάλειας - Security Quantification Tool (SQT)

6. Γενικά

Όπως αναφέρθηκε αναλυτικά στο δεύτερο κεφάλαιο, η διαδικασία διαχείρισης των κινδύνων στα συστήματα πληροφορικής, είναι μία διαδικασία που πρέπει να εμπεριέχεται σε όλες τις αποφάσεις της Διοίκησης μίας επιχείρησης. Ο εντοπισμός των κινδύνων, ο διαχωρισμός τους ανάλογα με την επικινδυνότητά τους, η λήψη μέτρων, τόσο προστασίας από αυτούς όσο και ανάκαμψης σε περίπτωση που συμβούν, και, τέλος, η αξιολόγηση των προτεινόμενων μέτρων, είναι μία αέναη διαδικασία που αυτοτροφοδοτείται και σηματοδοτεί σε μεγάλο βαθμό την ικανότητα της Διοίκησης να φέρει σε πέρας το ρόλο της.

Για να μπορέσει η Διοίκηση μια επιχείρησης να κάνει όλα τα παραπάνω, πρέπει να είναι σε θέση να αξιολογήσει τα συστήματα πληροφορικής που διαθέτει με τρόπο τέτοιο που να είναι ακριβής και αμερόληπτος.

Στο κομμάτι αυτό της παρούσας διατριβής, θα παρουσιαστεί ένα πρότυπο πρόγραμμα ποσοτικοποίησης του επιπέδου της ασφάλειας ενός προϊόντος ή συστήματος πληροφορικής, με τη χρήση στοχαστικών ολοκληρωμάτων. Το παρουσιαζόμενο πρόγραμμα που υλοποιεί την προτεινόμενη μεθοδολογία που αναλύθηκε στο πέμπτο κεφάλαιο, φέρει το χαρακτηριστικό όνομα «Security Quantification Tool (SQT)». Ο σκοπός της χρήσης ενός τέτοιου προγράμματος είναι να μας παρέχει ένα καθαρό νούμερο που θα αποτυπώνει το επίπεδο ασφαλείας ενός προϊόντος ή ενός συστήματος πληροφορικής.

6.1 Περιγραφή αναγκών του προγράμματος

Μια από τις αναγκαίες ενέργειες για κάθε πρόγραμμα λογισμικού, που προηγείται της υλοποίησής του, είναι η εκπόνηση της μελέτης σκοπιμότητας. Στην μελέτη

αυτή, ανάμεσα σε άλλα, περιγράφονται το κόστος και τα οφέλη από την υλοποίηση του προγράμματος λογισμικού, οι επιχειρησιακές απαιτήσεις που καλείται το πρόγραμμα να υλοποιήσει και φυσικά οι ομάδες των χρηστών που θα το χρησιμοποιήσουν. Επιπλέον, καθορίζονται τα εργαλεία που θα χρησιμοποιηθούν στην φάση της ανάπτυξης και οι ελάχιστες απαιτήσεις στους σταθμούς εργασίας των χρηστών που θα το χρησιμοποιήσουν.

6.1.1 Οφέλη από τη χρήση του SQT

Η παρούσα διατριβή, έχει σκοπό να βοηθήσει τα μέλη της Διοίκησης μίας εταιρείας ή / και Οργανισμού, στο να ενημερωθούν για το επίπεδο ασφάλειας των συστημάτων πληροφορικής που διαθέτουν. Η γνώση αυτή στη Διοίκηση, μπορεί να αξιολογηθεί ως ένα πολύ χρήσιμο και αναγκαίο εργαλείο για τη λήψη αποφάσεων. Όλες οι επενδύσεις που έχει κάνει μία επιχείρηση σε συστήματα πληροφορικής ή που σκοπεύει να κάνει, μπορούν να αξιολογηθούν με τη χρήση του SQT ως προς το κομμάτι της ασφάλειας που παρέχουν. Με τον τρόπο αυτό, είναι δυνατή η εξοικονόμηση πόρων, σε σχέση με τα οφέλη που παρέχουν τα διάφορα προϊόντα λογισμικού στον τομέα της ασφάλειας στην επιχείρηση. Με άλλα λόγια, με τη χρήση του SQT, η Διοίκηση κάθε επιχείρησης μπορεί με μεγαλύτερη ευχέρεια να εκπονήσει μελέτες κόστους/οφέλους των επενδύσεων που έχει κάνει, αλλά και να επανεξετάσει το στρατηγικό πλάνο των επενδύσεών της σε συστήματα πληροφορικής έτσι ώστε να πετύχει τα μεγαλύτερα για εκείνη οφέλη, στον τομέα της ασφάλειας.

6.1.2 Καθορισμός επιχειρησιακών απαιτήσεων

Για το συγκεκριμένο πρόγραμμα, (SQT), οι επιχειρησιακές απαιτήσεις που καλείται να υλοποιήσει είναι πολύ συγκεκριμένες. Θα πρέπει να λειτουργήσει σαν ένα πρόγραμμα υποστήριξης αποφάσεων (decision support system), με μοναδικό σκοπό την αξιολόγηση των συστημάτων πληροφορικής της επιχείρησης, με ακριβή και

αμερόληπτο τρόπο καθώς και την υποστήριξη των αποφάσεων για μελλοντικές επενδύσεις.

Για την πραγματοποίηση της αξιολόγησης, το πρόγραμμα SQT θα πρέπει να έχει στοιχεία για όσο το δυνατόν περισσότερα προϊόντα λογισμικού αλλά και ταυτόχρονα να ενημερώνεται συνεχώς, όπως και εγκαίρως, με νέα. Επιπλέον, τα στοιχεία που θα τροφοδοτούνται στο σύστημα θα πρέπει να είναι ακριβή, αμερόληπτα και αδιαμφισβήτητα.

6.1.3 Καθορισμός ομάδων χρηστών

Η μεθοδολογία που υλοποιεί το SQT, έχει ως σκοπό να βοηθήσει όλα τα στελέχη μίας επιχείρησης, ανεξαρτήτως του επιπέδου των τεχνικών γνώσεων που βρίσκονται, στο να κατανοήσουν το επίπεδο ασφάλειας των συστημάτων πληροφορικής που διαθέτουν. Για το λόγο αυτό, το εξαγόμενο προϊόν της προτεινόμενης μεθοδολογίας, είναι ένα αριθμητικό αποτέλεσμα, που μπορεί να αξιολογηθεί από όλα τα επίπεδα της Διοίκησης και από όλα τα στελέχη.

Συνεπώς, το SQT, μπορεί να χρησιμοποιηθεί από όλα τα στελέχη της επιχείρησης, είτε αυτά ανήκουν στη Διεύθυνση Πληροφορικής της επιχείρησης, είτε στη Διεύθυνση Προμηθειών, είτε σε άλλο επίπεδο της Διοίκησης. Το περιβάλλον που καλείται να χρησιμοποιήσει ο χρήστης είναι ιδιαίτερα φιλικό και διαισθητικό, που σκοπό έχει να βοηθήσει κάθε χρήστη, ανεξαρτήτως του επιπέδου εξοικείωσής του με τη χρήση ηλεκτρονικών υπολογιστών.

6.1.4 Καθορισμός εργαλείων ανάπτυξης

Είναι πάρα πολύ σημαντικό, τα εργαλεία ανάπτυξης ενός προγράμματος λογισμικού που θα επιλεχθούν, να παρέχουν τη δυνατότητα στον προγραμματιστή, πέρα από το να υλοποιήσει τις επιχειρησιακές απαιτήσεις, να μπορεί να προσφέρει ένα φιλικό, πλούσιο και εύχρηστο περιβάλλον εργασίας στους μελλοντικούς χρήστες. Ο τελικός χρήστης του προγράμματος, είναι σίγουρο ότι έχει χρησιμοποιήσει αρ-

κετά προϊόντα λογισμικού και πλέον, στις μέρες μας, θα σταθεί κριτικά απέναντι σε δύσχρηστα και φτωχά περιβάλλοντα εργασίας που θα κληθεί να χρησιμοποιήσει, με αποτέλεσμα τη μη αποδοχή του προγράμματος από αυτόν. Αυτό είναι ένα γεγονός που δεν θα πρέπει να παραλείπεται κατά τη διαδικασία επιλογής εργαλείων ανάπτυξης ενός προϊόντος λογισμικού.

Επιπλέον, οι λειτουργικές απαιτήσεις ενός προϊόντος λογισμικού, δηλαδή τα αναγκαία προγράμματα που πρέπει να προϋπάρχουν στο σταθμό εργασίας του τελικού χρήστη, παίζουν πολύ σημαντικό ρόλο, τόσο στην εύρυθμη λειτουργία όσο και στην αποδοχή του προϊόντος αυτού από τους χρήστες. Αν για παράδειγμα, ο τελικός χρήστης, θα πρέπει να εγκαταστήσει μία σειρά από εξειδικευμένα προϊόντα λογισμικού, πέρα από το ίδιο το πρόγραμμα, για να καταφέρει τελικά να χρησιμοποιήσει το εν λόγω πρόγραμμα, είναι σίγουρο ότι αυτό θα παίξει ένα πολύ αρνητικό ρόλο στην αποδοχή του. Εξάλλου, η εγκατάσταση επιπλέον προϊόντων λογισμικού είναι μία διαδικασία που κουράζει ιδιαίτερα τους χρήστες, και το λιγότερο, εγκυμονεί κινδύνους ως προς την επιτυχή ολοκλήρωσή τους.

6.2 Παρουσίαση του SQT

Έχοντας αναφέρει όλα τα παραπάνω, στο σημείο αυτό, γίνεται μία λεπτομερής περιγραφή, τόσο του λειτουργικού περιβάλλοντος όσο και των εργαλείων ανάπτυξης του SQT και να εξηγηθούν οι λόγοι των επιλογών τους.

Όπως έχουμε αναφέρει, το θέμα της ασφάλειας ενός προϊόντος ή συστήματος πληροφορικής δεν είναι μία στατική διαδικασία αλλά μία δυναμική. Συνεπώς, η αξιολόγηση του επιπέδου της ασφάλειας ενός συστήματος πληροφορικής, δεν μπορεί να είναι μία διαδικασία που θα γίνει μία φορά αλλά μια επαναλαμβανόμενη διαδικασία που δυνητικά θα παράγει διαφορετικά αποτελέσματα. Για το λόγο αυτό ένα εργαλείο σαν το SQT, πρέπει να έχει τη μέγιστη αποδοχή από τους τελικούς χρήστες έτσι ώστε να είναι όσο το δυνατό πιο ευχάριστη η διαρκής αξιολόγηση και τροφοδότησή του με τα στοιχεία που χρειάζεται για την αξιολόγηση.

6.2.1 Λειτουργικό περιβάλλον SQT

Αρχίζοντας λοιπόν την περιγραφή του SQT, πρέπει να αναφέρουμε ότι πρόκειται για μία παραθυρική εφαρμογή σε λειτουργικό περιβάλλον Windows και είναι υλοποιημένη σε γλώσσα προγραμματισμού VB.Net, με τη χρήση του Microsoft Visual Studio 2008. Ο λόγος που επιλέχθηκε αυτό το περιβάλλον, είναι λόγω της ευρείας αποδοχής των Windows αλλά και της υιοθέτησής τους ως το λειτουργικό περιβάλλον επιχειρησιακής λειτουργίας των περισσοτέρων επιχειρήσεων παγκοσμίως. Έχοντας ένα εργαλείο που λειτουργεί στο περισσότερο χρησιμοποιούμενο περιβάλλον, αυξάνεται κατακόρυφα η πιθανότητα αποδοχής του από την κοινότητα των χρηστών.

6.2.2 Προαπαιτούμενα προϊόντα λογισμικού

Κάθε μία εφαρμογή έχει κάποια προαπαιτούμενα προϊόντα λογισμικού για να λειτουργήσει. Το SQT, ως παραθυρική εφαρμογή, προϋποθέτει την ύπαρξη του .Net Framework 2.0 της εταιρείας Microsoft, στο σταθμό εργασίας κάθε χρήστη. Η έκδοση αυτή του .Net Framework δεν επιλέχθηκε τυχαία. Ο λόγος επιλογής της έγινε με γνώμονα την ελαχιστοποίηση των προβλημάτων εγκατάστασης της εφαρμογής, αφού η έκδοση 2.0 είναι εγκατεστημένη σε όλα τα λειτουργικά συστήματα της εταιρείας Microsoft, από την έκδοση Windows XP SP2 και μετά. Έχοντας ήδη φτάσει προ της επίσημης κυκλοφορίας των Windows 8, το .Net Framework 2.0 φαντάζει πλέον απίθανο να μην βρίσκεται εγκατεστημένο στο σταθμό εργασίας του τελικού χρήστη.

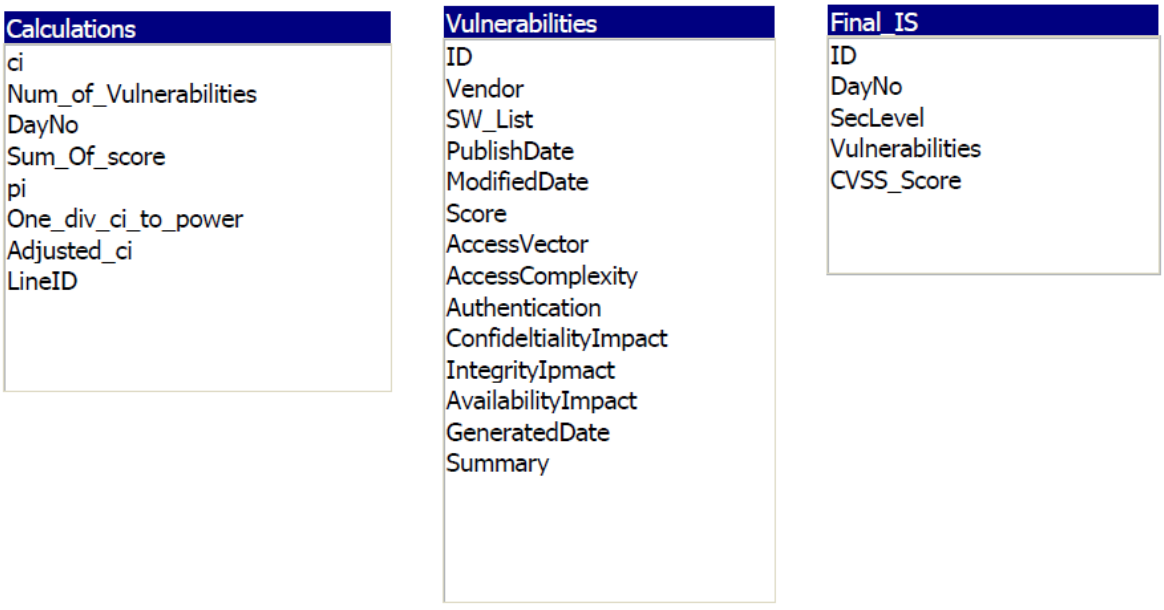
Πρέπει να τονιστεί, ότι το SQT υλοποιεί την προτεινόμενη μεθοδολογία ποσοτικοποίησης του επιπέδου της ασφάλειας με τη χρήση στοχαστικών ολοκληρωμάτων. Για την επίλυση των στοχαστικών ολοκληρωμάτων, έχει χρησιμοποιηθεί ένα εξειδικευμένο μαθηματικό πακέτο της MathWorks, το MatLab 2012a. Συνεπώς, το περιβάλλον του MatLab είναι προαπαιτούμενο για τη λειτουργία του SQT. Για το λόγο αυτό, έχει φτιαχτεί ένα ειδικό αρχείο εγκατάστασης (setup file), το οποίο εγκαθιστά την υπολογιστική μηχανή (runtime engine) του MatLab, που δίνεται

δωρεάν σε όσους έχουν αγοράσει το μαθηματικό πακέτο, για να μπορούν να διαμοιράσουν τη δουλειά τους.

Τέλος, το SQT χρησιμοποιεί μία βάση δεδομένων, την Microsoft Access, στην οποία αποθηκεύονται όλα τα συμβάντα ασφαλείας που θα χρησιμοποιήσει για τους διάφορους υπολογισμούς του προτεινόμενου μοντέλου. Αρχικά, είχε επιλεχθεί και χρησιμοποιηθεί η βάση δεδομένων της Microsoft, SQL Server 2008, αλλά για λόγους ευχρηστίας αλλάχθηκε με τη Microsoft Access. Με τον τρόπο αυτό, ο τελικός χρήστης δεν χρειάζεται να έχει καμία βάση δεδομένων στον σταθμό εργασίας του, αφού η επικοινωνία με την MS Access επιτυγχάνεται με ενσωματωμένους οδηγούς (drivers) της Microsoft στο .Net Framework 2.0, το οποίο είναι, πλέον, εγκατεστημένο σε όλα τα λειτουργικά συστήματα της Microsoft από την έκδοση XP SP2 και πάνω. Το αρχείο (mdb) της βάσης δεδομένων δίνεται μαζί με το SQT.

6.2.3 Πίνακες της βάσης δεδομένων

Οι πίνακες της βάσης δεδομένων παρουσιάζονται στη παρακάτω Εικόνα 14.



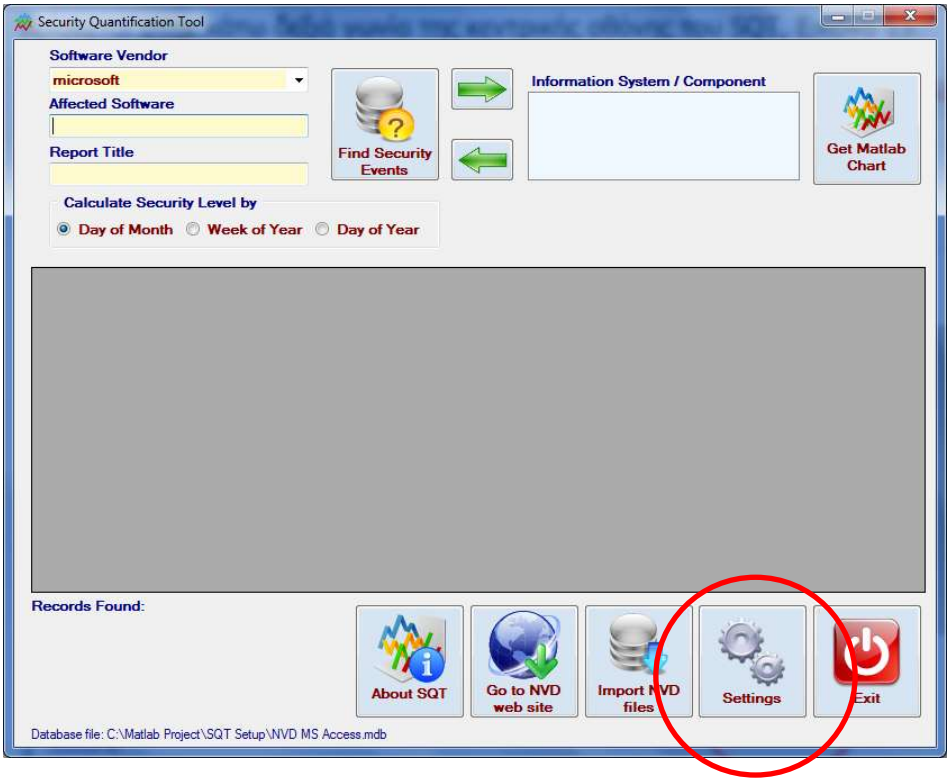
Εικόνα 14: Πίνακες που χρησιμοποιεί το SQT

Ο πίνακας «Vulnerabilities», περιέχει όλες τις ευπάθειες για όλα τα προϊόντα και έχει αναλυτικά παρουσιαστεί στην παράγραφο § 5.7.1 , ο πίνακας «Calculations» είναι ένας βοηθητικός πίνακας στον οποίο γίνονται όλοι οι υπολογισμοί του προτεινόμενου μοντέλου και τέλος ο πίνακας «Final_IS», περιέχει τα τελικά (συγκεντρωτικά) αποτελέσματα των υπολογισμών.

