ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ / ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΔΙΟΙΚΗΤΙΚΗ ΥΠΟΣΤΗΡΙΞΗ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ: ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ

Διδακτορική Διατριβή

Δημήτριος Γ. Πατσός

Δημήτριος Γ. Πατσός

Ειδικός Πληροφορικής, Τμήμα Πληροφορικής, Παν. Πειραιώς

Το έργο συγχρηματοδοτείται:

- 80% της Δημόσιας Δαπάνης από την Ευρωπαϊκή Ένωση – Ευρωπαϊκό Κοινωνικό Ταμείο
- 20% της Δημόσιας Δαπάνης από το Ελληνικό Δημόσιο – Υπουργείο Ανάπτυξης – Γενική Γραμματεία Έρευνας και Τεχνολογίας
- και από τον Ιδιωτικό Τομέα

στο πλαίσιο του Μέτρου 8.3 του Ε.Π. Ανταγωνιστικότητα – Γ΄ Κοινοτικό Πλαίσιο Στήριξης.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΑΤΡΙΒΗ

για την απόκτηση Διδακτορικού Διπλώματος του Τμήματος Πληροφορικής

Δημητρίου Γ. Πατσού

ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΔΙΟΙΚΗΤΙΚΗ ΥΠΟΣΤΗΡΙΞΗ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ: ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ

Τριμελής Συμβουλευτική Επιτροπή:

Επιβλέπων:

Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη:

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Γεώργιος Τσιχριντζής
Αναπληρωτής Καθηγητής Πανεπιστημίου Πειραιώς

Επταμελής Εξεταστική Επιτροπή:

Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Στέφανος Γκρίτζαλης
Καθηγητής Πανεπιστημίου Αιγαίου

Γεώργιος Τσιχριντζής
Αναπληρωτής Καθηγητής Πανεπιστημίου Πειραιώς

Δέσποινα Πολέμη
Επίκουρος Καθηγήτρια Πανεπιστημίου Πειραιώς

Γεώργιος Καρυστινός
Επίκουρος Καθηγητής Πολυτεχνείου Κρήτης

Δημήτριος Βέργαδος
Λέκτωρ Πανεπιστημίου Πειραιώς

ΔΕΣΜΕΥΤΙΚΗ ΔΗΛΩΣΗ

Οι διδακτορικές μου σπουδές διεξήχθησαν υπό την εποπτεία του Καθηγητή Χρήστου Δουληγέρη, μεταξύ Ιουλίου 2004 και Ιουνίου 2009 στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς.

Η παρούσα διδακτορική διατριβή είναι το αποτέλεσμα πρωτότυπης ερευνητικής δουλειάς που διεξήχθη από εμένα σε συνεργασία με άλλους, ενώ ήμουν υποψήφιος διδάκτωρ του Τμήματος Πληροφορικής στο Πανεπιστήμιο Πειραιώς και δεν έχει κατατεθεί για τίτλο σπουδών σε κανένα άλλο Πανεπιστήμιο ή εκπαιδευτικό ίδρυμα.

Δημήτριος Γ. Πατσός

Ιούνιος 2009

ΑΦΙΕΡΩΣΗ

Στην οικογένειά μου: Γιώργο, Σταματία, Αργυρώ και στον μικρό ανηψιό μου Αντώνη.

ΕΥΧΑΡΙΣΤΙΕΣ

Η συγκεκριμένη διατριβή δεν θα μπορούσε να ολοκληρωθεί χωρίς την καθοδήγηση και την υποστήριξη αρκετών ανθρώπων.

Πρώτα από όλα, θέλω να ευχαριστήσω τον επιβλέποντα Καθηγητή Χρήστο Δουληγέρη και το συνεργάτη Δρ. Σαράντη Μητρόπουλο για τη συνεχή υποστήριξη, ενδιαφέρον και υπομονή που επέδειξαν καθ' όλη τη διάρκεια των διδακτορικών μου σπουδών στο Πανεπιστήμιο Πειραιώς. Η καθοδήγησή τους, καθώς και τα σημαντικά σχόλια, παρατηρήσεις και προτάσεις τους με ενθάρρυναν διαρκώς να ολοκληρώσω τις ακαδημαϊκές και ερευνητικές μου ιδέες.

Επίσης, την Γενική Γραμματεία Έρευνας και Τεχνολογίας, για τη χρηματοδότησή που μου προσέφερε καθόλη τη διάρκεια της έρευνάς μου (στα πλαίσια του ερευνητικού έργου 03ΕΔ/546-ΠΕΝΕΔ 2003, Προηγμένα Συστήματα Ασφάλειας και Αντιμετώπισης Επιθέσεων).

Θέλω να ευχαριστήσω ένα πλήθος ανθρώπων που με υποστηρίζουν από την πρώτη στιγμή που ασχολήθηκα με την ασφάλεια πληροφοριών: τα μέλη του Information Security Group στο Royal Holloway University of London, τους καθηγητές μου στο Τμήμα Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών, τους συναδέλφους μου στη Space Hellas και στην Adacom, αλλά και όλους τους συνεργάτες στον επαγγελματικό μου βίο. Η καθημερινή επαφή μαζί τους με έκανε καλύτερο άνθρωπο, σωστότερο επαγγελματία και περισσότερο ανήσυχο ερευνητή.

Νιώθω ευγνώμων στους φίλους μου για την αγάπη, την ευγένεια και την υπομονή που επέδειξαν. Τους ευχαριστώ από καρδιάς και για την υποστήριξή τους στο σοβαρό τροχαίο ατύχημα που είχα κατά τη διάρκεια των σπουδών μου.

Η οικογένειά μου τοποθετεί συνεχώς ψηλότερα τις προσδοκίες μου. Με καθοδηγεί, με ενθαρρύνει και με υποστηρίζει σε όλη τη διάρκεια των σπουδών μου, στην επαγγελματική και στην προσωπική μου ζωή. Χωρίς την υποστήριξη και την ενθάρρυνσή της, δεν θα είχα καν ξεκινήσει τις διδακτορικές μου σπουδές. Μητέρα, πατέρα και αδελφή - ευχαριστώ!

Τέλος, πιστεύω πως δεν μπορώ να ευχαριστήσω αρκετά τους πνευματικούς μου μέντορες που αν και αποχώρησαν πρόωρα από τη ζωή, κατά τη διάρκεια των σπουδών μου, θα συνεχίσουν να με εμπνέουν για το υπόλοιπο της ζωής μου: τον Επίκουρο Καθηγητή Κωνσταντίνο Πατσό, τη Δρ. Μαντλέν Τεοφίλοβα, και το Δημήτρη Παππά.

ΠΕΡΙΛΗΨΗ

ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΔΙΟΙΚΗΤΙΚΗ ΥΠΟΣΤΗΡΙΞΗ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ: ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ

Δημήτριος Γ. Πατσός

Στη διατριβή αυτή εξετάζεται το πρόβλημα της αναγνώρισης και αντιμετώπισης περιστατικών ασφάλειας και προσεγγίζεται τη δυνατότητα διασφάλισης υπολογιστικών και δικτυακών επικοινωνιών προτείνοντας διοικητικές και τεχνικές προσεγγίσεις που βασίζονται σε μια σειρά μηχανισμών και μεθοδολογιών ασφάλειας.

Αρχικά παρουσιάζεται μια εννοιολογική θεμελίωση για το σύνολο των όρων που χρησιμοποιούνται στην ερευνητική περιοχή της αντιμετώπισης περιστατικών ασφάλειας, μέσα από μια ταξονομία που κατηγοριοποιεί τους όρους αυτούς, καθώς και τις μεταξύ τους συσχετίσεις.

Στη συνέχεια, αναλύονται εκτενώς τα ζητήματα αντιμετώπισης περιστατικών ασφάλειας πληροφοριών σε ένα εταιρικό περιβάλλον, ενώ προτείνεται ένα πρότυπο διοικητικό μοντέλο που βασίζεται τόσο σε ακαδημαϊκή και εφαρμοστέα έρευνα, όσο και σε βέλτιστες διεθνείς πρακτικές, πρότυπα ασφάλειας πληροφοριών και τεχνολογικές υλοποιήσεις. Επίσης, προτείνεται μια δομημένη μεθοδολογία για το χειρισμό περιστατικών ασφάλειας και παρουσιάζονται αναλυτικά οι διάφορες φάσεις της συγκεκριμένης μεθοδολογίας.

Στη συνέχεια, προσεγγίζεται η επίλυση τεχνικών ζητημάτων στην αντιμετώπιση περιστατικών ασφάλειας, μέσω καθορισμού των απαραίτητων πληροφοριών ασφάλειας, ενώ προτείνονται και αναλύονται εκτενώς οι απαιτήσεις ενός συστήματος αντιμετώπισης περιστατικών.

Προτείνεται και παρουσιάζεται το Σύστημα Ευφυούς Αντιμετώπισης Περιστατικών (Incident Response Intelligence System - IRIS), το οποίο κατανοεί το γενικότερο περιβάλλον των αδυναμιών ασφάλειας που ανακαλύπτονται από εργαλεία αυτόματης αξιολόγησης επικινδυνότητας, βαθμολογεί τη σημαντικότητά τους με προτυποποιημένο τρόπο, βρίσκει και συσχετίζει τον κώδικα εκμετάλλευσης που σχετίζεται με αυτές τις αδυναμίες και καθορίζει τις απαραίτητες υπογραφές ανίχνευσης παρεισφρήσεων.

Τέλος, αξιολογείται η ορθότητα της υλοποίησης του IRIS, παρουσιάζονται και αξιολογούνται μια σειρά από πειραματικά δεδομένα για τον έλεγχο των αποτελεσμάτων του συστήματος και αξιολογείται η λειτουργία του IRIS σε πραγματικό περιβάλλον.

ABSTRACT

EFFECTIVE MANAGEMENT SUPPORT ON NETWORK AND COMMUNICATIONS SECURITY: IDENTIFYING AND RESPONDING TO SECURITY INCIDENTS

Dimitrios G. Patsos

This work approaches a series of issues related to security incident identification and response, as well as the capability of information technology and communication systems security through effective management and technical mechanisms.

We initially propose a taxonomy that includes the main concepts of the research area, by defining relative terminology and examining the interrelationships between the basic terms.

We discuss in detail the main issues of incident identification and response within a corporate environment, while we propose a magamenent framework based on academic and applied research, as well as international best practices, security standards and technical implementations. Furthermore, we propose a structured methodology and discuss in detail every distinct phase of this methodology.

Furthermore, we approach the technical issues related to incident identification and response, while we propose and discuss in detail the requirements of an incident identification and response system.

We then propose and present the Incident Response Intelligence System - IRIS, a system performing topological analysis to vulnerabilities identified by associated tools, scoring their significance with a standardized method, while also correlates the relative exploit code and defines the corresponding intrusion detection signatures for these vulnerabilities.

Finally, we evaluate IRIS implementation against the design specifications, present and discuss a series of experimental data and we evaluate IRIS functionality in real-world scenarios.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΥΧΑΡΙΣΤΙΕΣ **6**

ΠΕΡΙΛΗΨΗ **7**

ABSTRACT **9**

1. Εισαγωγή **19**

1.1. Γενικά 20

1.2. Αναγνώριση και αντιμετώπιση περιστατικών ασφάλειας 21

1.2.1. Τεχνικά ζητήματα *22*

1.2.2. Διοικητικά ζητήματα *25*

1.3. Περιγραφή του προβλήματος – στόχος της διατριβής 26

1.4. Προτεινόμενη λύση – μεθοδολογία της διατριβής 29

1.5. Οργάνωση της διατριβής 33

2. Εννοιολογική Θεμελίωση **37**

2.1. Εισαγωγή 38

2.2. Γεγονότα ασφάλειας πληροφοριών 39

2.2.1. Ενέργειες και αντικείμενα *40*

2.3. Επιθέσεις ασφάλειας πληροφοριών 47

2.3.1. Τεχνικές *48*

2.3.2. Αδυναμίες *50*

2.3.3. Αποτέλεσμα *50*

2.4. Περιστατικά ασφάλειας πληροφοριών 51

2.4.1. Επιτιθέμενοι και στόχοι *52*

2.5. Ανακεφαλαίωση 55

3. Αντιμετώπιση περιστατικών ασφάλειας πληροφοριών **57**

3.1. Εισαγωγή 59

3.2. Η διοικητική πλευρά της αντιμετώπισης περιστατικών ασφάλειας πληροφοριών 60

3.2.1. Διοικητικό μοντέλο αντιμετώπισης περιστατικών ασφάλειας *62*

3.3. Μεθοδολογία αντιμετώπισης περιστατικών ασφάλειας 65

3.3.1. Προετοιμασία *67*

3.3.2. Αναγνώριση *73*

3.3.3. Περιορισμός *79*

3.3.4. Εξάλειψη *82*

3.3.5. Ανάκαμψη *84*

3.3.6. Επακόλουθα *85*

3.4. Ιχνηλάτηση περιστατικών ασφάλειας 85

3.4.1. Τεχνικές αυτόματης ιχνηλάτησης με σήμανση IP ... *87*
3.4.2. Τεχνικές ιχνηλάτησης με βάση το ICMP ... *87*
3.4.3. Τεχνικές ιχνηλάτησης με χρήση σηράγγων IP ... *89*
3.4.4. Τεχνικές ιχνηλάτησης σε δικτυακούς σταθμούς ... *90*
3.4.5. Τεχνικές ιχνηλάτησης σε επίπεδο εφαρμογής ... *91*
3.4.6. Κατηγοριοποίηση μηχανισμών ιχνηλάτησης ... *92*
3.5. Ανάλυση ψηφιακών πειστηρίων ... 92
3.5.1. Ανάλυση ψηφιακών πειστηρίων σε υπολογιστή ... *93*
3.5.2. Ανάλυση ψηφιακών πειστηρίων σε δίκτυο υπολογιστών ... *94*
3.5.3. Ανάλυση ψηφιακών πειστηρίων σε λογισμικό ... *95*
3.6. Ενδεικτική διαδικασία αντιμετώπισης περιστατικών ασφάλειας σε εταιρικά περιβάλλοντα ... 96
3.6.1. Επίπεδο κλιμάκωσης 0 ... *98*
3.6.2. Επίπεδο κλιμάκωσης 1 ... *98*
3.6.3. Επίπεδο κλιμάκωσης 2 ... *98*
3.6.4. Επίπεδο κλιμάκωσης 3 ... *99*
3.6.5. Περαιτέρω ανάλυση ... *99*
3.7. Ανοικτά ζητήματα ... 100
3.8. Ανακεφαλαίωση ... 101
4. Τοπολογική Ανάλυση Αδυναμιών Ασφάλειας Πληροφοριών ... 103
4.1. Εισαγωγή ... 104
4.2. Τοπολογική ανάλυση αδυναμιών και αντιμετώπιση περιστατικών ασφάλειας ... 105
4.3. Απαιτούμενες πληροφορίες ασφάλειας στην τοπολογική ανάλυση αδυναμιών ... 106
4.3.1. Καθορισμός πληροφοριών για αδυναμίες ασφάλειας ... *110*
4.3.2. Καθορισμός πληροφοριών για εκμεταλλεύσεις ... *113*
4.4. Τοπολογική ανάλυση αδυναμιών ασφάλειας και συστήματα IDP ... 115
4.4.1. Ανάπτυξη συστημάτων IDP με χρήση ζωνών ασφάλειας ... *115*
4.4.2. Ανάπτυξη συστημάτων IDP με χρήση ιδεατών τοπικών δικτύων ... *118*
4.4.3. Ανάπτυξη συστημάτων IDP με χρήση τεχνικών τοπολογικής ανάλυσης αδυναμιών ... *121*
4.5. Απαιτήσεις συστημάτων διαχείρισης πληροφοριών ασφάλειας στην αντιμετώπιση περιστατικών ... 123
4.5.1. Ανοικτή αρχιτεκτονική και πρότυπα μορφότυπα πληροφοριών ... *123*
4.5.2. Ενοποίηση με εργαλεία αποτίμησης αδυναμιών ασφάλειας και συστήματα ανίχνευσης και αποτροπής παρεισφρήσεων ... *124*
4.5.3. Βάση γνώσης ... *125*
4.5.4. Ανανέωση πληροφοριών ... *126*
4.5.5. Χειρισμός εξαιρέσεων ... *126*
4.5.6. Οπτικοποίηση πληροφορίας ... *127*

4.6. Ανακεφαλαίωση ... 129
5. Το Σύστημα Ευφυούς Αντιμετώπισης Περιστατικών IRIS ... 131
5.1. Σχετική έρευνα ... 132
5.2. Σύστημα ευφυούς αντιμετώπισης περιστατικών ... 135
5.2.1. Δυνατότητες του συστήματος ... 135
5.2.2. Τρόπος λειτουργίας ... 136
5.2.3. Αρχιτεκτονική συστήματος ... 149
5.2.4. Παρουσίαση πρωτοτύπου ... 154
5.2.5. Παρουσίαση λειτουργίας ... 156
5.2.6. Πλεονεκτήματα του IRIS στην αντιμετώπιση περιστατικών ... 159
5.3. Ανακεφαλαίωση ... 162
6. Αποτελέσματα και Αξιολόγηση ... 163
6.1. Εισαγωγή ... 164
6.2. Αξιολόγηση πληρότητας χαρακτηριστικών ... 164
6.2.1. Ανοικτή αρχιτεκτονική και πρότυποι μορφότυποι πληροφοριών ... 164
6.2.2. Ενοποίηση με εργαλεία αποτίμησης αδυναμιών ασφάλειας και συστήματα ανίχνευσης και αποτροπής παρεισφρήσεων ... 165
6.2.3. Βάση γνώσης & ανανέωση πληροφοριών ... 166
6.2.4. Χειρισμός εξαιρέσεων ... 167
6.2.5. Οπτικοποίηση πληροφορίας ... 169
6.2.6. Συμπεράσματα ... 169
6.3. Αξιολόγηση ορθότητας αποτελεσμάτων ... 170
6.3.2. Συμπεράσματα ... 174
6.4. Αξιολόγηση βελτίωσης στην παραμετροποίηση των συστημάτων IDP ... 175
6.4.1. Σενάριο 1: Υποδομή Σταθμών Διαδικτύου ... 176
6.4.2. Σενάριο 2: Υποδομή Σσταθμών Εργασίας ... 177
6.4.3. Σενάριο 3: Υποδομή Εξυπηρετητών ... 179
6.4.4. Σχολιασμός αποτελεσμάτων μετρήσεων ... 182
6.5. Συμπεράσματα χρηστών ... 183
6.5.1. Ανάλυση και αξιολόγηση δείγματος ... 183
6.5.2. Ανάλυση και αξιολόγηση απαιτήσεων ... 187
6.5.3. Ανάλυση και αξιολόγηση των λειτουργιών του IRIS ... 189
6.5.4. Προτάσεις και σχόλια χρηστών ... 194
6.5.5. Προτάσεις και συμπεράσματα ... 195
6.6. Χαρακτηριστικά της διαδικασίας αξιολόγησης ... 196
6.7. Ανακεφαλαίωση ... 197
7. Συμπεράσματα και Μελλοντική Έρευνα ... 199

7.1. Συμπεράσματα 200
7.2. Προτάσεις για μελλοντική έρευνα 203

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 4-1: Πλήθος δημοσιευμένων αδυναμιών κατά CVE (ανά έτος) (Πηγή: Πανεπιστήμιο Purdue) ... 111
Εικόνα 4-2: Δημοσιευμένες αδυναμίες ασφάλειας ανά έτος (έως 5/2009) (Πηγή: National Vulnerability Database, NIST) ... 126
Εικόνα 5-1: Βαθμολόγηση *αδυναμιών*, περιγραφή και αναζήτηση στη βάση SIG ... 158
Εικόνα 5-2: Παραπομπές σε σχετικές πηγές πληροφοριών για την αδυναμία CVE-2003-0854 ... 159
Εικόνα 5-3: Συσχετισμένες υπογραφές Snort και πολιτικές αντιμετώπισης ... 159
Εικόνα 6-1: Ενοποίηση του IRIS με τα εργαλεία Nessus και Snort ... 166
Εικόνα 6-2: Χειρισμός Εξαιρέσεων στο IRIS (Βήμα 1) ... 167
Εικόνα 6-3: Χειρισμός εξαιρέσεων στο IRIS (Βήμα 2) ... 168
Εικόνα 6-4: Οπτικοποίηση πληροφορίας ... 169
Εικόνα 6-5: Βαθμολόγηση ιστορικών μετρικών για αδυναμίες ασφάλειας ... 172
Εικόνα 6-6: Κατασκευή μονοπατιών επίθεσης και αντιμετώπισης ... 174

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 3-1: Πλεονεκτήματα και μειονεκτήματα των διαφορετικών τύπων CSIRT (Van Wyk, 2001) 61
Πίνακας 3-2: Κατηγοριοποίηση σημαντικότητας περιστατικών ασφάλειας, ανάλογα με τις επιπτώσεις 77
Πίνακας 3-3: Κατηγοριοποίηση μηχανισμών ιχνηλάτησης περιστατικών ασφάλειας (Mitropoulos, Patsos & Douligeris, 2005) 92
Πίνακας 5-2: Διαδικτυακές πηγές εργαλείων υπολογισμού τιμής CVSSv2 (NVD, 2009) 140
Πίνακας 5-3: Κατηγορίες και τιμές μετρικών για βασικά χαρακτηριστικά αδυναμιών 140
Πίνακας 5-4: Κατηγορίες και τιμές μετρικών για ιστορικά χαρακτηριστικά αδυναμιών 141
Πίνακας 5-5: Κατηγορίες και τιμές μετρικών για περιβαλλοντικά χαρακτηριστικά αδυναμιών 142
Πίνακας 6-1: Σχεδιαστικές απαιτήσεις και αποτελέσματα υλοποίησης του IRIS 170
Πίνακας 6-2: Αποτελέσματα για υποδομή σταθμών Διαδικτύου 177
Πίνακας 6-3: Αποτελέσματα για υποδομή σταθμών εργασίας 178
Πίνακας 6-4: Αποτελέσματα για υποδομή εξυπηρετητών 179
Πίνακας 6-5: Είδος Οργανισμού του χρήστη 184
Πίνακας 6-6: Πλήθος υπαλλήλων στον Οργανισμό του χρήστη 185
Πίνακας 6-7: Ρόλος χρήστη στον Οργανισμό 185
Πίνακας 6-8: Χρόνια απασχόλησης με την Ασφάλεια Πληροφοριών 186
Πίνακας 6-9: Περιοχές της ασφάλειας πληροφοριών στις οποίες διαθέτουν σχετική εμπειρία οι χρήστες 186
Πίνακας 6-10: Αξιολόγηση ζητημάτων που σχετίζονται με την Αντιμετώπιση Περιστατικών Ασφάλειας από τους χρήστες 187
Πίνακας 6-11: Χαρακτηριστικά εργαλείου αντιμετώπισης περιστατικών ασφάλειας που επιθυμούν οι χρήστες 189
Πίνακας 6-12: Αξιολόγηση της διεπαφής του IRIS 190
Πίνακας 6-13: Αξιολόγηση ποσότητας πληροφοριών που διαχειρίζεται το IRIS 190
Πίνακας 6-14: Αξιολόγηση δυνατότητας βαθμολόγησης των αδυναμιών ασφάλειας του IRIS 191
Πίνακας 6-15: Αξιολόγηση συσχέτισης των αδυναμιών με τα exploits και με τις υπογραφές intrusion detection 191
Πίνακας 6-16: Αξιολόγηση ταχύτητας υπολογισμών του IRIS 192
Πίνακας 6-17: Αξιολόγηση διάδρασης του IRIS με το χρήστη 193
Πίνακας 6-18: Αξιολόγηση συνολικών δυνατοτήτων του IRIS 193
Πίνακας 6-19: Αξιολόγηση πλατφόρμας του IRIS 194
Πίνακας 6-20: Χαρακτηριστικά βελτίωσης του IRIS 195
Πίνακας 6-21: Αξιολόγηση ερωτηματολογίου 195

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Σχήμα 2-1: Περιστατικό ασφάλειας πληροφοριών, επίθεση και γεγονός ασφάλειας 38
Σχήμα 2-2: Η χρήση επιθέσεων για την επίτευξη των στόχων του επιτιθέμενου 51
Σχήμα 2-3: Εννοιολογική θεμελίωση γεγονότων, επιθέσεων και περιστατικών ασφάλειας 54
Σχήμα 3-1: Διοικητικό Μοντέλο Αντιμετώπισης Περιστατικών Ασφάλειας 63
Σχήμα 3-2: Μεθοδολογία Αντιμετώπισης Περιστατικών Ασφάλειας 68
Σχήμα 3-3: Διαδικασία χειρωνακτικής ανάλυσης αρχείων ελέγχου και καταγραφής και αποφάσεις 76
Σχήμα 3-4: Η επικεφαλίδα του πρωτοκόλλου IP και το πεδίο επιλογών 88
Σχήμα 3-5: Ενδεικτική Διαδικασία Αντιμετώπισης Περιστατικών Ασφάλειας 97
Σχήμα 4-1 - Ένα μονοπάτι επίθεσης a_i , σε σχέση με τις v_k και e_j 112
Σχήμα 4-2 – Ένα ενδεικτικό μονοπάτι αντιμετώπισης 114
Σχήμα 4-3 – Μια τυπική διάταξη συστημάτων και αισθητήρων IDP σε λογικές ζώνες ενός δικτύου 117
Σχήμα 4-4 - Ανάπτυξη IDP συστημάτων σε ιδεατά τοπικά δίκτυα 119
Σχήμα 5-1 – Καθορισμός τιμής CVSSv2 με χρήση του υπολογιστή NVD 139
Σχήμα 5-2 – Τα δομοστοιχεία του συστήματος IRIS 143
Σχήμα 5-3 – Η αρχιτεκτονική του Συστήματος IRIS 149
Σχήμα 5-4: Διαμόρφωση Εργαστηριακού Δικτύου 157

Κεφάλαιο 1

Εισαγωγή

Every idea corresponds to an imperceptible lesion of the mind

- **M. Cioran**

1.1. Γενικά

Η ανάπτυξη του Διαδικτύου και η στενή εξάρτηση των ιδιωτών και των επιχειρήσεων από τις τεχνολογίες της πληροφορικής και των επικοινωνιών (ΤΠΕ) έχει επηρεάσει σε πολύ μεγάλο βαθμό τον τρόπο με τον οποίο οι οργανισμοί διεξάγουν τις επιχειρηματικές δραστηριότητές τους. Εκτός από τη μεταφορά των φυσικών επιχειρηματικών συναλλαγών και δραστηριοτήτων στα ηλεκτρονικά μέσα και τα πληροφοριακά συστήματα (ΠΣ), οι ΤΠΕ δημιούργησαν εκ του μηδενός νέες επιχειρηματικές δραστηριότητες, νέες ευκαιρίες και νέες αγορές. Η αλματώδης υιοθέτηση εφαρμογών και υποδομών, ειδικότερα τα τελευταία είκοσι χρόνια, συνέβαλε στη δημιουργία ενός νέου επιχειρηματικού τοπίου, χωρίς γεωγραφικούς, χρονικούς, συναλλαγματικούς ή κοινωνικοπολιτικούς περιορισμούς. Σε αυτό το τοπίο, αναπτύχθηκαν αναρίθμητες ηλεκτρονικές υπηρεσίες πολιτικού, εκπαιδευτικού, οικονομικού, ψυχαγωγικού και εμπορικού χαρακτήρα.

Από την άλλη πλευρά, το παραπάνω φαινόμενο δεν είναι άμοιρο ανθρωπίνων συμπεριφορών, καθώς –παράλληλα- αναπτύχθηκαν πολλαπλές κοινωνικές ομάδες με σκοπό την αθέμιτη εκμετάλλευση των ΠΣ για προσωπικό, πολιτικό ή οικονομικό όφελος.

Η *ασφάλεια πληροφοριών* είναι η επιστήμη που στοχεύει στην *πρόληψη, ανίχνευση, αντιμετώπιση και ανάκαμψη* από μη-εξουσιοδοτημένες ενέργειες (Gollmann, 1999), ώστε να διαφυλάττει την *εμπιστευτικότητα*, την *ακεραιότητα* και τη *διαθεσιμότητα* των πληροφοριών (ISO/IEC, 2005). Παράλληλα με την ανάπτυξη των ΤΠΕ, τόσο η ερευνητική κοινότητα όσο και η βιομηχανία ασφάλειας πληροφοριών ανέπτυξαν ένα πολύ μεγάλο πλήθος μηχανισμών (τεχνολογιών, μεθοδολογιών και μεθόδων) για την επίτευξη των παραπάνω στόχων, εστιάζοντας κυρίως στην πρόληψη και ανίχνευση ενεργειών με αρνητικό αντίκτυπο στις ιδιότητες ασφάλειας των ΠΣ. Κάθε τέτοια ενέργεια χαρακτηρίζεται ως *περιστατικό ασφάλειας* από τη σχετική βιβλιογραφία (CERT/CC, 1998).

Γενικά, ένα *περιστατικό ασφάλειας πληροφοριών* ορίζεται ως το αποτέλεσμα συγκεκριμένων ενεργειών που εκτελεί ένας επιτιθέμενος σε ένα πληροφοριακό σύστημα (βλ. ενότητα 2.4), μετά από την επιτυχή εκμετάλλευση των αδυναμιών (vulnerabilities) του ΠΣ ή της υποδομής σε λογικό επίπεδο. Ανεξάρτητα από την ικανότητα των προληπτικών ή ανιχνευτικών μηχανισμών ασφάλειας που λειτουργούν σε ένα πληροφοριακό σύστημα, η έγκαιρη αντιμετώπιση ενός περιστατικού στοχεύει αφενός στην ακριβή ανάλυση των χαρακτηριστικών του (αναγνώριση) και, αφετέρου, με βάση αυτήν την ανάλυση, στον καθορισμό των απαιτούμενων ενεργειών που θα περιορίσουν την έκταση και τις συνέπειές του στο ΠΣ και θα εμποδίσουν μελλοντική επανεμφάνισή του (αντιμετώπιση).

Οι παραπάνω ενέργειες χαρακτηρίζουν την ερευνητική περιοχή της αντιμετώπισης περιστατικών ασφάλειας πληροφοριών, που έχει τόσο τεχνικό όσο και διοικητικό χαρακτήρα σε ένα πληροφοριακό σύστημα. Χωρίς βλάβη της γενικότητας, υποθέτουμε πως η αντιμετώπιση περιστατικών ασφάλειας συμπεριλαμβάνει και τις απαραίτητες ενέργειες αναγνώρισής τους.

Τέλος, η αντιμετώπιση περιστατικών ασφάλειας συνδέεται στενά με πολλές άλλες ερευνητικές περιοχές της ασφάλειας πληροφοριών, όπως είναι η *αποτίμηση ή διαχείριση επικινδυνότητας* (vulnerability management ή assessment, αντίστοιχα), η *διαχείριση ασφάλειας πληροφοριακών συστημάτων* (risk management), τα *συστήματα ανίχνευσης και αντιμετώπισης παρεισφρήσεων* (Intrusion Detection and Prevention Systems - IDP), *οι μηχανισμοί αυτόματης ιχνηλάτησης* (automated trace-back mechanisms), η *ανάλυση ψηφιακών πειστηρίων* (digital forensics), κτλ.

1.2. Αναγνώριση και αντιμετώπιση περιστατικών ασφάλειας

Στην αντιμετώπιση περιστατικών ασφάλειας, η *σημαντικότητα* (severity) και η *έκταση* (magnitude) ενός περιστατικού είναι οι κύριοι παράγοντες που καθορίζουν την προτεραιότητα και τους τρόπους αντιμετώπισής του. Η σημαντικότητα ενός περιστατικού μπορεί να καθοριστεί αναλύοντας εκτενώς και με προτυποποιημένο τρόπο τα χαρακτηριστικά και τις συσχετίσεις των αδυναμιών ασφάλειας ενός ΠΣ, ή των

επιμέρους δομοστοιχείων αυτού (π.χ. συνδυασμός επιτυχών εκμεταλλεύσεων αδυναμιών για τη δημιουργία επίθεσης, ύπαρξη κώδικα αθέμιτης εκμετάλλευσης για συγκεκριμένες αδυναμίες, ύπαρξη διορθωτικών εκδόσεων από τον κατασκευαστή του λογισμικού, κτλ.), ενώ η έκταση μιας επίθεσης μπορεί να καθοριστεί αναλύοντας με προτυποποιημένο τρόπο τα ποσοτικά χαρακτηριστικά μιας επίθεσης (π.χ. ποσοστό ευάλωτων συστημάτων σε μια υποδομή).

Αξιωματικά, το γινόμενο της σημαντικότητας επί την έκταση ενός περιστατικού ασφάλειας εκφράζει την *προτεραιότητα* αντιμετώπισής του, ήτοι $P = S * M$, όπου P η *προτεραιότητα* (priority) αντιμετώπισης ενός περιστατικού, S η *σημαντικότητά* (severity) του και M η *έκτασή* (magnitude) του. Με βάση τη θεμελιώδη αυτή εξίσωση, ο καθορισμός της προτεραιότητας για την αντιμετώπιση περιστατικών ασφάλειας έγκειται στην εύρεση, αξιολόγηση και συσχέτιση πληροφοριών για τη σημαντικότητα και την έκταση ενός περιστατικού ασφάλειας.

Επαγωγικά, η εύρεση της πληροφορίας αυτής ανάγεται στην *εύρεση, αξιολόγηση και συσχέτιση* πρωτογενούς πληροφορίας σχετικά με αδυναμίες ασφάλειας για την εξαγωγή συμπερασμάτων που καθορίζουν τις ενέργειες αντιμετώπισής του.

1.2.1. Τεχνικά ζητήματα

Τα σημαντικότερα ζητήματα που σχετίζονται με την εύρεση, αξιολόγηση και συσχέτιση πρωτογενούς πληροφορίας ασφάλειας είναι:

- Η πρωτογενής πληροφορία ασφάλειας προέρχεται από **ετερογενείς πηγές**: η σχετική πληροφορία για αδυναμίες ασφάλειας σε μια υποδομή παράγεται – κυρίως- από εργαλεία εύρεσης και αποτίμησης αδυναμιών ασφάλειας, καθώς και από συστήματα ανίχνευσης και αποτροπής παρεισφρήσεων (Intrusion Detection and Prevention Systems – IDPs)[1]. Από την άλλη πλευρά, πληροφορία ασφάλειας

[1] Τα συγκεκριμένα συστήματα διαθέτουν, εκ κατασκευής, πολύ μεγάλες δυνατότητες ανάλυσης και αξιολόγησης δικτυακής κυκλοφορίας, ενώ παράγουν μεγάλο όγκο πληροφορίας ασφάλειας. Μία πλήρης περιγραφή των εν λόγω συστημάτων δίνεται στο (Scarfone, 2007)

υπάρχει διάσπαρτη σε δικτυακούς τόπους, θεματικές λίστες ηλεκτρονικού ταχυδρομείου, ιστοτόπους ανεξάρτητων ερευνητών αλλά και ιστοτόπους επιτιθέμενων.

- Η πρωτογενής πληροφορία ασφάλειας βρίσκεται σε **διαφορετικούς μορφότυπους** (formats): ανάλογα με τον τρόπο παραγωγής της, η πληροφορία μπορεί να βρίσκεται σε μορφότυπο ιστοσελίδας, μηνύματος ηλεκτρονικού ταχυδρομείου, πηγαίου κώδικα διαφόρων γλωσσών προγραμματισμού, αρχείου συστήματος, ή –τέλος- σε ιδιόκτητο μορφότυπο (proprietary format).
- Η πρωτογενής πληροφορία ασφάλειας έχει **πολλαπλές ανάγκες ταξινόμησης** και **κανονικοποίησης.** Ανάλογα με το τι αφορά, από πού παράγεται και τον τύπο του μορφοτύπου της, η πρωτογενής πληροφορία για αδυναμίες ασφάλειας, ταξινομείται σε μια από τις τρεις κύριες κατηγορίες:
    - Πληροφορία σχετική με αδυναμίες ασφάλειας (vulnerability information), η οποία μαρτυρά ένα πιθανό σύστημα-στόχο
    - Πληροφορία σχετική με κώδικα αθέμιτης εκμετάλλευσης (exploit information), ο οποίος αποδεικνύει τον τρόπο με τον οποίο κάποιος εκμεταλλεύεται μια αδυναμία
    - Υπογραφή συστήματος IDP (IDP/signature information), η οποία μαρτυρά την ύπαρξη μηχανισμού αντιμετώπισης της συγκεκριμένης αδυναμίας.

Μετά την επιτυχή συλλογή, κανονικοποίηση και ταξινόμηση της πρωτογενούς πληροφορίας ασφάλειας, η αντιμετώπιση ενός περιστατικού ασφάλειας απαιτεί τη συσχέτιση και την επεξεργασία της εν λόγω πληροφορίας, τόσο για την εύρεση των σχέσεων των αδυναμιών μεταξύ τους, όσο και για τη βαθμολόγηση των βασικών, ιστορικών και περιβαλλοντικών χαρακτηριστικών των αδυναμιών ασφάλειας. Οι επιθέσεις διεξάγονται με την επιτυχή εκμετάλλευση αδυναμιών ασφάλειας με προκαθορισμένη σειρά, άρα είναι ιδιαίτερα σημαντικό να βρεθεί ένα μοντέλο συσχέτισης των αδυναμιών μεταξύ τους. Από την άλλη πλευρά, κάθε αδυναμία διαθέτει βασικά χαρακτηριστικά (π.χ. δυνατότητα τοπικής ή απομακρυσμένης εκμετάλλευσης, πολυπλοκότητα πρόσβασης, επακόλουθα στην εμπιστευτικότητα/ακεραιότητα ή/και

διαθεσιμότητα ενός συστήματος), ιστορικά χαρακτηριστικά (π.χ. αποδεδειγμένη ύπαρξη κώδικα αθέμιτης εκμετάλλευσης, ύπαρξη διορθωτικού λογισμικού, κτλ.) καθώς και περιβαλλοντικά χαρακτηριστικά, τα οποία εξαρτώνται από το ιδιαίτερο περιβάλλον στο οποίο ανακαλύπτεται μια συγκεκριμένη αδυναμία. Η αξιολόγηση των παραπάνω χαρακτηριστικών είναι ζήτημα μείζονος σημασίας για τις ενέργειες που αφορούν στην επιτυχή αντιμετώπιση ενός περιστατικού ασφάλειας. Μέχρι και σήμερα, τα παραπάνω ζητήματα παραμένουν ανοικτά για αρκετούς λόγους.

Τα εργαλεία αυτοματοποιημένης αποτίμησης αδυναμιών παράγουν ένα μεγάλο σύνολο πληροφορίας, χωρίς ένδειξη συσχέτισης των αδυναμιών που ανακαλύπτουν. Για παράδειγμα, το πρότυπο εργαλείο Nessus και το δημοφιλές εργαλείο Qualys κατηγοριοποιούν τις αδυναμίες που ανακαλύπτουν σε μια υποδομή, ανάλογα με τη σημαντικότητά τους[2], σε υψηλής σημαντικότητας, μετρίας σημαντικότητας, χαμηλής σημαντικότητας και σε πληροφορίες πολύ χαμηλής σημαντικότητας (πληροφοριακά ευρήματα). Αυτά τα δύο χαρακτηριστικά (έλλειψη συσχέτισης αδυναμιών μεταξύ τους και έλλειψη κοινά αποδεκτού συστήματος αξιολόγησης) εισάγουν ένα ιδιαίτερα σημαντικό πρόβλημα στους διαχειριστές ασφάλειας, καθώς δεν παρέχουν μια ολοκληρωμένη προσέγγιση για την αντιμετώπιση των αδυναμιών.

Με άλλα λόγια, ένας διαχειριστής ασφάλειας δεν γνωρίζει με ποιες ενέργειες μπορεί να αντιμετωπίσει τα ευρήματα της διαδικασίας αποτίμησης επικινδυνότητας, αλλά ούτε και με ποια σειρά πρέπει να εφαρμόσει τις συγκεκριμένες ενέργειες (O'Hare, Noel, & Prole, 2008). Πιο συγκεκριμένα , η έλλειψη ενός τρόπου συσχέτισης των αδυναμιών, ώστε να παράγονται πληροφορίες σχετικές με επιθέσεις, δεν παρέχει την πλούσια εικόνα για την ασφάλεια ενός οργανισμού, παρά μόνο αποφάσεις τοπικής σημασίας για συγκεκριμένες αδυναμίες.

Τα συστήματα IDP παράγουν, επίσης, έναν μεγάλο όγκο πληροφορίας σχετιζόμενο με επιθέσεις σε συστήματα που εμφανίζουν αδυναμίες ασφάλειας. Οι πληροφορίες αυτές, ονομαζόμενες και συναγερμοί (alerts) στη σχετική ορολογία, είναι διακριτές για κάθε

[2] Χωρίς ωστόσο κάποιο κοινά αποδεκτό κριτήριο που ορίζει τη σημαντικότητα.

περίπτωση και προέρχονται από διακριτές υπογραφές που αντιμετωπίζουν συγκεκριμένα είδη επιθέσεων ή αδυναμιών (χωρίς σαφή διαχωρισμό μεταξύ τους). Με τον τρόπο αυτόν, είναι αρκετά συνηθισμένο το φαινόμενο να παράγονται λανθασμένοι συναγερμοί που προέρχονται είτε από δικτυακή κυκλοφορία που δεν αποτελεί επίθεση είτε από επιθέσεις που δεν αντιμετωπίστηκαν από συγκεκριμένες υπογραφές (Aberdeen Group, 2003). Επίσης, οι συναγερμοί που παράγονται από τα συγκεκριμένα συστήματα είναι απομονωμένοι σε σχέση με το γενικότερο περιβάλλον, καθώς τα συστήματα IDP εφαρμόζουν πολιτικές σε τοπικό επίπεδο αγνοώντας τη συνολική υποδομή (Jajodia, Noel, & O'Berry, 2006). Ενδεικτικά και μόνο μια απόφαση που βασίζεται σε λανθασμένο συναγερμό (π.χ. λανθασμένος χαρακτηρισμός μιας δικτυακής συνόδου ως επίθεσης) μπορεί να έχει δραματικές συνέπειες ανάλογα με την πολιτική που εφαρμόζει το σύστημα IDP (π.χ. διακοπή της συνόδου, αναδρομολόγηση κυκλοφορίας, κατασπατάληση υπολογιστικών πόρων κτλ.).

1.2.2. Διοικητικά ζητήματα

Από την άλλη πλευρά, υπάρχουν πολλαπλά διοικητικά και διαχειριστικά ζητήματα που πηγάζουν από τα προαναφερθέντα, καθώς απαιτούνται αυστηρά καθορισμένοι ρόλοι και διαδικασίες τόσο για την αποτελεσματική συλλογή και επεξεργασία των πληροφοριών που αφορούν στην αναγνώριση των περιστατικών, όσο και για τη λήψη και εφαρμογή αποφάσεων για την αντιμετώπισή τους.

Η αντιμετώπιση περιστατικών ασφάλειας αποτελεί μια εταιρική διαδικασία (ISO/IEC, 2005). Ως εκ τούτου, απαιτείται ένα καλά ορισμένο διοικητικό πλαίσιο το οποίο καθορίζει τους ρόλους και τις αρμοδιότητες των συμμετεχόντων, καθώς και τα κανάλια ενημέρωσης και ανταλλαγής πληροφοριών καθ' όλη τη διάρκεια ζωής ενός περιστατικού. Για παράδειγμα, όταν ένα περιστατικό έχει λάβει μεγάλες διαστάσεις μέσα σε έναν οργανισμό και απαιτείται η διακοπή της λειτουργίας μέρους ή και ολόκληρου του ΠΣ προκειμένου να αποφευχθούν περαιτέρω προβλήματα, η απόφαση αυτή πρέπει να ληφθεί μέσα από συγκεκριμένα διοικητικά κανάλια, εφόσον έχει αξιολογηθεί ο αντίκτυπος της συγκεκριμένης ενέργειας στη συνολική λειτουργία του οργανισμού.

Τέλος, η αναγνώριση και αντιμετώπιση περιστατικών ασφάλειας, δεδομένης και της πολυπλοκότητας που εμφανίζουν τα σύγχρονα ΠΣ, εισάγει την ανάγκη υιοθέτησης μιας μεθοδολογίας, η οποία περιλαμβάνει τις οδηγίες εργασίας για κάθε φάση του κύκλου ζωής ενός περιστατικού.

1.3. Περιγραφή του προβλήματος – στόχος της διατριβής

Το πρόβλημα που καλούμαστε να λύσουμε είναι σύνθετο και πολυδιάστατο:

- *Οριοθέτηση των όρων «περιστατικό ασφάλειας» και «αντιμετώπιση περιστατικού ασφάλειας», γιατί* τόσο η διεθνής βιβλιογραφία όσο και η βιομηχανία ασφάλειας δεν παρέχουν σαφείς πληροφορίες σχετικά με τα περιστατικά ασφάλειας και τους τρόπους αντιμετώπισής τους. Το γεγονός αυτό, συχνά, προκαλεί σύγχυση στους ειδικούς ασφάλειας, ενώ ο μη-πλήρης καθορισμός του όρου επηρεάζει τις ενέργειες που απαιτούνται για την αντιμετώπισή του. Προκειμένου να μπορεί να αναγνωριστεί και να αντιμετωπιστεί ένα περιστατικό ασφάλειας, χρειάζεται να έχουν οριοθετηθεί σαφώς τόσο η σημασία του όρου του, όσο και το εύρος των ενεργειών αντιμετώπισής του,
- *Πολλαπλές συναφείς ερευνητικές περιοχές:* Ιστορικά, η αντιμετώπιση περιστατικών ασφάλειας είναι συνδεδεμένη με τις ερευνητικές περιοχές των μηχανισμών αυτόματης ιχνηλάτησης δικτυακών συνδέσεων (automated trace-back mechanisms), καθώς και της ανάλυσης ψηφιακών πειστηρίων (forensics) σε επίπεδο συστήματος, δικτύου και εφαρμογής. Ωστόσο, οι συγκεκριμένες ερευνητικές περιοχές αναπτύσσονται και εξελίσσονται ανεξάρτητα από την αντιμετώπιση περιστατικών ασφάλειας,
- *Αναγνώριση και ανάλυση περιστατικών ασφάλειας:* Πριν αναζητηθούν τρόποι αντιμετώπισης ενός περιστατικού ασφάλειας, επιβάλλεται η κατανόηση των μεθόδων και των τεχνικών που επέτρεψαν την υλοποίησή του, ήτοι κατανόηση ενός πολύ μεγάλου πλήθους παραμέτρων, όπως αδυναμίες σε υποδομές/συστήματα/λογισμικό/εφαρμογές και δίκτυα, τεχνικές εκμετάλλευσης των αδυναμιών αυτών, αξιολόγηση των αντιμέτρων και των μηχανισμών

ασφάλειας που λειτουργούν στην υποδομή, αντίκτυπος στη λειτουργία του οργανισμού, προτεραιότητα αντιμετώπισής του, κτλ.,

- *Συνδυασμός τεχνικών και διοικητικών μέτρων σε έναν οργανισμό:* εκτός από την κατανόηση των τεχνικών παραμέτρων για την εκδήλωση και αντιμετώπιση ενός περιστατικού ασφάλειας, θα πρέπει να ληφθούν υπόψη και τα διοικητικά μέτρα που απαιτούνται για το σκοπό αυτό. Δεδομένης της στενής εξάρτησης από τα πληροφοριακά συστήματα, η αντιμετώπιση περιστατικών ασφάλειας εμπλέκει ένα μεγάλο σύνολο ανθρώπων από διαφορετικά τμήματα οι οποίοι, με τη σειρά τους, διαθέτουν διαφορετικές τεχνικές δεξιότητες και αρμοδιότητες. Η αντιμετώπιση ενός περιστατικού ασφάλειας (ανάλογα με την επίπτωσή του στις λειτουργίες ενός οργανισμού) είναι πιθανόν να απαιτεί –εκτός από τεχνικές- και πολιτικές, οικονομικές, κοινωνικές ή επικοινωνιακές ενέργειες. Αν και το τελευταίο είναι εκτός των ορίων της συγκεκριμένης διατριβής, ωστόσο αποτελεί ένα υπαρκτό ζήτημα,
- *Περιορισμοί μηχανισμών ασφάλειας:* Η αναγνώριση και αξιολόγηση ενός περιστατικού ασφάλειας εκμεταλλεύεται την υποδομή ασφάλειας ενός Οργανισμού, ιδιαίτερα τα συστήματα ανίχνευσης και αντιμετώπισης παρεισφρήσεων. Τα συστήματα αυτά διαθέτουν πολύ μεγάλες ικανότητες ανάλυσης της δικτυακής κυκλοφορίας και χαρακτηρισμού της ως επίθεσης (ή όχι). Παρ' όλα αυτά, τα εν λόγω συστήματα, λόγω έλλειψης προτυποποιημένης μεθόδου ανάπτυξης, είναι δυνατόν να προβαίνουν σε λανθασμένο χαρακτηρισμό της δικτυακής κυκλοφορίας. Χρειάζεται, λοιπόν, μια περισσότερο συστηματική μελέτη για τον περιορισμό της εμφάνισης ψευδοθετικών ή ψευδοαρνητικών σφαλμάτων (false positive και false negative, αντίστοιχα) προκειμένου να παρέχονται ουσιαστικές πληροφορίες για την αντιμετώπιση μιας επίθεσης,
- *Τοπολογικά κριτήρια ανάλυσης:* ένα περιστατικό ασφάλειας οφείλεται στην επιτυχή εκμετάλλευση αδυναμιών ασφάλειας με μια προκαθορισμένη σειρά (μονοπάτι επίθεσης). Αν δεν υπάρχουν αδυναμίες ασφάλειας, χωρίς βλάβη της γενικότητας, υποθέτουμε πως δεν μπορούν να εκδηλωθούν περιστατικά. Από την άλλη πλευρά, η ανάλυση ενός μονοπατιού επίθεσης οφείλει να συμπεριλαμβάνει τόσο τα βασικά, ιστορικά και περιβαλλοντικά χαρακτηριστικά μιας αδυναμίας,

όσο και την εύρεση διαθέσιμου κώδικα εκμετάλλευσης, καθώς και την εύρεση των κατάλληλων μηχανισμών αντιμετώπισης (υπογραφές ανίχνευσης και αντιμετώπιση παρεισφρήσεων), αφού όλοι αυτοί οι παράγοντες επηρεάζουν τη σημασία και την έκταση του περιστατικού. Από την άλλη πλευρά, σε κάθε μονοπάτι ασφάλειας αντιστοιχεί ένα (ή περισσότερα) μονοπάτια αντιμετώπισης που περιορίζουν την εμφάνιση ή την εκδήλωσή του,

- *Αυτοματοποίηση της αναγνώρισης και αντιμετώπισης περιστατικών:* η ανάλυση των περιστατικών με βάση τα τοπολογικά κριτήρια απαιτεί τη συλλογή, κανονικοποίηση και επεξεργασία ενός μεγάλου πλήθους ετερογενών πληροφοριών. Η αυτοματοποίηση των διεργασιών αυτών με την υλοποίηση ενός συστήματος αντιμετώπισης περιστατικών που απαιτεί μικρή εμπλοκή του χρήστη, μειώνει τον χρόνο που απαιτείται για την αναγνώριση ενός περιστατικού και την παροχή των τεχνικών μέτρων αντιμετώπισής του,
- *Αξιόπιστα αποτελέσματα:* Στόχος ενός συστήματος αντιμετώπισης περιστατικών είναι η αξιόπιστη αναγνώριση, ανάλυση και αντιμετώπιση περιστατικών ασφάλειας. Είναι σημαντικό τα αποτελέσματα που παράγει το σύστημα να είναι εύκολα αντιληπτά και να διευκολύνουν το έργο του διαχειριστή δικτύου στην ανάλυση και αντιμετώπιση των περιστατικών,
- *Αποτελέσματα σε –σχεδόν- πραγματικό χρόνο:* Οι λειτουργίες του συστήματος πρέπει να εκτελούνται σε –σχεδόν- πραγματικό χρόνο, έτσι ώστε να υπάρχει άμεση πληροφόρηση των διαχειριστών του συστήματος για την ύπαρξη του περιστατικού και πρόταση των ενεργειών που έπονται για την αντιμετώπιση του εν λόγω περιστατικού,
- *Διαχείριση και οπτικοποίηση πληροφοριών*: Το σύστημα θα πρέπει να αναλύει και να επεξεργάζεται δεδομένα ασφάλειας, για δικτυακά πρωτόκολλα και υπηρεσίες, που δεν είναι αναγνώσιμα από τον άνθρωπο και να τα παρέχει σε μορφή εύκολα αναγνώσιμης πληροφορίας,
- *Λειτουργίες αξιολόγησης επικινδυνότητας:* Το σύστημα δεν πρέπει να χάνει τη "γενική εικόνα" όταν εξετάζει λεπτομέρειες χαμηλού επιπέδου, ώστε οι αποφάσεις αντιμετώπισης να βασίζονται τόσο στα ιδιαίτερα χαρακτηριστικά της

υποδομής, στην οποία εκδηλώνεται ένα περιστατικό, όσο και στον αντίκτυπο των ενεργειών αντιμετώπισης,

- *Ευκολία χρήσης:* Δεν πρέπει να απαιτείται ο διαχειριστής του συστήματος αντιμετώπισης περιστατικών να έχει υπερβολική ειδίκευση προκειμένου να το διαχειριστεί,
- *Μεταφέρσιμη πλατφόρμα υλοποίησης:* Το εν λόγω σύστημα πρέπει να είναι απλό στην εφαρμογή του. Αυτό μπορεί να επιτευχθεί εάν η πλατφόρμα του συστήματος μπορεί εύκολα να μεταφερθεί σε διαφορετικές αρχιτεκτονικές και λειτουργικά συστήματα, μέσω απλών μηχανισμών εγκατάστασης,
- *Ανανέωση και συντήρηση συστήματος:* Το σύστημα αντιμετώπισης περιστατικών θα πρέπει να έχει τη δυνατότητα ανανέωσης, έτσι ώστε να ανταποκρίνεται σε νέες δικτυακές συνθήκες και επιθέσεις. Πρέπει, λοιπόν, να είναι προσαρμόσιμο τόσο στις αλλαγές της υποδομής που εξετάζει, όσο και στην ποιότητα και ποσότητα των πληροφοριών που επεξεργάζεται. Για παράδειγμα, θα πρέπει να μπορεί να αποτυπώνει στις λειτουργίες του τις νέες εφαρμογές που εγκαθίστανται αλλά και αυτές που καταργούνται, καθώς και την ανανέωση των μηχανισμών ασφάλειας της υποδομής. Επιπροσθέτως, το σύστημα θα πρέπει να είναι προσαρμόσιμο στις δικτυακές επιθέσεις οι οποίες εξελίσσονται καθημερινά. Οι αλλαγές στις δικτυακές επιθέσεις πρέπει να ενσωματώνονται στο σύστημα με εύκολο και διαφανή τρόπο.

1.4. Προτεινόμενη λύση – μεθοδολογία της διατριβής

Προκειμένου να επιλυθεί το πολύπλοκο πρόβλημα που περιγράφηκε στην προηγούμενη ενότητα, ακολουθήθηκε μία προσέγγιση πολλαπλών κατευθύνσεων ώστε να καλύψουμε όλες τις διαστάσεις του προβλήματος. Συγκεκριμένα οι συνεισφορές της διατριβής είναι οι ακόλουθες:

- *Εννοιολογική θεμελίωση όρων αντιμετώπισης περιστατικών:* Τόσο στην ερευνητική κοινότητα όσο και στη βιομηχανία ασφάλειας και την αντίστοιχη βιβλιογραφία, δεν υπάρχει σαφής προσδιορισμός των εννοιών και των όρων που σχετίζονται με τα περιστατικά ασφάλειας, την αναγνώριση και την αντιμετώπισή

τους. Συχνά, οι όροι γεγονός, επίθεση και περιστατικό ασφάλειας δεν είναι διακριτά διαχωρισμένοι προκαλώντας σύγχυση τόσο στην αναγνώριση, όσο και στην ταξινόμηση και την αντιμετώπιση των περιστατικών. Για το σκοπό αυτό, προτείνεται και παρουσιάζεται μια ταξονομία των όρων-εννοιών της γνωστικής περιοχής της αντιμετώπισης περιστατικών, η οποία περιλαμβάνει ορισμούς, εννοιολογικές συσχετίσεις και κατηγοριοποίηση των επιμέρους όρων,

- *Διοικητικό πλαίσιο αντιμετώπισης περιστατικών ασφάλειας σε οργανισμούς:* Τα πληροφοριακά συστήματα, εκτός από τεχνολογίες και υπολογιστικές υποδομές, υποστηρίζονται από μια σειρά οργανωτικών και διοικητικών δομών καθώς και από ένα πλήθος πολιτικών και διαδικασιών. Εκτός από τις τεχνικές συνέπειες, ένα περιστατικό ασφάλειας μπορεί να έχει οικονομικές, επιχειρησιακές, νομικές και κοινωνικές προεκτάσεις, ανάλογα με τις επιπτώσεις που επιφέρει σε έναν οργανισμό. Ανεξάρτητα, λοιπόν, από τους μηχανισμούς και το επίπεδο ασφάλειας ενός οργανισμού και τους τεχνικούς τρόπους που το υποστηρίζουν, η αντιμετώπιση περιστατικών αποτελεί εταιρική διαδικασία. Με βάση τα παραπάνω, προτείνεται και παρουσιάζεται εκτενώς ένα διοικητικό πλαίσιο αντιμετώπισης περιστατικών ασφάλειας, το οποίο ορίζει, περιγράφει και συσχετίζει τους ρόλους που συμμετέχουν στην αντιμετώπιση περιστατικών, το εύρος της δραστηριότητάς τους, τις διαδικασίες που ακολουθούν και τις αλληλοεπιδράσεις μεταξύ των ρόλων, έτσι ώστε να αναγνωριστεί και να χαρακτηριστεί –έγκαιρα- ένα περιστατικό και αφετέρου να περιοριστεί ο αντίκτυπός του με διαδικαστικά μέσα,
- *Μεθοδολογία αντιμετώπισης περιστατικών σε εταιρικά περιβάλλοντα:* Με βάση το παραπάνω διοικητικό πλαίσιο, παρουσιάζεται και αναλύεται μία πλήρης μεθοδολογία για την αντιμετώπιση περιστατικών σε εταιρικά περιβάλλοντα. Η μεθοδολογία αυτή χωρίζει τον κύκλο ζωής ενός περιστατικού ασφάλειας σε έξι διακριτές φάσεις και ορίζει τις ενέργειες που ακολουθούνται σε κάθε μια από αυτές. Προτείνονται και αναλύονται βέλτιστες πρακτικές για την αποδοτική προετοιμασία ενός οργανισμού για την αντιμετώπιση περιστατικών, την αναγνώριση των ιδιαίτερων χαρακτηριστικών του, τις ενέργειες που απαιτούνται για τον βραχυπρόθεσμο περιορισμό των συνεπειών που επιφέρει στις λειτουργίες

του Οργανισμού, καθώς και τις οδηγίες για την εξάλειψη του περιστατικού, την ανάκαμψη των συστημάτων και των διαδικασιών αλλά και για τις ενέργειες που έπονται μετά από αυτά,

- *Εταιρική διαδικασία και παράγοντες λήψης αποφάσεων στην αντιμετώπιση περιστατικών ασφάλειας:* Οι φάσεις της προαναφερθείσας μεθοδολογίας παρουσιάζονται μέσα από ένα διάγραμμα ροής, που στοχεύει στη δημιουργία μιας εταιρικής διαδικασίας αντιμετώπισης περιστατικών. Παρουσιάζονται και συζητούνται, αναλυτικά, παράγοντες που επηρεάζουν τη λήψη αποφάσεων κατά τη διάρκεια του κύκλου ζωής ενός περιστατικού ασφάλειας,
- *Καθορισμός και ανάλυση δομικών στοιχείων περιστατικών ασφάλειας μέσω τοπολογικής ανάλυσης:* Ένα περιστατικό αντιμετωπίζεται εφόσον αναγνωριστούν τα βασικά χαρακτηριστικά του αλλά και η υποδομή ασφάλειας στην οποία εκδηλώνεται. Για το σκοπό αυτό, ένα περιστατικό αναλύεται στα δομικά του χαρακτηριστικά, ήτοι σε μια σειρά επιτυχών εκμεταλλεύσεων αδυναμιών ασφάλειας στην πληροφοριακή υποδομή ενός οργανισμού, ενώ παράλληλα αξιολογείται η αποτελεσματικότητα των υπαρχόντων μηχανισμών ασφάλειας προκειμένου να επιβεβαιωθεί πως το περιστατικό –πράγματι- συμβαίνει (εξάλειψη λανθασμένων συναγερμών που μπορεί να οδηγήσουν σε εσφαλμένες ενέργειες με άμεσο αντίκτυπο στις λειτουργίες ενός οργανισμού),
- *Επέκταση της τοπολογικής ανάλυσης αδυναμιών στην ανίχνευση και αντιμετώπιση παρεισφρήσεων:* Η ανάλυση ενός περιστατικού ασφάλειας στα δομικά του χαρακτηριστικά είναι ένα, επίσης, αρκετά σύνθετο και πολυδιάστατο πρόβλημα. Η προσέγγιση του ερευνητή εστιάζει στην επέκταση της ερευνητικής περιοχής της τοπολογικής ανάλυσης αδυναμιών στην ανίχνευση παρεισφρήσεων, ήτοι στην κατασκευή μονοπατιών επίθεσης (εκμετάλλευση αδυναμιών με προκαθορισμένη σειρά) και στην αντιμετώπιση (ενεργοποίηση υπογραφών ανίχνευσης παρεισφρήσεων ανάλογα με το εκάστοτε περιστατικό),
- *Καθορισμός κριτηρίων συλλογής, ανάλυσης και επεξεργασίας πληροφοριών για τα δομικά στοιχεία περιστατικών ασφάλειας:* Η τοπολογική ανάλυση αδυναμιών και περιστατικών ασφάλειας βασίζεται στη συλλογή και επεξεργασία πληροφοριών που αφορούν σε αδυναμίες ασφάλειας (vulnerabilities), κώδικα αθέμιτης

εκμετάλλευσης (exploits) και σε υπογραφές ανίχνευσης και αντιμετώπισης παρεισφρήσεων (intrusion detection and prevention – IDP). Αυτό εισάγει την επίλυση ενός ακόμη επιμέρους προβλήματος που αφορά στη συλλογή και επεξεργασία πληροφοριών από ετερογενείς πηγές, συστήματα, μορφότυπους και σημασία, καθώς η ερευνητική κοινότητα και η βιομηχανία ασφάλειας δεν καθορίζουν συγκεκριμένα πρότυπα ή μεθόδους με τις οποίες κάτι τέτοιο θα μπορούσε να επιτευχθεί,

- *Κατασκευή και λειτουργία του συστήματος IRIS (Incident Response Intelligent System)*: Τα παραπάνω (συλλογή και επεξεργασία πληροφοριών που αφορούν σε αδυναμίες, κώδικα αθέμιτης εκμετάλλευσης και υπογραφές συστημάτων IDP πραγματοποιούνται από το εργαλείο IRIS (Incident Response Intelligent System) το οποίο, μεταξύ άλλων, κατασκευάζει τα προαναφερθέντα μονοπάτια επίθεσης και αντιμετώπισης για μια συγκεκριμένη υποδομή. Επίσης, το IRIS αναλύει τα χαρακτηριστικά των αδυναμιών ασφάλειας μιας υποδομής σε συνάρτηση με το διαθέσιμο κώδικα εκμετάλλευσης και τα αντίμετρα που λειτουργούν σε μια υποδομή και βαθμολογεί (με προτυποποιημένο τρόπο) τη σημαντικότητα μιας αδυναμίας ασφάλειας, λαμβάνοντας υπόψη τόσο τα εγγενή χαρακτηριστικά της, όσο και εκείνα τα χαρακτηριστικά που μεταβάλλονται συναρτήσει του χρόνου, καθώς επίσης και όσα χαρακτηριστικά επηρεάζονται από την –υπό εξέταση- υποδομή,
- *Αξιολόγηση αποτελεσμάτων και λειτουργιών του συστήματος σε εργαστηριακά και πραγματικά περιβάλλοντα:* Εφόσον οι περισσότερες ενέργειες που αφορούν στην αναγνώριση και αντιμετώπιση των περιστατικών ασφάλειας σε έναν οργανισμό εκτελούνται από το εργαλείο IRIS, αποτελεί απαραίτητη προϋπόθεση η αξιολόγηση της αποτελεσματικότητάς του για ένα πλήθος παραγόντων, όπως η ορθότητα των αποτελεσμάτων του, η συστημική λειτουργία με βάση το θεωρητικό μοντέλο ανάπτυξής του, η αξιολόγηση των επιμέρους χαρακτηριστικών του, η απόδοση και λειτουργία του σε εργαστηριακά και πραγματικά περιβάλλοντα, καθώς και η βελτίωση της απόδοσης των συστημάτων IDP. Τέλος αξιολογείται η ευκολία χρήσης, η αποδοχή του συστήματος από τους χρήστες και η ταχύτητα του εργαλείου IRIS.

1.5. Οργάνωση της διατριβής

Στο ***πρώτο κεφάλαιο*** περιγράφεται, σύντομα, η αντιμετώπιση περιστατικών ασφάλειας και τα συναφή ερευνητικά ζητήματα που σχετίζονται με τη συγκεκριμένη διατριβή. Περιγράφεται αναλυτικά το πρόβλημα και ο στόχος της διατριβής, αλλά και η προτεινόμενη λύση και μεθοδολογία.

Στο ***δεύτερο κεφάλαιο*** παρέχεται μια εννοιολογική θεμελίωση του συνόλου των όρων που χρησιμοποιούνται στην ερευνητική περιοχή της αντιμετώπισης περιστατικών ασφάλειας. Παράλληλα, δίνεται μια σύντομη επεξήγηση για κάθε έναν από αυτούς, ενώ παρουσιάζεται μια ταξονομία που κατηγοριοποιεί τους όρους αυτούς, καθώς και τις μεταξύ τους συσχετίσεις. Η πολυπλοκότητα του προβλήματος επιβάλλει τον σαφή προσδιορισμό των όρων που χρησιμοποιούνται στη συνέχεια της διατριβής.

Στο ***τρίτο κεφάλαιο*** ορίζεται η έννοια της Αντιμετώπισης Περιστατικών Ασφάλειας Πληροφοριών σε ένα εταιρικό περιβάλλον, ενώ παρουσιάζεται και ένα πρότυπο διοικητικό μοντέλο που βασίζεται σε ακαδημαϊκή και εφαρμοστέα έρευνα, βέλτιστες διεθνείς πρακτικές, πρότυπα ασφάλειας πληροφοριών και τεχνολογικές υλοποιήσεις. Παρουσιάζεται αφενός η έκταση και η πολυπλοκότητα της συγκεκριμένης εταιρικής διεργασίας, καθώς και τα διοικητικά ζητήματα που ανακύπτουν όταν ένας Οργανισμός ή μια εταιρεία αντιμετωπίζει ένα τέτοιο περιστατικό, ενώ διερευνώνται και κατηγοριοποιούνται οι συσχετίσεις της διεργασίας αυτής με την Ασφάλεια Πληροφοριών και τη Διοίκηση ενός πληροφοριακού συστήματος. Επίσης, προτείνεται μια δομημένη μεθοδολογία για τον χειρισμό περιστατικών ασφάλειας και παρουσιάζονται αναλυτικά οι διάφορες φάσεις της συγκεκριμένης μεθοδολογίας, ενώ –παράλληλα- προτείνονται βέλτιστες πρακτικές και διαδικασίες που μπορεί να ακολουθηθούν σε κάθε μια από τις φάσεις αυτές. Στη συνέχεια αναλύονται οι ενεργοί τρόποι αντιμετώπισης ενός περιστατικού, όπως π.χ. η ανεύρεση της πηγής προέλευσής του (π.χ. το δίκτυο, το σύστημα, ο χρήστης του συστήματος ή/και το φυσικό πρόσωπο) και παρουσιάζονται οι πιο διαδεδομένες τεχνικές εξιχνίασης (forensics) της πηγής προέλευσης ενός περιστατικού (automated trace-back) που εξετάζει η διεθνής βιβλιογραφία. Τέλος, παρουσιάζεται ένα γενικό σενάριο αντιμετώπισης περιστατικών ασφάλειας σε ένα

εταιρικό περιβάλλον, προκειμένου να αποδειχτεί η δυνατότητα υιοθέτησης των προαναφερθεισών τεχνικών.

Στο ***τέταρτο κεφάλαιο*** περιγράφεται η τοπολογική ανάλυση αδυναμιών ασφάλειας και οι επεκτάσεις της μεθόδου αυτής στην ερευνητική περιοχή των συστημάτων ανίχνευσης και αντιμετώπισης παρεισφρήσεων (IDP). Αρχικά, καθορίζονται οι απαραίτητες πληροφορίες για αδυναμίες ασφάλειας και κώδικα αθέμιτης εκμετάλλευσης που απαιτεί η μέθοδος, καθώς και οι αντίστοιχες απαιτούμενες πληροφορίες από τα συστήματα IDP με σκοπό την εξυπηρέτηση της αντιμετώπισης περιστατικών ασφάλειας. Αναλύονται και αξιολογούνται εκτενώς οι κυριότερες μέθοδοι ανάπτυξης συστημάτων IDP, ενώ προτείνεται και αναλύεται η μέθοδος ανάπτυξης με χρήση τεχνικών τοπολογικής ανάλυσης αδυναμιών. Τέλος, προτείνονται και αναλύονται εκτενώς οι απαιτήσεις ενός συστήματος αντιμετώπισης περιστατικών που βασίζεται στα παραπάνω.

Στο ***πέμπτο κεφάλαιο*** προτείνεται και παρουσιάζεται το Σύστημα Ευφυούς Αντιμετώπισης Περιστατικών (Incident Response Intelligence System - IRIS) το οποίο, κατανοεί το γενικότερο περιβάλλον των αδυναμιών ασφάλειας που ανακαλύπτονται από εργαλεία αυτόματης αξιολόγησης επικινδυνότητας, βαθμολογεί τη σημαντικότητά τους με προτυποποιημένο τρόπο, βρίσκει και συσχετίζει τον κώδικα εκμετάλλευσης που σχετίζεται με αυτές τις αδυναμίες και καθορίζει τις απαραίτητες υπογραφές που αντιστοιχούν στις εκμεταλλεύσεις, κατασκευάζοντας μονοπάτια αντιμετώπισης, δηλαδή δυναμικές και προσαρμοζόμενες πολιτικές συστημάτων IDP που αντιμετωπίζουν τα αντίστοιχα μονοπάτια επίθεσης. Παρουσιάζεται, λεπτομερειακά, η αρχιτεκτονική του συστήματος και το διάγραμμα ροής των λειτουργιών του, παρατίθενται οι λεπτομέρειες υλοποίησης και παρουσιάζεται η λειτουργία του σε μια πραγματική μελέτη περίπτωσης. Στη συγκεκριμένη μελέτη περίπτωσης, το IRIS κατασκευάζει αυτόματα την κατάλληλη πολιτική αντιμετώπισης περιστατικών σε ένα σύστημα, αφότου προσδιοριστεί, επαληθευτεί, συσχετιστεί και αξιολογηθεί για τη σημασία και τον αντίκτυπό της μια σειρά αδυναμιών και του αντίστοιχου κώδικα εκμετάλλευσης.

Στο ***έκτο κεφάλαιο*** παρουσιάζονται οι μεθοδολογίες αξιολόγησης και τα αποτελέσματα των χαρακτηριστικών και της λειτουργίας του IRIS. Αρχικά, αξιολογείται η ορθότητα

της υλοποίησης του IRIS, ενώ παρουσιάζονται και αξιολογούνται μια σειρά από πειραματικά δεδομένα για τον έλεγχο των αποτελεσμάτων του συστήματος. Στη συνέχεια αξιολογείται η λειτουργία του IRIS σε πραγματικό περιβάλλον, στα πλαίσια μιας μελέτης περίπτωσης (case study) που πραγματοποιήθηκε σε μεγάλη ελληνική Τράπεζα. Η συγκεκριμένη μελέτη περίπτωσης αποδεικνύει, με μετρήσιμα μεγέθη, τα οφέλη της τοπολογικής ανάλυσης αδυναμιών ασφάλειας και του IRIS στην αντιμετώπιση περιστατικών ασφάλειας αλλά και την αποδοτικότερη παραμετροποίηση των συστημάτων IDP. Επίσης, παρουσιάζονται και αναλύονται οι απόψεις χρηστών, που πειραματίστηκαν και εξοικειώθηκαν με το IRIS, για μια πλειάδα ζητημάτων που αφορούν στο σύστημα. Καταλήγοντας, εξετάζονται και συζητούνται γενικότερα συμπεράσματα καθώς και οι περιορισμοί της αξιολόγησης.

Τέλος, στο ***έβδομο κεφάλαιο*** παρουσιάζονται τα συμπεράσματα της διατριβής, τα θέματα μελλοντικής έρευνας και οι πιθανές επεκτάσεις.

Κεφάλαιο 2

Εννοιολογική Θεμελίωση

Don't let your intuition drive you to define something someone else has already defined

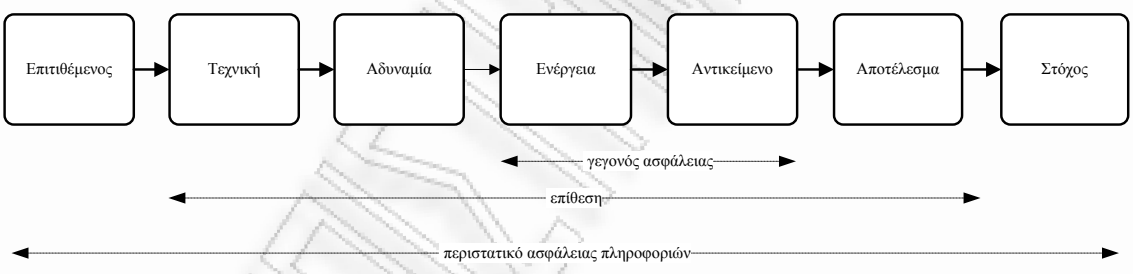
- **D. Gollmann**

2.1. Εισαγωγή

Η *ασφάλεια πληροφοριών* ορίζεται ως η διαφύλαξη της *εμπιστευτικότητας*, της *ακεραιότητας* και της *διαθεσιμότητας* των πληροφοριών[3] (ISO/IEC, 2005). Ως εταιρική διαδικασία, η ασφάλεια πληροφοριών στοχεύει στην *πρόληψη*, *ανίχνευση*, *αντιμετώπιση* και *ανάκαμψη* από ενέργειες που έχουν αρνητικό αντίκτυπο στις παραπάνω ιδιότητες (Patsos, 2002).

Οι *ενέργειες* αυτές προκαλούνται, συνήθως, από έναν ή περισσότερους επιτιθέμενους, οι οποίοι, χρησιμοποιώντας (χαμηλού-επιπέδου) τεχνικές προσπαθούν να επιτύχουν (υψηλού-επιπέδου) στόχους. Οι αρνητικές συνέπειες των ενεργειών αυτών αναφέρονται στη βιβλιογραφία ως *περιστατικά ασφάλειας πληροφοριών* (ή περιστατικά ασφάλειας, ή πιο απλά περιστατικά) (Mitropoulos, 2006).

