Τίτλος Έργου	Προηγμένη ανίχνευση εισβολών και παράνομου ηλεκτρονικού περιεχομένου για τη διασφάλιση επιχειρησιακής και λειτουργικής ασφάλειας σε κατανεμημένα συστήματα συστημάτων		
Ακρωνύμιο Έργου	ΜΥΡΙΩΠΟΣ		
Κωδικός Έργου	Τ2ΕΔΚ-04665		
Πρόσκληση / Θέμα	ΕΡΕΥΝΩ – ΔΗΜΙΟΥΡΓΩ - ΚΑΙΝΟΤΟΜΩ Β' ΚΥΚΛΟΣ / ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ, ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ & ΚΑΙΝΟΤΟΜΙΑ		
Ημερομηνία Εκκίνησης	16/06/2020	Διάρκεια	30 Μήνες

Π1.1 Αναφορά Αρχιτεκτονικής ΜΥΡΙΩΠΟΣ

Ενότητα Εργασίας	**ΕΕ1 Καθορισμός Απαιτήσεων και Προτεινόμενη Αρχιτεκτονική**
Επικεφαλής	**MAGGIOLI**
Συνεισφορές	**UBITECH**

Περιεχόμενα

1 Εισαγωγικά Στοιχεία 5
1.1 Βελτιωμένη Κυβερνοασφάλεια σε Οικοσυστήματα Υπολογιστικού Νέφους, Αναγκαιότητα και Σύνδεση με το Παραδοτέο 5
1.2 Στόχοι Παραδοτέου 7
1.3 Συσχέτιση με Δράσεις και Ενότητες Εργασίας του ΜΥΡΙΩΠΟΥ 8
1.4 Δομή Παραδοτέου 8
2 Μοντελοποίηση Ασφάλειας, Ιδιωτικότητας και Ευπαθειών 9
2.1 Αναγνωριστικές Επιθέσεις 9
2.2 Επιθέσεις κωδικών 10
2.3 Επιθέσεις Δικαιωμάτων Χρήσης 10
2.4 Επιθέσεις Απομακρυσμένης Πρόσβασης 11
2.5 Επιθέσεις Υποκλοπής 12
2.6 Επιθέσεις μέσω Δομημένων Επερωτήσεων 13
2.7 Ψάρεμα Κωδικών και Προσωπικών Στοιχείων 13
2.8 Επιθέσεις σε Υπηρεσίες και Εφαρμογές Ιστού 14
2.9 Κακόβουλο Λογισμικό 15
2.10 Επιθέσεις Πλημμύρας / Τερματισμού Υπηρεσίας 16
2.11 Ευπάθειες Πρωτοκόλλων και Επιθέσεις 17
2.12 Μοντελοποίηση Πόρων στο Οικοσύστημα του ΜΥΡΙΩΠΟΣ 18
3 Απαιτήσεις ασφάλειας, ιδιωτικότητας, ανθεκτικότητας και υψηλής διαθεσιμότητας 18
3.1 Μεθοδολογία Εξαγωγής Απαιτήσεων 18
3.1.1 Μεθοδολογία Καθορισμού Απαιτήσεων 19
3.1.2 Εξαγωγή Τεχνικών Απαιτήσεων 21
3.2 Χρήστες και Ρόλοι του ΜΥΡΙΩΠΟΥ 22
3.3 Λειτουργικές Απαιτήσεις και Τεχνικές Προδιαγραφές ΜΥΡΙΩΠΟΥ 24
3.3.1 Επόπτες Καταγραφής, Αναζήτησης και Επεξεργασίας Δεδομένων 27
3.3.2 Απαιτήσεις Ασφάλειας 31

3.3.3 Απαιτήσεις Απορρήτου και Ακεραιότητας Δεδομένων 33
3.3.4 Εκτίμηση Κινδύνων και Επιβολή Πολιτικών 34
3.3.5 Ενορχήστρωση Υπηρεσιών και Εφαρμογή Πολιτικών Ασφαλείας 35
3.4 Μη Λειτουργικές Απαιτήσεις 37
4 Στοιχεία Αρχιτεκτονικής 40
4.1 Εννοιολογική Αρχιτεκτονική 40
4.2 Αρχιτεκτονική Συστήματος 43
4.2.1 Ροή Πληροφοριών και Αρχικοποίηση Συστήματος 46
4.2.2 Λειτουργικά Στοιχεία Αρχιτεκτονικής 47
4.2.3 Στοιχεία Αρχιτεκτονικής Και Απαιτήσεις 50
4.3 Διάγραμμα Ροής Χρηστών 50
5 Καθορισμός Νέου Προϊόντος 53
5.1 Μεθοδολογία Καθορισμού και Προτεραιοποίησης Χαρακτηριστικών Νέου Προϊόντος 53
5.2 Μεθοδολογία Εξαγωγής Χαρακτηριστικών και Ιεράρχησης Προτεραιοτήτων 54
6 Επίλογος 56
7 Αναφορές 57