6.3 Ρυθμίσεις παραμέτρων του SQT

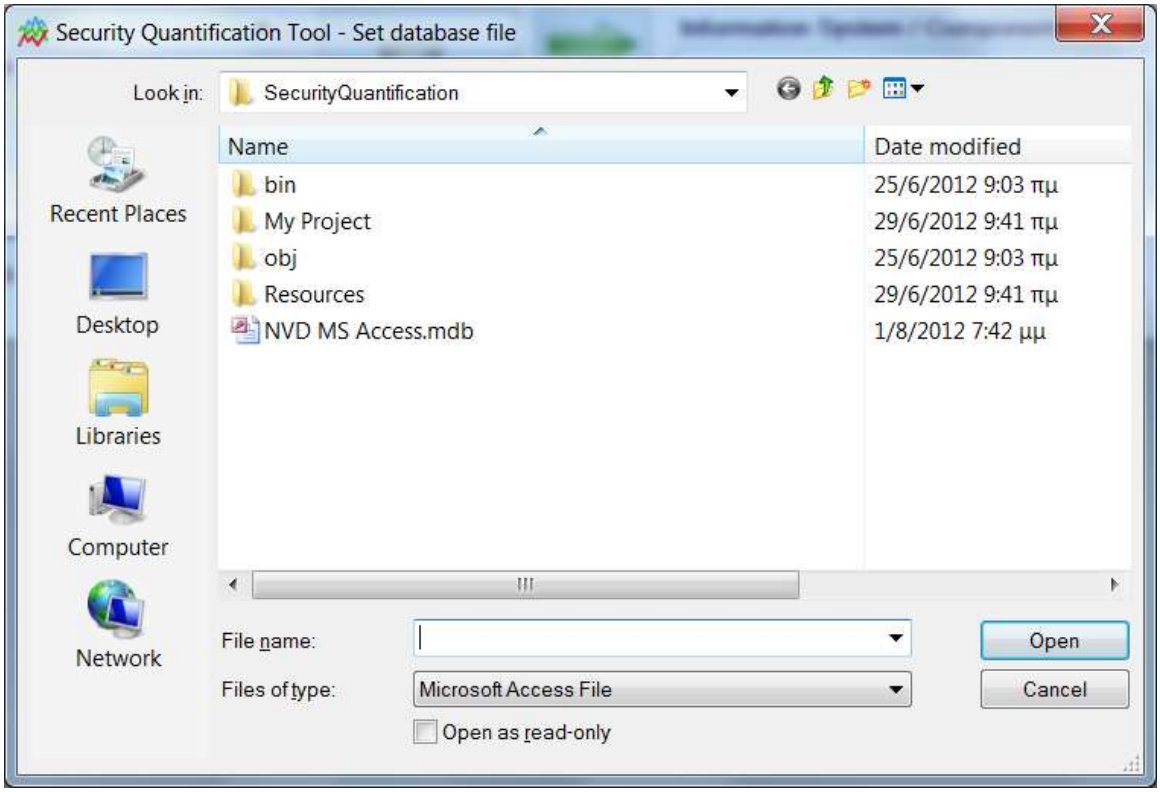
Όπως αναφέρθηκε το SQT χρησιμοποιεί τη MS Access ως βάση δεδομένων. Η MS Access πέρα από την απλή αποθήκευση των xml αρχείων, χρησιμοποιείται για την υποστήριξη σύνθετων και πολύπλοκων SQL ερωτημάτων τα οποία το προτεινόμενο μοντέλο ποσοτικοποίησης της ασφάλειας προϋποθέτει. Συνεπώς, η μοναδική ρύθμιση του SQT, έγκειται στον καθορισμό της τοποθεσίας του αρχείου mdb που αποτελεί τη εν λόγω βάση δεδομένων.

Για τη ρύθμιση αυτή, πρέπει ο χρήστης να επιλέξει το κουμπί «Settings», που βρίσκεται στην κάτω δεξιά γωνία της κεντρικής οθόνης του SQT, Εικόνα 15.



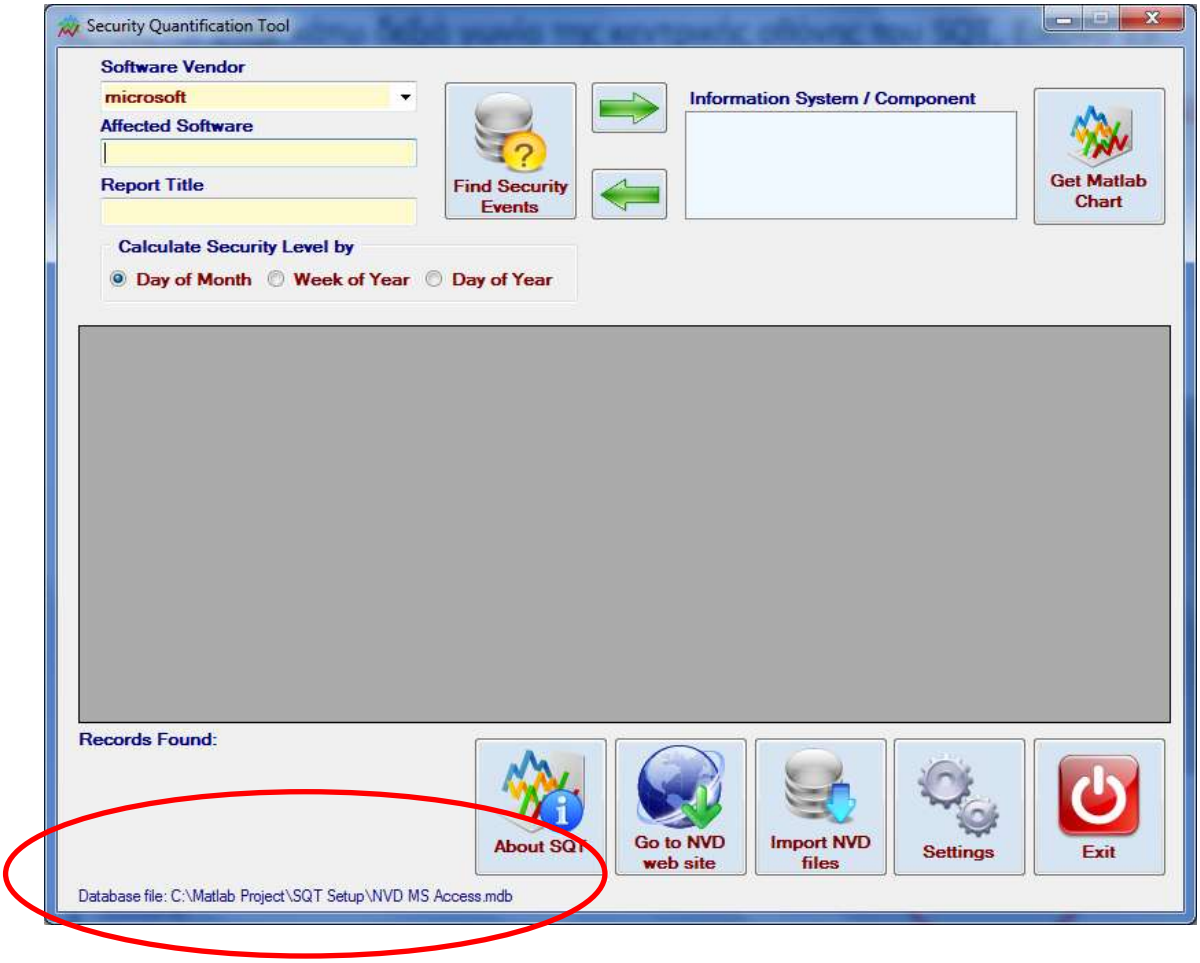
Εικόνα 15: Ρυθμίσεις παραμέτρων SQT

Μετά την επιλογή για ρύθμιση παραμέτρων εμφανίζεται το παρακάτω παράθυρο, στο οποίο ο χρήστης πρέπει να καθορίσει την τοποθεσία του αρχείου «NVD MS Access.mdb» της βάσης δεδομένων, Εικόνα 16.

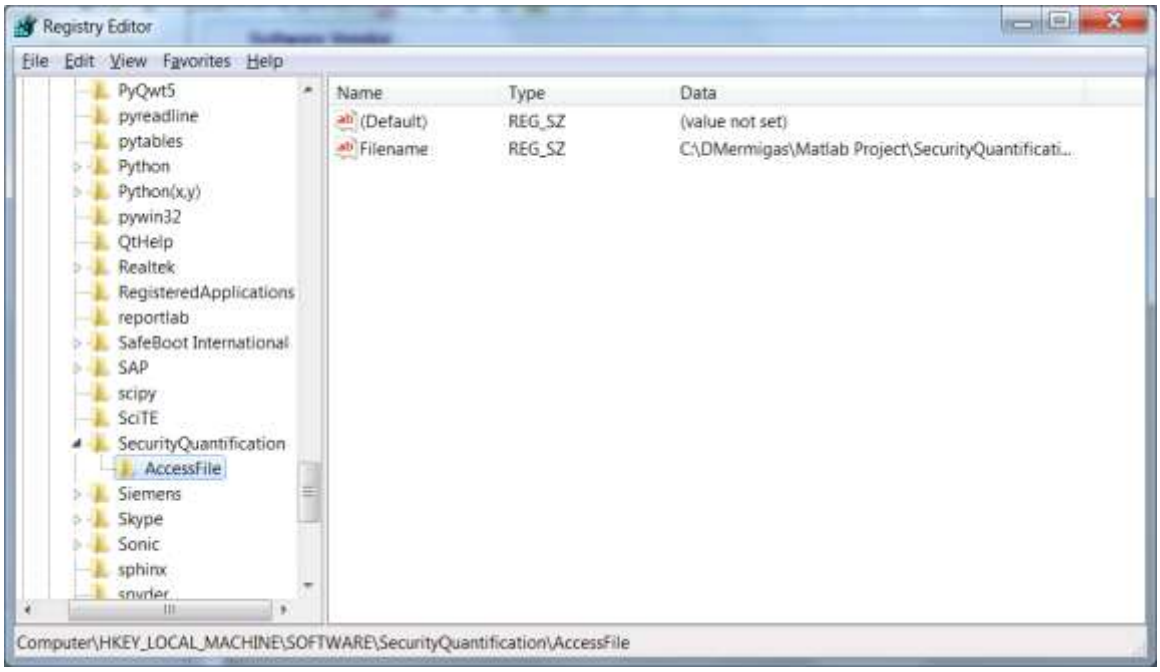


Εικόνα 16: Εύρεση αρχείου mdb

Όταν επιλεχθεί η βάση δεδομένων, στην κάτω αριστερή γωνία της κεντρικής οθόνης του SQT, Εικόνα 17, θα εμφανίσει την τοποθεσία που βρίσκεται. Ταυτόχρονα θα δημιουργηθεί μία εγγραφή στο μητρώο (registry) του σταθμού εργασίας του χρήστη, Εικόνα 18, έτσι ώστε όταν ξαναενεργοποιηθεί το SQT, να μπορεί να τη χρησιμοποιήσει χωρίς την παρέμβαση του χρήστη. Φυσικά, αν ο χρήστης επιλέξει να μετακινήσει τη βάση δεδομένων σε άλλη τοποθεσία, πρέπει να ξανακάνει την ίδια διαδικασία για να ενημερωθεί σωστά το μητρώο.



Εικόνα 17: Εμφάνιση τοποθεσίας αρχείου βάσης δεδομένων



Εικόνα 18: Αποθήκευση τοποθεσίας αρχείου της βάσης δεδομένων στο Registry

6.4 Ενημέρωση του SQT

Όπως αναφέρθηκε στην παράγραφο § 6.1.2, το SQT θα πρέπει να έχει στοιχεία για όσο το δυνατό περισσότερα προϊόντα λογισμικού και να μπορεί να ενημερώνεται διαρκώς. Επιπλέον, έχει ήδη αναφερθεί, ότι η παρούσα διατριβή χρησιμοποίησε ως πηγές ευπαθειών, δύο πολύ γνωστές και ανοικτού κώδικα (open source), βάσεις δεδομένων: α) την Open Source Vulnerability Database [92] και β) την National Vulnerability Database [93]. Για λόγους ενίσχυσης της αντικειμενικότητας της παρούσας έρευνας, χρησιμοποιήθηκε η δεύτερη (NVD), στην παραγωγή του πρωτότυπου συστήματος ποσοτικοποίησης της ασφάλειας, SQT.

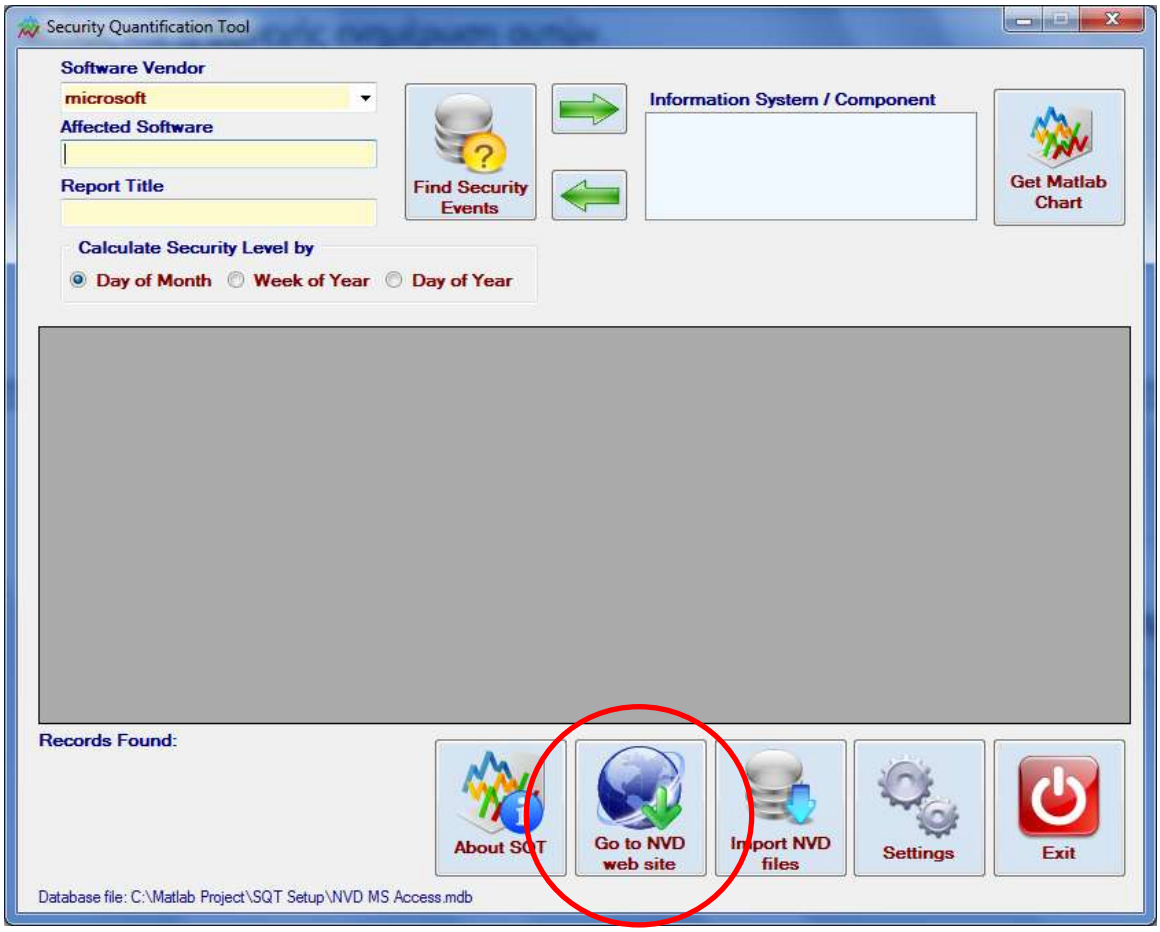
Η NVD παρέχει μέσα από την ιστοσελίδα της http://nvd.nist.gov/download.cfm, ένα σύνολο από xml αρχεία, σε όποιον ερευνητή ενδιαφέρεται, για τη μελέτη των ευπαθειών διαφόρων προϊόντων λογισμικού. Όμως, όπως και η ίδια αναφέρει, τα αρχεία αυτά, έχουν διαφορετική γραμμογράφηση (schema), με αποτέλεσμα να μην είναι δυνατή η άμεση εισαγωγή τους σε κάποια βάση δεδομένων.

Με σκοπό να ξεπεραστεί αυτό το πρόβλημα, αναπτύχθηκε ένα ειδικό πρόγραμμα, το οποίο διαβάζει τα παρεχόμενα xml αρχεία και, εν συνεχεία, εισάγει σε μία βάση δεδομένων τα στοιχεία που μας ενδιαφέρουν. Ο πηγαίος κώδικας, παρατίθεται αυτούσιος και συμπεριλαμβάνεται στην υπορουτίνα (sub routine) «ProcessXml» στο παράτημα που ακολουθεί.

Η υπορουτίνα αυτή, ζητά από τον χρήστη να καθορίσει την τοποθεσία που βρίσκονται τα προς εισαγωγή xml αρχεία των ευπαθειών από την NVD. Ο χρήστης έχει τη δυνατότητα να εισάγει στην βάση δεδομένων είτε ένα και μόνο αρχείο, είτε πολλά μαζί. Σε περίπτωση ακύρωσης της προσπάθειας από τον τελικό χρήστη, εμφανίζεται αντίστοιχο μήνυμα. Ομοίως, όταν η διαδικασία τελειώσει επιτυχώς, εμφανίζεται μήνυμα στον χρήστη.