Γενικά, ένα *περιστατικό ασφάλειας* είναι το αποτέλεσμα των ενεργειών ενός *επιτιθέμενου* που χρησιμοποιεί διάφορες *τεχνικές* για να εκμεταλλευτεί *αδυναμίες* και να προκαλέσει συγκεκριμένες *ενέργειες* σε *αντικείμενα* μια πληροφοριακής υποδομής, οι οποίες έχουν ως *αποτέλεσμα* να επιτύχει τους *στόχους* του (Piper, 2002).



Σχήμα 2-1: Περιστατικό ασφάλειας πληροφοριών, επίθεση και γεγονός ασφάλειας

Ο γενικευμένος αυτός ορισμός αναλύεται περισσότερο στις επόμενες ενότητες, με σκοπό να θεμελιωθεί εννοιολογικά το σύνολο των όρων που χρησιμοποιούνται στην αντιμετώπιση περιστατικών. Δεν αποτελεί στόχο της συγκεκριμένης ενότητας η κατασκευή ενός «πλήρους λεξικού» που μπορεί να χρησιμοποιηθεί στην γενικότερη ερευνητική περιοχή της ασφάλειας πληροφοριών, μιας και υπάρχουν ιδιαίτερα αξιόλογες προσπάθειες στη βιβλιογραφία (Κοκολάκης, 2000), (Howard, 1998), (ISO/IEC, 2005).

[3] Στον ίδιο ορισμό συμπεριλαμβάνονται και άλλες ιδιότητες, όπως η αυθεντικότητα, η μη αποποίηση ευθύνης και η αξιοπιστία.

Στόχος του συγκεκριμένου κεφαλαίου είναι η ανάπτυξη του συνόλου των όρων (σε υψηλό επίπεδο) που χρησιμοποιούνται στην περιοχή της αντιμετώπισης περιστατικών ασφάλειας, η επεξήγησή τους και η κατασκευή μιας ταξονομίας που κατηγοριοποιεί τους όρους αυτούς, καθώς και τις μεταξύ τους συσχετίσεις.

Ιδιαίτερα, κρίνεται σκόπιμο να διαχωριστεί εξαρχής η σημασία των όρων *γεγονός*, *επίθεση* και *περιστατικό ασφάλειας πληροφοριών* προκειμένου να αποφευχθεί οποιαδήποτε σύγχυση στον αναγνώστη, καθώς –όπως αποδεικνύεται στις παρακάτω ενότητες- κάθε όρος έχει το δικό του, συγκεκριμένο, νόημα.

2.2. Γεγονότα ασφάλειας πληροφοριών

Η λειτουργία των υπολογιστικών συστημάτων και των δικτύων χαρακτηρίζεται από ένα μεγάλο πλήθος γεγονότων. Ως γενική αίσθηση, *ένα γεγονός εκφράζει τη διακριτή μεταβολή της κατάστασης ενός συστήματος ή μιας συσκευής* (IEEE, 1996).

Από την πλευρά της ασφάλειας πληροφοριών, ένα *γεγονός* εκφράζει το αποτέλεσμα των ενεργειών που απευθύνονται σε συγκεκριμένους προορισμούς, που καλούνται αντικείμενα (όπως, π.χ., ένας χρήστης ο οποίος προσπαθεί να συνδεθεί (log in) σε έναν υπολογιστή). Στην περίπτωση αυτή, το γεγονός είναι η πιστοποίηση της ταυτότητάς του στη διαδικασία σύνδεσης, μέσω των ενεργειών που απαιτούνται (παροχή κατάλληλων διαπιστευτηρίων (credentials) στη συγκεκριμένη διαδικασία). Ο προορισμός, στην περίπτωση αυτή, είναι ο λογαριασμός ενός χρήστη.

Άλλα πιθανά σενάρια είναι οι διάφορες ενέργειες που μπορούν να πραγματοποιηθούν σε δεδομένα (π.χ. ανάγνωση, αντιγραφή, μετατροπή, κλοπή, διαγραφή, κτλ.), οι ενέργειες που προορίζονται για μια διεργασία ενός υπολογιστικού συστήματος (π.χ. έλεγχος, πιστοποίηση ταυτότητας, παράκαμψη ελέγχων ασφάλειας, κτλ.), καθώς και οι ενέργειες που απευθύνονται σε δομικά στοιχεία ενός υπολογιστή ή ενός δικτύου υπολογιστών.

Επισήμως, σύμφωνα με το ISO 18044 (ISO/IEC, 2004), ένα *γεγονός ασφάλειας ορίζεται ως η αναγνωρισμένη εμφάνιση κατάστασης ενός συστήματος, μιας υπηρεσίας ή ενός δικτύου που αποτελεί ένδειξη παραβίασης της πολιτικής ασφάλειας*[4] *ή αποτυχία των αντιμέτρων, ή μια άγνωστη κατάσταση που μπορεί να έχει σημασία ως προς την ασφάλειά του.*

[4] Περιγραφή του συνόλου των κανόνων, μέτρων και διαδικασιών που καθορίζουν τα φυσικά, διαδικαστικά και άλλα μέτρα ασφάλειας που λαμβάνονται κατά τη διαχείριση και προστασία των πληροφοριών (Γκρίτζαλης, 2004)

Είναι χρήσιμο να διευκρινιστούν διάφορες πτυχές του παραπάνω ορισμού. Πρώτον, η ύπαρξη ενός γεγονότος, προϋποθέτει την ύπαρξη μιας ενέργειας καθώς και ενός αντικειμένου, ακόμη και στην περίπτωση που η συγκεκριμένη ενέργεια δεν επιφέρει –τελικώς- αλλαγή στην κατάσταση του αντικειμένου αυτού. Στο παραπάνω παράδειγμα, αν ο χρήστης δεν εισαγάγει το σωστό συνδυασμό αναγνωριστικού χρήστη και συνθηματικού (username & password), το γεγονός έχει συμβεί (πιστοποίηση ταυτότητας), χωρίς –όμως- επιτυχία, μιας και ο χρήστης δεν επιβεβαίωσε τη σωστή ταυτότητα που απαιτείται για την πρόσβαση στον συγκεκριμένο λογαριασμό.

Μια άλλη διευκρίνιση στον παραπάνω ορισμό είναι η μη διαφοροποίηση μεταξύ εξουσιοδοτημένων και μη εξουσιοδοτημένων ενεργειών. Τα περισσότερα γεγονότα που συμβαίνουν στα υπολογιστικά συστήματα και δίκτυα είναι γεγονότα ρουτίνας που απαιτούνται για τις επιτυχείς λειτουργίες του συστήματος (κατά κάποιον τρόπο εξουσιοδοτημένα) και δεν μεταβάλλουν ιδιαίτερα την ασφάλειά του. Παρ' όλα αυτά, ένα γεγονός το οποίο είναι μέρος μιας επίθεσης, ή κάποιας άλλης αντίστοιχης ενέργειας, είναι ένα ζήτημα που μεταβάλλει την ασφάλεια ενός συστήματος. Στο παράδειγμα που παρουσιάστηκε παραπάνω, όταν ένας χρήστης συνδεθεί επιτυχώς με έναν λογαριασμό (δίνοντας τα κατάλληλα διαπιστευτήρια) τότε αποκτά πρόσβαση στο συγκεκριμένο λογαριασμό. Υπάρχει πάντοτε η περίπτωση ο χρήστης αυτός να προσποιείται τον πραγματικό κάτοχο ή εξουσιοδοτημένο χρήστη του συγκεκριμένου λογαριασμού (spoofing).

2.2.1. Ενέργειες και αντικείμενα

Ως *ενέργεια* ορίζεται ένα βήμα που λαμβάνει ένας χρήστης (ή μια διεργασία) προκειμένου να επιτύχει κάποιο αποτέλεσμα (IEEE, 1996), όπως π.χ. πιστοποίηση ταυτότητας, ανάγνωση δεδομένων, αντιγραφή δεδομένων, κτλ.

Οι *ενέργειες* αντικατοπτρίζουν το φάσμα των δραστηριοτήτων που μπορούν να εκτελεστούν από υπολογιστές και δίκτυα. Πιο συγκεκριμένα, οι ενέργειες αρχικοποιούνται από την πρόσβαση σε ένα αντικείμενο. Ως πρόσβαση ορίζεται η εγκαθίδρυση φυσικής ή/και λογικής επικοινωνίας ή επαφής (IEEE, 1996).

Οι ενέργειες κατευθύνονται σε πέντε κύριες κατηγορίες αντικειμένων. Οι τρεις πρώτες από αυτές είναι λογικές οντότητες (*λογαριασμός χρήστη*, *διεργασία συστήματος*, *δεδομένα*), ενώ οι υπόλοιπες αναφέρονται σε φυσικές οντότητες (υπολογιστής, δίκτυο).

Σε ένα πολυχρηστικό περιβάλλον χρήσης, ο *λογαριασμός* (account) είναι η περιοχή (domain) ενός χρήστη. Η περιοχή αυτή περικλείει τα *αρχεία* και τις διαδικασίες που ο χρήστης εξουσιοδοτείται να προσπελαύνει και να χρησιμοποιεί. Η πρόσβαση σε έναν *λογαριασμό* χρήστη ελέγχεται από ένα ειδικό πρόγραμμα που συμπεριλαμβάνει το αναγνωριστικό όνομα του *λογαριασμού* (account name), το συνθηματικό (password) και

τους περιορισμούς χρήσης. Μερικοί *λογαριασμοί* έχουν αυξημένα ή «ειδικά» προνόμια χρήσης που επιτρέπουν πρόσβαση σε *λογαριασμούς* συστήματος, σε *λογαριασμούς* άλλων χρηστών, σε αρχεία συστήματος και σεαντίστοιχες διαδικασίες. Οι *λογαριασμοί* αυτοί αναφέρονται στη βιβλιογραφία ως προνομιούχοι λογαριασμοί (privileged, superuser, administrator, root ή/και συστημικοί λογαριασμοί – system accounts).

Μερικές φορές, μια ενέργεια μπορεί να κατευθύνεται σε μια *διεργασία* (*process*) που εκτελείται σε έναν υπολογιστή ή ένα δίκτυο. Εκτός από το πρόγραμμα αυτό καθεαυτό η *διεργασία* συμπεριλαμβάνει τα δεδομένα και τη στοίβα εκτέλεσης του προγράμματος, τους μετρητές του προγράμματος, τους δείκτες της στοίβας και άλλους –αντίστοιχους- καταχωρητές, καθώς και άλλες πληροφορίες που απαιτούνται για την εκτέλεση του προγράμματος (Κάβουρας, 2003). Η ενέργεια, στην περίπτωση αυτή, είναι η παροχή των πληροφοριών αυτών στη διεργασία, ή ο έλεγχος –κατά κάποιον τρόπο- της *διεργασίας*.

Το αντικείμενο μιας ενέργειας μπορεί να είναι τα *δεδομένα* τα οποία βρίσκονται σε έναν υπολογιστή (ή δίκτυο υπολογιστών). Σύμφωνα με τον Gollmann (Gollmann, 1999), στην επιστήμη των υπολογιστών, τα δεδομένα ορίζονται ως «*τα φυσικά φαινόμενα που έχουν επιλεγεί , κατά συνθήκη, ώστε να αναπαριστούν συγκεκριμένες εκφάνσεις του εννοιολογικού και πραγματικού κόσμου. Η ερμηνεία που ο άνθρωπος προσδίδει στα δεδομένα καλείται πληροφορία. Τα δεδομένα χρησιμοποιούνται για να μεταδώσουν και να αποθηκεύσουν πληροφορίες και να δημιουργήσουν καινούργιες πληροφορίες με προκαθορισμένη επεξεργασία*».

Τα *δεδομένα* βρίσκονται σε δύο διαφορετικές καταστάσεις: αποθηκευμένα σε αρχεία ή σε κατάσταση μεταφοράς. Τα αρχεία είναι *δεδομένα* τα οποία ξεχωρίζουν από το όνομά τους και θεωρούνται ως μια αυτόνομη οντότητα από τους χρήστες και τις διεργασίες. Συχνά, τα αρχεία θεωρούνται πως είναι αποθηκευμένα σε διάφορα αποθηκευτικά μέσα (π.χ. σκληρό δίσκο), αλλά τα αρχεία μπορεί, επίσης, να βρίσκονται στην (πτητική ή μη) μνήμη ενός υπολογιστή. Τα μεταφερόμενα *δεδομένα* μεταδίδονται σε ένα δίκτυο υπολογιστών (ή εκπέμπονται από μια πηγή, όπως π.χ. εκείνα τα *δεδομένα* που μεταδίδονται μεταξύ των συσκευών ενός υπολογιστή και βρίσκονται σε αντίστοιχα ηλεκτρομαγνητικά πεδία που περιβάλλουν οθόνες υπολογιστών, συσκευές αποθήκευσης, επεξεργαστές κτλ.)

Συχνά, το *αντικείμενο μιας ενέργειας* είναι μια φυσική οντότητα. Η μικρότερη από τις φυσικές οντότητες είναι το δομοστοιχείο (module), ενώ η σύνθεση πολλαπλών δομοστοιχείων δημιουργεί ένα *υπολογιστικό σύστημα* ή ένα *δίκτυο υπολογιστών*. Το *δίκτυο* είναι ένα διασυνδεδεμένο σύνολο από υπολογιστές, που συμπεριλαμβάνει και τα στοιχεία διασύνδεσης και δρομολόγησης (IEEE, 1996). Όταν ένας υπολογιστής είναι

συνδεδεμένος σε ένα δίκτυο υπολογιστών, ονομάζεται *δικτυακός σταθμός* ή πιο απλά *σταθμός* (host).

Οι *ενέργειες ενός επιτιθέμενου* που προορίζονται για συγκεκριμένα αντικείμενα μιας πληροφοριακής υποδομής κατατάσσονται σε 5 διαφορετικές ομάδες σύμφωνα με όσα περιγράφονται στο (Scambray, 2001) που ουσιαστικά αποτελούν έναν ακολουθιακό αλγόριθμο επίθεσης. Οι ομάδες ενεργειών αναλύονται συνοπτικά στις παρακάτω παραγράφους.

2.2.1.1. Συλλογή διερευνητικών πληροφοριών, έλεγχος σάρωσης και απαρίθμηση χαρακτηριστικών

Στα αρχικά στάδια μιας επίθεσης, χρησιμοποιούνται τρεις κυρίως ενέργειες προκειμένου να συλλεχθούν πληροφορίες σχετικά με τα χαρακτηριστικά ασφάλειας ενός αντικειμένου: η *συλλογή διερευνητικών πληροφοριών* (footprinting), ο *έλεγχος σάρωσης* (scanning) και η *απαρίθμηση αντικειμένων (enumeration)*.

Η *συλλογή διερευνητικών πληροφοριών* αναπαριστά τις λειτουργίες που χρησιμοποιούνται προκειμένου να αποφασιστούν τα χαρακτηριστικά ενός συγκεκριμένου αντικειμένου. Ο *έλεγχος σάρωσης*, από την άλλη πλευρά, αναπαριστά τις λειτουργίες κατά τις οποίες ένας χρήστης ή μια διεργασία εξετάζει, ακολουθιακά, διάφορα αντικείμενα για την ύπαρξη ενός συγκεκριμένου χαρακτηριστικού (ιδιαίτερα μιας *αδυναμίας* ασφάλειας). Ο έλεγχος *σάρωσης* μπορεί να συνδυαστεί με τη *συλλογή διερευνητικών πληροφοριών*, με προκαθορισμένη σειρά, ώστε να συλλεχθούν περισσότερες πληροφορίες για συγκεκριμένα αντικείμενα, σε συντομότερο –σχετικά- χρόνο. Ο συνδυασμός αυτών των δύο τεχνικών ονομάζεται και *απαρίθμηση χαρακτηριστικών*, ιδιαίτερα όταν η *συλλογή διερευνητικών πληροφοριών* και ο *έλεγχος σάρωσης* απευθύνονται σε συγκεκριμένα χαρακτηριστικά που διαθέτουν συγκεκριμένα αντικείμενα (π.χ. αδυναμίες).

Αντίθετα με τη διερεύνηση και τη σάρωση, η απόπειρα *άρνησης εξυπηρέτησης* (denial of service - DoS) δεν χρησιμοποιείται για να συλλέξει χαρακτηριστικά σχετικά με ένα συγκεκριμένο αντικείμενο, αλλά στοχεύει στην υπερφόρτωση της δυνατότητας ενός αντικειμένου, με επαναλαμβανόμενες ενέργειες πρόσβασης και πιθανόν την πλήρη εξάντληση των υπολογιστικών ορίων ενός συστήματος ώστε εκείνο να πάψει να λειτουργεί. Παράδειγμα αποτελούν οι επαναλαμβανόμενες αιτήσεις στις ανοικτές συνδέσεις μιας δικτυακής πόρτας, ή η αρχικοποίηση μιας διαδικασίας σε έναν υπολογιστή. Άλλο παράδειγμα αποτελεί η αποστολή μεγάλου πλήθους μηνυμάτων ηλεκτρονικού ταχυδρομείου σε ένα συγκεκριμένο τέτοιο λογαριασμό, που υπερβαίνει τις δυνατότητες επεξεργασίας των μηνυμάτων του συγκεκριμένου λογαριασμού. Συνήθως, η απόπειρα *άρνησης εξυπηρέτησης* χρησιμοποιείται από τους επιτιθέμενους σε ειδικές μόνο περιπτώσεις που στοχεύουν κυρίως στην πρόκληση ζημιάς σε ένα αντικείμενο.

2.2.1.2. Απόκτηση πρόσβασης, υποκλοπή στοιχείων και απόκτηση ειδικών προνομίων

Στη συνέχεια, ένας επιτιθέμενος, αποπειράται να αποκτήσει πρόσβαση σε ένα αντικείμενο του ενδιαφέροντός του (ιδιαίτερα σε εκείνα τα αντικείμενα που εμφάνισαν συγκεκριμένα χαρακτηριστικά ασφάλειας κατά τα προηγούμενα βήματα), συνήθως εκμεταλλευόμενος τη διαδικασία *πιστοποίησης ταυτότητας*.

Η *πιστοποίηση ταυτότητας* ή *αυθεντικοποίηση* (authentication) είναι η ενέργεια που εκτελεί ένας χρήστης προκειμένου να επαληθεύσει την κατοχή μιας συγκεκριμένης ταυτότητας. Η *πιστοποίηση ταυτότητας* ξεκινά με ένα χρήστη που χρησιμοποιεί μια αντίστοιχη διαδικασία (π.χ. ένα πρόγραμμα σύνδεσης). Ο χρήστης πρέπει να αποδείξει ότι διαθέτει μια συγκεκριμένη ταυτότητα, όπως η εισαγωγή ενός αναγνωριστικού ονόματος (user name).

Στις περισσότερες περιπτώσεις, η *επαλήθευση της ταυτότητας* (verification) που ισχυρίζεται ότι κατέχει ο χρήστης αποτελεί ένα επιπλέον βήμα στη διαδικασία *πιστοποίησης ταυτότητας*. Για την επαλήθευση αυτής της ταυτότητας, ο χρήστης πρέπει να αποδείξει τουλάχιστον ένα από τα παρακάτω:

- τη γνώση μιας πληροφορίας (π.χ. ένα συνθηματικό που συνδέεται μονοσήμαντα με την ταυτότητα που ισχυρίζεται ότι έχει ο χρήστης, έναν κωδικό, μια λέξη, κτλ.),
- την κατοχή ενός αντικειμένου (π.χ. μια κάρτα που διατηρεί κωδικούς για το συγκεκριμένο λογαριασμό με βάση συγκεκριμένα χρονικά ή άλλα κριτήρια),
- την παροχή ενός συγκεκριμένου και μοναδικού χαρακτηριστικού που σχετίζεται με την ύπαρξή του (π.χ. ένα βιομετρικό).

Η πιστοποίηση ταυτότητας δεν χρησιμοποιείται μόνο στην περίπτωση σύνδεσης με έναν λογαριασμό, αλλά και για την εξουσιοδότηση πρόσβασης (authorization) σε άλλα αντικείμενα προκειμένου να εκτελεστεί μια διεργασία, να προσπελαστεί ένα συγκεκριμένο αρχείο, κτλ. Ως αντικείμενα της διαδικασίας πιστοποίησης ταυτότητας θεωρούνται ένας λογαριασμός χρήστη, μια διεργασία συστήματος, μια δομή δεδομένων, κτλ. προς τα οποία ο χρήστης πιστοποιεί την ταυτότητά του και όχι η διαδικασία της πιστοποίησης αυτή καθεαυτή.

Υπάρχουν δύο γενικές μέθοδοι που μπορούν να παραβιάσουν τη *διαδικασία πιστοποίησης ταυτότητας* και να οδηγήσουν σε απόκτηση μη-εξουσιοδοτημένης πρόσβασης καθώς και στην απόκτηση προνομιούχων δικαιωμάτων σε ένα σύστημα.

Πρώτον, ένας επιτιθέμενος μπορεί να προσποιηθεί ότι κατέχει την ταυτότητα ενός άλλου (εξουσιοδοτημένου) χρήστη αν αποδείξει πως κατέχει το κατάλληλο αναγνωριστικό και χαρακτηριστικό επαλήθευσης που χρησιμοποιεί -για την αντίστοιχη διαδικασία- ο εξουσιοδοτημένος χρήστης. Για παράδειγμα, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει μια διεργασία που εκτελείται σε έναν υπολογιστή συνδεδεμένο σε ένα δίκτυο και να υποκλέψει το αναγνωριστικό και το συνθηματικό που χρησιμοποιεί ένας εξουσιοδοτημένος χρήστης (υποκλοπή στοιχείων). Στη συνέχεια, ο επιτιθέμενος μπορεί να χρησιμοποιήσει τις πληροφορίες αυτές και να αποκτήσει ακριβώς το ίδιο επίπεδο πρόσβασης με το συγκεκριμένο χρήστη από τον οποίο υπέκλεψε τις πληροφορίες αυτές (πιθανόν και ενός λογαριασμού χρήστη με προνομιούχα δικαιώματα). Τονίζεται πως, ακόμη και στην περίπτωση αυτή, η διαδικασία *πιστοποίησης ταυτότητας* είναι έγκυρη, μιας και τα διαπιστευτήρια που χρησιμοποίησε ο επιτιθέμενος είναι έγκυρα, παρόλο που έχουν υποκλαπεί.

Η δεύτερη μέθοδος που μπορεί να παραβιάσει τη διαδικασία *πιστοποίησης ταυτότητας* είναι η *εκμετάλλευση* μιας *αδυναμίας* ώστε να παρακαμφθεί τελείως η διαδικασία και να επιτευχθεί απευθείας πρόσβαση στο αντικείμενο ενδιαφέροντος. Η παράκαμψη είναι μια ενέργεια που εκτελείται είτε για να παρακαμφθεί εντελώς η διαδικασία είτε για να χρησιμοποιηθεί μια εναλλακτική διαδικασία (συνήθως αρκετά πιο εύκολη) από τον επιτιθέμενο προκειμένου να αποκτήσει πρόσβαση στο αντικείμενο. Για παράδειγμα, ορισμένα λειτουργικά συστήματα έχουν συγκεκριμένες *αδυναμίες* που αν τύχουν κατάλληλης εκμετάλλευσης μπορούν να οδηγήσουν έναν επιτιθέμενο να αποκτήσει πρόσβαση σε έναν προνομιούχο λογαριασμό, χωρίς πραγματικά να υπάρξει *πιστοποίηση ταυτότητας*.

Όπως αναφέρθηκε στα προηγούμενα, η ενέργεια της *πιστοποίησης ταυτότητας* δεν υποδηλώνει απαραίτητα πως η ενέργεια αυτή είναι εξουσιοδοτημένη, ακόμη και όταν χρησιμοποιούνται έγκυροι συνδυασμοί διαπιστευτηρίων. Ομοίως, η ενέργεια παράκαμψης της *πιστοποίησης ταυτότητας* δεν σημαίνει απαραίτητα πως η ενέργεια αυτή είναι μη-εξουσιοδοτημένη. Για παράδειγμα, ορισμένοι προγραμματιστές βρίσκουν πρακτικό να επιτρέπουν μια μέθοδο γρήγορης συντόμευσης ή να δημιουργούν μια «κερκόπορτα» (“back door”) ώστε να συνδέονται με έναν λογαριασμό και να εκτελούν μια συγκεκριμένη διαδικασία, ιδιαίτερα κατά τη φάση ανάπτυξης και εκσφαλμάτωσης κώδικα. Η γρήγορη αυτή συντόμευση παρακάμπτει τη διαδικασία πιστοποίησης ταυτότητας προκειμένου να πραγματοποιηθεί περισσότερο γρήγορα ο αντικειμενικός στόχος του προγραμματιστή (π.χ. εκσφαλμάτωση, διόρθωση, προσθήκη κώδικα, κτλ). Μια τέτοια περίπτωση μπορεί να θεωρείται εξουσιοδοτημένη.

Μερικές ενέργειες είναι στενά συνδεδεμένες με τα δεδομένα που βρίσκονται σε υπολογιστές και δίκτυα, ιδιαίτερα με δομές αρχείων. Κάθε ένας από τους όρους «ανάγνωση», «μετατροπή», «κλοπή» ή «διαγραφή» περιγράφει παρόμοιες ενέργειες, με

διαφορετικό, όμως, αποτέλεσμα κάθε φορά. Η ανάγνωση είναι η ενέργεια που επιτρέπει την απόκτηση του περιεχομένου των δεδομένων μέσα σε ένα αρχείο, ή άλλη δομή (ή μέσο) δεδομένων. Η ενέργεια αυτή διαχωρίζεται, διαισθητικά, από τα φυσικά βήματα που απαιτούνται για την ανάγνωση. Για παράδειγμα, στη διαδικασία ανάγνωσης ενός υπολογιστικού αρχείου, το αρχείο είναι πιθανόν να αντιγράφεται από μια αποθηκευμένη περιοχή στη μνήμη του υπολογιστή και στη συνέχεια να απεικονίζεται σε μια οθόνη, προκειμένου να αναγνωστεί από το χρήστη. Τα φυσικά βήματα αυτά (αντιγραφή στη μνήμη, προβολή στην οθόνη) δεν ανήκουν στον ορισμό της ανάγνωσης που προαναφέρθηκε. Με άλλα λόγια, προκειμένου να αναγνωστεί το περιεχόμενο ενός αντικειμένου δεν απαιτείται –απαραίτητα- η αντιγραφή του αρχείου αυτού. Ο ίδιος διαχωρισμός γίνεται και στην ενέργεια της αντιγραφής ενός αρχείου. Στην περίπτωση αυτή, η αντιγραφή έχει ως αποτέλεσμα την απόκτηση ενός αντιγράφου ενός αντικειμένου, χωρίς τη διαγραφή του πρωτότυπου. Ο όρος αντιγραφή δεν υποδηλώνει πως αποκτάται το περιεχόμενο του αντικειμένου, αλλά πως αποκτάται ένα αντίγραφο αυτού. Προκειμένου να αποκτήσει κανείς το περιεχόμενο, πρέπει να διαβάσει το συγκεκριμένο αρχείο. Ένα χαρακτηριστικό παράδειγμα είναι η αντιγραφή ενός αρχείου από ένα σκληρό δίσκο σε ένα φορητό μέσο αποθήκευσης. Αυτό επιτυγχάνεται με τη δημιουργία ενός αντιγράφου, χωρίς να αλλοιώνεται το πρωτότυπο αρχείο.

Η αντιγραφή και η ανάγνωση διαφέρουν –ως έννοιες- από την κλοπή, η οποία αναφέρεται ως το αποτέλεσμα της αλλαγής της κατοχής ενός αντικειμένου από τον εξουσιοδοτημένο κάτοχό του σε έναν επιτιθέμενο (χωρίς τη σύμφωνη γνώμη του εξουσιοδοτημένου κατόχου).

Ο ορισμός αυτός συνάδει με την έννοια της φυσικής ιδιοκτησίας, ιδιαίτερα για περιπτώσεις που υπάρχει ένα αντικείμενο το οποίο δεν μπορεί να αντιγραφεί. Για παράδειγμα, όταν κάποιος κλέψει ένα αυτοκίνητο, τότε έχει στερήσει από τον κάτοχό του την ιδιοκτησία του αυτοκινήτου αυτού. Όταν αναφερόμαστε σε ζητήματα ιδιοκτησίας αντικειμένων που βρίσκονται σε ηλεκτρονική μορφή, όπως π.χ. ένα αρχείο, συχνά χρησιμοποιούμε τον όρο «κλοπή» ακριβώς όπως χρησιμοποιούμε την αντιγραφή. Η ειδοποιός διαφορά μεταξύ της αντιγραφής και της κλοπής είναι η ύπαρξη δικαιωμάτων χρήσης ή πρόσβασης του αντικειμένου από τον κάτοχό του. Στην περίπτωση των αρχείων, αυτό μπορεί να σημαίνει τις ενέργειες της αντιγραφής (από έναν επιτιθέμενο) και της διαγραφής ενός αρχείου στη συνέχεια. Από την άλλη πλευρά, μπορεί να σημαίνει και την κλοπή του αποθηκευτικού μέσου, ή ολόκληρου του υπολογιστή.

Δύο ακόμη ενέργειες συμπεριλαμβάνονται σε εκείνες που αλλάζουν, κατά κάποιον τρόπο, το αντικείμενο. Χαρακτηριστικά παραδείγματα είναι η αλλαγή/μεταβολή του περιεχομένου ενός αρχείου, η αλλαγή του συνθηματικού σε έναν λογαριασμό, η αποστολή εντολών που αλλάζουν τα αναμενόμενα αποτελέσματα μιας εκτελούμενης διεργασίας, καθώς και η μετατροπή των δομικών στοιχείων ενός συστήματος. Εάν το

αντικείμενο εξαφανίζεται ολοσχερώς, τότε χρησιμοποιούμε τον όρο διαγραφή προκειμένου να περιγράψουμε τη συγκεκριμένη ενέργεια.

2.2.1.3. Παραποίηση ταυτότητας και απόκρυψη ενεργειών

Η *πιστοποίηση ταυτότητας* (καθώς και η παράκαμψή της) είναι συνδεδεμένη με τους χρήστες που ταυτοποιούνται σε ένα σύστημα ή μια διεργασία. Στα δίκτυα υπολογιστών, οι διεργασίες συνήθως ταυτοποιούνται σε άλλες –αντίστοιχες- διεργασίες. Για παράδειγμα, κάθε πακέτο πληροφοριών που ταξιδεύει σε ένα δίκτυο έχει διευθύνσεις που ταυτοποιούν την προέλευση και τον προορισμό του, καθώς και άλλες σχετικές πληροφορίες ώστε να επιτευχθεί –όπως ακριβώς απαιτείται- η επικοινωνία και η δρομολόγηση μεταξύ δύο (ή περισσοτέρων) σημείων. Διαισθητικά, όταν επιτυγχάνεται η επιθυμητή επικοινωνία, θεωρείται πως οι πληροφορίες αυτές είναι «σωστές» και «ακριβείς». Παρ' όλα αυτά, είναι δυνατόν να επιτευχθεί η επικοινωνία μεταξύ δύο ή περισσοτέρων μερών, χρησιμοποιώντας «ανακριβείς» πληροφορίες. Η τακτική αυτή ονομάζεται *παραποίηση* (masquerade/spoofing) και μπορεί να γίνει με διάφορες τεχνικές και σε διάφορα αντικείμενα (π.χ. παραποίηση διεύθυνσης IP, παραποίηση διεύθυνσης αποστολέα ενός ηλεκτρονικού μηνύματος, κτλ).

Η *παραποίηση* είναι μια ενεργός επίθεση στην οποία μια οντότητα σε ένα δίκτυο υπολογιστών (ή ένα υπολογιστικό σύστημα) προσποιείται μια άλλη οντότητα, διακόπτοντας την «κανονική» ροή δεδομένων και εισάγοντας διαφορετικά δεδομένα δρομολόγησης[5] στον επικοινωνιακό δίαυλο μεταξύ άλλων μηχανών. Η *παραποίηση* στοχεύει στο να ξεγελάσει άλλες οντότητες στο δίκτυο, είτε για να παρουσιαστεί ως αυθεντική, είτε για να πείσει τις υπόλοιπες οντότητες να της στείλουν δεδομένα, είτε –τέλος- για να μπορεί να αλλάξει δεδομένα (Atkins et. al, 1996).

Επίσης, είναι αρκετά σύνηθες ο επιτιθέμενος να προσπαθεί να αποκρύψει τις ενέργειες που προκαλεί σε ένα σύστημα, είτε χρησιμοποιώντας τις τεχνικές παραποίησης που προαναφέρθηκαν, είτε διαγράφοντας συγκεκριμένα αρχεία σε υπολογιστικά συστήματα ή/και συσκευές που πιθανόν να καταγράφουν τις ενέργειές του.

2.2.1.4. Μελλοντική επανάληψη επίθεσης

Η επίθεση σε ένα υπολογιστικό σύστημα ή δίκτυο είναι μια διαδικασία που απαιτεί αρκετούς υπολογιστικούς πόρους και ένα –σχετικά- μεγάλο διάστημα χρόνου (άμεσα εξαρτώμενο από τους υπολογιστικούς πόρους που διαθέτει ο επιτιθέμενος και τα αντίμετρα που εφαρμόζονται στο αντικείμενο). Έτσι, αρκετά συχνά, μια επίθεση δεν

[5] Π.χ. παραποιεί τη διεύθυνση του αποστολέα, με σκοπό ο επιτιθέμενος να αποκρύψει τις ενέργειές του.

ολοκληρώνεται σε μια μόνο σύνδεση (ή ένα προκαθορισμένο χρονικό διάστημα). Με το δεδομένο αυτό, οι επιτιθέμενοι, τροποποιούν κατάλληλα τις ιδιότητες ασφάλειας των αντικειμένων ενδιαφέροντος προκειμένου να μην επαναλάβουν όλα τα προηγούμενα βήματα. Μια πιθανή ενέργεια είναι η μέθοδος συντόμευσης ("back door", βλ. *Απόκτηση πρόσβασης, υποκλοπή στοιχείων και απόκτηση ειδικών προνομίων*), ώστε να συνδεθούν με έναν προνομιούχο λογαριασμό και να συνεχίσουν την επίθεση σε μεταγενέστερη χρονική περίοδο.

2.2.1.5. Άρνηση εξυπηρέτησης

Τέλος, όπως αναφέρθηκε και στα προηγούμενα, η άρνηση στοχεύει στην υπερφόρτωση της δυνατότητας ενός αντικειμένου, με επαναλαμβανόμενες ενέργειες πρόσβασης ή αιτήσεις εξυπηρέτησης με σκοπό την εξάντληση των υπολογιστικών ορίων ενός συστήματος (με απώτερο στόχο τη διακοπή της λειτουργίας του). Η ενέργεια αυτή χρησιμοποιείται για διάφορους σκοπούς που εξαρτώνται κυρίως από τους στόχους που προσπαθεί να καταφέρει ο επιτιθέμενος και την κατηγορία του επιτιθέμενου (βλ. ενότητα 2.4.1). Για μια πλήρη περιγραφή των επιθέσεων άρνησης εξυπηρέτησης, ο αναγνώστης παραπέμπεται στο (Douligeris, 2007).

2.3. Επιθέσεις ασφάλειας πληροφοριών

Πολλές φορές, ένα γεγονός που συμβαίνει σε έναν υπολογιστή ή ένα δίκτυο αποτελεί μέρος μιας σειράς από βήματα που στοχεύουν σε μια μη εξουσιοδοτημένη ενέργεια. Σε αυτήν την περίπτωση, το γεγονός θεωρείται ως μέρος μιας επίθεσης.

Μια επίθεση αποτελείται από πολλά και διαφορετικά βήματα. Κατά πρώτον, πηγάζει από κάποιον επιτιθέμενο (ή επιτιθέμενους). Ανάμεσα σε αυτά τα βήματα είναι μια ενέργεια που προορίζεται για ένα αντικείμενο (δηλαδή ένα γεγονός), η χρήση ενός εργαλείου ή η *εκμετάλλευση* μιας *αδυναμίας*[6]. Κατά δεύτερον, η επίθεση στοχεύει στην επίτευξη μιας μη-εξουσιοδοτημένης ενέργειας, όπως αυτή ορίζεται από τον ιδιοκτήτη ή το διαχειριστή του συστήματος (αντικειμένου) για το οποίο προορίζεται η επίθεση. Τέλος, μια επίθεση είναι μια ακολουθία από ηθελημένα βήματα τα οποία εκτελεί ο επιτιθέμενος.

Ως *επίθεση*, λοιπόν, *ορίζεται η σειρά από τα βήματα που εκτελεί ένας επιτιθέμενος ώστε να επιτύχει ένα μη εξουσιοδοτημένο αποτέλεσμα*.

---

[6] Ο όρος *αδυναμία* (vulnerability) απαντάται, επίσης, στη βιβλιογραφία ως *ευπάθεια* ή *τρωτότητα*.

Οι επιθέσεις έχουν πέντε (5) διακριτά τμήματα τα οποία πρέπει να εκτελέσει ένας επιτιθέμενος, ο οποίος χρησιμοποιεί μια τεχνική προκειμένου να εκμεταλλευτεί μία *αδυναμία* σε ένα αντικείμενο και να εκτελέσει ενέργειες με μη-εξουσιοδοτημένα αποτελέσματα στο αντικείμενο αυτό. Προκειμένου να επιτύχει το στόχο του, ο επιτιθέμενος πρέπει να βρει κατάλληλα διασυνδεδεμένα μονοπάτια (επίθεση), χρησιμοποιώντας ταυτόχρονα (ή επαναλαμβανόμενα) τα τμήματα μιας επίθεσης.

Τα δύο πρώτα βήματα μιας επίθεσης (η τεχνική και η *αδυναμία*) χρησιμοποιούνται προκειμένου να προκαλέσουν ένα γεγονός σε έναν υπολογιστή ή δίκτυο. Το λογικό αποτέλεσμα μιας επιτυχημένης επίθεσης είναι μια μη-εξουσιοδοτημένη ενέργεια. Αν το αποτέλεσμα είναι μια εξουσιοδοτημένη ενέργεια, τότε –χωρίς βλάβη της γενικότητας- δεν έχει συμβεί επίθεση[7].

Ο διαχωρισμός της εξουσιοδοτημένης έναντι της μη-εξουσιοδοτημένης ενέργειας είναι αρκετά σημαντικός προκειμένου να τονιστεί η ειδοποιός διαφορά μιας επίθεσης από τα συνηθισμένα γεγονότα που συμβαίνουν σε ένα σύστημα ή ένα δίκτυο. Επίσης, μια ενέργεια που είναι εξουσιοδοτημένη σε ένα σύστημα μπορεί να είναι μη-εξουσιοδοτημένη σε κάποιο άλλο. Η έννοια της *εξουσιοδότησης* είναι *άμεσα εξαρτώμενη από το συγκεκριμένο σύστημα (δηλαδή το αντικείμενο), ή ακριβέστερα τον ιδιοκτήτη/διαχειριστή του.*

Για παράδειγμα, μερικές υπηρεσίες, όπως η ανώνυμη μεταφορά αρχείων (anonymous File Transfer Protocol - FTP) μπορεί να θεωρείται ως εξουσιοδοτημένη ενέργεια για μερικά συστήματα αλλά μη εξουσιοδοτημένη για κάποια άλλα (ακόμη και μέσα στον ίδιο οργανισμό). Ακόμη και ενέργειες που θεωρητικά αντιμετωπίζονται ως ενέργειες επίθεσης, όπως η παράκαμψη μεθόδων ελέγχου πρόσβασης για σύνδεση με έναν προνομιούχο λογαριασμό, μπορεί να θεωρηθούν ως εξουσιοδοτημένες ενέργειες σε ειδικές περιπτώσεις (π.χ. κατά τη διάρκεια του ελέγχου της ασφάλειας ενός συστήματος). Όπως προαναφέρθηκε, ο καθορισμός των εξουσιοδοτημένων ενεργειών, εγκρίνεται από τον ιδιοκτήτη (ή το διαχειριστή) ενός αντικειμένου μέσω της πολιτικής ασφάλειας.

2.3.1. Τεχνικές

Το πρώτο βήμα στην ακολουθία ενεργειών που ακολουθούν οι επιτιθέμενοι με στόχο μη-εξουσιοδοτημένες ενέργειες είναι η χρήση εργαλείων επίθεσης. Γενικά, *ένα εργαλείο εκφράζει έναν τρόπο εκμετάλλευσης μιας αδυναμίας σε έναν υπολογιστή ή ένα δίκτυο υπολογιστών*. Μερικές φορές το εργαλείο μπορεί να είναι κάτι ιδιαίτερα απλό, π.χ. μια

[7] Είτε η επίθεση δεν ήταν επιτυχημένη.

εντολή, ή μια φυσική επίθεση. Από την άλλη πλευρά, το εργαλείο μπορεί να είναι ένα ιδιαίτερα εξελιγμένο και πολύπλοκο πρόγραμμα, όπως π.χ. ένας Δούρειος Ίππος (Trojan horse), ένας υπολογιστικός ιός (computer virus) ή ένα εργαλείο κατανεμημένης άρνησης εξυπηρέτησης (distributed denial of service – DDoS) σε ένα σύστημα ή δίκτυο.

Εμπειρικά, οι παρακάτω κατηγορίες αποτελούν μια λίστα με τις δημοφιλέστερες τεχνικές που χρησιμοποιούν οι επιτιθέμενοι:

- *Φυσική επίθεση* (physical attack) –τρόπος φυσικής κλοπής ή καταστροφής ενός υπολογιστή, δικτύου, των δομοστοιχείων του ή των υποστηρικτικών του συστημάτων (π.χ. ηλεκτρικό ρεύμα, εξαερισμός, κτλ.)

- *Νοημοσύνη* (intelligence) – τρόπος συλλογής πληροφοριών από ηλεκτρονικά μέσα ή άλλους επιτιθέμενους. Για παράδειγμα, ένας επιτιθέμενος μπορεί να συλλέξει πληροφορίες από τον ιστότοπο ενός οργανισμού, από μηχανές αναζήτησης του Ιστού (Web), κανάλια συνομιλίας (chat rooms). Ένας άλλος τρόπος συλλογής πληροφοριών πραγματοποιείται με την απευθείας επαφή και εξαπάτηση εξουσιοδοτημένων χρηστών του συστήματος (ο τελευταίος όρος απαντάται στη βιβλιογραφία ως κοινωνική μηχανική - social engineering). Για παράδειγμα, ο επιτιθέμενος προσποιείται (σε έναν εξουσιοδοτημένο χρήστη) την ταυτότητα ενός «υψηλού προσώπου» στον Οργανισμό (συχνά χωρίς φυσική επαφή ανάμεσά τους) και ζητά ευαίσθητες πληροφορίες.

- *Εντολή* (command) - τρόπος *εκμετάλλευσης* μιας *αδυναμίας* με την απευθείας εισαγωγή εντολών σε μια διεργασία μέσω της διεπαφής του χρήστη με το σύστημα. Παράδειγμα αποτελεί η εισαγωγή εντολών σε μια σύνοδο telnet, η εισαγωγή ειδικά διαμορφωμένων URL σε έναν εξυπηρετητή ιστού (web server),

- *Πρόγραμμα* (program) – τρόπος *εκμετάλλευσης* μιας *αδυναμίας* με τη δομημένη αποστολή εντολών σε μια διεργασία και την εκτέλεση ενός αρχείου εντολών (σενάριο – script) ή κώδικα. Χαρακτηριστικά παραδείγματα αποτελούν ο προγραμματισμός φλοιού (shell scripting), το επιβλαβές /κακόβουλο ή ιομορφικό λογισμικό (malicious software – malware, virus),

- *Εργαλείο* (tool) – ένα πακέτο λογισμικού που περιέχει σενάρια, ειδικά προγράμματα και ειδικό λογισμικό που εκμεταλλεύεται *αδυναμίες*. Παραδείγματα τέτοιων εργαλείων είναι τα προγράμματα σάρωσης ενός δικτύου υπολογιστών για *αδυναμίες* (scanning tools), εργαλεία αναπαραγωγής συνθηματικών και λογαριασμών χρήσης (password cracking tools), εργαλεία υποκλοπής των διακινούμενων δεδομένων σε ένα δίκτυο (sniffers), κτλ.

2.3.2. Αδυναμίες

Ο όρος *αδυναμία* χρησιμοποιείται για να περιγράψει μια ευπάθεια σε ένα σύστημα, είτε λογισμικού (software), είτε υλισμικού (hardware), είτε υλικολογισμικού (firmware) που επιτρέπει σε έναν επιτιθέμενο να παραβιάσει τη διαθεσιμότητα, εμπιστευτικότητα, διαθεσιμότητα του συστήματος αυτού, των εφαρμογών που φιλοξενεί καθώς και των δεδομένων που το σύστημα αυτό διαχειρίζεται. Ειδικότερα, στα δίκτυα υπολογιστών, η *αδυναμία* ορίζεται ως η ευπάθεια σε κάποιο σταθμό που –μαζί με τη γνώση εκμετάλλευσης της συγκεκριμένης *αδυναμίας*- επιτρέπει την εισβολή στο συγκεκριμένο δίκτυο (Voas, et. al, 1996). Συμφωνα με τους Howard & Longstaff και τον Krsul (Howard, 1998), (Krsul, 1998), οι *αδυναμίες* διαιρούνται σε τρεις μεγάλες κατηγορίες:

- Σχεδιαστικές *αδυναμίες* – εγγενείς *αδυναμίες* στο σχεδιασμό ή στις προδιαγραφές του υλισμικού ή του λογισμικού που δεν αποφεύγονται ούτε με τέλεια υλοποίηση αυτών,

- *Αδυναμίες* υλοποίησης – *αδυναμίες* που πηγάζουν από λάθος στην υλοποίηση υλισμικού και λογισμικού αν και προέρχονται από ικανοποιητικό σχεδιασμό και προδιαγραφές,

- *Αδυναμίες* παραμετροποίησης – *αδυναμίες* που πηγάζουν από λάθη στην παραμετροποίηση και τις ρυθμίσεις ενός συστήματος.

Η βιβλιογραφία συμπεριλαμβάνει και τις ανθρώπινες *αδυναμίες* (π.χ. έλλειψη ευαισθητοποίησης σχετικά με την ασφάλεια πληροφοριών). Η *εκμετάλλευση* των ανθρωπίνων *αδυναμιών* γίνεται, συνήθως, με τεχνικές *κοινωνικής μηχανικής* (social engineering) (Mitnick, 2002).

2.3.3. Αποτέλεσμα

Το λογικό αποτέλεσμα μιας επίθεσης είναι μια μη εξουσιοδοτημένη ενέργεια. Ορίζουμε ως μη εξουσιοδοτημένες ενέργειες, σε μια μη εξαντλητική λίστα, τα παρακάτω φαινόμενα (Γκρίτζαλης, 2004):

- *Διακύβευση εμπιστευτικότητας:* αποκάλυψη πληροφοριών χωρίς την άδεια του ιδιοκτήτη τους

- *Διακύβευση ακεραιότητας:* μη εξουσιοδοτημένη τροποποίηση δεδομένων ή πληροφοριών

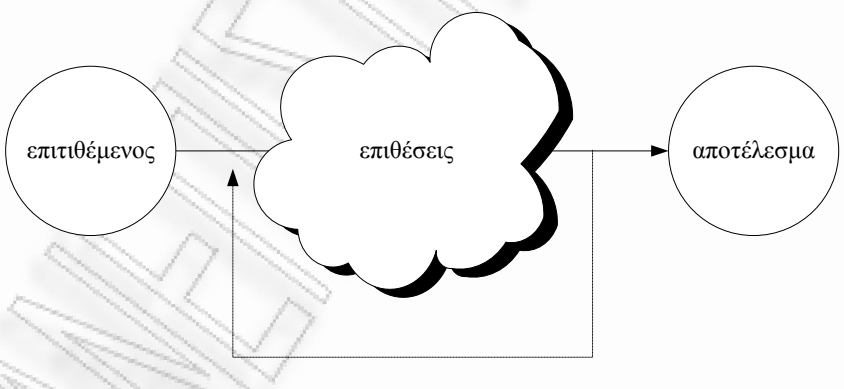
- *Διακύβευση διαθεσιμότητας:* μη εύλογες καθυστερήσεις εξουσιοδοτημένης πρόσβασης πληροφοριών ή υπολογιστικών πόρων

Άλλα πιθανά αποτελέσματα μπορούν να εκφραστούν (άμεσα ή έμμεσα) μέσω των παραπάνω. Για παράδειγμα, η διαγραφή δεδομένων εκφράζει μια διακύβευση της ακεραιότητας, η άρνηση εξυπηρέτησης εκφράζει μια (πλήρη) διακύβευση διαθεσιμότητας,

2.4. Περιστατικά ασφάλειας πληροφοριών

Συχνά, οι μεμονωμένες επιθέσεις που συμβαίνουν σε ένα σύνολο υπολογιστών ή ένα διακριτό τμήμα ενός δικτύου υπολογιστών θεωρούνται ως μέρος ενός περιστατικού ασφάλειας. Υπάρχουν διάφοροι παράγοντες που οδηγούν σε μεμονωμένες επιθέσεις, ενώ για κάθε παράγοντα υπάρχουν –συνήθως- αποσπασματικές πληροφορίες. Για παράδειγμα, μπορεί να υπάρχει είτε ένας μόνο επιτιθέμενος είτε μια ομάδα επιτιθέμενων, η οποία μοιράζεται έναν κοινό στόχο. Οι επιτιθέμενοι είναι πιθανόν να χρησιμοποιούν παρόμοιες επιθέσεις, ή μπορεί να προσπαθούν να επιτύχουν ένα παρεμφερές αποτέλεσμα. Επιπλέον, η τοποθεσία των επιθέσεων (είτε προέλευσης είτε προορισμού) και το χρονικό διάστημα των επιθέσεων μπορεί είτε να είναι το ίδιο, είτε να σχετίζεται με κάποιο τρόπο.

Έτσι, ένα περιστατικό ορίζεται ως ένα σύνολο από διακριτές επιθέσεις λόγω της ιδιομορφίας των επιτιθέμενων, των επιθέσεων, των στόχων, των τοποθεσιών και του χρόνου. Ένα περιστατικό μπορεί να αποτελείται είτε από μια μόνο επίθεση είτε από πολλαπλές επιθέσεις, όπως απεικονίζεται στο Σχήμα 2-2.



Σχήμα 2-2: Η χρήση επιθέσεων για την επίτευξη των στόχων του επιτιθέμενου

Μία πλήρης ταξινόμηση των όρων που σχετίζονται με τα περιστατικά ασφάλειας παρουσιάζεται στο Σχήμα 2-3, το οποίο απεικονίζει τη συσχέτιση των γεγονότων με τις επιθέσεις και τα περιστατικά.

Σύμφωνα με το ISO 18044 (ISO/IEC JTC 1, 2004), ένα περιστατικό ασφάλειας πληροφοριών ορίζεται ως μια σειρά από μη-επιθυμητά ή αναπάντεχα γεγονότα ασφάλειας πληροφοριών τα οποία έχουν μια σημαντική πιθανότητα διακύβευσης των

επιχειρηματικών λειτουργιών και απειλούν την ασφάλεια πληροφοριών μιας επιχείρησης.

2.4.1. Επιτιθέμενοι και στόχοι

Οι άνθρωποι επιτίθενται σε υπολογιστές, χρησιμοποιώντας μια μεγάλη ποικιλία μεθόδων για μια –αντίστοιχα μεγάλη ποικιλία- αντικειμενικών στόχων και επιδιώξεων. Έτσι, ένας επιτιθέμενος ορίζεται ως ένα άτομο (ή σύνολο ατόμων) το οποίο επιχειρεί μια ή περισσότερες επιθέσεις προκειμένου να επιτύχει τον αντικειμενικό στόχο ενός περιστατικού.

Ανάλογα με το στόχο τους, οι επιτιθέμενοι κατηγοριοποιούνται στις παρακάτω κατηγορίες (Σουρής, 2004):

- *Hacker* – επιτιθέμενος ο οποίος επιτίθεται σε υπολογιστικά συστήματα για την *πρόκληση* της απόκτησης πρόσβασης.

- *Κατάσκοπος* (spy) – επιτιθέμενος που επιτίθεται σε υπολογιστικά συστήματα για *πολιτικό ή επιχειρηματικό όφελος* (βιομηχανική κατασκοπία – industrial espionage).

- *Τρομοκράτης* (terrorist) - επιτιθέμενος που επιτίθεται σε υπολογιστικά συστήματα με σκοπό την *πρόκληση πολιτικής επιρροής*.

- *Βάνδαλος* (vandal) – επιτιθέμενος που επιτίθεται σε υπολογιστικά συστήματα με σκοπό την *πρόκληση ζημιάς* ή άρνησης εξυπηρέτησης (denial of service).

- *Κοινός εγκληματίας* (criminal) - επιτιθέμενος που επιτίθεται σε υπολογιστικά συστήματα με σκοπό το κέρδος (*προσωπικό, επαγγελματικό, οικονομικό*, κτλ.).

- *Ερασιτέχνης* (script kiddie) – επιτιθέμενος που επιτίθεται σε υπολογιστικά συστήματα για την επίτευξη ενός *προσωπικού* στόχου, όπως –για παράδειγμα- η καταξίωση σε μια κοινωνική ή πολιτική ομάδα (π.χ. hackers).

- *Εσωτερικός χρήστης* (insider) – εξουσιοδοτημένος χρήστης που επιτίθεται σε υπολογιστικά συστήματα με σκοπό το *προσωπικό* του όφελος.

Οι κατηγορίες των επιτιθέμενων, μαζί με τις κατηγορίες των κινήτρων τους απεικονίζονται στο Σχήμα 2-3, το οποίο απεικονίζει την ακολουθία των γεγονότων που χρησιμοποιούν οι επιτιθέμενοι προκειμένου να επιτύχουν το στόχο τους.

Οι στόχοι ποικίλλουν, ανάλογα με τις κατηγορίες των επιτιθέμενων που περιγράψαμε παραπάνω.

Σύμφωνα με τους Howard και Longstaff (Howard, 1998) είναι ιδιαίτερα σημαντικό να αποσαφηνιστεί η έννοια της επιτυχίας και της αποτυχίας. Ο χαρακτηρισμός μιας επίθεσης ως επιτυχημένης, οφείλεται αποκλειστικά και μόνο στην επιτυχημένη επίτευξη του στόχου του επιτιθέμενου, έχει δηλαδή ως αποτέλεσμα την πρόκληση μιας μη εξουσιοδοτημένης ενέργειας. Με άλλα λόγια, έχει παραβιαστεί η πολιτική ασφάλειας του συγκεκριμένου αντικειμένου.

Σχήμα 2-3: Εννοιολογική θεμελίωση γεγονότων, επιθέσεων και περιστατικών ασφάλειας

2.5. Ανακεφαλαίωση

Στις προηγούμενες ενότητες αναπτύχθηκε το σύνολο των όρων που χρησιμοποιούνται στην ερευνητική περιοχή της αντιμετώπισης περιστατικών ασφάλειας, δόθηκε μια σύντομη επεξήγηση, ενώ παρουσιάστηκε μια ταξονομία που κατηγοριοποιεί τους όρους αυτούς, καθώς και τις μεταξύ τους συσχετίσεις. Οι έννοιες αυτές θα χρησιμοποιηθούν, εκτενώς, στη συνέχεια της διατριβής.

Κεφάλαιο 3

Αντιμετώπιση Περιστατικών Ασφάλειας Πληροφοριών

It isn't that they can't see the solution. It is that they can't see the problem

- **D. K. Chesterton**

Στο κεφάλαιο αυτό ορίζεται η έννοια της Αντιμετώπισης Περιστατικών Ασφάλειας Πληροφοριών σε ένα εταιρικό περιβάλλον, ενώ παρουσιάζεται και ένα πρότυπο διοικητικό μοντέλο που βασίζεται σε ακαδημαϊκή και εφαρμοστέα έρευνα, βέλτιστες διεθνείς πρακτικές, πρότυπα ασφάλειας πληροφοριών και τεχνολογικές υλοποιήσεις. Οι στόχοι είναι:

- να παρουσιαστεί η έκταση και η πολυπλοκότητα της συγκεκριμένης εταιρικής διεργασίας,
- να παρουσιαστούν τα διοικητικά ζητήματα που ανακύπτουν όταν ένας Οργανισμός ή μια εταιρεία αντιμετωπίζει ένα τέτοιο περιστατικό,
- να διερευνηθούν και να κατηγοριοποιηθούν οι συσχετίσεις της διεργασίας αυτής με την Ασφάλεια Πληροφοριών και τη Διοίκηση ενός πληροφοριακού συστήματος.

Στη συνέχεια προτείνεται μια δομημένη μεθοδολογία για το χειρισμό περιστατικών ασφάλειας και παρουσιάζονται αναλυτικά οι διάφορες φάσεις της συγκεκριμένης μεθοδολογίας, ενώ –παράλληλα- προτείνονται βέλτιστες πρακτικές και διαδικασίες που μπορούν να ακολουθηθούν σε κάθε μία από τις φάσεις αυτές. Αναλύονται, επίσης, οι ενεργοί τρόποι αντιμετώπισης ενός περιστατικού, όπως π.χ. η ανεύρεση της πηγής προέλευσής του (π.χ. το δίκτυο, το σύστημα, ο χρήστης του συστήματος ή/και το φυσικό πρόσωπο). Στο πλαίσιο αυτό, παρουσιάζουμε τις πιο διαδεδομένες τεχνικές εξιχνίασης (forensics) της πηγής προέλευσης ενός περιστατικού (automated trace-back) που εξετάζει η διεθνής βιβλιογραφία, κατατάσσοντάς τες σε κατηγορίες. Επίσης, παρουσιάζεται ένα γενικό σενάριο αντιμετώπισης περιστατικών ασφάλειας σε ένα εταιρικό περιβάλλον, προκειμένου να αποδειχτεί η δυνατότητα υιοθέτησης των προαναφερθεισών τεχνικών.

Τέλος, εξετάζονται τα ανοικτά ζητήματα από τεχνικής, διοικητικής, νομικής και κοινωνικής πλευράς.

3.1. Εισαγωγή

Λαμβάνοντας υπόψη πως σχεδόν ενάμιση δισεκατομμύριο υπολογιστικά συστήματα είναι –σήμερα- συνδεδεμένα με το Διαδίκτυο (Miniwatts, 2009), καθώς πως η σύγκλιση των υπηρεσιών ευρυζωνικής πρόσβασης, κινητής τηλεφωνίας και ευρείας περιοχής ασύρματης πρόσβασης είναι γεγονός, τεράστιες ποσότητες πληροφοριών ρέουν μεταξύ πολλαπλών και ετερογενών δικτύων και υπηρεσιών με μια απλή εντολή, αίτηση ή ένα «κλικ» στον υπολογιστή του χρήστη.

Σε αυτή τη βάση, πολλές και διαφορετικές τεχνολογίες, πλατφόρμες και υποδομές διαλειτουργούν προκειμένου να παρέχουν υπηρεσίες στον τελικό χρήστη, ο οποίος αποτελεί το κεντρικό σημείο ενδιαφέροντος της ψηφιακής εποχής: ο χρήστης αιτείται κάποιες υπηρεσίες, ο χρήστης προσπελάζει δίκτυα και υπολογιστικούς πόρους και ο χρήστης απαιτεί ασφάλεια και ιδιωτικότητα. Ο χρήστης μεταφέρει την ψηφιακή του «ταυτότητα» (όπως το αναγνωριστικό χρήστη, το συνθηματικό, τον κωδικό PIN, το ψηφιακό πιστοποιητικό, το βιομετρικό χαρακτηριστικό, κτλ.) σε πολλαπλές διαφορετικές πλατφόρμες και εφαρμογές ώστε να αιτηθεί πρόσβασης στον εταιρικό ή/και οικιακό του υπολογιστή, στο κινητό του τηλέφωνο ή τον υπολογιστή παλάμης, αφήνοντας –παράλληλα- ίχνη των επιλογών, των προτιμήσεων και των συνηθειών του, μαζί με πολλά προσωπικά του δεδομένα.

Από την άλλη πλευρά, υπάρχουν πολλές *αδυναμίες* ασφάλειας στα προαναφερθέντα δίκτυα και συστήματα. Οι *αδυναμίες* αυτές, αν δεν αντιμετωπιστούν με κατάλληλο τρόπο και σε κατάλληλο χρόνο, είναι πιθανόν να οδηγήσουν σε πολλά διαφορετικά αποτελέσματα, όπως είδαμε και στο Κεφάλαιο 1. Κάθε περιστατικό ασφάλειας, ήτοι κάθε ενέργεια με αρνητική επίπτωση στην ασφάλεια ενός συστήματος (CERT/CC, 1998), απαιτεί κατάλληλες μεθόδους, μηχανισμούς και πολιτικές ασφάλειας ώστε να ελαχιστοποιηθούν οι –αρνητικές- συνέπειές του. Επιπλέον , οι μέθοδοι και οι μηχανισμοί αυτοί είναι πιθανόν να στοχεύουν στην εύρεση της πραγματικής προέλευσης του συγκεκριμένου περιστατικού. Τα αντίμετρα ποικίλλουν από απλές τεχνικές ενέργειες (π.χ. ενημέρωση ασφάλειας μιας εφαρμογής) μέχρι ιδιαίτερα πολύπλοκες διεργασίες που εφαρμόζονται στα εταιρικά περιβάλλοντα. Η αντιμετώπιση περιστατικών ασφάλειας

(Incident Response) ορίζεται, εδώ και αρκετά χρόνια, ως η εταιρική διεργασία που στοχεύει στην ελαχιστοποίηση της ζημίας που προκαλείται από ένα περιστατικό ασφάλειας, στη διαρκή επίβλεψη για περιστατικά ασφάλειας καθώς και στη μέγιστη απόκτηση γνώσης από τα περιστατικά που συμβαίνουν (BSI, 1999).

3.2. Η διοικητική πλευρά της αντιμετώπισης περιστατικών ασφάλειας πληροφοριών

Το Διαδίκτυο (Internet) είναι το μέσο που συνδέει συστήματα και δίκτυα υπολογιστών σε όλα τα μήκη και πλάτη του πλανήτη. Η γεωγραφική διασπορά του συγκεκριμένου μέσου απαιτεί, πολλές φορές, συντονισμένες ενέργειες για την αντιμετώπιση ενός περιστατικού ασφάλειας σε διεθνές επίπεδο. Η Ομάδα Αντιμετώπισης Έκτακτων Αναγκών (Computer Emergency Response Team/Coordination Center - CERT/CC) του Πανεπιστημίου Carnegie Melon των Η.Π.Α. ήταν η πρώτη προσπάθεια για την αναφορά περιστατικών ασφάλειας, καθώς και για την παροχή κατάλληλων οδηγιών αντιμετώπισης. Παρόμοιες προσπάθειες υπήρξαν και υπάρχουν στην Ευρώπη (όπως π.χ. το Forum of Incident Response and Security Teams - FIRST), την Αυστραλία (Australian Computer Emergency Response Team - AusCERT), κ.ά.. Οι Ομάδες Αντιμετώπισης Περιστατικών Ασφάλειας Πληροφοριών (Computer Security Incident Response Teams - CSIRTs) αποτελούν βασικό συστατικό σε κάθε σύγχρονο πρότυπο ασφάλειας πληροφοριών (π.χ. (ISO/IEC 17799), (ISO/IEC, 2005). Ο ρόλος των ομάδων αυτών (CSIRT) περιγράφεται πλήρως στο RFC 2350 (IEFT, 1998).

Οι ομάδες CSIRT κατηγοριοποιούνται ανάλογα με τον ιδιοκτήτη τους (π.χ. εσωτερικά σε έναν οργανισμό, εμπορική επιχείρηση, προμηθευτή/κατασκευαστή, κυβερνητική υπηρεσία, κτλ) καθώς και με τον τρόπο λειτουργίας τους (π.χ. επίσημη, ad-hoc) (Van Wyk, 2001). Τέλος, οι ομάδες CSIRT μπορεί να είναι μέλη διεθνών συνεργασιών καθώς και να λειτουργούν υπό καθεστώς διακρατικών συμφωνιών (Council of Europe, 2001).

Μια αναλυτική περιγραφή των οργανωτικών μοντέλων για τις ομάδες CSIRT υπάρχει στο (Killcrece, et. al, 2003). Οι Wan Wyk και Forno συνοψίζουν τα πλεονεκτήματα και

τα μειονεκτήματα των διαφορετικών τρόπων λειτουργίας στον Πίνακας 3-1 (Van Wyk, 2001).

Πίνακας 3-1: Πλεονεκτήματα και μειονεκτήματα των διαφορετικών τύπων CSIRT (Van Wyk, 2001)

Τύπος Ομάδας	Πλεονεκτήματα	Μειονεκτήματα
Δημόσιας Πρόσβασης (συντονιστικό κέντρο ή κέντρο ανάλυσης)	Χαμηλό κόστος για έναν οργανισμό Χρήσιμη πηγή στατιστικών στοιχείων Ευρεία διανομή των περιστατικών ασφάλειας	Μη ενδιαφέρον για παροχή υποστήριξης σε συγκεκριμένο οργανισμό Πολύπλοκο μοντέλο χρηματοδότησης που δεν εγγυάται πάντοτε την ενημέρωση των πληροφοριών
Εσωτερική (σε έναν οργανισμό)	Πλήρως αφοσιωμένη στο περιβάλλου του συγκεκριμένου οργανισμού Εμπειρία Άμεση επιρροή στη βελτίωση της συνολικής ασφάλειας ενός οργανισμού	Δύσκολη η κατασκευή της «πλούσιας εικόνας» ενός περιστατικού ευρείας κλίμακας και έκτασης Μεγάλο κόστος χρηματοδότησης
Εμπορική	Υψηλή τεχνογνωσία Κόστος ανάλογο της συχνότητας περιστατικών και του βαθμού εμπλοκής Υπηρεσία που καλύπτεται από αντίστοιχο συμβόλαιο	Χαμηλή γνώση ενός εταιρικού περιβάλλοντος Συνήθως χειρίζονται ευρείας έκτασης περιστατικά Πιθανή καθυστέρηση εμπλοκής και διαθεσιμότητας
Κατασκευαστή	Άμεση διόρθωση *αδυναμιών* ασφάλειας σε συγκεκριμένα προϊόντα Διαθεσιμότητα μηχανικών	Εμπειρία μόνο σε συγκεκριμένες τεχνολογίες Δύσκολη η κατασκευή της «πλούσιας εικόνας» ενός περιστατικού ευρείας κλίμακας και έκτασης
Κατά περίσταση	Εμπλοκή υποσυνόλου των εμπλεκομένων	Μη αφοσιωμένοι πόροι Δύσκολη διοικητική υποστήριξη

Εκτός των όσων αναφέρονται στον Πίνακα Πίνακας 3-1, υπάρχει μια έντονη διένεξη σχετικά με το ρόλο των συντονιστικών κέντρων, ο οποίος – σύμφωνα με τον Schultz- πρέπει να αλλάξει δραστικά, καθώς τα περισσότερα από τα συντονιστικά κέντρα παρέχουν τις ίδιες –σχεδόν- πληροφορίες, χωρίς να προχωρούν σε διεξοδική ανάλυση

των περιστατικών ασφάλειας, των *αδυναμιών* που σχετίζονται με αυτά, των κινδύνων που απορρέουν και των επιθέσεων που προκύπτουν (Schultz, 2004).

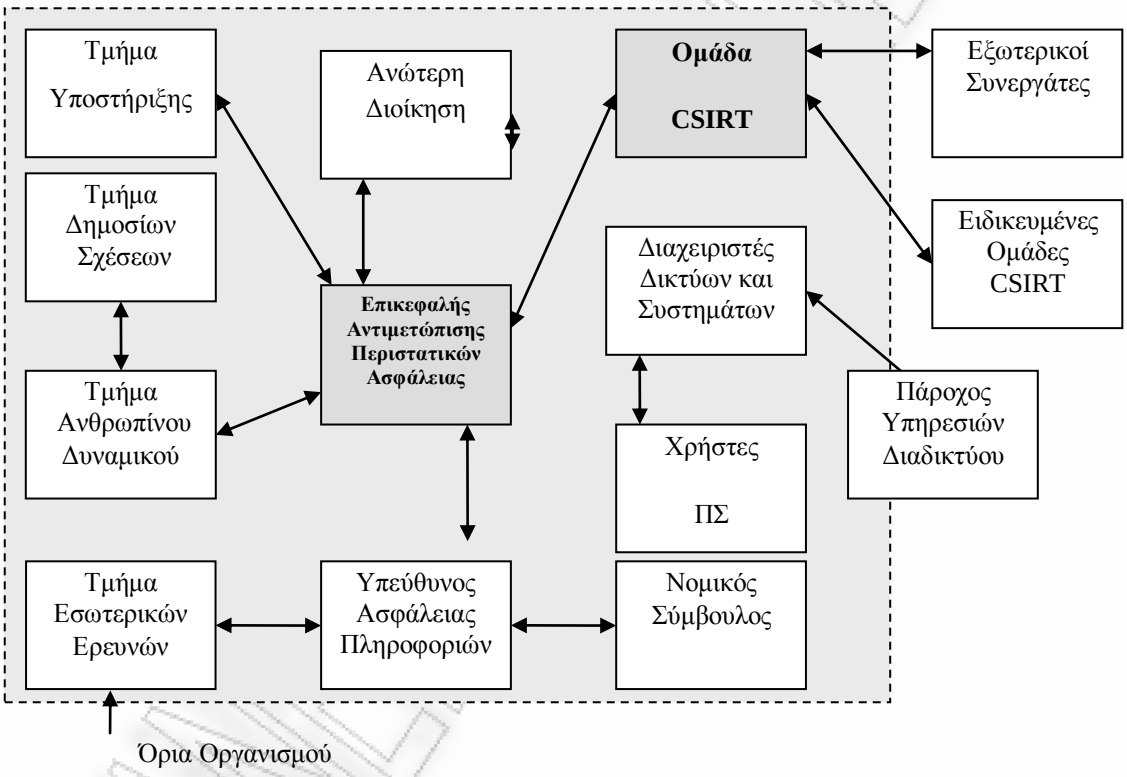
3.2.1. Διοικητικό μοντέλο αντιμετώπισης περιστατικών ασφάλειας

Όταν ένας οργανισμός υλοποιεί μια Εταιρική Πολιτική Αντιμετώπισης Περιστατικών Ασφάλειας Πληροφοριών (Incident Response Policy) γνωστή επίσης, και ως Δυνατότητα Αντιμετώπισης Περιστατικών - Incident Response Capability), είναι ιδιαίτερα σημαντικό να ξεκαθαριστούν οι ρόλοι και οι αρμοδιότητες των εμπλεκομένων. Κρίνεται σκόπιμο να τονιστεί πως η αντιμετώπιση περιστατικών δεν είναι ένα αμιγώς τεχνικό ζήτημα, καθώς πρέπει να συμμετέχουν σε αυτήν άτομα που δεν ανήκουν –κατ' ανάγκη- μόνο στο Τμήμα Πληροφορικής/Μηχανοργάνωσης ενός οργανισμού.

Για το σκοπό αυτό, απαιτείται ένα διοικητικό μοντέλο που να μπορεί εύκολα να υλοποιηθεί μέσα στον Οργανισμό και να υιοθετηθεί από όσο το δυνατόν περισσότερα μέλη του. Στο Σχήμα 3-1 απεικονίζεται ένα διοικητικό μοντέλο αντιμετώπισης περιστατικών που συμπεριλαμβάνει τα απαραίτητα μέλη (γνωστά και ως επαφές – Contacts) που θα πρέπει να συμμετέχουν σε μια αντίστοιχη εταιρική διαδικασία. Στο ίδιο σχήμα απεικονίζονται, επίσης, οι συσχετίσεις και οι διαδράσεις των επαφών αυτών.

Ο ρόλος-κλειδί σε μια τέτοια εταιρική διαδικασία είναι ο *Επικεφαλής Αντιμετώπισης Περιστατικών Ασφάλειας (Incident Response Capability Leader – IRCL)*, ο οποίος αναφέρεται απευθείας στην *Ανώτερη Διοίκηση* του οργανισμού. Είναι υπεύθυνος να συνεργάζεται με άλλα διοικητικά στελέχη ώστε αφενός να τους γνωστοποιεί την εμφάνιση ενός περιστατικού και αφετέρου να διευκολύνει τις διοικητικές αποφάσεις που πρέπει να ληφθούν. Ο συγκεκριμένος ρόλος μπορεί να διευθύνει, ανάλογα με την περίσταση, την *Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας (CSIRT)*, η οποία είναι υπεύθυνη για το σχεδιασμό, την υλοποίηση και την επικαιροποίηση των τεχνικών μέτρων που απαιτούνται, σύμφωνα με τις πολιτικές και τις διαδικασίες που εκδίδει ο *Υπεύθυνος Ασφάλειας (Security Officer)*.

Οι *Διαχειριστές Συστημάτων και Δικτύων (System and Network Administrators)* παρέχουν χρήσιμες πληροφορίες κατά τη διάρκεια ενός περιστατικού ασφάλειας, καθώς –συνήθως- διαθέτουν πολύ καλή γνώση των δικτυακών και πληροφοριακών υποδομών του Οργανισμού, μιας και το αντικείμενο της εργασίας τους περιλαμβάνει το σχεδιασμό, την εγκατάσταση και παραμετροποίηση συστημάτων και δικτύων, καθώς και τη συντήρησή τους. Οι *Διαχειριστές Συστημάτων και Δικτύων* μπορεί να ανήκουν στην CSIRT ή να συμμετέχουν σε αυτήν μόνο όταν απαιτείται από τις συνθήκες. Σε κάθε περίπτωση, όμως, χρειάζεται να ενημερώνονται κατάλληλα για την εμφάνιση ενός περιστατικού.



Σχήμα 3-1: Διοικητικό Μοντέλο Αντιμετώπισης Περιστατικών Ασφάλειας

Τέλος, το *Τμήμα Υποστήριξης (Help Desk)* χρειάζεται να συμμετέχει στην Αντιμετώπιση Περιστατικών, καθώς μπορεί να υπάρξουν περιπτώσεις που απαιτούν την απάντηση σχετικών ερωτημάτων (π.χ. σε περίπτωση άρνησης εξυπηρέτησης από δημόσια συστήματα του οργανισμού, όπως ο εξυπηρετητής ιστού ή ο εξυπηρετητής ηλεκτρονικού ταχυδρομείου).