Συντομογραφίες

DoS	Denial of Service
DDoS	Distributed Denial of Service
MITM	Man-in-the-Middle
MVP	Minimum Viable Product
SMART	Specific, Measurable, Achievable, Realistic, Timely
SQLI	Structured Query Language Injection
XSS	Cross Site Scripting
ΕΒΠ	Ελάχιστο Βιώσιμο Προϊόν
ΕΤΤ	Επίπεδο Τεχνολογικής Ετοιμότητας

Λίστα Εικόνων

Εικόνα 1. Μεθοδολογία για τον καθορισμό των λειτουργικών απαιτήσεων του ΜΥΡΙΩΠΟΣ 19
Εικόνα 2. Εννοιολογική Αρχιτεκτονική ΜΥΡΙΩΠΟΣ 41
Εικόνα 3. Αρχιτεκτονική Συστήματος ΜΥΡΙΩΠΟΣ 44
Εικόνα 4. Διάγραμμα Ροής της Κατανεμημένης Ευφυίας Ιστού και Σκοτεινού Δικτύου 51
Εικόνα 5. Διάγραμμα Ροής της Μηχανής Επιβολής Πολιτικών.....52
Εικόνα 6. Διάγραμμα Ροής της Αξιολόγησης Ιδιωτικότητας και Ασφαλείας 52
Εικόνα 7. Μεθοδολογία ενοποίησης του τελικού ΕΒΠ 55

Λίστα Πινάκων

Πίνακας 1. Κοινό και Πιθανοί Πελάτες του έργου ΜΥΡΙΩΠΟΣ 22
Πίνακας 2. Γενικές Λειτουργικές και Τεχνικές Απαιτήσεις 25
Πίνακας 3. Απαιτήσεις Πρακτόρων 27
Πίνακας 4. Απαιτήσεις Ασφαλείας 32
Πίνακας 5. Απαιτήσεις Απορρήτου και Ακεραιότητας Δεδομένων 33
Πίνακας 6. Απαιτήσεις Εκτίμησης Κινδύνου 34
Πίνακας 7. Απαιτήσεις Ενορχήστρωσης και Εφαρμογής Πολιτικών Ασφαλείας 35
Πίνακας 8. Μη Λειτουργικές Απαιτήσεις.....37
Πίνακας 9. Αντιστοίχιση Στοιχείων Αρχιτεκτονικής και Απαιτήσεων.....50

Περίληψη

Το έργο ΜΥΡΙΩΠΟΣ[1] εισάγει ένα πλήθος από καινοτόμες υπηρεσίες κυβερνοασφάλειας, αλγορίθμους και λύσεις που εστιάζουν σε υποδομές υπολογιστικού νέφους. Οι υπηρεσίες και εφαρμογές που αναπτύσσονται στοχεύουν στην: (i) κλιμακούμενη και βέλτιστη διαχείριση κατανεμημένων δεδομένων μεγάλης κλίμακας, ανάλυση και οπτικοποίηση τους, (ii) ανάλυση υποδομών δικτύων σε πραγματικό χρόνο, καθώς και την καταγραφή γεγονότων για τη διαχείριση δεδομένων παρακολούθησης δικτύων, υπηρεσιών και υποδομών με χρήση αλγορίθμων βαθιάς μηχανικής μάθησης και στατιστικής, (iii) εκπαίδευση μοντέλων ταξινόμησης για τον έγκαιρο εντοπισμό παραβατικών συμπεριφορών και μη κανονικής κίνησης εντοπίζονται μέσα σε υποδομές δικτύου, υπηρεσίες υπολογιστικού νέφους, κοινωνικά δίκτυα και τον σκοτεινό ιστό, (iv) εφαρμογή καινοτόμων λύσεων για την υποστήριξη ευέλικτων και κλιμακούμενων μεθόδων που στοχεύουν στην κατανεμημένη επεξεργασία δεδομένων σε περιβάλλοντα με γρήγορους μηχανισμούς δικτύωσης και μεταφόρτωσης δεδομένων σε πραγματικό χρόνο και (v) εφαρμογή προηγμένων και έξυπνων μηχανισμών εξόρυξης γνώσης από μεγάλα δεδομένα, με σκοπό την αξιοποίηση τους από εξειδικευμένους επιστήμονες ασφαλείας, κατόχους υποδομών δικτύων και υπηρεσιών υπολογιστικού νέφους καθώς και απλούς χρήστες.