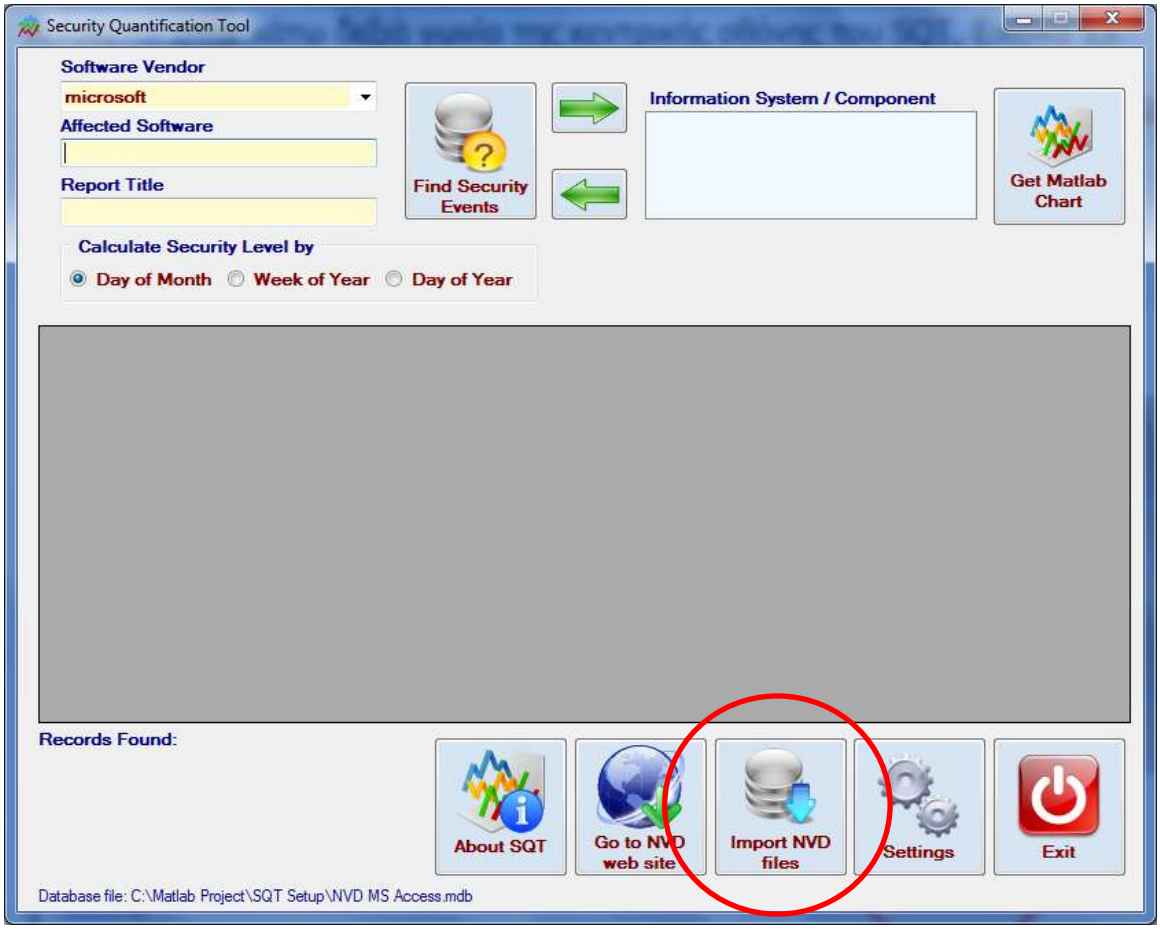
Με τη δημιουργία αυτής της διαδικασίας, υλοποιήθηκε η επιχειρησιακή απαίτηση για το SQT, της εισαγωγής στοιχείων ευπαθειών για πολλά προϊόντα λογισμικού καθώς και η συνεχής ενημέρωση αυτών.

Για την εύρεση των αρχείων xml της NVD, επιλέγουμε το κουμπί «Go To NVD web site», που βρίσκεται στην κάτω πλευρά της κεντρικής οθόνης του SQT και εμφανίζεται στην εικόνα που ακολουθεί, Εικόνα 19. Μετά την ενεργοποίηση της επιλογής αυτής, αυτόματα θα εμφανιστεί ένας Internet Explorer (Browser), που θα μας παραπέμπει στην ιστοσελίδα της NIST, που παρέχει τα xml αρχεία της NVD.



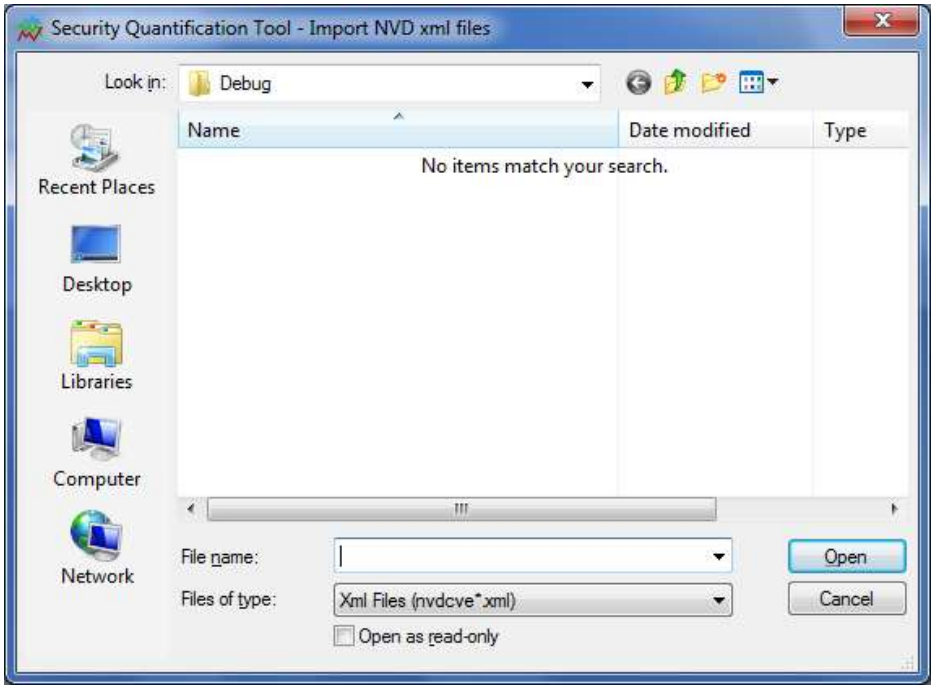
Εικόνα 19: Εύρεση αρχείων xml από τη NVD

Για την ενημέρωση της βάσης δεδομένων του SQT από τα αρχεία xml της NVD, επιλέγουμε το κουμπί «Import NVD files», που βρίσκεται στην κάτω δεξιά γωνία της κεντρικής οθόνης του SQT και εμφανίζεται στην εικόνα που ακολουθεί, Εικόνα 20.



Εικόνα 20: Εισαγωγή xml αρχείων από την NVD

Μετά την επιλογή για την εισαγωγή αρχείων xml εμφανίζεται το παρακάτω παράθυρο, Εικόνα 21, στο οποίο ο χρήστης πρέπει να καθορίσει την τοποθεσία των αρχείων xml προς εισαγωγή.

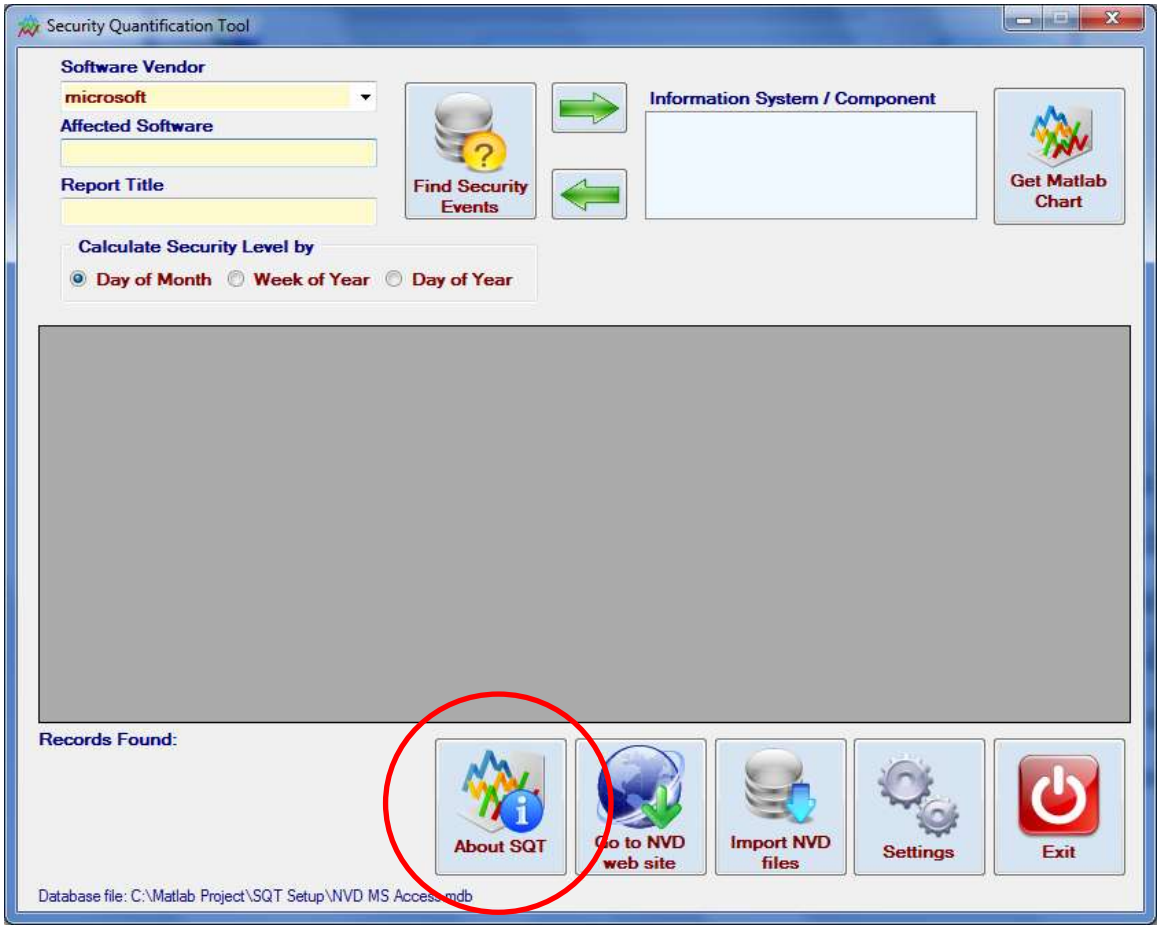


Εικόνα 21: Επιλογή xml αρχείων από την NVD

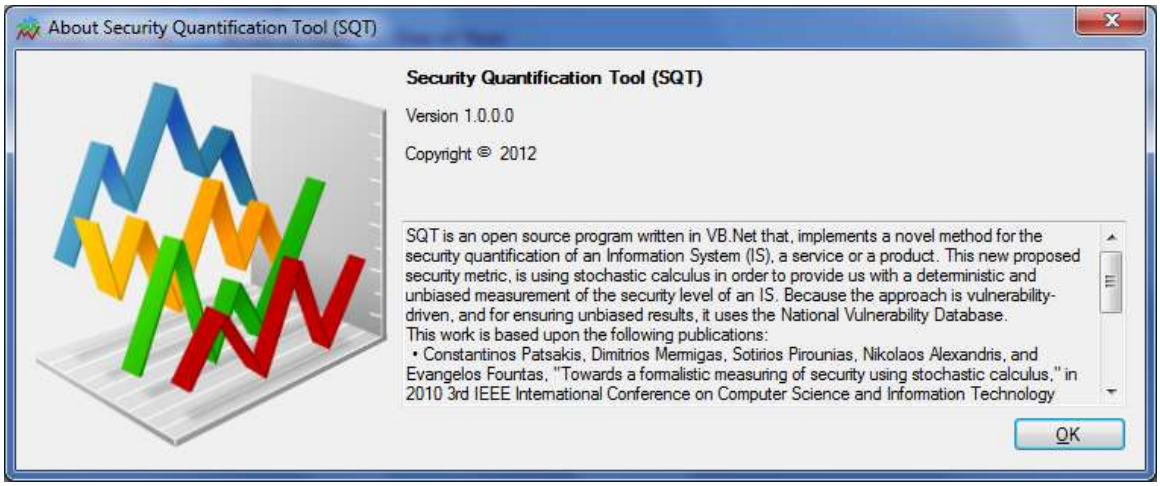
6.5 Πληροφορίες του SQT

Το SQT είναι ένα πρόγραμμα ανοικτού κώδικα (open source) υλοποιημένο σε VB.Net, και διατίθεται δωρεάν για χρήση, για όποιον επιθυμεί να το δοκιμάσει στην ιστοσελίδα www.sourceforge.net . Επιπλέον, στην ιστοσελίδα είναι διαθέσιμα αρχεία με τον πηγαίο κώδικα τόσο της διεπαφής με τον χρήστη (VB.Net), όσο και του υπολογιστικού προγράμματος που χρησιμοποιήθηκε (MatLab).

Τέλος, επιλέγοντας το κουμπί «About SQT», που βρίσκεται στην κάτω πλευρά της κεντρικής οθόνης του SQT και εμφανίζεται στην εικόνα που ακολουθεί, Εικόνα 20, μπορούμε να δούμε πληροφορίες αναφορικά με την τρέχουσα έκδοση του SQT αλλά και την ερευνητική δουλειά (δημοσιεύσεις) στην οποία βασίστηκε, Εικόνα 23.



Εικόνα 22: Εμφάνιση Πληροφοριών SQT

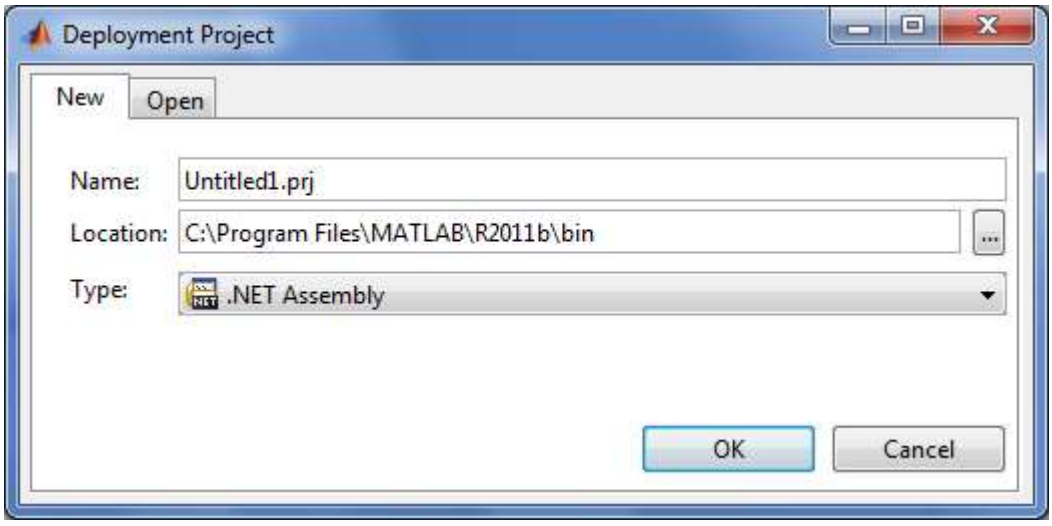


Εικόνα 23: Οθόνη πληροφοριών SQT

6.6 Διεπαφή του SQT με την υπολογιστική μηχανή του MatLab

Για τον υπολογισμό των στοχαστικών ολοκληρωμάτων της προτεινόμενης μεθοδολογίας, αλλά και για την παραγωγή σχεδιαγράμματος αποτύπωσης του επιπέδου της ασφάλειας ενός προϊόντος λογισμικού ή / και ενός συστήματος πληροφορικής, χρησιμοποιήθηκε το μαθηματικό πακέτο MatLab. Όμως, δεν είναι δυνατό να περιμένουμε πως κάθε χρήστης θα έχει, ένα τόσο εξειδικευμένο μαθηματικό πακέτο εγκατεστημένο στον σταθμό εργασίας του. Για το λόγο αυτό λοιπόν, δημιουργήθηκε ένα ειδικό πακέτο εγκατάστασης, της υπολογιστικής μηχανής (MatLab Engine) του MatLab, το οποίο απλά κάθε χρήστης μπορεί να εγκαταστήσει στον σταθμό εργασίας του, για να μπορεί να χρησιμοποιήσει τα εργαλεία και τις δυνατότητες του MatLab.

Για να είναι δυνατή η χρησιμοποίηση αυτού του πηγαίου κώδικα από το σύστημα που υλοποιήθηκε, έπρεπε να χρησιμοποιήσουμε μία από τις δυνατότητες του MatLab και να παράγουμε μία .NET Assembly. Για να το υλοποιήσουμε αυτό, στο command window του MatLab, καλέσαμε το εργαλείο «deploytool», Εικόνα 24.



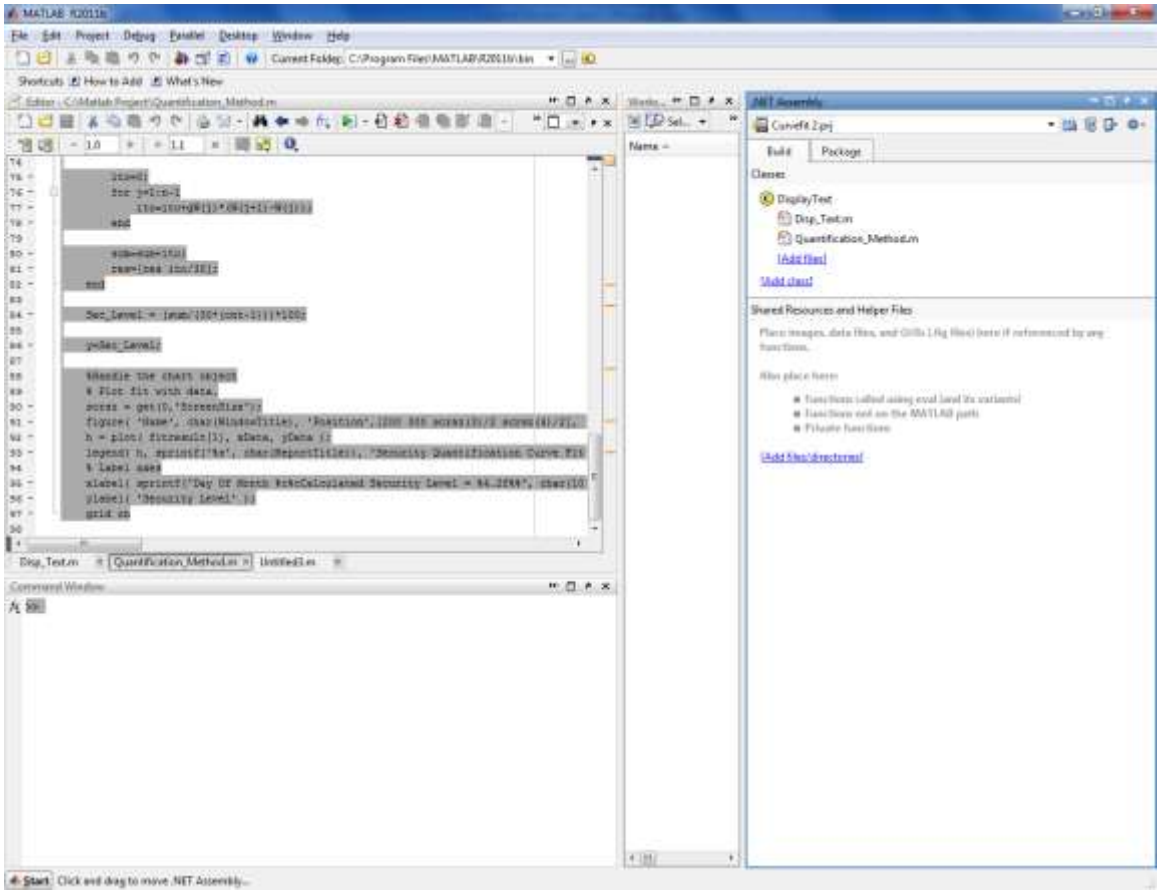
Εικόνα 24: Δημιουργία .NET Assembly από το MatLab

Αφού λοιπόν δημιουργήσαμε ένα Deployment Project, έπρεπε να δημιουργήσουμε την κλάση την οποία θα καλούσαμε μέσα από το σύστημά μας. Την κλάση αυτή

την ονομάσαμε «DisplayText» και της προσθέσαμε δύο μεθόδους τις: α) Disp_Tetx.m και β) Quantification_method.m.

Εδώ πρέπει να σημειωθεί, ότι το MatLab για να προσθέσει μεθόδους σε μία κλάση, αυτές πρέπει να είναι σε ξεχωριστά αρχεία τύπου MatLab script (*.m). Έτσι λοιπόν, υλοποιήσαμε δύο ξεχωριστά αρχεία *.m και μέσα σε αυτά γράψαμε τον πηγαίο κώδικα που θέλαμε να καλέσουμε από την κλάση.