Εκτός, όμως, από το Τμήμα Πληροφορικής ενός οργανισμού, υπάρχει ανάγκη συνεργασίας και με άλλα τμήματα. Για παράδειγμα, το *Τμήμα Δημοσίων Σχέσεων* μπορεί να χειριστεί τη δημόσια εικόνα ενός οργανισμού, σε περίπτωση που ένα περιστατικό ασφάλειας έχει αντίκτυπο σε αυτήν. Αυτό, πρακτικά, σημαίνει πως το *Τμήμα Δημοσίων Σχέσεων* αναλαμβάνει την επικοινωνία με τρίτες οντότητες, όπως π.χ. πελάτες, συνεργάτες, μέσα μαζικής επικοινωνίας, κτλ. Επίσης, το *Τμήμα Ανθρωπίνου Δυναμικού* μπορεί να συμμετέχει στην Αντιμετώπιση Περιστατικών, σε περιπτώσεις που ένα περιστατικό προκαλείται από το εσωτερικό του οργανισμού (π.χ. έναν υπάλληλο), μιας και είναι το καθ' ύλην αρμόδιο τμήμα για να διαχειριστεί αντίστοιχες καταστάσεις.

Ο ρόλος του *Τμήματος Εσωτερικών Ερευνών* είναι ιδιαίτερα σημαντικός ώστε να κρατήσει μυστικό ένα γεγονός-συνέπεια ενός περιστατικού ασφάλειας, να διευκολύνει την εξακρίβωση της πηγής προέλευσης του συγκεκριμένου περιστατικού καθώς και να μην επιτρέψει τη ροή πληροφοριών εκτός οργανισμού, γεγονός που θα μπορούσε να βλάψει τη δημόσια εικόνα του. Το *Τμήμα Εσωτερικών Ερευνών* συνεργάζεται συχνά με τον *Υπεύθυνο Ασφάλειας* καθώς και με *εξωτερικούς συνεργάτες*, ειδικούς στην ασφάλεια πληροφοριών και την έρευνα περιστατικών ασφάλειας.

Στην περίπτωση που ένα περιστατικό ασφάλειας επισύρει αστικές ή ποινικές ευθύνες (π.χ. κλοπή εξοπλισμού, μη εξουσιοδοτημένη αντιγραφή εμπιστευτικών πληροφοριών, κτλ.) το *Τμήμα Εσωτερικών Ερευνών*, σε συνεργασία με τον *Νομικό Σύμβουλο*, επικοινωνούν με τις Αρχές, προκειμένου να συντονιστούν περαιτέρω ενέργειες. Ο *Νομικός Σύμβουλος*, από την πλευρά του, εκτός από τη διαρκή επικοινωνία του με τον *Υπεύθυνο Ασφάλειας* για τα ζητήματα που αφορούν στην κανονιστική συμμόρφωση του οργανισμού, συμμετέχει στην αντιμετώπιση περιστατικών, παρέχοντας νομικές συμβουλές στους συμμετέχοντες, όποτε κάτι τέτοιο απαιτείται.

Οι *χρήστες του Πληροφοριακού Συστήματος* (ΠΣ) του οργανισμού συχνά ανακαλύπτουν διάφορα ζητήματα ασφάλειας. Με το δεδομένο αυτό, οι *χρήστες του ΠΣ* χρειάζονται κατάλληλη εκπαίδευση ώστε να γνωρίζουν αφενός πώς να χειρίζονται ένα ζήτημα ασφάλειας που πέφτει στην αντίληψή τους, καθώς και με ποιον (ή ποιους) να επικοινωνήσουν για το συγκεκριμένο ζήτημα (και με ποιον τρόπο).

Τέλος, ανάλογα και με τη σοβαρότητα ενός περιστατικού ασφάλειας, συχνά υπάρχει η ανάγκη επικοινωνίας και συνεργασίας με τρίτες οντότητες, οι οποίες μπορούν να βοηθήσουν σημαντικά στον χειρισμό ενός τέτοιου περιστατικού. Για παράδειγμα, ο *Πάροχος Υπηρεσιών Διαδικτύου (Internet Service Provider - ISP)* μπορεί να παρέχει χρήσιμες πληροφορίες για την ανίχνευση της πηγής μιας δικτυακής σύνδεσης, μιας και παρέχει τις υπηρεσίες πρόσβασης του οργανισμού στον έξω κόσμο (π.χ. Διαδίκτυο, τρίτα-δίκτυα, ιδεατά ιδιωτικά δίκτυα (Virtual Private Networks – VPNs), κτλ.). Τέλος, άλλες *ειδικευμένες ομάδες CSIRT* ή και *εξωτερικοί συνεργάτες* (ειδικοί στην ασφάλεια πληροφοριών) μπορεί να παρέχουν σημαντικές υπηρεσίες όταν ένα περιστατικό ασφάλειας ξεπερνά την τεχνογνωσία, τις ικανότητες ή/και την εκπαίδευση της εταιρικής ομάδας CSIRT που προαναφέρθηκε.

3.3. Μεθοδολογία αντιμετώπισης περιστατικών ασφάλειας

Εκτός από το διοικητικό μοντέλο που αναφέρθηκε στην προηγούμενη ενότητα, τόσο η βιβλιογραφία όσο και οι βέλτιστες πρακτικές παρέχουν δομημένες μεθοδολογίες αντιμετώπισης περιστατικών ασφάλειας, οι οποίες αποτελούνται από πολλές και διακριτές φάσεις που στοχεύουν στην έγκαιρη ανίχνευση ενός περιστατικού και την κατάλληλη αντιμετώπισή του στη συνέχεια.

Ενδεικτικά, μερικές από τις πλέον γνωστές μεθοδολογίες είναι το “Framework for Incident Response” της Ομάδας Ασφάλειας Πληροφοριών του Πανεπιστημίου DePaul (Information Security Team, 2002), το “Handbook For Computer Security Incident Response Teams” του Ινστιτούτου Μηχανικής Λογισμικού του Πανεπιστημίου Carnegie Mellon (West-Brown, 1998), καθώς και το “Computer Security Incident Handling Guide” του Εθνικού Ινστιτούτου Προτύπων Τεχνολογίας (NIST) στις Η.Π.Α. (NIST, 2004). Οι συγκεκριμένες μεθοδολογίες εστιάζουν τόσο στην ελαχιστοποίηση των συνεπειών ενός περιστατικού, όσο και στην εύρεση της προέλευσής του.

Μέχρι και σήμερα δεν υπάρχει ένα παγκόσμια αποδεκτό de jure πρότυπο για την Αντιμετώπιση Περιστατικών Ασφάλειας, ούτε ως αυτόνομο κείμενο, αλλά ούτε και ως μέρος ενός διεθνούς προτύπου ασφάλειας πληροφοριών. Για παράδειγμα, οι

κυβερνητικές υπηρεσίες των Η.Π.Α. είναι υποχρεωμένες να διαθέτουν μια Πολιτική Αντιμετώπισης Περιστατικών Ασφάλειας, σύμφωνα με όσα αναφέρονται στο Παράρτημα III της OMB's Circular No. A-130, (US Gov., 2000), αλλά και του Federal Information Security Management Act (FISMA) (US Gov., 2002). Επίσης, το πρότυπο ISO/IEC 17799:2000 (Τμήμα 7.3), δηλώνει πως μια τέτοια πολιτική είναι απαραίτητη, αλλά δεν παρέχει συγκεκριμένες οδηγίες για το πώς κάτι τέτοιο μπορεί να επιτευχθεί (ISO/IEC, 2005)[8].

Χρειάζεται να τονιστεί πως οι περισσότερες μεθοδολογίες Αντιμετώπισης Περιστατικών σχετίζονται με την επιστήμη της ψηφιακής εξιχνίασης ηλεκτρονικών εγκλημάτων (digital forensics), δηλαδή τις τεχνικές διαδικασίες που ανακαλύπτουν δεδομένα αποδεδειγμένης δικαστικής αξίας (πειστήρια) από υπολογιστικά και πληροφοριακά συστήματα (Mandia, 2002). Οι διαδικασίες forensics περιλαμβάνουν τις απαραίτητες ενέργειες εξακρίβωσης της προέλευσης ενός περιστατικού στην πραγματική του πηγή και, στις περισσότερες περιπτώσεις, του φυσικού προσώπου που το προκάλεσε. Οι διαδικασίες forensics απαιτούν μια βαθιά γνώση δικτύων υπολογιστών και λειτουργικών συστημάτων και απαιτούν μεγάλη υπομονή (καθώς οι συγκεκριμένες διαδικασίες είναι εξαιρετικά χρονοβόρες) και ικανότητα υιοθέτησης νομικών κανόνων και διαδικασιών.

Παρόλο που η ερευνητική περιοχή των forensics αναπτύχθηκε περισσότερο από τις αστυνομικές υπηρεσίες και όχι από την ακαδημαϊκή κοινότητα (Yasincac, 2001), φαίνεται πως οι βέλτιστες πρακτικές της και μεθοδολογίες μπορούν να μεταφερθούν και στον χώρο της Αντιμετώπισης Περιστατικών.

Οι περισσότερο γνωστές μεθοδολογίες Αντιμετώπισης Περιστατικών αποτελούνται από πολλά διακριτά στάδια, όπως και η μεθοδολογία που προτείνεται στο Σχήμα 3-2, η οποία βασίζεται στις φάσεις που περιγράφονται στα (NIST, 2004) και (Patsos, 2002). Με βάση τη διεθνή βιβλιογραφία (NIST, 2004), (Patsos, 2002), (Allen, 2001), (Kossakowski et al., 1999), παρουσιάζονται επίσης βέλτιστες πρακτικές και διαδικασίες

[8] Στην πραγματικότητα, το Τμήμα 6.3 του προτύπου παραπέμπει στο αντίστοιχο εδάφιο 12.1.7, το οποίο όμως ασχολείται μόνο με τα διοικητικά κανάλια αναφοράς περιστατικών ασφάλειας.

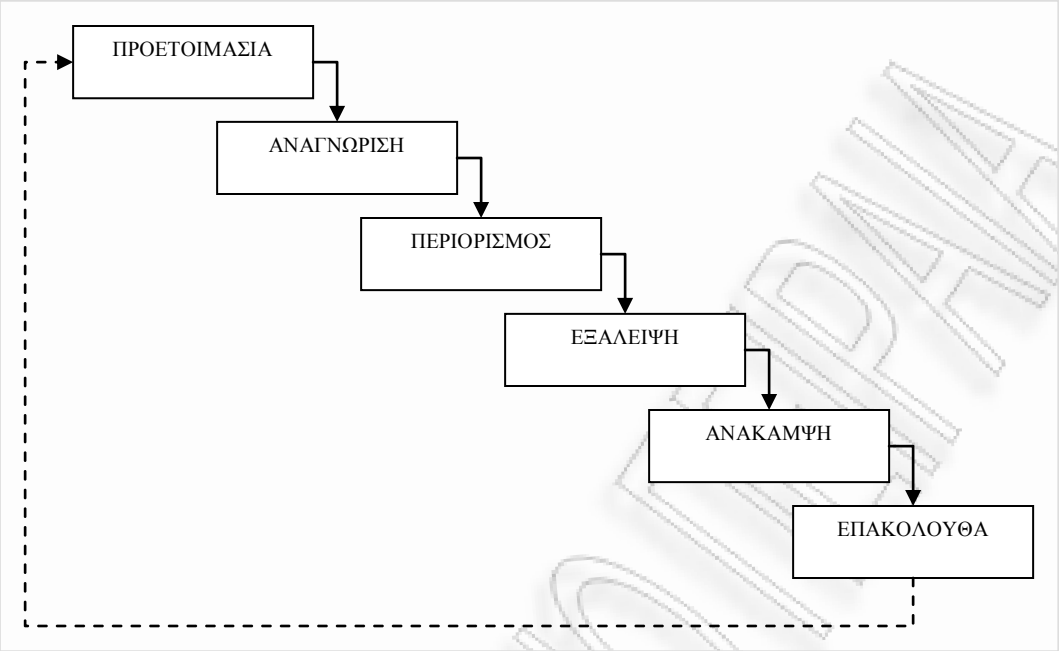
για κάθε ένα στάδιο της μεθοδολογίας. Στα παρακάτω, έχουν συμπεριληφθεί αντιπροσωπευτικές ενέργειες που μπορούν να γίνουν σε κάθε φάση, χωρίς να είναι δυνατό να απαριθμηθούν όλες οι πιθανές επιλογές και οι τυχόν διαφορετικές προσεγγίσεις.

3.3.1. Προετοιμασία

Θεωρώντας πως έχουν υλοποιηθεί μηχανισμοί ασφάλειας πληροφοριών τόσο στην περίμετρο ενός εταιρικού δικτύου (π.χ. τείχη προστασίας – firewalls, αντι-ιομορφικό λογισμικό, μηχανισμοί πιστοποίησης ταυτότητας, κτλ.), όσο και σε κρίσιμα σημεία του εσωτερικού δικτύου (π.χ. συστήματα ανίχνευσης και αποτροπής παρεισφρήσεων – IDS), η αντιμετώπιση περιστατικών απαιτεί την εγκατάσταση ειδικού λογισμικού και υλικού (όπως π.χ. προγράμματα sniffer, λογισμικό κεντρικής διαχείρισης αρχείων ελέγχου και καταγραφής – log files, λογισμικό αντιγράφων ασφάλειας – back up, κτλ.). Στη φάση προετοιμασίας, μερικές από τις χρήσιμες ενέργειες περιλαμβάνουν τα όσα περιγράφονται στα παρακάτω. Η φάση αυτή στοχεύει στην κατάλληλη προετοιμασία ενός οργανισμού για την έγκαιρη αναγνώριση και αντιμετώπιση περιστατικών ασφάλειας, ενώ πολλές πρακτικές που υλοποιούνται στη Φάση Προετοιμασίας χρησιμοποιούνται και σε επόμενες.

3.3.1.1. Μητρώο λειτουργικών συστημάτων και δίσκων εκκίνησης

Είναι ιδιαίτερα σημαντικό να υπάρχει ένα ενημερωμένο μητρώο με όλες τις διαφορετικές εκδόσεις των λειτουργικών συστημάτων που χρησιμοποιούνται στα συστήματα ενός οργανισμού. Επιπλέον, τα αυθεντικά (ή άλλα «έμπιστα») μέσα κάθε εφαρμογής που έχει εγκατασταθεί στα συστήματα αυτά πρέπει να συμπεριληφθούν στο μητρώο αυτό και να είναι διαθέσιμα όποτε οι περιστάσεις το απαιτήσουν. Είναι χρήσιμο, επίσης, να δημιουργηθούν και να διατηρηθούν δίσκοι εκκίνησης των λειτουργικών συστημάτων, καθώς οι δίσκοι αυτοί επιτρέπουν την εκκίνηση ενός συστήματος από ένα προϋπάρχον περιβάλλον λειτουργίας και παρέχουν διασφάλιση έναντι ιομορφικού (ή άλλου επιβλαβούς λογισμικού) καθώς και έναντι τροποποιημένων κρίσιμων αρχείων του συστήματος.



Σχήμα 3-2: Μεθοδολογία Αντιμετώπισης Περιστατικών Ασφάλειας

3.3.1.2. Μητρώο ενημερώσεων ασφάλειας

Κάθε λειτουργικό σύστημα και λογισμικό εφαρμογής έχει *αδυναμίες* ασφάλειας (vulnerabilities). Συνήθως, όταν ανακαλύπτονται και δημοσιεύονται *αδυναμίες* ασφάλειας, ο κατασκευαστής του λογισμικού διαθέτει την αντίστοιχη ενημέρωση (patch) που αντιμετωπίζει τη συγκεκριμένη *αδυναμία*, σε ένα μη προκαθορισμένο όμως χρονικό διάστημα. Η πιο συνηθισμένη πρακτική είναι η απόκτησή του μέσω του επίσημου ιστοτόπου (website) του κατασκευαστή. Καθώς οι ενημερώσεις γίνονται αρκετά συχνά[9], είναι ιδιαίτερα σημαντικό να διατηρείται ένα μητρώο των ενημερώσεων ασφάλειας του λογισμικού, μαζί με μια σύντομη περιγραφή και ένα κρυπτογραφικό άθροισμα ελέγχου, ώστε να διασφαλίζεται πως κάθε ενημέρωση είναι αυθεντική, αλλά και πως η ακεραιότητα του λογισμικού δεν έχει επηρεαστεί (βλ. 3.3.1.5).

[9] Κυρίως γιατί ανακαλύπτονται αρκετά συχνά αντίστοιχες *αδυναμίες*

3.3.1.3. Εργαλεία επανεγκατάστασης

Στην περίπτωση που απαιτείται επανεγκατάσταση ενός συστήματος (βλ. 3.3.3.5 και 3.3.5.1), αυτή θα πρέπει να πραγματοποιηθεί χρησιμοποιώντας εργαλεία από μια έμπιστη πηγή. Όταν χρειάζεται ταυτόχρονη επανεγκατάσταση για ένα πλήθος υπολογιστών (συνήθως σταθμών εργασίας), η διαδικασία μπορεί να πραγματοποιηθεί χρησιμοποιώντας έναν δικτυακό εξυπηρετητή που είτε περιέχει γενικές εκδόσεις των λειτουργικών συστημάτων, είτε περιέχει ακριβή αντίγραφα (γνωστά και ως images) των συστημάτων αυτών. Επίσης, ο εξυπηρετητής αυτός χρειάζεται να διαθέτει εργαλεία που μπορούν να ανακτήσουν, αποσυμπιέσουν, ελέγξουν και εγκαταστήσουν ενημερώσεις ασφάλειας.

3.3.1.4. Διαδικασίες δημιουργίας αντιγράφων ασφάλειας

Τα αντίγραφα ασφάλειας δεδομένων απαιτείται να λαμβάνονται σε συχνή βάση, ώστε όταν συμβεί κάποιο περιστατικό ασφάλειας, η ζημιά στα δεδομένα να είναι όσο το δυνατόν μικρότερη. Ένα ιδιαίτερα σημαντικό ζήτημα που πρέπει να λαμβάνουν υπόψη οι διαχειριστές συστημάτων είναι η ακεραιότητα των δεδομένων στα αντίγραφα ασφάλειας. Πιο συγκεκριμένα, πρέπει να λαμβάνεται ειδική μέριμνα για τον έλεγχο έναντι ιομορφικού λογισμικού που μπορεί να υπάρχει στα αντίγραφα ασφάλειας. Τέλος, ένα δεύτερο αντίγραφο ασφάλειας των δεδομένων θα πρέπει να διατηρείται εκτός των εγκαταστάσεων του οργανισμού (ISO/IEC 27001, 2005).

3.3.1.5. Κρυπτογραφικά αθροίσματα ελέγχου

Κατά τη διαδικασία εγκατάστασης ενός νέου συστήματος, κρίνεται σκόπιμο να καταγράφονται τα κρυπτογραφικά αθροίσματα ελέγχου των κρίσιμων αρχείων του λειτουργικού συστήματος και των εφαρμογών που εκτελούνται σε αυτό. Η συγκεκριμένη πρακτική εξυπηρετεί όταν απαιτείται επανεγκατάσταση ενός συστήματος του οποίου η ασφάλεια έχει παραβιαστεί. Τα κρυπτογραφικά αθροίσματα αυτά θα πρέπει να διατηρούνται σε ειδικά μέσα (π.χ. οπτικούς δίσκους) ώστε η τροποποίησή τους να είναι πρακτικά αδύνατη.

3.3.1.6. Μέσα αποθήκευσης αντιγράφων ασφάλειας

Κατά τη διάρκεια της αντιμετώπισης περιστατικών, τα αντίγραφα ασφάλειας χρησιμοποιούνται προκειμένου να επαναφέρουν ένα σύστημα στην τελευταία κατάσταση καλής λειτουργίας και, αντίστοιχα, στην τελευταία έκδοση των δεδομένων που διατηρούσε. Τα αντίγραφα αυτά μπορούν, επίσης, να χρησιμοποιηθούν και ως αποδεικτικά στοιχεία (στην περίπτωση που ο οργανισμός αποφασίσει να κινηθεί νομικά εναντίον κάποιου άλλου οργανισμού ή φυσικού προσώπου που θεωρείται ως ο αυτουργός του περιστατικού), καθώς και στην περίπτωση που αναλύεται ένα σύστημα δοκιμών, ή και ένα απομονωμένο σύστημα. Τα προτεινόμενα μέσα αποθήκευσης για αντίγραφα ασφάλειας είναι οι οπτικοί δίσκοι, οι οποίοι προσφέρουν σχετικά μεγάλη χωρητικότητα και προστατεύουν από τυχαίες ή σκόπιμες αλλαγές στα περιεχόμενά τους.

Άλλες επιλογές για μέσα αποθήκευσης είναι οι κασέτες (data tapes) που προσφέρουν πολύ μεγάλες χωρητικότητες, όταν γνώμονας είναι το πλήθος των δεδομένων που θα πρέπει να αποθηκευτούν σε αντίγραφα ασφάλειας. Τέλος, τα τελευταία χρόνια γίνονται όλο και περισσότερο διαδεδομένα τα συστήματα δικτυακής αποθήκευσης (Storage Area Network – SAN), τα οποία προσφέρουν έλεγχο πρόσβασης, κάτι ιδιαίτερα χρήσιμο για τις ασφαλείς λειτουργίες που απαιτεί η αντιμετώπιση ενός περιστατικού ασφάλειας.

3.3.1.7. Εργαλειοθήκη πόρων

Η εργαλειοθήκη πόρτων (resource kit) περιλαμβάνει όλα τα απαραίτητα εργαλεία που χρειάζεται η ομάδα CSIRT κατά τη διάρκεια αντιμετώπισης ενός περιστατικού ασφάλειας. Η σωστή οργάνωση και ενημέρωσή του γλιτώνει πολύτιμο χρόνο. Ενδεικτικά, το resource kit περιλαμβάνει λογισμικό κλωνοποίησης δίσκων (disk imaging), λογισμικό σύγκρισης αρχείων, λογισμικό παραμετροποίησης συστημάτων, λογισμικό υπολογισμού και επαλήθευσης κρυπτογραφικών αθροισμάτων ελέγχου, κτλ. Επίσης, κρίνεται σκόπιμο να συμπεριλαμβάνει κενά αποθηκευτικά μέσα διαφόρων τύπων και αρκετής χωρητικότητας, ενώ –σε αρκετές περιπτώσεις- συμπεριλαμβάνει και υλικό ειδικού σκοπού. Για παράδειγμα, ένας φορητός υπολογιστής μπορεί να χρησιμοποιηθεί κατά τη διάρκεια αντιμετώπισης ενός περιστατικού ώστε να επιβλέπει τη δικτυακή κυκλοφορία, ή να εκτελέσει ένα ειδικό λογισμικό ασφάλειας (π.χ. έλεγχο ενός

τρίτου συστήματος για ιομορφικό λογισμικό), Για την αποτελεσματικότερη διαχείριση του resource kit κρίνεται σκόπιμη η ύπαρξη μιας ειδική φόρμα καταγραφής του λογισμικού και του υλικού που συμπεριλαμβάνεται σε αυτό, προκειμένου η πληροφορία αυτή να είναι άμεσα διαθέσιμη στην ομάδα CSIRT ή σε άλλους εμπλεκόμενους. Η φόρμα αυτή μπορεί να αρχειοθετείται σε έντυπη μορφή, ή να αποθηκεύεται ηλεκτρονικά σε διάφορα μέσα (π.χ. οπτικό δίσκο, βάση δεδομένων, κτλ.).

3.3.1.8. Δοκιμαστικά συστήματα και δίκτυα

Αν υπάρχουν επαρκείς πόροι υλικού, είναι χρήσιμη η δημιουργία απομονωμένων (σε φυσικό και λογικό επίπεδο) δοκιμαστικών συστημάτων και δικτύων, όμοια –κατά το δυνατόν- με τα αντίστοιχα συστήματα και δίκτυα παραγωγικής λειτουργίας. Στην περίπτωση μιας σοβαρής –σε έκταση και σημαντικότητα- ζημιάς από ένα περιστατικό ασφάλειας, τα δοκιμαστικά συστήματα και δίκτυα επιτρέπουν την ομαλή και σταδιακή μετάβαση σε παραγωγική λειτουργία με την παράλληλη απόσυρση των διακυβευμένων συστημάτων για περαιτέρω ανάλυση και συλλογή αποδεικτικών στοιχείων. Στην αντίθετη περίπτωση, η ομάδα CSIRT θα πρέπει τουλάχιστον να έχει τη δυνατότητα –κατά περίσταση (ad hoc)- να δημιουργεί περιβάλλον(τα) δοκιμών. Κρίνεται σκόπιμο, από πλευράς ασφάλειας, τα περιβάλλοντα δοκιμών να έχουν το ίδιο επίπεδο ασφάλειας με το παραγωγικό περιβάλλον.

3.3.1.9. Αρχεία ελέγχου και καταγραφής

Η διαχείριση και προστασία των αρχείων ελέγχου και καταγραφής (audit log files) έχει ιδιαίτερη σημασία στην αντιμετώπιση περιστατικών ασφάλειας. Η πολυπλοκότητα των σημερινών συστημάτων και δικτύων έχει σαν αποτέλεσμα την παραγωγή μεγάλου πλήθους και διαφορετικών μορφοτύπων τέτοιων αρχείων. Μια προτεινόμενη πρακτική που υπαγορεύεται από πολλές κανονιστικές οδηγίες και πρότυπα ασφάλειας πληροφοριών (όπως π.χ. (ISO/IEC, 2005), (PCI SSC, 2008), (ΑΔΑΕ, 2005) είναι η χρήση ενός κεντρικού εξυπηρετητή διαχείρισης τέτοιων αρχείων (συχνά αναφέρεται ως

system log server ή πιο απλά syslog[10]), ο οποίος διατηρεί ένα αντίγραφο από όλα τα αντίστοιχα αρχεία ελέγχου και καταγραφής που διατηρούνται τοπικά σε κάθε ένα σύστημα (ή δικτυακή συσκευή, ή λογισμικό επιπέδου εφαρμογής, ή από όποιο άλλο στοιχείο της υποδομής διατηρεί τέτοιου είδους αρχεία). Το σύστημα αυτό θα πρέπει να είναι απομονωμένο και προστατευμένο, ώστε να ελέγχεται αφενός η πρόσβαση και αφετέρου η μεταβολή στα αρχεία που διατηρεί. Αν είναι δυνατόν, η επικοινωνία των συστημάτων και συσκευών που επικοινωνούν με το συγκεκριμένο σύστημα θα πρέπει να είναι κρυπτογραφημένη, ώστε να εμποδίζει κάποιον μη-εξουσιοδοτημένο χρήστη (ή επιτιθέμενο) από το να διαβάζει τις πληροφορίες που διακινούνται προς το εν λόγω σύστημα. Επιπλέον, το σύστημα αυτό θα πρέπει να παραμετροποιηθεί με συγκεκριμένες οδηγίες ασφάλειας (διαδικασία που αναφέρεται σαν hardening) ώστε να ελαχιστοποιεί την πρόσβαση. Η διαδικασία hardening, έχει ως γνώμονα την ελαχιστοποίηση των προσφερόμενων υπηρεσιών από το σύστημα διαχείρισης των αρχείων ελέγχου και καταγραφής, με σκοπό την –κατά το δυνατό- μεγαλύτερη ανθεκτικότητά του σε επιθέσεις ή ακούσιες ενέργειες με αρνητικό αντίκτυπο στην ασφάλειά του. Τέλος, η χρήση ενός πρωτοκόλλου συγχρονισμού (όπως το πρωτόκολλο NTP – Network Time Protocol) έχει ιδιαίτερα μεγάλη σημασία (όπως περιγράφεται και στο (IETF, 1992), καθώς μια έμπιστη πηγή συγχρονισμού επιτρέπει στις πληροφορίες αυτές να μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία στη συνέχεια.

Οι πρόσφατες τεχνολογικές εξελίξεις παρέχουν πλέον ολοκληρωμένα συστήματα διαχείρισης αρχείων ελέγχου και καταγραφής, τα οποία είναι γνωστά ως Συστήματα Διαχείρισης Πληροφοριών Ασφάλειας (Security Information Management Systems – SIMs). Τα συστήματα αυτά προσφέρουν συλλογή, κανονικοποίηση, συσχέτιση και αρχειοθέτηση των γεγονότων ασφάλειας, με βάση πληροφορίες που διατηρούνται –σε τοπικό επίπεδο- σε πολλά και διαφορετικά συστήματα ή συσκευές (π.χ. τείχη προστασίας, συστήματα ανίχνευσης και αποτροπής παρεισφρήσεων, δρομολογητές, κτλ.). Το πιο σημαντικό πλεονέκτημα των συστημάτων αυτών είναι ότι επιτρέπουν

[10] Χωρίς ο όρος syslog να συνδέεται αναγκαστικά με τα μηνύματα του μορφότυπου syslog που παράγονται από ενεργές δικτυακές συσκευές, π.χ. δρομολογητές (routers), μεταγωγείς (switches) ή και λειτουργικά συστήματα Unix.

δυναμικές αναζητήσεις σε πληροφορίες σχετικές με την πηγή και την προέλευση ενός περιστατικού ασφάλειας, καθώς και με τον τύπο του περιστατικού. Οι λειτουργίες και τα χαρακτηριστικά των συστημάτων αυτών, καθώς και των υπηρεσιών που προσφέρουν κατά τη διαδικασία αντιμετώπισης περιστατικών ασφάλειας, περιγράφονται αναλυτικά στο (Mitropoulos, et. al., 2007).

Εκτός από τα συστήματα SIM, οι απλοί και κοινοί εκτυπωτές μπορούν να βοηθήσουν σημαντικά σε μερικές περιπτώσεις. Για παράδειγμα, ένας εκτυπωτής ο οποίος συνδέεται τοπικά σε ένα σύστημα που βρίσκεται σε επίθεση μπορεί να εκτυπώσει οποιαδήποτε ενέργεια εκτελείται από το σύστημα αυτό. Με τον τρόπο αυτό, η παρουσία του δεν μπορεί να γίνει αντιληπτή από έναν επιτιθέμενο, ενώ τα στοιχεία που τυπώνονται είναι σχετικά δύσκολο να τροποποιηθούν από αυτόν (Stoll, 1990).

3.3.2. Αναγνώριση

Η φάση της αναγνώρισης ενός περιστατικού ασφάλειας έχει ιδιαίτερη σημασία, καθώς σε αυτή τη φάση αναγνωρίζεται η έναρξη ενός γεγονότος και λαμβάνονται οι αποφάσεις σχετικά με την κατηγοριοποίησή του και τις διαδικασίες αντιμετώπισής του. Πιθανές λάθος εκτιμήσεις στη φάση αυτή μπορεί να οδηγήσουν τις επόμενες φάσεις, καθώς και ολόκληρη τη μεθοδολογία, σε εσφαλμένα συμπεράσματα.

Η συλλογή αποδεικτικών στοιχείων αρχίζει αμέσως μετά την αναγνώριση ενός περιστατικού ασφάλειας. Από την άλλη πλευρά, η απόφαση για το αν μια μη-συνηθισμένη ενέργεια αντιστοιχεί σε μια πραγματική επίθεση (ή τμήματα αυτής) είναι ιδιαίτερα δύσκολη. Η τεχνολογία παρέχει σημαντικά εργαλεία και μεθόδους (όπως τα συστήματα IDP και SIM που προαναφέρθηκαν), τα οποία απαιτούν μία ευρεία ανάπτυξη στην εταιρική υποδομή. Στις περισσότερες των περιπτώσεων απαιτείται η ανθρώπινη παρέμβαση (και γνώση) για το τι αποτελεί ανώμαλη συμπεριφορά (πιθανή επίθεση) σε ένα συγκεκριμένο εταιρικό περιβάλλον. Στα κεφάλαιο αυτό παρουσιάζονται και αναλύονται προτεινόμενα συστήματα αυτόματης αναγνώρισης περιστατικών ασφάλειας, ενώ στα κεφάλαια 4, 5 & 6 προτείνεται, παρουσιάζεται, αναλύεται και αξιολογείται ένα πρότυπο –τέτοιο- σύστημα.

Ακόμα και στην περίπτωση που είναι δυνατή η εξάλειψη μιας *αδυναμίας* ή/και επίθεσης, υπάρχουν δύο διαφορετικές στρατηγικές που μπορεί να ακολουθήσει ένας οργανισμός:

- Άμεση εξάλειψη της *αδυναμίας* που οδήγησε σε επίθεση
- Μη-εξάλειψη της *αδυναμίας* κατά το μέτρο του δυνατού, αλλά συλλογή αποδεικτικών στοιχείων για τη συνέχεια.

3.3.2.1. Συγκέντρωση και ανάλυση αρχείων ελέγχου και καταγραφής

Μία από τις περισσότερο απαιτητικές και χρονοβόρες διεργασίες είναι η συλλογή και ανάλυση αρχείων ελέγχου και καταγραφής, όπως αναφέρθηκε και στα προηγούμενα. Οι πληροφορίες σχετικά με ένα περιστατικό βρίσκονται σε διάφορες πηγές (συστήματα, δίκτυα) και συχνά απαιτείται μεγάλη εξοικείωση με τον τρόπο και το μορφότυπο που οι πηγές αυτές καταγράφουν ένα περιστατικό, ώστε να μπορεί να πραγματοποιηθεί μια ανάλυση στην οποία θα βασιστούν οι περαιτέρω απαιτούμενες ενέργειες για την αντιμετώπιση του περιστατικού αυτού.

Η σημασία ενός κεντρικοποιημένου συστήματος επεξεργασίας αρχείων ελέγχου και καταγραφής (audit log files) αναλύθηκε, εν συντομία, στην ενότητα 3.3.1.9. Σε περίπτωση που είτε ένα τέτοιο σύστημα δεν υπάρχει εγκατεστημένο στον οργανισμό, είτε δεν συμπεριλαμβάνει το σύνολο των συστημάτων και δικτύων της υποδομής, απαιτείται μια χειρωνακτική διαδικασία. Το διάγραμμα ροής της χειρωνακτικής διαδικασίας ανάλυσης γεγονότων ασφάλειας παρουσιάζεται στο Σχήμα 3-5 (ειδικότερα για ένα σύστημα IDP το οποίο περιέχει πληροφορίες για μια συγκεκριμένη επίθεση καθώς και για τις σχετιζόμενες αδυναμίες), ενώ τα σχετικά βήματα που η διαδικασία καθορίζει περιγράφονται στη συνέχεια.

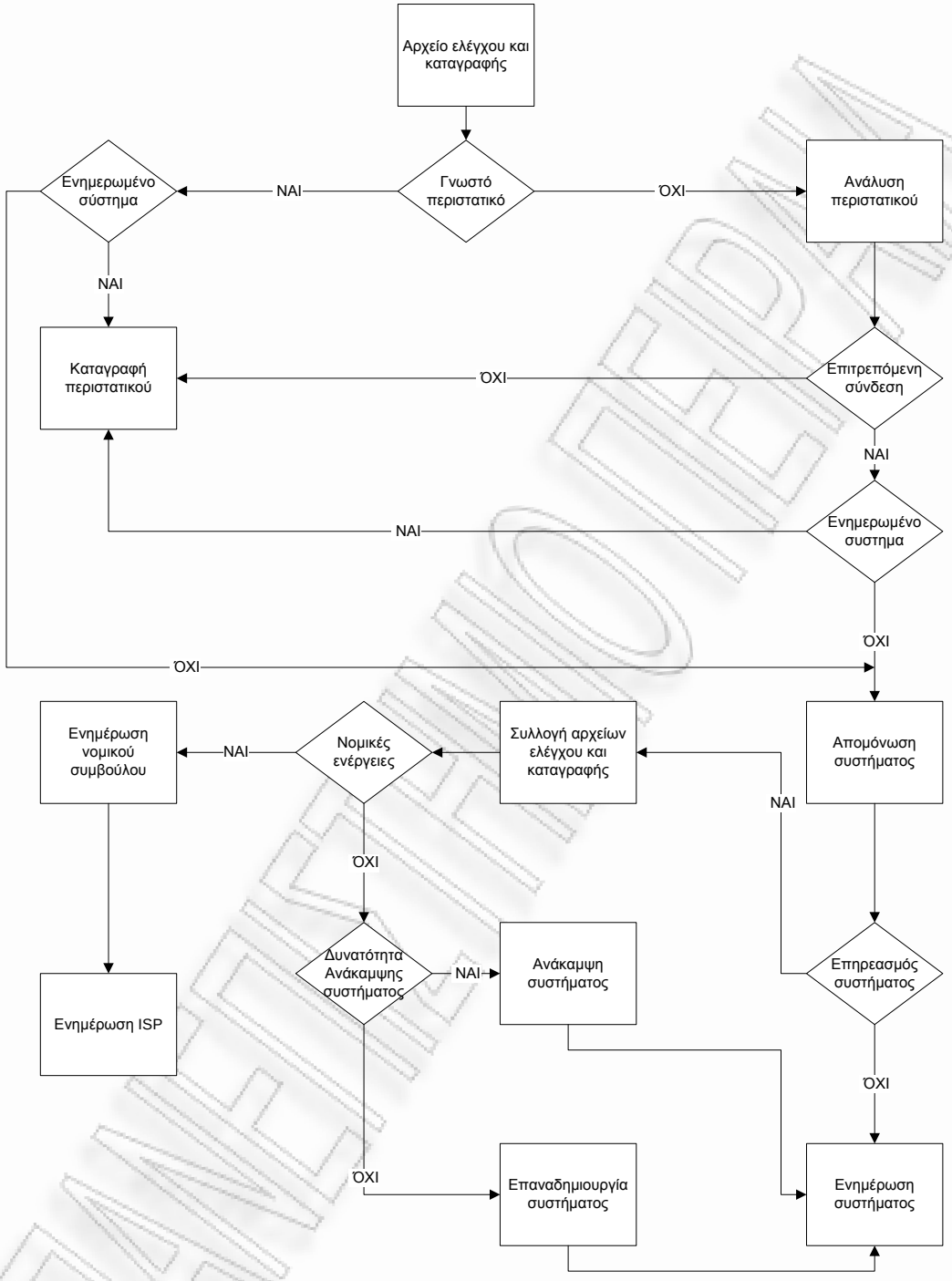
Τα συστήματα ανίχνευσης και αποτροπής παρεισφρήσεων (IDP) διατηρούν μια βάση δεδομένων από τύπους επιθέσεων (patterns), οι οποίες είναι γνωστές και ως «υπογραφές» (signatures), τόσο σε επίπεδο δικτύου όσο και σε επίπεδο τελικού σταθμού (host). Η βάση αυτή μπορεί –δυνητικά- να παρέχει αρκετά χρήσιμες πληροφορίες σχετικά με την προέλευση ενός περιστατικού, καθώς και για τον τύπο του.

Στην περίπτωση που ένα περιστατικό είναι γνωστό στο σύστημα IDP (δηλαδή συμπεριλαμβάνεται στη βάση με τις υπογραφές του), τότε τα επηρεαζόμενα συστήματα πρέπει να ελεγχθούν σχετικά με την *αδυναμία* (vulnerability) που προκάλεσε το συγκεκριμένο περιστατικό. Αν στο σύστημα μπορεί να υλοποιηθεί το απαιτούμενο αντίμετρο για τη συγκεκριμένη *αδυναμία* (συνήθως απαιτείται εγκατάσταση μιας ενημέρωσης ασφάλειας), τότε το περιστατικό καταγράφεται και αρχειοθετείται για μελλοντικές αναφορές.

Αν το περιστατικό δεν είναι γνωστό, τότε θα πρέπει να συλλεχθούν τα αρχεία ελέγχου και καταγραφής του περιμετρικού συστήματος ασφάλειας (π.χ. του τείχους προστασίας – firewall) και να συσχετιστούν με τα αντίστοιχα αρχεία του συστήματος IDP. Αν το τείχος προστασίας απαγορεύει, δεν επιτρέπει δηλαδή, την κυκλοφορία από και προς το σύστημα το οποίο εμφανίζει τη συγκεκριμένη *αδυναμία*, τότε η ένδειξη του συστήματος IDP είναι –πιθανότατα- εσφαλμένη. Στην περίπτωση αυτή, καταγράφεται το περιστατικό και η διαδικασία τερματίζεται.

Από την άλλη πλευρά, αν το τείχος προστασίας επιτρέπει την κυκλοφορία προς το σύστημα αυτό, τότε θα πρέπει να πραγματοποιηθεί έλεγχος σχετικά με την *αδυναμία* ασφάλειας (όπως ακριβώς αναφέρθηκε προηγουμένως). Στην περίπτωση που το σύστημα είναι εκτεθειμένο στη συγκεκριμένη *αδυναμία*, θα πρέπει να απομονωθεί –με συγκεκριμένες διαδικασίες- ώστε να ελαχιστοποιηθεί η πιθανότητα διάδοσης του περιστατικού σε άλλα δίκτυα και συστήματα.

Τονίζεται πως δύο μεγάλα ζητήματα ανακύπτουν όταν ένα σύστημα είναι εκτεθειμένο σε μια συγκεκριμένη *αδυναμία*, κατά τη διάρκεια της αντιμετώπισης ενός περιστατικού ασφάλειας. Πρώτον, η συλλογή αποδεικτικών στοιχείων με ένα συγκεκριμένο τρόπο (forensically-sound manner) ώστε να αναλυθούν σε μεταγενέστερο χρόνο. Δεύτερον, το σύστημα πρέπει να ανακτηθεί, είτε με την εγκατάσταση της κατάλληλης ενημέρωσης ασφάλειας (βλ. 3.3.1.2), είτε από κατάλληλα μέσα (βλ. 3.3.1.3), είτε να εγκατασταθεί και να παραμετροποιηθεί εξαρχής (βλ. 3.3.4.3 και 3.3.5.1).



Σχήμα 3-3: Διαδικασία χειρωνακτικής ανάλυσης αρχείων ελέγχου και καταγραφής και αποφάσεις

3.3.2.2. Αναφορά και ταξινόμηση περιστατικού

Μόλις αναγνωριστεί ή ύπαρξη ενός περιστατικού ασφάλειας, ανάλογα με το μέγεθος της επίπτωσής (impact) του ταξινομείται σε μια από τρεις κατηγορίες, όπως παρουσιάζονται στον Πίνακας 3-2. Οι επιπτώσεις είναι είτε άμεσες (π.χ. χρηματικές επιπτώσεις), είτε έμμεσες (π.χ. επιπτώσεις στη φήμη του οργανισμού ή στη δημόσια εικόνα του). Το εύρος των επιπτώσεων είναι συνήθως ο παράγοντας που καθορίζει τις αρχικές ενέργειες αντιμετώπισης ενός περιστατικού.

Πίνακας 3-2: Κατηγοριοποίηση σημαντικότητας περιστατικών ασφάλειας, ανάλογα με τις επιπτώσεις

Επίπεδο ασφάλειας	Επίπτωση	Παράδειγμα
Υψηλό	Καταστροφική	Διακοπή λειτουργίας εταιρικού δικτύου Διαρροή ευαίσθητων πληροφοριών Πλήρης διακύβευση ασφάλειας ενός σημαντικού αριθμού συστημάτων
Μεσαίο	Σοβαρή	Διακοπή λειτουργίας ενός συστήματος ή καθυστέρηση στη λειτουργία υπηρεσιών Διακύβευση ασφάλειας μεμονωμένου συστήματος Εγκατάσταση επιβλαβούς λογισμικού σε ένα μικρό υποσύνολο συστημάτων
Χαμηλό	Μικρή	Εγκατάσταση επιβλαβούς λογισμικού σε μεμονωμένο σύστημα

Η ταξινόμηση του περιστατικού στις κατηγορίες του Πίνακα Πίνακας 3-2, είναι αποτέλεσμα της Φόρμας Αναφοράς Περιστατικού Ασφάλειας, μιας φόρμας που καταγράφει τις σχετικές πληροφορίες σχετικά με το συγκεκριμένο περιστατικό. Η σημασία της συγκεκριμένης φόρμας είναι ιδιαίτερα μεγάλη, καθώς περιλαμβάνει χρήσιμες πληροφορίες για περαιτέρω ανάλυση, καθώς και γνώση για το συγκεκριμένο περιστατικό. Ενδεικτικά, οι πληροφορίες που μπορεί να περιλαμβάνει η συγκεκριμένη φόρμα περιλαμβάνουν:

- Ημερομηνία και ώρα αναφοράς,
- Ημερομηνία και ώρα αναγνώρισης του περιστατικού,

- Πληροφορίες σχετικά με το σύστημα όπου πρώτα ανιχνεύτηκε το συγκεκριμένο περιστατικό,
- Πιθανά άλλα συστήματα και δίκτυα που επηρεάζονται,
- Ρυθμίσεις συστήματος, εγκατεστημένο λογισμικό και κρισιμότητα για τον οργανισμό,
- Στοιχεία του προσώπου που συμπληρώνει τη φόρμα.

Όλες οι δικτυακές συνδέσεις, οι εκτελούμενες διεργασίες, τα ανοικτά αρχεία καθώς και οι χρήστες που είναι συνδεδεμένοι στο δίκτυο θα πρέπει να καταγραφούν ώστε να παρέχει πλούσια εικόνα της κατάστασης του συστήματος. Αυτό μπορεί να επιτευχθεί με τη χρήση της πληροφορίας που διατηρεί το σύστημα IDP παράλληλα με τη χρήση λογισμικού κλωνοποίησης του σκληρού δίσκου του συστήματος (disk image).

Ένα ακριβές αντίγραφο (αναφέρεται επίσης και ως αντίγραφο δυαδικής ακολουθίας – bit stream image) του συστήματος είναι ένα αντίγραφο (bit-προς-bit) του συστήματος που επηρεάζεται άμεσα από το περιστατικό ασφάλειας. Το αντίγραφο αυτό καταγράφει την τρέχουσα κατάσταση του συστήματος την ώρα της δημιουργίας του αντιγράφου. Συνήθως δημιουργούνται δύο τέτοια αντίγραφα για κάθε διακυβευμένο σύστημα (ένα που διατηρείται ως εχέγγυο εντός του οργανισμού και ένα που χρησιμοποιείται για ανάλυση forensics). Τα αντίγραφα αυτά αποθηκεύονται σε κατάλληλα προστατευμένα μέσα (βλ. 3.3.1.6).

Οι κοινές πρακτικές επιβάλλουν τη διαδικασία δημιουργίας των αντιγράφων αυτών εφόσον έχει συμβεί το περιστατικό ασφάλειας (και αφότου έχει διακυβευτεί η ασφάλεια του συστήματος), ώστε να μπορέσει να πραγματοποιηθεί ανάλυση forensics. Σε αρκετές περιπτώσεις, όμως, απαιτείται η δημιουργία του αντιγράφου ασφάλειας κατά τη διάρκεια που ένα συγκεκριμένο περιστατικό βρίσκεται σε εξέλιξη (σε πραγματικό χρόνο), διαδικασία που μπορεί να πραγματοποιηθεί αν το σύστημα διαθέτει κατάλληλη υλική υποδομή (π.χ. συστοιχίες RAID) ή κατάλληλο εγκατεστημένο λογισμικό (π.χ. λογισμικό forensics).

Ένα ιδιαίτερα σημαντικό γεγονός που δεν θα πρέπει να παραβλέπεται όταν ένας οργανισμός αποφασίσει να διεξαγάγει μια ανάλυση forensics, ώστε να βρει και να διώξει το δράστη, είναι η δημιουργία και διατήρηση της αλληλουχίας των γεγονότων (chain of custody). Τέλος, η διαδικασία δημιουργίας των αντιγράφων ακρίβειας θα πρέπει να γίνεται με μεγάλη προσοχή, καθώς μια μη-συνηθισμένη λειτουργία σε ένα σύστημα μπορεί να ειδοποιήσει τον επιτιθέμενο που έχει αποκτήσει πρόσβαση στο σύστημα.

3.3.2.3. Ανάλυση σε γειτονικά συστήματα

Σε ένα δικτυωμένο περιβάλλον, ένα περιστατικό ασφάλειας επηρεάζει –συνήθως- περισσότερα από ένα συστήματα. Με το δεδομένο αυτό, θα πρέπει να εξετάζονται διάφορα άλλα συστήματα, όπως:

- Συστήματα που ανήκουν στο ίδιο εύρος διευθύνσεων IP,
- Συστήματα που ανήκουν στο ίδιο υποδίκτυο,
- Συστήματα υποδομής που χρησιμοποιεί το σύστημα που έχει επηρεαστεί από το περιστατικό,
- Άλλα κρίσιμα συστήματα.

Για παράδειγμα, σε μια απομακρυσμένη επίθεση, το πλέον σύνηθες σημείο εισόδου είναι οι δημόσια προσβάσιμοι εξυπηρετητές που προσφέρουν τις υπηρεσίες HTTP (Hyper Text Transfer Protocol) και FTP (File Transfer Protocol). Στην περίπτωση ενός επιβλαβούς λογισμικού, ένας συνηθισμένος στόχος είναι ο εξυπηρετητής ηλεκτρονικού ταχυδρομείου (Simple Mail Transfer Protocol - SMTP).

3.3.3. Περιορισμός

Το επόμενο στάδιο αφορά στις άμεσες λύσεις που στοχεύουν στον περιορισμό της έκτασης του περιστατικού ασφάλειας. Οι πλέον συνηθισμένες τεχνικές, στο στάδιο αυτό, αφορούν σε εγκατάσταση ενημερώσεων ή διορθωτικών εκδόσεων ασφάλειας σε ένα

σύστημα, αλλαγές στην περίμετρο του εταιρικού δικτύου, αναθεώρηση των ρυθμίσεων ασφάλειας στα κρίσιμα δημόσια και εσωτερικά συστήματα, κτλ.

3.3.3.1. Απενεργοποίηση συγκεκριμένων υπηρεσιών

Τα αποτελέσματα από την ανάλυση των αρχείων ελέγχου και καταγραφής, σε συνδυασμό με τη Φόρμα Αναφοράς Περιστατικού Ασφάλειας, παρέχουν αρκετές πληροφορίες σχετικά με την έκταση ενός περιστατικού, καθώς και με την *αδυναμία* ασφάλειας (vulnerability) και την *εκμετάλλευση* (exploit) της οποίας είχε ως επακόλουθο το συγκεκριμένο περιστατικό.

Για το σκοπό αυτό, οι υπηρεσίες του συστήματος που σχετίζονται με τη συγκεκριμένη *αδυναμία* θα πρέπει να απενεργοποιηθούν, μέχρι να εκδοθεί, να επικυρωθεί και να εγκατασταθεί στο σύστημα η αντίστοιχη ενημέρωση ασφάλειας ή κάποια διορθωτική έκδοση από τον κατασκευαστή του λειτουργικού συστήματος ή της εφαρμογής.

Η απενεργοποίηση μιας συγκεκριμένης υπηρεσίας μέχρι να απομονωθεί και να επιδιορθωθεί η συγκεκριμένη *αδυναμία* παρέχει αρκετό χρόνο για ανάλυση, ενώ το σύστημα –στις περισσότερες περιπτώσεις- παρέχει τις υπόλοιπες υπηρεσίες. Παρ' όλα αυτά, όμως, αν η *αδυναμία* δεν είναι εκ των προτέρων γνωστή, είναι πιθανόν να περάσει αρκετό διάστημα προτού ο κατασκευαστής του λογισμικού προχωρήσει στην έκδοση του κατάλληλου λογισμικού ενημέρωσης. Στην περίπτωση αυτή, είτε η συγκεκριμένη υπηρεσία του συστήματος πρέπει να παραμείνει απενεργοποιημένη, είτε να ακολουθηθούν εναλλακτικές ενέργειες, σύμφωνα με τη φύση του περιστατικού (π.χ. απενεργοποίηση εντολών σε μια υπηρεσία, π.χ. ενεργοποίηση της εντολής `FTP-get` και όχι της `FTP-put` στην υπηρεσία FTP).

3.3.3.2. Απενεργοποίηση λογαριασμών συστήματος και αλλαγή συνθηματικών

Μια συνήθης πρακτική που ακολουθείται από τους διαχειριστές συστημάτων, όταν συμβαίνει ένα περιστατικό ασφάλειας, είναι η απενεργοποίηση συγκεκριμένων προνομιούχων λογαριασμών και η αλλαγή όλων των συνθηματικών στο σύστημα, μιας και ένα περιστατικό απαιτεί –συνήθως- κάποιας μορφής πρόσβαση στο σύστημα. Στην

περίπτωση αυτή, με δεδομένο ότι ο επιτιθέμενος δεν έχει εναλλακτικές μεθόδους πρόσβασης στο σύστημα (π.χ. μια άλλη *αδυναμία* που παρακάμπτει τους μηχανισμούς πιστοποίησης ταυτότητας), η συγκεκριμένη πρακτική θα τερματίσει την πρόσβαση στον επιτιθέμενο. Από την άλλη πλευρά, η συγκεκριμένη πρακτική θα ενημερώσει τον επιτιθέμενο πως κάποιος διαχειριστής είναι ενήμερος για το περιστατικό, κάτι που μπορεί να αντίκειται στη γενικότερη στρατηγική αντιμετώπισης περιστατικών ασφάλειας που επιβάλλει ότι ο οργανισμός δεν πρέπει να εξαλείψει άμεσα την *αδυναμία* ώστε να μπορέσει να ιχνηλατήσει την προέλευση του περιστατικού. Στην περίπτωση αυτή, χρησιμοποιούνται προηγμένες τεχνικές ασφάλειας (π.χ. χρήση honey pots).

3.3.3.3. Αποσύνδεση συστήματος από το δίκτυο

Σε σοβαρά περιστατικά ασφάλειας η αποσύνδεση ενός συστήματος από το δίκτυο απαιτείται ώστε να αποφευχθεί η απόκτηση πρόσβασης από τον επιτιθέμενο σε περαιτέρω συστήματα (escalation attack), ή η απόκτηση δικαιωμάτων πλήρους πρόσβασης σε ένα συγκεκριμένο σύστημα. Πριν γίνει αυτό, όμως, χρειάζεται να εκτιμηθεί πλήρως η σοβαρότητα ενός περιστατικού ασφάλειας σε σχέση με τις επιχειρησιακές ανάγκες του οργανισμού. Χρειάζεται να τονιστεί πως η αποσύνδεση ενός συστήματος από το δίκτυο είναι μια διοικητική ενέργεια, η οποία θα πρέπει να αποφασίζεται από κατάλληλα εξουσιοδοτημένο πρόσωπο, ιδιαίτερα όταν απαιτείται σε μη-εργάσιμες ώρες.

3.3.3.4. Παύση λειτουργίας του συστήματος

Αν οι παραπάνω πρακτικές δεν έχουν αποτέλεσμα έναντι ενός συγκεκριμένου περιστατικού, θα πρέπει να παύσει η λειτουργία του συγκεκριμένου συστήματος. Η ενέργεια αυτή αποτρέπει περαιτέρω συνέπειες τόσο στο συγκεκριμένο όσο και σε γειτονικά συστήματα. Παράλληλα, επιτρέπει την περαιτέρω ανάλυση και επαναξιολόγηση της κατάστασης. Από την άλλη πλευρά, η παύση λειτουργίας ενός συστήματος θα τερματίσει –αυτόματα- και τις επιχειρησιακές λειτουργίες που το σύστημα αυτό εξυπηρετεί, καθώς και οποιεσδήποτε ενεργές συνδέσεις εκείνη τη χρονική στιγμή. Επιπλέον, τα περιεχόμενα της (πτητικής) μνήμης θα εξαφανιστούν, καταστρέφοντας με τον τρόπο αυτό πιθανά αποδεικτικά στοιχεία που περιλαμβάνονται

σε αυτήν (π.χ. προγράμματα που εκτελούνται από τον επιτιθέμενο, ενεργές δικτυακές συνδέσεις, κτλ.). Αν και η συγκεκριμένη πρακτική δεν συνιστάται, υπάρχουν περιπτώσεις που κάτι τέτοιο είναι αναπόφευκτο[11]. Στις περιπτώσεις αυτές, θα πρέπει να εκτελείται μια ειδική λειτουργία (γνωστή ως memory dump), η οποία αποτυπώνει τα περιεχόμενα της μνήμης του συστήματος στο δίσκο, ώστε να μπορούν να αξιοποιηθούν για ανάλυση αργότερα.

3.3.3.5. Επανεγκατάσταση του συστήματος

Όταν υπάρχουν διαθέσιμοι και κατάλληλοι πόροι υλισμικού, τα δεδομένα του διακυβευμένου συστήματος θα πρέπει να αντικατασταθούν από ένα αξιόπιστο αντίγραφο ασφάλειας. Προτού πραγματοποιηθεί αυτό, η πηγή του περιστατικού (π.χ. *αδυναμία* και δικαιώματα πρόσβασης που εκμεταλλεύτηκε ο επιτιθέμενος, κτλ.) θα πρέπει να έχουν αναγνωριστεί και εκτιμηθεί πλήρως, καθώς και να έχει προηγηθεί η εγκατάσταση των απαιτούμενων διορθωτικών εκδόσεων του λογισμικού.

3.3.4. Εξάλειψη

Η φάση αυτή περιλαμβάνει τις μεσοπρόθεσμες ενέργειες που πρέπει να γίνουν στα συστήματα που επηρέασε το περιστατικό, με σκοπό να εξαλειφθεί κάθε πιθανότητα επανεμφάνισης του συγκεκριμένου περιστατικού. Πιθανά μέτρα που λαμβάνονται στη φάση αυτή περιλαμβάνουν έλεγχο και ενημέρωση των πολιτικών και διαδικασιών ασφάλειας (ειδικότερα στα ζητήματα που σχετίζονται με τον έλεγχο πρόσβασης), ανεξάρτητους ελέγχους ασφάλειας, επαναφορά του συστήματος από (έμπιστα) αντίγραφα ασφάλειας, κτλ.

---

[11] Π.χ. όταν υπάρχουν εμφανείς ενδείξεις πλήρους κατοχής του ελέγχου ενός συστήματος από τον επιτιθέμενο, εμφάνιση μηνυμάτων στην οθόνη που οφείλονται σε ενέργειες του επιτιθέμενου, έναρξη διαδικασίας μορφοποίησης (format) του σκληρού δίσκου του συστήματος, κτλ.

3.3.4.1. Αλλαγή συνθηματικών στα επηρεασμένα συστήματα

Εάν η σύγκριση των κρυπτογραφικών αθροισμάτων ελέγχου που ελήφθησαν κατά τη φάση προετοιμασίας δείξει αλλαγές, επιβάλλεται η αλλαγή των συνθηματικών στους λογαριασμούς πρόσβασης σε όλα τα συστήματα που έχουν επηρεαστεί από το περιστατικό. Αν και είναι μια χρονοβόρα διαδικασία, η πρακτική αυτή παρέχει μια μορφή εξασφάλισης στους διαχειριστές των συστημάτων (καθώς και στα διοικητικά στελέχη).

3.3.4.2. Αλλαγή δικαιωμάτων πρόσβασης

Οι επιτιθέμενοι αφήνουν συνήθως εγκατεστημένα προγράμματα που επιτρέπουν τη μεταγενέστερη σύνδεσή τους με ένα σύστημα (γνωστά και ως προγράμματα backdoor ή Δούρειοι Ίπποι - Trojan horses).

Αρχικά, μια σύγκριση των κρυπτογραφικών αθροισμάτων ελέγχου μπορεί να αποδείξει την ύπαρξη τέτοιων προγραμμάτων. Σε δεύτερο στάδιο, ο έλεγχος του συστήματος με ειδικά εργαλεία ασφάλειας (π.χ. αντι-ιομορφικό λογισμικό ειδικού σκοπού) είναι αρκετά πιθανόν να ανακαλύψει και να αντιμετωπίσει τέτοια προγράμματα.

Σε κάθε περίπτωση πάντως, συνιστάται η επιθεώρηση όλων των λογαριασμών του συστήματος, καθώς και τα δικαιώματα πρόσβασης για κάθε έναν από αυτούς, καθώς, πιθανότατα, ο επιτιθέμενος θα έχει τροποποιήσει (άμεσα ή έμμεσα) κάποιον λογαριασμό που θα του επιτρέψει μελλοντική επανασύνδεση.

3.3.4.3. Επανεγκατάσταση συστήματος από ακριβή αντίγραφα ασφάλειας

Η πλήρης επανεγκατάσταση των συστημάτων που επηρέασε το περιστατικό αποτελεί βέλτιστη πρακτική. Η επανεγκατάσταση μπορεί να πραγματοποιηθεί γρηγορότερα από τα ακριβή αντίγραφα ασφάλειας (3.3.1.4), καθώς αυτά περιλαμβάνουν και όλες τις απαραίτητες δικτυακές και συστημικές ρυθμίσεις (εκτός από τα δεδομένα χρήσης που περιλαμβάνονται στα εφεδρικά αντίγραφα ασφάλειας). Σε κάθε περίπτωση, το σύνολο των ενδεικνυόμενων ενημερώσεων και διορθωτικών εκδόσεων ασφάλειας θα πρέπει να εγκατασταθούν στο σύστημα προτού τεθεί ξανά σε παραγωγική λειτουργία.

3.3.5. Ανάκαμψη

Μετά την επιτυχημένη ακολουθία των προηγουμένων σταδίων, ακολουθεί η πλήρης ανάκαμψη του συστήματος, προκειμένου να τεθεί ξανά σε παραγωγική λειτουργία, χωρίς τα κενά ασφάλειας που οδήγησαν στη διακύβευση της ασφάλειάς του. Οι ενέργειες που εκτελούνται στη φάση αυτή περιλαμβάνουν την πλήρη επανεγκατάσταση του συστήματος, την αναθεώρηση των υπαρχόντων μηχανισμών ασφάλειας, κτλ.

3.3.5.1. Πλήρης επανεγκατάσταση συστήματος

Στην περίπτωση που δεν έχουν ληφθεί (πλήρη) αντίγραφα ασφάλειας κατά τη φάση προετοιμασίας, τότε ο διαχειριστής θα πρέπει να επανεγκαταστήσει τα συστήματα εξαρχής (χρησιμοποιώντας όσα περιγράφονται στις ενότητες 3.3.1.1, 3.3.1.2, 3.3.1.3).

3.3.5.2. Επιθεώρηση ρυθμίσεων συστήματος

Μια συνιστώμενη μέθοδος, προτού το σύστημα επανατοποθετηθεί σε παραγωγική λειτουργία είναι η διεξοδική επιθεώρηση και ο έλεγχος των ρυθμίσεών του. Η πρακτική αυτή στοχεύει στο να ανακαλυφθούν όλα τα πιθανά λάθη ή τυχόν παραλείψεις στις ρυθμίσεις του συστήματος. Τέλος, η βιβλιογραφία αναφέρει τη διεξαγωγή αξιολόγησης ευπαθειών ασφάλειας (vulnerability assessment), ώστε το σύστημα να αξιολογηθεί κατάλληλα προτού λειτουργήσει ξανά παραγωγικά.

3.3.5.3. Επιθεώρηση μηχανισμών ασφάλειας

Στην περίπτωση ενός δικτυακού περιστατικού ασφάλειας, πρέπει να αναθεωρηθούν τόσο οι ρυθμίσεις όσο και η πολιτική ασφάλειας του τείχους προστασίας (firewall). Μιας και η ασφάλεια πληροφοριών δεν αποτελεί μια στατική διαδικασία σε έναν οργανισμό, καθώς νέες μέθοδοι επιθέσεων προκύπτουν καθημερινά, οι διαχειριστές των συστημάτων και οι ειδικοί ασφάλειας πρέπει να επικαιροποιούν τους μηχανισμούς ασφάλειας σε τακτά χρονικά διαστήματα. Ειδικότερα, για τα συστήματα IDP, απαιτείται καθημερινή βελτιστοποίηση των ρυθμίσεών τους, μιας και η αποδοτικότητά τους εξαρτάται –άμεσα- αφενός από τη συνεχή αναβάθμιση της βάσης των *υπογραφών* τους και αφετέρου από τη συνεχή αναθεώρηση των πολιτικών ασφάλειας που υλοποιούν.

3.3.6. Επακόλουθα

Τέλος, κάθε ενέργεια και πληροφορία που σχετίζεται με ένα περιστατικό ασφάλειας θα πρέπει να τεκμηριώνεται επαρκώς (π.χ. μέσω της Φόρμας Αναφοράς Περιστατικού), ενώ κάθε ηλεκτρονικό αποδεικτικό στοιχείο (π.χ. αρχεία ελέγχου και καταγραφής, ακριβή αντίγραφα ασφάλειας,) θα πρέπει να παραδίδονται για περαιτέρω ανάλυση (π.χ. forensics) σε αντίστοιχους ειδικούς. Επιπλέον, μια συνάντηση του Επικεφαλής Αντιμετώπισης Περιστατικών με την ομάδα CSIRT και τη διοίκηση του οργανισμού, επιτρέπει την αξιολόγηση των επιπτώσεων ενός περιστατικού ασφάλειας, την αναθεώρηση μηχανισμών ασφάλειας και αντίστοιχων πολιτικών και διαδικασιών.

3.4. Ιχνηλάτηση περιστατικών ασφάλειας

Ο χειρισμός ενός περιστατικού ασφάλειας μπορεί να αποτελεί μόνο την έναρξη της διαδικασίας αντιμετώπισης, καθώς υπάρχουν περιπτώσεις όπου απαιτείται από έναν Οργανισμό η εξακρίβωση της πηγής προέλευσής του (δηλαδή το φυσικό πρόσωπο/επιτιθέμενος). Η διαδικασία αυτή είναι αρκετά περίπλοκη, καθώς οι επιτιθέμενοι χρησιμοποιούν πολλαπλές τεχνικές απόκρυψης των ιχνών και των ταυτοτήτων τους. Η παραποίηση ταυτότητας (βλ. Ενότητα 2.3) αποτελεί μια τεχνική που μπορεί να επιτευχθεί με πολλαπλούς τρόπους. Οι περισσότερο διαδεδομένοι από αυτούς είναι:

- Παραποίηση ταυτότητας σε επίπεδο διεύθυνσης MAC, δηλαδή η χρήση μιας εξουσιοδοτημένης διεύθυνσης MAC από έναν επιτιθέμενο,
- Παραποίηση ταυτότητας σε επίπεδο IP (Bellovin, 1989), δηλαδή η χρήση μιας εξουσιοδοτημένης διεύθυνσης IP από έναν επιτιθέμενο,
- Παραποίηση ταυτότητας σε επίπεδο εφαρμογής, δηλαδή η χρήση μιας εξουσιοδοτημένης ταυτότητας χρήστη από έναν επιτιθέμενο.

Η ανάλυση των κατανεμημένων επιθέσεων άρνησης εξυπηρέτησης (DDoS) δείχνει πως οι επιτιθέμενοι χρησιμοποιούν συχνά ενδιάμεσους σταθμούς και δίκτυα προτού

εξαπολύσουν μια επίθεση, προκειμένου να ακολουθήσουν διαφορετικά μονοπάτια δρομολόγησης (Lemos, 2001). Εκτός από αυτό, είναι αρκετά διαδεδομένη η χρήση διακυβευμένων ενδιάμεσων σταθμών. Οι διακυβευμένοι αυτοί σταθμοί είναι γνωστοί και ως σκαλοπάτια (stepping stones) που, όταν χρησιμοποιούνται ως κανάλια διακίνησης επιθέσεων, αλλάζουν τη φύση της επίθεσης (π.χ. κρυπτογραφούν τη δικτυακή κίνηση που μεταφέρει την επίθεση (Zhang and Paxson, 2000)). Η ανακατασκευή της διαδρομής που ακολουθεί ένας επιτιθέμενος, ο οποίος έχει χρησιμοποιήσει μια από τις παραπάνω τεχνικές, δεν είναι μια μονοσήμαντη διαδικασία, καθώς υπάρχουν πολλοί τρόποι που παρεμποδίζουν την αντίστροφη κατασκευή της διαδρομής μιας επίθεσης (από το σταθμό-στόχο προς το σταθμό του επιτιθέμενου). Γενικά, *αν η διαδρομή* $c = h_1,h_2,h_3,\ldots,h_n$ *απεικονίζει τη διαδρομή μιας επίθεσης από το σταθμό του επιτιθέμενου (*h_1*) προς το σταθμό-στόχο (*h_n*), το πρόβλημα της ιχνηλάτησης ενός περιστατικού ορίζεται ως η επαγωγική αναγνώριση της πραγματικής διεύθυνσης IP του σταθμού* h_1 *όταν είναι γνωστή η διεύθυνση IP του σταθμού* h_n*.*

Προτού αναλυθεί η ουσία των μηχανισμών αυτόματης ιχνηλάτησης περιστατικών, κρίνεται σκόπιμο να οριστεί το ζήτημα της δικτυακής ιχνηλάτησης, το οποίο χρησιμοποιείται –παραδοσιακά- από μηχανικούς δικτύων υπολογιστών για την αντιμετώπιση προβλημάτων που σχετίζονται με δικτυακές λειτουργίες και πρωτόκολλα. Όπως ορίζεται στο (Postel, 1981), το πρωτόκολλο IP παρέχει την επιλογή εγγραφής δρομολόγησης (Record Route) στην επικεφαλίδα του πρωτοκόλλου. Όταν ενεργοποιείται η συγκεκριμένη επιλογή, όλες οι συσκευές δρομολόγησης σε μία αντίστοιχη διαδρομή είναι υποχρεωμένες να τοποθετούν τις διευθύνσεις IP στο αντίστοιχο πεδίο της επικεφαλίδας. Από την άλλη πλευρά, η επικεφαλίδα στο πρωτόκολλο IP έχει ένα σταθερό μήκος 20 ψηφιοσυλλαβών (bytes) και ένα μεταβλητό μήκος (ανάλογα με το πόσες επιλογές είναι ενεργοποιημένες), το οποίο μπορεί να είναι –το μέγιστο- 40 bytes[12]. Με δεδομένο το πλήθος του διαδικτύου και τις πολλαπλές πληροφορίες δρομολόγησης των σημερινών δικτύων, το πλήθος που προσφέρει το πεδίο Record Route για εγγραφή

[12] Παρ' όλα αυτά, το συνολικό μέγεθος της επικεφαλίδας ενός πακέτου IP ορίζεται από το πεδίο IHL (IP Header Length), το οποίο έχει μέγεθος 4 δυφίων (bits), άρα μπορεί να πάρει κατά μέγιστο την τιμή 15 (1111 στο δυαδικό σύστημα αρίθμησης).

πληροφοριών δρομολόγησης είναι αρκετά μικρό. Επιπλέον, εκτός από το πρόσθετο υπολογιστικό κόστος που απαιτεί η εγγραφή πληροφοριών δρομολόγησης, ένας επιτιθέμενος μπορεί –επίσης- να ενεργοποιήσει (από έναν ενδιάμεσο σταθμό-σκαλοπάτι της δικτυακής διαδρομής) πρόσθετες επιλογές (π.χ. την επιλογή Χαλαρής Δρομολόγησης Πηγής – Loose Source Routing), η οποία καθορίζει υποχρεωτικές συσκευές δρομολόγησης κατά τη δικτυακή κυκλοφορία, ή να προσθέσει διακυβευμένους σταθμούς, εξαντλώντας ιδιαίτερα εύκολα το πλήθος των διαθέσιμων 40 byte.

Υπό το πρίσμα των παραπάνω περιορισμών του πρωτοκόλλου IP, έχει αναπτυχθεί ένα μεγάλο σύνολο τεχνολογιών και μηχανισμών αυτόματης ανίχνευσης πηγής περιστατικών ασφάλειας, οι οποίοι παρουσιάζονται συνοπτικά παρακάτω.

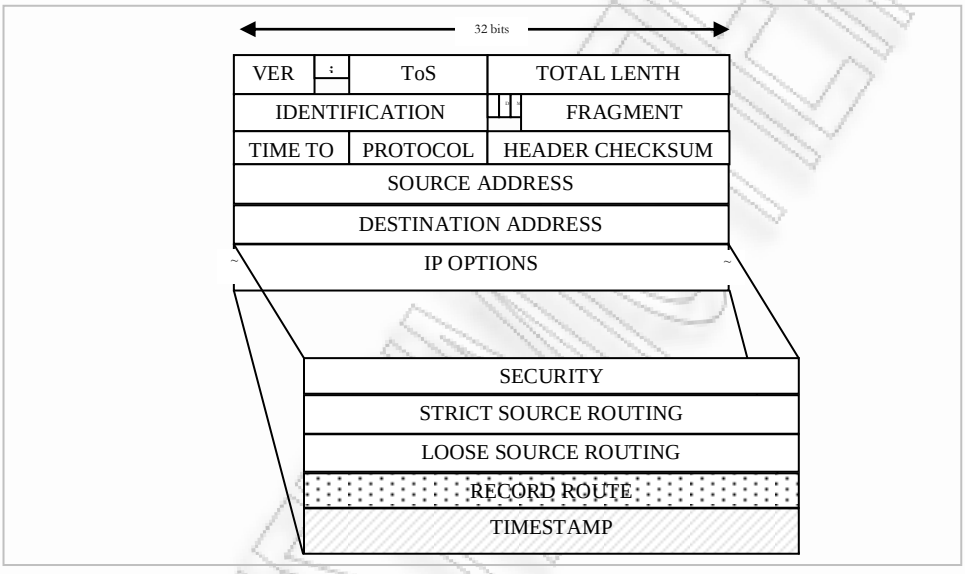
3.4.1. Τεχνικές αυτόματης ιχνηλάτησης με σήμανση IP

Μια σειρά μηχανισμών αυτόματης ιχνηλάτησης βασίζεται στη δυνατότητα της πιθανοτικής σήμανσης πληροφορίας δρομολόγησης στις συσκευές δρομολόγησης, ώστε να μπορεί να αναπαραχθεί πλήρως η διαδρομή της δικτυακής κυκλοφορίας μιας επίθεσης (Savage et al., 2000; Song and Perrig, 2001; Park and Lee, 2001). Οι μηχανισμοί που βασίζονται στην αυτόματη ιχνηλάτηση με σήμανση IP χρησιμοποιούν ιδιαίτερα πολύπλοκους μαθηματικούς αλγόριθμους ώστε να ανακαλύπτουν την προέλευση ενός πακέτου IP, ιδιαίτερα δε των παραποιημένων πακέτων. Οι συγκεκριμένοι μηχανισμοί είναι ιδιαίτερα αποδοτικοί στην ταχύτητά τους, παρέχουν υψηλούς δείκτες πιθανότητας αυτόματης ιχνηλάτησης και μπορούν, σχετικά απλά, να κλιμακωθούν σε ευρεία κλίματα. Δεν μπορούν, όμως, να χειριστούν κρυπτογραφημένη κυκλοφορία και ως εκ τούτου δεν μπορούν να λειτουργήσουν, όταν αντί του πρωτοκόλλου IP –για ένα μέρος της διαδρομής- χρησιμοποιείται η ασφαλής υλοποίηση IPSec (Kent and Atkinson, 1998) ή άλλες τεχνικές κρυπτογράφησης που εμποδίζουν τις συσκευές δρομολόγησης από το να εγγράφουν πληροφορίες δρομολόγησης και να επιτυγχάνουν την αυτόματη ιχνηλάτηση.

3.4.2. Τεχνικές ιχνηλάτησης με βάση το ICMP

Εκτός από του μηχανισμούς ιχνηλάτησης με χρήση τεχνικών σήμανσης IP, τόσο η ερευνητική κοινότητα όσο και ο διεθνής οργανισμός IETF αξιολογούν μια σειρά από

μηχανισμούς ιχνηλάτησης που βασίζονται στη χρήση του Πρωτοκόλλου Ελέγχου Μηνυμάτων Διαδικτύου (Internet Control Message Protocol – ICMP). Το τρέχον πρότυπο του IETF ονομάζεται iTrace, προτάθηκε αρχικά από τον Steve Bellovin (Bellovin, 2003) και βασίζεται στη δυνατότητα των συσκευών δρομολόγησης να δημιουργούν ένα πακέτο «ιχνηλάτησης» για κάθε πακέτο IP που προωθούν (και το οποίο μαρκάρεται για ιχνηλάτηση). Το πακέτο ιχνηλάτησης είναι μια κρυπτογραφική σύνοψη του πρωτότυπου πακέτου.