[1] ΜΥΡΙΩΠΟΣ: ὁ ἔχων ἀναριθμήτους ὀφθαλμούς, ἐπὶ τοῦ Ἄργου, Αἰσχύλ. Πρ. 569.

1 Εισαγωγικά Στοιχεία

Στην παρούσα ενότητα παρουσιάζουμε συνοπτικά το αντικείμενο του έργου, τους στόχους του και πως σχετίζονται με την εξέλιξη του έργου ΜΥΡΙΩΠΟΣ. Τέλος, περιγράφουμε τη δομή του παραδοτέου, τη μεθοδολογία που ακολουθήσαμε για να ορίσουμε προδιαγραφές συστήματος, υπηρεσιών και τις απαιτήσεις χρηστών καθώς και την Αρχιτεκτονική της Λύσης ΜΥΡΙΩΠΟΣ.

Το αντικείμενο του έργου και οι στόχοι του συνοψίζονται, ως ακολούθως:

- ✓ **Στόχος 1:** Ανάπτυξη μιας νέας υποδομής με κλιμακούμενες υπηρεσίες ασφάλειας δικτύων ώστε να επιτρέπει την ασφαλή παραμετροποίηση, εγκατάσταση και λειτουργία κατανεμημένων υπηρεσιών ανίχνευσης και προστασίας σε ετερογενή λογισμικό και υλικό.
- ✓ **Στόχος 2:** Ανάπτυξη καινοτόμων μεθόδων ανίχνευσης ανωμαλιών μέσω εκπαίδευσης μοντέλων ταξινόμησης σε πραγματικό χρόνο που επεκτείνουν την τρέχουσα τεχνολογική στάθμη. Αξιοποίηση μοντελοποίησης και ευφυΐας ιστού για την εξαγωγή σημασιολογικής γνώσης αξιοποιώντας τεχνικές παραλληλοποιημένης βαθιάς μηχανικής μάθησης και έξυπνες κάρτες δικτύου που προσφέρουν κατανεμημένη επεξεργασία, γρήγορη εκφόρτωση (ή τερματισμό) «ύποπτης πληροφορίας» για την αποτελεσματική, ευέλικτη και έγκαιρη ανίχνευση παραβατικών δραστηριοτήτων στον κυβερνοχώρο.
- ✓ **Στόχος 3:** Ανάπτυξη ενός μοντέλου αξιολόγησης κινδύνου σε πραγματικό χρόνο που διευκολύνει τον έγκαιρο χειρισμό απειλών, σε συνδυασμό με ένα μοντέλο επιβολής πολιτικών ασφάλειας, ανθεκτικότητας και επιχειρησιακής προστασίας που λαμβάνει υπόψη το περιβάλλον εκτέλεσης. Δημιουργία και εφαρμογή μέτρων περιορισμού, συστάσεων και καταστολής ανεπιθύμητων ενεργειών, ύποπτου λογισμικού και απόπειρας υποκλοπής ιδιωτικών δεδομένων.
- ✓ **Στόχος 4:** Επίδειξη πιλοτικής λειτουργίας, αξιολόγηση αποδοχής και υιοθέτησης της ενοποιημένης Αρχιτεκτονικής Λύσης ΜΥΡΙΩΠΟΣ σε μια περίπτωση χρήσης Έξυπνων Υποδομών Κτηρίου με συσκευές και υπηρεσίες από το άκρο ως το κέντρο υποδομών και δεδομένων. Οι περιπτώσεις χρήσης περιλαμβάνουν διαφορετικά ρίσκα από κυβερνοεπιθέσεις και σενάρια επίθεσης που επηρεάζονται από την ετερογένεια και την πολυπλοκότητα ενός συστήματος συστημάτων με συσκευές άκρου και κεντρικές υποδομές.