Στη συνέχεια επιλέγοντας την επιλογή «Build» υλοποιήσαμε την κλάση (dll) που θέλαμε να χρησιμοποιήσουμε. Αυτή η κλάση (dll) θα εισαχθεί ως Reference στο SQT. Εν συνεχεία, επιλέγοντας την επιλογή «Package», δημιουργήσαμε το πακέτο εγκατάστασης τόσο της μηχανής του MatLab όσο και της κλάσης που μόλις είχαμε υλοποιήσει, Εικόνα 25.



Εικόνα 25: Δημιουργία αρχείου εγκατάστασης (setup file) του MatLab runtime engine

6.7 Χρήση του SQT

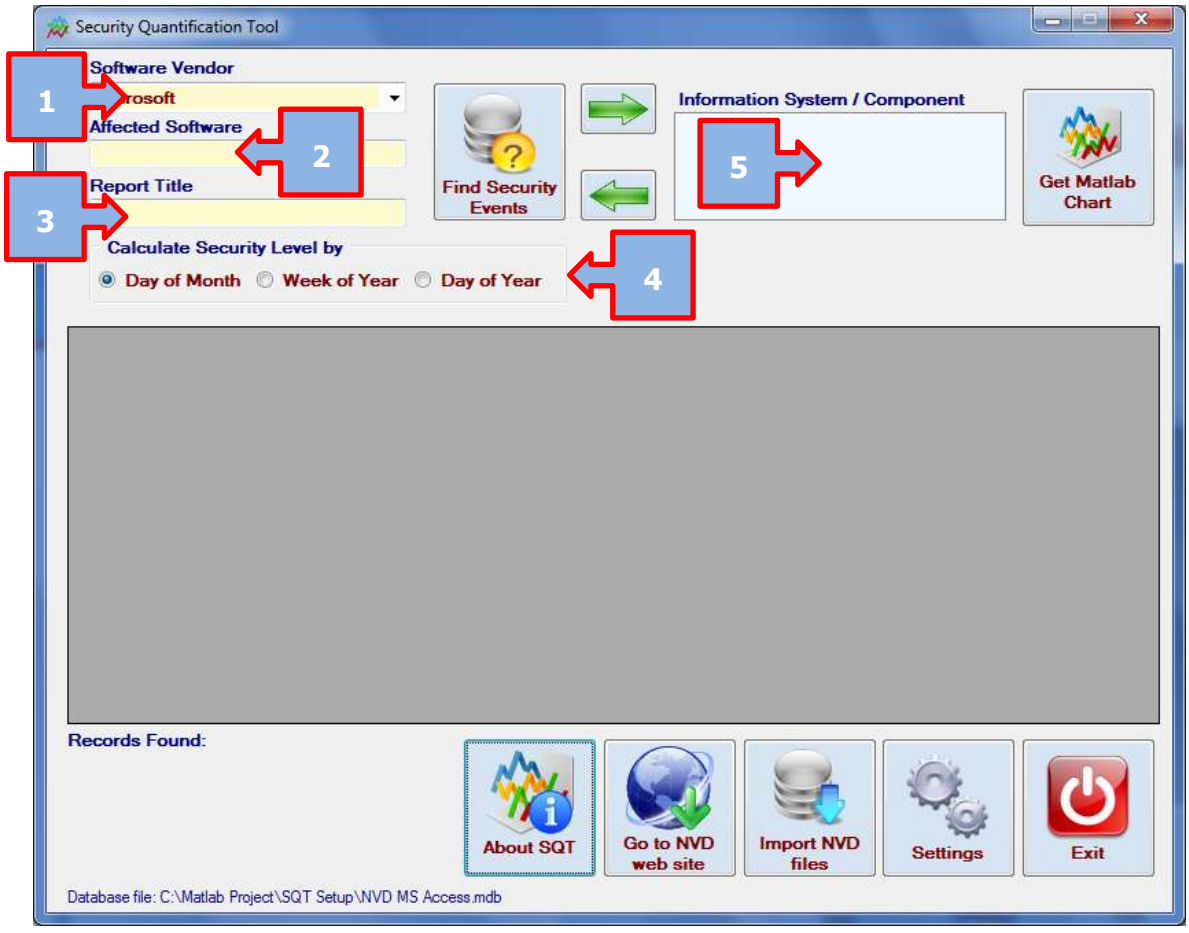
Για να υπολογίσουμε το επίπεδο ασφάλειας ενός προϊόντος πρέπει να το αναζητήσουμε στη βάση δεδομένων με τα στοιχεία από την NVD. Για να το κάνουμε αυτό πρέπει να επιλέξουμε τουλάχιστον ένα από τα δύο στοιχεία του προϊόντος: α) τον κατασκευαστή του ή /και β) το όνομά του. Στη κεντρική οθόνη του SQT, υπάρχει μία λίστα με όλους τους κατασκευαστές λογισμικού, για τους οποίους υπάρχει κάποια ευπάθεια καταχωρημένη (Εικόνα 26, σημείο 1), και ένα πεδίο που μπορούμε να γράψουμε όλο ή κομμάτι από το όνομά του (Εικόνα 26, σημείο 2). Στο σημείο 2, μπορούμε να χρησιμοποιήσουμε και το χαρακτήρα «%» αν δεν ξέρουμε το ακριβές όνομα του προϊόντος. Αν για παράδειγμα θέλαμε να βρούμε όλα τα προϊόντα που περιείχαν την λέξη «windows» αλλά και τον αριθμό 2003, θα γράφαμε στο σημείο 2, «windows%2003».

Πατώντας το κουμπί «Find Security Events», που βρίσκεται στην επάνω αριστερή γωνία της κεντρικής οθόνης του SQT, θα μας εμφανιστούν όλες οι ευπάθειες για το προϊόν που έχουμε επιλέξει στα σημεία 1 & 2. Αν είναι αυτό το προϊόν λογισμικού για το οποίο αναζητούμε το επίπεδο ασφάλειας, πρέπει να πατήσουμε το δεξί πράσινο βελάκι, που εμφανίζεται στην επάνω πλευρά της κεντρικής οθόνης του SQT, έτσι ώστε αυτό να εμφανιστεί πλαίσιο «Information System / Component», (Εικόνα 26, σημείο 5).

Στο σημείο 3, πρέπει να γράψουμε τον τίτλο που επιθυμούμε να εμφανιστεί στο παραγόμενο διάγραμμα του MatLab και να επιλέξουμε το διάστημα υπολογισμού του επιπέδου ασφάλειας, (Εικόνα 26, σημείο 4). Στη συνέχεια πατώντας το κουμπί «Get MatLab Chart», που βρίσκεται στην επάνω δεξιά γωνία της κεντρικής οθόνης του SQT, θα εμφανιστεί το σχετικό διάγραμμα από το MatLab, που θα αποτυπώνει το επίπεδο ασφάλειας του προϊόντος που επιλέξαμε.

Τέλος, αν θέλουμε να υπολογίσουμε το επίπεδο ασφάλειας ενός συστήματος πληροφορικής, πρέπει να το συνθέσουμε, αναζητώντας όλα τα επιμέρους προϊόντα λογισμικού που το απαρτίζουν. Για κάθε ένα προϊόν λογισμικού, ανανεώνουμε τα κριτήρια αναζήτησης, σημεία 1 & 2, και το προσθέτουμε στο πλαίσιο, «Information System / Component», (Εικόνα 26, σημείο 5). Ένα σύστημα πληροφορι-

κής, μπορεί να έχει δύο, τρία ή και περισσότερα προϊόντα λογισμικού. Όταν συνθέσουμε το σύστημα πληροφορικής που θέλουμε να μελετήσουμε, πατάμε το κουμπί «Get MatLab Chart», που βρίσκεται στην επάνω δεξιά γωνία της κεντρικής οθόνης του SQT, και θα εμφανιστεί το σχετικό διάγραμμα από το MatLab, που θα αποτυπώνει το συνολικό επίπεδο ασφάλειας για το σύστημα πληροφορικής που συνθέσαμε.

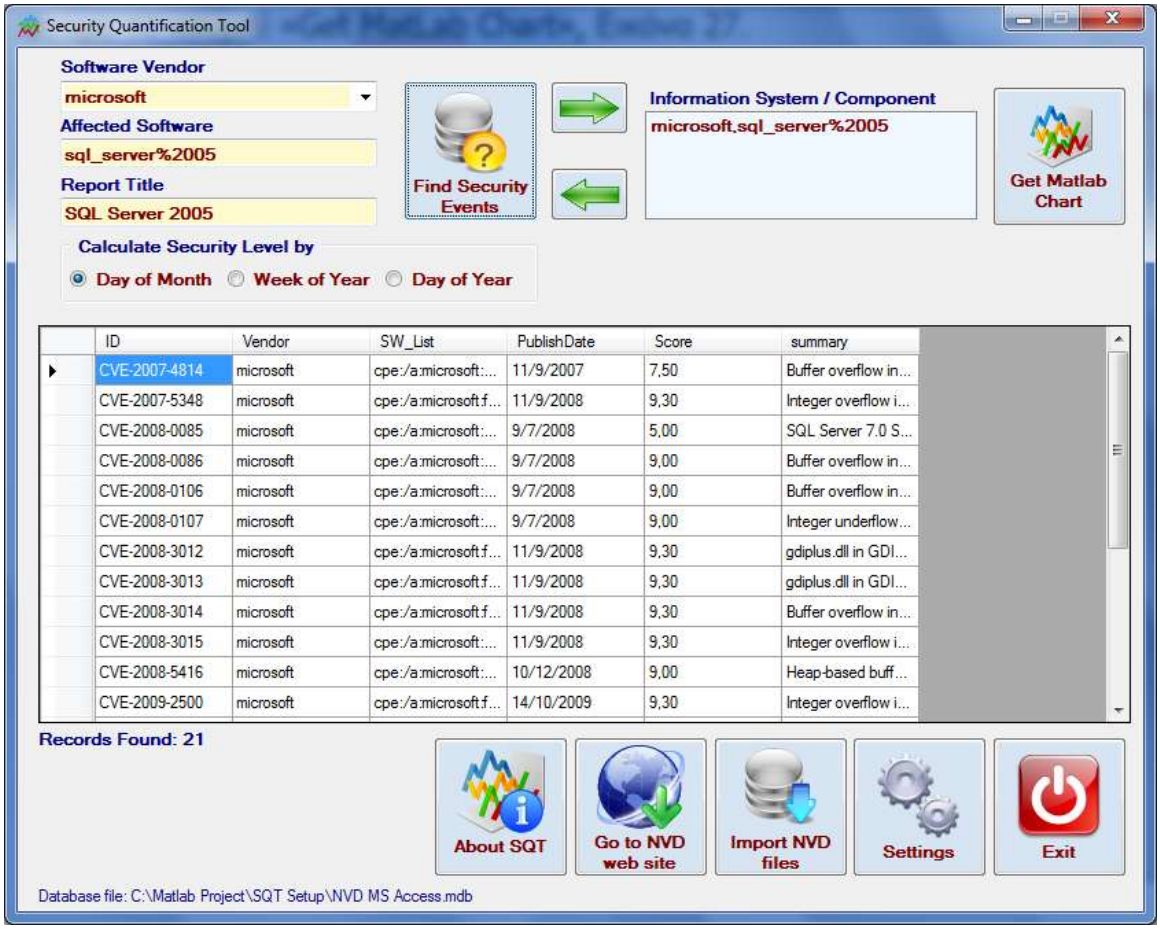


Εικόνα 26: Κεντρική οθόνη του SQT

6.8 Παραδείγματα χρήσης SQT

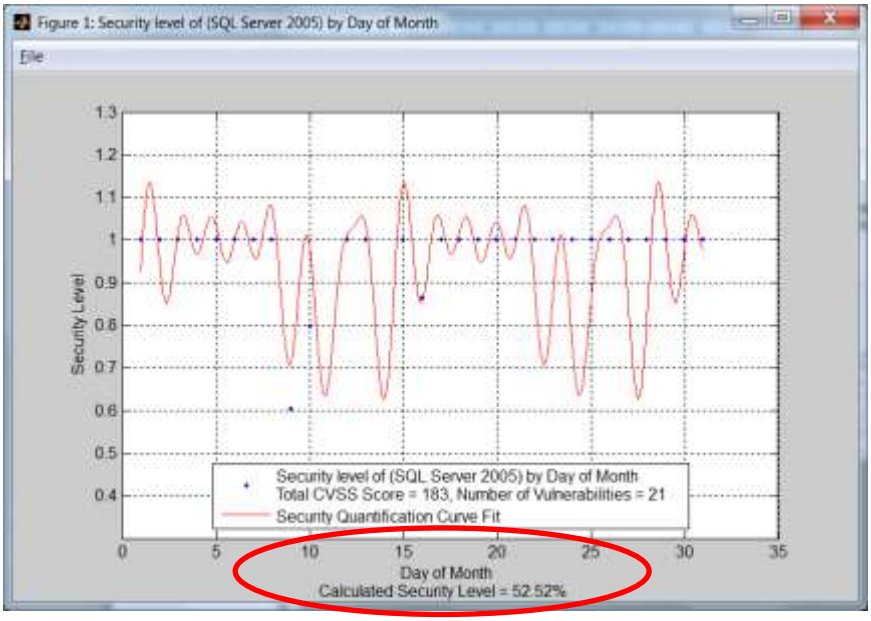
Έστω ότι για παράδειγμα θέλουμε να υπολογίσουμε το επίπεδο ασφαλείας ανά ημέρα του μήνα, του προϊόντος «SQL Server 2005». Τότε στο σημείο 1 θα επιλέξουμε τον κατασκευαστή λογισμικού «Microsoft» και στο σημείο 2, θα γράψουμε

«SQL_Server%2005». Μετά θα το εισάγουμε στο πλαίσιο, σημείο 5, και θα πατήσουμε το κουμπί «Get MatLab Chart», Εικόνα 27.



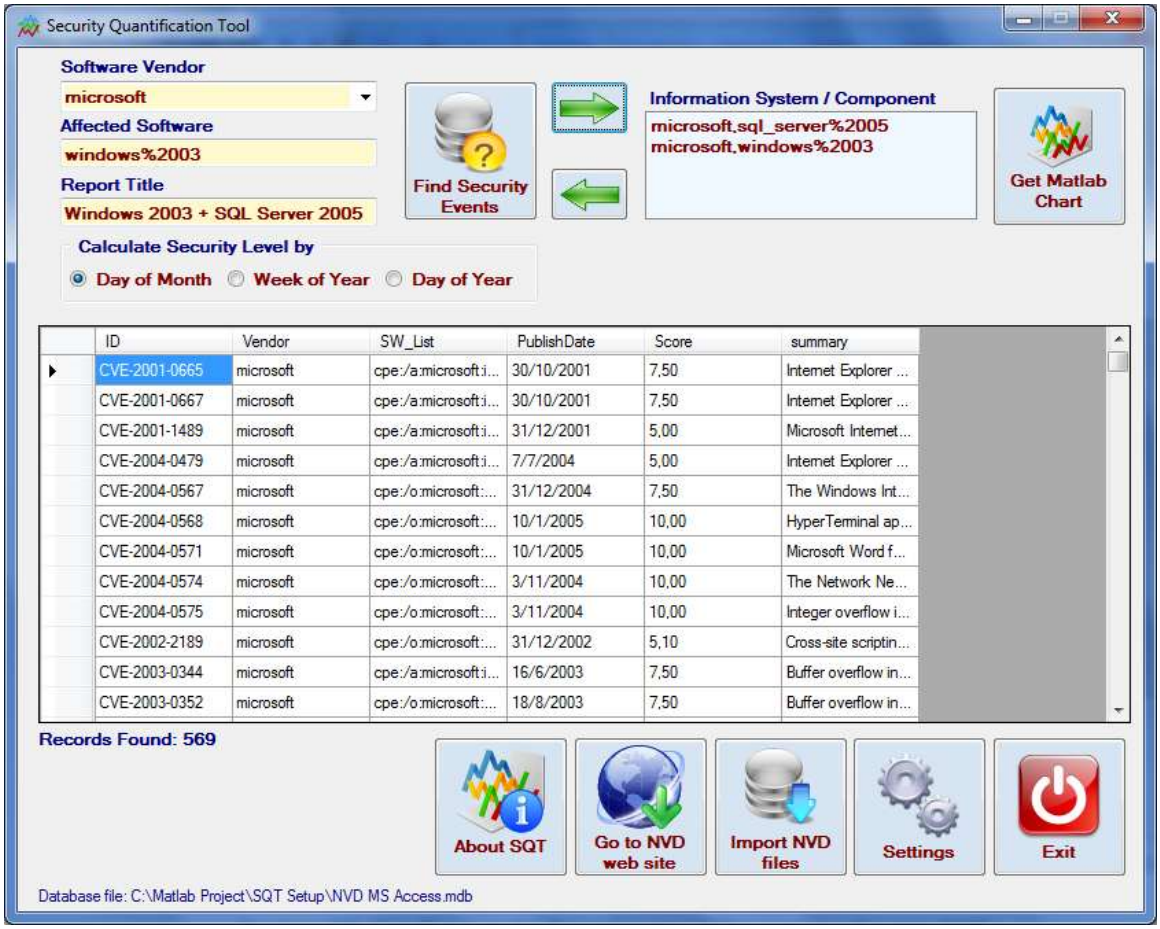
Εικόνα 27: Αναζήτηση δεδομένων στη βάση του SQT

Το αποτέλεσμα του παραπάνω υπολογισμού εμφανίζεται στο παρακάτω διάγραμμα, Διάγραμμα 35, το οποίο υποδεικνύει ότι το επίπεδο ασφάλειας του προϊόντος «SQL Server 2005», είναι 52,52%.



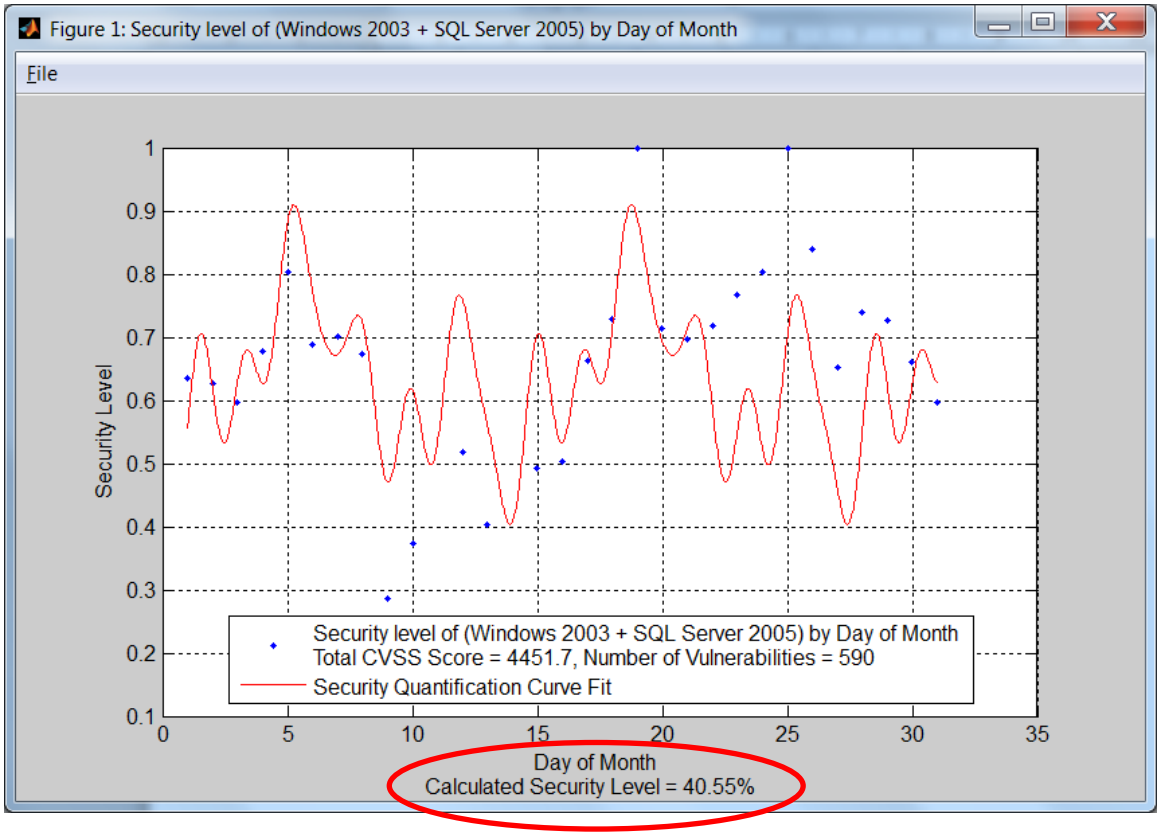
Διάγραμμα 35: Παραγόμενο διάγραμμα για ένα προϊόν λογισμικού από το SQT

Αν στη συνέχεια θέλαμε να μελετήσουμε το επίπεδο ασφαλείας ενός συστήματος πληροφορικής που θα είχε λειτουργικό σύστημα «Windows Server 2003» και εγκατεστημένο ένα «SQL Server 2005», απλά ανανεώνουμε το κριτήρια αναζήτησης σημείο 2, διορθώνουμε τον τίτλο του παραγόμενου διαγράμματος σημείο 3 και το προσθέτουμε στο πλαίσιο, σημείο 5, όπως φαίνεται στην Εικόνα 28.