Σχήμα 3-4: Η επικεφαλίδα του πρωτοκόλλου IP και το πεδίο επιλογών

Τόσο το πρωτότυπο πακέτο, όσο και το πακέτο ιχνηλάτησης, συλλέγονται στον σταθμό προορισμού όπου και επαναδημιουργείται το κανάλι δρομολόγησης. Το iTrace υποστηρίζει τον αλγόριθμο HMAC (US Department of Commerce, 2002) και το πρωτόκολλο X.509 για την πιστοποίηση των μηνυμάτων iTrace. Στην τρέχουσα έκδοση του προτύπου iTrace το πλήθος των πακέτων iTrace που δημιουργούνται από τις συσκευές δρομολόγησης είναι ιδιαίτερα μικρό (στατιστικά γύρω στο 0,005%), με αποτέλεσμα να μην επιβαρύνεται η λειτουργία των συσκευών αυτών. Παρ' όλα αυτά, το συγκεκριμένο πρότυπο απαιτεί έναν αξιοσημείωτο όγκο κυκλοφορίας από ένα -σχετικά- μικρό πλήθος πηγών, λόγω της μικρής πιθανότητας δημιουργίας πακέτων iTrace (Savage et al., 2000). Μια βελτίωση στην προσέγγιση του Bellovin αποτελεί το σχήμα Intention-driven iTrace (Mankin et al., 2001), το οποίο βασίζεται στην προσθήκη ενός δυφίου (το

οποίο ονομάζεται δυφίο σκοπού (intention-bit) στη διαδικασία δρομολόγησης και προώθησης μηνυμάτων καθώς και στις λειτουργίες που παρέχει το Πρωτόκολλο Περιμετρικής Πύλης ((Border Gateway Protocol - BGP) (Rekhter and Watson)).

3.4.3. Τεχνικές ιχνηλάτησης με χρήση σηράγγων IP

Το σχήμα CenterTrack εισάγει την έννοια ενός ειδικού τύπου συσκευών δρομολόγησης (οι οποίες ονομάζονται δρομολογητές ίχνους (Stone, 2000)) και οι οποίες δημιουργούν ένα δίκτυο επικάλυψης (overlay network). Οι συγκεκριμένες συσκευές δρομολόγησης έχουν μια φυσική (ή και λογική) γειτνίαση με τους ακραίους δρομολογητές ενός αυτόνομου συστήματος. Με τη σειρά τους, όλοι οι ακραίοι δρομολογητές συνδέονται με έναν κεντρικό δρομολογητή ίχνους (ή ένα απλό δίκτυο δρομολογητών ίχνους) μέσω σηράγγων IP και δημιουργούν ένα δίκτυο επικάλυψης. Το σχήμα CenterTrack απαιτεί όπως τόσο οι δρομολογητές ίχνους όσο και οι ακραίοι δρομολογητές να μπορούν να υποστηρίξουν λειτουργίες εκσφαλμάτωσης. Αν κάτι τέτοιο δεν είναι δυνατό για το σύνολο των δρομολογητών, ενθαρρύνεται η χρήση εργαλείων ανάλυσης δικτυακής κυκλοφορίας.

Η κυκλοφορία επίθεσης που προορίζεται για το σταθμό στόχο δρομολογείται μέσα από το επικαλυπτόμενο δίκτυο με χρήση πρωτοκόλλων δυναμικής δρομολόγησης, ώστε να επιτρέπεται η βήμα-προς-βήμα ιχνηλάτηση της διαδρομής, ξεκινώντας από το δρομολογητή που είναι πλησιέστερα στο σταθμό-στόχο. Σε όλη τη διάρκεια της διαδικασίας εισάγεται ένα μεγάλο πλήθος εντολών στατικής δρομολόγησης (τόσο στις συσκευές εισερχόμενης όσο και στις συσκευές εξερχόμενης κυκλοφορίας προς/από το σταθμό στόχο, αντίστοιχα), ώστε η συγκεκριμένη κυκλοφορία να δρομολογείται αποκλειστικά μέσα από το δίκτυο επικάλυψης, ενώ –την ίδια στιγμή- όλη η υπόλοιπη κυκλοφορία δρομολογείται εκτός του δικτύου αυτού. Το χαρακτηριστικό αυτό υλοποιείται με ιδιαίτερα περίπλοκο τρόπο, καθώς –σε γενικές γραμμές- είναι αρκετά δύσκολο να χαρακτηρίζεται δυναμικά η κυκλοφορία επίθεσης από την κυκλοφορία μη-επίθεσης και να δρομολογείται αντίστοιχα. Ένα μειονέκτημα του συγκεκριμένου σχήματος είναι πως ο επιτιθέμενος μπορεί να καταλάβει τη λειτουργία ενός τέτοιου δικτύου παρατηρώντας –στατιστικά- τη δικτυακή απόκριση σε τεμαχισμένα πακέτα που

αποστέλλει προς το σταθμό-στόχο στα προκαταρτικά στάδια μιας επίθεσης (McClure et al., 2001). Επίσης, ο επιτιθέμενος μπορεί να επιτεθεί απευθείας στο δίκτυο CenterTrack (π.χ. προκαλώντας μία επίθεση άρνησης εξυπηρέτησης), αχρηστεύοντας, πρακτικά, τη λειτουργία του. Τέλος, όταν ο σταθμός-στόχος είναι ο ακραίος δρομολογητής, τότε το CenterTrack προσπαθεί να δρομολογήσει την κυκλοφορία μέσα από αυτόν το συγκεκριμένο δρομολογητή, με αποτέλεσμα άπειρους επαναλαμβανόμενους βρόχους ή πιθανή κατάρρευση των σηράγγων. Μια εναλλακτική προσέγγιση με χρήση δικτύων επικάλυψης υπάρχει, επίσης, στο (Baba and Matsuda, 2002).

3.4.4. Τεχνικές ιχνηλάτησης σε δικτυακούς σταθμούς

Ιστορικά, οι πρώτοι μηχανισμοί αυτόματης ιχνηλάτησης στόχευαν στην ανακάλυψη των δικτυακών σταθμών που δημιουργούσαν τη διαδρομή σύνδεσης. Οι πλέον διαδεδομένες στη βιβλιογραφία τεχνικές ιχνηλάτησης σε δικτυακούς σταθμούς είναι το σύστημα Caller Identification System (CIS) και το σύστημα CallerID, τα οποία επεξηγούνται συνοπτικά παρακάτω.

Το σύστημα CIS είναι ένα σύστημα ιχνηλάτησης που στοχεύει στην ανακάλυψη ενός επιτιθέμενου εκμεταλλευόμενο τη διαδικασία σύνδεσης με ένα σύστημα (login) (Jung et al., 1993). Η λειτουργία του βασίζεται στην πληροφορία που ανταλλάσσεται μεταξύ δύο συστημάτων κατά τη διαδικασία σύνδεσης. Έτσι, όταν κάποιος χρήστης από το σταθμό h_1 συνδέεται στο σταθμό h_n μέσω ενδιάμεσων σταθμών (h_2,..h_{n-1}), ο σταθμός h_n ερωτά το σταθμό h_{n-1} συγκεκριμένα στοιχεία σχετικά με τη διαδικασία σύνδεσης και συνεχίζει την ίδια λειτουργία (αναδρομικά) μέχρι το σταθμό h_1.

Έτσι, για κάθε σύστημα με το οποίο συνδέεται ένας χρήστης, ελέγχεται όλη η πρότερη πληροφορία σύνδεσης με ενδιάμεσα συστήματα (σταθμούς), προτού παραχωρηθεί (ή όχι) η πρόσβαση. Στο συγκεκριμένο σύστημα υπάρχουν αρκετά σημαντικά μειονεκτήματα, κυρίως λόγω της απαρχαιωμένης μεθόδου ιχνηλάτησης και των εγγενών αδυναμιών αυθεντικοποίησης στις διαδικασίες σύνδεσης (που μπορούν εύκολα να παρακαμφθούν από έναν επιτιθέμενο). Τέλος, εισάγεται σημαντική καθυστέρηση στη διαδικασία σύνδεσης, λόγω του χρόνου που απαιτείται για τον έλεγχο όλων των προηγουμένων συνδέσεων, γεγονός που μπορεί να γίνει αντιληπτό από τον επιτιθέμενο.

Το σύστημα CallerID, το οποίο προτάθηκε από τους Staniford-Chen και Heberlein (Staniford-Chen, 1995) εισάγει μια χειρωνακτική διαδικασία ιχνηλάτησης στη διαδρομή σύνδεσης. Όταν ο επιτιθέμενος συνδέεται στο σταθμό h_n μέσω των $h_1,h_2,...,h_{n-1}$, ο ιδιοκτήτης του σταθμού h_n συνδέεται –με τη σειρά του- στο σταθμό h_{n-1} ώστε να επιβεβαιώσει την προέλευση της σύνδεσης, πολύ συχνά χρησιμοποιώντας τεχνικές επίθεσης. Στη συνέχεια, με τον ίδιο τρόπο, συνδέεται αναδρομικά στους σταθμούς h_{n-2}, $h_{n-3}, ..., h_2$ μέχρι και τον h_1, ο οποίος είναι –θεωρητικά- ο σταθμός του επιτιθέμενου.

Ξεπερνώντας τον ηθικό και νομικό αντίκτυπο του συγκεκριμένου συστήματος, η χρήση του δεν εισάγει καθυστέρηση (όπως στην περίπτωση του CIS) καθώς η λειτουργία του δεν είναι αντιληπτή από τον επιτιθέμενο. Το χαρακτηριστικό αυτό κάνει το σύστημα CallerID ιδιαίτερα ευέλικτο για κλιμάκωση σε αυτόνομα συστήματα και διαδίκτυα. Όμως, τα δίκτυα υψηλών ταχυτήτων, τα μέτρα ασφάλειας και η χειρωνακτική διαδικασία ιχνηλάτησης που απαιτεί η μέθοδος (άμεσα συνυφασμένης με τις ικανότητες ενός διαχειριστή του συστήματος), η χρήση του συγκεκριμένου συστήματος δεν εφαρμόστηκε στην πράξη (αν και στο (Wang et al., 2001) αναφέρεται η χρήση του συστήματος από την Πολεμική Αεροπορία των ΗΠΑ).

3.4.5. Τεχνικές ιχνηλάτησης σε επίπεδο εφαρμογής

Μια ιδιαίτερα υποσχόμενη ερευνητική προσπάθεια, στα πλαίσια της αυτοματοποιημένης αντιμετώπισης περιστατικών, είχε ως αποτέλεσμα την κατασκευή του Πρωτοκόλλου Ανίχνευσης και Απομόνωσης Επιτιθέμενων (Intruder Detection and Isolation Protocol - IDIP) (Schnackenberg et al., 2002; Feiertag et al., 1999). Το IDIP χρησιμοποιείται και επεκτείνεται σε πολλαπλά αυτόνομα συστήματα του Διαδικτύου, καθώς χαρακτηρίζεται από ιδιαίτερα μικρό κόστος ενοποίησης με συστήματα αντιμετώπισης παρεισφρήσεων, τα οποία επεκτείνει με πρόσθετους μηχανισμούς και αλγόριθμους αντιμετώπισης. Το IDIP βασίζεται στην Κοινή Γλώσσα Προδιαγραφών Παρεισφρήσεων (Common Intrusion Specification Language (CISL), η οποία αναπτύχθηκε από το Κοινό Πλαίσιο Ανίχνευσης Παρεισφρήσεων (Common Intrusion Detection Framework - CIDF) και παρέχει μία ενιαία επεξήγηση περιστατικών ασφάλειας (Feiertag et al., 1999).

Οι έλεγχοι αξιολόγησης που διεξήχθησαν στην ερευνητική κοινότητα του DARPA έδειξαν ιδιαίτερα μεγάλη ενοποίηση με συστήματα IDP (Schnackenberg et al., 2002). Παρόλο που η τρέχουσα έκδοση του πρωτοκόλλου υποστηρίζει ένα μικρό σύνολο εντολών («απαγόρευση» και «παραχώρηση» πρόσβασης) της CISL, οι εντολές μπορούν να επεκταθούν σε ένα μεγάλο σύνολο αντικειμένων (π.χ. χρήστες, εφαρμογές, διεργασίες, συνδέσεις, καταστάσεις συστήματος, δικτυακούς σταθμούς,), ώστε ο συνολικός συνδυασμός των εντολών να παρέχει ευέλικτη ανάπτυξη αντίστοιχων πολιτικών.

Πίνακας 3-3: Κατηγοριοποίηση μηχανισμών ιχνηλάτησης περιστατικών ασφάλειας (Mitropoulos, Patsos & Douligeris, 2005)

Μέθοδος	Φύση	Συμπεριφορά	Αρχιτεκτονική	Πεδίο Εφαρμογής	Πολυπλοκότητα
Σήμανσης IP	Δικτυακή	Προληπτική	Κατανεμημένη	Διαδίκτυο	Υψηλή
Χρήσης του ICMP	Δικτυακή	Προληπτική	Κατανεμημένη	Διαδίκτυο	Μεσαία
Χρήσης σηράγγων IP	Δικτυακή	Προληπτική	Κεντρικοποιημένη	Αυτόνομα Συστήματα	Μεσαία
Δικτυακών σταθμών	Σταθμοί Δικτύου	Επανορθωτική	Κεντρικοποιημένη	Αυτόνομα Συστήματα, διαδίκτυα	Χαμηλή
Επιπέδου Εφαρμογής	Δικτυακή, Σταθμοί Δικτύου	Επανορθωτική	Κεντρικοποιημένη	Διαδίκτυο	Υψηλή

3.4.6. Κατηγοριοποίηση μηχανισμών ιχνηλάτησης

Το πρόβλημα της ιχνηλάτησης περιστατικών ασφάλειας είναι ίσως ένα από τα δυσκολότερα στην ασφάλεια πληροφοριών, ενώ η ιδιαίτερα μεγάλη ερευνητική προσπάθεια στη συγκεκριμένη περιοχή δημιουργεί νέες προτεινόμενες λύσεις. Στον Πίνακα Πίνακας 3-3, και με όσα περιγράφονται παραπάνω και αναφέρονται λεπτομερώς στο (Mitropoulos, Patsos & Douligeris, 2005) ταξινομούνται οι προαναφερόμενοι μηχανισμοί, με βάση τη μέθοδο, τη φύση, τη συμπεριφορά, την αρχιτεκτονική, το πεδίο εφαρμογής και την πολυπλοκότητά τους.

3.5. Ανάλυση ψηφιακών πειστηρίων

Εκτός από τους μηχανισμούς ιχνηλάτησης, οι οποίοι στοχεύουν στην εύρεση του σταθμού/συστήματος του επιτιθέμενου, στόχος μιας ανάλυσης ψηφιακών πειστηρίων είναι η ανάπτυξη τεχνικών που αντιστοιχίζουν τις μη-εξουσιοδοτημένες ενέργειες που έγιναν σε έναν υπολογιστή από ένα φυσικό πρόσωπο.

3.5.1. Ανάλυση ψηφιακών πειστηρίων σε υπολογιστή

Η ανάλυση ψηφιακών πειστηρίων σε υπολογιστή είναι η επιστήμη που ασχολείται με την εύρεση αποδεικτικών στοιχείων σε τελικά συστήματα μιας επίθεσης (όπως στα συστήματα του επιτιθέμενου και του στόχου μιας επίθεσης). Ουσιαστικά, ασχολείται με τη διαφύλαξη, ταυτοποίηση, εξαγωγή, τεκμηρίωση και την ερμηνεία υπολογιστικών δεδομένων (Kruse and Heiser, 2002). Σκοπός της είναι η ταυτοποίηση των πραγματικών προγραμμάτων και εντολών που χρησιμοποιήθηκαν κατά τη διάρκεια μιας επίθεσης και η ανακατασκευή (προσομοίωση) της συγκεκριμένης επίθεσης.

Η ανάλυση είναι μια ιδιαίτερα απαιτητική και χρονοβόρα διαδικασία, καθώς απαιτείται η ανάλυση ενός εξαιρετικά μεγάλου πλήθους αρχείων με παράλληλη γνώση του ισχύοντος νομικού πλαισίου για το χειρισμό αποδεικτικών στοιχείων (ώστε να μην παραβιαστεί η ακεραιότητα των δεδομένων που αναλύονται). Εκτός αυτού, απαιτείται η χρήση ενός ειδικευμένου συνόλου εργαλείων λογισμικού και υλισμικού που αναλύει και συσχετίζει δεδομένα και αρχεία ελέγχου και καταγραφής ώστε να εξαχθούν τα κατάλληλα συμπεράσματα. Οι πιθανές ενέργειες σε μια τέτοια ανάλυση, συμπεριλαμβάνουν, μεταξύ άλλων, την (Berghel, 2003):

- αποκρυπτογράφηση αρχείων,
- αποσυμπίεση δεδομένων,
- ανάκτηση κωδικών και συνθηματικών,
- δημιουργία αντιγράφων σε σκληρούς δίσκους,

- ανάλυση του ελεύθερου και ανενεργού χώρου (slack space) σκληρών δίσκων,
- εξέταση πραγματικών αρχείων επιπέδου εφαρμογής,
- ανασύσταση αρχείων συστήματος, κτλ.

Σημειώνεται πως, αν και η συγκεκριμένη ανάλυση μπορεί να οδηγήσει στο πραγματικό φυσικό πρόσωπο του επιτιθέμενου, είναι συχνά δύσκολο να τεκμηριωθούν οι ενέργειες αυτές με τρόπο τέτοιο ώστε να ευσταθούν ενώπιον ενός δικαστηρίου. Επιπλέον, είναι –επίσης- δύσκολο να ερμηνευτεί σε ένα νομικό ακροατήριο το πώς ακριβώς διεξήχθη η συγκεκριμένη ανάλυση. Οι παράγοντες αυτοί απαιτούν τη χρήση συγκεκριμένων εργαλείων και τεχνικών, καθώς η παραμικρή αλλοίωση ενός αρχείου μπορεί να καταστρέψει ολόκληρη τη διαδικασία.

3.5.2. Ανάλυση ψηφιακών πειστηρίων σε δίκτυο υπολογιστών

Η ανάλυση ψηφιακών πειστηρίων σε δίκτυο υπολογιστών (ή και το Διαδίκτυο (Berghel, 2003)) ασχολείται κυρίως με τα δεδομένα μιας δικτυακής σύνδεσης (εισερχόμενα και εξερχόμενα προς/από έναν συγκεκριμένο σταθμό δικτύου). Η ειδοποιός διαφορά των μηχανισμών ιχνηλάτησης (που περιγράφηκαν στα προηγούμενα) με την ανάλυση ψηφιακών πειστηρίων είναι ο σκοπός για τον οποίο η πραγματοποιείται ανάλυση (νομικά και όχι τεχνικά κίνητρα).

Σε αντίθεση με την ανάλυση που πραγματοποιείται σε ένα υπολογιστικό σύστημα (δεδομένα που κλωνοποιούνται και αναλύονται στη συνέχεια), η ανάλυση σε ένα δίκτυο υπολογιστών αναλύει πτητικά και εφήμερα δεδομένα που καταγράφονται –κατά τη διάρκεια- μιας δικτυακής σύνδεσης από αντίστοιχες συσκευές και μηχανισμούς (π.χ. δρομολογητές, τείχη προστασίας, συστήματα IDP, κτλ.).

Σε μια τέτοια ανάλυση οι ενέργειες που πραγματοποιούνται συμπεριλαμβάνουν –μεταξύ άλλων- (Berghel, 2003):

- αρχεία σύνδεσης σε τείχη προστασίας,
- αρχεία σε συστήματα IDP,

- άλλο λογισμικό και συσκευές επίβλεψης,
- αρχεία σε δρομολογητές,
- αρχεία καταλόγου χρηστών.

Στην ανάλυση ψηφιακών πειστηρίων σε δίκτυο υπολογιστών χρησιμοποιούνται τεχνικές τεχνητής νοημοσύνης και σύντηξης (fusion) ώστε να επιταχύνεται η διαδικασία (Nong et al., 1998). Τέλος, η συγκεκριμένη ανάλυση διεξάγεται παράλληλα με την αντίστοιχη ανάλυση σε υπολογιστικά συστήματα, αν απαιτείται τέτοιος διαχωρισμός κατά την αντιμετώπιση ενός περιστατικού ασφάλειας.

3.5.3. Ανάλυση ψηφιακών πειστηρίων σε λογισμικό

Μια ερευνητική ιδέα που προτάθηκε στις αρχές της δεκαετίας του 1990 από τους Spafford και Weeber προτείνει την ανάλυση πειστηρίων σε λογισμικό, ήτοι την εύρεση του αυθεντικού συγγραφέα ενός επιβλαβούς τμήματος κώδικα (Spafford and Weeber, 1992). Αν και κάτι τέτοιο φαίνεται εξαρχής ως μαθηματικά αδύνατο πρόβλημα, η ιδέα στηρίζεται σε συγκεκριμένα μοναδικά χαρακτηριστικά που υπάρχουν σε κάθε υπολογιστικό πρόγραμμα, όπως η γλώσσα, η μορφοποίηση, κάποια ειδικά χαρακτηριστικά, το είδος σχολίων, τα ονόματα μεταβλητών, η χρήση συγκεκριμένων χαρακτηριστικών της γλώσσας, τα μονοπάτια εκτέλεσης, τα μετρικά, κτλ. Οι προφανείς περιορισμοί σε μια τέτοια ανάλυση είναι η ευρεία επαναχρησιμοποίηση κώδικα από διαφορετικούς προγραμματιστές, οι αλλαγές που πραγματοποιούνται σε επίπεδο εφαρμογής καθώς και το μέγεθος του κώδικα αυτού καθεαυτού .

Παρ' όλα αυτά η συγκεκριμένη ανάλυση δεν στοχεύει από μόνη της στην εύρεση του επιτιθέμενου αλλά στη συμπλήρωση των δύο προαναφερόμενων τεχνικών.

Τονίζεται πως, από την άλλη πλευρά, το πρόβλημα της αυθεντικότητας του κώδικα είναι συνυφασμένο με το οικονομικό έγκλημα, την προστασία των πνευματικών δικαιωμάτων και την πειρατεία ψηφιακών μέσων καθώς και το ιομορφικό λογισμικό (στο σύνολό του).

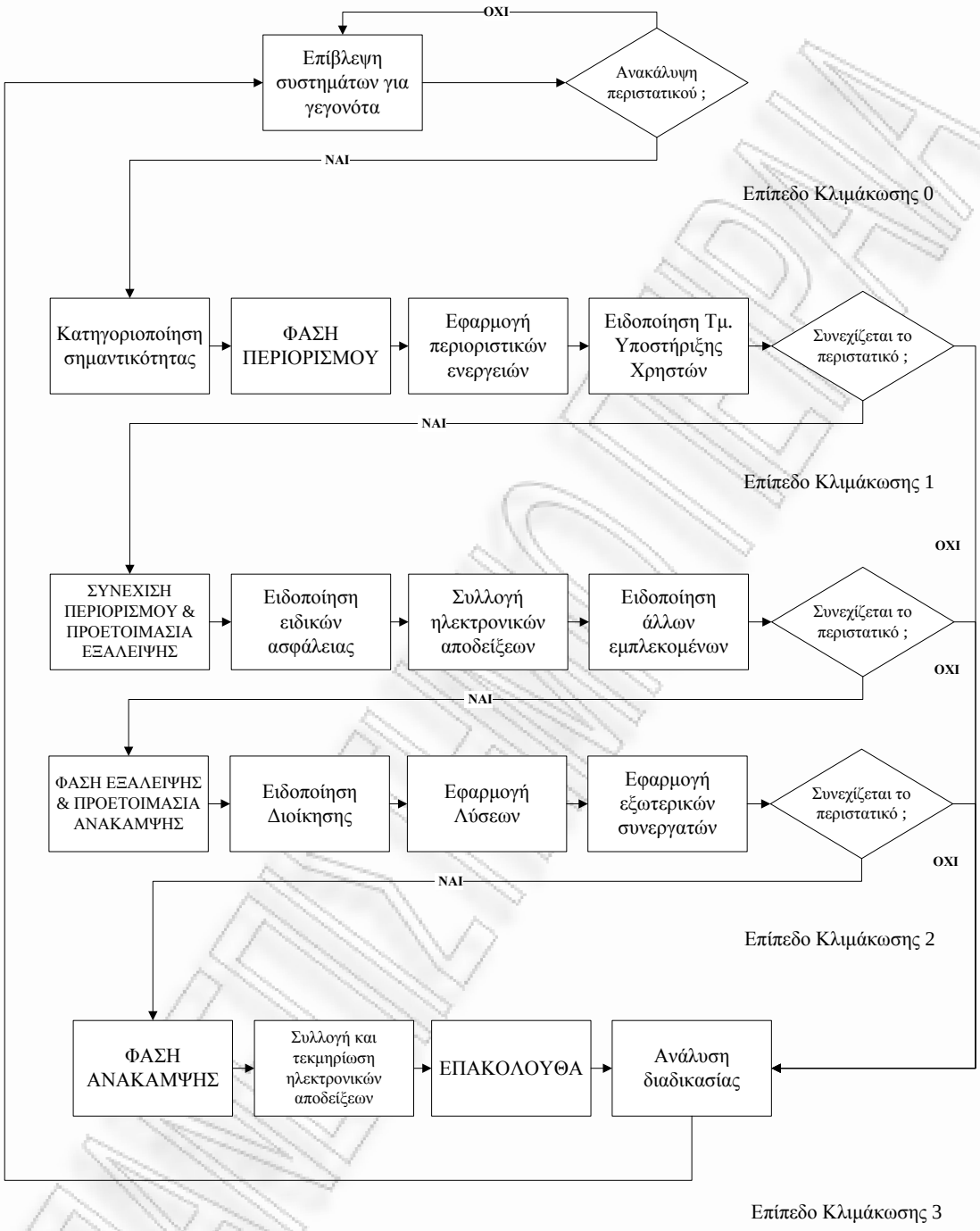
3.6. Ενδεικτική διαδικασία αντιμετώπισης περιστατικών ασφάλειας σε εταιρικά περιβάλλοντα

Στη συγκεκριμένη ενότητα παρουσιάζεται μια συνδυασμένη προσέγγιση του διοικητικού μοντέλου που αναλύθηκε στην ενότητα 3.2.1 και της μεθοδολογίας που αναλύθηκε στις ενότητες 3.3.1-3.3.6. Εν συντομία, προτείνονται και παρουσιάζονται οι απαραίτητες ενέργειες που πρέπει να ακολουθήσει ένας οργανισμός προκειμένου να περιορίσει τις συνέπειες ενός περιστατικού, σε συνδυασμό με τις απαιτούμενες ενέργειες που πιθανόν να οδηγήσουν στην ανεύρεση της πηγής προέλευσης του συγκεκριμένου περιστατικού.

Με τα δεδομένα αυτά, δεν θα πρέπει –επίσης- να παραβλεφθεί το γεγονός ότι η σημαντικότητα ενός περιστατικού αυξάνεται συναρτήσει του χρόνου. Η παράμετρος αυτή, γνωστή και ως «επίπεδο κλιμάκωσης» (escalation level) ταξινομείται σε μία από τις παρακάτω –ευρείες- κατηγορίες.

- Επίπεδο 0, όπου οι επιχειρησιακές διαδικασίες λειτουργούν κανονικά και δεν υπάρχει ένδειξη για την ύπαρξη ενός περιστατικού.
- Επίπεδο 1, όπου ανακαλύπτεται ένα περιστατικό ασφάλειας και λαμβάνουν χώρα οι αρχικές ενέργειες αντιμετώπισης.
- Επίπεδο 2, όπου η έκταση του περιστατικού αυξάνεται και λαμβάνουν χώρα ενέργειες εξάλειψής του.
- Επίπεδο 3, όπου η έκταση του περιστατικού έχει λάβει σημαντικές διαστάσεις και λαμβάνουν χώρα ενέργειες ανάκαμψης.

Οι προτεινόμενες διεργασίες, σε συνδυασμό με τις ενέργειες που πρέπει να ακολουθήσει κάθε μέλος της Αντιμετώπισης Περιστατικών (Incident Response Contact) απεικονίζονται στο Σχήμα 3-5, ενώ παρουσιάζονται συνοπτικά στις παρακάτω ενότητες.



Σχήμα 3-5: Ενδεικτική Διαδικασία Αντιμετώπισης Περιστατικών Ασφάλειας

3.6.1. Επίπεδο κλιμάκωσης 0

Η ομάδα CSIRT παρακολουθεί τις κατάλληλες πηγές για την ύπαρξη πιθανών κινδύνων. Οι πηγές αυτές περιλαμβάνουν διάφορους μηχανισμούς ασφάλειας (π.χ. συστήματα firewall, IDP, συστήματα κεντρικής διαχείρισης αρχείων ελέγχου και καταγραφής, κτλ.), καθώς και πληροφορίες που βρίσκονται εκτός των ορίων του οργανισμού (π.χ. ενημερωτικές λίστες, ιστοτόπους ενημέρωσης σχετικά με προβλήματα ασφάλειας, κτλ.)

3.6.2. Επίπεδο κλιμάκωσης 1

Όταν ανακαλύπτεται και ταξινομείται ένα περιστατικό ασφάλειας, τότε η *Ομάδα CSIRT* τεκμηριώνει την ύπαρξη του συγκεκριμένου περιστατικού (συνήθως μέσω της αντίστοιχης Φόρμας Αναφοράς Περιστατικού Ασφάλειας) και ενημερώνει τον *Επικεφαλής Αντιμετώπισης Περιστατικών Ασφάλειας* για τις πιθανές ενέργειες αρχικής αντιμετώπισης. Ο επικεφαλής πρέπει να εγκρίνει τις ενέργειες αυτές και να ενημερώσει το *Τμήμα Υποστήριξης*, αν απαιτείται κάτι τέτοιο.

3.6.3. Επίπεδο κλιμάκωσης 2

Όταν το περιστατικό έχει λάβει διαστάσεις, ο *Επικεφαλής Αντιμετώπισης Περιστατικών Ασφάλειας* ενημερώνεται από την *Ομάδα CSIRT* σχετικά με τις πιθανές συνέπειες και ενημερώνει με τη σειρά του τους διαχειριστές συστημάτων και δικτύων. Στη συνέχεια, συλλέγει τις αναφορές και εκκινεί τη διαδικασία συλλογής αποδεικτικών στοιχείων. Η *Ομάδα CSIRT* αποφασίζει τις απαραίτητες ενέργειες περιορισμού της έκτασης του περιστατικού (πιθανόν σε συνεργασία με *εξωτερικές ομάδες CSIRT* ή *εξωτερικούς συνεργάτες*) και ενημερώνει –για κάθε ενέργεια- τον *Επικεφαλής Αντιμετώπισης Περιστατικών Ασφάλειας*. Ανάλογα με τη σοβαρότητα του περιστατικού, ο *Επικεφαλής Αντιμετώπισης Περιστατικών Ασφάλειας* ενημερώνει άλλα εμπλεκόμενα μέλη (π.χ. *Τμήμα Εσωτερικών Ερευνών*, *Νομικό Σύμβουλο*, κτλ.)

3.6.4. Επίπεδο κλιμάκωσης 3

Όταν η έκταση του περιστατικού έχει λάβει διαστάσεις, ή οι συνέπειές του είναι σοβαρές, ο *Επικεφαλής Αντιμετώπισης Περιστατικών Ασφάλειας* επικοινωνεί με την *Ανώτερη Διοίκηση* του οργανισμού, προκειμένου να την ενημερώσει για την ανάγκη περαιτέρω ενεργειών (π.χ. αποσύνδεση ενός συστήματος από το δίκτυο, απενεργοποίηση υπηρεσιών, κτλ.) και να λάβει τις σχετικές εγκρίσεις. Η *Ομάδα CSIRT*, σε συνεργασία με τους *διαχειριστές συστημάτων και δικτύων*, αναλύουν τις δυνατές επιλογές που θα περιορίσουν ή/και εξαλείψουν το συγκεκριμένο περιστατικό. Καθ' όλη τη διάρκεια της διαδικασίας συλλέγονται ηλεκτρονικές αποδείξεις, ώστε να είναι δυνατή μια ανάλυση forensic σε μεταγενέστερο χρόνο (αν κάτι τέτοιο αποφασιστεί από την *Ανώτερη Διοίκηση* του οργανισμού).

3.6.5. Περαιτέρω ανάλυση

Όταν το περιστατικό έχει αντιμετωπιστεί κατάλληλα, σε σχετικά σύντομο χρονικό διάστημα, ο *Επικεφαλής Αντιμετώπισης Περιστατικών Ασφάλειας* πρέπει να οργανώσει μια συνάντηση με όσα περισσότερα μέλη της ομάδας αντιμετώπισης περιστατικών είναι διαθέσιμα, καθώς και την *Ανώτερη Διοίκηση* του οργανισμού, ώστε να αναλυθούν τα παρακάτω ζητήματα:

- Εκτίμηση των ζημιών/συνεπειών,
- Ανάλυση των ενεργειών που απαιτήθηκαν,
- Απαιτούμενες ενέργειες για την πλήρη εξάλειψη της *αδυναμίας* που οδήγησε στην εμφάνιση του συγκεκριμένου περιστατικού,
- Πολιτικές και διαδικασίες που χρήζουν αναθεώρησης,
- Άλλες περαιτέρω ενέργειες που απαιτούνται,
- Παράδοση των ηλεκτρονικών αποδείξεων σε εκπρόσωπο της διοίκησης του οργανισμού,

- Επικαιροποίηση των εταιρικών διαδικασιών αντιμετώπισης περιστατικών ασφάλειας.

3.7. Ανοικτά ζητήματα

Οι μεθοδολογίες, οι μηχανισμοί και τα μέτρα που παρουσιάστηκαν παραπάνω παρέχουν την «πλούσια εικόνα» της τρέχουσας κατάστασης στην αντιμετώπιση περιστατικών ασφάλειας. Παρ' όλα αυτά , χρειάζεται να τονιστεί πως όλες αυτές οι πρακτικές είναι στενά συνδεδεμένες με τα εταιρικά περιβάλλοντα και τις αντίστοιχες Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ), καθώς αυτές αποτελούν τον κύριο στόχο επιθέσεων μέχρι και σήμερα. Τα τελευταία χρόνια, παράλληλα με τη σύγκλιση των τεχνολογιών 3G και της ευρυζωνικότητας (broadband) καθώς και με την πρόοδο που συντελείται στις εφαρμογές ηλεκτρονικής διακυβέρνησης και ηλεκτρονικού εμπορίου, υπάρχει μια ραγδαία αύξηση των επιθέσεων σε απλούς χρήστες του Διαδικτύου. Οι συνέπειες των επιθέσεων αυτών ποικίλουν, από μια απλή επανεγκατάσταση του συστήματος ενός χρήστη έως την πλήρη κλοπή της ψηφιακής του ταυτότητας (identify theft). Η κλοπή ψηφιακής ταυτότητας μπορεί να οδηγήσει στην ανυπαρξία ενός ατόμου σε πολλές καθημερινές συναλλαγές, όπως εκείνες που προαναφέρθηκαν. Η συγκεκριμένη συνέπεια, όπως δείχνουν οι στατιστικές, είναι η μάστιγα της εποχής (Harris Interactive, 2003), με σχεδόν 33.4 εκατομμύρια θύματα μόνο στις Η.Π.Α. Αν και ο όρος «κλοπή ταυτότητας» είναι περισσότερο τεχνικός παρά νομικός (καθώς η ταυτότητα δεν κλέβεται αλλά αναπαράγεται από μη εξουσιοδοτημένες οντότητες, χρησιμοποιώντας τεχνικές εναντίον της θέλησης του χρήστη), ουσιαστικά αντικατοπτρίζει τη μη εξουσιοδοτημένη *εκμετάλλευση* προσωπικών δεδομένων που βρίσκονται σε δημόσιες ή ιδιωτικές βάσεις δεδομένων, ως αποτέλεσμα ανεπαρκών μέτρων ασφάλειας. Ως παράδειγμα προσωπικών δεδομένων αναφέρουμε το όνομα και το επώνυμο, τη φορολογική ενημερότητα, τη διεύθυνση κατοικίας, το ποινικό μητρώο, τη στρατιωτική κατάσταση/ικανότητα, το ιατρικό ιστορικό ενός ατόμου κτλ. Τα δεδομένα αυτά βρίσκονται διάσπαρτα και αποκεντρωμένα σε πολλές και διάφορες βάσεις δεδομένων. Η συγκεκριμένη επίθεση δεν είναι κάτι καινούργιο στην ασφάλεια πληροφοριών, αλλά έχει εξελιχθεί με την πάροδο του χρόνου, λόγω της στενότατης εξάρτησης της σημερινής κοινωνίας από τα πληροφοριακά συστήματα για οικονομικές,

στρατιωτικές, κυβερνητικές, εμπορικές και πολλές άλλες χρήσεις. Όπως χαρακτηριστικά αναφέρει ο D. Solove, «Η κλοπή ψηφιακής ταυτότητας δεν συνέβη έτσι απλά – κατασκευάστηκε» (Solove, 2004).

Αν και η τεχνολογία φαίνεται ως υπαίτιος σε μια τέτοια επίθεση, μιας και αποτελεί μετενσάρκωση μιας τυπικής επίθεσης μεταμφίεσης, η οποία έχει αναλυθεί εκτενώς στη σύγχρονη βιβλιογραφία, η έλλειψη διεθνών εναρμονισμένων πρακτικών είναι εκείνη που δυσκολεύει μία αποτελεσματική αντιμετώπιση σε τέτοιου είδους περιπτώσεις.

Το ζήτημα του πώς μια οντότητα πρέπει να αντιδρά σε μια κλοπή ψηφιακής ταυτότητας παραμένει ακόμη ανοικτό, χωρίς κάποια ερευνητική μεθοδολογία, βέλτιστη πρακτική, ή/και RFC να έχει προταθεί μέχρι σήμερα. Οι κλασικές μεθοδολογίες αντιμετώπισης περιστατικών δεν μπορούν να εξυπηρετήσουν την περίπτωση αυτή, καθώς οι διακριτές φάσεις που αναφέρουν είναι αρκετά δύσκολο να εφαρμοστούν (άμεσα ή έμμεσα). Το χαρακτηριστικό δίλημμα μεταξύ της ασφάλειας και της ιδιωτικότητας (privacy) παραμένει.

3.8. Ανακεφαλαίωση

Η αντιμετώπιση περιστατικών ασφάλειας σε ένα εταιρικό περιβάλλον ήταν πάντοτε ένας σημαντικός παράγοντας στην ασφάλεια πληροφοριών, που συχνά παραβλέπεται από τους υπευθύνους ασφάλειας. Η αντιμετώπιση περιστατικών δεν είναι ένα αμιγώς τεχνικό ζήτημα, καθώς έχει αρκετές διοικητικές, νομικές και κοινωνικές προεκτάσεις. Στο κεφάλαιο αυτό προτάθηκε ένα διοικητικό μοντέλο αντιμετώπισης περιστατικών ασφάλειας, μαζί με μια πλήρη και αρθρωτή μεθοδολογία, η οποία βασίζεται σε βέλτιστες διεθνείς πρακτικές για τον κατάλληλο χειρισμό ενός περιστατικού. Παρουσιάστηκε, επίσης, η τρέχουσα κατάσταση της τεχνολογίας σχετικά με την ανάλυση forensics σε επίπεδο υπολογιστή, δικτύου και λογισμικού, καθώς και οι δημοφιλέστερες τεχνικές αυτόματης εξιχνίασης της πηγής ενός περιστατικού. Τέλος, προτάθηκε και παρουσιάστηκε μια γενική διαδικασία αντιμετώπισης περιστατικών ασφάλειας για ένα εταιρικό περιβάλλον.

Κεφάλαιο 4

Τοπολογική Ανάλυση Αδυναμιών Ασφάλειας Πληροφοριών

"In theory, there is nothing to hinder our following what we are taught, but in life there are many things to draw us aside"

- Epictetus

Στο παρόν κεφάλαιο περιγράφεται η τοπολογική ανάλυση αδυναμιών ασφάλειας και οι επεκτάσεις της μεθόδου στην ερευνητική περιοχή των συστημάτων ανίχνευσης και αντιμετώπισης παρεισφρήσεων (IDP). Αρχικά, καθορίζονται οι απαραίτητες πληροφορίες για αδυναμίες ασφάλειας και κώδικα αθέμιτης εκμετάλλευσης που απαιτεί η μέθοδος, καθώς και οι αντίστοιχες απαιτούμενες πληροφορίες από τα συστήματα IDP με σκοπό την εξυπηρέτηση της αντιμετώπισης περιστατικών ασφάλειας. Αναλύονται και αξιολογούνται εκτενώς οι κυριότερες μέθοδοι ανάπτυξης συστημάτων IDP, ενώ προτείνεται και αναλύεται η μέθοδος ανάπτυξης με χρήση τεχνικών τοπολογικής ανάλυσης αδυναμιών. Τέλος, προτείνονται και αναλύονται εκτενώς οι απαιτήσεις ενός συστήματος αντιμετώπισης περιστατικών που βασίζεται στα παραπάνω.

4.1. Εισαγωγή

Η *αποτίμηση αδυναμιών ασφάλειας (Vulnerability Assessment – VA)* και η *ανίχνευση/αντιμετώπιση παρεισφρήσεων (Intrusion Detection and Prevention – IDP)* είναι ευρέως καθιερωμένες πρακτικές στη βιομηχανία ασφάλειας και αποτελούν ένα ζωτικής σημασίας τμήμα στα περισσότερα σύγχρονα σχέδια και πρότυπα ασφάλειας (ISO/IEC JTC1, 2005), (PCI SSC, 2008). Εν τούτοις, αυτές οι δύο πρακτικές ερευνήθηκαν και αναπτύχθηκαν παράλληλα με αποτέλεσμα να μην υπάρχει επίσημο μέσο συσχετισμού της γνώσης που παράγεται, διατήρηση της γνώσης αυτής, καθώς επίσης και δυνατότητα σύγκρισης των πληροφοριών αυτών με σενάρια επιθέσεων σε πραγματικές συνθήκες (Noel, 2009).

Σε αυτό το κεφάλαιο, εξετάζονται εκ νέου οι σχέσεις μεταξύ των *αδυναμιών ασφάλειας (vulnerabilities)*, των *(αθέμιτων) εκμεταλλεύσεων (exploits)* και των *υπογραφών ανίχνευσης παρεισφρήσεων (IDP signatures)*, αναλύοντας και συσχετίζοντας τις πληροφορίες που εμπεριέχονται σε αυτές με σκοπό την παραγωγή γνώσης και ευφυΐας ασφάλειας πληροφοριών. Οι σχέσεις αυτές εξετάζονται στο πλαίσιο της ερευνητικής περιοχής της Τοπολογικής Ανάλυσης *Αδυναμιών* Ασφάλειας (Topological Vulnerability Analysis – TVA) (Jajodia, et. al., 2006), η οποία εξετάζει τα χαρακτηριστικά των *αδυναμιών* και των *εκμεταλλεύσεων* σε σχέση με το περιβάλλον στο οποίο βρίσκονται,

προτείνοντας την κατασκευή *μονοπατιών επίθεσης* που περιγράφουν αντίστοιχα πιθανά σενάρια.

Στόχος του κεφαλαίου αυτού είναι η ανάλυση των τοπολογικών χαρακτηριστικών των αδυναμιών ασφάλειας, η αποτίμηση της σημασίας για το συγκεκριμένο περιβάλλον στο οποίο ανακαλύπτονται, και η κατασκευή μονοπατιών (σεναρίων) επίθεσης, μέσω των συσχετίσεων των αδυναμιών με τμήματα κώδικα αθέμιτης εκμετάλλευσης και υπογραφών IDP. Το αποτέλεσμα της τοπολογικής ανάλυσης των αδυναμιών ασφάλειας είναι η κατηγοριοποίηση της σημαντικότητας των επιθέσεων που μπορεί –δυνητικά- να δεχθεί μία υπολογιστική και πληροφοριακή υποδομή καθώς και του συνόλου των πιθανών αντιμέτρων που θα αποτρέψουν ή θα ελαχιστοποιήσουν τις πιθανές ζημιές στη συγκεκριμένη υποδομή.

4.2. Τοπολογική ανάλυση αδυναμιών και αντιμετώπιση περιστατικών ασφάλειας

Τόσο στη βιομηχανία ασφάλειας όσο και στην ερευνητική κοινότητα χρησιμοποιείται ένα μεγάλο πλήθος εργαλείων που ελέγχουν ένα δίκτυο για γνωστές αδυναμίες. Σχεδόν το σύνολο των εργαλείων αυτών εξετάζουν κάθε μια αδυναμία ξεχωριστά, χωρίς να ελέγχουν τις μεταξύ τους σχέσεις, κυρίως λόγω της πολύπλοκης διασύνδεσης των δικτύων, των μηχανισμών ελέγχου της δικτυακής κυκλοφορίας αλλά και της ανεξαρτησίας των αδυναμιών ασφάλειας (Jajodia, et. al., 2006). Έτσι, ενώ μια ομάδα από αδυναμίες μπορεί να εμφανίζει χαρακτηριστικά που δεν εγκυμονούν μεγάλο κίνδυνο, ένας συγκεκριμένος συνδυασμός τους μπορεί να επιτρέψει στους επιτιθέμενους να προκαλέσουν μεγάλης έκτασης ζημιά.

Από την άλλη πλευρά, ο συνδυασμός μιας ομάδας αδυναμιών προϋποθέτει την ύπαρξη κώδικα αθέμιτης εκμετάλλευσης για κάποιες από τις αδυναμίες αυτές. Κάνοντας χρήση αυτού του κώδικα, ο επιτιθέμενος μπορεί να εκμεταλλευτεί τις αδυναμίες σε διαφορετικά συστήματα (μονοπάτι επίθεσης) ώστε να επιτύχει το στόχο της επίθεσής του. (O' Hare, Noel and Prole, 2008).

Σε αντίθεση με τις παραδοσιακές τεχνικές και τα συστήματα που στοχεύουν στην πρόληψη από τις συνέπειες μιας επίθεσης, η αντιμετώπιση περιστατικών στοχεύει στην ελαχιστοποίηση του αντίκτυπου μιας επίθεσης. Κάτι τέτοιο μπορεί να επιτευχθεί με πλήρη γνώση των πιθανών μονοπατιών επίθεσης ενός δικτύου. Ενώ οι ανθρώπινες ενέργειες (βλ. Κεφάλαιο 3) βοηθούν σημαντικά στη διαδικασία της αντιμετώπισης περιστατικών, είναι εξαιρετικά ωφέλιμη η χρήση αυτοματοποιημένων εργαλείων που παρέχουν τη δυνατότητα πλήρους ανάλυσης και αναπαράστασης των μονοπατιών επίθεσης, για την παραγωγή αντίστοιχων μονοπατιών αντιμετώπισης (Jajodia and Noel, 2007). Η προσέγγιση αυτή ονομάζεται Τοπολογική Ανάλυση Αδυναμιών και στοχεύει στη μοντελοποίηση της κατάστασης των συστημάτων ενός δικτύου (αδυναμίες) και των πιθανών εκμεταλλεύσεων, έτσι ώστε να παράγει όλα τα πιθανά σενάρια με τα οποία ένας επιτιθέμενος μπορεί να εκμεταλλευτεί το δίκτυο. Ένα σύστημα Τοπολογικής Ανάλυσης Αδυναμιών μετατρέπει διάφορα δεδομένα ασφάλειας (π.χ. εργαλεία αποτίμησης αδυναμιών ασφάλειας, συστήματα ανίχνευσης παρεισφρήσεων, διάσπαρτες πληροφορίες από το Διαδίκτυο) ώστε να παρέχει πλήρη κατανόηση του πώς οι μεμονωμένες και οι συνδυασμένες αδυναμίες ασφάλειας επηρεάζουν τη συνολική ασφάλεια του δικτύου, καθώς και τις τεχνικές ενέργειες που απαιτούνται για την αντιμετώπισή τους.

4.3. Απαιτούμενες πληροφορίες ασφάλειας στην τοπολογική ανάλυση αδυναμιών

Ο όρος *αδυναμία ασφάλειας (vulnerability)* χρησιμοποιείται για να περιγράψει μία ατέλεια ή ευπάθεια σε ένα σύστημα (είτε στο *λογισμικό*, είτε στο *υλισμικό*, είτε στο *υλικολογισμικό (firmware))*, η οποία επιτρέπει σε έναν επιτιθέμενο να διακυβεύσει την *ακεραιότητα*, την *εμπιστευτικότητα*, τον *έλεγχο πρόσβασης*, τη *διαθεσιμότητα*, ή τους *μηχανισμούς ελέγχου* του συστήματος, στο λειτουργικό του σύστημα, στις εφαρμογές που αυτό φιλοξενεί, καθώς επίσης και στα δεδομένα που διαχειρίζεται.

Ένας εναλλακτικός, περισσότερο επίσημος, ορισμός περιγράφει την *αδυναμία* ως την έλλειψη μέτρων προστασίας και ασφάλειας σε ένα σύστημα, καθώς και την έκθεση του συστήματος σε κίνδυνο (Chambers, 2006). Αν και υπάρχουν πολλά κριτήρια που αποφασίζουν και υπολογίζουν τη σημασία και το μέγεθος μιας *αδυναμίας*, όπως εκείνα

που περιγράφονται στο (Hansman & Hunt, 2005) και στο (Kim, et.al, 2008), η πραγματική σημασία κάθε *αδυναμίας* μπορεί να αξιολογηθεί μόνο μέσα στο ευρύτερο πλαίσιο, δηλαδή το ιδιαίτερο πληροφοριακό περιβάλλον μέσα στο οποίο ανακαλύπτεται[13].

Για παράδειγμα, ένα σύστημα που προσφέρει τις υπηρεσίες *Hyper Text Transfer Protocol - HTTP (RFC 2316), File Transfer Protocol – FTP (RFC 959)* και *Simple Mail Transfer Protocol –SMTP (RFC 821)* μπορεί να έχει διάφορες *αδυναμίες* -στα αντίστοιχα πρωτόκολλα- οι οποίες μπορεί να επιτρέψουν την απομακρυσμένη εκτέλεση αθέμιτου κώδικα και να διακυβεύσουν μία από τις ιδιότητες ασφάλειας που προαναφέρθηκαν. Όταν το ίδιο ακριβώς σύστημα είναι δικτυακά απομονωμένο και ένα τείχος προστασίας απαγορεύει την κυκλοφορία για τις υπηρεσίες SMTP και FTP, ενώ επιτρέπει την κυκλοφορία της *HTTP*, τότε οι *αδυναμίες* που υπάρχουν στις υπηρεσίες *SMTP* και *FTP* έχουν εξ ολοκλήρου διαφορετική σημασία ασφάλειας. Η ύπαρξη του μηχανισμού αυτού (τείχος προστασίας) επιτρέπει να υποθέσουμε, χωρίς βλάβη της γενικότητας, πως οι αδυναμίες που υπάρχουν στις υπηρεσίες *SMTP* και *FTP* δεν μπορούν να τύχουν αθέμιτης εκμετάλλευσης από έναν απομακρυσμένο επιτιθέμενο, μιας και δεν επιτρέπεται η δικτυακή κυκλοφορία στα συγκεκριμένα πρωτόκολλα. Παρ' όλα αυτά, οι αδυναμίες (στις υπηρεσίες SMTP & FTP) εξακολουθούν να υπάρχουν και μπορεί να οδηγήσουν σε διακύβευση των ιδιοτήτων ασφάλειας αν τύχουν τοπικής εκμετάλλευσης, από μια διαδρομή στην οποία δεν παρεμβάλλεται μηχανισμός ασφάλειας (π.χ. όταν ο επιτιθέμενος βρίσκεται στο ίδιο τοπικό δίκτυο με το σύστημα).

Η συστηματική εξέταση ενός συστήματος για τον προσδιορισμό των υποδομών ή των σχετικών στοιχείων του συστήματος που βρίσκονται σε κίνδυνο λόγω ύπαρξης *αδυναμιών* ασφάλειας, καθώς και ο προσδιορισμός των καταλλήλων διαδικασιών που μπορούν να εφαρμοστούν για να μειώσουν αυτό το επίπεδο κινδύνου, είναι γνωστή ως *αποτίμηση αδυναμιών ασφάλειας (vulnerability assessment - VA)*. Με απλά λόγια, η *αποτίμηση αδυναμιών ασφάλειας* είναι η διαδικασία μέσω της οποίας ανακαλύπτονται και

---

[13] Απλούστερα, αν υπάρχουν –ή όχι- πολιτικές ασφάλειας που κάνουν την *εκμετάλλευση* της συγκεκριμένης αδυναμίας περισσότερο (ή λιγότερο) πολύπλοκη.

(πολλές φορές αντιμετωπίζονται) οι *αδυναμίες* ασφάλειας στο λειτουργικό σύστημα, στο δίκτυο και στις εφαρμογές μιας δεδομένης υποδομής.

Το εύρος και η σημασία μιας *αδυναμίας* μπορεί να γίνουν πλήρως κατανοητά μόνο όταν λαμβάνεται υπόψη το ευρύτερο περιβάλλον στο οποίο ανακαλύπτεται η συγκεκριμένη *αδυναμία*, καθώς η ύπαρξη μηχανισμών ασφάλειας μπορεί να κάνει την *εκμετάλλευσή* της περισσότερο (ή λιγότερο) πολύπλοκη. Από την άλλη πλευρά, έχει ιδιαίτερη σημασία να εξεταστεί η ύπαρξη κώδικα που μπορεί να εκμεταλλευτεί τη συγκεκριμένη *αδυναμία* και να αναλυθούν οι πολιτικές που εφαρμόζονται από τα αντίμετρα ασφάλειας.

Ένα *μονοπάτι επίθεσης (attack path)* ορίζεται ως η *εκμετάλλευση* μιας ή περισσοτέρων *αδυναμιών* με προκαθορισμένη σειρά, δηλαδή η διαδρομή που ακολουθεί ένας επιτιθέμενος προκειμένου να επιτύχει υψηλού επιπέδου στόχους (βλ. ενότητα 2.4.1) χρησιμοποιώντας χαμηλού επιπέδου τεχνικές (βλ. ενότητα 2.1). Οι σύγχρονες απειλές ασφάλειας, όπως οι συνδυασμένες επιθέσεις (blended attacks) εκμεταλλεύονται - με μια προκαθορισμένη σειρά- ένα συνδυασμό δύο, τριών ή ίσως και περισσοτέρων *αδυναμιών* που μπορεί να υπάρχουν σε ένα δικτυωμένο περιβάλλον (Chien & Szor, 2002), (Conklin, 2008).

Η πλειονότητα των εργαλείων *αυτόματης αποτίμησης αδυναμιών* στερείται της δυνατότητας να εξετάζει την αλληλεξάρτηση μιας σειράς *αδυναμιών*, να παραπέμπει γνωστές *αδυναμίες* σε αντίστοιχο κώδικα αθέμιτης *εκμετάλλευσης* καθώς και να παρέχει αντίστοιχες πολιτικές επίβλεψης και αντιμετώπισης (Debar, et. al, 2007). Όπως αναφέρθηκε στο Κεφάλαιο 3, αυτά τα χαρακτηριστικά αποτελούν γνωρίσματα της Αντιμετώπισης Περιστατικών, μιας διαδικασίας που υλοποιείται από ένα ευρύ σύνολο ανθρώπινων διαδικασιών.

Από την άλλη πλευρά, η έννοια του κώδικα αθέμιτης *εκμετάλλευσης* (καθώς και τα διάφορα μοτίβα ή παραλλαγές του κώδικα αυτού) είναι γνωστή στα *Συστήματα Ανίχνευσης και Αποτροπής Αντιμετώπισης Παρεισφρήσεων (Intrusion Detection and Prevention - IDP)*, τα οποία χρησιμοποιούν *υπογραφές*. Οι *υπογραφές* καταπολεμούν

γνωστές [14] επιθέσεις με τη χρήση στατιστικής (statistical) ή/και συμπεριφορικής (behavioral) ανάλυσης. Τα συστήματα έχουν εξελιχθεί με τέτοιον τρόπο ώστε να μπορούν να ανιχνεύσουν και παραλλαγές των γνωστών-επιθέσεων (που καλούνται, επίσης, άγνωστες επιθέσεις στη βιομηχανία ασφάλειας).

Στις περισσότερες περιπτώσεις, μια *υπογραφή IDP* περιλαμβάνει το ακριβές κομμάτι του κώδικα αθέμιτης *εκμετάλλευσης*, ή ένα μοτίβο/παραλλαγή του κώδικα αυτού. Το ωφέλιμο φορτίο κάθε μεταφερόμενου δικτυακού πακέτου (ή μια σύνοψη (hash) από αυτό) συγκρίνεται με το σύνολο κάθε υπογραφής (ή σύνοψη αυτής) που έχει καθορίσει η αντίστοιχη πολιτική IDP, στο τμήμα του δικτύου όπου εφαρμόζεται η αντίστοιχη υπογραφή.

Όταν επιτυγχάνεται ένα καθορισμένο όριο ομοιότητας, τότε, είτε προκαλείται ένας συναγερμός που ειδοποιεί τους διαχειριστές των συστημάτων για την ύπαρξη αυτού του γεγονότος, είτε λαμβάνουν χώρα άλλες ενέργειες που καθορίζει η πολιτική (π.χ. διακοπή σύνδεσης, αναδρομολόγηση δικτυακής κυκλοφορίας, κτλ.). Χρησιμοποιώντας αυτές τις τεχνικές, τα συστήματα IDP μπορούν να ανιχνεύουν τις παραβιάσεις της πολιτικής ασφάλειας ενός συστήματος (Srilatha, Ajith, & Johnson, 2004). Επιπλέον, τα συστήματα IDP μπορούν να επαληθεύουν, να αναλύουν και να χαρακτηρίζουν τις απειλές τόσο στην περίμετρο όσο και στο εσωτερικό ενός εταιρικού δικτύου, εξυπηρετώντας τη διαδικασία λήψης αποφάσεων για τον επιμερισμό των πόρων ασφάλειας των υπολογιστών (Scarfone & Mell, 2008).

Εν τούτοις, τα συστήματα IDP υποφέρουν από μεγάλες αναλογίες θετικών σφαλμάτων (false positives) ως αποτέλεσμα μη-αποδοτικής πολιτικής (Pietraszek, 2004), (Mitropoulos, Patsos and Douligeris, 2007), (Tian et. al, 2008). Το γεγονός αυτό μπορεί – σταδιακά- να απαξιώσει τη σημασία της πλεονάζουσας πληροφορίας που παράγεται από τα συστήματα αυτά (η πλεονάζουσα πληροφορία καλείται και «θόρυβος ασφάλειας», (Aberdeen Group, 2003)). Προκειμένου να ελαχιστοποιείται το φαινόμενο του θορύβου ασφάλειας και να αυξάνεται η αποτελεσματικότητα της πολιτικής των συστημάτων,

[14] Στον κατασκευαστή του συγκεκριμένου συστήματος.

απαιτούνται συνεχείς –χειρωνακτικές- διαδικασίες επαναξιολόγησης της πολιτικής ασφάλειας που εφαρμόζεται (ήτοι των ενεργοποιημένων *υπογραφών*) και τακτική παραμετροποίηση των συστημάτων.

Η κύρια αιτία για τις μεγάλες αναλογίες θετικών σφαλμάτων και τη μη-αποτελεσματική πολιτική οφείλεται στο κενό μεταξύ του αυτόματου και ταυτόχρονου προσδιορισμού για την ύπαρξη μιας *αδυναμίας*, της εύρεσης του αντίστοιχου κώδικα (αθέμιτης) *εκμετάλλευσης* και της επιλογής των κατάλληλων *υπογραφών* αντιμετώπισής τους. Ο στόχος της ελαχιστοποίησης ή εξάλειψης αυτού του κενού ορίζεται στην ερευνητική κοινότητα ως *αυτοματοποιημένη αντιμετώπιση παρεισφρήσεων (automated intrusion response)* (Newsome & Song, 2005), (Brumley, et.al., 2006), (Cui, Peinado, Wang, & Locasto, 2007).

4.3.1. Καθορισμός πληροφοριών για *αδυναμίες* ασφάλειας

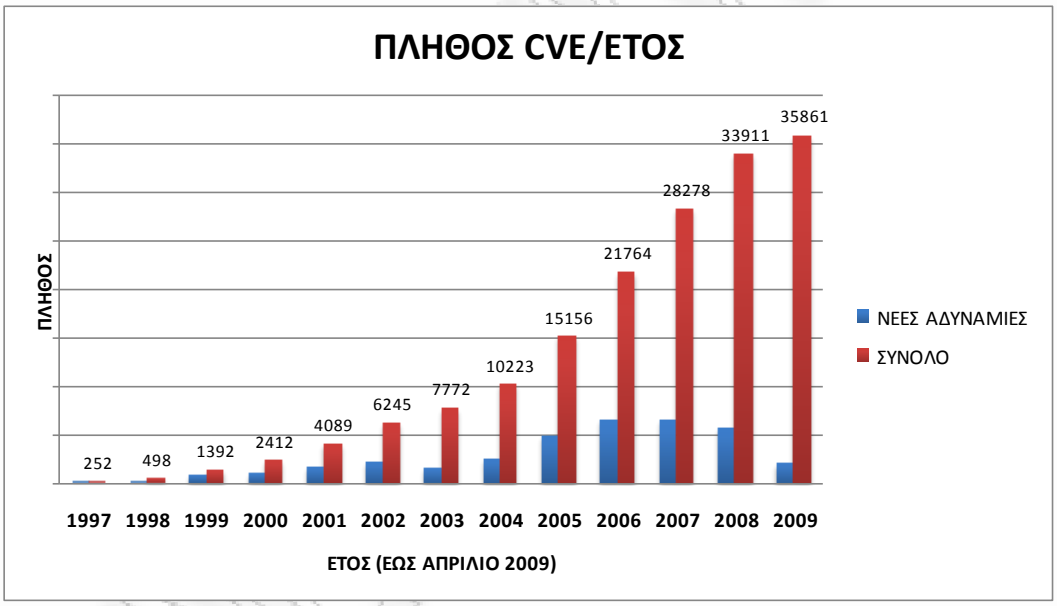
Η διεθνής ερευνητική βιβλιογραφία περιλαμβάνει αρκετές χαρακτηριστικές προσπάθειες μοντέλων ταξινόμησης των *αδυναμιών*, όπως στο (Killourhy, 2004) και (Hansman & Hunt, 2005), αλλά –μέχρι και σήμερα- δεν υπάρχει καμία επίσημη ή τυποποιημένη μέθοδος. Επιπλέον, η διεθνής κοινότητα δεν έχει καθορίσει μια τυποποιημένη γλώσσα με την οποία θα περιγράφεται η σημασιολογία της κάθε *αδυναμίας*, αν και προς αυτήν την κατεύθυνση υπάρχουν ιδιαίτερα ενδιαφέρουσες προσεγγίσεις, όπως αναφέρονται στα (Jajodia, Noel, & O'Berry, 2006), (Yegneswaran, et. al., 2005), (Brumley, et. al, 2006), (Brumley et. al., 2007), κτλ.

Από την άλλη πλευρά, στη βιομηχανία ασφάλειας χρησιμοποιείται ένα μεγάλο σύνολο καταλόγων αναφοράς και περιγραφής *αδυναμιών* από διάφορες εταιρείες, οργανισμούς ή ερευνητικά ιδρύματα. Στους καταλόγους αυτούς ανήκει ο CERT Advisories του CERT/CC στο Πανεπιστήμιο Carnegie Mellon των ΗΠΑ (US-CERT, 2009), ο κατάλογος CVE του κυβερνητικού οργανισμού Mitre (MITRE, 2009), η λίστα *αδυναμιών* που διατηρείται από το δικτυακό τόπο Security Focus (SecurityFocus, 2009), η λίστα Bugtraq (BugTraq, 2009), ενώ σημαντικοί κατασκευαστές -όπως η Microsoft, η Cisco, η IBM και άλλοι- διατηρούν δημοσιευμένους καταλόγους που περιγράφουν τις

αδυναμίες των προϊόντων που κατασκευάζουν στους αντίστοιχους ιστοτόπους (Microsoft, 2009), (Cisco, 2009).

Επιπλέον, διάφορες ομάδες αντιμετώπισης περιστατικών και κέντρα ανάλυσης σε ολόκληρο τον κόσμο διατηρούν και δημοσιεύουν πληροφορίες *αδυναμιών* με το δικό τους τρόπο, όπως π.χ. το γιαπωνέζικο Japan Computer Emergency Response Team Coordination Center (JPCERT, 2009)), το ελληνικό GRNET-CERT (ΕΔΕΤ, 2009), κτλ.

Τέλος, τα περισσότερα ανοικτού κώδικα και εμπορικά εργαλεία VA, όπως το Nessus (Tenable, 2009), το Foundstone (McAfee, 2009), και το ISS (IBM, 2009) είτε παρέχουν κάποιο είδος ιδιόκτητης περιγραφής *αδυναμιών*, είτε παραπέμπουν σε κάποιους από τους προαναφερθέντες καταλόγους.

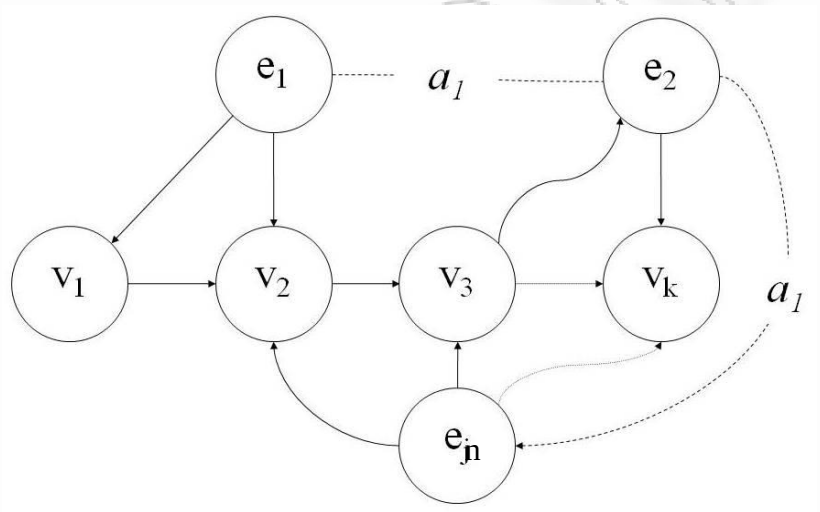


Εικόνα 4-1: Πλήθος δημοσιευμένων αδυναμιών κατά CVE (ανά έτος) (Πηγή: Πανεπιστήμιο Purdue)

Εφεξής, και για τους σκοπούς της συγκεκριμένης διατριβής, ο κατάλογος αναφοράς CVE της Mitre Corporation χρησιμοποιείται ως ένα de facto πρότυπο, ακολουθώντας την αποδοχή που έχει κερδίσει από τη διεθνή ερευνητική κοινότητα και τη βιομηχανία ασφάλειας στη διάρκεια των τελευταίων ετών (βλ. Εικόνα 4-1).

Ένας κώδικας αθέμιτης *εκμετάλλευσης* (exploit, ή *εκμετάλλευση* για την απλούστευση των ορισμών) είναι ένα κομμάτι κώδικα που εκμεταλλεύεται την ύπαρξη μιας συγκεκριμένης *αδυναμίας*. Ένα *μονοπάτι επίθεσης (attack path)* είναι μια σειρά διαδοχικών τέτοιων τμημάτων κώδικα που επιτρέπει σε έναν επιτιθέμενο να επιτύχει τους στόχους του.

Ένα μονοπάτι επίθεσης a_i ορίζεται, τυπικά, ως η μοναδική ακολουθία επιτυχών *εκμεταλλεύσεων*, ήτοι $a_i = \{(e_l|v_m), \ldots,(e_j|v_k)\}$, $\forall\, a \in A, \forall\, e \in E, \forall\, v \in V, i, j, k, l, m, n \in N$, όπου A είναι το σύνολο των μονοπατιών επιθέσεων a_i, E είναι το σύνολο των *εκμεταλλεύσεων* e_j και V είναι το σύνολο των *αδυναμιών* v_k, αντιστοίχως.



Σχήμα 4-1 - Ένα μονοπάτι επίθεσης a_i , σε σχέση με τις v_k και e_j

Κάθε *εκμετάλλευση* αντιστοιχεί σε μια ή περισσότερες *αδυναμίες* και μια *αδυναμία* μπορεί να υλοποιηθεί από περισσότερες της μιας *εκμετάλλευσης* (δηλαδή υπάρχει μια M-M σχέση μεταξύ των *αδυναμιών* και των *εκμεταλλεύσεων*[15]). Το Σχήμα 4-1 απεικονίζει ένα μονοπάτι επίθεσης, συμπεριλαμβάνοντας τις σχέσεις μεταξύ των *αδυναμιών* v_k και

[15] Υποθέτουμε ότι ένα *μονοπάτι επίθεσης* διαμορφώνεται μόνον όταν εκμεταλλεύονται (με επιτυχία) τις *αδυναμίες* με μια προκαθορισμένη σειρά. Χάριν απλότητας και χωρίς βλάβη της γενικότητας, μπορεί να υποτεθεί πως μια διαφορετική σειρά *εκμεταλλεύσεων* δεν οδηγεί στο ίδιο *μονοπάτι επίθεσης*, ενώ είναι πιθανό να μην οδηγεί καν σε *μονοπάτι επίθεσης*. Για την απόδειξη του παραπάνω ισχυρισμού, η οποία βρίσκεται πέρα από τους σκοπούς της συγκεκριμένης εργασίας, ο αναγνώστης παραπέμπεται στο (Ammann et. al, 2002).

εκμεταλλεύσεων e_j. Σε αυτό το παράδειγμα, η *αδυναμία* v_1 μπορεί να υλοποιηθεί από την *εκμετάλλευση* e_1, η *αδυναμία* v_2 από τις *εκμεταλλεύσεις* e_1 και e_n, η *αδυναμία* v_3 από τις *εκμεταλλεύσεις* e_2 και e_j, ενώ η *αδυναμία* v_k μπορεί να υλοποιηθεί από τις *εκμεταλλεύσεις* e_2 και e_n.

Επομένως, το *μονοπάτι επίθεσης* a_1 είναι η σειρά των *αδυναμιών* v_k που υλοποιήθηκαν από έναν επιτιθέμενο μέσω των *εκμεταλλεύσεων* e_j. Για περισσότερο περίπλοκα σενάρια επίθεσης, το παραπάνω γράφημα αναμένεται να είναι σημαντικά πιο συνεκτικό. Μια περισσότερο αναλυτική περιγραφή των *μονοπατιών ασφάλειας* αναφέρεται στο (Krasser, 2005).

4.3.2. Καθορισμός πληροφοριών για εκμεταλλεύσεις

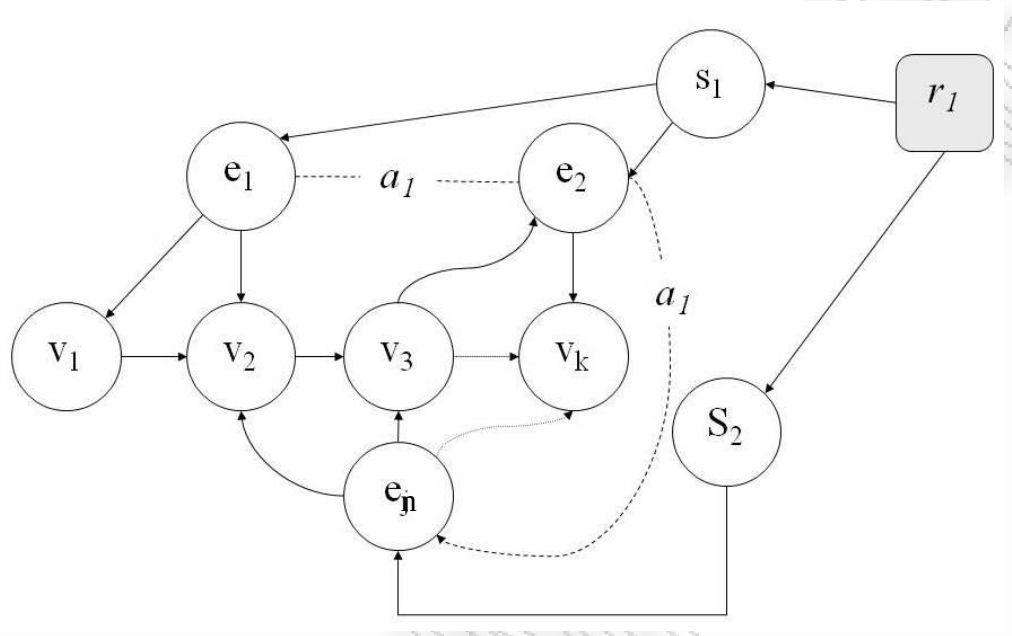
Πληροφορίες σχετικά με τις *εκμεταλλεύσεις* υπάρχουν σε ένα μεγάλο αριθμό ιστοχώρων που συντηρούνται από επιτιθέμενους (για αντίστοιχους σκοπούς) καθώς και σε συστήματα ασφάλειας, όπως οι *υπογραφές* στα συστήματα IDP.

Η τοπολογική ανάλυση μιας επίθεσης, μέσω της κατασκευής των αντίστοιχων *μονοπατιών επίθεσης* σε πραγματικό χρόνο, έχει ιδιαίτερη σημασία όταν μπορούν – επίσης δυναμικά- να κατασκευαστούν αντίστοιχα *μονοπάτια αντιμετώπισης (response paths)* που αντιμετωπίζουν αυτήν τη συγκεκριμένη επίθεση. Ένα *μονοπάτι αντιμετώπισης (response path)* περιέχει την κατάλληλη πολιτική (δηλαδή σύνολο ενεργών *υπογραφών s* στα συστήματα IDP) για την αντιμετώπιση της συγκεκριμένης επίθεσης. Τυπικά, οι υπογραφές s_1, s_2 που αντιμετωπίζουν τις εκμεταλλεύσεις e_1, e_2,...,e_j (άρα επιτυγχάνουν μη-υλοποίηση των *αδυναμιών* v_1, v_2, v_3,…,v_k) αποτελούν το *μονοπάτι αντιμετώπισης*, το οποίο απεικονίζεται σαν r_1 στο Σχήμα 4-2.

Το μονοπάτι αντιμετώπισης r_i που αντιστοιχεί στο *μονοπάτι επίθεσης* a_i, ορίζεται ως $r_i = \{ (e_k \mid s_k),..,(e_i \mid s_i), \forall r_i \in R, \forall a_i \in A, \forall s_i \in S, \forall i, k \in N$, όπου R το σύνολο των *μονοπατιών αντιμετώπισης* r_i *και S το σύνολο των υπογραφών* s_i.