1.1 Βελτιωμένη Κυβερνοασφάλεια σε Οικοσυστήματα Υπολογιστικού Νέφους, Αναγκαιότητα και Σύνδεση με το Παραδοτέο

Το 2017 ξεκίνησε να διαδίδεται ένα από τα πιο απλά αλλά ταχέως επεκτεινόμενα κακόβουλα λογισμικά που έχει αντιμετωπίσει ως σήμερα η ανθρωπότητα με το όνομα “NotPetya” [1], [2]. Μετεξελίχθηκε έπειτα στο γνωστό “WannaCry” που είχε ως αποτέλεσμα να μολύνει περισσότερους από 200.000 υπολογιστές σε 150 διαφορετικές χώρες[2]. Άμεσο αποτέλεσμα ήταν η παύση των δραστηριοτήτων πολλών μικρό-μεσαίων και μεγάλων επιχειρήσεων με ανυπολόγιστο κόστος. Επιπροσθέτως, με βάση την ετήσια έκθεση για τις ευρωπαϊκές εταιρίες [3], το 99.8% των επιχειρήσεων που ανήκουν σε μικρές (5.8%), μεσαίες (0.9%) και πολύ μικρές (93.1%) εταιρίες, απασχολούν 2 στους 3 εργαζόμενους πανευρωπαϊκά και έχουν κεντρικό ρόλο στην οικονομική και τη κοινωνική ανάπτυξη της Ευρωπαϊκής Ένωσης (ΕΕ). Η επιχειρησιακή τους ευρωστία και συνέχεια είναι ως εκ τούτου απαραίτητη και για την οικονομική συνέχεια της ΕΕ.

[2] https://www.bbc.com/news/world-39919249

Ως συνέπεια, η προστασία των επιχειρήσεων μέσω υπηρεσιών ψηφιακής ασφάλειας, αυξημένης ιδιωτικότητας και αύξησης της εκπαίδευσης των εργαζομένων μέσω ευαισθητοποίησης σχετικά με τους διάφορους κινδύνους του κυβερνοχώρου αποτελεί επίκαιρο θέμα καθώς και βασικό αντικείμενο του έργου ΜΥΡΙΩΠΟΣ. Συνεπώς κρίνεται απαραίτητη η παροχή υπηρεσιών και μεθόδων για την καταστολή επιθέσεων από διάφορες κατηγορίες malware και ransomware. Αυτό έχει ως άμεσο αποτέλεσμα **την ελάττωση των πιθανών επιχειρηματικών απωλειών που προέρχονται εξαιτίας είτε ενός φτωχού σχεδιασμού, είτε μη διάθεσης αποκλειστικού για κυβερνοασφάλεια προϋπολογισμού.** Δεδομένου ότι οι εγκληματίες του κυβερνοχώρου αντιλαμβάνονται τους απλούς χρήστες και τις επιχειρήσεις ως μια σχετικά εύκολη επιλογή που συνήθως έχει μειωμένη εκπαίδευση σε θέματα ασφαλείας στον κυβερνοχώρο, οι λόγοι αυτοί τους καθιστούν τον πιο πιθανό στόχο μιας κυβερνοεπίθεσης [3].

Σύμφωνα με τις προβλέψεις της Gartner για το μέλλον της ιδιωτικότητας [4], η δημιουργία αντιγράφων ασφαλείας και η αρχειοθέτηση των προσωπικών δεδομένων θα αποτελέσει τον μεγαλύτερο κίνδυνο διαρροής προσωπικών και ιδιωτικών δεδομένων για το 70% των οργανισμών. Για παράδειγμα, πολύ πρόσφατα η iNSYNQ, μια εταιρεία παροχής υπηρεσιών υπολογιστικού νέφους επλήγη από το ransomware MegaCortex [5], το οποίο παρέλυσε ολοσχερώς τις υποδομές της, εμποδίζοντας έτσι τους πελάτες της να έχουν πρόσβαση στα λογιστικά τους δεδομένα. Επιπρόσθετα, ένα νέο κακόβουλο λογισμικό τύπου trojan με το όνομα Ursnif έχει αρχίσει να εξαπλώνεται μέσω μηνυμάτων ηλεκτρονικού "ψαρέματος" χρησιμοποιώντας μολυσμένα έγγραφα Word [6], καθώς και ένα νέο trojan, που ονομάστηκε Saefko, βρέθηκε προς πώληση στον σκοτεινό ιστό στοχεύοντας στην υποκλοπή στοιχείων πιστωτικών καρτών, συλλογές λογαριασμών κρυπτονομισμάτων και διάφορων άλλων [7]. Στην πραγματικότητα, το 93% των επιχειρήσεων που έχουν βιώσει ένα περιστατικό στον κυβερνοχώρο ανέφεραν σοβαρές επιπτώσεις στην επιχείρησή τους. Σχεδόν όλοι ανέφεραν απώλεια χρημάτων και αποταμιεύσεων, ενώ το 31% ανέφερε ότι επηρεάστηκε η φήμη τους, οδηγώντας έτσι είτε σε απώλεια πελατών είτε σε δυσκολία προσέλκυσης νέων υπαλλήλων και επενδύσεων. Το πιο σημαντικό από τα ανωτέρω είναι ότι σχεδόν το 50% των επιχειρήσεων ανέφερε διακοπή των δραστηριοτήτων τους.