Εικόνα 28: Σύνθεση ενός Συστήματος Πληροφορικής στο SQT

Στη συνέχεια πατάμε το κουμπί «Get MatLab Chart», και παράγεται το ακόλουθο διάγραμμα, Διάγραμμα 36, όπου απεικονίζεται το ζητούμενο επίπεδο ασφάλειας, 40,55%, για το συγκεκριμένο σύστημα πληροφορικής που συνθέσαμε.



Διάγραμμα 36: Παραγόμενο διάγραμμα για ένα σύστημα πληροφορικής από το SQT

6.9 Σύνοψη

Στο κεφάλαιο αυτό παρουσιάστηκε το πρωτότυπο εργαλείο υπολογισμού του επιπέδου ασφάλειας ενός προϊόντος λογισμικού ή ενός συστήματος πληροφορικής με την ονομασία «Security Quantification Tool (SQT)», που υλοποιεί την προτεινόμενη μεθοδολογία της χρήσης στοχαστικών ολοκληρωμάτων.

Η δημιουργία του SQT, έγινε με γνώμονα το εύχρηστο και πλούσιο περιβάλλον του χρήστη, τη συνεχή ενημέρωσή του από τα αρχεία xml της NVD και την ευκολία εγκατάστασης. Η επίτευξη της ποσοτικοποίησης του επιπέδου της ασφάλειας, που γίνεται μέσω της χρήσης του SQT, θα βοηθήσει σημαντικά όλα τα στελέχη της επιχείρησης που θα το υιοθετήσει, με τη παραγωγή ενός αριθμητικού αποτελέσματος που θα μπορέσει να το χρησιμοποιήσει για να αξιολογήσει ή να συγκρίνει τα συστήματα πληροφορικής που διαθέτει.

ΚΕΦΑΛΑΙΟ 7: Συμπεράσματα - Μελλοντική έρευνα

7. Επίλογος

7.1 Συμπεράσματα

Η μεγάλη ανάπτυξη που συντελείται τα τελευταία χρόνια στον κλάδο της Πληροφορικής, είναι ένα αδιαμφισβήτητο γεγονός. Αυτό όμως με τη σειρά του, δημιουργεί κάποια νέα προβλήματα, όπως για παράδειγμα του ότι οδηγούμαστε σε ολοένα και μεγαλύτερη εξάρτηση από τα συστήματα πληροφορικής των διαφόρων επιχειρήσεων ή / και οργανισμών. Ένα χαρακτηριστικό παράδειγμα του γεγονότος αυτού, είναι η μεγάλη ανάπτυξη της χρήσης του διαδικτύου, που έχει αυξήσει αισθητά, την πολυπλοκότητα των επιθέσεων στις ευπάθειες των υποδομών των συστημάτων πληροφορικής.

Ο αριθμός των επιθέσεων στις πληροφοριακές υποδομές επιχειρήσεων ή / και οργανισμών, έχει επίσης αυξηθεί αισθητά. Το γεγονός αυτό αποδεικνύεται περίτρανα, από τα πέντε εκατομμύρια νέα malware που κυκλοφόρησαν, σε διάστημα μόλις τριών μηνών, το καλοκαίρι του 2011, σύμφωνα με την συγκεντρωτική αναφορά του 3ου τριμήνου του 2011, από τα PandaLabs [102]. Αν στο γεγονός αυτό προσθέσουμε την αύξηση των επιθέσεων ασφαλείας από οργανωμένες ομάδες hacker, όπως Lulsec και Anonymous, καταλαβαίνουμε αμέσως, την αναγκαιότητα διαχείρισης της ασφάλειας των συστημάτων πληροφορικής.

Για να καταφέρουμε όμως επιτυχώς, να διαχειριστούμε την ασφάλεια των συστημάτων πληροφορικής μίας επιχείρησης ή / και οργανισμού, πρέπει πρώτα να μπορούμε να αντιληφθούμε το επίπεδο ασφάλειας στο οποίο βρισκόμαστε και να μπορούμε να κάνουμε προβλέψεις για το που μπορούμε να βρεθούμε. Ένα μέσο για να επιτευχθεί αυτός ο στόχος είναι η ποσοτικοποίηση της ασφάλειας. Για το λόγο αυτό, η κοινότητα των ερευνητών, έχει εισάγει την έννοια των μέτρων (metrics). Η ύπαρξη τέτοιων μέτρων είναι προϋπόθεση:

1. Για την εκτίμηση του ζητούμενου επιπέδου ασφάλειας των συστημάτων πληροφορικής.
2. Για την ανάπτυξη επιχειρησιακών βέλτιστων πρακτικών.
3. Για να βοηθήσει τη μελλοντική έρευνα στον τομέα της ασφάλειας των συστημάτων πληροφορικής.

Η παρούσα έρευνα ως σκοπό είχε να προσεγγίσει το θέμα της ποσοτικοποίησης του επιπέδου της ασφάλειας, ενός συστήματος πληροφορικής, προτείνοντας μία νέα μεθοδολογία μέτρησης. Η προτεινόμενη μεθοδολογία, βασίζεται στη χρήση των στοχαστικών μεθόδων, με σκοπό την παραγωγή ενός αριθμητικού αποτελέσματος, για κάθε δεδομένη στιγμή, που θα μπορεί να χρησιμοποιηθεί σε όλα τα επίπεδα διοίκησης μίας εταιρείας ή / και οργανισμού. Η παραγωγή αριθμητικού αποτελέσματος, ήταν μία από τις κύριες επιδιώξεις της προτεινόμενης μεθοδολογίας, επειδή α) λόγω του αριθμητικού αποτελέσματός της, δεν αφήνει περιθώρια ερμηνείας σε όποιον το χρησιμοποιήσει, β) είναι κατανοητό από τα ανώτερα στελέχη της επιχείρησης, ανεξαρτήτως από το επίπεδο των τεχνικών γνώσεων που διαθέτουν, και γ) η έννοια του δείκτη ο οποίος αλλάζει με την πάροδο του χρόνου, προσφέρει σε όποιον τον χρησιμοποιήσει, τη δυνατότητα να δει τη μεταβολή και δεν αποτελεί ένα απλό αριθμό.

Βασική παραδοχή της έρευνας αυτής, ήταν η υιοθέτηση του όρου «τεχνικός παράγοντας κινδύνου (technical risk factor)», όπως αναφέρθηκε και επεξηγήθηκε στην παράγραφο § 5.1.1. Με την παραδοχή αυτή, επιχειρήθηκε η αποφυγή της ανάλυσης των παραγόντων κινδύνου των συστημάτων πληροφορικής, που είναι βασισμένη στην ταξινόμηση των ευπαθειών και έγινε προσπάθεια δημιουργίας ενός πιο γενικευμένου μοντέλου εκτίμησης κινδύνων.

Με την χρήση της σταθμισμένης εντροπίας, § 5.8, συσχετίσαμε τις ευπάθειες κάθε στοιχείου που συμπεριλαμβάνεται σε ένα σύστημα πληροφορικής, π.χ. το λειτουργικό του σύστημα, με το επίπεδο ασφαλείας του συστήματος που μελετούσαμε, λαμβάνοντας υπόψη:

1. Τον αριθμό των ευπαθειών για κάθε στοιχείο του συστήματος πληροφορικής.
2. Την κατηγορία της επίπτωσης που ανήκε κάθε ευπάθεια (π.χ. Υψηλή, Χαμηλή, Καθόλου).
3. Το χρόνο ανακοίνωσής τους σε σχέση με το χρόνο που το κάθε προϊόν (στοιχείο) ήταν στην αγορά.
4. Το ποσοστό χρησιμοποίησης του στοιχείου στο χρόνο.

Στη συνέχεια, υπολογίσαμε την σταθμισμένη εντροπία που έχει κάθε προϊόν και δώσαμε κάποια αριθμητικά παραδείγματα. Ακολούθησε η προσέγγιση της στοχαστικής συνάρτησης που έχει κάθε προϊόν, μελετώντας τα χρονικά πρότυπα (time patterns) που επιδεικνύουν οι ανακοινώσεις των ευπαθειών του. Τέλος, με τη βοήθεια του μαθηματικού πακέτου MatLab, μπορέσαμε να προσεγγίσουμε με μεγάλη ακρίβεια την καμπύλη ανακοινώσεων των ευπαθειών ενός προϊόντος. Για το σκοπό αυτό χρησιμοποιήθηκε η ανάλυση κατά Fourier με οκτώ βαθμούς ελευθερίας.

Όλα τα παραπάνω, έκαναν εφικτό να ποσοτικοποιήσουμε το επίπεδο ασφάλειας ενός συστήματος πληροφορικής, και να μελετήσουμε, αριθμητικά πλέον, το επίπεδο ασφάλειας γνωστών προϊόντων λογισμικού αλλά και τη συνολική συμπεριφορά, αναφορικά με την ασφάλεια, γνωστών κατασκευαστών λογισμικού, όπως Microsoft και Oracle. Συνεχίζοντας, η παρούσα έρευνα, χρησιμοποίησε την προτεινόμενη μεθοδολογία για να συγκρίνει δύο συστήματα πληροφορικής και να εξάγει χρήσιμα συμπεράσματα. Τα αποτελέσματα της ερευνητικής προσπάθειας, φαίνεται να επιβεβαιώνονται εμπειρικά, και από άλλες, ευρέως γνωστές και αποδεκτές, μεθοδολογίες όπως η Common Vulnerability Scoring System (CVSS) που αναφέρθηκε στην παράγραφο § 4.10.4. Τελειώνοντας, αναπτύξαμε ένα πρότυπο εργαλείο υπολογισμού του επιπέδου ασφάλειας ενός προϊόντος λογισμικού ή ενός συστήματος πληροφορικής. Με τη χρήση αυτού του εργαλείου, γίνεται άμεσα αντιληπτή η χρησιμότητα της προτεινόμενης μεθοδολογίας, αφού κάθε χρήστης

μπορεί από μόνος του να εξαγάγει χρήσιμα αριθμητικά συμπεράσματα αναφορικά με το προϊόν λογισμικού ή συστήματος πληροφορικής που μελετά.

Ο υπολογισμός του επιπέδου ασφαλείας ενός συστήματος πληροφορικής με την προτεινόμενη μεθοδολογία, έχει πολλά οφέλη που μπορούν να συνοψιστούν ακολούθως:

1. Έχουμε τη δυνατότητα, να συγκρίνουμε μεταξύ τους διαφορετικά συστήματα πληροφορικής, δημιουργώντας ένα κοινό σημείο αναφοράς.
2. Έχουμε τη δυνατότητα, να εφαρμόσουμε την προτεινόμενη μέθοδο, τόσο σε μία υπηρεσία ή / και εφαρμογή, όσο και σε ένα σύστημα πληροφορικής.
3. Η μεθοδολογία ξεπερνά το πρόβλημα της ύπαρξης ικανού αριθμού συμβάντων ασφαλείας (security breaches) για να λειτουργήσει, με τη χρήση της εντροπίας της πληροφορίας.
4. Η μεθοδολογία χρησιμοποιεί τον παράγοντα του χρόνου, που δεν λαμβανόταν υπόψη, από τις υπάρχουσες μεθοδολογίες εκτίμησης κινδύνων.
5. Ο σχεδιασμός της μεθοδολογίας, εξασφαλίζει αμερόληπτο και μη αμφισβητήσιμο αποτέλεσμα αφού είναι ένας αριθμός, ο οποίος βασίζεται σε επίσημες ανακοινώσεις ευπαθειών.
6. Το αποτέλεσμα της μεθόδου μπορεί να χρησιμοποιηθεί σε όλα τα επίπεδα διοίκησης μίας εταιρείας ή / και οργανισμού, ανεξαρτήτως του επιπέδου των τεχνικών γνώσεων που διαθέτουν.
7. Η μέθοδος αυτή, μπορεί να χρησιμοποιηθεί για την εκτίμηση μελλοντικών επενδύσεων στον τομέα της πληροφορικής, αξιολογώντας το κομμάτι της ασφάλειας, με αποτέλεσμα την εξοικονόμηση μεγάλων ποσών.

8. Η μέθοδος αυτή μπορεί να χρησιμοποιηθεί για την αμερόληπτη αξιολόγηση ανταγωνιστικών προτάσεων σε διαγωνισμούς οργανισμών, αξιολογώντας το κομμάτι της ασφάλειας του προτεινόμενου συστήματος πληροφορικής.

7.2 Μελλοντική έρευνα

Η παρούσα διατριβή είναι το αποτέλεσμα μίας έρευνας σε μία σειρά θεμάτων, που έχουν να κάνουν με την εκτίμηση κινδύνων και την ποσοτικοποίησή τους. Έγινε μία προσπάθεια να συσχετιστούν δύο εντελώς διαφορετικοί τομείς έρευνας, α) της διαχείρισης των κινδύνων και β) της ασφάλειας των συστημάτων πληροφορικής, με τη χρήση των στοχαστικών μεθόδων. Ο σκοπός ήταν να συγκεραστούν οι ανάγκες και των δύο, αφενός για τη διαχείριση των κινδύνων και αφετέρου για την ύπαρξη ενός τρόπου μέτρησης της ασφάλειας, το αποτέλεσμα του οποίου θα είχε ως χαρακτηριστικά: α) την ακρίβεια των μετρήσεων και β) την αμεροληψία.

Η παρούσα έρευνα όμως, αφήνει μία σειρά από ανοικτά θέματα, τα οποία θα μπορούσαν να αποτελέσουν πόλο έλξης για μελλοντικούς ερευνητές.

Ένα πολύ ενδιαφέρον πεδίο έρευνας, θα είναι η εμπειρική επαλήθευση του προτεινόμενου μοντέλου εκτίμησης κινδύνων, με στοιχεία από μία επιχείρηση ή / και οργανισμό. Θα είχε ιδιαίτερο ενδιαφέρον ένας ερευνητής, να μπορούσε να εφαρμόσει την προτεινόμενη μεθοδολογία στα συστήματα πληροφορικής μίας εταιρείας ή / και οργανισμού, χρησιμοποιώντας την πραγματική σύνθεση των εξυπηρετητών και των συστημάτων πληροφορικής που διαθέτουν, και να τη διασταυρώσει με τα αποτελέσματα της προτεινόμενης μεθοδολογίας.

Ένα επίσης ενδιαφέρον πεδίο έρευνας, θα είναι η χρησιμοποίηση των αποτελεσμάτων της προτεινόμενης μεθοδολογίας, ως δεδομένα εισόδου σε κάποια μέθοδο πρόβλεψης (forecasting). Ένας ερευνητής, θα μπορούσε να χρησιμοποιήσει τα αριθμητικά αποτελέσματα της μεθόδου και να προσπαθήσει να προσδιορίσει μελλοντικά συμβάντα ασφαλείας, χρησιμοποιώντας μια μέθοδο της πρόβλεψης (forecasting), όπως για παράδειγμα Ανάλυση Παλινδρόμησης (Regression Analysis) ή /

και Ελαχίστων Τετραγώνων (Least Squares Analysis) ή ακόμα και περισσότερα εργαλεία από τα χρηματοοικονομικά.

Η προτεινόμενη μεθοδολογία, όπως αναφέρθηκε, λαμβάνει υπόψη της τους τεχνικούς παράγοντες κινδύνου (technical risk factors). Μία φυσική εξέλιξη της μεθόδου θα ήταν η ενσωμάτωση και άλλων παραμέτρων, όπως παράγοντες κινδύνου επιχειρησιακής λειτουργίας ή / και φυσικής ασφάλειας. Επίσης, θα ήταν πολύ ενδιαφέρον η ενσωμάτωση στο προτεινόμενο μοντέλο και των μέτρων προστασίας για την ασφάλεια των πληροφοριών που έχει εφαρμόσει η επιχείρηση, όπως προγράμματα προστασίας από ιούς, Intrusion Detection Systems, Intrusion Prevention Systems, firewalls κτλ. Αυτό θα είχε ως αποτέλεσμα μια ανάλυση συμβάντων (event based analysis), αναφορικά με το τί συμβαίνει σε μία εταιρεία, γεγονός που θα οδηγούσε σε πιο ακριβή μέτρηση του επιπέδου ασφάλειας ενός συστήματος πληροφορικής.

Η μετεξέλιξη του πρότυπου εργαλείου SQT που αναπτύχθηκε, σε ένα ολοκληρωμένο πληροφοριακό σύστημα ή μίας διαδικτυακής υπηρεσίας, που θα υλοποιούσε την προτεινόμενη μέθοδο, και θα κρατούσε ιστορικό μετρήσεων για περαιτέρω στατιστική επεξεργασία και θα παρείχε μία σειρά από στατιστικά γραφήματα, θα αποτελούσε ένα πολύ ενδιαφέρον ερευνητικό έργο. Το σύστημα ή / και διαδικτυακή υπηρεσία θα λάμβανε ως δεδομένα εισόδου, την τεχνική περιγραφή του συστήματος πληροφορικής που θέλουμε να εκτιμήσουμε, και θα μας παρείχε το αμερόληπτο και αντικειμενικό αποτέλεσμα του επιπέδου της ασφάλειας του συστήματος που μελετάμε μαζί με μία σειρά από στατιστικά γραφήματα που θα αποτύπωναν την ιστορική εξέλιξη του επιπέδου ασφάλειας. Αυτό το σύστημα ή / και διαδικτυακή υπηρεσία, θα μπορούσε να χρησιμοποιηθεί από κάποιον οργανισμό, για τυχόν νέες παραγγελίες συστημάτων πληροφορικής, με γνώμονα την επίτευξη της μεγαλύτερης δυνατής ασφάλειας των συστημάτων πληροφορικής, στα οποία πρόκειται να επενδύσει και την εξοικονόμηση οικονομικών πόρων, αφού η επιχείρησης θα γλύτωνε το κόστος από πιθανές παραβιάσεις ασφαλείας.