Ο παραπάνω ισχυρισμός αναμένεται να παρέχει νέες δυνατότητες παραμετροποίησης στα συστήματα IDP, εφαρμόζοντας δυναμικές πολιτικές αντιμετώπισης *αδυναμιών* και

εκμεταλλεύσεων (υπό την έννοια ότι οι πολιτικές αυτές μπορούν να προσαρμόζονται κατάλληλα σε κάθε διαφορετικό *μονοπάτι επίθεσης*[16]).



Σχήμα 4-2 – Ένα ενδεικτικό μονοπάτι αντιμετώπισης

Στις παρακάτω ενότητες, ο παραπάνω ισχυρισμός αξιολογείται σε σχέση με την τρέχουσα κατάσταση στις επικρατέστερες προσεγγίσεις για την ανάπτυξη συστημάτων IDP σε εταιρικά περιβάλλοντα, αναλύοντας εκτενώς τους περιορισμούς κάθε μιας από αυτές.

Σημειώνεται πως η δημιουργία δυναμικών πολιτικών αντιμετώπισης περιστατικών που περιγράφεται στη συγκεκριμένη εργασία βασίζεται στην αυτόματη δημιουργία *μονοπατιών επίθεσης* (και αντίστοιχων *μονοπατιών αντιμετώπισης*) και όχι στην αυτόματη δημιουργία *υπογραφών*, όπως αυτή περιγράφεται στα (Newsome & Song, 2005), (Brumley, et.al., 2006), ή (Cui, Peinado, Wang, & Locasto, 2007), που θεωρείται μια διαφορετική ερευνητική περιοχή.

[16] δημιουργώντας το αντίστοιχο μονοπάτι αντιμετώπισης.

4.4. Τοπολογική ανάλυση αδυναμιών ασφάλειας και συστήματα IDP

Στις παρακάτω ενότητες, παρουσιάζεται μια ανάλυση των επικρατέστερων μεθοδολογιών ανάπτυξης συστημάτων IDP, ενώ αξιολογείται η επίδραση της τοπολογικής ανάλυσης αδυναμιών ασφάλειας στα πλαίσια της αντιμετώπισης περιστατικών.

4.4.1. Ανάπτυξη συστημάτων IDP με χρήση ζωνών ασφάλειας

Τα συστήματα IDP παραμετροποιούνται με κριτήριο τον προσδιορισμό της επιβλαβούς δραστηριότητας, σε συγκεκριμένα τμήματα δικτύων, εφαρμόζοντας πολιτικές (δηλαδή σύνολο υπογραφών) σε αντίστοιχους αισθητήρες (sensors). Ένας αισθητήρας εκτελεί μια συγκεκριμένη λειτουργία σε μια δικτυακή διεπαφή (κάρτα δικτύου, network interface card – NIC) ώστε όλη η κυκλοφορία σε ένα υποδίκτυο να ελέγχεται ως προς την ομοιότητά της με ένα σύνολο *υπογραφών* που απαρτίζουν την πολιτική του συγκεκριμένου αισθητήρα. Ο συγκεκριμένος τρόπος λειτουργίας απαιτεί την ύπαρξη ενεργού δικτυακού εξοπλισμού και συγκεκριμένα ενός μεταγωγέα (switch), στον οποίο ρυθμίζεται – με κατάλληλο τρόπο - μια συγκεκριμένη πόρτα (η οποία αποκαλείται και πόρτα επίβλεψης – span ή monitor port). Το Σχήμα 4-3 απεικονίζει μια γενική αρχιτεκτονική ανάπτυξης συστημάτων IDP σε ένα δίκτυο με τη χρήση αισθητήρων. Σε αυτό το σενάριο, ένα τείχος προστασίας διαιρεί το δίκτυο σε *x* λογικές διαφορετικές ζώνες ασφάλειας, ενώ απαιτούνται και *x* αισθητήρες IDP για να ελέγχουν πλήρως την κίνηση που διέρχεται από αυτές τις ζώνες. Με τον τρόπο αυτό, σε κάθε ζώνη αντιστοιχεί μια μόνο πολιτική ασφάλειας.

Η πολιτική ανίχνευσης και αποτροπής παρεισφρήσεων ενός αισθητήρα IDP (η οποία εφαρμόζεται σε ένα συγκεκριμένο υποδίκτυο-ζώνη σύμφωνα με το σχήμα Σχήμα 4-3) συνήθως επιλέγεται με κριτήριο τις επιθέσεις που είναι πιθανόν να εκτελεστούν στο λειτουργικό σύστημα και στο λογισμικό εφαρμογής που εκτελείται από τους σταθμούς που ανήκουν στη ζώνη αυτή (καθώς και στα ενεργά δικτυακά στοιχεία). Κατά συνέπεια και σύμφωνα με το σχήμα Σχήμα 4-3, στην ιδιαίτερη περίπτωση όπου υπάρχουν δύο

διαφορετικά συστήματα (σε ό,τι αφορά στα επίπεδα εφαρμογής και λειτουργικού συστήματος) στη ζώνη DMZ-1[17], η πολιτική του συστήματος IDP για τη ζώνη DMZ-1 περιλαμβάνει το σύνολο των *υπογραφών* που αντιμετωπίζουν όλους τους πιθανούς συνδυασμούς *αδυναμιών* των συγκεκριμένων σταθμών σε επίπεδο λειτουργικού συστήματος και λογισμικού εφαρμογής.

Γενικά, με δεδομένο ότι σε κάθε έναν (από τους *n* σε πλήθος) διαφορετικούς υπολογιστές μπορεί να εκτελείται μόνο ένα (από τα *j* σε πλήθος) λειτουργικά συστήματα και από 0 έως *p* (σε πλήθος) εφαρμογές ($n, j, p \in \mathrm{N}$), η πολιτική ανίχνευσης και αποτροπής παρεισφρήσεων ενός αισθητήρα IDP σε μια ζώνη απαιτεί τη χρήση του συνόλου των *υπογραφών* s_1 που απαιτούνται για τις παραπάνω υπογραφές και εκφράζεται από τον παρακάτω τύπο:

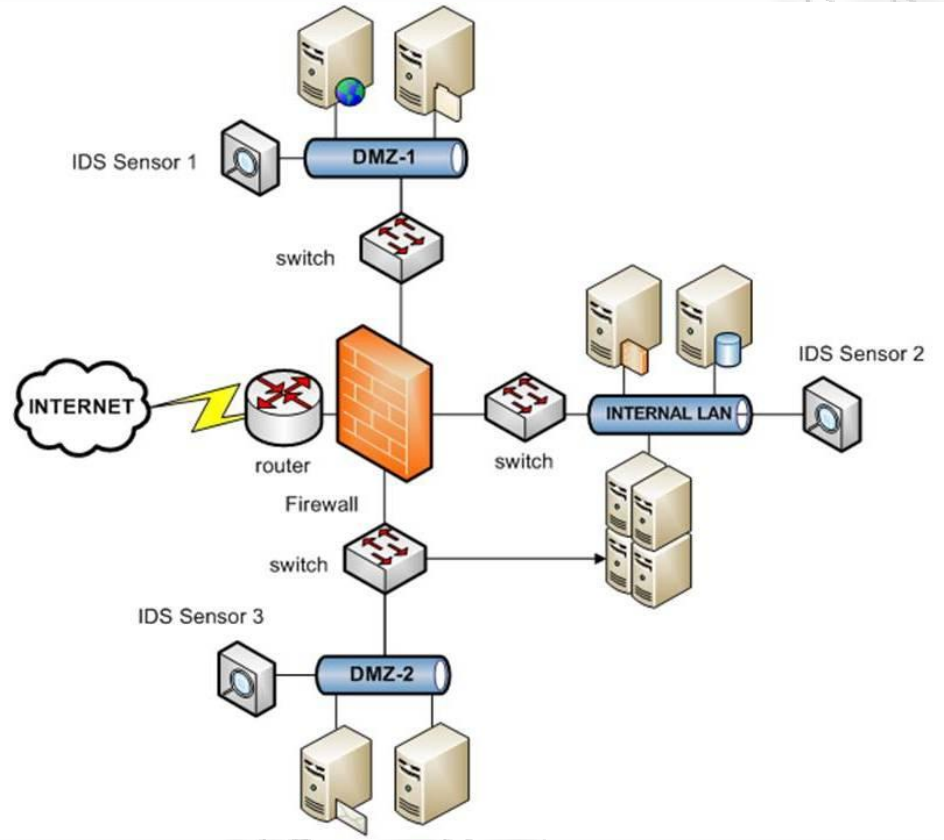
$$s_1 = \sum_{j=1}^{n} s(j) + \sum_{p=1}^{n} s(p)$$

Με άλλα λόγια, στο συγκεκριμένο σενάριο παραμετροποίησης δεν πραγματοποιείται κάποια ανάλυση του περιβάλλοντος σχετικά με τις απαιτήσεις ασφάλειας, αλλά ενεργοποιούνται οι υπογραφές για όλες τις πιθανές αδυναμίες των λειτουργικών συστημάτων και εφαρμογών στους σταθμούς του συγκεκριμένου υποδικτύου (ζώνη DMZ-1). Το γεγονός αυτό εισάγει μια σειρά ζητημάτων, τα οποία αναλύονται συνοπτικά παρακάτω.

Το μεγάλο πλήθος ελέγχων που πραγματοποιείται για τη σύγκριση κάθε δικτυακού πακέτου με ένα μεγάλο πλήθος υπογραφών σε μια ζώνη του δικτύου εισάγει μεταβαλλόμενη καθυστέρηση στις απαντήσεις επιπέδου εφαρμογής. Ένας επιτιθέμενος μπορεί να ανιχνεύσει και να αποφύγει την παρουσία ενός αισθητήρα IDP κατευθύνοντας ένα μεγάλο όγκο μοτίβων επίθεσης προς όλα τα συστήματα που επιβλέπει ο

[17] Ο όρος DMZ απαντάται στη βιβλιογραφία ως αποστρατικοποιημένη ζώνη (DeMilitarized Zone) και εκφράζει ένα φυσικό υποδίκτυο που προστατεύεται από ένα τείχος προστασίας, το οποίο διαχωρίζει και ελέγχει την κυκλοφορία από και προς το υπόλοιπο δίκτυο.

συγκεκριμένος αισθητήρας IDP και παρακολουθώντας πώς αυτά τα συστήματα αποκρίνονται[18].



Σχήμα 4-3 – Μια τυπική διάταξη συστημάτων και αισθητήρων IDP σε λογικές ζώνες ενός δικτύου

Σε ακραίες περιπτώσεις (π.χ. πολύ μεγάλο πλήθος ή μέγεθος πακέτων), οι πεπερασμένοι υπολογιστικοί πόροι του συστήματος IDP είναι αρκετά πιθανόν να εξαντληθούν. Όταν συμβεί αυτό, το σύστημα IDP αδυνατεί να ελέγξει τη δικτυακή κυκλοφορία, γεγονός που

[18] Η ύπαρξη διαφορετικών χρόνων απάντησης (π.χ. μέσω των εντολών `echo request/echo reply`) μαρτυρά την ύπαρξη ενός μηχανισμού ασφάλειας που ελέγχει κάθε διακινούμενο πακέτο στο συγκεκριμένο υποδίκτυο. Αυτό το έργο εκτελείται πιο εύκολα σε περιπτώσεις όπου ένας αισθητήρας IDP επιβλέπει τη δικτυακή κυκλοφορία για ένα μεγάλο σύνολο διαφορετικών συστημάτων (π.χ. εταιρικοί σταθμοί εργασίας).

οδηγεί (ανάλογα με τις δυνατότητες και τις ρυθμίσεις του συστήματος IDP) σε δύο διαφορετικές εκδοχές:

- Να επιτρέπεται η διέλευση της δικτυακής κυκλοφορίας χωρίς έλεγχο από το σύστημα IDP (ανοικτή αποτυχία – fail open),
- Να εμποδίζεται όλη η δικτυακή κυκλοφορία, εφόσον δεν ελέγχεται από το σύστημα IDP (κλειστή αποτυχία – fail closed).

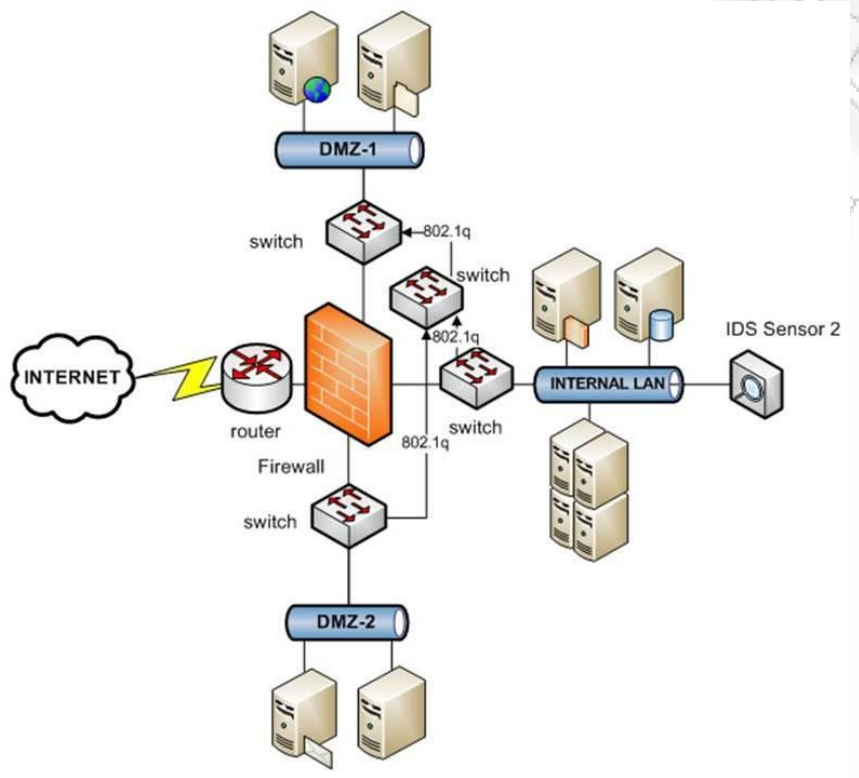
Στο σενάριο ανοικτής αποτυχίας, ο επιτιθέμενος μπορεί να εκμεταλλευτεί *αδυναμίες* στο σύστημα του ενδιαφέροντός του, ενώ στο σενάριο κλειστής αποτυχίας έχει προκαλέσει μια επίθεση άρνηση-εξυπηρέτησης (DoS) τόσο στο σύστημα IDP όσο και στο (υπο)δίκτυο που επιβλέπει το συγκεκριμένο σύστημα.

4.4.2. Ανάπτυξη συστημάτων IDP με χρήση ιδεατών τοπικών δικτύων

Μια εναλλακτική προσέγγιση που χρησιμοποιείται από περισσότερο σύγχρονα συστήματα IDP, είναι η χρήση του πρωτοκόλλου 802.1q (IEEE, 2003), το οποίο επιτρέπει τη χρήση ιδεατών τοπικών δικτύων (Virtual Local Area Network – VLAN). Η χρήση της τεχνικής αυτής επιτρέπει την κατασκευή και επίβλεψη πολλαπλών λογικών υποδικτύων (ζωνών) από έναν και μόνο αισθητήρα IDP που εκτελείται σε μια μόνο φυσική δικτυακή διεπαφή. Το πλήθος των υποδικτύων που μπορούν να επιβλέπονται από έναν τέτοιο αισθητήρα, όταν χρησιμοποιείται η συγκεκριμένη τεχνική, περιορίζεται μόνο από τις υπολογιστικές δυνατότητες του συστήματος IDP (οι οποίες εξαρτώνται από τον επεξεργαστή και τη μνήμη του συστήματος).

Το Σχήμα 4-4 απεικονίζει μία ανάπτυξη συστημάτων IDP με τη χρήση του πρωτοκόλλου 802.1q. Μια εμφανής και ορατή διαφορά με την προηγούμενη προσέγγιση είναι πως και οι τρεις ζώνες (DMZ-1, DMZ-2 και internal LAN) επιβλέπονται πλέον από έναν μόνο αισθητήρα, αντί τριών (έναν για κάθε ζώνη) που απαιτούνταν στα προηγούμενα (βλ. Σχήμα 4-2). Η επεκτασιμότητα και η αποδοτικότητα της

συγκεκριμένης προσέγγισης είναι μεγαλύτερη, ιδιαίτερα για ένα μεγάλο πλήθος από ζώνες και σταθμούς δικτύου.



Σχήμα 4-4 - Ανάπτυξη IDP συστημάτων σε ιδεατά τοπικά δίκτυα

Επίσης, η συγκεκριμένη προσέγγιση επιτρέπει μια περισσότερο ασφαλειο-κεντρική προσέγγιση, σε ό,τι αφορά στην ομαδοποίηση των συστημάτων που επιβλέπει το σύστημα IDP. Ο διαχωρισμός ενός δικτύου με τη χρήση VLAN παρέχει ιδιαίτερη ευελιξία ώστε να τοποθετούνται σε ένα συγκεκριμένο VLAN οι σταθμοί εκείνοι που έχουν ένα κοινό χαρακτηριστικό ασφάλειας (π.χ. παρόμοιες *αδυναμίες* ασφάλειας, παρόμοιο λειτουργικό σύστημα ή λογισμικό εφαρμογής, κτλ.), ενώ η βιομηχανία παρέχει σήμερα συστήματα που μπορούν να εφαρμόζουν και διαφορετικές πολιτικές ανά VLAN, επιτρέποντας ακόμη μεγαλύτερη ευελιξία στη συγκεκριμένη μέθοδο.

Επιπλέον, η χρήση του πρωτοκόλλου 802.1q επιτρέπει τη λειτουργία του συστήματος IDP με τελείως «διάφανο» τρόπο (ήτοι χωρίς τη χρήση της διεύθυνσης IP) κάνοντας το συγκεκριμένο σύστημα αθέατο για έναν πιθανό επιτιθέμενο.

Τέλος, η συγκεκριμένη μέθοδος μπορεί να χρησιμοποιηθεί όταν το σύστημα IDP απαιτείται να ενεργεί σε συγκεκριμένες συνθήκες ασφάλειας (π.χ. επιθέσεις σε λειτουργίες του επιπέδου 2 του OSI 7498 (OSI/IEC, 1994), όπως εκείνες της εγκαθίδρυσης σύνδεσης και δρομολόγησης σε περιβάλλοντα που υπάρχει μεταγωγέας), εμποδίζοντας τη διέλευση της δικτυακής κυκλοφορίας για την οποία ισχύει η συγκεκριμένη συνθήκη.

Παρ' όλα αυτά, υπάρχει ένα πλήθος επιχειρημάτων που αποτρέπουν την καθολική αποδοχή της συγκεκριμένης προσέγγισης. Αρχικά, η προσέγγιση αυτή απαιτεί όπως όλα τα ενεργά συστατικά του δικτύου, καθώς και το ίδιο το σύστημα IDP, να υποστηρίζουν το πρωτόκολλο 802.1q, μια ικανή και αναγκαία συνθήκη που περιορίζει σημαντικά το πεδίο εφαρμογής της μεθόδου. Εκτός από το πρόσθετο κόστος για την αναβάθμιση της δικτυακής υποδομής, αρκετά συστήματα IDP εγκαθίστανται σε λειτουργικά συστήματα που δεν υποστηρίζουν το συγκεκριμένο πρωτόκολλο (όπως π.χ. τα Microsoft Windows και αρκετές παραλλαγές του δημοφιλούς λειτουργικού συστήματος Linux). Επιπλέον, λόγω της χρήσης του πρωτοκόλλου και από άλλες μη-σχετιζόμενες με την ασφάλεια επιχειρησιακές ανάγκες (π.χ. ποιότητα υπηρεσίας, διαχωρισμού συστημάτων, κτλ.), η μέθοδος είναι ιδιαίτερα ευάλωτη σε ατυχείς ή/και ηθελημένες δικτυακές αλλαγές που επιβάλλουν οι ανάγκες αυτές.

Όπως αναφέρθηκε και παραπάνω, η δυνατότητα εφαρμογής πολλαπλών πολιτικών σε μια δικτυακή διεπαφή (κάρτα δικτύου) ενός συστήματος IDP επιφέρει κατακόρυφη αύξηση της απαιτούμενης επεξεργαστικής ισχύος. Επιπροσθέτως, η συγκεκριμένη προσέγγιση είναι εκτεθειμένη σε επιθέσεις άρνησης εξυπηρέτησης, είτε λόγω υπερβολικών απαιτήσεων από την επεξεργαστική ισχύ του IDP, είτε όταν ενεργοποιείται η επιλογή της δρομολόγησης ανάμεσα σε VLANs, μια αρκετά συνηθισμένη περίπτωση για τη λειτουργία εφαρμογών πολλαπλών επιπέδων (multi tiered applications), είτε – τέλος- στην περίπτωση συνδυασμένων επιθέσεων (blended attack) (Cisco, 2008).

Τέλος, υπάρχει πάντοτε η περίπτωση ένας επιτιθέμενος να παρακάμψει το σύστημα IDP, εξαπολύοντας επίθεση στο μεταγωγέα δικτύου με τέτοιον τρόπο ώστε, ρυθμίζοντας κατάλληλα τη δρομολόγηση στα VLAN, ολόκληρη η κυκλοφορία της επίθεσης να μην ελέγχεται από το IDP (τεχνική του χαμηλότερου επιπέδου – layer below) (Gollmann, 1999).

Γενικά, με δεδομένο ότι σε κάθε έναν (από τους *n* σε πλήθος) διαφορετικούς υπολογιστές μπορεί να εκτελείται μόνο ένα (από *j* σε πλήθος) λειτουργικά συστήματα και από 0 έως *q* (σε πλήθος) εφαρμογές ($n, j, p \in \mathrm{N}$), η πολιτική (ανίχνευσης και αποτροπής παρεισφρήσεων) ενός αισθητήρα IDP σε *m* ζώνες (trunks) που απαρτίζουν ένα VLAN απαιτεί τη χρήση του συνόλου των *υπογραφών* s_2 που απαιτούνται για τους παραπάνω υπολογιστές και εκφράζεται από τον παρακάτω τύπο:

$$s_2 = \sum_{i=1}^{m} * \left(\sum_{j=1}^{n} s(j) + \sum_{p=1}^{n} s(p) \right)$$

4.4.3. Ανάπτυξη συστημάτων IDP με χρήση τεχνικών τοπολογικής ανάλυσης αδυναμιών

Παρακάτω παρουσιάζεται μια εναλλακτική προσέγγιση για την αποτελεσματικότερη παραμετροποίηση συστημάτων IDP, χρησιμοποιώντας πολιτικές βασισμένες σε *μονοπάτια αντιμετώπισης*, ήτοι εφαρμόζοντας μόνο τις υπογραφές που αντιμετωπίζουν συγκεκριμένα *μονοπάτια επίθεσης*. Η συγκεκριμένη προσέγγιση κερδίζει συνεχώς έδαφος μεταξύ της ερευνητικής κοινότητας και της βιομηχανίας ασφάλειας, όπως χαρακτηριστικά αναφέρεται στα (Patsos, Mitropoulos & Douligeris, 2007), (Miura-Ko & Bambos, 2007), (Gula, 2009), οι οποίοι προτείνουν τη χρήση ενός ελαχίστου συνόλου υπογραφών που –πρακτικά- αντιστοιχούν στις αδυναμίες των συστημάτων, για την αντιμετώπιση των αδυναμιών αυτών.

Η προσέγγιση για ανάπτυξη συστημάτων IDP με βάση την τοπολογική ανάλυση αδυναμιών εισάγει την έννοια ενός συστήματος αυτόματης δημιουργίας και εφαρμογής τέτοιων πολιτικών. Το σύστημα αυτό ορίζεται ως *Σύστημα Αντιμετώπισης Περιστατικών*

(Incident Response System – IRS), ενώ οι απαιτήσεις σχεδιασμού και οι λειτουργικών δυνατοτήτων του συστήματος περιγράφονται συνοπτικά στα επόμενα.

Το IRS, σαν σύστημα διαχείρισης πληροφοριών ασφάλειας, πρέπει να συλλέγει και συσχετίζει, σε πραγματικό χρόνο, πληροφορίες σχετικές με *αδυναμίες*, τον αντίστοιχο κώδικα αθέμιτης *εκμετάλλευσης* των *αδυναμιών* αυτών, καθώς και τις αντίστοιχες υπογραφές IDP που απαιτούνται για την αντιμετώπιση των αδυναμιών αυτών.

Πρωταρχικός σκοπός του συστήματος είναι η αυτόματη συσχέτιση των πληροφοριών αυτών και η εξαγωγή κατάλληλων συμπερασμάτων σχετικά με την αντιμετώπιση μιας συγκεκριμένης ακολουθίας *αδυναμιών (μονοπάτι επίθεσης)*. Επιπλέον, το σύστημα στοχεύει στην αύξηση της αποτελεσματικότητας των εργαλείων VA όσο και των συστημάτων IDP, μειώνοντας τις αναλογίες αρνητικών και θετικών σφαλμάτων (false negatives και false positives, αντίστοιχα).

Η λειτουργία του συστήματος απαιτεί την ενεργοποίηση υπογραφών IDP μόνο για το σύνολο των μονοπατιών επίθεσης που υπολογίζει το σύστημα. Ήτοι, το σύνολο των υπογραφών s_3 που απαιτείται για την αντιμετώπιση των q σε πλήθος μονοπατιών επίθεσης σε n το πλήθος υπολογιστές, στους οποίους εκτελείται μόνο ένα (από j το πλήθος) λειτουργικά συστήματα και από 0 έως p (σε πλήθος) εφαρμογές ($n, j, p \in \mathrm{N}$), εκφράζεται ως συνάρτηση των a_i με τον παρακάτω τύπο:

$$s_3 = \sum_{i=1}^{q} \mathrm{s}(a_i)$$

Επίσης, το σύστημα στοχεύει στο να παρέχει στα εμπλεκόμενα μέλη της Ομάδας Αντιμετώπισης Περιστατικών (βλ. Ενότητα 3.2.1) περισσότερο ακριβείς πληροφορίες σχετικά με το εύρος και τη σημασία μιας επίθεσης, ελαχιστοποιώντας το χρόνο για την ακριβή ανίχνευση και τον προσδιορισμό ενός περιστατικού (βλ. 3.3.2), επιταχύνοντας τις επόμενες φάσεις στη διαδικασία Αντιμετώπισης Περιστατικών. Οι πληροφορίες αυτές μειώνουν σημαντικά τον όγκο των στοιχείων που πρέπει να εξετάζονται από τους ειδικούς ανάλυσης ψηφιακών πειστηρίων (forensics), προκειμένου να οδηγηθούν ταχύτερα σε συγκεκριμένα συμπεράσματα (Adelstein, 2006). Τέλος, το σύστημα

συμβάλλει στην αυτόματη δημιουργία πολιτικών IDP και, έμμεσα, στην αυτόματη δημιουργία πολιτικών αντιμετώπισης περιστατικών ασφάλειας.

4.5. Απαιτήσεις συστημάτων διαχείρισης πληροφοριών ασφάλειας στην αντιμετώπιση περιστατικών

Στις παρακάτω ενότητες ορίζονται οι λειτουργικές απαιτήσεις ενός συστήματος αντιμετώπισης περιστατικών.

4.5.1. Ανοικτή αρχιτεκτονική και πρότυπα μορφότυπα πληροφοριών

Μία θεμελιώδης σχεδιαστική έννοια για κάθε παρόμοιο σύστημα είναι η χρήση ανοικτής αρχιτεκτονικής, ώστε αφενός να εξυπηρετείται η εξέλιξη του συστήματος και αφετέρου να μπορεί να υποστηρίζει επεξεργασία δεδομένων από ετερογενείς πηγές (π.χ. εργαλεία, πληροφορίες που βρίσκονται σε ιστοτόπους, μηνύματα ηλεκτρονικού ταχυδρομείου), κτλ.

Η έννοια της ανοικτής αρχιτεκτονικής δεν περιορίζεται μόνο στην πλατφόρμα ανάπτυξης και την επιλογή της γλώσσας προγραμματισμού, αλλά και στους μορφότυπους των πληροφοριών που διαχειρίζεται το συγκεκριμένο σύστημα, κάτι ιδιαίτερα σημαντικό στην αντιμετώπιση περιστατικών. Αρκετές φορές, τα περιστατικά ασφάλειας εξαπλώνονται μέσα σε δευτερόλεπτα και άρα είναι ιδιαίτερα σημαντικό για ένα σύστημα διαχείρισης πληροφοριών ασφάλειας να συλλέγει, να κανονικοποιεί και να συσχετίζει πληροφορίες σε –σχεδόν- πραγματικό χρόνο ώστε να εξάγονται στον ίδιο χρόνο συμπεράσματα που αφορούν στη σημασία, το εύρος και το μέγεθος ενός περιστατικού. Οι παράγοντες αυτοί καθορίζουν και τις ενέργειες που πραγματοποιούνται για την αντιμετώπισή του. Επιπλέον, όταν απαιτείται να εξαχθούν και να μεταδοθούν πληροφορίες εκτός του οργανισμού που χρησιμοποιεί το συγκεκριμένο σύστημα (π.χ. σε εξωτερικές ομάδες αντιμετώπισης περιστατικών, (βλ. ενότητα 3.2.1)), η διαδικασία αυτή θα πρέπει να στηρίζεται σε προτυποποιημένες δομές και μορφότυπους δεδομένων (ή και πρότυπα αναπαράστασης αυτών), ώστε να αποφεύγεται η λανθασμένη ερμηνεία τους.

4.5.2. Ενοποίηση με εργαλεία αποτίμησης αδυναμιών ασφάλειας και συστήματα ανίχνευσης και αποτροπής παρεισφρήσεων

Όπως αναφέρθηκε και στα παραπάνω, η αποτίμηση αδυναμιών ασφάλειας είναι η διαδικασία εύρεσης και αξιολόγησης πιθανών αδυναμιών στο λογισμικό, στο υλισμικό και στο υλικολογισμικό μιας πληροφοριακής υποδομής. Μέχρι και σήμερα, οι αδυναμίες ασφάλειας κατηγοριοποιούνται με βάση διάφορα σχήματα (λίστες) που έχουν προταθεί από την ερευνητική κοινότητα και τη βιομηχανία ασφάλειας, τα οποία περιγράφουν τα χαρακτηριστικά των αδυναμιών αυτών. Οι περισσότερο διαδεδομένες λίστες αδυναμιών είναι, μεταξύ άλλων, οι:

- Η λίστα Common Vulnerabilities and Exposures (CVE, http://cve.mitre.org), η οποία συντηρείται από τον Κυβερνητικό Οργανισμό Mitre των ΗΠΑ και χρησιμεύει ως ένα λεξικό των γνωστών (ήτοι καταγεγραμμένων) αδυναμιών ασφάλειας. Η συγκεκριμένη λίστα παρέχει ένα μοναδικό αναγνωριστικό (το οποίο είναι γνωστό, επίσης, ως όνομα CVE - CVE name, αριθμός CVE - CVE number, ή απλά CVE) το οποίο ταυτοποιεί με μοναδικό τρόπο μια καταγεγραμμένη αδυναμία ασφάλειας. Τα αναγνωριστικά CVE χρησιμοποιούνται τόσο από την ερευνητική και ακαδημαϊκή κοινότητα όσο και από τη βιομηχανία ασφάλειας ως μια πρότυπη μέθοδος για αναγνώριση αδυναμιών και συσχέτισή τους με άλλες λίστες περιγραφής τους.

- Η λίστα Bugtraq (http://www.securityfocus.com), η οποία είναι μια λίστα ηλεκτρονικού ταχυδρομείου αφιερωμένη στην ασφάλεια πληροφοριών. Περιλαμβάνει πληροφορίες και συζητήσεις σχετικά με αδυναμίες ασφάλειας, πληροφορίες από τους κατασκευαστές, μεθόδους εκμετάλλευσης των αδυναμιών καθώς και άλλες πληροφορίες. Σε κάθε αδυναμία ασφάλειας δίνεται ένα μοναδικό αναγνωριστικό (BugtraqID). Η Bugtraq είναι μια ευρέως διαδεδομένη λίστα, η οποία σήμερα συντηρείται από την εταιρεία Symantec.

- Η λίστα US-CERT του Υπουργείου Εσωτερικής Ασφάλειας των ΗΠΑ εκδίδει πληροφορίες για μια ευρεία γκάμα αδυναμιών (http://www.us-cert.gov), με βάση συγκεκριμένα κριτήρια σημαντικότητας που καθορίζει εκείνο.

Επίσης, οι διάφοροι κατασκευαστές υλισμικού και λογισμικού διατηρούν δικές τους λίστες περιγραφής αδυναμιών[19]. Τέλος, τα εργαλεία αποτίμησης αδυναμιών διατηρούν εσωτερικές λίστες περιγραφής και ταξινόμησης των αδυναμιών που ανακαλύπτουν ή παραπέμπουν σε μια από τις προαναφερθείσες λίστες.

Από την άλλη πλευρά, τα συστήματα IDP διατηρούν μια εσωτερική ταξινόμηση των υπογραφών που χρησιμοποιούν, οι οποίες –σε αρκετές περιπτώσεις- συσχετίζονται με τις παραπάνω λίστες. Για παράδειγμα, το πρότυπο σύστημα (IDP) Snort παραπέμπει στις λίστες CVE ή/και Bugtraq για ένα μεγάλο σύνολο υπογραφών του.

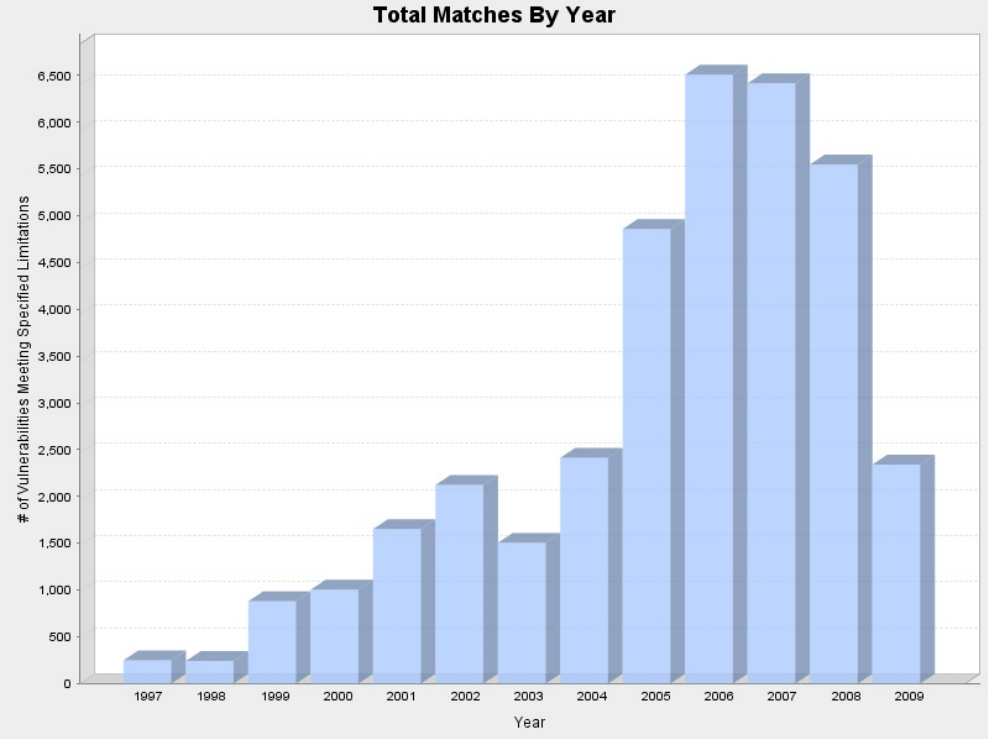
4.5.3. Βάση γνώσης

Οι μοντέρνες επιθέσεις αποτελούνται από την επιτυχή εκμετάλλευση μιας ή περισσοτέρων αδυναμιών ασφάλειας, ενώ οι επιτιθέμενοι εφευρίσκουν –σχεδόν-καθημερινά νέους τρόπους επιθέσεων, όπως δείχνει και η Εικόνα 4-2. Παράλληλα, η βιομηχανία ασφάλειας εκδίδει ανά τακτά χρονικά διαστήματα ενημερωτικά δελτία (γνωστά και ως advisories) που περιγράφουν την ύπαρξη νέων αδυναμιών και επιθέσεων.

Προκειμένου να μπορέσει να παράγει πληροφορίες που αφορούν στη διαχείριση της ασφάλειας της υποδομής που επιβλέπει, ένα σύστημα διαχείρισης πληροφοριών συλλέγει πρωτογενείς πληροφορίες ασφάλειας από πολλαπλές και ετερογενείς πηγές, τις οποίες επεξεργάζεται και αποθηκεύει σε βάσεις δεδομένων που διατηρεί, ώστε να κατασκευάζει μια βάση γνώσης για τις δημοσιευμένες αδυναμίες ασφάλειας, τις –κατά το δυνατόν περισσότερο- ακριβείς πληροφορίες που αφορούν σε εκμεταλλεύσεις (exploits) και τα δυνατά αντίμετρα (π.χ. υπογραφές συστημάτων IDP).

---

[19] Μία αναλυτική απαρίθμηση των διαθέσιμων λιστών αδυναμιών δίνεται στο Παράρτημα Α.



Εικόνα 4-2: Δημοσιευμένες αδυναμίες ασφάλειας ανά έτος (έως 5/2009) (Πηγή: National Vulnerability Database, NIST)

4.5.4. Ανανέωση πληροφοριών

Δύο σημαντικές παράμετροι στην επεξεργασία πληροφοριών ασφάλειας από ένα αντίστοιχο σύστημα αφορούν στην ακεραιότητα και την ακρίβεια των πληροφοριών που διαχειρίζεται το σύστημα.

Καθώς οι πληροφορίες ασφάλειας μεταβάλλονται στη διάρκεια του χρόνου (π.χ. χαρακτηριστικά αδυναμιών, πλήθος διαθέσιμων εκμεταλλεύσεων και υπογραφών από συστήματα IDP, κτλ.), το σύστημα πρέπει να ανανεώνει –σε τακτά χρονικά διαστήματα ή κατ' απαίτηση των διαχειριστών του- τις πληροφορίες που διαθέτει, προκειμένου να ανανεώνονται –αντίστοιχα- και τα αποτελέσματα που διαθέτει.

4.5.5. Χειρισμός εξαιρέσεων

Η πολυπλοκότητα των εφαρμογών, σε συνδυασμό με τις ετερογενείς πλατφόρμες (σε επίπεδο λειτουργικού συστήματος, δικτυακής υποδομής και λογισμικό επιπέδου

εφαρμογής) εισάγουν την ανάγκη του χειρισμού εξαιρέσεων σε ένα σύστημα διαχείρισης πληροφοριών ασφάλειας. Με άλλα λόγια, μια δικτυακή κυκλοφορία που χαρακτηρίζεται ως εκδήλωση επίθεσης από την υποδομή ασφάλειας ενός οργανισμού, είναι αρκετά πιθανόν να μην προκαλεί καμιά ζημιά στα υπολογιστικά συστήματα ή και ακόμη να έχει χαρακτηριστεί, εσφαλμένα, ως επιθετική κυκλοφορία (ψευδοθετικά σφάλματα στα συστήματα IDP, λάθη στη διαμόρφωση των συστημάτων ασφάλειας, ιδιαιτερότητες κώδικα εφαρμογής, κτλ.).

Στις περιπτώσεις αυτές, απαιτείται μια σειρά από διαδικασίες ανθρώπινης παρέμβασης για την αξιολόγηση και το χαρακτηρισμό της δικτυακής κυκλοφορίας, καθώς οι συνέπειες είναι αρκετά πιθανόν να προκαλέσουν ανεπιθύμητα αποτελέσματα στη λειτουργία του οργανισμού (π.χ. διακοπή εξουσιοδοτημένων δικτυακών συνόδων).

4.5.6. Οπτικοποίηση πληροφορίας

Ως σύστημα διαχείρισης πληροφοριών ασφάλειας, το σύστημα αντιμετώπισης περιστατικών θα πρέπει να διαθέτει μια σειρά λειτουργιών που στοχεύουν στην οπτικοποίηση των αποτελεσμάτων του, παρέχοντας την «πλούσια εικόνα» για την κατάσταση της ασφάλειας της υπολογιστικής και δικτυακής υποδομής που εξετάζει. Συνοπτικά, τα χαρακτηριστικά οπτικοποίησης των πληροφοριών είναι:

- Παροχή πληροφοριών που αφορούν στα χαρακτηριστικά αδυναμιών (με δυνατότητα αναζήτησης στις τοπικές βάσεις που διατηρεί το σύστημα, καθώς και σε προεπιλεγμένους δικτυακούς τόπους του Διαδικτύου). Τα χαρακτηριστικά αυτά είναι:
    - Αριθμός (κατά CVE) της αδυναμίας,
    - Σύντομη περιγραφή της αδυναμίας,
    - Σοβαρότητα της αδυναμίας,
    - Κατάσταση της αδυναμίας,
    - Ημερομηνία έκδοσης της αδυναμίας,

- Ημερομηνία τελευταίας μεταβολής της αδυναμίας,
- Βαθμολόγηση βασικών μετρικών της αδυναμίας κατά CVSSv2,
- Βαθμολόγηση περιβαλλοντικών μετρικών της αδυναμίας κατά CVSSv2,
- Βαθμολόγηση ιστορικών μετρικών της αδυναμίας κατά CVSSv2,
- Παροχή των ευάλωτων εκδόσεων (στη συγκεκριμένη αδυναμία) του λειτουργικού συστήματος και του λογισμικού εφαρμογής,
- Παροχή πρόσθετων πληροφοριών και παραπομπή σε δικτυακούς τόπους.

- Παροχή πληροφοριών που αφορούν στα χαρακτηριστικά υπογραφών των συστημάτων IDP (με δυνατότητα αναζήτησης στις τοπικές βάσεις που διατηρεί το σύστημα) Τα χαρακτηριστικά αυτά είναι:
  - Αριθμός υπογραφής (σύμφωνα με το σύστημα αναφοράς Snort),
  - Παροχή του αυτούσιου κώδικα της υπογραφής (σύμφωνα με το σύστημα αναφοράς Snort).
- Παροχή πληροφοριών που αφορούν στον κώδικα αθέμιτης εκμετάλλευσης που διατηρεί το σύστημα (με δυνατότητα αναζήτησης στις τοπικές βάσεις που διατηρεί το σύστημα, καθώς και σε προεπιλεγμένους δικτυακούς τόπους του Διαδικτύου),
- Απαρίθμηση όλων των δικτυακών σταθμών που εμφανίζουν αδυναμίες ασφάλειας και ταξινόμηση των αδυναμιών κατά CVE, σύμφωνα με τις πληροφορίες που διατηρεί το σύστημα στις βάσεις του. Οι αδυναμίες ασφάλειας που απαριθμεί το IRIS πηγάζουν από αντίστοιχες αναφορές εξειδικευμένων εργαλείων αποτίμησης αδυναμιών ασφάλειας (πιο συγκεκριμένα, του εργαλείου Nessus),
- Απαρίθμηση όλων των υπογραφών IDP που απαιτούνται για την αντιμετώπιση των προαναφερθεισών αδυναμιών ασφάλειας, σύμφωνα με τις πληροφορίες που διατηρεί το σύστημα στις βάσεις του,

- Απαρίθμηση όλων των τμημάτων κώδικα αθέμιτης εκμετάλλευσης που σχετίζονται με τις αδυναμίες που προαναφέρθηκαν, σύμφωνα με τις πληροφορίες που διατηρεί το σύστημα στις βάσεις του,

- Παροχή όλων των μετρικών που χαρακτηρίζουν τις αδυναμίες ασφάλειας της υποδομής (βασικών, ιστορικών και περιβαλλοντικών), με δυνατότητα επεξεργασίας των ιστορικών και περιβαλλοντικών μετρικών, ανάλογα με την περίσταση (π.χ. χειρισμός εξαιρέσεων, βλ. ενότητα 4.5.5).

4.6. Ανακεφαλαίωση

Στο παρόν κεφάλαιο περιγράφηκε η τοπολογική ανάλυση αδυναμιών ασφάλειας και οι επεκτάσεις της μεθόδου στην ερευνητική περιοχή των συστημάτων ανίχνευσης και αντιμετώπισης παρεισφρήσεων (IDP). Αρχικά, καθορίστηκαν οι απαραίτητες πληροφορίες για αδυναμίες ασφάλειας και κώδικα αθέμιτης εκμετάλλευσης που απαιτεί η μέθοδος, καθώς και οι αντίστοιχες απαιτούμενες πληροφορίες από τα συστήματα IDP με σκοπό την εξυπηρέτηση της αντιμετώπισης περιστατικών ασφάλειας. Αναλύθηκαν και αξιολογήθηκαν εκτενώς οι κυριότερες μέθοδοι ανάπτυξης συστημάτων IDP, ενώ προτάθηκε και αναλύθηκε η μέθοδος ανάπτυξης με χρήση τεχνικών τοπολογικής ανάλυσης αδυναμιών. Τέλος, προτάθηκαν και αναλύθηκαν εκτενώς οι απαιτήσεις ενός συστήματος αντιμετώπισης περιστατικών που βασίζεται στα παραπάνω.

Κεφάλαιο 5

Το Σύστημα Ευφυούς Αντιμετώπισης Περιστατικών - IRIS

"Those who desire to give up freedom in order to gain security will not have, nor do they deserve, either one."

- **Benjamin Franklin**

Στην ενότητα αυτή προτείνεται και παρουσιάζεται το *Σύστημα Ευφυούς Αντιμετώπισης Περιστατικών (Incident Response Intelligence System - IRIS)* το οποίο κατανοεί το γενικότερο περιβάλλον των *αδυναμιών* ασφάλειας που ανακαλύπτονται από εργαλεία αυτόματης αξιολόγησης επικινδυνότητας, βαθμολογεί τη σημαντικότητά τους με προτυποποιημένο τρόπο, βρίσκει και συσχετίζει τον κώδικα *εκμετάλλευσης* που σχετίζεται με αυτές τις *αδυναμίες* και καθορίζει τις απαραίτητες *υπογραφές* που αντιστοιχούν στις *εκμεταλλεύσεις*, κατασκευάζοντας *μονοπάτια αντιμετώπισης*. Τα *μονοπάτια αντιμετώπισης* εκφράζουν δυναμικές και προσαρμοζόμενες πολιτικές συστημάτων IDP και αντιμετωπίζουν τα αντίστοιχα *μονοπάτια επίθεσης*.

Παρουσιάζεται, λεπτομερειακά, η αρχιτεκτονική του συστήματος και το διάγραμμα ροής των λειτουργιών. Παρατίθενται οι λεπτομέρειες υλοποίησης και παρουσιάζεται η λειτουργία του σε μια πραγματική μελέτη περίπτωσης. Στη συγκεκριμένη μελέτη περίπτωσης, το *IRIS* κατασκευάζει αυτόματα την κατάλληλη πολιτική αντιμετώπισης περιστατικών σε ένα σύστημα, αφότου προσδιοριστεί, επαληθευτεί, συσχετιστεί και αξιολογηθεί για τη σημασία και τον αντίκτυπό της μια σειρά *αδυναμιών* και αντίστοιχου κώδικα *εκμετάλλευσης*.

5.1. Σχετική έρευνα

Η διεθνής βιβλιογραφία αναφέρει σημαντικές προσπάθειες στην ερευνητική περιοχή της τοπολογικής ανάλυσης αδυναμιών, καθώς και της συσχέτισης ετερογενούς πληροφορίας που σχετίζεται με αδυναμίες ασφάλειας, εκμεταλλεύσεις και δημιουργία πολιτικών IDP.

Χαρακτηριστικά, οι Templeton και Levitt περιγράφουν ένα ευέλικτο μοντέλο για επιθέσεις σε υπολογιστικά συστήματα, συμπεριλαμβανομένης και μιας γλώσσας για τη διευκρίνιση αυτού του μοντέλου, μαζί με προτάσεις για εφαρμογή του εν λόγω μοντέλου στη διαδικασία αποτίμησης *αδυναμιών* ασφάλειας και την ανίχνευση παρεισφρήσεων (Templeton & Levitt, 2000). Ο Sheyner έχει δημιουργήσει ένα εργαλείο για την αξιολόγηση των ιδιοτήτων των *αδυναμιών* ασφάλειας στα δίκτυα υπολογιστών που συσχετίζει, επίσης, τις γραφικές παραστάσεις επίθεσης με τα περισσότερο ευάλωτα σε *εκμετάλλευση* στοιχεία των ρυθμίσεων ενός συστήματος (Sheyner, et. al., 2002). Ο

Swiler έχει κατασκευάσει, επίσης, ένα εργαλείο που παράγει και αναλύει πληροφορίες σχετικές με ένα *μονοπάτι επίθεσης* το οποίο βασίζεται σε αλγόριθμους ελέγχου συμβολικών μοντέλων (Swiler, et. al., 2001). Οι Ammann, Wijesekera και Kaushik παρέχουν μια συμπαγέστερη, εξελικτική προσέγγιση των γραφικών αναπαραστάσεων των επιθέσεων στηριζόμενοι στην προϋπόθεση της μονοτονικότητας, που δηλώνει πως η απαραίτητη προϋπόθεση ενός δεδομένου κώδικα αθέμιτης *εκμετάλλευσης* δεν ακυρώνεται ποτέ από την επιτυχή εφαρμογή ενός άλλου κώδικα αθέμιτης *εκμετάλλευσης* (Ammann, Wijesekera, & Kaushik, 2002). Αυτή η προσέγγιση εστιάζει στο συνδυασμό των *αδυναμιών* που ανακαλύπτονται από εργαλεία VA προκειμένου να κατασκευαστούν σενάρια επίθεσης.

Οι εργασίες που συζητούνται παραπάνω εστιάζουν περισσότερο στη διαμόρφωση προτύπων για επιθέσεις σε υπολογιστικά συστήματα ή δίκτυα και στην παραγωγή μονοπατιών επίθεσης ή/και γραφικών παραστάσεων των επιθέσεων, παρά στη δημιουργία ενός συστήματος που χρησιμοποιεί τις πληροφορίες αυτές για να εκπληρώσει σενάρια που ταιριάζουν με πολιτικές ανίχνευσης παρεισφρήσεων. Εν τούτοις, μια σειρά πρόσφατων ερευνητικών εργασιών έχει στοχεύσει προς την κατεύθυνση αυτή, οι σημαντικότερες των οποίων αναφέρονται παρακάτω.

Ο Gula έχει επεξηγήσει διάφορα σενάρια που θα μπορούσαν να χρησιμοποιηθούν στη συσχέτιση αρχείων ανίχνευσης παρεισφρήσεων με πληροφορίες σχετικές με *αδυναμίες* ασφάλειας (Gula, 2009). Αυτή η προσέγγιση στοχεύει στο να μειώσει τις πληροφορίες θετικών σφαλμάτων που παρέχονται από τα συστήματα IDP, αλλά στερείται μηχανισμών «φιλτραρίσματος» στις πληροφορίες που χρησιμοποιούνται ως εισαγωγή (τόσο στα εργαλεία VA όσο και στα συστήματα IDP). Οι Ning και Xu έχουν παρουσιάσει τεχνικές αυτόματης εκμάθησης στρατηγικών επίθεσης από συσχετιζόμενους συναγερμούς, παραγόμενους από συστήματα IDP, μέσα από ένα μοντέλο που αναπαριστά μια στρατηγική επίθεσης ως γραφική αναπαράσταση επιθέσεων με περιορισμούς στις ιδιότητες επίθεσης και ως μια χρονική σειρά μεταξύ αυτών των επιθέσεων (Ning & Xu, 2003). Αυτή η εργασία παρουσιάζει μια μεθοδολογία συσχέτισης πληροφοριών ανίχνευσης παρεισφρήσεων με τη στατική εισαγωγή πληροφορίας από εργαλεία VA, χωρίς να εξετάζει τις υπάρχουσες συνθήκες ασφάλειας και τον κώδικα αθέμιτης

εκμετάλλευσης, ούτε να αναλύει τα μονοπάτια επίθεσης (attack paths) που οδηγούν σε συγκεκριμένους στόχους επίθεσης. Το τελευταίο περιγράφεται από τους Jajodia, Noel και O' Berry (Jajodia, Noel, & O'Berry, 2006), οι οποίοι δεν κάνουν –όμως- ιδιαίτερη θεώρηση στις σχέσεις των *αδυναμιών* με τον κώδικα αθέμιτης *εκμετάλλευσης*.

Οι Papadaki και Furnel (Papadaki & Furnell, 2006), προτείνουν μια αρχιτεκτονική ενός ευέλικτου και ευφυούς αυτοματοποιημένου συστήματος αντιμετώπισης επιθέσεων που είναι σε θέση να προσαρμόζει τις αποφάσεις αντιμετώπισης βασιζόμενο στο περιβάλλον ενός περιστατικού (και πιο συγκεκριμένα σε παρεισφρήσεις). Οι αποφάσεις για την αντιμετώπιση των περιστατικών, όμως, βασίζονται σε εμπειρική γνώση, ενώ δεν περιλαμβάνεται στη συγκεκριμένη προσέγγιση κάποιος συσχετισμός *αδυναμίας* ασφάλειας και *υπογραφών* IDP. Ο Debar και άλλοι (Debar, et. al., 2007) προτείνουν μια αρχιτεκτονική που επιτρέπει τη δυναμική δημιουργία συγκεκριμένων πολιτικών από μια γενική πολιτική ασφάλειας, λαμβάνοντας υπόψη το επίπεδο απειλής που έχουν προσδιορίσει τα συστήματα IDP. Αυτή η προσέγγιση βασίζεται, επίσης, σε εμπειρική γνώση για ένα μικρό σύνολο κινδύνων κάθε πρωτοκόλλου, περιορίζοντας –με τον τρόπο αυτό- το πεδίο εφαρμογής αυτής της ιδιαίτερα ενδιαφέρουσας προσέγγισης.

Τέλος, οι O'Hare, Noel και Prole ανέπτυξαν ένα εργαλείο οπτικοποίησης για πληροφορίες σχετικές με τοπολογική ανάλυση αδυναμιών (O'Hare, Noel, & Prole, 2008), το οποίο βασίζεται σε μια βάση γνωστών αδυναμιών και εκμεταλλεύσεων που παρέχουν έναν γράφο αναπαράστασης επιθέσεων σε ένα δεδομένο δίκτυο. Η συγκεκριμένη προσέγγιση θεωρείται ιδιαίτερα νεωτεριστική σε ό,τι αφορά στην αναπαράσταση των συγκεκριμένων γραφημάτων, χωρίς όμως να στοχεύει –εκ κατασκευής- στην αντιμετώπιση επιθέσεων, καθώς στερείται πληροφορίας που σχετίζεται με συστήματα IDP. Το χαρακτηριστικό αυτό, στερεί από τη συγκεκριμένη προσέγγιση, αφενός μεν τις δυνατότητες αναγνώρισης ενός περιστατικου αφετέρου δε την παροχή των απαραίτητων υπογραφών για την αντιμετώπισή του.

5.2. Σύστημα ευφυούς αντιμετώπισης περιστατικών

5.2.1. Δυνατότητες του συστήματος

Συνοπτικά, οι δυνατότητες του συστήματος IRIS είναι:

1. Συλλογή πληροφοριών που σχετίζονται με *αδυναμίες* ασφάλειας, *εκμεταλλεύσεις* και *υπογραφές* από πολλαπλές πηγές, όπως το Web, αντίστοιχες λίστες πληροφοριών που διατηρούνται από τη βιομηχανία ασφάλειας, δικτυακούς τόπους επιτιθέμενων [20] , συστήματα ανίχνευσης και αντιμετώπισης παρεισφρήσεων, αποτελέσματα εργαλείων VA, κτλ.,

2. Βαθμολόγηση των *αδυναμιών* ασφάλειας με χρήση του πρότυπου συστήματος CVSSv2 (Mell, Scarfone, & Romanosky, 2006), ώστε να παρέχεται ένα μετρήσιμο αποτέλεσμα σχετικά με τη σημασία μιας συγκεκριμένης *αδυναμίας*,

3. Κανονικοποίηση και συσχέτιση των πληροφοριών που περιγράφει *αδυναμίες* ασφάλειας,

4. Εύρεση και συσχέτιση του κώδικα αθέμιτης *εκμετάλλευσης* των αντίστοιχων *αδυναμιών*,

5. Εύρεση των σχετικών *υπογραφών* από συστήματα IDP, οι οποίες αντιμετωπίζουν τους προαναφερόμενους συνδυασμούς *αδυναμιών* και *εκμεταλλεύσεων*,

6. Κατασκευή μονοπατιών επίθεσης και αντιμετώπισης για τις συγκεκριμένες *αδυναμίες* και εκμεταλλεύσεις,

---

[20] *Προσωπική σημείωση του ερευνητή:* Η ακαδημαϊκή τεκμηρίωση των δικτυακών τόπων που συντηρούνται από επιτιθέμενους (hacking websites) δεν είναι πάντοτε εφικτή, διότι αφενός μεν διότι οι τόποι αυτοί έχουν πολύ μικρή διάρκεια ζωής (αφού οι επιτιθέμενοι δεν αφήνουν τα ίχνη τους στο Διαδίκτυο για μεγάλο χρονικό διάστημα) αφετέρου δε η παραπομπή σε τέτοιους τόπους θα μπορούσε – δυνητικά- να χρησιμοποιηθεί για μη ακαδημαϊκούς ή ερευνητικούς σκοπούς. Τέλος, η ονοματοδοσία και το περιεχόμενο που χρησιμοποιείται στους τόπους αυτούς δεν συνάδει πάντοτε με τα χρηστά ήθη και μπορεί να θεωρηθεί υβριστική ή προσβλητική από πολλούς.

7. Καθορισμός της σημασίας και της έκτασης μιας επίθεσης, παρέχοντας –μεταξύ άλλων- μετρικά αξιολόγησης του συνολικού ρίσκου για έναν οργανισμό,

8. Καθορισμός πολιτικών αντιμετώπισης περιστατικών ασφάλειας.

Στις επόμενες ενότητες παρουσιάζεται η αρχιτεκτονική του προτεινόμενου συστήματος, καθώς και οι υπηρεσίες που παρέχει.

5.2.2. Τρόπος λειτουργίας

5.2.2.1. Συλλογή πληροφοριών σχετικά με *αδυναμίες* ασφάλειας

Σε πρώτη φάση, το σύστημα IRIS συλλέγει –και διατηρεί σε μια εσωτερική βάση δεδομένων – ένα μεγάλο πλήθος από τεκμηριωμένες *αδυναμίες* ασφάλειας. Το σύστημα χρησιμοποιεί τη λίστα Common Vulnerabilities and Exposures (CVE) της εταιρείας Mitre ως την πρωτεύουσα πηγή πληροφοριών σχετικά με *αδυναμίες* ασφάλειας, καθώς και ένα μεγάλο πλήθος από παρόμοιες λίστες που τυγχάνουν αποδοχής από τη βιομηχανία ασφάλειας, καθώς και λίστες που διατηρούνται από κατασκευαστές λογισμικού και υλισμικού (όπως π.χ. Microsoft, Cisco Systems, Check Point Software Technologies, κτλ). Οι συγκεκριμένες λίστες διατηρούνται και ανανεώνονται τακτικά, μερικές καθημερινά, από τους αντίστοιχους κατόχους. Χαρακτηριστικά, το IRIS συλλέγει πληροφορίες σχετικές με αδυναμίες ασφάλειας από τις πηγές που παρατίθενται στο *Παράρτημα Α*.

5.2.2.2. Συσχέτιση πληροφοριών σχετικά με *αδυναμίες* ασφάλειας

Η συσχέτιση των πληροφοριών που συλλέγονται από το IRIS έχει ιδιαίτερη σημασία καθώς στη βιομηχανία ασφάλειας κάθε *αδυναμία* περιγράφεται με διαφορετικό τρόπο και διαφορετική συμβατική ονοματοδοσία. Για παράδειγμα, η *αδυναμία* με το CVE αναγνωριστικό 2000-0246 αντιστοιχεί στην *αδυναμία* που περιγράφεται από τη Microsoft σαν MS00-019, ενώ η *αδυναμία* με το CVE αναγνωριστικό 2003-0100 αντιστοιχεί στην *αδυναμία* που περιγράφεται από τη Cisco ως 20030507. Το IRIS παρέχει έναν απευθείας σύνδεσμο σε όλες τις προαναφερόμενες (διαδικτυακές) τοποθεσίες, τόσο για εξακρίβωση όσο και για ενημέρωση της πληροφορίας που παρέχει, ενώ διατηρείται –σε τοπική βάση

δεδομένων- μια λίστα με *αδυναμίες* που έχουν επιβεβαιώσει οι αντίστοιχοι κατασκευαστές.

5.2.2.3. Βαθμολόγηση *αδυναμιών* ασφάλειας

Για όλες τις *αδυναμίες* που διατηρεί το IRIS, υπολογίζεται η βαθμολόγηση της σημασίας τους με βάση το πρότυπο CVSSv2, ενώ κάθε αναγνωριστικό CVE χρησιμοποιείται ως πρωτεύον κλειδί για τη συσχέτιση κάθε *αδυναμίας* με τις υπόλοιπες λίστες. Ο στόχος είναι η παροχή ενός μετρικού για τη σημασία μιας ανακαλυπτόμενης *αδυναμίας*, καθώς και πλεονάζουσες πληροφορίες για την *αδυναμία* αυτή (π.χ. από λίστες κατασκευαστών)

Η διεργασία της βαθμολόγησης *αδυναμιών* είναι ιδιαίτερα πολύπλοκη, καθώς αφενός μεν διενεργείται για κάθε ανακαλυπτόμενη *αδυναμία*, αφετέρου δε εξαρτάται από τη γενικότερη υποδομή ασφάλειας στην οποία ανακαλύπτεται η συγκεκριμένη *αδυναμία* (security context). Επίσης, η βαθμολόγηση μιας *αδυναμίας* θα πρέπει να βασίζεται τόσο σε εγγενή χαρακτηριστικά της *αδυναμίας* όσο και σε χαρακτηριστικά του ευρύτερου περιβάλλοντος, ενώ θα πρέπει να παρέχει μια ενιαία γλώσσα που θα κομίζει πληροφορίες σχετικά με τη σημασία μιας *αδυναμίας* και να εξυπηρετεί στην απόφαση της προτεραιότητας και της σημασίας για την κατάλληλη αντιμετώπισή της. Τέλος, ο τρόπος που θα βαθμολογείται μια *αδυναμία* θα πρέπει να είναι ανοικτός, χρήσιμος και κατανοητός από σχεδόν οποιονδήποτε συμμετέχει σε λειτουργίες ασφάλειας μέσα σε έναν οργανισμό.

Ένα πρότυπο σύστημα βαθμολόγησης *αδυναμιών* παρέχεται από το National Infrastructure Advisory Council των ΗΠΑ, ως μια κοινή προσπάθεια σημαντικών οργανισμών του Διαδικτύου, όπως το CERT/CC, η εταιρεία Cisco Systems, το Υπουργείο Εθνικής Ασφάλειας και η εταιρεία MITRE, το eBay, η εταιρεία IBM Internet Security Systems, η Microsoft, η Qualys και η Symantec. Το κοινό σύστημα βαθμολόγησης *αδυναμιών* (Common Vulnerability Scoring System - CVSS) συντηρείται από το διεθνές Φόρουμ Ομάδων Αντιμετώπισης Περιστατικών Ασφάλειας (Forum of Incident Response Teams - FIRST), ενώ η βιβλιογραφία αναφέρει παρόμοιες

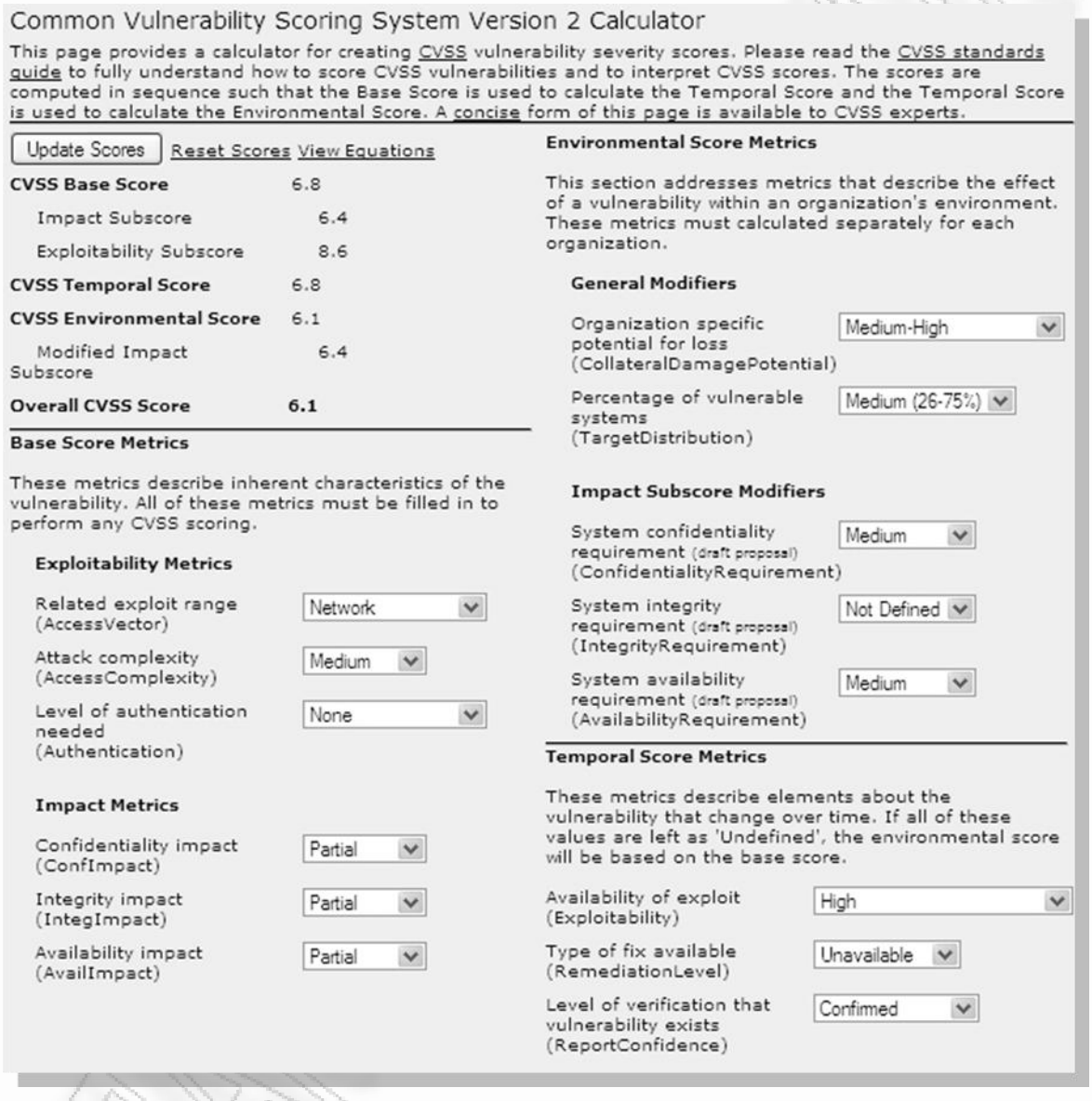
(μεμονωμένες) προσπάθειες πριν την καθολική υιοθέτηση του συγκεκριμένου προτύπου, όπως οι (Microsoft, 2002) και (US-CERT, 2009).

Το σύστημα CVSS στοχεύει στην παροχή μιας τιμής στην κλίμακα 1 μέχρι 10, που αναπαριστά τη σημασία και το ρίσκο μιας *αδυναμίας* και βασίζεται σε μετρικά και εξισώσεις, όπως φαίνεται και στο Σχήμα 5-1 (στο οποίο χρησιμοποιείται η πηγή NVD που αναφέρεται στον Πίνακα Πίνακας 5-1. Τα μετρικά του συγκεκριμένου συστήματος παρουσιάζονται τόσο με ποιοτικό όσο και με ποσοτικό τρόπο και περιλαμβάνουν:

- *Βασικά Μετρικά (Base Metrics)*, τα οποία είναι εγγενή για κάθε *αδυναμία* και τα οποία δεν μεταβάλλονται στην πάροδο του χρόνου. Τα βασικά μετρικά είναι το αποτέλεσμα μιας πολύπλοκης εξίσωσης η οποία έχει ως παράγοντες συγκεκριμένα χαρακτηριστικά μιας *αδυναμίας*, όπως η δυνατότητα τοπικής ή απομακρυσμένης *εκμετάλλευσης*, η πολυπλοκότητα πρόσβασης, τα επακόλουθα στην εμπιστευτικότητα/ακεραιότητα ή/και διαθεσιμότητα μιας πληροφορίας, κτλ.,
- *Ιστορικά Μετρικά (Temporal Metrics)*, που βασίζονται στα χαρακτηριστικά μιας *αδυναμίας* τα οποία μεταβάλλονται κατά τον κύκλο ζωής μιας συγκεκριμένης *αδυναμίας*. Τα ιστορικά μετρικά βασίζονται σε παράγοντες όπως η αποδεδειγμένη *εκμετάλλευση*, το επίπεδο επανόρθωσης μιας *αδυναμίας*, καθώς και η ακεραιότητα της συγκεκριμένης αναφοράς,
- *Περιβαλλοντικά Μετρικά (Environmental Metrics)*, τα οποία εξαρτώνται από το ιδιαίτερο περιβάλλον στο οποίο ανακαλύπτεται μια συγκεκριμένη *αδυναμία*. Στην περίπτωση αυτή, τα περιβαλλοντικά μετρικά είναι το αποτέλεσμα μιας ιδιαίτερα περίπλοκης εξίσωσης που βασίζεται σε παράγοντες όπως η πιθανή παράπλευρη ζημιά και η κατανομή του στόχου,

Τα βασικά και ιστορικά μετρικά είναι διαθέσιμα από κάθε μηχανισμό ασφάλειας που είναι συμβατός με το πρότυπο CVE. Ο υπολογισμός των περιβαλλοντικών μετρικών είναι ευθύνη της λειτουργίας του IRIS, μιας και το IRIS μπορεί να κατασκευάσει –σε πραγματικό χρόνο- ένα χάρτη αντιστοίχησης μεταξύ *αδυναμιών* ασφάλειας, σχετικών *εκμεταλλεύσεων* και IDP *υπογραφών*. Στην περίπτωση που δεν υπάρχει *υπογραφή* στο σύστημα IDP που αντιστοιχεί σε μια συγκεκριμένη *αδυναμία*, η τιμή των

περιβαλλοντικών μετρικών υπολογίζεται στην υψηλότερη δυνατή τιμή, σε συνδυασμό με τις διαθέσιμες τιμές που διατηρούνται από την Εθνική Βάση Δεδομένων για *Αδυναμίες* Ασφάλειας των Η.Π.Α. (NVD, 2009).