Ανεξάρτητα από τον κλάδο και το μέγεθος της εκάστοτε επιχείρησης, η προστασία του οργανισμού από κακόβουλες διαδικτυακές δραστηριότητές που μπορεί να στοιχίσουν εκατομμύρια ευρώ πρέπει να είναι μία από τις κορυφαίες προτεραιότητες. Λαμβάνοντας υπόψη τη συνεχή εξέλιξη και προσαρμογή των τεχνολογιών ηλεκτρονικού εγκλήματος, καθώς και τον τεράστιο αριθμό επιχειρήσεων, υπηρεσιών και εργαζομένων που επηρεάζουν, συμπεραίνουμε ότι χρειάζεται να αναπτυχθούν προηγμένες μεθοδολογίες και επιχειρησιακά εργαλεία για την αντιμετώπιση των κυβερνοαπειλών. **Επίσης, η μείωση της πολυπλοκότητας πρέπει να συνοδεύεται από την εισαγωγή υψηλού βαθμού αυτοματοποίησης, διαλειτουργικότητας και χρηστικότητας στα παρεχόμενα εργαλεία διαχείρισης της κυβερνοασφάλειας.**

Το έργο ΜΥΡΙΩΠΟΣ έρχεται να εξασφαλίσει την επιχειρησιακή και λειτουργική ασφάλεια των υποδομών υπολογιστικού νέφους των επιχειρήσεων εισάγοντας και προτείνοντας νέες τεχνικές και συνεργατικές υπηρεσίες τόσο σε επίπεδο υλικού όσο και σε επίπεδο λογισμικού για την έγκαιρη ανίχνευση εισβολών και παράνομου ηλεκτρονικού περιεχομένου με στόχο την επίτευξη αυξημένης προστασίας σε υποδομές δικτύου και υπολογιστικού νέφους, υπηρεσίες και εφαρμογές. Η αποκλιμάκωση των πιθανών εισβολών και κινδύνων περιλαμβάνει τη συλλογή μεγάλων δεδομένων μέσω πρακτόρων καταγραφής γεγονότων, την ανάλυση και δεικτοδότηση εμπλουτισμένης πληροφορίας που συνδυάζεται με αντίστοιχα ευρήματα στο σκοτεινό δίκτυο (π.χ. διαρροή προσωπικών δεδομένων, πώληση προσωπικών στοιχείων χρηστών στο σκοτεινό δίκτυο, κ.α.). Η λύση ολοκληρώνεται με υπηρεσίες έγκαιρου εντοπισμού πιθανών εισβολών μέσω κατανεμημένης

επεξεργασίας, γρήγορης εκφόρτωσης δεδομένων και επιβολής πολιτικών ασφάλειας ή / και αποτροπής κακόβουλων ενεργειών. Επιπρόσθετα, σε επίπεδο έγκαιρου εντοπισμού παράνομου περιεχομένου και παραβατικών συμπεριφορών (π.χ. αναφορές κυβερνοεπιθέσεων σε web forums, σχόλια και παραβατικές συμπεριφορές στο σκοτεινό δίκτυο), η συλλογή δεδομένων από πολλαπλές πηγές με διαφορετική γραμμογράφηση (π.χ. εξόρυξη γνώσης και εντοπισμός γεγονότων από τον ιστό, κατανεμημένα κέντρα δεδομένων και το σκοτεινό δίκτυο) και η εκπαίδευση μοντέλων ταξινόμησης (μέσω στατιστικής και βαθιάς μηχανικής μάθησης) εγγυώνται τη διασφάλιση επιχειρησιακής και λειτουργικής ασφάλειας [8], [9], [10].