Τέλος, το προτεινόμενο μοντέλο ποσοτικοποίησης του επιπέδου ασφαλείας ενός συστήματος πληροφορικής μπορεί να χρησιμοποιηθεί ως επί μέρους μεταβλητή εισόδου για την προσέγγιση της πιθανότητας εμφάνισης περιστατικών παραβιά-

σεων ασφαλείας. Επιπρόσθετα, υφίσταται ένα ερευνητικό ρεύμα εκτίμησης του κόστους παραβιάσεων ασφαλείας με την χρήση της μεθοδολογίας ανάλυσης γεγονότων (event analysis methodology). Χαρακτηριστικές μελέτες αυτού του είδους είναι οι [103], [104], [105] στις οποίες αποτυπώνονται οι πρόσφατες εξελίξεις στην χρήση της συγκεκριμένης μεθοδολογίας για την εκτίμηση του κόστους παραβιάσεων ασφαλείας. Τα εμπειρικά αποτελέσματα αυτού του είδους μελετών, σε συνδυασμό με την προσέγγιση της πιθανότητας παραβιάσεων ασφαλείας, μέσω της χρήσης του προτεινόμενου μοντέλου ποσοτικοποίησης του επιπέδου ασφαλείας αλλά και λοιπών επεξηγηματικών μεταβλητών, μπορούν να αποδώσουν ποσοτικές εκτιμήσεις για το επίπεδο των κινδύνων παραβιάσεων ασφαλείας ενός οργανισμού. Η χρήση στοχαστικών μεθόδων για την ποσοτικοποίηση της ασφάλειας καθώς και η χρήση της ανάλυσης γεγονότων για την εκτίμηση του κόστους παράγουν αντικειμενικά αποτελέσματα και συνεπώς ο συνδυασμός τους για την εκτίμηση των κινδύνων παραβιάσεων ασφαλείας αποτελεί ένα πολύ ενδιαφέρον ερευνητικό αντικείμενο καθώς μπορεί να αποφέρει ποσοτικά, αντικειμενικά αποτελέσματα με ευρεία χρήση μέσα στη διοικητική δομή ενός οργανισμού.

Τα παραπάνω θέματα, αποτελούν κάποιες και σαφώς όχι όλες, από τις πιθανές επεκτάσεις του ερευνητικού πεδίου της παρούσας διατριβής. Κάθε μελλοντική ερευνητική προσπάθεια, που θα δοκιμάσει να δώσει λύση σε ένα τόσο κρίσιμο θέμα όσο η ποσοτικοποίηση της ασφάλειας ενός συστήματος πληροφορικής, θα πρέπει να έχει υπόψη της, ότι η επιχειρηματική κοινότητα έχει άμεση ανάγκη από τη λύση του προβλήματος αυτού, και θα επιδοκίμαζε την προσπάθεια.

Λεξικό όρων

Ξένος όρος	**Μετάφραση όρου**
Availability	Διαθεσιμότητα. Αποτελεί μία από τις κύριες επιδιώξεις για την ασφάλεια ενός συστήματος πληροφορικής.
Automated tools	Αυτοματοποιημένα εργαλεία.
***B*otnets**	Ελεγχόμενα δίκτυα από hackers.
BPEST	Μεθοδολογία αποτίμησης κινδύνων σε μία επιχείρηση που περιλαμβάνει επιχειρηματικούς, πολιτικού, οικονομικούς, κοινωνικούς, και τεχνολογικούς κινδύνους
Confidentiality	Εμπιστευτικότητα. Αποτελεί μία από τις κύριες επιδιώξεις για την ασφάλεια ενός συστήματος πληροφορικής.
Counter measures	Αντίμετρα
Database	Βάση δεδομένων
Density functions	Συναρτήσεις πυκνότητας
Effectiveness	Αποτελεσματικότητα
Efficiency	Αποδοτικότητα
Enterprise risk management	Συνολική Διαχείριση Κινδύνων μιας επιχείρησης
Event Based Analysis	Ανάλυση συμβάντων
Expected losses	Αναμενόμενες ζημίες
Hardware	Υλικό
Impact measures	Μέτρα μέτρησης των επιπτώσεων
Information Communication Technology products	Προϊόντα νέας τεχνολογίας, πληροφορικής και επικοινωνιών
Integrity	Ακεραιότητα. Αποτελεί μία από τις κύριες επιδιώξεις για την ασφάλεια ενός συστήματος πληροφορικής.

Ξένος όρος	**Μετάφραση όρου**
IT Governance	Ηλεκτρονική διακυβέρνηση
Least Squares Analysis	Ελαχίστων Τετραγώνων
Malware	Προγράμματα με σκοπό τη διακοπή λειτουργίας του υπολογιστή στον οποίο εγκαθίστανται.
Maintainability	Συντηρησιμότητα. Αποτελεί ένας από τους κυριότερους παράγοντες για ένα σύστημα πληροφορικής
Open source	Ανοικτού κώδικα
Organizational Information Security Management	Οργάνωση και διαχείριση της πληροφορίας μιας επιχείρησης
Patterns	Πρότυπα. Αναφερόμαστε στα χρονικά πρότυπα συμπεριφοράς που εμφανίζουν οι ευπάθειες των προϊόντων λογισμικού που μελετήθηκαν.
Performance measurement	Μέτρηση των επιδόσεων
Privacy	Ιδιωτικότητα
Proactive	Προληπτική
Product Development	Κατασκευή προϊόντων
PESTLE	Μεθοδολογία αποτίμησης κινδύνων σε μία επιχείρηση που περιλαμβάνει πολιτικούς, οικονομικούς, κοινωνικούς, τεχνολογικούς, νομικούς και περιβαλλοντικούς κινδύνους
Qualitative distinction	Ποιοτική διάκριση. Τη χρησιμοποιούμε για να θέσουμε διαφορετικές τιμές, στους διάφορους παράγοντες κινδύνου, ενός συστήματος πληροφορικής.
Random Walk	Τυχαίο περίπατο
Randomness	Τυχαιότητα
Regression Analysis	Ανάλυση παλινδρόμησης

Ξένος όρος	**Μετάφραση όρου**
Reliability	Αξιοπιστία. Αποτελεί ένας από τους κυριότερους παράγοντες για ένα σύστημα πληροφορικής
Resource management	Διαχείρισης των πόρων
Risk Management	Διαχείριση Κινδύνων
Safety	Ασφάλεια. Αποτελεί ένα από τους κυριότερους παράγοντες για ένα σύστημα πληροφορικής
Security breach	Παραβίαση ασφαλείας
Server	Εξυπηρετητής
Software	Λογισμικό
Strategic alignment	Εναρμόνιση των διαφόρων στρατηγικών μίας επιχείρησης ή ενός οργανισμού
SWOT	Μια μέθοδο στρατηγικής που χρησιμοποιείται για να αποτιμήσει τα δυνατά, αδύνατα σημεία μίας επιχείρησης, καθώς και τις ευκαιρίες και τις απειλές που μπορεί να έχει στον κλάδο που δραστηριοποιείται
Unbiased	Αμερόληπτα
Value delivery	Παραγωγή προστιθέμενης αξίας στην επιχείρηση μέσω διαδικασιών
Vulnerability	Ευπάθεια
Vulnerability Disclosure Date	Ημερομηνία ανακοίνωσης ευπάθειας σε ένα προϊόν λογισμικού
Web service	Διαδικτυακή υπηρεσία
Weighted Entropy	Σταθμισμένη εντροπία
Value at Risk	Ο όρος αυτός χρησιμοποιείται στα οικονομικά, ως μέτρο για την αποτίμηση του κινδύνου ζημιάς σε ένα συγκεκριμένο χαρτοφυλάκιο ενός οικονομικού πόρου.

Πίνακας 28: Λεξικό όρων

Πηγές – Βιβλιογραφία

[1] Committee of Sponsoring Organizations of the Treadway Commission, Internal Control—Integrated Framework, 2006.

[2] (2011, January) Pingdom Blog. [Online]. http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/

[3] (2012, June) Netcraft. [Online]. http://news.netcraft.com/archives/2012/

[4] Gartner. (2012, March) Worldwide IT spendings forecast. [Online]. http://blogs.wsj.com/tech-europe/2012/01/05/it-global-spending-forecast-cut/

[5] R. N. Charette, "Why software fails?," in *IEEE Spectrum*, 2006.

[6] Detica, "The cost of cyber crime," , 2011.

[7] Holton H. A., "Defining risk," *Financial Analyst Journal*, vol. 60, no. 6, pp. 19-25, 2004.

[8] Ernst & Young, The top 10 risks for business, 2010.

[9] The IT Service Management Forum, *IT Infrastructure Library (ITILv3)*, Alison Cartlidge and Mark Lillycrop, Eds.: The UK Chapter of the itSMF, 2007.

[10] ENISA. (2005, September 1) European Network and Information Security Agency. [Online]. http://www.enisa.europa.eu/

[11] ISO/IEC 27005:2008, "Information technology -- Security techniques -- Information security risk management," International Organization for Standardization, Geneva, Switzerland, 2008.

[12] Information Systems Audit and Control Association (ISACA), The Risk IT Framework, 2009.

[13] Information Systems Audit and Control Association (ISACA), IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals, 2010.

[14] Goguen A., Feninga A., and Stonebumer G., "Risk management guide for information technology systems," NIST, 2001.

[15] National Institute of Standards and Technology Special Publication #800-39, "Managing information security risk," 2011.

[16] B. W. Boehm, "Software risk management: Principles and practices," vol. 8, no. 1, 1991.

[17] David G.W. Birch and Neil A. McEvoy, "Risk analysis for information systems," *Journal of Informatin Technology*, vol. 7, pp. 44-53, 1992.

[18] Institute of Risk Management, "Risk Management Standard," 2002.

[19] Jake Koons and Daniel Minoli, *Information Technology Risk Management in Entreprise Environments*.: John Wiley and Sons, Inc, 2010.

[20] John R. Vacca, *Computer and Information Security handbook*.: Morgan Kaufmann, 2009.

[21] Merrill Warkentin and Rayford Vaughn, *Information System Assurance and System Security: Managerial and Technical Issues*.: Idea Group Inc, 2006.

[22] Kabay M.E. and Bosworth S., *Computer Security Handbook*.: John Wiley & Sons, Inc, 2002.

[23] Ενδιάμεση έκθεση για τη χρηματοπιστωτική σταθερότητα Τράπεζα της Ελλάδος. (2009, Δεκ.) http://www.bankofgreece.gr/BogEkdoseis/fstability200912.pdf ανακτήθηκε στις 6-6-2011. [Online]. www.bankofgreece.gr

[24] "Κίνηση Brown," *Scientific American Ελληνκή Έκδοση*, Feb. 2006.

[25] Fima C. Klebaner, *Introduction to Stochastic Calculus with Applications*.: Imperial College Press, 2005.

[26] X. Mao, *Stochastic Differential Equations and Applications Horwood Series in Mathematics and Applications*, Horwood Publishing Chichester ed., 1997.

[27] Defense Technical Information Center's (DTIC) and Information Assurance Technical Analysis Center(IATAC), "IA Metrics," 2001.

[28] National Institute of Standard and Technology, "Performance Measuremnet Guide for Infromation Security," NIST SP 800-55 2003.

[29] National Institute of Standards and Technology, "Performance Measurement Guide from Information Security Revision 1," NIST SP 800-55 Rev. 1 2008.

[30] ISO/IEC 27004:2009, "Information Technology - Security techniques - Information Management - ISMS Measurement," International Organization for Standarization, Geneva, Switzerland, 2009.

[31] ISO/IEC 15939:2007, "Systems and Software engineering - Measurement process," International Organization for Standarization, Geneva, Switzerland, 2007.

[32] Stuart Edward Schechter, "Toward Econometric Models of the Security Risk

from Remote Attack," *IEEE Security & Privacy*, vol. 3, no. 1, pp. 40-44, January/February 2005.

[33] Nguyen Pham, Loic Baud, Patrick Bellot, Michel Riguidel, and Telecom ParisTech, "A Near Real-time System for Security Assurance Assessment", in Proceedings of the Third International Conference on Internet Monitoring and Protection (ICIMP 2008), Bucharest, Romania, 29 June-5 July 2008.

[34] IT Governance Institute, COBIT 4.1, 2007.

[35] IT Governance Institute, IT using governance COBIT and VAL IT, 2007.

[36] Software Assurance Community Resource and Information Clearinghouse Measurement Working Group. (2009, April) [Online]. https://buildsecurityin.us-cert.gov/swa/measwg.html

[37] National Institude of Standards and Technology, "Recommended Security Controls for Federal Information Systems and Organizations," NIST SP 800-53 2008.

[38] US-CERT, Briefings from Workshop on Assurance with CMMI, August 2007.

[39] Rini van Solingen and Egon Berghout, *The Goal/Question/Metric Method: a practical guide for quality improvement of software development*.: McGraw-Hill, 1999.

[40] Plumtree Portal. [Online]. http://www.plumtree.com

[41] Symbiot Security. [Online]. http://www.symbiot.com/riskmetricsolutions.html

[42] CSAM and ASSERT OMB Security Line of Business Solutions. [Online]. http://csrc.nist.gov/groups/SMA/fisma/ support_tools.html

[43] Trusted Agent. [Online]. http://www.trustedintegration.com

[44] Splunk. [Online]. http://www.splunk.com/article/2307

[45] Klocwork Insight. [Online]. http://www.klocwork.com/products/insight.asp

[46] Ounce Suite. [Online]. http://www.ouncelabs.com/products

[47] Fortify Suite. [Online]. http://www.fortify.com/products/detect

[48] IBM Cognos software. Business intelligence and performance management. [Online]. http://www-01.ibm.com/software/analytics/cognos/

[49] CORDA. Real-time access to enterprise data, via performance dashboards from any location. [Online]. http://www.corda.com

[50] Clear Point Metrics. Security Performance Manager. [Online]. http://www.clearpointmetrics.com

[51] DHS-DoD-DoC, Software Assurance Forum Measurement Working Group Status Briefing, May 2008.

[52] Software Assurance (SwA) Measurement Working Group. [Online]. https://buildsecurityin.us-cert.gov/swa/measresrc.html

[53] Donald L. Buckshaw et al., "Mission Oriented Risk and Design Analysis of Critical Information Systems," *Military Operations Research*, vol. 10, no. 2, November 2005, Accessed 14 April 2009 at: http://www.mors.org/awards/mor/2006.pdf.

[54] Donald L. Buckshaw et al., "Mission Oriented Risk and Design Analysis of Critical Information Systems," *Military Operations Research,* vol. 10, no. 2,

November 2009.

[55] CIS, Clint Kreitner, "The CIS Security Metrics and Benchmarking Service," in *Metricon 3.0, San Jose*, California, 29 July 2008.

[56] CIS, The CIS Security Metrics, May 2009.

[57] W. Krag Brotby, *IT Governance Institute. Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd ed.: Rolling Meadows, IL: ISACA, 2006.

[58] John P. Pironti, "Developing Metrics for Effective Information Security Governance," *Information Systems Control Journal*, vol. 2, April 2009.

[59] Akridge, Chapin David, and Steven David, "How Can Security Be Measured," *Information Systems Control Journal*, vol. 2, February 2009.

[60] Security Standards Council, Payment Card Industry (PCI) Data Security Standard, Security Scanning Procedures Version 1.1, September 2006.

[61] ISO/IEC 27002:2005, "Information technology - Security techniques - Code of practice for information security management," International Organization for Standarization, Geneva, Switzerland, 2005.

[62] Deepti Juneja, Kavita Arora, and Sonia Duggal, "Developing Security Metrics for Information Security Measuring System," *International Journal of Enterprise Computing and Business Systems,* vol. 1, no. 2, July 2011.

[63] Reijo Savola, "Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry," 2007.

[64] I3P Institude for Infromation Protection, "Better Security through Risk

Pricing," 2010.

[65] Applied Computer Security Associates and The MITRE Corporation, "Workshop on Information Security System Scoring and Ranking Information System Security," , Williamsburg, Virginia, 2009.

[66] ISO/IEC 17799:2005, "Information technology – Security techniques – Code of practice for information security management," International Organization for Standarization, Geneva, Switzerland, 2005.

[67] ISO/IEC 27001:2005, "Information technology - Security techniques - Information security management systems - Requiremnets," International Organization for Standarization, Geneva, Switzerland, 2005.

[68] (ISA) and American National Standards Institute (ANSI) International Society of Automation, Security Technologies for Manufacturing and Control Systems, 2004.

[69] Peter Pieda, Ashraf Matrawy, Biswajit Nandy, John Lambadaridis, Adam Hatfield, Nabil Seddigh, Current Trends and Advances in Information Assurance Metrics, 2004.

[70] Vaughn, Rayford, Ambareen Siraj, and David Dampier, "Information Security System Rating and Ranking, CROSSTALK, The Journal of Defense Software Engineering," pp. 30-32, May 2002.

[71] Pratyusa K. Manadhata and Jeannette M. Wing, An Attack Surface Metric, IEEE Transactions on Software Engineering, 2010.

[72] Alhazmi OH et al., Measuring, analyzing and predicting security vulnerabilities in software systems, Computers & Security, doi:10.1016/j.cose.2006.10.002, 2006.

[73] David R. Kaeli, Vilas Sridharan, Quantifying Software Vulnerability, 2008.

[74] Lawrence Carin, George Cybenko, and Jeff Huges, Quantitative Evaluation of Risk for Investment Efficient Strategies in Cybersecurity: The QuERIES Methodology, 2007.

[75] Victor-Valeriu Patriciu, Iustin Priescu, and Sebastian Nicolaescu, "New approaches and Prespectives in the use of Quantitative Methods," *Journal of Applied Quantitative Methods,* vol. 1, no. 2, 2006.

[76] Cisco Systems Inc., Mike Schiffman, The Common Vulnerability Reporting Framework, 2011.

[77] Εμμανουήλ Δ. Σερέλης, Διαχείριση Κρίσιμων Πληροφοριακών Υποδομών με τη Χρήση Μεθόδων Ποσοστικοποίησης της Ασφάλειας, 2009.

[78] OpenVAS. Open Vulnerability Assessment System. [Online]. http://www.openvas.org

[79] MSBSA. Microsoft Baseline Security Analyzer. [Online]. http://www.microsoft.com/en-gb/download/details.aspx?id=7558

[80] Nessus. Vulnerability scanner. [Online]. www.nessus.org

[81] US Congress, H.R. 2548-48, Federal Information Security Management Act, 2002.

[82] Insight Consulting, CRAMM User Guide, Issue 5.1, 2005 , United Kingdom.

[83] Carnegie Mellon University. (2001, June (accessed August 2012)) OCTAVE Method Implementation Guide Version 2.0. [Online]. http://www.cert.org/octave

[84] Crespo F., Gomez M., Candau J., and Manas J.A., *MAGERIT - version 2, Methodology for Information Systems Risk Analysis and Management, Books I - The Method*.: Ministerio de Administraciones Publicas, June 2006.

[85] Crespo F., Gomez M., Candau J., and Manas J.A., *MAGERIT - version 2, Methodology for Information Systems Risk Analysis and Management, Books II - Catalogue of Elements*.: Ministerio de Administraciones Publicas, June 2006.

[86] Crespo F., Gomez M., Candau J., and Manas J.A., *MAGERIT - version 2, Methodology for Information Systems Risk Analysis and Management, Books III - Techniques*.: Ministerio de Administraciones Publicas, June 2006.

[87] PREMIER MINISTRE Secretariat general de la defence nationale Direction centrale de la securite des systems d'informatin Sous-direction des operations Bureau conseil. Expression of Needs and Identification of Security Objectives. Available at: www.ssi.gouv.fr, (accessed August 2012).