Σχήμα 5-1 – Καθορισμός τιμής CVSSv2 με χρήση του υπολογιστή NVD

Ο καθορισμός της τιμής CVSSv2 μπορεί να παραχθεί είτε με χρήση αυτοματοποιημένων εργαλείων, είτε με χρήση κατάλληλων εργαλείων στο Διαδίκτυο. Ενδεικτικά, ο Πίνακας 5-1 αναφέρει μερικές διαδικτυακές πηγές στις οποίες υπάρχουν διαθέσιμα σχετικά εργαλεία:

Πίνακας 5-1: Διαδικτυακές πηγές εργαλείων υπολογισμού τιμής CVSSv2 (NVD, 2009)

Όνομα υπολογιστή	Διαδικτυακός Σύνδεσμος
Υπολογιστής NVD	http://nvd.nist.gov/cvss.cfm?calculator
Patch Advisor	http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx
Information-Technology Promotion Agency, Japan	http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/en/index.01.html
Cisco	http://intellishield.cisco.com/security/alertmanager/cvss

Εξίσου σημαντικό, τέλος, είναι να αναλυθεί ο όρος του διανύσματος CVSSv2, το οποίο περιγράφει τα χαρακτηριστικά μιας συγκεκριμένης αδυναμίας. Αναλυτικά, για τα βασικά χαρακτηριστικά μιας αδυναμίας, το διάνυσμα CVSSv2 έχει την παρακάτω μορφή:

(AV:[L,A,N]/AC:[H,M,L]/Au:[N,S,M]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C])

Τα γράμματα στις αγκύλες αντιπροσωπεύουν τις πιθανές τιμές ενός μετρικού CVSSv2 και παίρνουν μόνο μια τιμή από όσες αναφέρονται σε κάθε μια ξεχωριστή αγκύλη. Όλα τα παραπάνω μετρικά (ήτοι γράμματα εκτός αγκυλών) συνοδεύουν υποχρεωτικά κάθε διάνυσμα CVSSv2. Οι τιμές κάθε βασικού μετρικού παριστάνονται στον ΠίνακαΠίνακας 5-2:

Πίνακας 5-2: Κατηγορίες και τιμές μετρικών για βασικά χαρακτηριστικά αδυναμιών

Κατηγορία Μετρικού /Τιμή/ Περιγραφή					
AV *Περιοχή εκμετάλλευσης*		***AC*** *Πολυπλοκότητα επίθεσης*		***Au*** *Επίπεδα αυθεντικοποίησης*	
L	Τοπική	H	Υψηλή	N	Κανένα
A	Γειτονικό Δίκτυο	M	Μέτρια	S	Ένα επίπεδο
N	Δικτυακή	L	Χαμηλή	M	Πολλαπλά Επίπεδα
C *Επίπτωση Εμπιστευτικότητας*		***I*** *Επίπτωση Ακεραιότητας*		***A*** *Επίπτωση Διαθεσιμότητας*	
N	Καμία	N	Καμία	N	Καμία
P	Μερική	P	Μερική	P	Μερική
C	Πλήρης	C	Πλήρης	C	Πλήρης

Αντίστοιχα, το διάνυσμα CVSSv2 που περιλαμβάνει τα ιστορικά μετρικά ακολουθεί το αντίστοιχο διάνυσμα των βασικών μετρικών και έχει την παρακάτω μορφή:

/E:[U,P,F,H]/RL:[O,T,W,U]/RC:[N,U,C]

Και στην περίπτωση των ιστορικών μετρικών, τα γράμματα στις αγκύλες αντιπροσωπεύουν τις πιθανές τιμές ενός μετρικού CVSSv2 και παίρνουν μόνο μια τιμή από όσες αναφέρονται σε κάθε μια ξεχωριστή αγκύλη. Οι τιμές κάθε ιστορικού μετρικού παριστάνονται στον Πίνακα Πίνακας 5-3:

Πίνακας 5-3: Κατηγορίες και τιμές μετρικών για ιστορικά χαρακτηριστικά αδυναμιών

Κατηγορία Μετρικού /Τιμή/ Περιγραφή					
E *Διαθεσιμότητα κώδικα εκμετάλλευσης*		***RL*** *Είδος διορθωτικού λογισμικού*		***RC*** *Επίπεδο επιβεβαίωσης απόδειξης της αδυναμίας*	
U	Χωρίς Απόδειξη	O	Επίσημο	N	Χωρίς επίσημη απόδειξη
P	Αποδεδειγμένη	T	Προσωρινό	U	Μη αποδεδειγμένη
F	Λειτουργική	W	Τεχνοτροπία	C	Επιβεβαιωμένη
W	Ευρέως Διαθέσιμη	U	Μη διαθέσιμο		

Τέλος, το διάνυσμα CVSSv2 που περιλαμβάνει τα περιβαλλοντικά μετρικά ακολουθεί το αντίστοιχο διάνυσμα των ιστορικών και βασικών μετρικών και έχει την παρακάτω μορφή:

/CD[N,L,LM,MH,H]:/TD:[N,L,M,H]/CR:[L,M,H]/IR:[L,M,H]/AR:[L,M,H]

Οι τιμές κάθε περιβαλλοντικού μετρικού παριστάνονται στον Πίνακας 5-4:

Πίνακας 5-4: Κατηγορίες και τιμές μετρικών για περιβαλλοντικά χαρακτηριστικά αδυναμιών

Κατηγορία Μετρικού /Τιμή/ Περιγραφή					
CD *Πιθανότητα παράπλευρης ζημιάς*		***TD*** *Ποσοστό αδύναμων συστημάτων*		***CR*** *Απαιτήσεις Εμπιστευτικότητας συστήματος*	
N	Καμία	N	Κανένα (0%),	L	Χαμηλές
L	Χαμηλή	L	Χαμηλό (1-25%),	M	Μεσαίες
LM	Χαμηλή-προς-μεσαία	M	Μεσαίο (26-75%),	H	Υψηλές
MH	Μεσαία-προς-υψηλή	H	Υψηλό (76-100%)	-	-
H	Υψηλή	-	-	-	-

Κατηγορία Μετρικού /Τιμή/ Περιγραφή			
IR *Απαιτήσεις Ακεραιότητας Συστήματος*		***AR*** *Απαιτήσεις Διαθεσιμότητας Συστήματος*	
L	Χαμηλές	L	Χαμηλές
M	Μεσαίες	M	Μεσαίες
H	Υψηλές	H	Υψηλές

5.2.2.4. Διεργασίες και δομοστοιχεία *αδυναμιών*

Όσα προαναφέρθηκαν εκτελούνται από διάφορες διεργασίες του IRIS, οι οποίες αντιστοιχούν στα παρακάτω δομοστοιχεία:

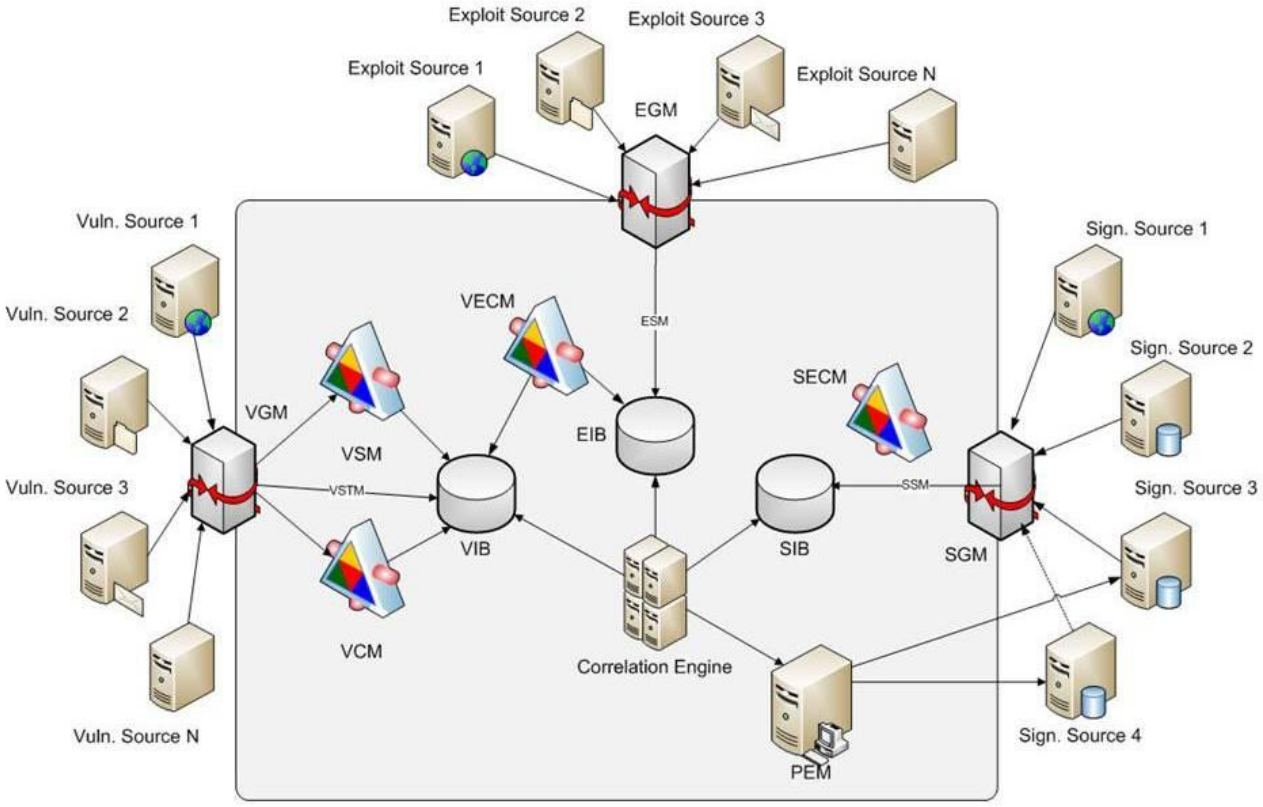
- Διεργασία συλλογής πληροφοριών από διαφορετικές ετερογενείς πηγές (π.χ. το Διαδίκτυο, λίστες αναφορών και εργαλεία VA), η οποία εκτελείται από το *Δομοστοιχείο Συλλογής Πληροφοριών Αδυναμιών Ασφάλειας (Vulnerability Gathering Module - VGM),*

- Διεργασία κανονικοποίησης και συσχέτισης πληροφοριών σχετικών με *αδυναμίες* ασφάλειας, η οποία εκτελείται από το *Δομοστοιχείο Συσχέτισης Αδυναμιών (Vulnerability Correlation Module - VCM),*

- Διεργασία βαθμολόγησης *αδυναμιών* σύμφωνα με το πρότυπο CVSSv2, η οποία εκτελείται από το *Δομοστοιχείο Βαθμολόγησης Αδυναμιών (Vulnerability Scoring Module - VSM),*

- Διεργασία αποθήκευσης των παραπάνω πληροφοριών στη Βάση Πληροφοριών *Αδυναμιών* (Vulnerability Information Base - VIB), η οποία εκτελείται από το *Δομοστοιχείο Αποθήκευσης Αδυναμιών (Vulnerability Storage Module - VSTM)*.

Παράλληλα με τη συλλογή, συσχέτιση, (βαθμολόγηση) και αποθήκευση των πληροφοριών που σχετίζονται με *αδυναμίες*, στο IRIS εκτελούνται παρόμοιες διεργασίες σχετικά με εκμεταλλεύσεις και υπογραφές.



Σχήμα 5-2 – Τα δομοστοιχεία του συστήματος IRIS

5.2.2.5. Συλλογή πληροφοριών για εκμεταλλεύσεις και υπογραφές

Πληροφορίες σχετικές με εκμεταλλεύσεις (καθώς και με τον κώδικα αθέμιτης *εκμετάλλευσης*) υπάρχουν διάσπαρτες στο Διαδίκτυο και σε λίστες ηλεκτρονικού ταχυδρομείου. Από την άλλη πλευρά, αντίστοιχες πληροφορίες υπάρχουν στα συστήματα IDP (συνήθως μια *υπογραφή* εμπεριέχει αυτούσιο τον κώδικα αθέμιτης

εκμετάλλευσης για μια συγκεκριμένη αδυναμία καθώς και πιθανές παραλλαγές αυτού). Επίσης, στη διεθνή βιβλιογραφία αναφέρεται μια σειρά εργασιών σχετικών με κατηγοριοποίηση συστημάτων εισβολών, όπως στο (Ragsdale, Carver, Humphries, & Pooch, 2000), το οποίο χρησιμοποιείται ακόμη ως σύστημα αναφοράς, στο (Rasheed & Chow, 2007), στο (Stakhanova, Basu, & Wong, 2007), , από τις οποίες θα μπορούσε κανείς να αντλήσει αντίστοιχες πληροφορίες.

Στο IRIS, οι πληροφορίες αυτές παράγονται από τις παρακάτω διεργασίες και δομοστοιχεία του συστήματος, τα οποία απεικονίζονται στο Σχήμα 5-2:

- Διεργασία συλλογής πληροφοριών για εκμεταλλεύσεις, η οποία εκτελείται από το *Δομοστοιχείο Συλλογής Πληροφοριών Εκμεταλλεύσεων (Exploit Gathering Module - EGM)*,
- Διεργασία αποθήκευσης στη *Βάση Πληροφοριών Εκμεταλλεύσεων (Exploit Information Base - EIB)*, η οποία εκτελείται από το *Δομοστοιχείο Αποθήκευσης Εκμεταλλεύσεων (Exploit Storage Module - ESM)*,
- Διεργασία συλλογής πληροφοριών για υπογραφές από συστήματα IDP, η οποία εκτελείται από το *Δομοστοιχείο Συλλογής Πληροφοριών Υπογραφών (Signature Gathering Module - SGM)*,
- Διεργασία συσχέτισης των *εκμεταλλεύσεων* με τις *αδυναμίες*, η οποία εκτελείται από το *Δομοστοιχείο Συσχέτισης Εκμεταλλεύσεων και Αδυναμιών (Vulnerability Exploit Correlation Module - VECM)*,
- Διεργασία συσχέτισης των *υπογραφών* με τις εκμεταλλεύσεις, η οποία εκτελείται από το *Δομοστοιχείο Συσχέτισης Υπογραφών και Εκμεταλλεύσεων (Signature Exploit Correlation Module - SECM)*,
- Διεργασία αποθήκευσης στη *Βάση Πληροφοριών Υπογραφών Signature Information Base (SIB)*, η οποία εκτελείται από το *Δομοστοιχείο Αποθήκευσης Υπογραφών (Signature Storage Module - SSM)*.

Με την ολοκλήρωση των διεργασιών αυτών, παρέχεται μία πλήρης αντιστοίχηση μεταξύ *αδυναμιών*, εκμεταλλεύσεων και υπογραφών, όπως απεικονίζεται στο Σχήμα 4-2.

5.2.2.6. Συσχέτιση και αντιστοίχηση *αδυναμιών*, *εκμεταλλεύσεων* και *υπογραφών*

Όταν έχουν κατασκευαστεί πλήρως οι VIB, EIB και SIB, μια μηχανή συσχέτισης (*correlation engine*) αναλαμβάνει να αντιστοιχήσει τις πληροφορίες που είναι καταχωρημένες στις βάσεις αυτές και να παρέχει τη σχέση μεταξύ *αδυναμιών*, *εκμεταλλεύσεων* και *υπογραφών*, ήτοι την τοπολογική ανάλυση μιας επίθεσης.

Στόχος της μηχανής αυτής, εκτός από τη λειτουργία του συστήματος IRIS, είναι η συνεισφορά και η βελτίωση της ερευνητικής περιοχής που ασχολείται με την Τοπολογική Ανάλυση *Αδυναμιών* (Topological Vulnerability Analysis - TVA) μέσω της παροχής μιας πλήρους συσχέτισης μεταξύ *αδυναμιών*, *εκμεταλλεύσεων* και *υπογραφών*, ήτοι όχι μόνο του *μονοπατιού επίθεσης* (*αδυναμίες* που εκμεταλλεύεται ένας επιτιθέμενος) αλλά και του *μονοπατιού αντιμετώπισης*, το οποίο περιγράφει τις υπογραφές που πρέπει να συμπεριληφθούν σε ένα αντίστοιχο μονοπάτι αντιμετώπισης και οι οποίες αποτελούν μια πολιτική αντιμετώπισης (μιας εισβολής).

Ένα μονοπάτι αντιμετώπισης (r_i), όπως προαναφέρθηκε, αποτελείται από τις υπογραφές IDP που αντιστοιχούν σε ένα μονοπάτι επίθεσης (a_i), οπότε και αναμένεται ότι για κάθε a_i θα χρησιμοποιείται τουλάχιστον μια τέτοια *υπογραφή*. Σε απλουστευμένες περιπτώσεις, μπορεί να υποτεθεί πως η χρήση μιας και μόνο *υπογραφής* που αντιστοιχεί στην *εκμετάλλευση* μιας τυχαίας αδυναμίας του μονοπατιού a_i μπορεί –πρακτικά- να αντιμετωπίσει το συγκεκριμένο μονοπάτι (καθώς η επίθεση δεν μπορεί να συνεχιστεί από το σημείο αυτό εφεξής). Αν και κάτι τέτοιο είναι πιθανόν, η γενίκευση του παραπάνω ισχυρισμού δεν ευσταθεί, καθώς υπάρχουν περιπτώσεις επιθέσεων, όπως π.χ. οι επιθέσεις πολλαπλών σταδίων (multistage attacks) και οι συνδυασμένες επιθέσεις (blended attacks), όπου η *εκμετάλλευση* μιας συγκεκριμένης *αδυναμίας* ενός μονοπατιού επίθεσης μπορεί να εκκινήσει διαφορετικά μονοπάτια επίθεσης από το σημείο αυτό (Mathew, Britt, Giomundo, & Upadhyaya, 2005).

5.2.2.7. Εφαρμογή πολιτικής και επαναπαραμετροποίηση συστημάτων IDP

Το *Δομοστοιχείο Εφαρμογής Πολιτικής (Policy Enforcement Module - PEM)* είναι υπεύθυνο για την ανάλυση της πολιτικής (ήτοι το σύνολο των *υπογραφών*) που εφαρμόζει ένα σύστημα IDP, καθώς επίσης και για την κατασκευή και εφαρμογή των αντίστοιχων πολιτικών, εφόσον έχουν κατασκευαστεί τα αντίστοιχα μονοπάτια επίθεσης και αντιμετώπισης.

Με άλλα λόγια, το PEM βρίσκει και επιλέγει το ελάχιστο σύνολο *υπογραφών* (από την αντίστοιχη βάση του συστήματος IDP) που απαιτούνται για την ανίχνευση ή και παρεμπόδιση ενός μονοπατιού επίθεσης, ανάλογα με τη φύση της υπογραφής. Στην παρούσα φάση, η ενεργοποίηση του ελάχιστου αυτού συνόλου γίνεται χειρωνακτικά, αλλά υπάρχουν αρκετές επιλογές για την αυτοματοποίηση της συγκεκριμένης διαδικασίας. Για παράδειγμα, μπορεί να χρησιμοποιηθεί μια αυτοματοποιημένη και τυποποιημένη γλώσσα γι΄ αυτό, όπως η γλώσσα SISL που ορίζεται στο (Tung, 2000), η χρήση τρίτων προϊόντων ή και ο προγραμματισμός σεναρίων (scripting). Από την άλλη πλευρά, όλα τα απαραίτητα στοιχεία της πολιτικής είναι διαθέσιμα στην κονσόλα του IRIS.

Το χαρακτηριστικό αυτό επιτρέπει αρκετά ενδιαφέροντα σενάρια για την παραμετροποίηση των συστημάτων IDP, ιδιαίτερα σε στιγμές που απαιτείται άμεση αντιμετώπιση ενός περιστατικού για το οποίο δεν υπάρχει αντίστοιχη πολιτική στα συστήματα IDP κατά τη χρονική περίοδο που το περιστατικό βρίσκεται σε εξέλιξη.

Τέλος, μια πολιτική IDP που ορίζεται από το IRIS μπορεί να ενεργοποιήσει την εφαρμογή μιας ακόμη πολιτικής IDP (με αλυσιδωτό τρόπο), ώστε να κατασκευαστεί μια ενιαία πολιτική αντιμετώπισης σε ένα συγκεκριμένο πεδίο εφαρμογής (π.χ. σε έναν ολόκληρο οργανισμό). Τα αναμενόμενα πλεονεκτήματα για την περίπτωση αυτή περιγράφονται στις επόμενες ενότητες, στο πλαίσιο της αντιμετώπισης περιστατικών ασφάλειας και της ανάλυσης ψηφιακών πειστηρίων.

5.2.2.8. Βελτιώσεις στην αντιμετώπιση περιστατικών ασφάλειας και στην ανάλυση ψηφιακών πειστηρίων

Οι τυπικές μεθοδολογίες αντιμετώπισης περιστατικών ασφάλειας, όπως εκείνη που παρουσιάστηκε στην ενότητα 3.3, απαιτούν τη χειρωνακτική ή την ημι-αυτόματη διαδικασία του καθορισμού και της συσχέτισης πληροφοριών από γεγονότα ασφάλειας έτσι ώστε οι αποφάσεις που λαμβάνονται για την πλήρη και αποτελεσματική αντιμετώπιση ενός περιστατικού ασφάλειας να βασίζονται στην πιθανότητα εμφάνισης, το πεδίο, το εύρος και τη σημασία του συγκεκριμένου περιστατικού. Οι αποφάσεις αυτές κατευθύνουν μια μεγάλη λίστα από αντίστοιχες ενέργειες, σχεδόν σε όλο το φάσμα ενός οργανισμού (Mitropoulos, Patsos, & Douligeris, 2006). Για το σκοπό αυτό, είναι ιδιαίτερα σημαντικό αφενός να ταυτοποιηθεί η ύπαρξη ενός περιστατικού ασφάλειας σε σύντομο χρόνο και αφετέρου να συλλεχθούν (ή να παραχθούν) ακριβείς και έγκυρες πληροφορίες σχετικά με τη φύση του συγκεκριμένου περιστατικού.

Η παρούσα κατάσταση στη βιομηχανία ασφάλειας παρέχει αρκετά εργαλεία διαχείρισης που υποβοηθούν τη διαδικασία αντιμετώπισης περιστατικών. Για παράδειγμα, τα Συστήματα Διαχείρισης Πληροφοριών Ασφάλειας (Security Information Management systems - SIMs) βασίζουν τις αποφάσεις τους στη συσχέτιση αρχείων ελέγχου και καταγραφής που υπάρχουν σε συστήματα, δίκτυα, εφαρμογές, μηχανισμούς ασφάλειας, κτλ. και που απαρτίζουν μια συγκεκριμένη υποδομή που παρακολουθεί το SIM. Στη συνέχεια, οι πληροφορίες που παρέχει το SIM χρησιμοποιούνται για να ανιχνεύσουν και να αποφασίσουν, εξετάζοντας τα ψευδοθετικά αποτελέσματα των συστημάτων IDP, την ύπαρξη και ταυτοποίηση ενός περιστατικού ασφάλειας (Mitropoulos, Patsos, & Douligeris, 2007). Τονίζεται πως τα συμπεράσματα των SIM βασίζονται σε πληροφορίες μετά την εμφάνιση ενός περιστατικού, όπως είναι τα αρχεία ελέγχου και καταγραφής (audit logs).

Το σύστημα IRIS, από την άλλη πλευρά, παρέχει το απολύτως ελάχιστο σύνολο *υπογραφών* IDP προκειμένου να επιληφθεί μιας αναγνωρισμένης επίθεσης, βασιζόμενο σε πληροφορίες που υπάρχουν πριν την ύπαρξη ενός περιστατικού και αναλύοντας πληροφορίες σχετικές με *αδυναμίες*, εκμεταλλεύσεις και υπογραφές. Σε μια

ολοκληρωμένη αρχιτεκτονική ασφάλειας, τα δύο αυτά συστήματα διαχείρισης (IRIS, SIM) μπορεί να λειτουργήσουν παράλληλα, ενώ τα αποτελέσματά τους μπορεί να αλληλοτεκμηριώνονται για ένα υψηλό επίπεδο διασφάλισης στη λήψη αποφάσεων για την αντιμετώπιση περιστατικών ασφάλειας.

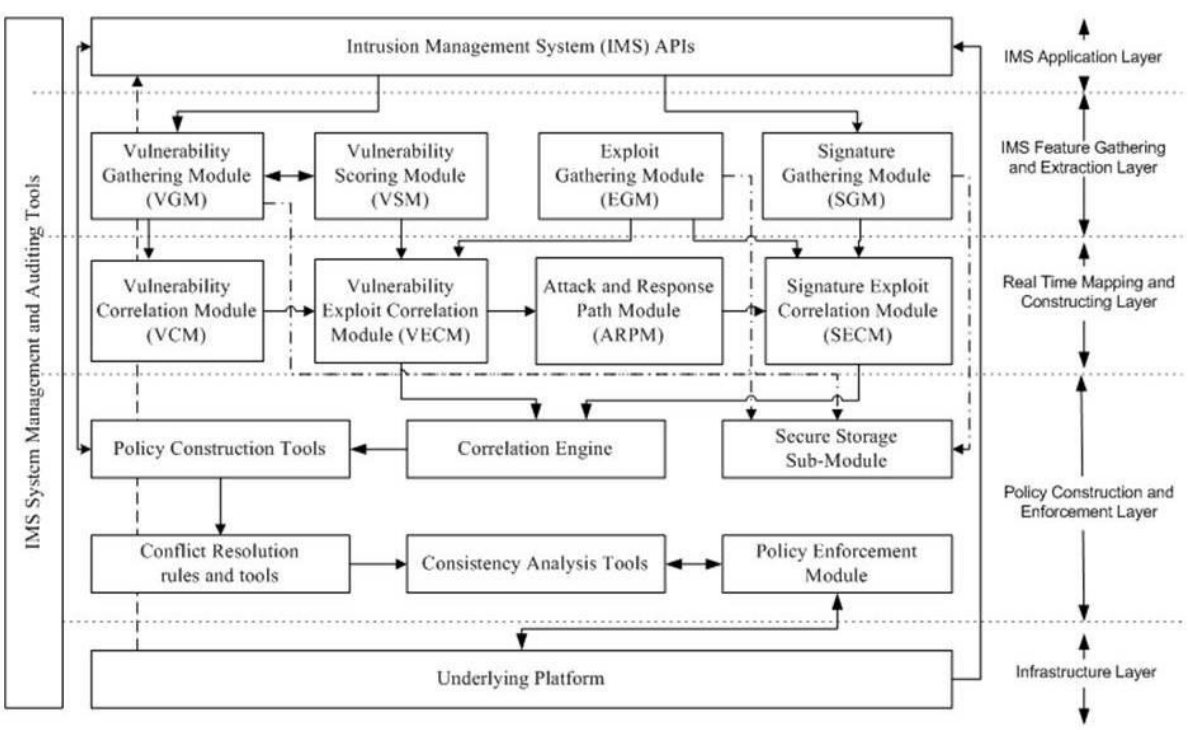
Επιπροσθέτως, οι κύριες λειτουργίες του IRIS μπορούν να χρησιμοποιηθούν στη φάση προετοιμασίας μιας εταιρικής διαδικασίας αντιμετώπισης περιστατικών, όταν επιλέγεται και παραμετροποιείται η υποδομή ασφάλειας του οργανισμού (όπως αναφέρθηκε στην ενότητα 3.3.1).

Επιπλέον, στην περίπτωση που ένας οργανισμός επιλέξει να διεξαγάγει μία ανάλυση ψηφιακών πειστηρίων, το IRIS μπορεί να εξυπηρετήσει το σκοπό αυτό, παρέχοντας σύντομες και ακριβείς πληροφορίες σχετικά με ένα περιστατικό. Η ουσία του παραπάνω ισχυρισμού μπορεί να εκτιμηθεί στην περίπτωση που η ανάλυση πραγματοποιηθεί σε «ζωντανά» συστήματα (ήτοι κατά τη διάρκεια που ένα περιστατικό βρίσκεται σε εξέλιξη). Στην περίπτωση αυτή, η κρίσιμη πληροφορία αφορά στην κατάλληλη περιγραφή των –πιθανών- *αδυναμιών* που το προκάλεσαν, την επιβεβαίωση πως ένα περιστατικό βρίσκεται σε εξέλιξη καθώς και την αξιολόγηση της πληρότητας της εφαρμοζόμενης πολιτικής ασφάλειας (Adelstein, 2006). Τα παραπάνω παρέχονται από το IRIS, καθώς το σύστημα παρέχει το μονοπάτι επίθεσης, τη συσχετισμένη πληροφορία περιγραφής της συγκεκριμένης επίθεσης και το ευρύτερο περιβάλλον αυτής, καθώς και το ελάχιστο σύνολο απαιτουμένων *υπογραφών* IDP για την κατασκευή της πολιτικής αντιμετώπισης.

Η οπτικοποίηση της πληροφορίας αυτής σε μία μόνο οθόνη μπορεί να αντιμετωπίσει τους περιορισμούς στα διάφορα (ειδικής-κατασκευής) εργαλεία ανάλυσης ψηφιακών πειστηρίων που δεν παρέχουν αποδοτικές τεχνικές φιλτραρίσματος της συγκεκριμένης πληροφορίας (Krasser, et.al., 2005). Οι τεχνικές φιλτραρίσματος απαιτούνται ώστε να παρέχεται μία επίβλεψη του περιστατικού ασφάλειας σε πραγματικό χρόνο, παράλληλα με τις αντίστοιχες ενέργειες αντιμετώπισης και τη (σύντομη) περιγραφή της επίθεσης που βρίσκεται σε εξέλιξη.

5.2.3. Αρχιτεκτονική συστήματος

Το IRIS αποτελείται από πέντε (5) κύρια επίπεδα, όπως απεικονίζει το Σχήμα 5-3.



Σχήμα 5-3 – Η αρχιτεκτονική του Συστήματος IRIS

5.2.3.1. Επίπεδο εφαρμογής

Το επίπεδο εφαρμογής του συστήματος IRIS παρέχει τη διεπαφή με τον τελικό χρήστη (καθώς και τον προγραμματιστή του IRIS). Περιλαμβάνει τις κατάλληλες Διεπαφές Προγραμματισμού της Εφαρμογής (Application Programming Interface – API) για τον καθορισμό των πηγών αναζήτησης πληροφοριών για *αδυναμίες*, εκμεταλλεύσεις και υπογραφές IDP, τη βαθμολόγηση των *αδυναμιών*, τη συνολική παραμετροποίηση του συστήματος, τη διαδικασία ενημέρωσης του συστήματος, κτλ. Η τρέχουσα έκδοση του συστήματος ανανεώνεται αυτόματα από το Διαδίκτυο, μέσω κατάλληλων αναλυτών (parsers) XML[21].

[21] eXtensive Markup Language

5.2.3.2. Επίπεδο συλλογής και εξόρυξης πληροφοριών

Το Επίπεδο Συλλογής και Εξόρυξης Πληροφοριών (Feature Gathering and Extraction Layer) του IRIS συλλέγει δεδομένα από διάφορες πηγές και εξάγει τις κατάλληλες πληροφορίες. Στο επίπεδο αυτό βρίσκονται τα παρακάτω δομοστοιχεία:

- Το *Δομοστοιχείο Συλλογής Πληροφοριών Αδυναμιών Ασφάλειας (Vulnerability Gathering Module - VGM)* συλλέγει πληροφορίες από διάφορες πηγές (όπως ιστοτόπους, λίστες κατασκευαστών και αποτελέσματα –σε μορφότυπο HTML[22]- από εργαλεία VA). Οι πληροφορίες αυτές, μέσω αναλυτών XML, κανονικοποιούνται και ταξινομούνται με βάση το αναγνωριστικό CVE,

- Το *Δομοστοιχείο Βαθμολόγησης Αδυναμιών (Vulnerability Scoring Module - VSM)* υπολογίζει το βαθμό (κατά το πρότυπο σύστημα CVSSv2) όλων των καταχωρήσεων CVE που παρέχονται από το VGM,

- Το *Δομοστοιχείο Συλλογής Πληροφοριών Υπογραφών (Signature Gathering Module - SGM)* συλλέγει και κανονικοποιεί, μέσω ενός αντίστοιχου αναλυτή XML, τις υπογραφές από τη βάση του συστήματος IDP,

- Το *Δομοστοιχείο Αποθήκευσης Εκμεταλλεύσεων (Exploit Storage Module - ESM)* συλλέγει και ταξινομεί (επίσης, μέσω ενός αντίστοιχου αναλυτή XML) κώδικα αθέμιτης *εκμετάλλευσης* από το Διαδίκτυο και άλλες πηγές.

5.2.3.3. Επίπεδο τοπολογικής ανάλυσης επιθέσεων

Το *Επίπεδο Κατασκευής Αντιστοιχιών σε Πραγματικό Χρόνο* εκτελεί μία αντιστοίχηση μεταξύ *αδυναμιών*, ευπαθειών και *υπογραφών* (σε πραγματικό χρόνο), καθώς και την κατασκευή των μονοπατιών επίθεσης. Περιλαμβάνει τα ακόλουθα δομοστοιχεία:

[22] Hyper Text Markup Language

- Το *Δομοστοιχείο Συσχέτισης Αδυναμιών (Vulnerability Correlation Module - VCM)* που συσχετίζει πληροφορίες *αδυναμιών* και καταχωρίσεις CVE με αντίστοιχες λίστες κατασκευαστών και άλλες πηγές,

- Το *Δομοστοιχείο Συσχέτισης Εκμεταλλεύσεων και Αδυναμιών (Vulnerability Exploit Correlation Module - VECM)* το οποίο συσχετίζει καταχωρίσεις CVE με εκμεταλλεύσεις, αναλύοντας συγκεκριμένα χαρακτηριστικά μέσα στον κώδικα αθέμιτης *εκμετάλλευσης*,

- Το *Δομοστοιχείο Συσχέτισης Υπογραφών και Εκμεταλλεύσεων (Signature Exploit Correlation Module - SECM)* που συσχετίζει IDP υπογραφές με εκμεταλλεύσεις που συλλέγονται από το EGM,

- Το *Δομοστοιχείο Μονοπατιού Επίθεσης και Αντιμετώπισης (Attack and Response Path - ARPM)* παρέχει τη συσχέτιση μεταξύ των VECM και SECM, καθώς και την κατασκευή μονοπατιών επίθεσης και αντιμετώπισης.

5.2.3.4. Επίπεδο κατασκευής και εφαρμογής πολιτικών

Το *Επίπεδο Κατασκευής και Εφαρμογής Πολιτικών* χρησιμοποιεί τις παραπάνω πληροφορίες ώστε να ορίσει και να κατασκευάσει κατάλληλες πολιτικές αντιμετώπισης που έχουν ως στόχο τα αντίστοιχα μονοπάτια επίθεσης του ARPM. Περιλαμβάνει τα παρακάτω δομοστοιχεία:

- Τα *Δομοστοιχεία Αποθήκευσης (Storage Modules)*, τα οποία χρησιμοποιούνται για να αποθηκεύσουν τα αποτελέσματα των VGM, SGM και EGM (στις βάσεις EIB, SIB και EIB, αντίστοιχα),

- Τη *Μηχανή Συσχέτισης (Correlation Engine), η οποία* χρησιμοποιεί τις πληροφορίες που παρέχουν τα VCM, VECM και SECM, ως είσοδο, προκειμένου να τις συσχετίσει, καθώς και να εξαλείψει τυχόν διπλές ή πολλαπλές εγγραφές (ή να συμπληρώσει ελλιπείς εγγραφές, σε ό,τι αφορά *αδυναμίες* και υπογραφές),

- Τα *Εργαλεία Κατασκευής Πολιτικών (Policy Construction Tools), τα οποία* παρέχουν την απαραίτητη διεπαφή στον διαχειριστή του IRIS, προκειμένου να ορίσει και να προσαρμόσει τις πολιτικές αντιμετώπισης που αντιστοιχούν σε κάθε μονοπάτι επίθεσης, καθώς και των ενεργειών αντιμετώπισης σε συγκεκριμένους συναγερμούς εισβολής,

- Τα *Εργαλεία και τους Κανόνες Επίλυσης Συγκρούσεων (Conflict Resolution Rules and Tools)* που χρησιμοποιούνται για να επιλύουν προβλήματα και συγκρούσεις στις πολιτικές του IRIS και να παρέχουν πολιτικές χωρίς λάθη. Για παράδειγμα, ως σύγκρουση θεωρείται η παραλλαγή μιας γνωστής επίθεσης η οποία κατασκευάζει διαφορετικά μονοπάτια επίθεσης (με αποτέλεσμα διαφορετικές πολιτικές αντιμετώπισης),

- Το *Δομοστοιχείο Ανάλυσης Συνέπειας (Consistency Analysis Module)*, το οποίο χρησιμοποιείται για να ελέγξει την πληρότητα μιας πολιτικής, σε ό,τι αφορά στην ολοκλήρωση των αντιστοιχιών μεταξύ *αδυναμιών*, *εκμεταλλεύσεων* και *υπογραφών*, καθώς και την «ηλικία» των πληροφοριών που τηρούνται στις βάσεις του συστήματος (μέσω της διαδικασίας ενημέρωσης του συστήματος), κτλ,

- Το *Δομοστοιχείο Εφαρμογής Πολιτικής (Policy Enforcement Module - PEM)*, το οποίο παρέχει το σύνολο των *υπογραφών* IDP ή/και τους αντίστοιχους κανόνες που πρέπει να προστεθούν στην πολιτική του IDP προκειμένου να αντιμετωπίσουν ένα μονοπάτι επίθεσης. Στην παρούσα υλοποίηση του συστήματος, αυτό επιτυγχάνεται με την παροχή των κανόνων που πρέπει να ενεργοποιηθούν στο IDP σύστημα αναφοράς Snort. Σε επόμενο κεφάλαιο παρουσιάζεται μια τυπική γλώσσα Αντιμετώπισης Περιστατικών, η οποία βασίζεται σε μια άλγεβρα συμφραζομένων (context algebra) που συμπεριλαμβάνει τα μέλη που συμμετέχουν στην εταιρική διαδικασία, όπως ορίζονται στο (Mitropoulos, Patsos, & Douligeris, 2006) και στην ενότητα 3.2.1, με απλουστευμένους κανόνες που αντιστοιχούν σε ενέργειες αντιμετώπισης περιστατικών.

5.2.3.5. Επίπεδο υποδομής

Το Επίπεδο Υποδομής παρέχει τις απαραίτητες διεπαφές για την αλληλεπίδραση με την υποκείμενη πλατφόρμα. Παρέχει την υποστήριξη για την ομαλή λειτουργία του IRIS, σε ό,τι αφορά στο λειτουργικό σύστημα, την αποθήκευση, το δίκτυο και τις τρίτες-εφαρμογές. Συμπεριλαμβάνει τα ακόλουθα δομοστοιχεία:

- Το *Δομοστοιχείο Υποστήριξης Εκτελέσιμου Περιβάλλοντος* που εξυπηρετεί την αλληλεπίδραση του IRIS με το λειτουργικό σύστημα και το περιβάλλον όπου εκτελείται το IRIS,

- Το *Δομοστοιχείο Υποστήριξης Δικτύου* εξυπηρετεί τις δικτυακές δυνατότητες που απαιτούνται τόσο για τις εσωτερικές επικοινωνίες των δομοστοιχείων του IRIS όσο και για τις εξωτερικές επικοινωνίες του IRIS (π.χ. συστήματα IDP, εργαλεία VA, Διαδίκτυο, κτλ.),

- Το *Δομοστοιχείο Διαχείρισης Σχεσιακών Βάσεων Δεδομένων (Relational DataBase Management Systems – RDBMS)* που παρέχει τις απαραίτητες λειτουργίες βάσης δεδομένων στο IRIS, σε ό,τι αφορά στην επερώτηση (query) των εσωτερικών βάσεων του συστήματος (VIB, SIB και EIB), καθώς και την αποθήκευση πληροφοριών σε αυτές.

5.2.3.6. Υποστηρικτικά εργαλεία

Το IRIS υποστηρίζεται από ένα σύνολο εργαλείων για την αποτελεσματική διαχείριση, επίβλεψη και λογιστική πόρων της λειτουργίας του. Αναλυτικότερα από:

- Τα Εργαλεία Επίβλεψης Κατάστασης (System health monitoring tools), που παρέχουν ένα σύνολο εργαλείων για την επίβλεψη του συνόλου της λειτουργίας του IRIS, καθώς και κάθε δομοστοιχείου του συστήματος.

- Τα Εργαλεία Επίβλεψης και Λογιστικής Πόρων (Auditing and Accounting Tools), που δημιουργούν και αποθηκεύουν αρχεία ελέγχου και καταγραφής και παρέχουν αναφορές σε σχέση με τη λειτουργία του IRIS. Επιπλέον,

συμπεριλαμβάνονται εργαλεία ελέγχου πρόσβασης για τις αντίστοιχες αιτήσεις μεταξύ των δομοστοιχείων του συστήματος.

- Τα Εργαλεία Διαχείρισης (Management tools), που υποστηρίζουν τις λειτουργίες του IRIS, σε σχέση με την ενημέρωση των δομοστοιχείων του συστήματος, τις καταχωρίσεις σχετικά με τις *αδυναμίες*, τις εκμεταλλεύσεις και τις υπογραφές, τις εναλλακτικές εκδόσεις δομοστοιχείων (π.χ. ανανεωμένη έκδοση της μηχανής συσχέτισης), καθώς και με την υποστήριξη άλλων πηγών πληροφορίας (π.χ. διαλειτουργικότητα με νέα εργαλεία VA και νέα συστήματα IDP).

- Τα εργαλεία συστήματος (System tools), που παρέχουν τις απαραίτητες αναφορές σχετικά με τις πολιτικές αντιμετώπισης, την κατασκευή (σε πραγματικό χρόνο) μονοπατιών επίθεσης και αντιμετώπισης, κτλ.

Τέλος, το IRIS υποστηρίζεται από κατάλληλα διαχειριστικά εργαλεία που εγγυώνται τις απαραίτητες ενημερώσεις ασφάλειας που απαιτούν τα διαφορετικά δομοστοιχεία του συστήματος, καθώς και την υποστήριξη προϊόντων τρίτων κατασκευαστών για τη μελλοντική επέκταση των λειτουργιών του συστήματος.

5.2.4. Παρουσίαση πρωτοτύπου

Το δομοστοιχείο *VGM* ελέγχει συνεχώς και συλλέγει πληροφορίες σχετικές με *αδυναμίες* ασφάλειας από πηγές που έχουν ορισθεί και επιλεχθεί εξαρχής. Στο σύστημα μπορεί να δηλωθεί μια μεγάλη λίστα από τέτοιες πηγές, ενώ –παράλληλα- το σύστημα μπορεί να λάβει ως είσοδο αρχεία που περιλαμβάνουν τα αποτελέσματα αποτίμησης *αδυναμιών* ασφάλειας από αντίστοιχα εργαλεία VA (στην περίπτωσή μας επιλέχθηκε και χρησιμοποιείται το εργαλείο αναφοράς Nessus) για μια συγκεκριμένη υποδομή.

Οι πληροφορίες αυτές μεταδίδονται στο *VSM*, με σκοπό τη βαθμολόγηση (κατά το πρότυπο CVSSv2) κάθε μιας από τις *αδυναμίες* που συλλέχθηκαν από το *VGM* (με τον τρόπο που προαναφέρθηκε, εφόσον οι *αδυναμίες* έχουν κανονικοποιηθεί και ταξινομηθεί κατά CVE). Το IRIS είναι παραμετροποιημένο ώστε να αναζητεί τη βαθμολόγηση της συγκεκριμένης *αδυναμίας* σε αντίστοιχα εργαλεία στο Διαδίκτυο.

Στη συνέχεια, το *VCM* παρέχει την πλούσια εικόνα για τη συγκεκριμένη *αδυναμία*, παρέχοντας τη βαθμολογία, καθώς και πληροφορίες από σχετικές λίστες κατασκευαστών ή/και συντονιστικά κέντρα. Το αποτέλεσμα αποθηκεύεται στη *VIB*, ενώ οι πληροφορίες μεταδίδονται στη *Μηχανή Συσχέτισης*.

Παράλληλα με τα παραπάνω, αντίστοιχες λειτουργίες (σχετικές με εκμεταλλεύσεις) συλλέγονται από το *EGM*, από πηγές που καθορίστηκαν στην αρχική παραμετροποίηση του IRIS. Επιπροσθέτως, το συγκεκριμένο δομοστοιχείο ελέγχει τις πηγές αυτές για πιθανές ανανεώσεις. Το δομοστοιχείο *SGM*, από την άλλη πλευρά, συλλέγει αντίστοιχες πληροφορίες για υπογραφές IDP από αντίστοιχες πηγές. Οι παραπάνω πληροφορίες αποθηκεύονται, αντίστοιχα, στις βάσεις *EIB* και *SIB*, ενώ στη συνέχεια μεταβιβάζονται στη Μηχανή Συσχέτισης, η οποία τις ταξινομεί (εξαρχής) σύμφωνα με το CVE αναγνωριστικό τους. Στην περίπτωση που μια *εκμετάλλευση* ή μια *υπογραφή* αντιστοιχεί σε περισσότερα από ένα CVE αναγνωριστικά, τότε η *Μηχανή Συσχέτισης* ανακτά τις υπόλοιπες εγγραφές CVE από τη βάση VIB, ενώ ένας έλεγχος διασταύρωσης πραγματοποιείται από τη *Μηχανή Ανάλυσης Συνέπειας*, καθώς και τα *Δομοστοιχεία Ανάλυσης Συγκρούσεων* (επαναλαμβανόμενες αντίστροφες αναζητήσεις στις βάσεις *VIB*, *EIB* και *SIG*, αντίστοιχα).

Όταν δεν απαιτούνται περισσότερες αναζητήσεις, η Μηχανή Συσχέτισης μεταβιβάζει τις πληροφορίες στο *Δομοστοιχείο Κατασκευής Μονοπατιών Επίθεσης και Αντιμετώπισης*, το οποίο, εκτός του ότι παρέχει την τοπολογική ανάλυση της *αδυναμίας*, εκτελεί –πρακτικά- και το ρόλο μιας βάσης γνώσεως για μελλοντικές αναζητήσεις των ίδιων πληροφοριών. Οι ίδιες πληροφορίες μεταβιβάζονται, επίσης, στο Δομοστοιχείο Εφαρμογής Πολιτικής, το οποίο παρέχει τις απαραίτητες υπογραφές που αντιστοιχούν στο συγκεκριμένο μονοπάτι, ήτοι την πολιτική αντιμετώπισης.

Στην παρούσα έκδοση, το IRIS έχει τη δυνατότητα συλλογής πληροφοριών από 18 διαφορετικές πηγές κατασκευαστών και 12 διαφορετικά συμβουλευτικά κέντρα για περισσότερες από 32000 *αδυναμίες* που διατηρεί στη βάση VIB. Το *SGM* επικοινωνεί, με

επιτυχία, με το ανοικτού-κώδικα σύστημα IDP Snort[23], καθώς και με ένα ακόμη (εμπορικού χαρακτήρα) σύστημα IDP, ενώ η βάση *SIB* διατηρεί περισσότερες από 15499 διαφορετικές υπογραφές. Τέλος, το *EGM* συλλέγει πληροφορίες για εκμεταλλεύσεις και αντίστοιχο κώδικα από 3 διαφορετικές πηγές, διατηρώντας περισσότερες από 1969 διαφορετικές εκμεταλλεύσεις στη βάση *SIG*. Αντίστοιχα, το δομοστοιχείο *ARP* διατηρεί 289 διαφορετικές πολιτικές αντιμετώπισης που αντιστοιχούν σε 289 μοναδικά μονοπάτια επίθεσης, τα οποία –με τη σειρά τους- αντικατοπτρίζουν 1097 επιβεβαιωμένες (από τους αντίστοιχους κατασκευαστές) *αδυναμίες* για 1338 διαφορετικές CVE καταχωρήσεις.

Χρειάζεται να σημειωθεί πως, τα παραπάνω στοιχεία, μεταβάλλονται (αυξάνονται) με τις –πρακτικά- καθημερινές ενημερώσεις των βάσεων *VIB, EIB & SIG* του IRIS.

5.2.5. Παρουσίαση λειτουργίας

Η λειτουργία του IRIS παρουσιάζεται μέσα από μια μελέτη περίπτωσης, όπου επιδεικνύονται οι βασικές λειτουργίες της τρέχουσας έκδοσης του IRIS, μέσω ανάλυσης μιας αναφοράς ασφάλειας από το εργαλείο Nessus, της εύρεσης του αντίστοιχου κώδικα αθέμιτης *εκμετάλλευσης*, καθώς και των σχετικών *υπογραφών* του IDP συστήματος Snort μιας συγκεκριμένης υποδομής.

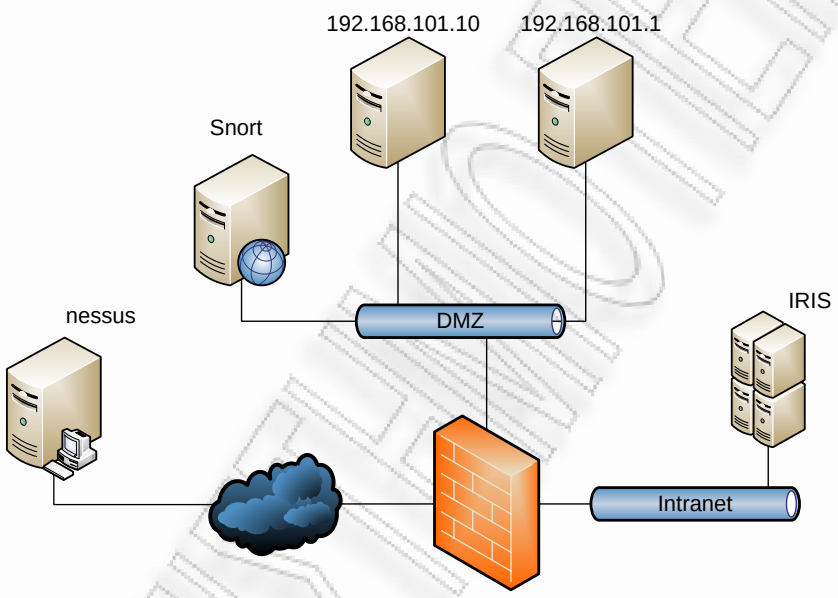
Επίσης, παρουσιάζονται οι λειτουργίες των μηχανών συσχέτισης του IRIS, καθώς και η κατασκευή του μονοπατιού επίθεσης για το συγκεκριμένο συνδυασμό *αδυναμιών/εκμεταλλεύσεων*. Τέλος, παρουσιάζονται οι κανόνες του Snort που απαρτίζουν την πολιτική αντιμετώπισης, οι οποίοι δημιουργούνται αυτόματα από το IRIS.

Η διαμόρφωση της εργαστηριακού δικτύου στο οποίο εξετάζεται η λειτουργία του IRIS απαιτεί το διαχωρισμό του σε τρεις (3) διαφορετικές ζώνες με τη χρήση ενός τείχους προστασίας (βλ. Σχήμα 5-4). Οι ζώνες αυτές είναι:

---

[23] Το Snort χρησιμοποιείται ως σύστημα αναφοράς τόσο από τη διεθνή ερευνητική κοινότητα, όσο και από τη βιβλιογραφία αλλά και τη βιομηχανία.

- Ζώνη Ενδοδικτύου (Intranet Zone), στην οποία λειτουργεί το IRIS,
- Ζώνη Διαδικτύου (Internet Zone), που συνδέει το ενδοδίκτυο με το Διαδίκτυο και στην οποία λειτουργεί το εργαλείο Nessus
- Αποστρατικοποιημένη Ζώνη (DeMilitarized Zone – DMZ), η οποία περιλαμβάνει τους δύο σταθμούς που εξετάζονται από το Nessus (διευθύνσεις IP 192.168.101.10 και 192.168.101.1).



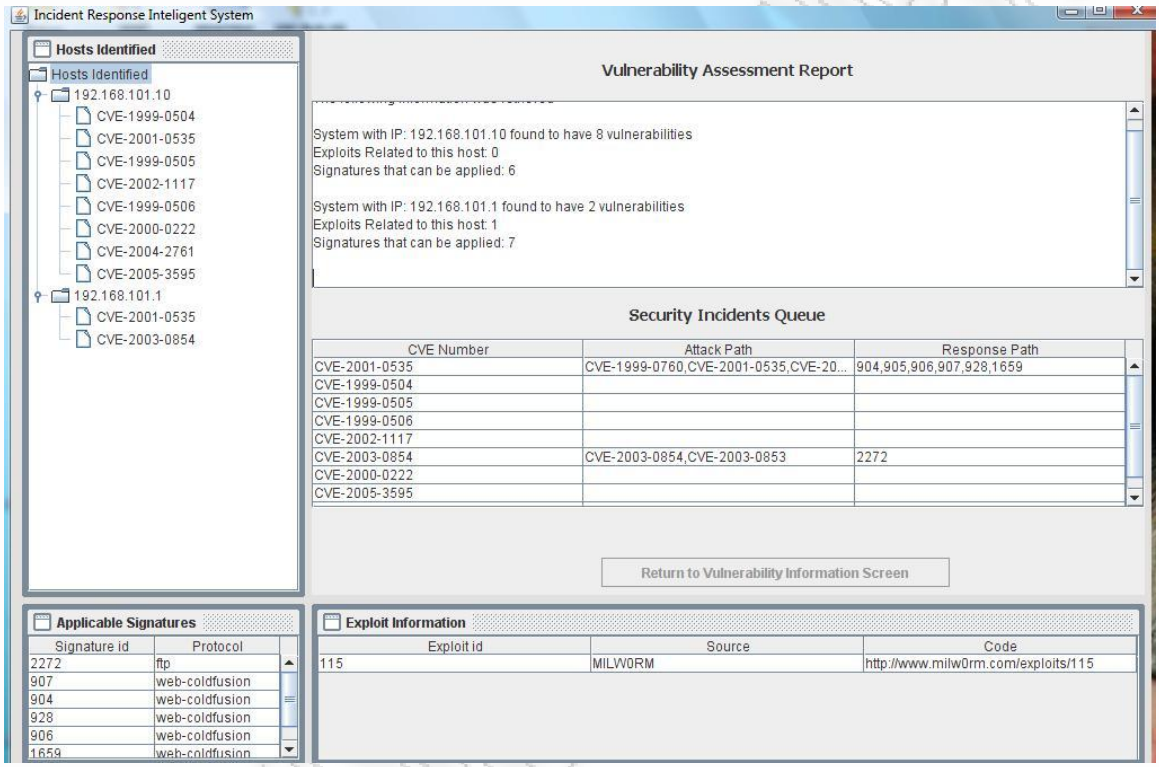
Σχήμα 5-4: Διαμόρφωση Εργαστηριακού Δικτύου

Στην DMZ τοποθετείται, επίσης, το σύστημα Snort, χωρίς προκαθορισμένη πολιτική (σε ό,τι αφορά σε ενεργοποιημένες υπογραφές στη συγκεκριμένη ζώνη). Ωστόσο, το δομοστοιχείο SGM έχει συλλέξει, από τη βάση του Snort, όλες τις υπογραφές που διαθέτει μέχρι εκείνη τη στιγμή το σύστημα.

Αρχικά, το εργαλείο Nessus αναφέρει την ύπαρξη μιας σειράς αδυναμιών για τα εν λόγω συστήματα, όπως δείχνει η Εικόνα 5.1. Χάριν ευκολίας, επιλέγεται η αδυναμία με αναγνωριστικό CVE-2003-0854.

Η αναφορά συλλέγεται από το VGM και μεταβιβάζεται στο VSM, απ΄όπου είναι διαθέσιμες οι (CVSS) τιμές για κάθε αδυναμία που αναφέρει το Nessus.

Ο διαχειριστής του IRIS μπορεί να αναζητήσει περισσότερες πληροφορίες για τον ακριβή κώδικα αθέμιτης *εκμετάλλευσης* που παρέχει το IRIS από το κατάλληλο κουμπί της κονσόλας του συστήματος.



Εικόνα 5-1: Βαθμολόγηση *αδυναμιών*, περιγραφή και αναζήτηση στη βάση SIG

Ο διαχειριστής του IRIS έχει στη διάθεσή του, επίσης, μια μεγάλη λίστα από αναφορές και συμβουλές για τη συγκεκριμένη *αδυναμία* (όπως δείχνει η Εικόνα 5-2), η οποία είναι –ουσιαστικά- το αποτέλεσμα της λειτουργίας του δομοστοιχείου VCM. Με τη χρήση των πληροφοριών αυτών, ο διαχειριστής του IRIS μπορεί να εξαγάγει άμεσα συμπεράσματα για τα χαρακτηριστικά της συγκεκριμένης *αδυναμίας*.

Παράλληλα, το δομοστοιχείο SECM συσχετίζει τις πληροφορίες αυτές με τη βάση του Snort και αναφέρει πως με τη συγκεκριμένη *αδυναμία* και *εκμετάλλευση* σχετίζεται η *υπογραφή* με αναγνωριστικό (Snort ID) 2272. Ωστόσο, η συγκεκριμένη *υπογραφή*

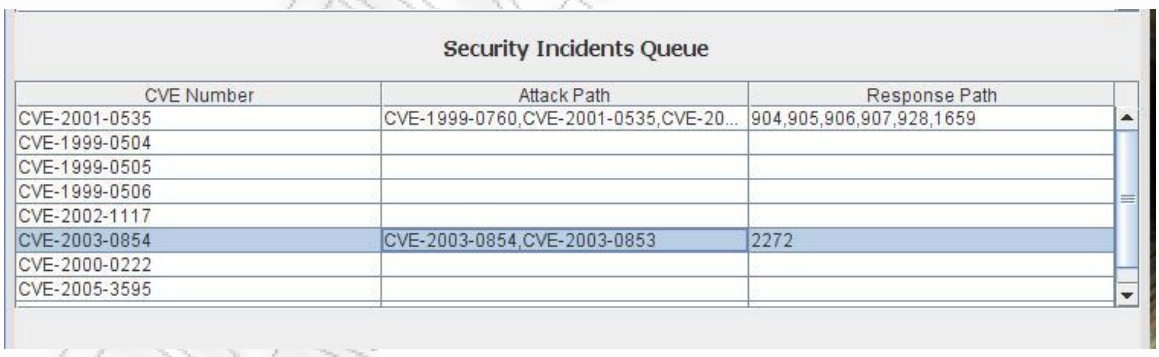
σχετίζεται με μία ακόμη *αδυναμία* (με αναγνωριστικό CVE-2003-0854) που είναι ευάλωτη στον παραπάνω κώδικα *εκμετάλλευσης*.

Source	URL
DEBIAN	http://www.debian.org/security/2005/dsa-705
SECUNIA	http://secunia.com/advisories/17069
MANDRAKE	http://www.mandriva.com/security/advisories?na...
REDHAT	http://www.redhat.com/support/errata/RHSA-2003...
FULLDISC	http://lists.grok.org.uk/pipermail/full-disclosure/20...
CONECTIVA	http://distro.conectiva.com.br/atualizacoes/?id=a&...
TURBO	http://www.turbolinux.com/security/TLSA-2003-60.txt
REDHAT	http://www.redhat.com/support/errata/RHSA-2003...
CONFIRM	http://support.avaya.com/elmodocs2/security/ASA-...
CONECTIVA	http://distro.conectiva.com.br/atualizacoes/?id=a&...
IMMUNIX	http://www.securityfocus.com/advisories/6014
SECUNIA	http://secunia.com/advisories/10126
MISC	http://www.guninski.com/binls.html
MILW0RM	http://www.milw0rm.com/exploits/115

Close

Εικόνα 5-2: Παραπομπές σε σχετικές πηγές πληροφοριών για την αδυναμία CVE-2003-0854

Τέλος, το IRIS απεικονίζει τους απαραίτητους κανόνες αντιμετώπισης της συγκεκριμένης *αδυναμίας* στην κονσόλα του, όπως δείχνει η Εικόνα 5-3 ως το αποτέλεσμα του Δομοστοιχείου Μονοπατιού Επίθεσης και Αντιμετώπισης.



Security Incidents Queue

CVE Number	Attack Path	Response Path
CVE-2001-0535	CVE-1999-0760,CVE-2001-0535,CVE-20...	904,905,906,907,928,1659
CVE-1999-0504		
CVE-1999-0505		
CVE-1999-0506		
CVE-2002-1117		
CVE-2003-0854	CVE-2003-0854,CVE-2003-0853	2272
CVE-2000-0222		
CVE-2005-3595		

Εικόνα 5-3: Συσχετισμένες υπογραφές Snort και πολιτικές αντιμετώπισης

5.2.6. Πλεονεκτήματα του IRIS στην αντιμετώπιση περιστατικών

Το IRIS αποτελεί ένα σύστημα για χρήση σε εταιρικά περιβάλλοντα, κατά τη διαδικασία αντιμετώπισης περιστατικών ασφάλειας. Οι κύριες δυνατότητες του συγκεκριμένου

συστήματος είναι η συλλογή, κανονικοποίηση, συσχέτιση και ενοποίηση πληροφοριών σχετικά με *αδυναμίες*, εκμεταλλεύσεις και υπογραφές IDP. Με το δεδομένο αυτό, το IRIS μπορεί να χρησιμοποιείται ως σύστημα αναφοράς όταν απαιτούνται τέτοιες πληροφορίες κατά τη διάρκεια αντιμετώπισης περιστατικών ασφάλειας. Όπως αναφέρθηκε σε προηγούμενες ενότητες (3.3.1 έως 3.3.6), οι πρότυπες μεθοδολογίες αντιμετώπισης περιστατικών αποτελούνται από έξι (6) διακριτές φάσεις (προετοιμασία, αναγνώριση, περιορισμός, εξάλειψη, ανάκαμψη και επακόλουθα), όπως επίσης περιγράφονται στα (NIST, 2004) και (Mitropoulos, Patsos, & Douligeris, 2006). Το IRIS μπορεί –με επιτυχία- να χρησιμοποιηθεί στις περισσότερες από τις φάσεις αυτές.

Ειδικότερα, κατά τη φάση προετοιμασίας, η χρήση του συστήματος IRIS μπορεί να εξυπηρετήσει τους διαχειριστές συστημάτων και δικτύων ώστε να παραμετροποιούν κατάλληλα τα εργαλεία VA και τα συστήματα IDP, ελαχιστοποιώντας πιθανές παραβλέψεις που οδηγούν σε ψευδοαρνητικά αποτελέσματα στα εργαλεία VA (αποτυχία ανεύρεσης μιας πραγματικής *αδυναμίας*) και σε ψευδοθετικά αποτελέσματα στα συστήματα IDP (ανεύρεση μιας μη-πραγματικής επίθεσης).

Κατά τη διάρκεια της αναγνώρισης, όταν ένα περιστατικό αναγνωρίζεται από την υποδομή ασφάλειας του οργανισμού, ο διαχειριστής του IRIS μπορεί να βρει συγκεντρωμένες πληροφορίες που αφορούν στο περιστατικό (ήτοι τις *αδυναμίες* που εκμεταλλεύτηκε ένας επιτιθέμενος προκειμένου να προκαλέσει το συγκεκριμένο περιστατικό) στις βάσεις του συστήματος (VIB, EIB και SIG αντίστοιχα). Επίσης, μπορεί να αξιολογήσει τη σημασία της εκμεταλλευθείσας *αδυναμίας* (μέσα από το αποτέλεσμα κατά CVSS που παρέχει το IRIS), καθώς και την προτεραιότητα που απαιτεί η αντιμετώπισή της (κοιτάζοντας αν η *αδυναμία* είναι επιβεβαιωμένη, αν υπάρχουν πραγματικές εκμεταλλεύσεις, καθώς και αν τα συστήματα IDP είναι κατάλληλα παραμετροποιημένα ώστε να αντιμετωπίζουν τη συγκεκριμένη *αδυναμία*). Οι δύο αυτοί παράγοντες, σημασία και προτεραιότητα, καθορίζουν –στη φάση αυτή- τις περισσότερες από τις ενέργειες που απαιτούνται στις μεταγενέστερες φάσεις.

Κατά τη διάρκεια του περιορισμού και της εξάλειψης ενός περιστατικού, οι διαχειριστές του IRIS μπορούν να αξιολογήσουν την αποτελεσματικότητα των *υπογραφών* των

συστημάτων IDP. Περιληπτικά, όταν ένα περιστατικό αφορά σε παρείσφρηση και μπορεί να αντιμετωπιστεί με ένα σύνολο *υπογραφών* που πρέπει να ενεργοποιηθούν στα εν λόγω συστήματα, ο διαχειριστής του IRIS μπορεί –άμεσα- να βρει και να αξιολογήσει τις απαιτούμενες υπογραφές για τη συγκεκριμένη εισβολή.

Τέλος, για τις φάσεις ανάκαμψης και επακόλουθων, το IRIS παρέχει συγκεντρωμένες πληροφορίες που εξυπηρετούν την τεκμηρίωση του περιστατικού και των σχετιζόμενων τεχνικών ενεργειών που απαιτήθηκαν για την αντιμετώπισή του (π.χ. σημασία και προτεραιότητα, τεχνικά αντίμετρα (ενεργοποίηση *υπογραφών*), επαναπαραμετροποίηση συστημάτων IDP, κτλ.).

Από την άλλη πλευρά, το IRIS είναι ένα διαχειριστικό εργαλείο και δεν στοχεύει στην κατάργηση των εργαλείων VA ή των συστημάτων IDP. Στην πραγματικότητα, η απόδοση του IRIS εξαρτάται άμεσα από την αποτελεσματικότητα των μηχανισμών αυτών. Όταν ένα εργαλείο VA δεν ανιχνεύει την παρουσία μιας *αδυναμίας* ή ένα σύστημα IDP δεν παρέχει την κατάλληλη *υπογραφή*, είναι αρκετά πιθανόν πως και τα αποτελέσματα του IRIS θα είναι παραπλανητικά. Αν και δεν διαφαίνεται, προς το παρόν, κάποιος ντετερμινιστικός τρόπος να παρακαμφθεί ο συγκεκριμένος περιορισμός, στην παρούσα φάση εξετάζονται μηχανισμοί κατάλληλων αλγορίθμων ελέγχου των πληροφοριών που τροφοδοτούν το IRIS, καθώς και μηχανισμών για αυτόματη ενημέρωση και εισαγωγή τροποποιημένων *υπογραφών* IDP και ενοποίηση με μηχανισμούς αυτόματης δημιουργίας *υπογραφών*, όπως αναφέρεται στα (Newsome & Song, 2005), (Brumley, et. al., 2006) και (Cui, et. al., 2007).

Τέλος, το IRIS μπορεί να κατασκευάσει μονοπάτια επίθεσης και αντιμετώπισης χρησιμοποιώντας το αναγνωριστικό CVE ως πρωτεύον κλειδί για μία *αδυναμία*. Στην περίπτωση μιας άγνωστης (μη τεκμηριωμένης) ή μη-συμβατής με το CVE *αδυναμίας*, το IRIS δεν μπορεί –πρακτικά- να παρέχει πληροφορίες. Αν και το τελευταίο δεν είναι ένα ζήτημα που οφείλεται στην αποτελεσματικότητα του IRIS αλλά στη λειτουργία των εργαλείων VA και των συστημάτων IDP, η ολοένα και ευρύτερη υιοθέτηση του συγκεκριμένου προτύπου από κατασκευαστές, περιγραφείς *αδυναμιών* και σχετικές λίστες, αναμένεται να εξαλείψει τον συγκεκριμένο περιορισμό στο άμεσο μέλλον.

5.3. Ανακεφαλαίωση

Στην ενότητα αυτή προτάθηκε και παρουσιάστηκε το Σύστημα Ευφυούς Αντιμετώπισης Περιστατικών (Incident Response Intelligence System - IRIS) το οποίο κατανοεί το γενικότερο περιβάλλον των αδυναμιών ασφάλειας που ανακαλύπτονται από εργαλεία αυτόματης αξιολόγησης επικινδυνότητας, βαθμολογεί τη σημαντικότητά τους με προτυποποιημένο τρόπο, βρίσκει και συσχετίζει τον κώδικα εκμετάλλευσης που σχετίζεται με αυτές τις αδυναμίες και καθορίζει τις απαραίτητες υπογραφές που αντιστοιχούν στις εκμεταλλεύσεις, κατασκευάζοντας μονοπάτια αντιμετώπισης. Τα μονοπάτια αντιμετώπισης εκφράζουν δυναμικές και προσαρμοζόμενες πολιτικές συστημάτων IDP και αντιμετωπίζουν τα αντίστοιχα μονοπάτια επίθεσης.

Παρουσιάστηκε, λεπτομερειακά, η αρχιτεκτονική του IRIS καθώς και το διάγραμμα ροής των λειτουργιών, συζητήθηκαν οι λεπτομέρειες υλοποίησης και παρουσιάζεται η λειτουργία του πρωτοτύπου σε μια πραγματική μελέτη περίπτωσης. Στη συγκεκριμένη μελέτη περίπτωσης, το IRIS κατασκεύασε αυτόματα την κατάλληλη πολιτική αντιμετώπισης περιστατικών για μια δικτυακή υποδομή, συσχέτισε και αξιολόγησε τη σημασία και τον αντίκτυπο μιας σειράς αδυναμιών και του αντίστοιχου κώδικα εκμετάλλευσης.

Κεφάλαιο 6

Αξιολόγηση του εργαλείου IRIS

"To my extreme mortification, I grow wiser every day"

- **Lord Byron**

6.1. Εισαγωγή

Στο παρόν κεφάλαιο παρουσιάζονται οι μεθοδολογίες αξιολόγησης και τα αποτελέσματα των χαρακτηριστικών αλλά και της λειτουργίας του IRIS. Αρχικά, αξιολογείται η ορθότητα της υλοποίησης του IRIS σύμφωνα με την αρχιτεκτονική που παρουσιάστηκε στην ενότητα 5.2.3, ενώ παρουσιάζονται και αξιολογούνται μια σειρά από πειραματικά δεδομένα για τον έλεγχο των αποτελεσμάτων του συστήματος. Στη συνέχεια αξιολογείται η λειτουργία του IRIS σε πραγματικό περιβάλλον, στα πλαίσια μιας μελέτης περίπτωσης (case study) που πραγματοποιήθηκε σε μεγάλη ελληνική Τράπεζα. Η συγκεκριμένη μελέτη περίπτωσης αποδεικνύει, με μετρήσιμα μεγέθη, τα οφέλη της τοπολογικής ανάλυσης αδυναμιών ασφάλειας και του IRIS στην αντιμετώπιση περιστατικών ασφάλειας αλλά και την αποδοτικότερη παραμετροποίηση των συστημάτων IDP. Επίσης, παρουσιάζονται και αναλύονται οι απόψεις χρηστών που πειραματίστηκαν και εξοικειώθηκαν με το IRIS για μια πλειάδα ζητημάτων που αφορούν στο σύστημα. Τέλος, εξετάζονται και συζητούνται γενικότερα συμπεράσματα καθώς και οι περιορισμοί της αξιολόγησης.

6.2. Αξιολόγηση πληρότητας χαρακτηριστικών

Στην ενότητα 4.5 παρουσιάστηκαν οι απαιτήσεις των συστημάτων διαχείρισης ασφάλειας στην αντιμετώπιση περιστατικών ασφάλειας ενώ, παρακάτω, περιγράφονται οι τρόποι και οι τεχνικές με τις οποίες το IRIS υλοποιεί τις απαιτήσεις αυτές.

6.2.1. Ανοικτή αρχιτεκτονική και πρότυποι μορφότυποι πληροφοριών

Μία θεμελιώδης σχεδιαστική απαίτηση για τα συστήματα διαχείρισης πληροφοριών είναι η χρήση ανοικτής αρχιτεκτονικής, ώστε να εξυπηρετείται η δυνατότητα εξέλιξης του συστήματος από τρίτους αλλά και να υποστηρίζεται η επεξεργασία δεδομένων από διαφορετικές και ετερογενείς πηγές (π.χ. μηνύματα ηλεκτρονικού ταχυδρομείου, εργαλεία ασφάλειας, ιστοτόπους, κτλ).

Η αρχιτεκτονική του IRIS βασίζεται σε ευρέως διαδεδομένες πλατφόρμες ανάπτυξης και γλώσσες προγραμματισμού (γλώσσα Java, βάση δεδομένων mySQLκαι τεχνολογίες XML για τη συλλογή και επεξεργασία δεδομένων).

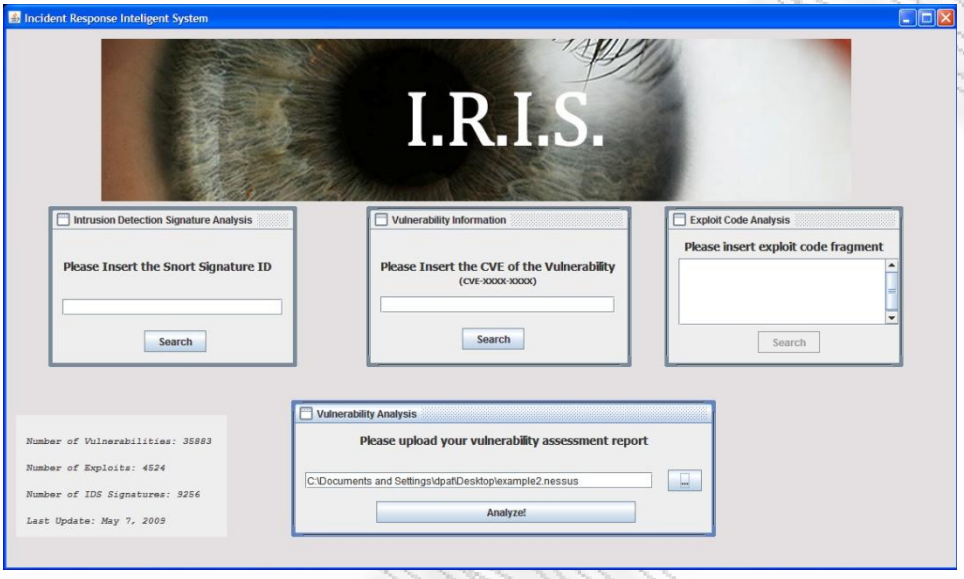
Σε ό,τι αφορά στους μορφότυπους πληροφοριών που διαχειρίζεται το IRIS, ο τρόπος επεξεργασίας των δεδομένων από τις πηγές που παρατίθενται στο Παράρτημα Α είναι μέσω κατάλληλων ρουτινών XML που συλλέγουν και κανονικοποιούν τις πληροφορίες σε ένα καλά προκαθορισμένο σχήμα. Με τον τρόπο αυτόν, οποιοσδήποτε μορφότυπος στον οποίο βρίσκεται μία πρωτογενής πληροφορία μετατρέπεται σε δομημένα σχήματα XML, τα οποία αντιστοιχούν σε πίνακες της βάσης δεδομένων. Αντίστοιχοι τρόποι συλλογής και κανονικοποίησης δεδομένων υλοποιούν την επεξεργασία πληροφοριών από τα συστήματα αποτίμησης αδυναμιών ασφάλειας, καθώς και από τα συστήματα IDP.

6.2.2. Ενοποίηση με εργαλεία αποτίμησης αδυναμιών ασφάλειας και συστήματα ανίχνευσης και αποτροπής παρεισφρήσεων

Το IRIS συνεργάζεται με το εργαλείο Nessus σε ό,τι αφορά στην αποτίμηση αδυναμιών ασφάλειας. Το Nessus θεωρείται ως εργαλείο αναφοράς, καθώς είναι από τα παλαιότερα προγράμματα αποτίμησης αδυναμιών ασφάλειας στη διεθνή κοινότητα (η διανομή του ξεκίνησε το 1998, ενώ μέχρι και σήμερα διανέμεται δωρεάν για προσωπική χρήση). Στις αξιολογήσεις της βιομηχανίας ασφάλειας, το Nessus καταλαμβάνει σταθερά την πρώτη θέση, ενώ υπάρχουν εκατοντάδες αναφορές στη βιβλιογραφία.

Από την άλλη πλευρά, το σύστημα ανίχνευσης και παρεισφρήσεων Snort αποτελεί de facto πρότυπο τόσο στην ερευνητική και ακαδημαϊκή κοινότητα, όσο και τη βιομηχανία ασφάλειας (πολλοί διεθνείς κατασκευαστές αντίστοιχων εμπορικών συστημάτων, όπως η Cisco, η IBM και η Mc Afee συνεργάζονται με τις υπογραφές του Snort). Το Snort εμφανίστηκε στην κοινότητα ασφάλειας το 1999, ενώ μέχρι και σήμερα διανέμεται δωρεάν, κερδίζοντας μεγάλη απήχηση από τους ειδικούς ασφάλειας.

Το IRIS συνεργάζεται με τα δύο προαναφερθέντα συστήματα (Nessus & Snort), επιτυγχάνοντας έτσι την ανταλλαγή πληροφοριών ασφάλειας που αφορούν σε αδυναμίες ασφάλειας και υπογραφές IDP,αντίστοιχα, όπως δείχνει και η Εικόνα 6-1.



Εικόνα 6-1: Ενοποίηση του IRIS με τα εργαλεία Nessus και Snort

Επίσης, η αρχιτεκτονική του IRIS –εκ κατασκευής- παρέχει τη δυνατότητα συλλογής και επεξεργασίας οποιουδήποτε παρεμφερούς εργαλείου, με δεδομένο ότι το εργαλείο παρέχει αναφορές σε μορφότυπο XML, όπως π.χ. το ιδιαίτερα διαδεδομένο εργαλείο αποτίμησης αδυναμιών Qualys (Qualys, 2009).

6.2.3. Βάση γνώσης & ανανέωση πληροφοριών

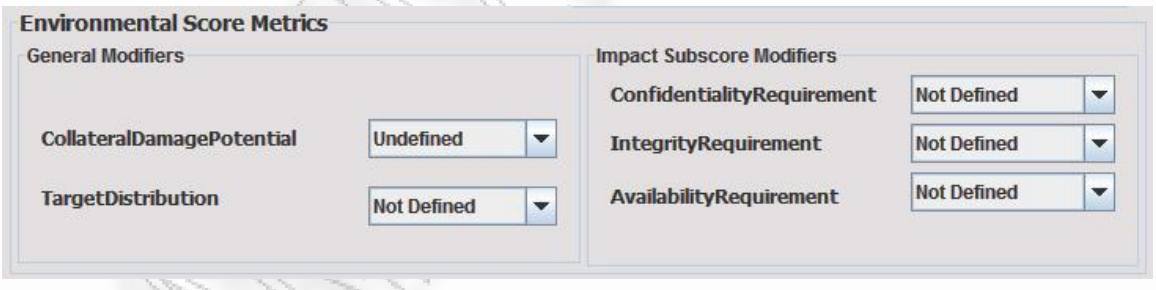
Το IRIS διαθέτει μια εκτενή βάση δεδομένων που συλλέγει από πρωτογενείς πληροφορίες ασφάλειας από πολλαπλές και ετερογενείς πηγές, τις οποίες επεξεργάζεται και αποθηκεύει σε βάσεις δεδομένων που διατηρεί (VIB, EID και SID, βλέπε ενότητα 5.2.3.2), ώστε να κατασκευάζει μια βάση γνώσης για τις δημοσιευμένες αδυναμίες ασφάλειας, τις –κατά το δυνατόν περισσότερο- ακριβείς πληροφορίες που αφορούν σε εκμεταλλεύσεις (exploits) και τις υπογραφές συστημάτων IDP που αντιστοιχούν σε αυτές. Η βάση γνώσης που διατηρεί και ανανεώνει το IRIS παρατίθεται αναλυτικά στην

ενότητα 5.2.1. Η τρέχουσα έκδοση του IRIS (Μάιος 2009), διατηρεί πληροφορίες για 35883 αδυναμίες ασφάλειας, 4524 εκμεταλλεύσεις και 9256 υπογραφές IDP.