Η αυξημένη συνδεσιμότητα των σημερινών υποδομών, οι ποικίλες εφαρμογές κοινωνικής δικτύωσης και οι κατανεμημένες λειτουργικές δυνατότητες σε συστήματα και εφαρμογές υπογραμμίζουν την αναγκαιότητα παροχής προηγμένης αξιολόγησης κινδύνου, νέων μηχανισμών ανίχνευσης εισβολών και άμεσης επιβολής πολιτικών για την εξάλειψη και αντιμετώπιση των κινδύνων και των πιθανών παραβιάσεων όχι μόνο σε επίπεδο υποδομών και λογισμικού αλλά και στον παγκόσμιο ιστό [11], [12], [13]. Η εισαγωγή νέων τεχνικών και συνδυαστικών υπηρεσιών σε επίπεδο υλικού και λογισμικού επιτρέπει τη διασφάλιση αυξημένης επιχειρησιακής προστασίας και λειτουργικής ασφάλειας, με σεβασμό των υφιστάμενων πολιτικών προστασίας δεδομένων (π.χ. GDPR [14]) και των καινοτόμων υποδομών δικτύωσης για τη ροή της πληροφορίας και τον έλεγχο πρόσβασης. Ο στόχος του έργου ΜΥΡΙΩΠΟΣ είναι να υλοποιηθεί μια **ολιστική λύση ασφάλειας, ικανή να εξαλείψει τις κυβερνοεπιθέσεις, να προσδιορίσει και κατηγοριοποιήσει εγκαίρως παραβατικές συμπεριφορές στο διαδίκτυο και στο σκοτεινό δίκτυο μέσω της κατάλληλης μοντελοποίησης των διαφορετικών εννοιών του συστήματος, των απειλών, των ευπαθειών, της προηγμένης επαλήθευσης και επιβολής πολιτικών ασφάλειας σε πραγματικό χρόνο.**

1.2 Στόχοι Παραδοτέου

Ο σκοπός του Παραδοτέου Π1.1 είναι να παρέχει τις εννοιολογικές προδιαγραφές της αρχιτεκτονικής λύσης του ΜΥΡΙΩΠΟΣ. Συγκεκριμένα, είναι η τεχνική αναφορά και το αποτέλεσμα της Ενότητας Εργασίας 1 (ΕΕ1) Καθορισμός Απαιτήσεων και Προτεινόμενη Αρχιτεκτονική. Στο εν λόγω παραδοτέο περιγράφονται οι διαφορετικές απαιτήσεις ασφαλείας, ιδιωτικότητας, ανθεκτικότητας και υψηλής διαθεσιμότητας, η αρχιτεκτονική λύση του ΜΥΡΙΩΠΟΣ, οι διεπαφές μεταξύ των λειτουργικών στοιχείων καθώς και οι τελικοί αποδέκτες του ενοποιημένου συστήματος.

Το παραδοτέο Π1.1 ορίζει και εισάγει νέες μεθοδολογίες ανίχνευσης και ποσοτικοποίησης κινδύνων, έγκαιρου εντοπισμού παραβατικών συμπεριφορών από τον ιστό και το σκοτεινό δίκτυο, πολυτροπικών ειδοποιήσεων, συλλογής αποδείξεων, και διαλειτουργικότητας. Οι **στόχοι του έργου ΜΥΡΙΩΠΟΣ (Στόχος 1 - 4)** θα επιτηρούνται καθόλη τη διάρκειά του μαζί με τις **τεχνικές προδιαγραφές** (π.χ. Τεχνικές και Λειτουργικές Απαιτήσεις του Π1.1) ώστε να ικανοποιούνται από την τεχνική λύση. Επίσης, οι **δείκτες απόδοσης και επιτυχίας** θα επιβλέπονται καθόλη τη διάρκεια του έργου ως προς τη συλλογή κατάλληλων μετρικών για την εξασφάλιση και ποσοτικοποίησή τους (π.χ., μείωση των αναφερόμενων απειλών στον κυβερνοχώρο, 100% επιτυχής αναγνώριση της παραβίασης της εμπιστευτικότητας ως μη εξουσιοδοτημένη πρόσβαση σε προσωπικά, κοινωνικά και εμπορικά δεδομένα, αυξημένη ασφάλεια δικτύου, >95% ακρίβεια βαθιάς επιθεώρησης πακέτων, >98% αποτελεσματικότητα δυναμικής ανίχνευσης κυβερνοαπειλών μέσω έγκαιρης προειδοποίησης, ενισχυμένη προστασία, βελτιωμένη αξιολόγηση κινδύνου, συνεχής άμβλυνση επιθέσεων και κινδύνων, αυτοματοποιημένη προσαρμογή και έλεγχος).