[88] Club de la Securite de L' information Francais Methods Commision, "Mehari 2010 Risk analysis and treatment Guide," France, http://www.clussif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Risk-Analysis-and-Treatment-Guide.pdf August 2010 (accessed December 2010).

[89] Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Nikolaos Alexandris, and Evangelos Fountas, "Towards a formalistic measuring of security using stochastic calculus," in *2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010), Chengdu, China, July 9-11 2010*, p. 4.

[90] Sung-Whan Woo, Yashwant K. Malaiya Omar H. Alhazmi, Security

vulnerability categories in major software systems.

[91] Emmanouil Serrelis and Nikolaos Alexandris, "An Empirical Model for Quantifying Security based on Services," in *2nd Internation Multi-Conference on Computing in the Global Information Technology (ICCGI 2007)*, 2007, p. 30.

[92] OSVDB. Open Source Vulnerability Database. [Online]. http://osvdb.org/

[93] National Vulnerabilty Database. (2012, May) NIST Computer Security Division. [Online]. http://nvd.nist.gov/

[94] Department of Homeland Security. (2012, May) National Cyber Security Division. [Online]. http://www.us-cert.gov/

[95] C.E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech.* , no. 27, 1948.

[96] Nikolaos Alexandris, Evangelos Fountas, Dimitrios Mermigas, and Sotirios Pirounias, "Using time patterns to verify the utilization of stochastic calculus in security quantification," in *2010 IEEE International Conference on Information Security and Artificial (ISAI 2010), Chengdu, China, Dec. 17-19 2010, επίσης παρουσιάστηκε στο 2011 Global Congress on Science and Engineering (GCSE 2011), Dubai, Dec. 28-30 2011*, 2010-2011, p. 5.

[97] Symantec. (2009, June 29) Patch Tuesday/Exploit Wednesday? [Online]. http://www.symantec.com/connect/blogs/patch-tuesdayexploit-wednesday

[98] ZDNet. (2007, June 13) Exploit Wednesday follows MS Patch Tuesday. [Online]. http://www.zdnet.com/blog/security/exploit-wednesday-follows-ms-patch-tuesday/296

[99] Dimitrios Mermigas, Sotirios Pirounias, and Nikolaos Alexandris, "A probabilistic method for the quantification of corporate losses due to security breaches," in *2012 International Congress on Mathematics (MICOM)*, Serajevo, Bosnia, Sep. 19-23 2012.

[100] Dimitrios Mermigas and Constantinos Patsakis. (2012) SourceForge - Security Quantification Tool (SQT). [Online]. www.sourceforge.net/projects/sqt

[101] Constadinos Patsakis. (2012) Program for Security Quantification, "SecQua". [Online]. http://sourceforge.net/projects/secqua/

[102] Quarterly Report Q3 2011, PandaLabs. (2011, July - September 2011) Panda Security. [Online]. http://www.pandasecurity.com

[103] Gatzlaff K. and McCullough K., "The effect of data breaches on shareholder wealth," *Risk Management and Insurance Review* , vol. 1, no. 13, pp. 61-83, 2010.

[104] Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou, "The impact of information security breaches: Has there been a downward shift in costs?," *Journal of Computer Security*, vol. 19, pp. 33-56, 2011.

[105] Ali Alper and Qing Hu, "The impact of information security events on the stock value of firms: The effect of contigency factors," *Journal of Information Technology*, vol. 26, pp. 60-77, 2011.

[106] National Institude of Standards and Technology, "Guide to Performance Measures for Information Security," DRAFT SP 800-80 2006.

[107] Swanson M, National Institute of Standards and Technology Special Publication #800-26, Security Metrics Guide for Information Technology

Systems, November 2001.

[108] Swanson M, National Institute of Standards and Technology Special Publication #800-55, Security Metrics Guide for Information Technology Systems, July 2003.

[109] The Institute of Risk Management, A Risk Management Standard, 2002.

[110] NAO, National Audit Office, Managing risk in government departments, 2000.

[111] Tripwire, Operational Excellence: Linking your Business, Compliance, Operations and Security, 2006.

[112] Peter R. Bitterli, IT Security Governance—A Slow Start to a High Maturity Level, 2005.

[113] Information Systems Audit and Control Association (ISACA), The Risk IT Practitioner Guide, June 2010.

[114] Information Systems Audit and Control Association (ISACA), What Every IT Auditor Should Know About Access Controls, 2008.

[115] Information Systems Audit and Control Association (ISACA), What Every IT Auditor Should Know About Cyberforensics, 2006.

[116] Federal finincial institutions examination council (FFIEC), Information security, July 2006.

[117] Hank Peybylski and Tom Campanile, The Future Of Risk Forecasting, August 2009.

[118] Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo, Security Metrics Guide for Information Technology Systems, July 2003.

[119] Jean - Phillipe Bouchaud and Marc Potters, *Theory of financial risks from statistical physics to risk management*.: Univarsity of Cambridge, 2000.

[120] Ν. Αλεξανδρής, Β. Χρυσικόπουλος, and Κ. Πατσάκης, *Εισαγωγή στην θεωρία πληροφοριών κωδίκων και κρυπτογραφίας*.: Εκδόσεις Βαρβαρήγου, 2010.

[121] Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, and Gregory Chondrokoukis, "The role of weighted entropy in security quantification," in *2010 IEEE International Conference on Information Security and Artificial Intelligence (ISAI 2010), Chengdu, China, Dec. 17-19 2010, επίσης παρουσιάστηκε στο 2011 Global Congress on Science and Engineering (GCSE 2011), Dubai, Dec. 28-30 2011*, p. 4.

[122] "Cost of data breach study in United States," Ponemon Institute, Benchmark research 2011.

[123] Cavusoglu H., The Effect of Internet Security Breach Announsements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, 2004.

[124] Sotirios Pirounias, Dimitrios Mermigas, and Constantinos Patsakis, "The relation between information security events and firm market value, empirical evidence, on recent disclosures," *Information Systems Research Journal*, 2012.

[125] Dimitrios Mermigas, Constantinos Patsakis, and Sotirios Pirounias, "A formalistic quantification of information systems security with stochastic

calculus," in *8th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW 2012) also sponsored by National Nuclear Security Administration Cyber Sciences Laboratory*, Oak Ridge, TN, USA, 30th Oct – 1st Nov, 2012.

[126] Θεόδωρος Ν. Ντούσκας, Συνεργατική πολυκριτηριακή διαχείριση ασφάλειας Πληροφοριακών Συστημάτων, Σεπτέμβριος 2012.

ΠΑΡΑΡΤΗΜΑ

Π1. Πηγαίος κώδικας MatLab

Για να μπορέσουμε να δώσουμε λύση στο στοχαστικό ολοκλήρωμα που απαιτεί η προτεινόμενη μεθοδολογία, αναπτύχθηκε ένα ειδικό πρόγραμμα χρησιμοποιώντας το μαθηματικό πακέτο MatLab. Ο πηγαίος κώδικας του προγράμματος ακολουθεί:

Στην αρχή του κώδικα γίνεται η διασύνδεση του MatLab με την εφαρμογή SQT, με το διάβασμα των δύο αρχείων, «Day_Of_Month.txt» και «Final_IS.txt». Το SQL παράγει αυτά τα δύο αρχεία που περιέχουν τα δεδομένα από τη βάση δεδομένων της NVD, και θα χρησιμοποιηθούν από το MatLab για τον υπολογισμό του προτεινόμενου μοντέλου. Τα δύο αυτά αρχεία, περνιούνται με την ενσωματωμένη συνάρτηση του MatLab σε τοπικές –για το MatLab- μεταβλητές και εν συνεχεία χρησιμοποιούνται στον κώδικα.

```
function y = Quantification_Method(RptTitle, LegendTitle)
   %Get The days of month into a variable
    Day_Of_Month = importdata('Day_Of_Month.txt');
    %GET the IS values into a variable
    IS = importdata('Final_IS.txt');

    cr=sprintf('%c%c',char(10), char(13));
    lines = regexp(RptTitle, char(cr), 'split');
    line1 = lines(1);
    WindowTitle = sprintf('%s', char(line1));

    ReportTitle = sprintf('%s', RptTitle);

    %Handle the Curve Fitting object
    [xData, yData] = prepareCurveData( Day_Of_Month, IS );

    % Set up fittype and options.
    ft = fittype( 'fourier8' );
    opts = fitoptions( ft );
    opts.Display = 'Off';
    opts.Lower = [-Inf -Inf -Inf -Inf -Inf -Inf -Inf -Inf -Inf -Inf -Inf -Inf -Inf -
    Inf -Inf -Inf -Inf];
    opts.StartPoint = [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4.26616646728179];
    opts.Upper = [Inf Inf Inf Inf Inf Inf Inf Inf Inf Inf Inf Inf Inf Inf Inf Inf Inf
    Inf];
    opts.Normalize = 'on';

    % Fit model to data.
    [fitresult{1}, gof(1)] = fit( xData, yData, ft, opts );

    %Get the coeff values
    coeffvals = coeffvalues(fit( xData, yData, ft, opts) );

    %Calculate the security level
    randn('state',0);
    sum=0;
    res=[];

    for cnt=1:1000
        %create a random walk from 0 to 31
        T=30;n=1000;
        dt=T/n;
        displacement = randn(1,n);
        W = cumsum(displacement);
        local_range=max(W)-min(W);
        ratio=local_range/31;
```

```
    W=W/ratio;
    mn=min(W);
    if mn<0
        W=W-mn;
    end

    %t=[1:dt:T];
    W=[0,W];

    a0 = coeffvals(1);
    a1 = coeffvals(2);      b1 = coeffvals(3);
    a2 = coeffvals(4);      b2 = coeffvals(5);
    a3 = coeffvals(6);      b3 = coeffvals(7);
    a4 = coeffvals(8);      b4 = coeffvals(9);
    a5 = coeffvals(10);      b5 = coeffvals(11);
    a6 = coeffvals(12);      b6 = coeffvals(13);
    a7 = coeffvals(14);      b7 = coeffvals(15);
    a8 = coeffvals(16);      b8 = coeffvals(17);
    w = coeffvals(18);

    gW=[];
    for j=1:n
             gW=[gW  a0 + a1*cos((1+j*dt)*w) + b1*sin((1+j*dt)*w) + a2*cos(2*(1+j*dt)*w) +
             b2*sin(2*(1+j*dt)*w) + a3*cos(3*(1+j*dt)*w) + b3*sin(3*(1+j*dt)*w) +
             a4*cos(4*(1+j*dt)*w) + b4*sin(4*(1+j*dt)*w) + a5*cos(5*(1+j*dt)*w) +
             b5*sin(5*(1+j*dt)*w) + a6*cos(6*(1+j*dt)*w) + b6*sin(6*(1+j*dt)*w) +
             a7*cos(7*(1+j*dt)*w) + b7*sin(7*(1+j*dt)*w) + a8*cos(8*(1+j*dt)*w) +
             b8*sin(8*(1+j*dt)*w)];
    end

    ito=0;

    for j=1:n-1
        ito=ito+gW(j)*(W(j+1)-W(j));
    end

    sum=sum+ito;
    res=[res ito/30];
end

Sec_Level = (sum/(30*(cnt-1)))*100;
y=Sec_Level;

%Handle the chart object
% Plot fit with data.
scrsz = get(0,'ScreenSize');

figure( 'Name', char(WindowTitle), 'Position',[200 300 scrsz(3)/2 scrsz(4)/2],
        'Toolbar', 'none');

h = plot( fitresult{1}, xData, yData );

legend( h, sprintf('%s', char(ReportTitle)), 'Security Quantification Curve Fit',
                     'Location', 'Best' );

% Label axes
xlabel( sprintf('%s %c%cCalculated Security Level = %4.2f%%',
                                      LegendTitle, char(10), char(13), Sec_Level));

ylabel( 'Security Level' );

grid on
```

Π2. Πηγαίος κώδικας SQT

Ο πηγαίος κώδικας που ακολουθεί, είναι ο κώδικας που χρησιμοποιήθηκε για την ανάπτυξη της εφαρμογής SQT, είναι ανεπτυγμένος σε VB.Net και χρησιμοποιήθηκε το Microsoft Visual Studio 2008.

Η εφαρμογή ως παραθυρική, είναι event-oriented και για το λόγο αυτό οι ρουτίνες που ακολουθούν, αντιστοιχούν σε πιθανές επιλογές του χρήστη, για παράδειγμα