Οι πληροφορίες αυτές συγκεντρώνονται, ανανεώνονται και αποθηκεύονται στις βάσεις του συστήματος αυτόματα, από τις αντίστοιχες τοποθεσίες που αναφέρονται στην ενότητα 5.2.1 μέσω των ρουτινών XML του IRIS, ενώ είναι δυνατή η τροποποίηση των πηγών από τις οποίες το σύστημα συλλέγει και επεξεργάζεται πληροφορίες. Το τελευταίο χαρακτηριστικό επιτρέπει τη διαμόρφωση των πηγών του IRIS σύμφωνα με τις απαιτήσεις του διαχειριστή ασφάλειας ενός Οργανισμού (π.χ. συνδρομή σε ιστοτόπους πληροφοριών, αναφορές ασφάλειας, κτλ.).

6.2.4. Χειρισμός εξαιρέσεων

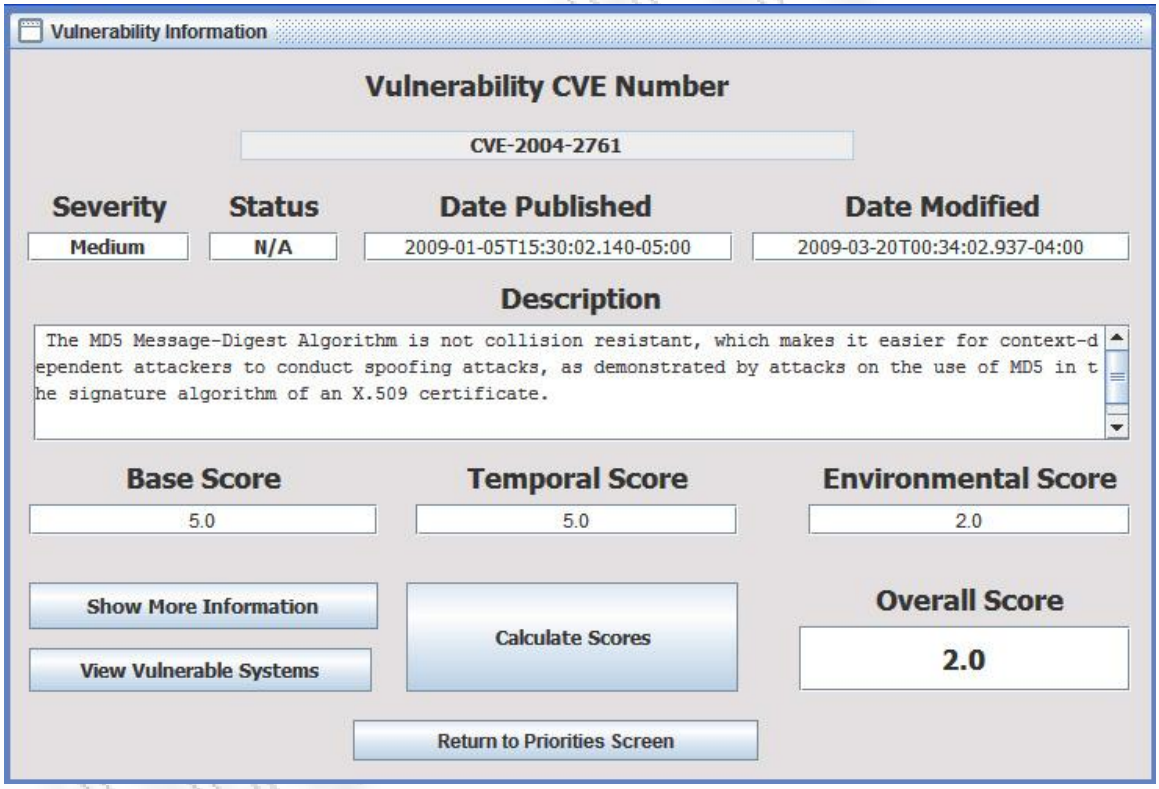
Όπως αναφέρθηκε στην ενότητα 4.5.5, η πολυπλοκότητα των εφαρμογών, σε συνδυασμό με τις ετερογενείς πλατφόρμες εισάγουν την ανάγκη του χειρισμού εξαιρέσεων σε ένα σύστημα διαχείρισης πληροφοριών ασφάλειας, ώστε να αποφεύγεται η εσφαλμένη αντιμετώπιση της εξουσιοδοτημένης δικτυακής κυκλοφορίας, μιας και οι συνέπειες είναι αρκετά πιθανόν να προκαλέσουν ανεπιθύμητα αποτελέσματα στη λειτουργία του οργανισμού (π.χ. διακοπή εξουσιοδοτημένων δικτυακών συνόδων).



Εικόνα 6-2: Χειρισμός Εξαιρέσεων στο IRIS (Βήμα 1)

Το σύστημα IRIS, μέσω της υλοποίησης του πρότυπου συστήματος βαθμολόγησης αδυναμιών ασφάλειας CVSSv2 (Mell, Scarfone, & Romanosky, 2006), παρέχει μια ειδική κονσόλα αλληλεπίδρασης του διαχειριστή ασφάλειας με το σύστημα (βλ. Εικόνα 6-2), ώστε να επιλέγει και να χαρακτηρίζει εκείνος τη συγκεκριμένη δικτυακή κυκλοφορία, με βάση τις πληροφορίες που του παρέχει το σύστημα IRIS.

Με τον τρόπο αυτό, αφενός μεν ενημερώνεται ο διαχειριστής άμεσα για τα τοπολογικά χαρακτηριστικά των αδυναμιών ασφάλειας που υπάρχουν στο περιβάλλον του και τη σημασία που αυτά τα χαρακτηριστικά έχουν τη συγκεκριμένη χρονική στιγμή, αφετέρου δε του παρέχεται από το σύστημα μια σειρά επιλογών για την αντιμετώπιση της συγκεκριμένης αδυναμίας. Έτσι, ο διαχειριστής μπορεί να βαθμολογεί τα χαρακτηριστικά της συγκεκριμένης αδυναμίας (βλ. Εικόνα 6-2) σύμφωνα με τις ιδιαιτερότητες της υποδομής του και έπειτα να επιλέγει -ή όχι- την εφαρμογή του προτεινόμενου αντίμετρου και να αποφασίζει τις περαιτέρω ενέργειες, κρίνοντας από τη συνολική βαθμολογία που αποκτά η αδυναμία μετά τη δική του αξιολόγηση (βλ. Εικόνα 6-3, όπου η αρχική βαθμολογία μιας αδυναμίας μειώνεται δραστικά μετά την αξιολόγηση του διαχειριστή ασφάλειας).

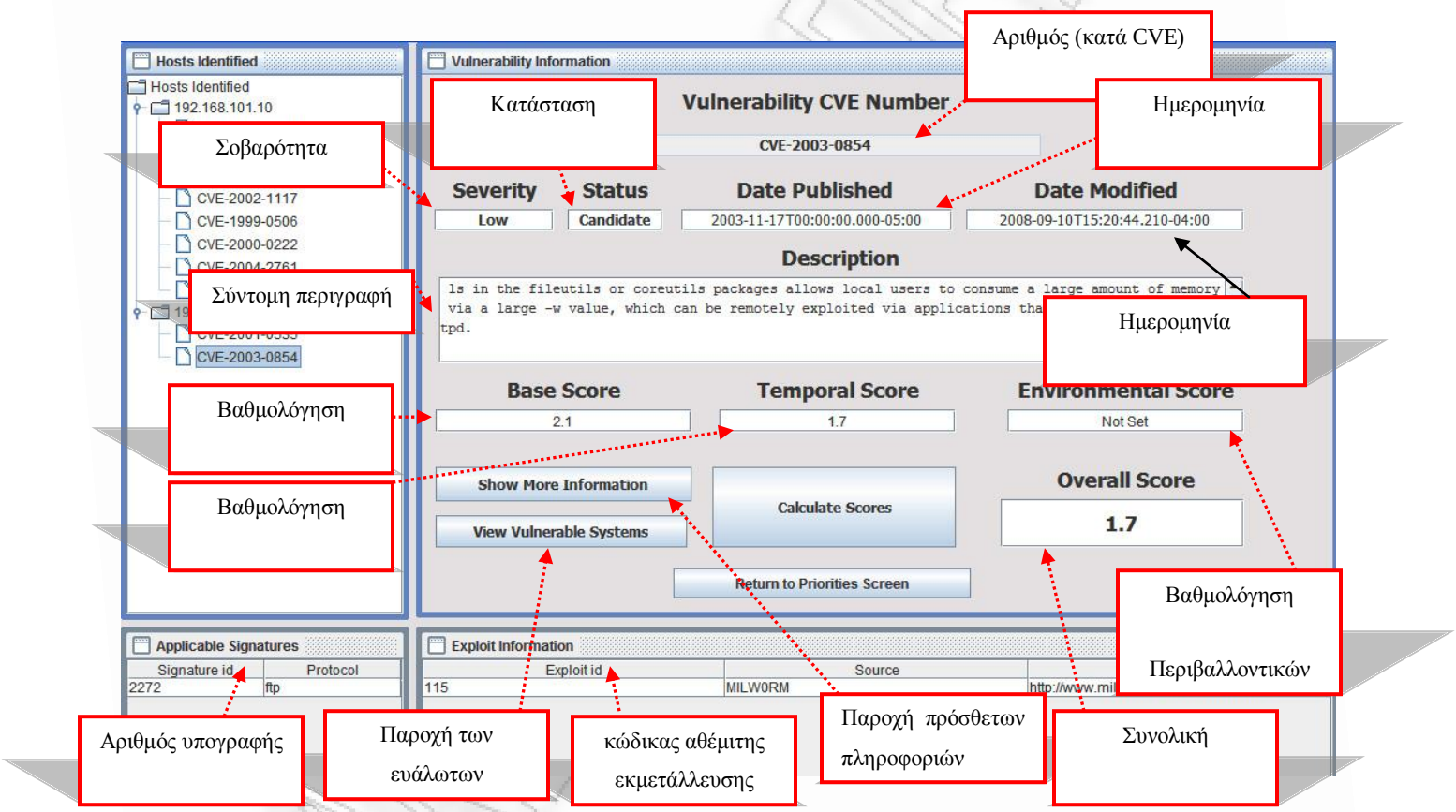


Εικόνα 6-3: Χειρισμός εξαιρέσεων στο IRIS (Βήμα 2)

6.2.5. Οπτικοποίηση πληροφορίας

Το IRIS διαθέτει μια σειρά λειτουργιών οπτικοποίησης της πληροφορίας ασφάλειας που διαχειρίζεται, παρέχοντας την «πλούσια εικόνα» για την κατάσταση της ασφάλειας της υπολογιστικής και δικτυακής υποδομής που αναλύει. Συνοπτικά, τα χαρακτηριστικά οπτικοποίησης των πληροφοριών που διαθέτει το IRIS (όπως αναφέρθηκαν στην ενότητα 4.5.6) παρουσιάζονται στην Εικόνα

Εικόνα 6-4.



Εικόνα 6-4: Οπτικοποίηση πληροφορίας

6.2.6. Συμπεράσματα

Συνοπτικά, το IRIS υλοποιεί το σύνολο των απαιτήσεων πληρότητας χαρακτηριστικών που τέθηκαν στην ενότητα 4.5, ενώ οι σχεδιαστικές απαιτήσεις και το αποτέλεσμα της υλοποίησης του IRIS παρουσιάζονται στον Πίνακα Πίνακας 6-1.

Πίνακας 6-1: Σχεδιαστικές απαιτήσεις και αποτελέσματα υλοποίησης του IRIS

Σχεδιαστική Απαίτηση	Αποτέλεσμα Υλοποίησης
Ανοικτή αρχιτεκτονική και πρότυπα μορφότυπα πληροφοριών	Επιτυχές
Ενοποίηση με εργαλεία αποτίμησης αδυναμιών ασφάλειας και συστήματα ανίχνευσης και αποτροπής παρεισφρήσεων	Επιτυχές
Βάση Γνώσης	Επιτυχές
Ανανέωση πληροφοριών	Επιτυχές
Χειρισμός Εξαιρέσεων	Επιτυχές
Οπτικοποίηση πληροφορίας	Επιτυχές

6.3. Αξιολόγηση ορθότητας αποτελεσμάτων

Η αξιολόγηση της ορθότητας των αποτελεσμάτων του IRIS έγκειται τόσο στην αξιολόγηση της ορθότητας των αποτελεσμάτων των δομοστοιχείων του, όσο και της ορθότητας των λογικών αποτελεσμάτων που υπολογίζει το εργαλείο.

Με τα δεδομένα αυτά και καθώς η ορθότητα των αποτελεσμάτων των δομοστοιχείων του αποτελεί –ουσιαστικά- αξιολόγηση των βάσεων δεδομένων που διατηρεί το σύστημα και των ρουτινών XML που εκτελεί το εργαλείο (τεχνική –ουσιαστικά- αξιολόγηση των προγραμματιστικών χαρακτηριστικών και ατελειών του IRIS), κρίνεται σκόπιμο να εστιάσει η αξιολόγηση στην ορθότητα των λογικών αποτελεσμάτων που υπολογίζει το εργαλείο.

6.3.1.1. Βαθμολόγηση ιστορικών μετρικών για αδυναμίες ασφάλειας

Τα ιστορικά μετρικά των αδυναμιών ασφάλειας υπολογίζονται σύμφωνα με το σύστημα CVSSv2, σύμφωνα με όσα απεικονίζει ο Πίνακας Πίνακας 5-3. Μιας και τα συγκεκριμένα χαρακτηριστικά των αδυναμιών μεταβάλλονται με την πάροδο του χρόνου, είναι ιδιαίτερα σημαντική η συσχέτιση των δεδομένων που διατηρεί το IRIS στις βάσεις SIB, EIB και VIB για τον υπολογισμό της τιμής των ιστορικών μετρικών των αδυναμιών.

Έτσι, για κάθε αδυναμία που επεξεργάζεται το IRIS, οι τιμές *E* (Διαθεσιμότητα κώδικα εκμετάλλευσης - Exploitability), *RL* (Είδος διορθωτικού λογισμικού - Remediation Level) και *RC* (Επίπεδο επιβεβαίωσης απόδειξης της αδυναμίας - Report Confidence) των ιστορικών μετρικών μιας αδυναμίας συμπληρώνονται αυτόματα από το IRIS, ως εξής:

- E = Λειτουργική (Functional Exploit Exists), αν το IRIS διαθέτει στη βάση EID σχετικό κώδικα αθέμιτης εκμετάλλευσης,
- RL = Τεχνοτροπία (Workaround), όταν το IRIS διαθέτει στη βάση SID σχετιζόμενες υπογραφές,
- RC = Επιβεβαιωμένη ή Μη αποδεδειγμένη (Confirmed ή Unconfirmed, αντίστοιχα), ανάλογα με την τιμή που διαθέτει η καταχώρηση CVE της συγκεκριμένης αδυναμίας.

Με τον τρόπο αυτό, μιας και η τιμή των ιστορικών μετρικών υπερισχύει της τιμής των βασικών μετρικών (σύμφωνα με το CVSSv2), το IRIS βαθμολογεί αυτόματα τη συνολική βαθμολογία των αδυναμιών που επεξεργάζεται.

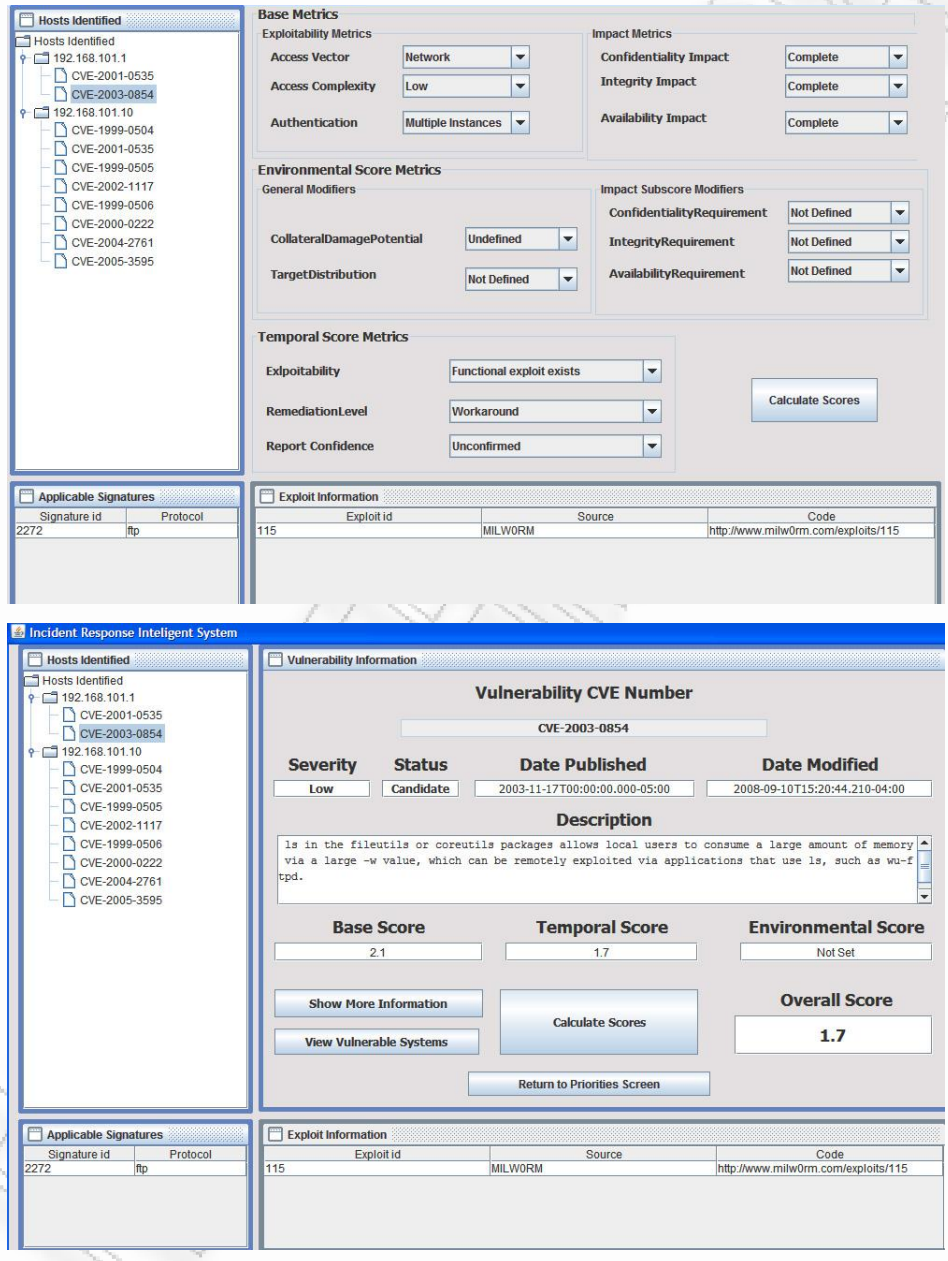
Για παράδειγμα, όπως απεικονίζει η Εικόνα 6-5, για την αδυναμία με CVE αναγνωριστικό CVE-2003-0854, υπάρχει αφενός μεν κώδικας αθέμιτης εκμετάλλευσης (με αναγνωριστικό 115), αφετέρου δε διαθέσιμες υπογραφές IDP (με αναγνωριστικό 2272) που αντιστοιχούν στη συγκεκριμένη αδυναμία. Με τον τρόπο αυτό, η βαθμολογία της συγκεκριμένης αδυναμίας μεταβάλλεται, από 2.1 (σύμφωνα με τη βαθμολογία των βασικών μετρικών) σε 1.7 (με την αυτόματη βαθμολόγηση των ιστορικών μετρικών της).

6.3.1.2. Βαθμολόγηση περιβαλλοντικών μετρικών για αδυναμίες ασφάλειας

Η βαθμολόγηση των περιβαλλοντικών μετρικών των αδυναμιών ασφάλειας που διαχειρίζεται το IRIS είναι μία από τις πλέον σημαντικές λειτουργίες στη διαδικασία αντιμετώπισης περιστατικών.

Η αξιολόγηση των περιβαλλοντικών μετρικών είναι μια καθαρά ανθρώπινη διαδικασία η οποία πραγματοποιείται από τους χρήστες του IRIS. Σύμφωνα με το CVSSv2, η ύπαρξη

τιμής περιβαλλοντικών μετρικών για μια αδυναμία υπερισχύει τόσο των βασικών όσο και των ιστορικών μετρικών μιας αδυναμίας. Με βάση αυτό το δεδομένο, η αξιολόγηση των περιβαλλοντικών μετρικών μεταβάλλει δραστικά τη σημασία ασφάλειας μιας αδυναμίας.



Εικόνα 6-5: Βαθμολόγηση ιστορικών μετρικών για αδυναμίες ασφάλειας

Επίσης, μιας και οι αποφάσεις για την αξιολόγηση των τιμών αυτών λαμβάνονται κάτω από πίεση (ιδιαίτερα όταν ένα περιστατικό είναι σε εξέλιξη), κρίνεται σκόπιμο οι επιλογές που έχει ο χρήστης να είναι απλές και κατανοητές. Η αξιολόγηση των περιβαλλοντικών μετρικών για μια αδυναμία ασφάλειας με σύντομο και κατανοητό τρόπο, επιλύει κάποιο πιθανό αντίκτυπο στο συνολικό επίπεδο της ασφάλειας μιας υποδομής λόγω αποφάσεων που παίρνονται με «τοπικά» κριτήρια (π.χ. βαθμολόγηση μιας αδυναμίας μόνο βάσει των ιστορικών ή βασικών μετρικών).

Έτσι, το IRIS προσφέρει μια σειρά επιλογών για τη βαθμολόγηση των περιβαλλοντικών χαρακτηριστικών των αδυναμιών που διαχειρίζεται, οι οποίες ισοδυναμούν –πρακτικά- με διαδικασίες αξιολόγησης ρίσκου (risk assessment). Οι επιλογές αυτές αφορούν σε όσα περιγράφει ο Πίνακας 5-4, ενώ ο υπολογισμός των τιμών γίνεται σύμφωνα με όσα περιγράφονται στο (Mell, Scarfone, & Romanosky, 2006).

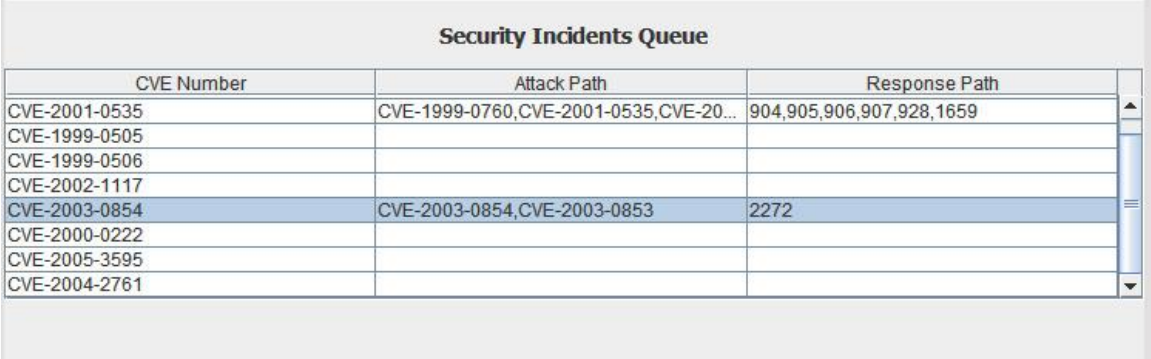
6.3.1.3. Δημιουργία μονοπατιών επίθεσης και αντιμετώπισης

Όπως αναφέρθηκε σε προηγούμενες ενότητες (ειδικότερα στις ενότητες 4.2 και 4.3), η ύπαρξη μηχανισμών ασφάλειας σε μια υποδομή μεταβάλλει δραστικά τη σημασία των αδυναμιών ασφάλειας που υπάρχουν σε αυτήν. Χαρακτηριστικά, ένα τείχος προστασίας το οποίο δεν επιτρέπει την επικοινωνία από και προς συγκεκριμένα συστήματα για μια σειρά από δικτυακές υπηρεσίες καθιστά –πρακτικά- αδύνατη την εκμετάλλευση αδυναμιών στα συγκεκριμένα συστήματα[24], για συνδέσεις που διέρχονται από το συγκεκριμένο τείχος προστασίας.

Το γεγονός αυτό μεταβάλλει δραστικά τόσο τη σημαντικότητα όσο και την έκταση πιθανών περιστατικών ασφάλειας που ξεκινούν με την εκμετάλλευση μίας ή περισσοτέρων αδυναμιών με προκαθορισμένη σειρά (μονοπάτι επίθεσης). Από την άλλη πλευρά, οι μηχανισμοί ασφάλειας στοχεύουν στο να αντιμετωπίσουν το συγκεκριμένο

[24] Δεδομένου ότι και το τείχος προστασίας δεν εμφανίζει, με τη σειρά του, άλλες αδυναμίες ασφάλειας.

μονοπάτι με αντίστοιχες υπογραφές IDP, περιορίζοντας ή εξαλείφοντας τις συνέπειες του συγκεκριμένου περιστατικού



Εικόνα 6-6: Κατασκευή μονοπατιών επίθεσης και αντιμετώπισης

Οι λειτουργίες του IRIS, μέσω των δυνατοτήτων τοπολογικής ανάλυσης αδυναμιών και βαθμολόγησης των αδυναμιών που διαχειρίζεται, παρέχουν τόσο μια λεπτομερή ανάλυση των μονοπατιών επίθεσης, όσο και των μονοπατιών αντιμετώπισης μιας συγκεκριμένης υποδομής. Για παράδειγμα, όπως χαρακτηριστικά φαίνεται στην Εικόνα 6-6, για την αδυναμία με αναγνωριστικό CVE-2003-0854, το IRIS παρέχει τόσο το μονοπάτι ασφάλειας (συνδυασμός των CVE-2003-0854 και CVE-2003-0853) όσο και το μονοπάτι αντιμετώπισης (χρήση της υπογραφής με αναγνωριστικό 2272).

6.3.2. Συμπεράσματα

Τα αποτελέσματα του IRIS βασίζονται σε μια σειρά από χαρακτηριστικά και λειτουργίες, που παρουσιάστηκαν αναλυτικά στις ενότητες 5.2.2-5.2.5. Κρίθηκε σκόπιμο να αναλυθούν περισσότερο τα χαρακτηριστικά βαθμολόγησης ιστορικών μετρικών και περιβαλλοντικών μετρικών για αδυναμίες ασφάλειας, καθώς και οι δυνατότητες δημιουργίας μονοπατιών επίθεσης και αντιμετώπισης που αποτελούν θεμελιώδεις λειτουργίες του εργαλείου. Το IRIS εφαρμόζει λογικές που εξυπηρετούν την αυτόματη συμπλήρωση των παραμέτρων που συνεισφέρουν στην αυτόματη βαθμολόγηση των αδυναμιών ασφάλειας, ενώ παρέχει άμεσα –στον διαχειριστή του συστήματος- τα μονοπάτια επίθεσης και αντιμετώπισης για τις αδυναμίες που επεξεργάζεται.

Στις επόμενες ενότητες παρουσιάζονται και αναλύονται οι λειτουργίες του IRIS σε πραγματικό περιβάλλον (τρεις διαφορετικές υποδομές), όπου αξιολογείται τόσο η ακρίβεια και η ορθότητα των υπολογισμών του συστήματος όσο και η γενικότερη συνεισφορά του εργαλείου στη διαχείριση ασφάλειας των συγκεκριμένων υποδομών.

6.4. Αξιολόγηση βελτίωσης στην παραμετροποίηση των συστημάτων IDP

Στις επόμενες ενότητες, παρουσιάζεται η πειραματική εφαρμογή ανάπτυξης συστημάτων IDP μέσω τοπολογικής ανάλυσης αδυναμιών και η αξιολόγηση της προσφοράς του IRIS στη βελτίωση της παραμετροποίησης των συστημάτων IDP. Στόχος είναι η κάλυψη ακριβώς των ίδιων αδυναμιών με τη χρήση ενός ελαχίστου πλήθους υπογραφών. Τα πειραματικά δεδομένα, αποτελούν αποτελέσματα αξιολόγησης αδυναμιών με αντίστοιχο εργαλείο (nessus), ενώ ως σύστημα αναφοράς χρησιμοποιείται το Snort (σύστημα IDP). Για την ορθότητα της αξιολόγησης της μεθόδου δεν λαμβάνονται υπόψη οι αδυναμίες που αφορούν στο λειτουργικό σύστημα της υποδομής, αλλά οι αδυναμίες που αφορούν σε δικτυακά προσφερόμενες υπηρεσίες. Στο γεγονός αυτό συμβάλλει η αποκλειστική λειτουργία του Snort ως δικτυακού συστήματος IDP.

Οι μετρήσεις πραγματοποιήθηκαν σε πραγματικά περιβάλλοντα παραγωγής, για τα παρακάτω τρία σενάρια,

- **Σενάριο 1: υποδομή διαδικτύου**, στην οποία ελέγχθηκαν συνολικά 4 δικτυακοί σταθμοί,
- **Σενάριο 2: υποδομή σταθμών εργασίας**, στην οποία ελέγχθηκαν συνολικά 22 δικτυακοί σταθμοί (σταθμοί εργασίας),
- **Σενάριο 3: υποδομή εξυπηρετητών**, στην οποία ελέγχθηκαν συνολικά 18 δικτυακοί σταθμοί (εξυπηρετητές).

Για την αξιολόγηση των αποτελεσμάτων χρησιμοποιήθηκε η έκδοση 4 του εργαλείου Nessus, και η τελευταία –κατά τη διάρκεια συγγραφής της παρούσας διατριβής- έκδοση του Snort (Ημ. Έκδοσης 2009-04-14, με MD5: `cba0c34191bfeca748ab7cba8559d8b6`).

Η μεθοδολογία αξιολόγησης –για το σύνολο των περιπτώσεων- ακολούθησε τα παρακάτω βήματα:

1. Έλεγχος αδυναμιών ασφάλειας με χρήση του Nessus
2. Απάλειψη των αδυναμιών που αφορούν σε λειτουργικό σύστημα
3. Επιλογή αδυναμιών που αφορούν σε δικτυακές υπηρεσίες
4. Ανάπτυξη συστημάτων IDP και δημιουργία πολιτικής με χρήση:
    a. Ζωνών ασφάλειας
    b. Τεχνικών τοπολογικής ανάλυσης (χρήση IRIS)
5. Καταγραφή και επεξεργασία των αποτελεσμάτων

Κρίθηκε σκόπιμο να εξεταστούν μόνο οι περιπτώσεις ανάπτυξης συστημάτων IDP και δημιουργίας πολιτικής με ζώνες ασφάλειας και τη χρήση του IRIS, ήτοι να μην εξεταστεί η περίπτωση της ανάπτυξης συστημάτων IDP με χρήση ιδεατών τοπικών δικτύων. Ο κυριότερος λόγος γι' αυτό οφείλεται στην υποκειμενικότητα που εισάγει ο ανθρώπινος παράγοντας (σχεδιαστής δικτύου), καθώς και το γεγονός πως ο διαχωρισμός ενός δικτύου με χρήση VLAN αποφασίζεται με διαφορετικά –κάθε φορά- κριτήρια.

Στα παρακάτω (Πίνακας 6-2, Πίνακας 6-3, Πίνακας 6-4) το πλήθος των υπογραφών s_1 που απαιτούνται για την πλήρη διασφάλιση των προσφερόμενων υπηρεσιών με το σύστημα Snort υπολογίζεται από τον τύπο $s_1 = \sum_{j=1}^{n} s(j) + \sum_{p=1}^{n} s(p)$, με j=0, λόγω της αποκλειστικής λειτουργίας του Snort ως συστήματος δικτύου IDP (όπου *p*, το πλήθος των δικτυακά προσφερομένων υπηρεσιών για τους *n* υπολογιστές που ελέγχθηκαν ελέχθηκαν, βλ. ενότητα 4.4.1).

6.4.1. Σενάριο 1: Υποδομή Σταθμών Διαδικτύου

Στο συγκεκριμένο σενάριο ελέγχθηκαν συνολικά 4 σταθμοί διαδικτύου από την υποδομή σταθμών Διαδικτύου μεγάλης ελληνικής Τράπεζας. Οι εν λόγω σταθμοί προσφέρουν διάφορες διαδικτυακές υπηρεσίες (συγκεκριμένα υπηρεσίες ονοματοδοσίας, ηλεκτρονικού ταχυδρομείου και εξυπηρετητή ιστοσελίδων). Ο Πίνακας 6-2 παρουσιάζει το σύνολο των υπογραφών που απαιτούνται για τις δύο διαφορετικές τεχνικές

αξιολόγησης. Όπως προαναφέρθηκε, το σύνολο s_1 προκύπτει από το άθροισμα των απαιτούμενων υπογραφών για τις διαφορετικές προσφερόμενες υπηρεσίες των συστημάτων.

Πίνακας 6-2: Αποτελέσματα για υποδομή σταθμών Διαδικτύου

A/A	Όνομα υπολογιστή	Λειτουργικό Σύστημα	Services	s_1 (υπηρεσία)	s_1 (σύστημα)	s_2 IRIS
1	dune.example.com	Sun Solaris	DNS	29	29	1
2	ermis.example.com	Sun Solaris	POP3	36	160	0
			SMTP	102		
			ICMP	22		
3	pythia.example.com	Sun Solaris	SMTP	102	102	0
4	spider.example.com	Sun Solaris	HTTP	143	212	2
			IMAP	69		
Σύνολο διαφορετικών υπογραφών IDP					**401**	**4**

Για τη συγκεκριμένη υποδομή, φαίνεται πως η χρήση του IRIS προσφέρει επακριβώς το ίδιο επίπεδο ασφάλειας με ενεργοποίηση 4 μόλις υπογραφών, έναντι των 401 που απαιτούνται για την κάλυψη όλων των προσφερομένων υπηρεσιών της εν λόγω υποδομής.

6.4.2. Σενάριο 2: Υποδομή Σταθμών Εργασίας

Το δεύτερο σενάριο λειτουργίας εξετάζει μια περισσότερο τυποποιημένη υποδομή σταθμών εργασίας στο ίδιο εταιρικό δίκτυο. Πιο συγκεκριμένα, ελέγχθηκαν (με το εργαλείο Nessus) 22 υπολογιστικοί σταθμοί που ανήκουν στο ίδιο λογικό υποδίκτυο. Τα αποτελέσματα του Nessus έδειξαν ένα μικρό σύνολο δικτυακών υπηρεσιών, που όμως απασχολούν ένα μεγάλο πλήθος υπογραφών του Snort. Ο Πίνακας 6-3 απαριθμεί τα χαρακτηριστικά των σταθμών εργασίας (διεύθυνση IP, λειτουργικό σύστημα), τις προσφερόμενες υπηρεσίες, καθώς και το πλήθος των Snort υπογραφών χωρίς και με τη χρήση του IRIS (s_1 και s_2 αντίστοιχα).

Πίνακας 6-3: Αποτελέσματα για υποδομή σταθμών εργασίας

A/A	IP	Λειτουργικό Σύστημα	Services	s_1 (υπηρεσία)	s_1 (σύστημα)	s_2 IRIS
1	10.2.1.13	Windows XP	RPC	171	797	136
			Terminal Services	13		
			NetBIOS	613		
2	10.2.1.18	Windows XP	RPC	171	797	136
			Terminal Services	13		
			NetBIOS	613		
3	10.2.1.26	Windows XP	NetBIOS	613	613	136
4	10.2.1.30	Windows XP	Terminal Services	13	711	136
			FTP	85		
			NetBIOS	613		
5	10.2.1.43	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
6	10.2.1.46	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
7	10.2.1.47	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
8	10.2.1.55	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
9	10.2.1.70	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
10	10.2.1.73	Windows XP	RPC	171	852	136
			Terminal Services	13		
			NetBIOS	613		
			NNTP	14		
			ICMP	22		
			SNMP	19		
11	10.2.1.78	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
12	10.2.1.106	Windows XP	NetBIOS	613	613	136
13	10.2.1.114	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
14	10.2.1.116	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
15	10.2.1.117	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
16	10.2.1.118	Windows XP	Terminal Services	13	626	136
			NetBIOS	613		
17	10.2.1.125	Windows XP	RPC	171	816	136
			Terminal Services	13		
			NetBIOS	613		

			SNMP	19		
18	10.2.1.140	Windows XP	RPC	171	797	136
			Terminal Services	13		
			NetBIOS	613		
19	10.2.1.141	Windows XP	RPC	171	797	136
			Terminal Services	13		
			NetBIOS	613		
20	10.2.1.152	Windows XP	NetBIOS	613	613	136
21	10.2.1.154	Windows XP	NetBIOS	613	613	136
22	10.2.1.155	Windows XP	NetBIOS	613	613	136
Σύνολο διαφορετικών υπογραφών IDP					**937**	**136**

Τα αποτελέσματα των μετρήσεων δείχνουν πως η χρήση του IRIS μειώνει κατά 85,5% το πλήθος των απαιτούμενων υπογραφών Snort (136 έναντι 937, αντίστοιχα) για τη συγκεκριμένη υποδομή.

6.4.3. Σενάριο 3: Υποδομή Εξυπηρετητών

Το τελευταίο δείγμα μετρήσεων αναφέρεται στην υποδομή εξυπηρετητών του ίδιου Οργανισμού, στην οποία ελέγχθηκαν 18 διαφορετικοί εξυπηρετητές που εκτελούν διαφόρους ρόλους (εξυπηρετητές ηλεκτρονικού ταχυδρομείου, εξυπηρετητές ονοματοδοσίας, εξυπηρετητές βάσεων δεδομένων και εξυπηρετητές ιστού, αντίστοιχα).

Ο Πίνακας 6-4 απαριθμεί τα χαρακτηριστικά των σταθμών εργασίας (διεύθυνση IP, λειτουργικό σύστημα), τις προσφερόμενες υπηρεσίες, καθώς και το πλήθος των υπογραφών Snort χωρίς και με τη χρήση του IRIS (s_1 και s_2 αντίστοιχα).

Πίνακας 6-4: Αποτελέσματα για υποδομή εξυπηρετητών

A/A	IP	Λειτουργικό Σύστημα	Services	s_1 (υπηρεσία)	s_1 (σύστημα)	s_2 IRIS
1	10.10.0.10	Windows 2003	RPC	171	827	1
			NetBIOS	613		
			NNTP	14		
			DNS	29		
2	10.10.0.11	Windows 2003	RPC	171	970	1
			NetBIOS	613		
			NNTP	14		
			HTTP	143		
			DNS	29		

3	10.10.0.18	Windows 2003	HTTP	143	1134	0
			RPC	171		
			IMAP	69		
			NetBIOS	613		
			POP3	36		
			SMTP	102		
4	10.10.0.19	Windows 2003	RPC	171	1032	0
			IMAP	69		
			NetBIOS	613		
			POP3	36		
			HTTP	143		
5	10.10.0.20	Windows 2003	Terminal Services	13	534	0
			HTTP	143		
			RPC	171		
			IMAP	69		
			POP3	36		
			SMTP	102		
6	10.10.0.21	Windows 2003	RPC	171	927	0
			NetBIOS	613		
			HTTP	143		
7	10.10.0.22	Windows 2003	Terminal Services	13	940	0
			RPC	171		
			HTTP	143		
			NetBIOS	613		
8	10.10.0.23	Windows 2003	Terminal Services	13	940	0
			RPC	171		
			HTTP	143		
			NetBIOS	613		
9	10.10.0.24	Windows 2003	Terminal Services	13	940	0
			NetBIOS	613		
			RPC	171		
			HTTP	143		
10	10.10.0.25	Windows 2003	Terminal Services	13	940	0
			NetBIOS	613		
			RPC	171		
			HTTP	143		
11	10.10.0.26	Windows 2003	Terminal Services	13	940	0
			NetBIOS	613		
			RPC	171		
			HTTP	143		
12	10.10.0.27		Terminal Services	13	1147	0
			RPC	171		

		Windows 2003	IMAP	69		
			POP3	36		
			HTTP	143		
			SMTP	102		
			NetBIOS	613		
13	10.10.0.28	Windows 2003	Terminal Services	13	1147	0
			RPC	171		
			IMAP	69		
			POP3	36		
			HTTP	143		
			SMTP	102		
			NetBIOS	613		
14	10.10.0.29	Windows 2003	Terminal Services	13	1147	0
			RPC	171		
			IMAP	69		
			POP3	36		
			HTTP	143		
			SMTP	102		
			NetBIOS	613		
15	10.10.0.30	Windows 2003	SQL	116	1056	0
			Terminal Services	13		
			RPC	171		
			NetBIOS	613		
			HTTP	143		
16	10.10.0.31	Windows 2003	Terminal Services	13	769	0
			HTTP	143		
			NetBIOS	613		
17	10.10.0.32	Windows 2003	Terminal Services	13	769	0
			HTTP	143		
			NetBIOS	613		
18	10.10.0.40	Windows 2003	Terminal Services	13	1147	0
			RPC	171		
			IMAP	69		
			POP3	36		
			HTTP	143		
			SMTP	102		
			NetBIOS	613		
Σύνολο διαφορετικών υπογραφών IDP					**1147**	**1**

Στο συγκεκριμένο σενάριο, η χρήση του IRIS είναι καταλυτική, καθώς απαιτείται μόλις 1 υπογραφή (έναντι 1147 χωρίς τη χρήση του εργαλείου) για το ισοδύναμο επίπεδο ασφάλειας.

6.4.4. Σχολιασμός αποτελεσμάτων μετρήσεων

Οι μετρήσεις αποδεικνύουν πως η χρήση του IRIS μειώνει δραστικά το σύνολο των απαιτούμενων υπογραφών Snort για την κάλυψη μιας υποδομής. Ο κυριότερος λόγος γι' αυτό είναι πως το εργαλείο λαμβάνει υπόψη του τις ιδιαιτερότητες μιας συγκεκριμένης υποδομής, καθώς και τις αδυναμίες ασφάλειας που είναι ενεργές ακόμη και μετά την υλοποίηση μέτρων ασφάλειας, συνυπολογίζοντας –δηλαδή- την παρουσία μηχανισμών ασφάλειας που μεταβάλλουν τη σημασία ασφάλειας σε μια υποδομή.

Στους ελέγχους που πραγματοποιήθηκαν, το εργαλείο Nessus αποτέλεσε την κυριότερη πηγή συλλογής πληροφοριών και θεωρείται δεδομένο πως η κάθε υποδομή που παρουσιάστηκε στους παραπάνω πίνακες αποτελεί μέρος μόνο της συνολικής υποδομής της –υπό εξέταση- επιχείρησης. Με άλλα λόγια, η υποδομή ασφάλειας της συγκεκριμένης επιχείρησης (π.χ. διαχωρισμός δικτύων, συστήματα ελέγχου δικτυακής κυκλοφορίας και τείχη προστασίας) επηρέασε σημαντικά τα αποτελέσματα των μετρήσεων (υπήρξαν, δηλαδή, συστήματα στα οποία το Nessus δεν μπόρεσε να βρει σχετικές αδυναμίες, ώστε με βάση αυτές, να υπολογίσει το σύνολο των απαιτούμενων υπογραφών). Το γεγονός αυτό καθιστά ακόμη πιο αξιόπιστη τη μέθοδο της ανάπτυξης συστημάτων IDP με χρήση τοπολογικής ανάλυσης (χρήση IRIS), καθώς απαλείφεται η επικάλυψη μηχανισμών ασφάλειας για μια συγκεκριμένη υποδομή. Ουσιαστικά, η ύπαρξη ενός καλά παραμετροποιημένου μηχανισμού ασφάλειας, ο οποίος περιορίζει το σύνολο των προσφερόμενων υπηρεσιών και επικοινωνιών σε όσα καθορίζει η πολιτική ασφάλειας της υποδομής, περιορίζει σημαντικά τη δυνατότητα εμφάνισης ενός περιστατικού ασφάλειας στο υποσύνολο των υπηρεσιών που ο συγκεκριμένος μηχανισμός ασφάλειας επιτρέπει. Ο ισχυρισμός αυτός αποδεικνύεται από τα αποτελέσματα του Πίνακα Πίνακας 6-4, όπου η υποδομή των εξυπηρετητών της επιχείρησης προστατεύεται από ένα μεγάλο σύνολο μηχανισμών ασφάλειας (κάτι που δεν ισχύει για την υποδομή των σταθμών εργασίας).

Συμπερασματικά, η δραστική μείωση των χρησιμοποιούμενων υπογραφών Snort, περιορίζει σημαντικά την εμφάνιση των ψευδοθετικών σφαλμάτων στην ανάπτυξη και συντήρηση των συστημάτων IDP για μια συγκεκριμένη υποδομή[25].

6.5. Συμπεράσματα χρηστών

Το σύστημα IRIS αξιολογήθηκε, επίσης, από ένα πλήθος ειδικών ασφάλειας, οι οποίοι είχαν την ευκαιρία να δοκιμάσουν τις δυνατότητες του εργαλείου και να πειραματιστούν με τις λειτουργίες του. Πιο συγκεκριμένα, δημιουργήθηκε ένα πρόγραμμα-πελάτης σε γλώσσα Java (Java client), το οποίο διανεμήθηκε στους συγκεκριμένους χρήστες μέσω ιστοτόπου. Το πρόγραμμα-πελάτης συνδεόταν με τον αντίστοιχο εξυπηρετητή (server) ο οποίος φιλοξενούσε τις βάσεις δεδομένων του IRIS. Για τη διευκόλυνση των χρηστών και την αποφυγή μη εξουσιοδοτημένων ελέγχων ασφάλειας για την αξιολόγηση του εργαλείου, παραδόθηκαν –επίσης- στους χρήστες δύο αναφορές ασφάλειας (του εργαλείου nessus) οι οποίες περιείχαν πραγματικά πειραματικά δεδομένα. Τέλος, οι χρήστες απάντησαν σε ειδικά διαμορφωμένο ερωτηματολόγιο, το οποίο παρατίθενται στα παραρτήματα.

6.5.1. Ανάλυση και αξιολόγηση δείγματος

Το ερωτηματολόγιο αξιολόγησης στάλθηκε αρχικά σε 40 στελέχη ελληνικών οργανισμών που ασχολούνται ενεργά με την ασφάλεια πληροφοριών, από το σύνολο σχεδόν των καθέτων αγορών (ιδιωτικές επιχειρήσεις, Τράπεζες και χρηματοπιστωτικοί οργανισμοί, ακαδημαϊκά ιδρύματα, δημόσιοι οργανισμοί και τηλεπικοινωνιακές επιχειρήσεις). Ανάμεσα στις εταιρείες που συμμετείχαν στην αξιολόγηση είναι η Εμπορική Τράπεζα της Ελλάδος, Τράπεζα Αττικής, Πανεπιστήμιο Πειραιά, Cosmote, Alpha Bank, Adacom, PriceWaterhouseCoopers, Ernst & Young, WIND, BeSecure, SocieteGeneral/Geniki Bank, Πανελλήνια Τράπεζα, κ.ά. Συλλέχθηκαν συνολικά 20

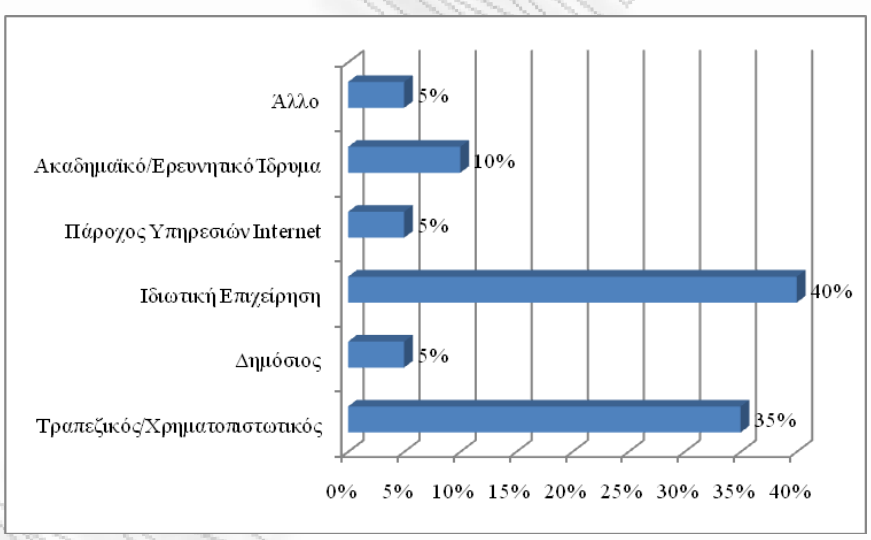
[25] Η πρακτική απόδειξη του συγκεκριμένου ισχυρισμού, ωστόσο, δεν αποτελεί στόχο της συγκεκριμένης διατριβής.

πλήρως απαντημένα ερωτηματολόγια. Η ανάλυση που ακολουθεί στις παρακάτω ενότητες στοχεύει στην ανάλυση της αξιοπιστίας του δείγματος, σε ό,τι αφορά τόσο σε δημογραφικά χαρακτηριστικά (π.χ. είδος και μέγεθος Οργανισμού), όσο και σε συγκεκριμένους δείκτες (εμπειρία χρηστών, εξοικείωση με τεχνολογίες/τεχνικές ασφάλειας πληροφοριών, εξοικείωση με την αντιμετώπιση περιστατικών, κτλ.). Η ανάλυση του δείγματος παρουσιάζεται σταδιακά στα επόμενα.

Ο Πίνακας 6-5 παρουσιάζει την ποσόστωση των Οργανισμών ανά κάθετη αγορά, με βάση τις απαντήσεις που συλλέχθηκαν.

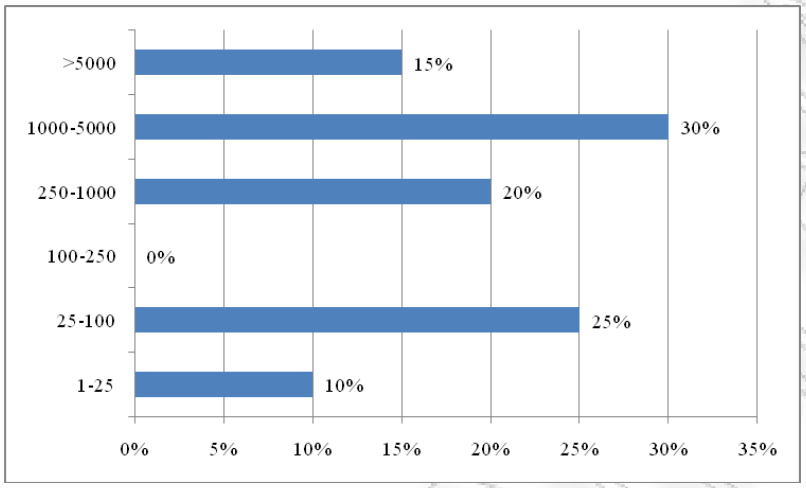
Οι περισσότερες απαντήσεις προήλθαν από στελέχη Ιδιωτικών Επιχειρήσεων (40% του δείγματος) καθώς και Τραπεζικών και Χρηματοπιστωτικών Οργανισμών (35% του δείγματος), ενώ υπάρχουν απαντήσεις για το σύνολο των καθέτων αγορών.

Πίνακας 6-5: Είδος Οργανισμού του χρήστη



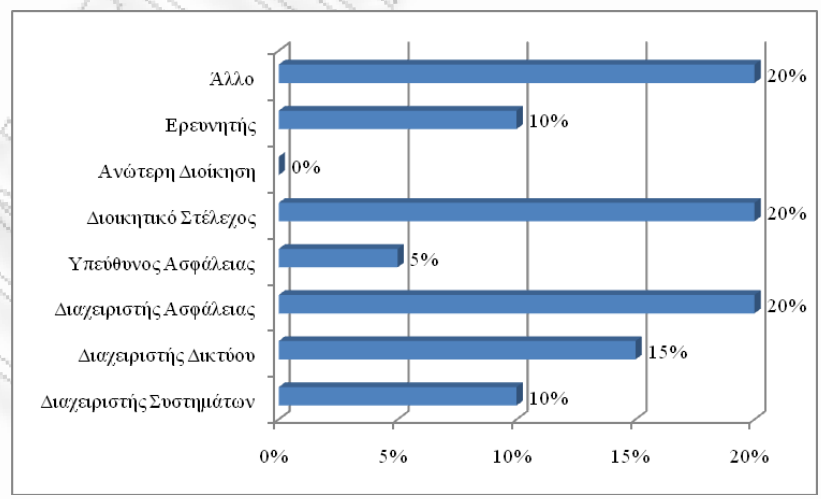
Ο Πίνακας 6-6 απεικονίζει το μέγεθος (σε χρήστες) των Οργανισμών που συμμετείχαν στην αξιολόγηση. Η πλειονότητα των απαντήσεων αφορά σε μικρές/μικρομεσαίες επιχειρήσεις (1-250 χρήστες), ενώ ένα μεγάλο ποσοστό του δείγματος (45%) αφορά σε μεγάλες/πολύ μεγάλες επιχειρήσεις. Το σύνολο των απαντήσεων καλύπτει όλο το εύρος για το μέγεθος των εταιρειών που συμμετείχαν στην αξιολόγηση.

Πίνακας 6-6: Πλήθος υπαλλήλων στον Οργανισμό του χρήστη



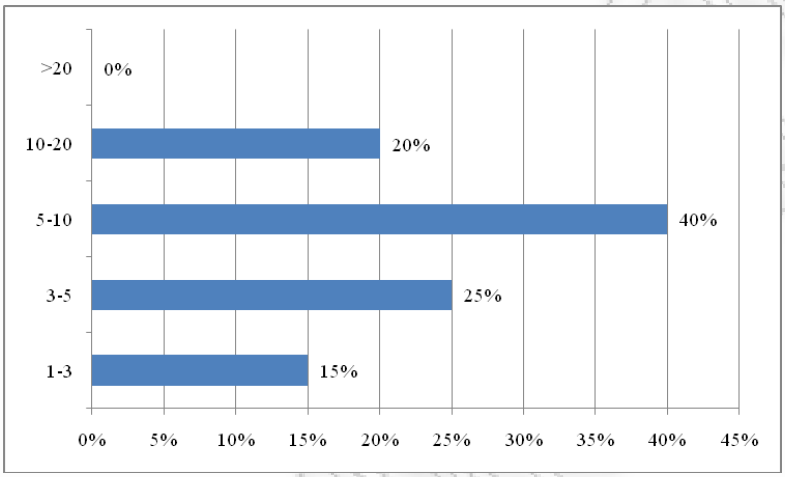
Ο Πίνακας 6-7 απεικονίζει το ρόλο των χρηστών που συμμετείχαν στην αξιολόγηση μέσα στον Οργανισμό τους και ιδιαίτερα στις λειτουργίες ασφάλειας του Οργανισμού. Οι απαντήσεις καλύπτουν όλο το φάσμα των διαθεσίμων επιλογών, ενώ το μεγαλύτερο ποσοστό του δείγματος (περίπου 75%) αφορά σε ρόλους που σχετίζονται άμεσα με τη χρήση του IRIS (διαχειριστές δικτύου, ασφάλειας και συστημάτων, υπευθύνους ασφάλειας και διοικητικά στελέχη), καθώς και με τη γενικότερη εταιρική διαδικασία αντιμετώπισης περιστατικών (βλ. Ενότητα 3.2.1).

Πίνακας 6-7: Ρόλος χρήστη στον Οργανισμό



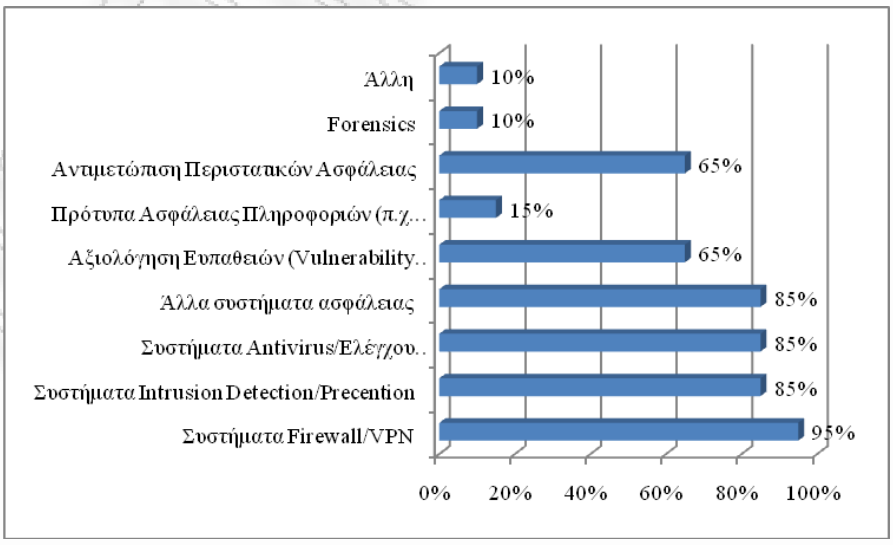
Η εμπειρία των χρηστών που συμμετείχαν στην αξιολόγηση κρίνεται επαρκής, καθότι η πλειονότητα του δείγματος διαθέτει περισσότερα από 5 χρόνια εμπειρίας στην περιοχή της ασφάλειας πληροφοριών (ποσοστό 60% του δείγματος).

Πίνακας 6-8: Χρόνια απασχόλησης με την Ασφάλεια Πληροφοριών



Κρίθηκε σκόπιμο, εκτός της εμπειρίας των χρηστών του δείγματος, να αξιολογηθεί και η τεχνογνωσία του δείγματος σε περιοχές της ασφάλειας πληροφοριών που σχετίζονται με την αντιμετώπιση περιστατικών ασφάλειας.

Πίνακας 6-9: Περιοχές της ασφάλειας πληροφοριών στις οποίες διαθέτουν σχετική εμπειρία οι χρήστες



Σύμφωνα με τα στοιχεία που παρουσιάζονται στον Πίνακα Πίνακας 6-9, το δείγμα διαθέτει υψηλή τεχνογνωσία στις δημοφιλείς περιοχές ασφάλειας πληροφοριών.

Συνολικά, το δείγμα κρίνεται αξιόπιστο για τους παρακάτω λόγους:

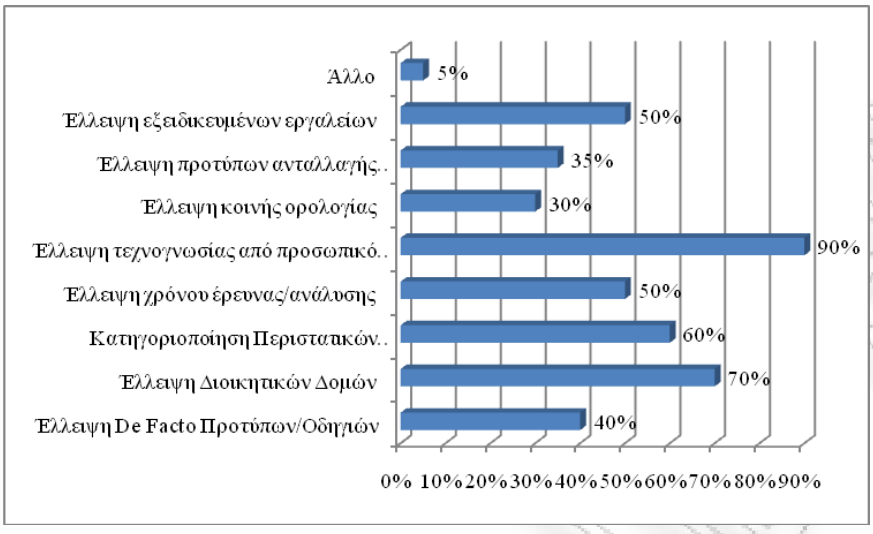
- Οι απαντήσεις καλύπτουν, αντιπροσωπευτικά, χρήστες από το σύνολο των καθέτων αγορών,
- Οι απαντήσεις καλύπτουν, αντιπροσωπευτικά, όλα τα μεγέθη Οργανισμών (από μικρούς έως πολύ μεγάλους),
- Οι απαντήσεις καλύπτουν, αντιπροσωπευτικά, όλους τους ρόλους που σχετίζονται –άμεσα ή έμμεσα- με την ασφάλεια πληροφοριών σε έναν Οργανισμό,
- Οι χρήστες διαθέτουν, στην πλειοψηφία τους, πολυετή εμπειρία στην ασφάλεια πληροφοριών,
- Οι χρήστες διαθέτουν, υψηλή τεχνογνωσία σε μια μεγάλη ομάδα τεχνολογιών/τεχνικών της ασφάλειας πληροφοριών.

6.5.2. Ανάλυση και αξιολόγηση απαιτήσεων

Στη συγκεκριμένη ενότητα, καταγράφονται και αναλύονται οι απόψεις των χρηστών σχετικά με την αντιμετώπιση περιστατικών ασφάλειας, καθώς και οι απαιτήσεις τους σχετικά με συγκεκριμένα χαρακτηριστικά που θα πρέπει να διαθέτουν αντίστοιχα εργαλεία.

Ο Πίνακας 6-10 παρουσιάζει τις απαντήσεις των χρηστών σχετικά με την κατηγοριοποίηση και αξιολόγηση των κυριοτέρων ζητημάτων στην αντιμετώπιση περιστατικών ασφάλειας (βλ. Ενότητες 3.2 και 4.3).

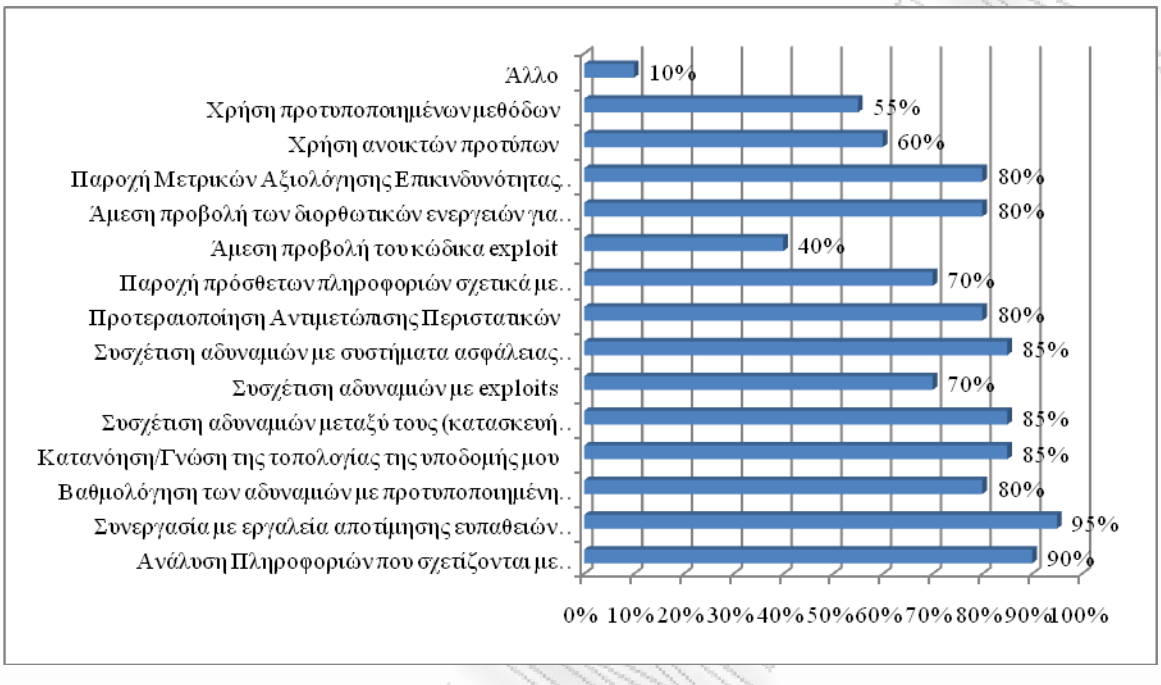
Πίνακας 6-10: Αξιολόγηση ζητημάτων που σχετίζονται με την Αντιμετώπιση Περιστατικών Ασφάλειας από τους χρήστες



Το σύνολο σχεδόν του δείγματος (ποσοστό 90%) αναφέρει πως το σημαντικότερο ζήτημα στην αντιμετώπιση περιστατικών ασφάλειας είναι η έλλειψη τεχνογνωσίας από το προσωπικό του Οργανισμού ή/και την αγορά, ενώ είναι εμφανής η έλλειψη εξειδικευμένων εργαλείων (50% των απαντήσεων). Με βάση το γεγονός αυτό, ζητήθηκε από τους συμμετέχοντες να επιλέξουν τα χαρακτηριστικά που θα έπρεπε –κατά την άποψή τους- να διαθέτει ένα εξειδικευμένο εργαλείο αντιμετώπισης περιστατικών. Τα αποτελέσματα παρουσιάζονται στον Πίνακα Πίνακας 6-11.

Οι απαντήσεις των χρηστών του δείγματος παρουσιάζουν ανάγκες για μια μεγάλη και ευρεία γκάμα λειτουργιών από ένα εξειδικευμένο εργαλείο αντιμετώπισης περιστατικών ασφάλειας. Οι δημοφιλέστερες απαντήσεις περιλαμβάνουν (μεταξύ άλλων) τη συνεργασία με εργαλεία αποτίμησης αδυναμιών ασφάλειας (ποσοστό 95%), συσχέτιση αδυναμιών με συστήματα IDP (ποσοστό 80%), συσχέτιση αδυναμιών με εκμεταλλεύσεις (ποσοστό 70) και κατανόηση/γνώση της τοπολογίας της εκάστοτε υποδομής (ποσοστό 85%), ήτοι τα κύρια γνωρίσματα της τοπολογικής ανάλυσης αδυναμιών ασφάλειας και των λειτουργιών του IRIS.

Πίνακας 6-11: Χαρακτηριστικά εργαλείου αντιμετώπισης περιστατικών ασφάλειας που επιθυμούν οι χρήστες

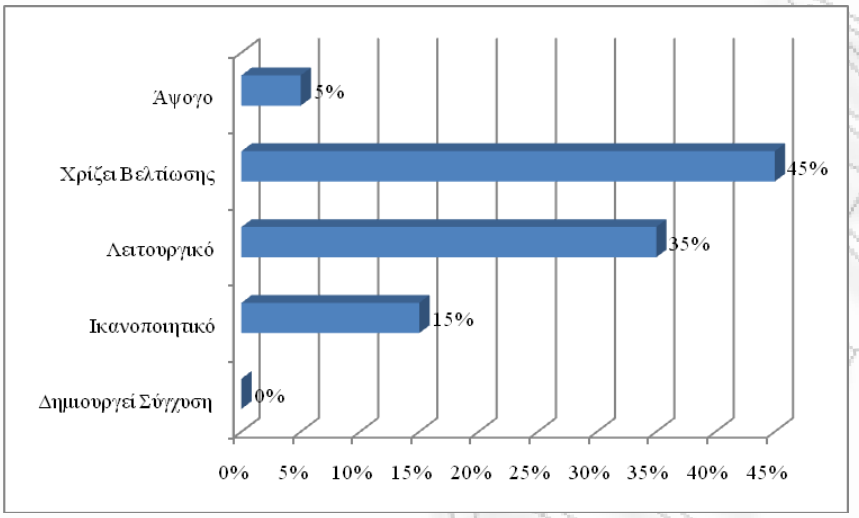


Με δεδομένες τις παραπάνω απαντήσεις, οι χρήστες προχώρησαν στην αξιολόγηση των λειτουργιών του IRIS. Για τη διευκόλυνση των χρηστών, δόθηκαν στη διάθεσή τους δύο ενδεικτικές αναφορές αποτίμησης αδυναμιών (σε μορφότυπο του εργαλείου Nessus), ώστε αφενός μεν να επιταχυνθεί η διαδικασία, αφετέρου δε να μη χρειαστεί να εκτελέσουν οι ίδιοι αντίστοιχους ελέγχους (κάτι που πιθανόν να αντιβαίνει στην πολιτική ασφάλειας του Οργανισμού τους).

6.5.3. Ανάλυση και αξιολόγηση των λειτουργιών του IRIS

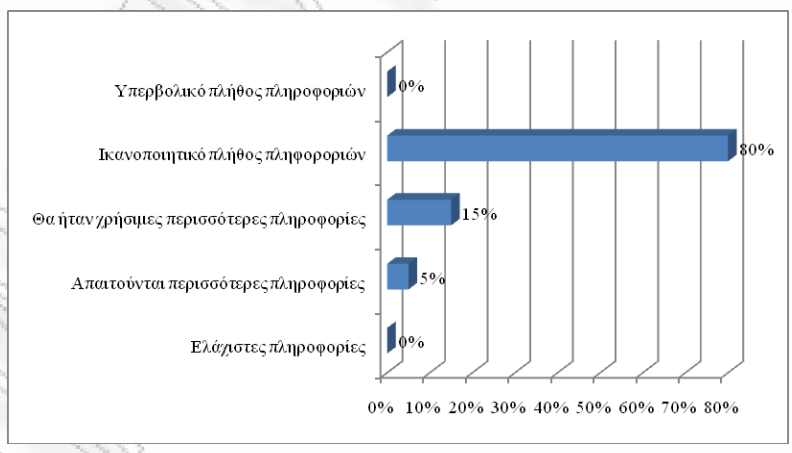
Η πλειοψηφία των χρηστών που συμμετείχαν στην αξιολόγηση έκριναν θετικά τη διεπαφή του IRIS (ποσοστό 85%), ενώ το υπόλοιπο ποσοστό (15% των απαντήσεων) την χαρακτήρισαν ως ικανοποιητική. Η διεπαφή σε ένα σύστημα διαχείρισης πληροφοριών ασφάλειας, όπως είναι το IRIS, είναι ιδιαίτερα σημαντικός παράγοντας, δεδομένου του πλήθους των πληροφοριών που διαχειρίζεται καθώς και των αναφορών που παράγει (βλ. ενότητα 4.5.6).

Πίνακας 6-12: Αξιολόγηση της διεπαφής του IRIS



Αντίστοιχα, οι χρήστες που συμμετείχαν στην αξιολόγηση χαρακτήρισαν ως ικανοποιητικό το πλήθος των πληροφοριών που διαχειρίζεται το IRIS (ποσοστό 80%) σύμφωνα με όσα περιγράφονται στην ενότητα 5.2.2.1, ενώ το 20% του δείγματος υπέδειξε πως οι λειτουργίες του IRIS θα εξυπηρετούνται καλύτερα με περισσότερες πληροφορίες, όπως δείχνουν τα αποτελέσματα του Πίνακα Πίνακας 6-13.

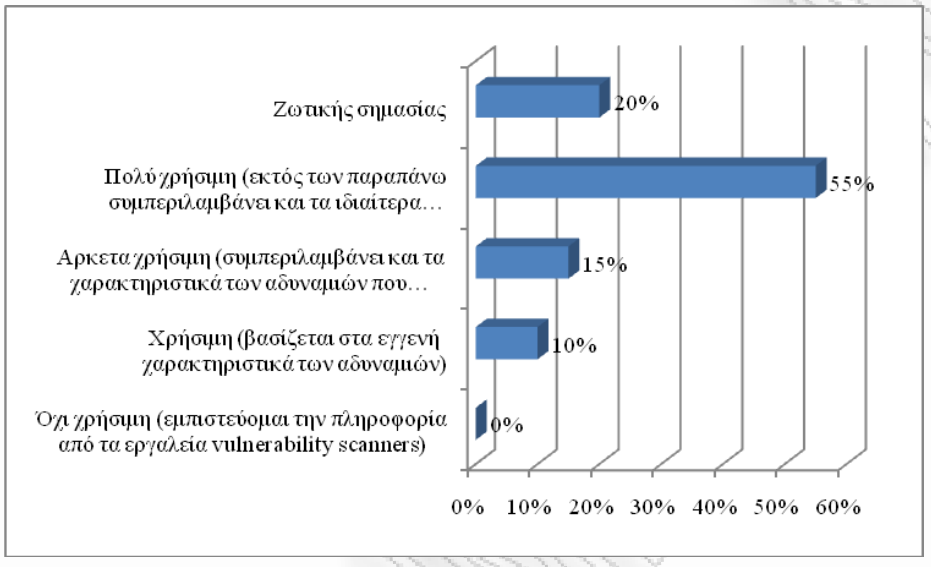
Πίνακας 6-13: Αξιολόγηση ποσότητας πληροφοριών που διαχειρίζεται το IRIS



Στη συνέχεια, οι χρήστες αξιολόγησαν επιμέρους δυνατότητες του IRIS. Για παράδειγμα, η δυνατότητα βαθμολόγησης των αδυναμιών ασφάλειας (μετά την τοπολογική ανάλυση των αδυναμιών που ανακαλύπτονται), χαρακτηρίστηκε ως πολύ χρήσιμη/ζωτικής

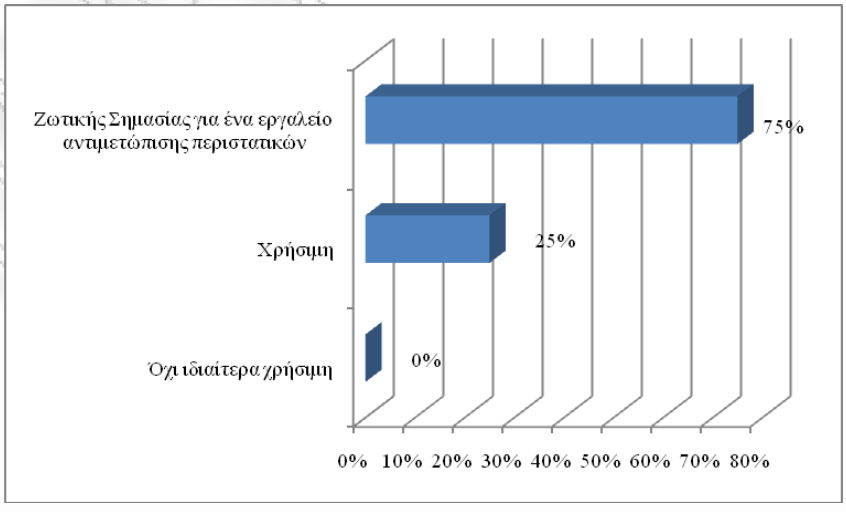
σημασίας από την πλειοψηφία του δείγματος (συνολικό ποσοστό 75%, 55% και 20% αντίστοιχα).