1.3 Συσχέτιση με Δράσεις και Ενότητες Εργασίας του ΜΥΡΙΩΠΟΥ

Ως παραδοτέο τεχνικών απαιτήσεων για το έργο στο σύνολό του, το Π1.1 σχετίζεται (και χρησιμεύει ως βάση) με όλες τις μεταγενέστερες ΕΕ και παραδοτέα. Επίσης, το Π1.1 αποτελεί τη βάση για τα επόμενα παραδοτέα Π2.1 (Κλιμακούμενη διαδικτυακή ανίχνευση, πολλαπλά επίπεδα επεξεργασίας και συλλογή αποδείξεων), καθώς και Π2.2 (Αναλυτική και εξαγωγή γνώσης από δεδομένα ιστού και σκοτεινού δικτύου, Πολυτροπική ειδοποίηση και διαλειτουργικότητα με τρίτα εργαλεία) αφού ορίζει τις απαιτήσεις του συστήματος και παρουσιάζει την ενιαία αρχιτεκτονική που υιοθετείται στο έργο. Στο πλαίσιο της ΕΕ1, αυτό το παραδοτέο συνδέεται άμεσα με τα αποτελέσματα των Δράσεων Δ1.1 – Δ1.3 και συγκεκριμένα: Δ1.1 Απαιτήσεις ασφάλειας, ιδιωτικότητας, ανθεκτικότητας και υψηλής διαθεσιμότητας, Δ1.2 Αρχιτεκτονική πλαισίου ΜΥΡΙΩΠΟΣ και ορισμός νέου προϊόντος και Δ1.3 Διευρυμένο μοντέλο ασφάλειας, ιδιωτικότητας, ευελιξίας και πολιτικών έγκαιρου εντοπισμού απειλών.

1.4 Δομή Παραδοτέου

Το παραδοτέο Π1.1 περιγράφει στο **Κεφάλαιο 2** τη Μοντελοποίηση Ασφαλείας, Ιδιωτικότητας, Ευελιξίας και Πολιτικών Έγκαιρου Εντοπισμού Απειλών καθώς εξετάζεται το τοπίο απειλών και ευπαθειών ενός συστήματος.

Στη συνέχεια, στο **Κεφάλαιο 3** παρουσιάζονται οι απαιτήσεις ασφαλείας, ιδιωτικότητας, ανθεκτικότητας και υψηλής διαθεσιμότητας. Πιο συγκεκριμένα, περιγράφεται με σαφήνεια η μεθοδολογία ορισμού και εξαγωγής των απαιτήσεων, οι χρήστες του συστήματος καθώς και οι Τεχνικές, Λειτουργικές και μη Λειτουργικές απαιτήσεις της λύσης.

Στο **Κεφάλαιο 4** περιγράφονται τα Στοιχεία της Αρχιτεκτονικής με όλα τα επιμέρους λειτουργικά μέρη και τις εκάστοτε διεπαφές. Επιπλέον, παρέχονται οι προβλεπόμενες περιπτώσεις χρήσης.

Το **Κεφάλαιο 5** παρέχει τον Καθορισμό του Νέου Προϊόντος καθώς και τη μεθοδολογία που ακολουθείται για τον Καθορισμό και την Προτεραιοποίηση των Χαρακτηριστικών του Νέου Προϊόντος.

Τέλος, το παραδοτέο ολοκληρώνεται με το **Κεφάλαιο 6** το οποίο ανακεφαλαιώνει τα ζητήματα που παρουσιάστηκαν στο εξής παραδοτέο.