«ImportBtn_Click». Επιπλέον ακολουθούν και άλλες βοηθητικές / συμπληρωματικές ρουτίνες που χρησιμοποιούνται από το SQT.

```
Imports System.Xml
Imports System.IO
Imports System.Data.SqlClient
Imports Microsoft.Win32

Public Class frmSecurityQuantification
Private xmlDir As String = My.Application.Info.DirectoryPath
Private AccessDir As String = My.Application.Info.DirectoryPath
Private AccessFileName As String = Nothing
Private Sum_CVSSScore As String = Nothing
Private Sum_Vulnerabilities As String = Nothing
Private xmlFile As String = ""
Private APP_TITLE As String = "Security Quantification Tool"
Private REG_KEY As String = "Software\SecurityQuantification\AccessFile"
Private SQLConnection As OleDb.OleDbConnection = Nothing

Private Sub ImportBtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                                    Handles ImportBtn.Click
        Try
            With OpenFileDialog
                .ShowReadOnly = True
                .Multiselect = True
                .CheckFileExists = True
                .CheckPathExists = True
                .Filter = "Xml Files (nvdcve*.xml)|nvdcve*.xml"
                .FileName = ""
                .InitialDirectory = xmlDir
                .Title = APP_TITLE & " - Import NVD xml files"

                Cursor.Current = Cursors.WaitCursor

                If .ShowDialog = Windows.Forms.DialogResult.OK Then
                    If Not .FileNames Is Nothing Then
                        For l As Integer = 0 To .FileNames.LongLength - 1
                            AccessFileLbl.Text = "Database file: " & AccessFileName & _
                                                 " (Processing xml file " & l + 1 & " of "
                                                       & .FileNames.LongLength & ")"
                            If ProcessXml(.FileNames(l)) = False Then
                                Exit Sub
                            End If
                        Next
                    End If
                Else
                    MsgBox("The action was cancelled by the user.", MsgBoxStyle.Exclamation, APP_TITLE)
                    Exit Sub
                End If
            End With

            MsgBox("The procedure ended successfully.", MsgBoxStyle.Information, APP_TITLE)

        Catch ex As Exception
            MsgBox("There was an error processind NVD xml file." & vbCrLf & _
                   "Error: " & ex.Message, MsgBoxStyle.Critical, APP_TITLE)
        Finally
            If Not SQLConnection Is Nothing AndAlso SQLConnection.State <> ConnectionState.Closed Then
                SQLConnection.Close()
            End If

            AccessFileLbl.Text = "Database file: " & AccessFileName
            Cursor.Current = Cursors.Arrow
        End Try
    End Sub

    Public Function ProcessXml(ByVal xmlFile As String) As Boolean
        Dim xmldoc As New XmlDataDocument()
        Dim xmlnode As XmlNodeList

        Dim i As Integer
        Dim fs As New FileStream(xmlFile, FileMode.Open, FileAccess.Read)

        Dim id As String, vendor As String, SW_List As String, access_vector As String,
              access_complexity As String, authentication As String
        Dim confidentiality_impact As String, integrity_impact As String,
              availability_impact As String, summary As String
        Dim PublishDate As Date, ModifiedDate As Date, GeneratedDate As Date
        Dim Score As Double

        Cursor.Current = Cursors.WaitCursor
```

```
        ProcessXml = False

        xmldoc.Load(fs)
        xmlnode = xmldoc.GetElementsByTagName("entry")

        'entries loop
        For i = 0 To xmlnode.Count - 1
            SW_List = ""

            id = xmlnode(i).Attributes("id").Value

            For k As Integer = 0 To xmlnode(i).ChildNodes.Count - 1
                Select Case xmlnode(i).ChildNodes(k).Name
                    Case Is = "vuln:published-datetime"
                        PublishDate = xmlnode(i).ChildNodes(k).InnerText

                    Case Is = "vuln:last-modified-datetime"
                        ModifiedDate = xmlnode(i).ChildNodes(k).InnerText

                    Case Is = "vuln:vulnerable-software-list"
                        For j As Integer = 0 To xmlnode(i).ChildNodes(k).ChildNodes.Count - 1
                            SW_List += xmlnode(i).ChildNodes(k).ChildNodes(j).InnerText()
                        Next
                        vendor = xmlnode(i).ChildNodes(k).ChildNodes(0).InnerText().Split(":")(2)

                    Case Is = "vuln:cvss"
                        For j As Integer = 0 To
                                        xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes.Count - 1
                            Select Case xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes(j).Name
                                Case "cvss:score"
                                    Score =
                               xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes(j).InnerText() / 10
                                Case "cvss:access-vector"
                                    access_vector =
                               xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes(j).InnerText()
                                Case "cvss:access-complexity"
                                    access_complexity =
                               xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes(j).InnerText()
                                Case "cvss:authentication"
                                    authentication =
                               xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes(j).InnerText()
                                Case "cvss:confidentiality-impact"
                                    confidentiality_impact =
                               xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes(j).InnerText()
                                Case "cvss:integrity-impact"
                                    integrity_impact =
                               xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes(j).InnerText()
                                Case "cvss:availability-impact"
                                    availability_impact =
                               xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes(j).InnerText()
                                Case "cvss:generated-on-datetime"
                                    GeneratedDate =
                               xmlnode(i).ChildNodes(k).ChildNodes(0).ChildNodes(j).InnerText()
                                End Select
                        Next

                    Case Is = "vuln:summary"
                        summary = xmlnode(i).ChildNodes(k).InnerText()
                End Select
            Next

            Dim SQLParameters(,) As Object = {{"@ID", id}, _
                                              {"@Vendor", vendor}, _
                                              {"@SW_List", SW_List}, _
                                              {"@PublishDate", Format(PublishDate, "yyyy-MM-dd")}, _
                                              {"@ModifiedDate", Format(ModifiedDate, "yyyy-MM-dd")}, _
                                              {"@Score", Score}, _
                                              {"@AccessVector", access_vector}, _
                                              {"@AccessComplexity", access_complexity}, _
                                              {"@Authentication", authentication}, _
                                              {"@ConfideltialityImpact", confidentiality_impact}, _
                                              {"@IntegrityIpmact", integrity_impact}, _
                                              {"@AvailabilityImpact", availability_impact}, _
                                              {"@GeneratedDate", Format(GeneratedDate, "yyyy-MM-dd")},_
                                              {"@Summary", summary} _
                                             }
            ExecSP("Insert into Vulnerabilities Values (?,?,?,?,?,?,?,?,?,?,?,?,?,?)",
                        Nothing, SQLParameters)
        Next

        ProcessXml = True
    End Function

    Private Sub SettingsBtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                                        Handles SettingsBtn.Click
        Try
            With OpenFileDialog
                .ShowReadOnly = True
```

```
            .Multiselect = False
            .CheckFileExists = True
            .CheckPathExists = True
            .Filter = "Microsoft Access File |*.mdb"
            .FileName = ""
            .InitialDirectory = AccessDir
            .Title = APP_TITLE & " - Set database file"

            Cursor.Current = Cursors.WaitCursor

            If .ShowDialog = Windows.Forms.DialogResult.OK Then
                InitialiseConnection(.FileName)
                HandleRegistry(REG_KEY, .FileName)
            Else
                MsgBox("The action was cancelled by the user.", MsgBoxStyle.Exclamation, APP_TITLE)
            End If
        End With

    Catch ex As Exception
        MsgBox("There was an setting the database file." & vbCrLf & _
               "Error: " & ex.Message, MsgBoxStyle.Critical, APP_TITLE)
    Finally
        Cursor.Current = Cursors.Arrow
    End Try
End Sub

Public Sub HandleRegistry(ByVal RegKey As String, ByVal RegValue As String)
    If RegKey_Exists().Length = 0 Then
        Try
            Dim newKey As RegistryKey
            newKey = My.Computer.Registry.LocalMachine.CreateSubKey(RegKey)

        Catch ex As Exception
            MsgBox(ex.Message, MsgBoxStyle.Critical, APP_TITLE)
        End Try
    End If

    My.Computer.Registry.SetValue("HKEY_LOCAL_MACHINE\" & REG_KEY, "Filename", RegValue)
End Sub

Public Function ExecSP(ByVal SQLStr As String, Optional ByVal Tbl As String = Nothing, _
                       Optional ByVal SQLParameters(,) As Object = Nothing) As DataTable
    Dim cmd As New OleDb.OleDbCommand
    Dim da As New OleDb.OleDbDataAdapter
    Dim ds As New DataSet("Myds")
    Dim dt As New DataTable(Tbl)

    ExecSP = Nothing

    Try
        If Not SQLConnection Is Nothing AndAlso SQLConnection.State = ConnectionState.Closed Then
            SQLConnection.Open()
        End If

        cmd.CommandType = CommandType.Text
        cmd.CommandText = SQLStr
        cmd.Connection = SQLConnection

        If Not SQLParameters Is Nothing AndAlso SQLParameters.Length <> 0 Then
            For i As Integer = 0 To SQLParameters.GetUpperBound(0)
                If SQLParameters(i, 1) Is Nothing Then SQLParameters(i, 1) = System.DBNull.Value
                cmd.Parameters.AddWithValue(SQLParameters(i, 0).ToString, SQLParameters(i, 1))
            Next
        End If

        If Tbl Is Nothing Then
            cmd.ExecuteNonQuery()
            Exit Function
        End If

        da.SelectCommand = cmd

        Try
            da.Fill(dt)

        Catch ex As Exception
            dt = Nothing
        End Try

        ExecSP = dt

    Catch ex As Exception
        If Err.Number = 5 Then
            'MsgBox("Primary key violation. Please choose another file to import.",
                     MsgBoxStyle.Critical, APP_TITLE)
        Else
            'MsgBox(ex.Message, MsgBoxStyle.Critical, APP_TITLE)
        End If
```

```
    Finally
        cmd = Nothing
    End Try
End Function

Private Sub ExitBtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                                    Handles ExitBtn.Click
    If MsgBox("Do you want to terminate the application?", _
        MsgBoxStyle.Question + MsgBoxStyle.YesNo + MsgBoxStyle.DefaultButton2,
                                                    APP_TITLE) = MsgBoxResult.Yes Then
        SQLConnection = Nothing
        End
    End If
End Sub

Private Sub FindSecurityEventsBtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                    Handles FindSecurityEventsBtn.Click
    Cursor.Current = Cursors.WaitCursor
    Dim VendorTxt As String = ""

    If VendorCbo.Text.Length > 0 Then
        VendorTxt = VendorCbo.Text
    End If

    If HasNoSQLInjectionTrap(VendorTxt) = False Then Exit Sub
    If HasNoSQLInjectionTrap(SW_ListTxt.Text) = False Then Exit Sub

    Me.DataGridView.DataSource = Nothing
    RecordsLbl.Text = "Records Found: "
    Application.DoEvents()

    Dim dt As DataTable = ExecSP("Select ID, Vendor, SW_List, PublishDate, Score, summary from
                                  Vulnerabilities " & _
                                 "WHERE SW_List Like '%" & SW_ListTxt.Text & "%'" & _
                                 "  and Vendor Like '%" & VendorTxt & "%'", "Tbl", Nothing)

    If Not dt Is Nothing AndAlso dt.Rows.Count > 0 Then
        RecordsLbl.Text = "Records Found: " & dt.Rows.Count
    End If

    Me.DataGridView.DataSource = dt

    Cursor.Current = Cursors.Arrow
End Sub

Public Function HasNoSQLInjectionTrap(ByVal SQLStr As String) As Boolean
    HasNoSQLInjectionTrap = False

    If InStr(SQLStr, ";", CompareMethod.Binary) + _
       InStr(SQLStr, "?", CompareMethod.Binary) + _
       InStr(SQLStr, "'", CompareMethod.Binary) > 0 Then
        MsgBox("The filters you have entered are wrong. Please try again.", MsgBoxStyle.Critical,
                                                                        APP_TITLE)
        Exit Function
    End If

    HasNoSQLInjectionTrap = True
End Function

Private Function RegKey_Exists() As String
    Dim FileName As String

    RegKey_Exists = ""

    FileName = My.Computer.Registry.GetValue("HKEY_LOCAL_MACHINE\" & REG_KEY, "FileName", "")
    If FileName IsNot Nothing AndAlso FileName.Length > 0 Then RegKey_Exists = FileName
End Function

Private Sub frmSecurityQuantification_Load(ByVal sender As Object, ByVal e As System.EventArgs)
                                                                        Handles Me.Load
    If RegKey_Exists().Length > 0 Then InitialiseConnection(RegKey_Exists())
    Me.DayOfMonthRadio.Checked = True
End Sub

Private Sub InitialiseConnection(ByVal Filename As String)
    If Not SQLConnection Is Nothing AndAlso SQLConnection.State <> ConnectionState.Closed Then
        SQLConnection.Close()
    End If

    SQLConnection = Nothing
    SQLConnection = New OleDb.OleDbConnection
    SQLConnection.ConnectionString = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Filename & _
                                     ";User Id=admin;Password=;"

    AccessFileLbl.Text = "Database file: " & Filename
    AccessFileName = Filename
End Sub
```

```
Private Sub RightBtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                                        Handles RightBtn.Click
    Dim VendorTxt As String = ""

    If VendorCbo.Text.Length > 0 Then
        VendorTxt = VendorCbo.Text
    End If

    IS_ListBox.Items.Add(VendorTxt & "," & SW_ListTxt.Text)
End Sub

Private Sub LeftBtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                                        Handles LeftBtn.Click
    If IS_ListBox.SelectedItem Is Nothing Then Exit Sub

    VendorCbo.Text = IS_ListBox.SelectedItem.ToString.Split(",")(0)
    SW_ListTxt.Text = IS_ListBox.SelectedItem.ToString.Split(",")(1)
    IS_ListBox.Items.Remove(IS_ListBox.SelectedItem)
    Me.DataGridView.DataSource = Nothing
End Sub

Private Sub IS_ListBox_DoubleClick(ByVal sender As Object, ByVal e As System.EventArgs)
                                                            Handles IS_ListBox.DoubleClick
    If IS_ListBox.SelectedItem Is Nothing Then Exit Sub

    IS_ListBox.Items.Remove(IS_ListBox.SelectedItem)
End Sub

Private Sub MatlabBtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                                        Handles MatlanBtn.Click
    Dim DatePart As String = "d" 'DatePart d=day of month, ww=week of year, y=day of year
    Dim PeriodDays As String = 31
    Dim LegentTitle As String = Nothing

    If DayOfMonthRadio.Checked = True Then DatePart = "d"
    If WeekRadio.Checked = True Then DatePart = "ww"
    If DayOfYearRadio.Checked = True Then DatePart = "y"

    Select Case DatePart
        Case "d"    'Day of month
            PeriodDays = 31
            LegentTitle = "Day of Month"
        Case "ww"   'Week of year
            PeriodDays = 52
            LegentTitle = "Week of Year"
        Case "y"    'Day of year
            PeriodDays = 366
            LegentTitle = "Day of Year"
    End Select

    If IS_ListBox.Items.Count = 0 OrElse IS_ListBox.Items(0).ToString = "," Then
        IS_ListBox.Items.Clear()
        MsgBox("Please include at least one software component for the calculation to take place.",
                                                                MsgBoxStyle.Critical, APP_TITLE)
        Exit Sub
    End If

    Cursor.Current = Cursors.WaitCursor
    Dim dt As DataTable
    Dim s As String = ""

    ExecSP("Delete * from Final_IS")

    For i As Integer = 1 To PeriodDays
        ExecSP("Insert into Final_IS(DayNo, SecLevel, Vulnerabilities, CVSS_Score) values (" &
               i.ToString & ", 1, 0, 0)")
        s += i.ToString & vbCrLf
    Next
    My.Computer.FileSystem.WriteAllText(AccessDir & "\Day_Of_Month.txt", s, False,
                                        System.Text.Encoding.ASCII)

    For i As Integer = 0 To IS_ListBox.Items.Count - 1
        Dim WhereStr As String = " where Vendor like '%" &
                                        IS_ListBox.Items(i).ToString.Split(",")(0) & "%' " & _
                                 "   and SW_List like '%" &
                                        IS_ListBox.Items(i).ToString.Split(",")(1) & "%' "

        ExecSP("Delete * from Calculations")

        Dim Num_of_Vulnerabilities_by_day_SQL As String = _
            "Insert into Calculations(Num_of_Vulnerabilities, DayNo, Sum_Of_score) " & _
           "select count(*) as Num_Of_Vulnerabilities, DatePart(""" & DatePart & """, PublishDate)
            as Day_Of_Month, SUM(Score) as Score " & _
            "from vulnerabilities " & _
            WhereStr & _
            "group by Vendor, DatePart(""" & DatePart & """, PublishDate) " & _
            "order by DatePart(""" & DatePart & """, PublishDate) "
        ExecSP(Num_of_Vulnerabilities_by_day_SQL)
```

```
        Dim Get_ciSQL As String = _
                                "SELECT Sum(ci_part_entropy_with_years) AS
                                SumOfci_part_entropy_with_years " & _
                                "FROM (SELECT ci_part_entropy*2.71828183^(-ydiff) AS
                                ci_part_entropy_with_years " & _
                                "      From  " & _
                                "       (SELECT -Score*prob*Log(prob) AS ci_part_entropy, ydiff " & _
                                "            FROM " & _
                                "                 (SELECT CountOfScore/total_vulns AS prob, Score,
                                                  ydiff " & _
                                "                  FROM  " & _
                                "                        (SELECT vendor_vulnerabilities.ydiff,
                                                         vendor_vulnerabilities.Score, " & _
                                "                        Count(vendor_vulnerabilities.Score) AS
                                                         CountOfScore, total_vulns " & _
                                "                        FROM (SELECT DatePart(""" & DatePart & """,
                                                         PublishDate) AS month_day, " & _
                                "                                    Score, DateDiff(""yyyy"",
                                                           PublishDate, now()) AS ydiff " & _
                                "                              FROM Vulnerabilities " & _
                                                               WhereStr & _
                                "                              ) as vendor_vulnerabilities, " & _
                                "                              (SELECT Count(b.Score) AS total_vulns
                                                               " & _
                                "                               FROM (SELECT DatePart(""" & DatePart
                                                            & """, PublishDate) AS month_day, " & _
                                "                                    Score, DateDiff(""yyyy"",
                                                               PublishDate, now()) AS ydiff " & _
                                "                                    FROM Vulnerabilities " & _
                                                                     WhereStr & _
                                "                                    ) as b " & _
                                "                              ) " & _
                                "                        GROUP BY vendor_vulnerabilities.ydiff,
                                                      vendor_vulnerabilities.Score, total_vulns " & _
                                "                              )" & _
                                "                    )" & _
                                "                ) " & _
                                "     )  AS alias1 "
        ExecSP("Update Calculations set ci = " & Replace(ExecSP(Get_ciSQL,
                                                 "Tbl").Rows(0).Item(0).ToString, ",", "."))

        ExecSP("Update Calculations set pi  =  Sum_Of_Score / " & Replace(ExecSP("select
               SUM(Sum_Of_Score) FROM Calculations", "Tbl").Rows(0).Item(0).ToString, ",", "."))

        ExecSP("Update Calculations set One_div_ci_to_power =  pi ^ (1 / ci)")

        ExecSP("Update Calculations set Adjusted_ci =  1 - One_div_ci_to_power ")

        ExecSP("UPDATE Final_IS INNER JOIN Calculations ON Calculations.DayNo = Final_IS.DayNo SET
               SecLevel = SecLevel * Adjusted_ci")

        ExecSP("Update Final_IS set Vulnerabilities =  Vulnerabilities + " & Replace(ExecSP("Select
                sum(Num_of_Vulnerabilities) from Calculations", "Tbl").Rows(0).Item(0).ToString,
                ",", "."))
        ExecSP("Update Final_IS set CVSS_Score = CVSS_Score + " & Replace(ExecSP("Select
               sum(Sum_Of_score) from Calculations", "Tbl").Rows(0).Item(0).ToString, ",", "."))

        dt = ExecSP("Select * from Calculations", "Tbl")
        Me.DataGridView.DataSource = dt

        If Not dt Is Nothing AndAlso dt.Rows.Count > 0 Then
            Me.RecordsLbl.Text = "Records Found: " & dt.Rows.Count
        Else
            Me.RecordsLbl.Text = "Records Found: 0"
        End If

        Application.DoEvents()
    Next

    dt = ExecSP("Select * from Final_IS", "Tbl")

    If Not dt Is Nothing AndAlso dt.Rows.Count > 0 Then
        s = ""
        For i As Integer = 0 To dt.Rows.Count - 1
            s += Replace(dt.Rows(i).Item("SecLevel").ToString, ",", ".") & vbCrLf
        Next

        Sum_CVSSScore = Replace(dt.Rows(0).Item("CVSS_Score").ToString, ",", ".")
        Sum_Vulnerabilities = Replace(dt.Rows(0).Item("Vulnerabilities").ToString, ",", ".")
    End If
    My.Computer.FileSystem.WriteAllText(AccessDir & "\Final_IS.txt", s, False,
                                                          System.Text.Encoding.ASCII)

    dt = Nothing
    Call_Matlab(ReportTitleTxt.Text, LegentTitle)

    Cursor.Current = Cursors.Arrow
End Sub
```

```
    Private Sub Call_Matlab(ByVal RptTitle As String, ByVal LegentTitle As String)
        Cursor.Current = Cursors.WaitCursor
        Try
            Dim a As New Curvefit2Native.DisplayText
            Dim IS_InfoStr As String = ""

            If Sum_CVSSScore IsNot Nothing Then IS_InfoStr += "Total CVSS Score = " & Sum_CVSSScore
            If Sum_Vulnerabilities IsNot Nothing Then IS_InfoStr += ", Number of Vulnerabilities = " &
                 Sum_Vulnerabilities

            If RptTitle.Length = 0 Then
                RptTitle = "Security level by " & LegentTitle
            Else
                RptTitle = "Security level of (" & RptTitle & ") by " & LegentTitle
            End If

            Dim ThreeLineReportLegend As String = ""
            Dim LineChars As Integer = 0
            For i As Integer = 0 To RptTitle.Split(" ").Length - 1
                If LineChars + RptTitle.Split(" ")(i).Length > 75 Then
                    ThreeLineReportLegend += Chr(10) & Chr(13)
                    LineChars = 0
                End If
                ThreeLineReportLegend += RptTitle.Split(" ")(i) & " "
                LineChars += RptTitle.Split(" ")(i).Length + 1
            Next
            ThreeLineReportLegend += Chr(10) & Chr(13) & IS_InfoStr

            a.Quantification_Method(ThreeLineReportLegend, LegentTitle)
            a = Nothing

        Catch ex As Exception
            MsgBox(ex.Message, MsgBoxStyle.Critical, APP_TITLE)
        Finally
            Cursor.Current = Cursors.Arrow
        End Try
    End Sub

    Private Sub VendorCbo_Enter(ByVal sender As Object, ByVal e As System.EventArgs)
                                                                                Handles VendorCbo.Enter
        If VendorCbo.DataSource IsNot Nothing Then Exit Sub

        Dim Vendor_dt As DataTable = ExecSP("select distinct Vendor from Vulnerabilities", "Tbl")

        If Vendor_dt Is Nothing OrElse Vendor_dt.Rows.Count = 0 Then Exit Sub

        With VendorCbo
            .DataSource = Vendor_dt
            .ValueMember = "Vendor"
            .DisplayMember = "Vendor"
            .AutoCompleteMode = AutoCompleteMode.SuggestAppend
            .AutoCompleteSource = AutoCompleteSource.ListItems
        End With

        Vendor_dt = Nothing
    End Sub

    Private Sub GoToNVDwebsiteBtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                            Handles GoToNVDwebsiteBtn.Click
         Process.Start("IExplore.exe", "http://nvd.nist.gov/download.cfm")
    End Sub

    Private Sub AboutBtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                                                Handles AboutBtn.Click
        Dim f As New AboutBox
        f.Show()
        f = Nothing
    End Sub
End Class

Public NotInheritable Class AboutBox

    Private Sub AboutBox_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                                                Handles MyBase.Load
        Dim Str As String = "SQT is an open source program written in VB.Net that, implements a novel
                            method " & _
                            "for the security quantification of an Information System (IS), a service
                            or a product. " & _
                            "This new proposed security metric, is using stochastic calculus in order
                            to " & _
                            "provide us with a deterministic and unbiased measurement of the security
                            level " & _
                            "of an IS. Because the approach is vulnerability-driven, and for ensuring
                            unbiased results, " & _
                            "it uses the National Vulnerability Database. " & vbCrLf & _
                            "This work is based upon the following publications: " & vbCrLf & _
                            " • Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Nikolaos
                            Alexandris, " & _
```

```
                            "and Evangelos Fountas, ""Towards a formalistic measuring of security using
                                stochastic calculus,"" in " & _
                            "2010 3rd IEEE International Conference on Computer Science and Information
                                Technology (ICCSIT2010), 2010, p. 4" & vbCrLf & _
                            " • Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, and
                                Gregory Chondrokoukis, " & _
                            """The role of weighted entropy in security quantification,"" in 2010 IEEE
                                International Conference " & _
                            "on Information Security and Artificial Intelligence (ISAI 2010), also
                                appearing in 2011 Global Congress " & _
                            "on Science and Engineering (GCSE 2011), 2010-2011, p. 4." & vbCrLf & _
                            " • Nikolaos Alexandris, Evangelos Fountas, Dimitrios Mermigas, and
                                Sotirios Pirounias, " & _
                            """Using time patterns to verify the utilization of stochastic calculus in
                                security quantification,"" in 2010 " & _
                            "IEEE International Conference on Information Security and Artificial (ISAI
                                2010), also appearing in " & _
                            "2011 Global Congress on Science and Engineering (GCSE 2011), 2010-2011, p.
                                5."

        ' Set the title of the form.
        Dim ApplicationTitle As String

        If My.Application.Info.Title <> "" Then
            ApplicationTitle = My.Application.Info.Title
        Else
            ApplicationTitle =
                        System.IO.Path.GetFileNameWithoutExtension(My.Application.Info.AssemblyName)
        End If

        Me.Text = String.Format("About {0}", ApplicationTitle)

        Me.LabelProductName.Text = "Security Quantification Tool (SQT)"
        Me.LabelVersion.Text = String.Format("Version {0}", My.Application.Info.Version.ToString)
        Me.LabelCopyright.Text = My.Application.Info.Copyright
        Me.LabelCompanyName.Text = My.Application.Info.CompanyName
        Me.TextBoxDescription.Text = Str
        Me.Icon = My.Resources.ChartLine
        Me.LogoPictureBox.Image = My.Resources.ChartLine256
    End Sub

    Private Sub OKButton_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
                                                                                Handles OKButton.Click
        Me.Close()
    End Sub
End Class
```