Πίνακας 6-14: Αξιολόγηση δυνατότητας βαθμολόγησης των αδυναμιών ασφάλειας του IRIS



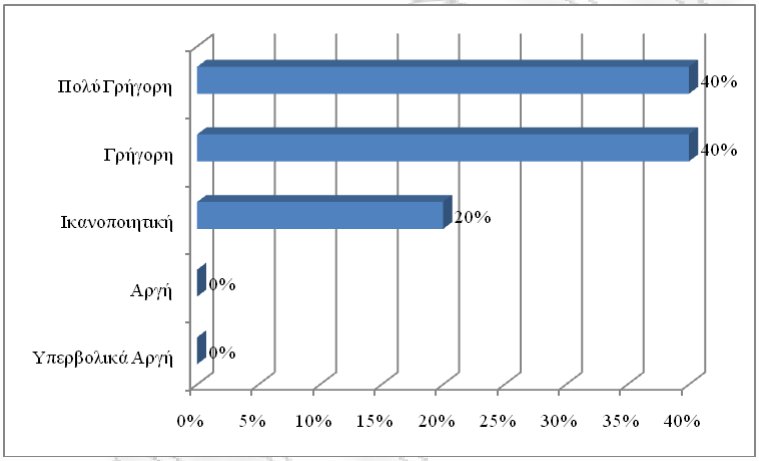
Η δυνατότητα του IRIS να αναλύει και να συσχετίζει πληροφορίες σχετικές με εκμεταλλεύσεις και υπογραφές συστημάτων IDP χαρακτηρίστηκε ως λειτουργία ζωτικής σημασίας από το 75% του δείγματος, όπως δείχνει ο Πίνακας 6-15, γεγονός που συνάδει με τις απαντήσεις που παρουσιάστηκαν παραπάνω (Πίνακας 6-11).

Πίνακας 6-15: Αξιολόγηση συσχέτισης των αδυναμιών με τα exploits και με τις υπογραφές intrusion detection



Δεδομένου του μεγάλου όγκου των πληροφοριών που επεξεργάζεται το IRIS, κρίθηκε σκόπιμο να αξιολογηθεί η ταχύτητα των υπολογισμών του. Αν και το συγκεκριμένο χαρακτηριστικό εξαρτάται άμεσα από ένα πλήθος παραγόντων που πιθανόν να επηρεάσουν τις απαντήσεις των χρηστών (π.χ. επεξεργαστική ισχύς του υπολογιστή του χρήστη καθότι το IRIS είναι μια εφαρμογή Java, ταχύτητα σύνδεσης με το Διαδίκτυο, δεδομένου πως οι βάσεις δεδομένων του IRIS βρίσκονται στο Διαδίκτυο, κτλ.), η πλειοψηφία του δείγματος (ποσοστό 80%) χαρακτήρισε θετικά την ταχύτητα των υπολογισμών, όπως δείχνει ο Πίνακας 6-16.

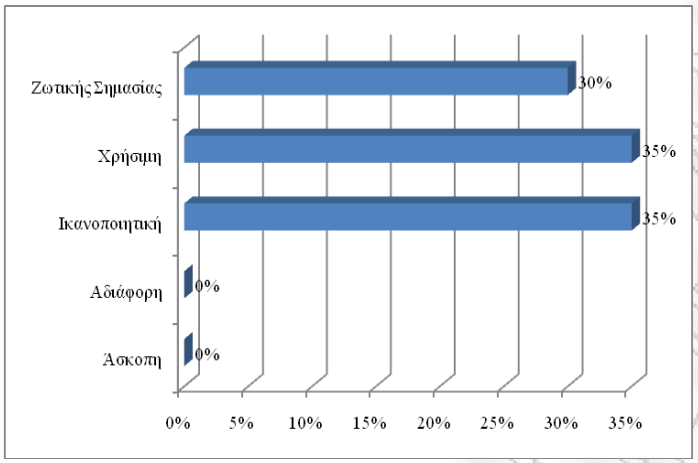
Πίνακας 6-16: Αξιολόγηση ταχύτητας υπολογισμών του IRIS



Η αξιολόγηση της ταχύτητας των υπολογισμών του IRIS κρίθηκε σκόπιμο να αξιολογηθεί, δεδομένου πως οι χρήστες ανέφεραν (σε ποσοστό 50%) το ζήτημα έλλειψης χρόνου για έρευνα και ανάλυση των περιστατικών ασφάλειας.

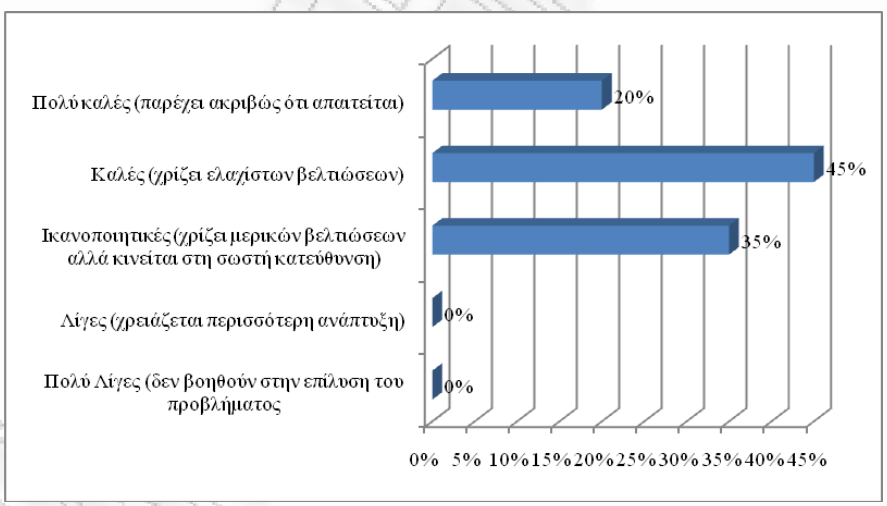
Το IRIS προσφέρει τη δυνατότητα διάδρασης με τον χρήστη, κατά τη φάση αξιολόγησης των περιβαλλοντικών μετρικών των αδυναμιών που ανακαλύπτονται σε μια υποδομή (βλ. Πίνακας 5-4). Το συγκεκριμένο χαρακτηριστικό αξιολογήθηκε θετικά από το σύνολο του δείγματος (ποσοστό 100%).

Πίνακας 6-17: Αξιολόγηση διάδρασης του IRIS με το χρήστη



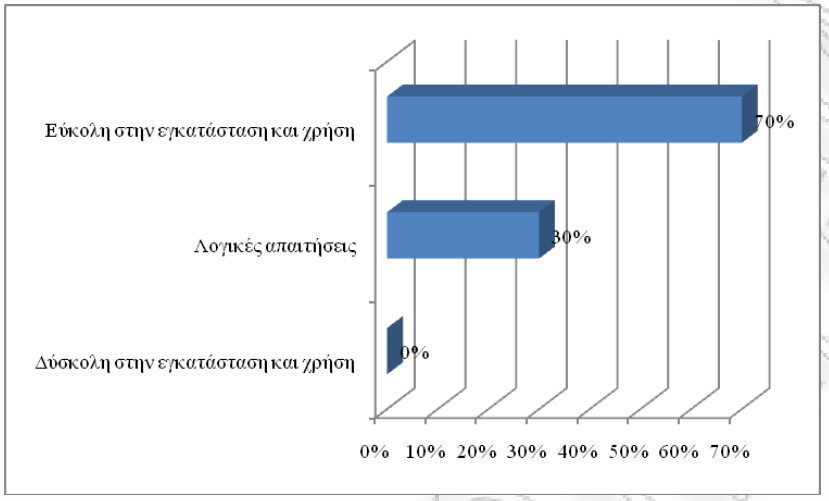
Στη συνέχεια, ζητήθηκε από το δείγμα να αξιολογήσει τις συνολικές δυνατότητες και λειτουργίες του IRIS. Οι απαντήσεις του συνόλου του δείγματος χαρακτηρίζει θετικά το εργαλείο, όπως δείχνει ο Πίνακας 6-18.

Πίνακας 6-18: Αξιολόγηση συνολικών δυνατοτήτων του IRIS



Τέλος, ζητήθηκε από το δείγμα να αξιολογήσει τις απαιτήσεις εγκατάστασης και λειτουργίας του IRIS. Το σύνολο του δείγματος δεν αντιμετώπισε κάποιο ιδιαίτερο ζήτημα ή δυσκολία στη λειτουργία του εργαλείου, όπως δείχνουν οι απαντήσεις που παρουσιάζονται στον Πίνακας 6-19.

Πίνακας 6-19: Αξιολόγηση πλατφόρμας του IRIS



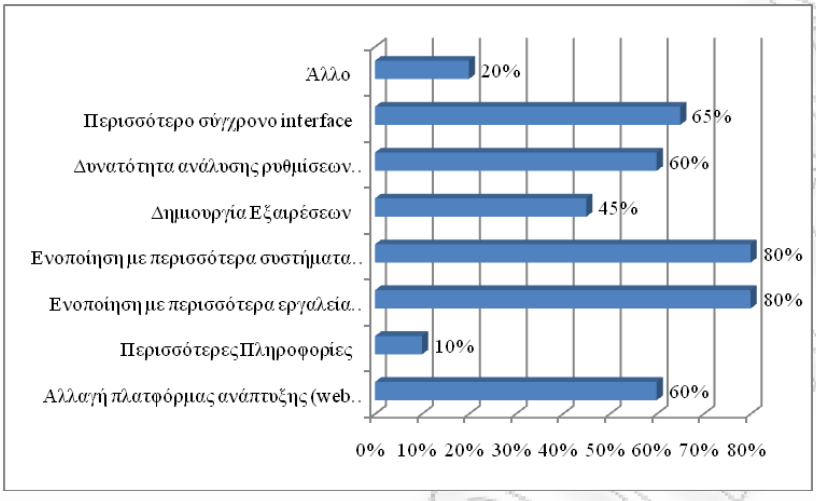
Συμπερασματικά, οι χρήστες του δείγματος κρίνουν θετικά τόσο το σύνολο όσο και τα επιμέρους χαρακτηριστικά και λειτουργίες του IRIS.

6.5.4. Προτάσεις και σχόλια χρηστών

Από το δείγμα ζητήθηκε, επίσης, να προτείνει πρόσθετες λειτουργίες/χαρακτηριστικά που θα επιθυμούσε από το συγκεκριμένο εργαλείο, όσο και να σχολιάσει ελεύθερα (ήτοι χωρίς την επιλογή προκαθορισμένων απαντήσεων) τις λειτουργίες του εργαλείου. Τα δεδομένα αυτά παρουσιάζονται στις επόμενες ενότητες.

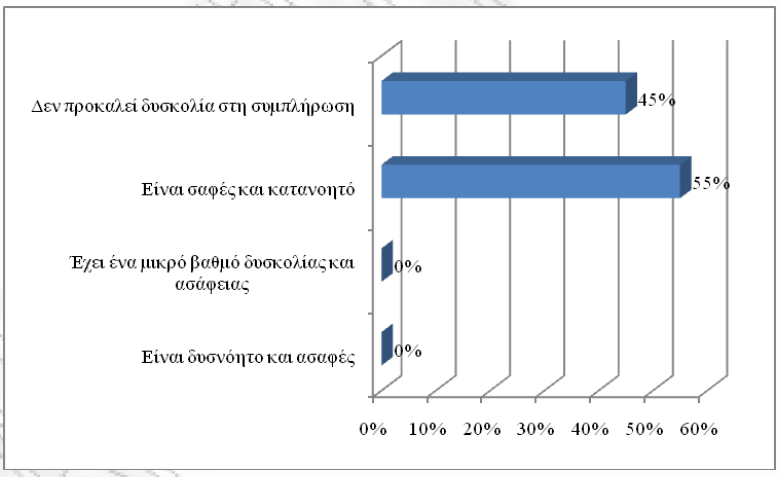
Τα περισσότερο σημαντικά χαρακτηριστικά που επιθυμούν οι χρήστες από την μελλοντική ανάπτυξη του IRIS εστιάζουν στη συνεργασία του IRIS με περισσότερα εργαλεία αποτίμησης επικινδυνότητας και συστήματα IDP (ποσοστό 80%), ενώ το 60% του δείγματος θα έβλεπε θετικά την αλλαγή της πλατφόρμας του IRIS από εφαρμογή πελάτη-εξυπηρετητή (client/server) σε εφαρμογή ιστού (web application). Αναλυτικά, οι απαντήσεις των χρηστών απεικονίζονται στον Πίνακας 6-20.

Πίνακας 6-20: Χαρακτηριστικά βελτίωσης του IRIS



Προκειμένου, τέλος, να αξιολογηθεί και η σαφήνεια των ερωτήσεων που υποβλήθηκαν στους χρήστες, ζητήθηκε από το δείγμα να χαρακτηρίσει το ερωτηματολόγιο. Ο Πίνακας 6-20 δείχνει πως, το σύνολο του δείγματος, δεν αντιμετώπισε κάποιο ιδιαίτερο ζήτημα.

Πίνακας 6-21: Αξιολόγηση ερωτηματολογίου



6.5.5. Προτάσεις και συμπεράσματα

Ιδιαίτερα χρήσιμα χαρακτηρίζονται, τέλος, τα ελεύθερα σχόλια των χρηστών που συμμετείχαν στην αξιολόγηση του IRIS (το σύνολο των απαντήσεων παρατίθεται στο Παράρτημα). Όπως χαρακτηριστικά αναφέρει διοικητικό στέλεχος μεγάλης ελληνικής

Τράπεζας, «*…ένα τέτοιο εργαλείο έρχεται να αυξήσει την ακρίβεια και να μειώσει τον χρόνο αντίδρασης (πράγμα) το οποίο αποτελεί θεμελιώδες κριτήριο αξιολόγησης για τέτοιου είδους εργαλεία…*». Η σημασία και των δύο αυτών παραγόντων αναλύθηκαν διεξοδικά στις ενότητες 3.3.2, 3.3.3 και 3.3.4).

Επίσης, το IRIS εξυπηρετεί τόσο στην αρχική αξιολόγηση ενός περιστατικού ασφάλειας, όσο και στην αξιολόγησή του σε βάθος χρόνου (μέσω των λειτουργιών βαθμολόγησης αδυναμιών με χρήση ιστορικών και περιβαλλοντικών μετρικών), γεγονός που εκτιμήθηκε ιδιαίτερα από έμπειρο διαχειριστή ασφάλειας μεγάλης ελληνικής Τράπεζας, ο οποίος αναφέρει –μεταξύ άλλων- πως «*…το γεγονός ότι το IRIS μπορεί να βοηθήσει και σε αυτό το τελευταίο βήμα, ενώ επιπλέον μπορεί να χρησιμοποιηθεί και για την επαναξιολόγηση του περιστατικού σε βάθος χρόνου, αυξάνει κατά πολύ την αξία του ως εργαλείο για την ομάδα IT security ενός οργανισμού…*».

Τέλος, ιδιαίτερα ενδιαφέρουσα ήταν η πρόταση ενοποίησης του IRIS με συστήματα διαχείρισης αρχείων ελέγχου και καταγραφής (audit log files), για την αξιολόγηση πληροφοριών που έπονται της εμφάνισης ενός περιστατικού, καθώς και την παροχή τοπολογικών χαρτών για την οπτικοποίηση της πληροφορίας που διαχειρίζεται το εργαλείο.

6.6. Χαρακτηριστικά της διαδικασίας αξιολόγησης

Η διαδικασία αξιολόγησης της λειτουργίας του IRIS και οι μετρήσεις σε εταιρικά περιβάλλοντα παρουσιάζουν αρκετά διαδικαστικά προβλήματα, κυρίως λόγω της ιδιαιτερότητας των δεδομένων που συλλέγει το IRIS για την υποδομή ενός Οργανισμού (αναφορά αδυναμιών ασφάλειας). Τα δεδομένα αυτά χαρακτηρίζονται ως απόρρητα από την πλειονότητα των Οργανισμών και δεν παρέχονται χωρίς κατάλληλη εξουσιοδότηση από υπευθύνους ασφάλειας ή/και νομικούς συμβούλους. Για το σκοπό αυτό, καθώς αποδείχθηκε διαδικαστικά πολύπλοκο στον ερευνητή, επιλέχθηκε η διαδικασία της αξιολόγησης του IRIS από ειδικούς ασφάλειας, οι οποίοι είχαν ελεύθερα διαθέσιμο το εργαλείο και μπορούσαν να χρησιμοποιήσουν τις δικές τους αναφορές ασφάλειας, προκειμένου να μπορέσουν να αξιολογήσουν τις λειτουργίες του. Με βάση τα ελεύθερα

σχόλια, την ταυτότητα του δείγματος αλλά και την πληρότητα των απαντήσεων, η διαδικασία που επιλέχθηκε κρίνεται ως επιτυχημένη.

6.7. Ανακεφαλαίωση

Στο συγκεκριμένο κεφάλαιο παρουσιάστηκε μια αναλυτική αξιολόγηση των χαρακτηριστικών και των λειτουργιών του IRIS. Αξιολογήθηκε η ορθότητα της υλοποίησης του IRIS σύμφωνα με τις απαιτήσεις που ορίστηκαν και παρουσιάστηκαν στα προηγούμενα κεφάλαια, ενώ τα αποτελέσματα των λειτουργιών του εργαλείου αξιολογήθηκαν με πειραματικά δεδομένα. Επίσης, μέσα από μελέτη περίπτωσης (case study) αξιολογήθηκε η λειτουργία του εργαλείου και η συνεισφορά του στην παραμετροποίηση των συστημάτων IDP, αποδεικνύοντας τα οφέλη της τοπολογικής ανάλυσης αδυναμιών ασφάλειας και της λειτουργίας του IRIS. Τέλος, παρουσιάστηκαν και αναλύθηκαν οι απόψεις ειδικών ασφάλειας πληροφοριών από μεγάλους ελληνικούς οργανισμούς, για μια πλειάδα ζητημάτων που αφορούν στο σύστημα. Οι απόψεις των ειδικών ασφάλειας συλλέχθηκαν με τη συμπλήρωση ερωτηματολογίου που διανεμήθηκε, μαζί με την εκτελέσιμη μορφή του εργαλείου, προκειμένου να μπορέσουν να πειραματιστούν και να εξοικειωθούν με το IRIS. Τέλος, συζητήθηκαν γενικότερα χαρακτηριστικά της διαδικασίας αξιολόγησης.

Κεφάλαιο 7

Συμπεράσματα και Μελλοντική Έρευνα

"There is no security on this planet. There is only opportunity"

- **Douglas Mc Arthur**

7.1. Συμπεράσματα

Στη διατριβή αυτή έγινε μία προσπάθεια προσέγγισης του προβλήματος αναγνώρισης και αντιμετώπισης περιστατικών ασφάλειας, έτσι ώστε να δοθούν αποτελεσματικές και αξιόπιστες απαντήσεις στο πρόβλημα. Ακολουθήσαμε μία προσέγγιση πολλαπλών κατευθύνσεων ώστε να καλύψουμε όλες τις διαστάσεις του προβλήματος. Τα προβλήματα, που ορίστηκαν στην ενότητα 1.3, επιλύθηκαν σύμφωνα με όσα περιγράφονται παρακάτω:

- *Οριοθέτηση των όρων «περιστατικό ασφάλειας» και «αντιμετώπιση περιστατικού ασφάλειας»* - για την επίλυση του συγκεκριμένου ζητήματος προτάθηκε και περιγράφηκε μία πλήρης εννοιολογική θεμελίωση των κυριοτέρων όρων που χρησιμοποιούνται στην αντιμετώπιση περιστατικών ασφάλειας, αναλύθηκαν οι μεταξύ τους συσχετίσεις ενώ –παράλληλα- αναλύθηκαν και ταξινομήθηκαν τα δομικά συστατικά ενός περιστατικού ασφάλειας (βλ. ενότητες 2.2 - 2.4),
- *Πολλαπλές συναφείς ερευνητικές περιοχές:* Στις ενότητες 3.4 - 3.4.6 αναλύθηκαν διεξοδικά οι σχετιζόμενες ερευνητικές περιοχές των μηχανισμών αυτόματης ιχνηλάτησης (automated trace back) και ανάλυσης ψηφιακών πειστηρίων (forensics). Για κάθε μία από τις ερευνητικές, αυτές, περιοχές αναλύθηκε εκτενώς η τρέχουσα κατάσταση των δημοφιλέστερων μεθόδων, ενώ αξιολογήθηκαν και παρουσιάστηκαν τα πλεονεκτήματα, τα μειονεκτήματα, καθώς και το πεδίο εφαρμογής και επεκτασιμότητα κάθε μιας από τις μεθόδους αυτές,
- *Αναγνώριση και ανάλυση περιστατικών ασφάλειας:* Στην ενότητα 3.3.2 προτάθηκε και συζητήθηκε μια διαδικασία αναγνώρισης και ανάλυσης περιστατικών ασφάλειας σε έναν οργανισμό,
- *Συνδυασμός τεχνικών και διοικητικών μέτρων σε έναν οργανισμό:* Στην ενότητα 3.2 προτάθηκε και συζητήθηκε εκτενώς ένα διοικητικό μοντέλο αντιμετώπισης περιστατικών ασφάλειας, το οποίο περιλαμβάνει τους ρόλους, τις αρμοδιότητες και τις αλληλεπιδράσεις μεταξύ των ρόλων, στα πλαίσια αντιμετώπισης

περιστατικών ασφάλειας σε έναν οργανισμό. Επίσης, στην ενότητα 3.3 προτάθηκε και αναλύθηκε μια δομημένη μεθοδολογία έξι φάσεων που καλύπτει τον κύκλο ζωής ενός περιστατικού ασφάλειας: πριν την εκδήλωσή του (φάση προετοιμασίας/ενότητες 3.3.1.1-3.3.1.9), κατά την αναγνώρισή του (φάση αναγνώρισης/ενότητες 3.3.2.1-3.3.2.3), κατά την ανάπτυξή του (φάση περιορισμού/ενότητες 3.3.3.1-3.3.3.5 και φάση εξάλειψης/ενότητες 3.3.4.1-3.3.4.3), όσο και μετά την επιτυχή αντιμετώπισή του (φάση ανάκαμψης/ενότητες 3.3.5.1-3.3.5.3 και φάση επακόλουθων/ενότητα 3.3.6). Επίσης, προτάθηκε μια ενδεικτική διαδικασία αντιμετώπισης περιστατικών για έναν Οργανισμό, η οποία περιλαμβάνει ένα διάγραμμα ροής των αποφάσεων που καθορίζουν τις ενέργειες αντιμετώπισης (βλ. ενότητα 3.6),

- *Περιορισμοί μηχανισμών ασφάλειας:* Στις ενότητες 4.4.1-4.4.2 αναλύονται εκτενώς οι περιορισμοί που διέπουν την ανάπτυξη συστημάτων ανίχνευσης και αντιμετώπισης παρεισφρήσεων (IDP) σε μια υπολογιστική υποδομή, ενώ στην ενότητα 4.4.3 παρουσιάζεται το θεωρητικό υπόβαθρο της ανάπτυξης συστημάτων IDP με χρήση τεχνικών τοπολογικής ανάλυσης αδυναμιών ασφάλειας. Το συγκεκριμένο θεωρητικό μοντέλο υλοποιείται σύμφωνα με όσα περιγράφονται στις ενότητες 4.5.1-4.5.6, παρουσιάζεται στις ενότητες 5.2.1-5.2.6 και αξιολογείται σύμφωνα με όσα περιγράφονται στις ενότητες 6.4.1-6.4.4,
- *Τοπολογικά κριτήρια ανάλυσης:* Σύμφωνα με όσα περιγράφηκαν στην ενότητα 4.3, ένα περιστατικό ασφάλειας οφείλεται στην επιτυχή εκμετάλλευση αδυναμιών ασφάλειας με μια προκαθορισμένη σειρά (μονοπάτι επίθεσης). Από την άλλη πλευρά, η ανάλυση ενός μονοπατιού επίθεσης οφείλει να συμπεριλαμβάνει τόσο τα βασικά, ιστορικά και περιβαλλοντικά χαρακτηριστικά μιας αδυναμίας (βλ. ενότητα 5.2.2.3), όσο και την εύρεση διαθέσιμου κώδικα εκμετάλλευσης και των κατάλληλων μηχανισμών αντιμετώπισης (υπογραφές ανίχνευσης και αντιμετώπισης παρεισφρήσεων- (βλ. ενότητα 5.2.2.5)), αφού όλοι αυτοί οι παράγοντες επηρεάζουν τη σημασία και την έκταση του περιστατικού. Από την άλλη πλευρά, σε κάθε μονοπάτι ασφάλειας αντιστοιχεί ένα (ή περισσότερα) μονοπάτια αντιμετώπισης που περιορίζουν την εμφάνιση ή την εκδήλωσή του (βλ. ενότητες 5.2.2.6-5.2.2.7),

- *Αυτοματοποίηση της αναγνώρισης και αντιμετώπισης περιστατικών:* η ανάλυση των περιστατικών με βάση τα τοπολογικά κριτήρια απαιτεί τη συλλογή, κανονικοποίηση και επεξεργασία ενός μεγάλου πλήθους ετερογενών πληροφοριών (βλ. ενότητες 5.2.2.1, 5.2.2.5 και 5.2.2.6). Η αυτοματοποίηση των διεργασιών αυτών με υλοποίηση ενός Συστήματος Αντιμετώπισης Περιστατικών (βλ. κεφάλαιο 5) που απαιτεί μικρότερη εμπλοκή του χρήστη, μειώνει το χρόνο που απαιτείται για την αναγνώριση ενός περιστατικού και την παροχή των τεχνικών μέτρων αντιμετώπισής του,
- *Αξιόπιστα αποτελέσματα:* Τα αποτελέσματα που παράγει το σύστημα IRIS είναι εύκολα αντιληπτά και διευκολύνουν το έργο του διαχειριστή δικτύου στην ανάλυση και αντιμετώπιση των περιστατικών (βλ. ενότητες 6.3, 6.5 και Πίνακα 6-18),
- *Αποτελέσματα σε –σχεδόν- πραγματικό χρόνο:* Οι λειτουργίες του συστήματος εκτελούνται σε –σχεδόν- πραγματικό χρόνο προκειμένου να υπάρχει άμεση πληροφόρηση των διαχειριστών του συστήματος και των ενεργειών που έπονται για την αντιμετώπιση του εν λόγω περιστατικού (βλ. ενότητες 5.2.2.6 και Πίνακα 6-16),
- *Διαχείριση και οπτικοποίηση πληροφοριών*: Το σύστημα αναλύει και επεξεργάζεται δεδομένα ασφάλειας για δικτυακά πρωτόκολλα και υπηρεσίες που δεν είναι αναγνώσιμα από τον άνθρωπο και τα παρέχει σε μορφή –εύκολα-αναγνώσιμης πληροφορίας (βλ. ενότητα 5.2.2.6 και Πίνακες 6-12, 6-14, 6-15 και 6-17,
- *Λειτουργίες αξιολόγησης επικινδυνότητας:* Το σύστημα δεν χάνει τη "γενική εικόνα" όταν εξετάζει λεπτομέρειες χαμηλού επιπέδου, με αποτέλεσμα οι αποφάσεις αντιμετώπισης να βασίζονται τόσο στα ιδιαίτερα χαρακτηριστικά της υποδομής στην οποία εκδηλώνεται ένα περιστατικό, όσο και στον αντίκτυπο των ενεργειών αντιμετώπισης (βλ. ενότητα 5.2.2.3 και Πίνακα 6-17),
- *Ευκολία χρήσης:* Σύμφωνα με όσα περιγράφονται στους Πίνακες 6-12 και 6-19, ο διαχειριστής του συστήματος δεν απαιτείται να έχει υπερβολική ειδίκευση,
- *Μεταφέρσιμη πλατφόρμα υλοποίησης:* Η υλοποίηση του συστήματος, σύμφωνα με όσα περιγράφονται στις ενότητες 5.2.3.1-5.2.3.6 και 6.2.1 έχει βασιστεί σε

ανοικτά πρότυπα και τεχνολογίες, ώστε να διευκολύνεται η πρόσβαση στην πλατφόρμα του IRIS μέσω διαφορετικών συστημάτων,

- *Ανανέωση και συντήρηση συστήματος:* Το σύστημα IRIS έχει τη δυνατότητα ανανέωσης ώστε να ανταποκρίνεται σε νέες δικτυακές συνθήκες και επιθέσεις, σύμφωνα με όσα περιγράφονται στην ενότητα 4.5.3 και στην ενότητα 6.2.3), και να είναι προσαρμόσιμο τόσο στις αλλαγές της υποδομής που εξετάζει, όσο και στην ποιότητα και ποσότητα των πληροφοριών που επεξεργάζεται.

7.2. Προτάσεις για μελλοντική έρευνα

Η αναγνώριση και αντιμετώπιση περιστατικών ασφάλειας αποτελεί ένα δομικό στοιχείο σε –σχεδόν- κάθε μοντέρνο σχέδιο ασφάλειας ενός Οργανισμού. Η συγκεκριμένη διατριβή πρότεινε και παρουσίασε τρόπους, μεθόδους, τεχνικές και εργαλεία για την επίλυση μιας σειράς ζητημάτων που σχετίζονται με το συγκεκριμένο πρόβλημα, τόσο από ερευνητική όσο και από πρακτική πλευρά. Υπάρχουν, όμως, πολλές δυνατότητες για τη βελτίωση, τον εμπλουτισμό και τη βελτιστοποίηση των προτεινόμενων προσεγγίσεων, τόσο μέσα από προγραμματιστικές/αλγοριθμικές τροποποιήσεις όσο και με νέες τεχνικές εξερεύνησης και χρήσης διαφορετικών μεθοδολογιών.

Για παράδειγμα, σύμφωνα με τον Πίνακα 6-20, το 60% του δείγματος αξιολόγησης προτείνει να μετατραπεί το IRIS σε εφαρμογή ιστού (web application). Με δεδομένη την ολοένα και μεγαλύτερη αποδοχή των εφαρμογών ιστού στις επιχειρησιακές εφαρμογές, η υλοποίηση του IRIS σε συγκεκριμένη πλατφόρμα θα μπορούσε, δυνητικά, να προσφέρει τις παρακάτω λειτουργίες:

- Ελεγχόμενη πρόσβαση από πολλαπλούς χρήστες
- Πρόσβαση με βάση το ρόλο (Role Based Access Control – RBAC) για το σύνολο των συμμετεχόντων στην εταιρική διαδικασία αντιμετώπισης περιστατικών
- Εκτέλεση του εργαλείου υπό τη μορφή υπηρεσίας ιστού (software as a service – SaaS)

- Ελάχιστες απαιτήσεις από τη μεριά του χρήστη (χρήση μόνο ενός προγράμματος φυλλομέτρησης ιστοσελίδων – web browser, που αποτελεί δομικό στοιχείο κάθε σύγχρονου λειτουργικού συστήματος)
- Πρόσβαση στην εφαρμογή από ετερογενείς πλατφόρμες και συσκευές (π.χ. φορητές συσκευές, κινητά τηλέφωνα, κτλ.)

Επίσης, αποτελεί μελλοντικό στόχο η ενοποίηση του IRIS με περισσότερα εργαλεία αποτίμησης αδυναμιών και συστημάτων IDP, για την αύξηση του πεδίου εφαρμογής του εργαλείου (περισσότερο ετερογενείς υποδομές). Αν και η συγκεκριμένη προσπάθεια στηρίζεται κατά πολύ στους κατασκευαστές των συγκεκριμένων εργαλείων/συστημάτων (παροχή προγραμματιστικού περιβάλλοντος – API στον ερευνητή για τα συστήματα ενδιαφέροντος), διαφαίνεται η τάση εξαγωγής των αναφορών των συγκεκριμένων εργαλείων/συστημάτων σε μορφότυπο XML για επεξεργασία από τρίτα προϊόντα. Κατά τη διάρκεια της συγγραφής της διατριβής, ολοκληρώθηκε η ενοποίηση του συστήματος με ένα εμπορικό εργαλείο αποτίμησης ευπαθειών (Qualys) και ένα εμπορικό σύστημα IDP (IBM/ISS).

Επιπροσθέτως, κρίνεται σκόπιμο να ερευνηθεί η ενοποίηση του IRIS με μια σειρά από ερευνητικές προσπάθειες που αφορούν στη διαχείριση πληροφοριών ασφάλειας. Ενδεικτικά, εκτός από τη λίστα CVE και το σύστημα βαθμολόγησης CVSSv2 που ήδη ενσωματώνονται στο εργαλείο και λειτουργούν αποδοτικά, αποτελεί μεγάλη ερευνητική πρόκληση η ενοποίηση με τα παρακάτω –παρόμοια- πρότυπα:

- Πρότυπο κοινής περιγραφής πλατφόρμας (Common Platform Enumeration – CPE, (CPE, 2009), το οποίο παρέχει ένα δομημένο σχήμα ονοματοδοσίας και περιγραφής για πληροφοριακά συστήματα, συστήματα τεχνολογίας, πλατφόρμες και πακέτα λογισμικού,
- Πρότυπο κοινής περιγραφής ευπαθειών (Common Weaknesses Enumeration – CWE, (CWE, 2009), το οποίο παρέχει ένα ενιαίο και μετρήσιμο σύνολο αδυναμιών λογισμικού που επιτρέπει την αποδοτική περιγραφή, επιλογή και χρήση εργαλείων λογισμικού με σκοπό την ανεύρεση και αξιολόγηση αδυναμιών στον πηγαίο κώδικα του λογισμικού,

- Πρότυπο κοινής περιγραφής διαμόρφωσης συστήματος (Common Configuration Enumeration – CCE, (CCE, 2009), το οποίο παρέχει μοναδιαίους περιγραφητές σε διαμορφώσεις και ρυθμίσεις συστημάτων, με σκοπό τη γρήγορη και ακριβή συσχέτιση δεδομένων παραμετροποίησης μεταξύ πολλαπλών πηγών και εργαλείων,
- Πρότυπο κοινής περιγραφής και ταξινόμησης επιθέσεων (Common Attack Pattern Enumeration and Classification – CAPEC, (CAPEC, 2009)), το οποίο στοχεύει στην παροχή μιας δημόσιας-προσβάσιμης λίστας μοτίβων επίθεσης, μαζί με ένα σχήμα περιγραφής και ταξινόμησης αυτών.

Από την άλλη πλευρά, η εξέλιξη των πληροφοριακών συστημάτων και των εφαρμογών, η υιοθέτηση των εφαρμογών ιστού (web applications) και τα κοινωνικά δίκτυα (social networks), φαίνεται πως αλλάζουν αρκετά το είδος και τη συχνότητα των επιθέσεων. Για παράδειγμα, τα τελευταία χρόνια, οι επιθέσεις στις εφαρμογές ιστού αποτελούν ένα μεγάλο ποσοστό των συνολικών επιθέσεων σε πληροφοριακά συστήματα. Οι συγκεκριμένες επιθέσεις βασίζονται σε ξεχωριστή λογική και φιλοσοφία από τις αντίστοιχες σε υπολογιστικά συστήματα και δίκτυα, ενώ η αντιμετώπισή τους απαιτεί διαφορετικούς μηχανισμούς ασφάλειας (π.χ. τείχη προστασίας για εφαρμογές ιστού – web application firewalls/WAFs). Τα συστήματα WAF ακολουθούν τη φιλοσοφία των συστημάτων IDP (αναγνώριση μοτίβων και στατιστική ανάλυση) για συγκεκριμένα δικτυακά πρωτόκολλα και εφαρμογές (π.χ. HTTP, SQL, LDAP, κτλ.). Από την άλλη πλευρά, έχουν αναπτυχθεί ειδικά εργαλεία και τεχνικές αποτίμησης αδυναμιών εφαρμογών ιστού (web application vulnerability scanners), τα οποία λειτουργούν – επίσης- με την αντίστοιχη φιλοσοφία των παραδοσιακών εργαλείων αποτίμησης αδυναμιών ασφάλειας. Συχνά, τόσο για τα συστήματα WAF όσο και για τα εργαλεία αποτίμησης αδυναμιών εφαρμογών ιστού υπάρχει επικάλυψη με τα συστήματα IDP και τα παραδοσιακά εργαλεία αποτίμησης αδυναμιών.

Με δεδομένη την έξαρση των συγκεκριμένων επιθέσεων, αποτελεί πρόταση για μελλοντική ανάπτυξη του IRIS η ενοποίησή του με εργαλεία αποτίμησης αδυναμιών εφαρμογών ιστού και συστήματα WAF, για την αύξηση του πεδίου εφαρμογής του

εργαλείου. Προς τον σκοπό αυτό, υπάρχει μια πλειάδα ερευνητικών ζητημάτων που παραμένουν ακόμη ανοικτά, όπως:

- Η ταξινόμηση των επιθέσεων εφαρμογών ιστού
- Η υιοθέτηση μιας κοινά αποδεκτής ονοματοδοσίας και μορφότυπου περιγραφής των επιθέσεων εφαρμογών ιστού (αντίστοιχη της λίστας CVE)
- Η ανάπτυξη και υιοθέτηση ενός πρότυπου συστήματος βαθμολόγησης των συγκεκριμένων αδυναμιών
- Η ενοποίηση των συστημάτων WAF με συστήματα βάσεων δεδομένων

Εκτός των διαφόρων προγραμματιστικών βελτιώσεων του IRIS, αποτελεί μελλοντικό στόχο η ανάπτυξη φορμαλισμού για την αντιμετώπιση περιστατικών, προκειμένου να παρουσιαστεί και να τεκμηριωθεί ακαδημαϊκά η διοικητική προσέγγιση της αντιμετώπισης περιστατικών. Ενδεικτικά, μία τέτοια προσέγγιση θα μπορούσε να ξεκινήσει με την κατασκευή μιας γλώσσας πολιτικών (policy language) με την παρακάτω δομή:

- πεδίο εφαρμογής αντιμετώπισης περιστατικών ασφάλειας (incident response policy domain), το οποίο θα περιγράφει λεπτομερώς το σύστημα στο οποίο διενεργείται η συγκεκριμένη διαδικασία,
- ρόλους, που θα περιγράφουν το σύνολο των συμμετεχόντων στην εταιρική διαδικασία αντιμετώπισης περιστατικών ασφάλειας,
- δραστηριότητες, οι οποίες θα περιγράφουν την παροχή (ή μη) ενός δικαιώματος πρόσβασης ενός ρόλου σε ένα αντικείμενο,
- αντικείμενα, τα οποία θα περιλαμβάνουν τα λογικά αντικείμενα της υπολογιστικής και δικτυακής υποδομής που ανήκουν στο πεδίο εφαρμογής,
- εξουσιοδοτήσεις, οι οποίες θα περιγράφουν τις ενέργειες αντιμετώπισης περιστατικών,
- καταστάσεις συστήματος και μεταβολές, όπου θα περιγράφονται οι καταστάσεις του συστήματος κατά τη διάρκεια του κύκλου ζωής ενός περιστατικού ασφάλειας (π.χ. κανονική κατάσταση, κατάσταση εκδήλωσης περιστατικού, κατάσταση

αντιμετώπισης, κτλ.) καθώς και τα κριτήρια μεταβολής από μια κατάσταση του συστήματος σε μια άλλη,

- Κανόνες αντιμετώπισης περιστατικών εκφρασμένους με αλγεβρική λογική.

Ιδανικά, η παραπάνω γλώσσα θα μπορούσε, επίσης, να ενσωματωθεί στο IRIS, για την κατασκευή των διοικητικών ενεργειών που αφορούν στην αντιμετώπιση περιστατικών, με βάση τις πληροφορίες που παρέχει το συγκεκριμένο σύστημα.

Βιβλιογραφία

Aberdeen Group. (2003). *Turning IT security into effective business risk management.* NJ, USA: Computer Associates S.A.

Adelstein, F. (2006). Live Forensics: Diagnosing your system without killing it first. *Communications of the ACM , 49* (2), 63-66.

Allen, J. (2001). *CERT Guide to System and Network Security Practices.* NY: Addison-Wesley.

Ammann, P., Wijesekera, D., & Kaushik, S. (2002). Scalable, graph-based network vulnerability analysis. *Proceedings of the 9th ACM conference on Computer and communications security*, (pp. 217-224). Washington, DC, USA .

Atkins D., Buis, P., Hare, C., Kelley, R., Nachenberg, C., Nelson, A., Phillips, P., Ritchey, T., and Steen, W. (1997), Internet Security Professional Reference, New Riders Publishing; 2nd edition

Brumley, D., Newsome, J., Song, D., Wang, H., & Jha, S. (2006). Towards Automatic Generation of Vulnerability-Based Signatures. *IEEE Symposium on Security and Privacy*, (pp. 2-16). Oakland, California.

Brumley, et. al. (2007). *Theory and Techniques for Automatic Generation of Vulnerability-Based Signatures.* Pittsburgh, PA: Carnegie Mellon University, School of Computer Science.

BSI. (1999). *BS 7799-1:1999 Information security management - Part 1:Code of practice for information security management.* London: British Standard Organization.

BugTraq. (2009). *BugTraq.* Retrieved March 8, 2009, from SecurityFocus: http://www.securityfocus.com/archive/1

CAPEC (2009), Common Attack Pattern Enumeration and Classification, A Community Knowledge Resource for Building Secure Software, online: http://capec.mitre.org/, ανακτήθηκε: 25 Μαϊου 2009

CCE (2009), Common Configuration Enumeration, Unique Identifiers for Common System Configuration Issues, online: http://cce.mitre.org/, ανακτήθηκε: 25 Μαϊου 2009

CERT/CC. (1998, February). *Security Of The Internet.* Ανάκτηση 17-2-2009, από http://www.cert.org/encyc_article/tocencyc.html

Chien, E., & Szor, P. (2002). Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques in Computer Viruses. *Virus Bulletin Conference* (pp. 1-35). Louisiana: Virus Bulletin Ltd.

Cisco. (2008), *Cisco Security Response: Cisco VLAN Trunking Protocol Vulnerability, Document ID: 108203.* Ανάκτηση, Μάρτιος 8, 2009, από Cisco Systems: http://www.cisco.com/

Cisco. (2009). *Products & Services Security Advisories, Cisco Security Advisories and Notices.* Ανάκτηση, Μάρτιος 8, 2009, από Cisco Systems: www.cisco.com/web/go/psirt

Conklin, A. D. (2008). Systems Theory Model for Information Security. *41st Annual International Conference on System Sciences.* Hawaii.

Council of Europe. (2001). *Convention on Cyber Crime, European Treaty Series – No. 185.* Budapest.

CPE (2009), Common Platform Enumeration, A structured naming scheme for IT systems, platforms and packages, online: http://cpe.mitre.org/, ανακτήθηκε: 25 Μαϊου 2009

Cui, W., Peinado, M., Wang, H., & Locasto, M. (2007). ShieldGen: Automatic Data Patch Generation for Unknown Vulnerabilities with Informed Probing. *Proceedings of IEEE Symposium on Security and Privacy*, (pp. 252-266). Oakland, California.

CWE (2009), Common Weaknesses Enumeration, A community-developed dictionary of software weakness types, online: http://cwe.mitre.org/, ανακτήθηκε: 25 Μαϊου 2009

Debar, H., Thomas, Y., Cuppens, F., & Cuppens-Boulahia, N. (2007). Enabling automated threat response through the use of a dynamic security policy. *Journal of Computer Virology , 3* (195-2).

Douligeris, C., & Mitrokotsa, A. (2007). Denial-of-Service Attacks. Στο C. Douligeris, & D. Serpanos, *Network Security: Current status and future directions* (σσ. 117-135). Wiley.

Gollmann, D. (1999). *Computer Security.* London, UK: Wiley and Sons.

Gula, R. (2009, January). *Correlating IDS Alerts with Vulnerability Information.* Ανάκτηση, Μάρτιος 8, 2009, από Tenable Network Security: http://www.nessus.org

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security , 42* (1), 31-43.

Harris Interactive. (2003). *Identity Theft New Survey & Trend Report.* Privacy & American Business.

Howard, J. D., & Longstaff, T. (1998). *A Common Language for Computer Security Incidents.* California, US: Sandia National Laboratories.

IBM. (2009). *Proventia Network Enterprise Scanner*. Ανάκτηση, Μάρτιος 8, 2009, από IBM Corporation: http://www-935.ibm.com/services/us/index.wss/offering/iss/a1027216

IEEE (1996), The IEEE Standard Dictionary of Electrical and Electronics Terms, Sixth Edition, John Radatz, Editor, Institute of Electrical and Electronics Engineers, Inc., New York, NY.

IEEE. (2003). *802.1q, IEEE Standards for Local and metropolitan area networks, Virtual Bridged Local Area Networks.* New York, NY: IEEE Computer Society, Sponsored by the LAN/MAN Standards Committee.

IEFT. (1998). *Request for Comments (RFC) 2350, "Expectations for Computer Security Incident Response".* Internet Engineering Task Force .

IETF. (1992). *Request for Comments (RFC) 1305, Network Time Protocol (Version 3) – Specification, Implementation and Analysis.* Internet Engineering Task Force.

Information Security Team. (2002). *A Framework for Incident Response (Draft).* Chicago, IL: DePaul University.

ISO/IEC JTC 1. (2004). *ISO/IEC TR 18044, Information technology -- Security techniques -- Information security incident management.* Geneva: ISO.

ISO/IEC JTC 1/SC 27. (2005). *ISO/IEC FDIS 17999 - Information technology — Security techniques - Code of Practice for information security management.* DIN, Germany: ISO.

ISO/IEC JTC1. (2005). *ISO/IEC FDIS 27001:2005, Information Technology - Security Techniques - Information Security Management systems - Requirements.* Gevena: ISO/IEC.

Jajodia, S., Noel, S., & O'Berry, B. (2006). Topological Analysis of Network Attack Vulnerability. In V. Kumar, J. Srivastava, & A. Lazarevic, *Managing Cyber Threats: Issues, Approaches, and Challenges* (pp. 247-266). Heidelberg: Springer.

Jajodia, S., Noel, S., (2007) Topological Vulnerability Analysis: A Powerful New Approach for Network Attack Prevention, Detection, and Response,*in Algorithms, Architectures, and Information Systems Security, B. Bhattacharya, S. Sur-Kolay, S. Nandy, and A. Bagchi (eds.), World Scientific Press,*

JPCERT. (2009). *JPCERT/CC*. Ανάκτηση, Μάρτιος 8, 2009, από Japan Computer Emergency Response Team Coordination Center: http://www.jpcert.or.jp/english/

Killcrece, G., Kossakowski, K. P., Ruefle, R., & Zajicek, M. (2003). *Organizational Models for Computer Incident Response Teams (CSIRTs), , Report: CMU/SEI-2003-HB-001*. Pittsburgh: Carnegie Melon University/Software Engineering Institute.

Killourhy, K., Maxion, R., and Tan, K. (2004), A Defense-Centric Taxonomy Based on Attack Manifestations, *Proceedings of the International Conference on Dependable Systems & Networks: Florence, Italy, 28 June - 01 July*

Kim, D. W., Choi, Y., Kim, I. K., Oh, J. T., & Oh, J. T. (2008). *Patent No. US20080083034A1*. US.

Kossakowski, K. P., & al., e. (1999). *Responding to Intrusions, Report: CMU/SEI-SIM-006.* Pittsburgh: Carnegie Melon University/Software Engineering Institute.

Krasser, S., Conti, G., Grizzard, J., & Gribschaw, J. (2005). Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization. *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security,* (pp. 42-49). United States Military Academy, West Point, NY.

Krsul, I. (1998). *Software Vulnerability Analysis (Ph.D. Dissertation).* Lafayette, IN: Computer Sciences Department, Purdue University.

Lampson, B., Abadi, M., Burrows, M., & Wobber, E. (1992). Authentication in Distributed Systems:Theory and Practice. *ACM Trans. Computer Systems , 10* (4), 265-310.

Mandia, C., & Procise, C. (2002). *Incident Response, Investigating Computer Crime.* NY: Osborne/McGraw-Hill.

Mathew, S., Britt, D., Giomundo, R., & Upadhyaya, S. (2005). Real-time multistage attack awareness through enhanced intrusion alert clustering. *Proceedings of Military Communications Conference, MILCOM.,* (pp. 1801-1806). New Jersey, NJ.

McAfee. (2009). *McAfee Vulnerability Manager (formerly Foundstone)*. Ανάκτηση, Μάρτιος 8, 2009, από McAfee Inc: http://www.mcafee.com/

Mell, P., Scarfone, K., & Romanosky, S. (2006). Common Vulnerability Scoring System. *IEEE Security & Privacy , 4* (6), 85-89.

Microsoft. (2002). *Microsoft Security Response Center Security Bulletin Severity Rating System.* Ανάκτηση, Μάρτιος 8, 2009, από Microsoft Corporation: http://www.microsoft.com/technet/security/

Microsoft. (2009). *Microsoft Security Response Center.* Ανάκτηση, Μάρτιος 8, 2009, από Microsoft Corporation: http://www.microsoft.com/security/msrc/default.mspx

Miniwatts Marketing Group. (2009). *The Internet Big Picture:World Internet Users and Population Stats*. Ανάκτηση 17-2-2009, από Internet World Stats, Usage and Population Statistics: http://www.internetworldstats.com/stats.htm

Mitnick, K., Simon, W., & Wozniak, S. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN: Wiley Publishing.

MITRE. (2009). *Common Vulnerabliities and Exposures, The Standard for Information Vulnerability Names.* Ανάκτηση, Μάρτιος 8, 2009, από http://cve.mitre.org/

Mitropoulos S., Patsos D., and Douligeris C. (2005), Network Forensics: Towards a classification of traceback mechanisms, *Proceedings of Network Forensics Research Workshop, First IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SECURECOMM 2005), Athens, Greece, 5-9 September*

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A State of the Art Approach. *Computers and Security , 25* (5), 351-370.

Mitropoulos, S., Patsos, D., & Douligeris, C. (2007). Incident Response Requirements for Distributed Security Information Management. *Journal of Information Management & Computer Security, , 15* (3), 226-240.

Miura-Ko, R., & Bambos, N. (2007). SecureRank: A Risk-Based Vulnerability Management Scheme for Computing Infrastructures. *Proceedings of the ICC07, IEEE International Conference on Communications.* Glasgow.

Noel, S., Jajodia, S. (2009), Advanced Vulnerability Analysis and Intrusion Detection through Predictive Attack Graphs, *Critical Issues in C4I, Armed Forces Communications and Electronics Association (AFCEA) Solutions Series, Lansdowne, Virginia, May*

Newsome, J., & Song, D. (2005). Dynamic Taint Analysis for Automatic Detection, Analysis, and Signature Generation of Exploits on Commodity Software. *Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS).* California.

Ning, P., & Xu, D. (2003). Learning attack strategies from intrusion alerts. *Learning attack strategies from intrusion alerts*, (pp. 200-209). Washington D.C.

NIST. (2004). *Computer Security Incident Handling Guide, NIST Special Publication 800-61*. National Institute of Standards and Technology.

NVD. (2009). *National Vulnerability Database Version 2.2*. Ανάκτηση, Μάρτιος 8, 2009, από NIST Computer Security Resource Center (CSRC): http://nvd.nist.gov/

O'Hare, S. Noel, S. and Prole, K. (2008), A Graph-Theoretic Visualization Approach to Network Risk Analysis, *J.R. Goodall, G. Conti, and K.-L. Ma (Eds.): VizSec 2008, LNCS 5210, pp. 60–67, Springer-Verlag Berlin Heidelberg*

OSI/IEC. (1994). *ISO 7498-1, Information Technology, Open Systems Interconnection, Basic Reference Model: The Basic Model* . Geneva: International Standards Organization, .

Papadaki, M., & Furnell, S. M. (2006). Achieving automated intrusion response: a prototype implementation. *Information Management & Computer Security , 14* (3), 235-251.

Patsos, D., Mitropoulos, S., & Douligeris, C. (2007). Generating adaptive security policies and automated configuration scenarios by correlating vulnerability and intrusion information. *Proceedings of the PCI07, 11th Panhellenic Conference on Informatics*, (pp. 117-130). Patras, Greece.

Patsos, D. (2002). *A Strategic Approach to Incident Response (M.Sc. Thesis).* London, UK: Royal Holloway University of London.

PCI SSC. (2008). *Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures, Version 1.2.* Wakefield, MA: PCI Standards Security Council.

Pietraszek, T. (2004), Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection, *Lecture Notes in Computer Science, Volume 3224/2004, p.p. 102-124, Springer Berlin / Heidelberg*

Piper, F. (2002, April). Personal Conversations and Lectures. (D. Patsos, Συνέντευξη στον/στην) London, UK.

Qualys, QualysGuard Vulnerability Management, Operationalize Vulnerability and Risk Management — On Demand, Διαθέσιμο: http://www.qualys.com/, Ανακτήθηκε στις: 17 Μαΐου 2009

Ragsdale, D., Carver, C., Humphries, J., & Pooch, U. (2000). Adaptation techniques for intrusion detection and intrusionresponse systems. *Proceedings of the 2000 IEEE International Conference on Systems, Man, and Cybernetics, ,* (pp. 2344-2349). Nashville, TN.

Rasheed, H., & Chow, R. (2007). An Information Model for Security Integration. *Proceedings of the 11th IEEE International Workshop on Future Trends of Distributed Computing Systems*, (pp. 41-47). Sedona, Arizona.

Scambray, J., Mc Clure, S., & Kurtz, G. (2001). *Hacking Exposed.* Berkeley, California: Osborne/McGraw-Hill.

Scarfone, K., & Mell, P. (2008). *Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology, SP 800-94.* Gaithersburg, MD: NIST.

Schultz, E. (2004). Incident Response Teams Need to Change. *Computers and Security Journal* 4, 87-88.

SecurityFocus. (2009). *Vulnerabilities.* Ανάκτηση, Μάρτιος 8, 2009, από Security Focus: http://www.securityfocus.com/vulnerabilities

Sheyner, O., Haines, J., Jha, S., & Lippmann, R. (2002). Automated Generation and Analysis of Attack Graphs. *Proceedings of IEEE Symposium on Security and Privacy*, (pp. 273-284). Oakland, California.

Solove, D. (2004). The Legal Construction of Identity Theft. *Symposium: Digital Cops in a Virtual Environment.* Yale Law School, March 26-28.

Srilatha, C., Ajith, A., & Johnson, P. T. (2004). Feature deduction and ensemble design of intrusion detection systems. *Computers & Security , 24* (4), 295-307.

Stakhanova, N., Basu, S., & Wong, J. (2007). A taxonomy of intrusion response systems. *International Journal of Information and Computer Security , 1* (1-2), 169-184.

Stoll, C. (1990). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (Paperback).* Pocket Books.

Swiler, L., Phillips, C., Ellis, D., & Chaker, M. (2001). Computer-Attack Graph Generation Tool. *DISCEXII Proceedings, DARPA's Information Survivability Conference and Exposition. 2,* (pp. 307-321). Anaheim, California: IEEE Computer Society Press.

Tian Z., Zhang, W., Ye Z., Yu, A., Zhang, H. (2008), Reduction of false positives in intrusion detection via adaptive alert classifier, *Proceedings of the International Conference on Information and Automation (ICIA 2008), p.p. 1599-1602, Changsha. 20-23 June*

Templeton, S., & Levitt, K. (2000). A Requires/Provides Model for Computer Attacks. *Proceedings of the New Security Paradigms Workshop,* (pp. 31-38). Ballycotton, County Cork, Ireland.

Tenable. (2009). *The Network Vulnerability Scanner*. Ανάκτηση, Μάρτιος 8, 2009, από Tenable Network Security: http://www.nessus.org/nessus/

Tung, B. (2000). The Common Intrusion Specification Language: A Retrospective. *DARPA Information Survivability Conference & Exposition - Volume 2,* (pp. 36-45). Hilton Head, SC.

US Gov. (2000). *OMB's Circular No. A-130, Appendix III, Transmittal Memorandum No. 4.* Washington, DC: Office of Management and Budget.

US Gov. (2002). *United States Code, Chapter 35 of Title 44, Subchapter III – Information Security, Federal Information Security Management Act (FISMA) of 2002,* Washington, DC.

US-CERT. (2009). *Technical Security Alerts.* Ανάκτηση, Μάρτιος 8, 2009, από United States Computer Emergency Readiness Team: http://www.cert.org/advisories/

US-CERT. (2009). *Vulnerability Notes Database Field Descriptions.* Ανάκτηση, Μάρτιος 8, 2009, από United States Computer Emergency Readiness Team.

Van Wyk, K., & Forno, R. (2001). *Incident Response.* NY: O'Reilly.

Voas, J., Ghosh, A., McGraw, G., Charron, F., & Miller, K. (1996). Defining an adaptive software security metric from a dynamicsoftware failure tolerance measure. *Proceedings of the Eleventh Annual Conference on Computer Assurance, COMPASS '96, 'Systems Integrity. Software Safety. Process Security'*, (σσ. 250-263). Gaithersburg, MD, USA.

West-Brown, M., Stikvoort, D., & Kossakowski, K. (1998). *Handbook for Computer Security Incident Response Teams (CSIRTs), Report: CMU/SEI-98-HB-001.* Pittsbugh, PA: Carnegie Melon University/Software Engineering Institute.

Yasincac, E., & Manzano, Y. (2001). Policies to Enhance Computer and Network Forensics. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.* United States Military Academy, West Point, NY.

Yegneswaran, V., Giffin, J., Barford, P., & Jha, S. (2005). An Architecture for Generating Semantics-Aware Signatures. *Proceedings of the 14th USENIX Security Symposium.* Baltimore, MD.

ΑΔΑΕ (2005), Αρχή Διασφάλισης Απορρήτου Επικοινωνιών, ΑΠΟΦΑΣΗ 630 α «Κανονισμός για την Διασφάλιση του Απορρήτου κατά την Παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών» (ΦΕΚ Β' 87, σελ. 1020-1025)

Γκρίτζαλης, Δ. (2004). Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση. Στο Σ. Κάτσικας, Σ. Γκρίτζαλης, & Δ. Γκρίτζαλης, *Ασφάλεια Πληροφοριακών Συστημάτων* (σσ. 19-50). Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

ΕΔΕΤ. (2009). *CERT*. Ανάκτηση, Μάρτιος 8, 2009, από GRNET-CERT, Greek Research and Technology Network - Computer Emergency Response Team: http://cert.grnet.gr/

Κάβουρας, Ι. (2003). *Οργάνωση Συστημάτων Υπολογιστών*. Αθήνα: Κλειδάριθμος.

Κοκολάκης, Σ. (2000). *Ανάπτυξη και Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων (Διδακτορική Διατριβή)*. Αθήνα: Οικονομικό Πανεπιστήμιο Αθηνών.

Σουρής, Α., Πατσός, Δ., & Γρηγοριάδης, Ν. (2004). *Ασφάλεια της Πληροφορίας: στους υπολογιστές, στο Internet, στην καθημερινή ζωή*. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

Παράρτημα Α – Πηγές Συλλογής Πληροφοριών του IRIS

ΟΝΟΜΑ	ΠΕΡΙΓΡΑΦΗ	ΠΗΓΗ	ΤΥΠΟΣ
AUSCERT	AUSCERT advisory	http://www.auscert.org.au/Information/advisories.html	ΣΥΝΤΟΝΙΣΤΙΚΟ ΚΕΝΤΡΟ
CERT	CERT/CC Advisories	http://www.cert.org/advisories	ΣΥΝΤΟΝΙΣΤΙΚΟ ΚΕΝΤΡΟ
CERT-VN	CERT/CC vulnerability note	http://www.kb.cert.org/vuls	ΣΥΝΤΟΝΙΣΤΙΚΟ ΚΕΝΤΡΟ
CIAC	DOE CIAC (Computer Incident Advisory Center) bulletins	http://ciac.llnl.gov/cgi-bin/index/bulletins	ΣΥΝΤΟΝΙΣΤΙΚΟ ΚΕΝΤΡΟ
FRSIRT	French Security Incident Response Team (FrSIRT) Database	http://www.frsirt.com/english/	ΣΥΝΤΟΝΙΣΤΙΚΟ ΚΕΝΤΡΟ
JVN	Japanese CERT (JPCERT) vulnerability notes	http://jvn.jp/en/report/index.html	ΣΥΝΤΟΝΙΣΤΙΚΟ ΚΕΝΤΡΟ
JVNDB	JVN iPedia	http://jvndb.jvn.jp/	ΣΥΝΤΟΝΙΣΤΙΚΟ ΚΕΝΤΡΟ
EEYE	eEye security advisory	http://www.eEye.com	ΕΜΠΟΡΙΚΗ ΥΠΗΡΕΣΙΑ
IDEFENSE	iDEFENSE advisory	http://labs.idefense.com/intelligence/vulnerabilities/	ΕΜΠΟΡΙΚΗ ΥΠΗΡΕΣΙΑ
SECUNIA	Secunia Advisories	http://secunia.com/advisories/	ΕΜΠΟΡΙΚΗ ΥΠΗΡΕΣΙΑ
SREASON	SecurityReason SecurityAlert	http://securityreason.com/security_alert	ΕΜΠΟΡΙΚΗ ΥΠΗΡΕΣΙΑ
SREASONRES	SecurityReason Research Advisory	http://securityreason.com/research	ΕΜΠΟΡΙΚΗ ΥΠΗΡΕΣΙΑ
BEA	BEA security advisory	http://dev2dev.bea.com/advisoriesnotifications/index.csp	ΛΙΣΤΑ
BID	Security Focus Bugtraq ID database entry	http://online.securityfocus.com/bid	ΛΙΣΤΑ
BINDVIEW	BindView security advisory	http://razor.bindview.com/publish/index.shtml	ΛΙΣΤΑ
BUGTRAQ	Posting to Bugtraq mailing list	http://www.securityfocus.com/archive/1	ΛΙΣΤΑ
FULLDISC	Full-Disclosure mailing list	http://lists.grok.org.uk/pipermail/full-disclosure/	ΛΙΣΤΑ
NTBUGTRAQ	Posting to NTBugtraq mailing list	http://www.ntbugtraq.com/default.asp?pid=36&sid=1	ΛΙΣΤΑ
SECTRACK	SecurityTracker Alerts	http://www.securitytracker.com	ΛΙΣΤΑ
SGI	SGI Security Advisory	http://www.sgi.com/support/security/advisories.html	ΛΙΣΤΑ
VIM	Vulnerability Information Managers mailing list	http://www.attrition.org/pipermail/vim/	ΛΙΣΤΑ
VULN-DEV	Posting to VULN-DEV mailing list	http://online.securityfocus.com/archive/82/	ΛΙΣΤΑ
VULNWATCH	VulnWatch mailing list	http://archives.neohapsis.com/archives/vulnwatch/	ΛΙΣΤΑ
VUPEN	VUPEN Security Database	http://www.vupen.com/english/	ΛΙΣΤΑ
MILW0RM	milw0rm exploit web site	http://www.milw0rm.com/	ΕΡΕΥΝΑ
OSVDB	Open Source Vulnerability Database (OSVDB) entry	http://www.osvdb.org	ΕΡΕΥΝΑ
OVAL	Open Vulnerability Assessment Language (OVAL) vulnerability definition	http://oval.mitre.org	ΕΡΕΥΝΑ

XF	X-Force Vulnerability Database	http://xforce.iss.net	ΕΡΕΥΝΑ
ATSTAKE	@stake security advisory	http://www.atstake.com/research/advisories/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
APPLE	Apple Security Update	http://lists.apple.com/archives/security-announce	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
CALDERA	Caldera security advisory	http://www.calderasystems.com/support/security/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
CHECKPOINT	Check Point Alert	http://www.checkpoint.com/techsupport/alerts/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
CISCO	Cisco security advisory	http://www.cisco.com/warp/public/707/advisory.html	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
COMPAQ	COMPAQ Service Security Patch	http://ftp.support.compaq.com/patches/.new/security.html	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
CONECTIVA	Conectiva Linux advisory	http://lwn.net/Alerts/Conectiva/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
DEBIAN	Debian Linux Security Information	http://www.debian.org/security/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
ENGARDE	En Garde Linux advisory	http://lwn.net/Alerts/EnGarde/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
FEDORA	Fedora Project security advisory	http://www.redhat.com/archives/fedora-announce-list/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
FREEBSD	FreeBSD security advisory	http://www.freebsd.org/security/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
GENTOO	Gentoo Linux security advisory	http://www.gentoo.org/security/en/glsa/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
HP	HP security advisories	http://archives.neohapsis.com/archives/hp/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
IBM	IBM ERS/BRS advisories	http://www-1.ibm.com/support/apar_search.html http://www-1.ibm.com/services/continuity/recover1.nsf/advisories?OpenView&Start=1&Count=30&Expand=3#3 http://www-1.ibm.com/services/continuity/recover1.nsf/advisories?OpenView&Start=1&Count=30&Expand=3#3	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
IMMUNIX	Immunix Linux advisory	http://download.immunix.org/ImmunixOS/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
ISS	ISS Security Advisory	http://xforce.iss.net/alerts	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
L0PHT	L0pht Security Advisory	http://www.l0pht.com/advisories.html	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
MACROMEDIA	Macromedia Security Bulletin	http://www.macromedia.com/v1/developer/securityzone/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
MANDRAKE	Linux-Mandrake advisory	http://www.mandrakesecure.net/en/advisories/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
MANDRIVA	Mandriva security advisory	http://www.mandriva.com/security/advisories	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
MS	Microsoft Security Bulletin	http://www.microsoft.com/technet/security/CurrentDL.aspx	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
MSKB	Microsoft Knowledge Base article	http://support.microsoft.com/search/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
NAI	NAI Labs security advisory	http://www.nai.com/research/covert/advisories.asp	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
NETBSD	NetBSD Security Advisory	http://www.netbsd.org/Security/advisory.html	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
OPENBSD	OpenBSD Security Advisory	http://www.openbsd.org/security.html	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
OPENPKG	OpenPKG security advisory	http://www.openpkg.com/security/advisories/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ

REDHAT	Security advisories	http://www.redhat.com/support/errata/index.html	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
SCO	SCO security bulletins	http://www.sco.com/support/security/index.html	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
SLACKWARE	Slackware Networks, Inc. security advisory security advisory SNI Secure	http://www.slackware.com/security/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
SUN	Sun security bulletin	http://sunsolve.sun.com/pub-cgi/secBulletin.pl	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
SUNALERT	Sun security alert	http://sunsolve.sun.com/pub-cgi/search.pl?mode=results&origin=advanced&range=20&so=date&coll=fsalert&zone_32=category:security	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
SUSE	SuSE Linux: Security Announcements	http://www.novell.com/linux/security/advisories.html	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
TRUSTIX	Trustix Security Advisory	http://www.trustix.net/errata/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
TURBO	TurboLinux advisory	http://www.turbolinux.com/security/	ΚΑΤΑΣΚΕΥΑΣΤΗΣ
UBUNTU	Ubuntu Linux security advisory	http://www.ubuntulinux.org/support/documentation/usn/errorreferencefolder_view	ΚΑΤΑΣΚΕΥΑΣΤΗΣ

Παράρτημα Β – Ερωτηματολόγιο Αξιολόγησης

Παρακαλώ επιλέξτε το είδος του Οργανισμού σας

Παρακαλώ επιλέξτε τον αριθμό των χρηστών του Οργανισμού σας

Παρακαλώ επιλέξτε το ρόλο σας στον Οργανισμό

Παρακαλώ επιλέξτε τα χρόνια απασχόλησης με την Ασφάλεια Πληροφοριών

Παρακαλώ επιλέξτε τις περιοχές της ασφάλειας πληροφοριών στις οποίες διαθέτετε σχετική εμπειρία

- ☐ Συστήματα Firewall/VPN
- ☐ Συστήματα Intrusion Detection/Precention
- ☐ Συστήματα Antivirus/Ελέγχου Περιεχομένου
- ☐ Άλλα συστήματα ασφάλειας
- ☐ Αξιολόγηση Ευπαθειών (Vulnerability Assessment)
- ☐ Πρότυπα Ασφάλειας Πληροφοριών (π.χ. BS/ISO, PCI-DSS, κανονιστικές οδηγίες, κτλ)
- ☐ Αντιμετώπιση Περιστατικών Ασφάλειας
- ☐ Forensics
- ☐ Άλλο:

Παρακαλώ επιλέξτε -κατά την κρίση σας- τα σημαντικότερα ζητήματα που σχετίζονται με την Αντιμετώπιση Περιστατικών Ασφάλειας

- ☐ Έλλειψη De Facto Προτύπων/Οδηγιών
- ☐ Έλλειψη Διοικητικών Δομών
- ☐ Κατηγοριοποίηση Περιστατικών Ανάλογα με τη σημαντικότητα και την έκτασή τους
- ☐ Έλλειψη χρόνου έρευνας/ανάλυσης
- ☐ Έλλειψη τεχνογνωσίας από προσωπικό οργανισμού/αγορά
- ☐ Έλλειψη κοινής ορολογίας
- ☐ Έλλειψη προτύπων ανταλλαγής πληροφοριών
- ☐ Έλλειψη εξειδικευμένων εργαλείων
- ☐ Άλλο:

Ποιά από τα παρακάτω χαρακτηριστικά θα επιθυμούσατε σε ένα εργαλείο αντιμετώπισης περιστατικών ασφάλειας;

- ☐ Ανάλυση Πληροφοριών που σχετίζονται με αδυναμίες ασφάλειας (vulnerability information)
- ☐ Συνεργασία με εργαλεία αποτίμησης ευπαθειών (vulnerability assessment)

- ☐ Βαθμολόγηση των αδυναμιών με προτυποποιημένη κλίμακα (π.χ. 1-10)
- ☐ Κατανόηση/Γνώση της τοπολογίας της υποδομής μου
- ☐ Συσχέτιση αδυναμιών μεταξύ τους (κατασκευή σεναρίων επίθεσης)
- ☐ Συσχέτιση αδυναμιών με exploits
- ☐ Συσχέτιση αδυναμιών με συστήματα ασφάλειας (π.χ. Intrusion Detection/Prevention)
- ☐ Προτεραιοποίηση Αντιμετώπισης Περιστατικών
- ☐ Παροχή πρόσθετων πληροφοριών σχετικά με αδυναμίες (από "επίσημους" δικτυακούς τόπους)
- ☐ Άμεση προβολή του κώδικα exploit
- ☐ Άμεση προβολή των διορθωτικών ενεργειών για την αντιμετώπιση του περιστατικού (π.χ. κανόνες/υπογραφές σε συστήματα Intrusion Detection/Prevention)
- ☐ Παροχή Μετρικών Αξιολόγησης Επικινδυνότητας (Risk Assessment)
- ☐ Χρήση ανοικτών προτύπων
- ☐ Χρήση προτυποποιημένων μεθόδων
- ☐ Άλλο: [ ]

Πώς σας φαίνεται το περιβάλλον (interface) του IRIS [ ]

Πώς σας φαίνεται η ποσότητα πληροφοριών που διαχειρίζεται το IRIS (Πλήθος vulnerabilities, exploits και υπογραφών Intrusion Detection) [ ]

Πώς σας φαίνεται η δυνατότητα βαθμολόγησης των αδυναμιών ασφάλειας του IRIS (χρήση πρότυπης μεθόδου CVSSv2)

[ ]

Πώς αξιολογείτε τη συσχέτιση των αδυναμιών με τα exploits του IRIS (χρησιμεύει για την κατασκευή σεναρίων επίθεσης)

[ ]

Πώς αξιολογείτε τη συσχέτιση των αδυναμιών με τα exploits και με τις υπογραφές intrusion detection (χρησιμεύει για την ελαχιστοποίηση των false positives στα συστήματα Intrusion Detection/Prevention)

[ ]

Πώς αξιολογείτε την ταχύτητα υπολογισμών του IRIS [ ]

Πώς χαρακτηρίζετε τη διάδραση του IRIS με το χρήστη; (δυνατότητα καθορισμού τοπολογικών κριτηρίων για αδυναμίες, παροχή ενεργειών χειρισμού των περιστατικών, προτεραιοποίηση ενεργειών) [ ]

Πώς χαρακτηρίζετε τις συνολικές δυνατότητες του IRIS

[ ]

Πώς χαρακτηρίζετε την πλατφόρμα του IRIS (περιβάλλον προγραμματισμού, απαιτήσεις εγκατάστασης, απαιτήσεις διασύνδεσης)

Παρακαλώ σημειώστε τα χαρακτηριστικά που πιστεύετε πως θα βελτίωναν τη συνολική εικόνα του IRIS

- Αλλαγή πλατφόρμας ανάπτυξης (web application)
- Περισσότερες Πληροφορίες
- Ενοποίηση με περισσότερα εργαλεία vulnerability assessment
- Ενοποίηση με περισσότερα συστήματα Intrusion Detection/Prevention
- Δημιουργία Εξαιρέσεων
- Δυνατότητα ανάλυσης ρυθμίσεων συστημάτων (configuration)
- Περισσότερο σύγχρονο interface
- Other:

Συνολικά, πώς κρίνετε το IRIS σαν εργαλείο αντιμετώπισης περιστατικών;

Τέλος, πιστεύετε πως το παρόν ερωτηματολόγιο:

Παρακαλώ, συμπληρώστε το ονοματεπώνυμό σας

Σύντομο Βιογραφικό Σημείωμα

Ο Δημήτριος Γ. Πατσός γεννήθηκε το 1977 στην Αθήνα. Είναι απόφοιτος του Τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών (2001) και κάτοχος Μεταπτυχιακού Διπλώματος Ειδίκευσης στην Ασφάλεια Πληροφοριών (M.Sc. with distinction in Information Security) από το Τμήμα Μαθηματικών του Royal Holloway University of London (2002). Από τον Ιούλιο του 2004, μέχρι και σήμερα, είναι υποψήφιος διδάκτορας του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς.

Το συγγραφικό του έργο περιλαμβάνει, μεταξύ άλλων ένα από τα πρώτα ελληνικά βιβλία ασφάλειας πληροφοριών (το οποίο χρησιμοποιείται ως σύγγραμμα σε ελληνικά ακαδημαϊκά ιδρύματα), δημοσιεύσεις σε διεθνή επιστημονικά και πρακτικά διεθνών συνεδρίων, ενώ έχει συμμετάσχει –σαν προσκεκλημένος ομιλητής- σε ένα μεγάλο πλήθος συνεδρίων και ημερίδων στην Ελλάδα και το εξωτερικό.

Διαθέτει 13ετή επαγγελματική εμπειρία στην Ασφάλεια Πληροφοριών και τα Δίκτυα Υπολογιστών, ενώ έχει εκτελέσει χρέη τεχνικού διευθυντή/υπευθύνου έργου μιας σειράς έργων Ασφάλειας Πληροφοριών σε μεγάλους ελληνικούς οργανισμούς, όπως Ο.Σ.Ε. Δίκτυο Δημόσιας Διοίκησης «Σύξευξις», Γενικό Επιτελείο Ναυτικού, Γεν. Γραμ. Αθλητισμού, Εθνική Τράπεζα Ελλάδος, Alpha Bank, Emporiki Bank/Societe Generale, Eurobank, Geniki Bank,Wind Hellas, Όμιλος Εταιριών Γερμανός, Πλαίσιο, ενώ έχει αποκτήσει ένα μεγάλο πλήθος πιστοποιήσεων για διάφορες τεχνολογίες και μεθοδολογίες ασφάλειας.

Τα επιστημονικά του ενδιαφέροντα εστιάζουν στα συστήματα αντιμετώπισης περιστατικών, την αξιολόγηση επικινδυνότητας και ρίσκου, το ηλεκτρονικό έγκλημα, την κρυπτογραφία και τις εφαρμογές της ασφάλειας πληροφοριών στην καθημερινή ζωή.

Διετέλεσε μέλος της Μόνιμης Επιστημονικής Επιτροπής της Ελληνικής Εταιρείας Επιστημόνων Πληροφορικής και Υπολογιστών (2004-2006), είναι τακτικό μέλος της ΕΠΥ, ισόβιο μέλος του ISG Alumni και μέλος του Επαγγελματικού Επιμελητηρίου Πειραιά.