2 Μοντελοποίηση Ασφάλειας, Ιδιωτικότητας και Ευπαθειών

Σε αυτή την ενότητα, εξετάζουμε το τοπίο απειλών καθώς και την ύπαρξη τόσο **εσωτερικών** όσο και **εξωτερικών επιθέσεων**. Σε γενικές γραμμές, οι εσωτερικοί επιτιθέμενοι θεωρείται ότι έχουν μεγαλύτερο αντίκτυπο κατά τη διάρκεια μιας επίθεσης σε κάποια υπολογιστική υποδομή, επειδή μπορούν να εξαπολύουν επιθέσεις μέσα από τα όρια του δικτύου. Ωστόσο, η σημασία των εξωτερικών επιτιθέμενων δεν πρέπει επίσης να υποτιμάται. Σε αυτό το σημείο διευκρινίζουμε ότι το πεδίο εφαρμογής του **συστήματος ΜΥΡΙΩΠΟΣ είναι η προστασία των κατανεμημένων συσκευών και των υπολογιστικών πόρων εντός μιας ιδιωτικής υποδομής που θα μπορούσε να ανήκει είτε σε τελικό χρήστη, είτε σε εταιρία, είτε σε πάροχο υπηρεσιών υπολογιστικού νέφους**.

Ουσιαστικά εξετάζουμε ένα ευρύ φάσμα επιθέσεων με στόχο όλους τους πιθανούς στόχους, συμπεριλαμβανομένων των τεχνολογικών στοιχείων και των ιδιωτικών δεδομένων που αποθηκεύονται σε βάσεις δεδομένων. Εξετάζουμε επίσης όλα τα πιθανά επίπεδα μιας στοίβας εφαρμογών, συμπεριλαμβανομένων του επιπέδου συστήματος, λογισμικού και δικτύου, καθώς και διαφορετικούς τύπους επιθέσεων όπως DDoS, κ.λπ. που αναλύονται περαιτέρω στη συνέχεια.

Στις ενότητες που ακολουθούν, δίνουμε μια πλήρη περιγραφή του τοπίου των απειλών που μπορούν να θεωρηθούν ως πιθανές/επικίνδυνες στο πλαίσιο του ΜΥΡΙΩΠΟΣ με υποδομές υπολογιστικού νέφους και συσκευές άκρου. Δεν υπονοείται ότι όλες οι επιθέσεις που παρατίθενται έχουν τον ίδιο αντίκτυπο και την ίδια σοβαρότητα, αλλά εξαρτάται από τις συνθήκες και τα χαρακτηριστικά της εκάστοτε εταιρίας, καθώς και από τις ιδιαιτερότητες κάθε περίπτωσης χρήσης. Εδώ δίνουμε την περιγραφή ενός γενικού τύπου επιθέσεων που μπορούν να εμφανιστούν, καθώς και την αντιστοίχιση των επιπτώσεων κάθε κινδύνου σε κάθε περίπτωση χρήσης, ώστε να μπορούν να ληφθούν υπόψη στη μεθοδολογία αξιολόγησης κινδύνων. Για λόγους ορθότητας τα ονόματα των επιθέσεων διατηρήθηκαν και δε μεταφράστηκαν.

2.1 Αναγνωριστικές Επιθέσεις

Ο όρος *Reconnaissance*[3] στην κυβερνοασφάλεια αναφέρεται στο προκαταρκτικό στάδιο μιας κυβερνοεπίθεσης, όπου ο αντίπαλος ανιχνεύει το σύστημα-στόχο. Ο όρος προέρχεται από τη στρατιωτική ορολογία και αναφέρεται σε μια αποστολή σε εχθρικό έδαφος για την απόκτηση πληροφοριών. Λόγω του ότι η ενέργεια αυτή πραγματοποιείται πριν από την πραγματική πρόκληση ζημίας, θεωρείται τεχνική ελάχιστου αντικτύπου.

Γενικά, κατά τη διάρκεια αυτού του βήματος, οι κακόβουλες οντότητες προσπαθούν να συλλέξουν πληροφορίες από οπουδήποτε και παντού για να δημιουργήσουν έναν φάκελο πληροφοριών για μια εταιρεία-στόχο. Αυτός ο φάκελος μπορεί να περιέχει διευθύνσεις δικτύου, ενεργές υπηρεσίες, ανοικτές πόρτες, αναμεταδότες μεσολάβησης, συναθροιστές συνδέσεων VPN, εφαρμογές που χρησιμοποιούνται από την εταιρεία, καθώς και κρίσιμα ονόματα χρήστη και κωδικούς πρόσβασης που σχετίζονται με τον τομέα και τους χρήστες του οργανισμού. Τελικά, οι πληροφορίες που συγκεντρώνονται χρησιμοποιούνται για να επιτεθούν σε μια εταιρεία στα πιο αδύναμα σημεία της, επιδιώκοντας την πρόσβαση στα συστήματα, τα δίκτυα και τα αποθετήρια δεδομένων.

[3] https://intellipaat.com/blog/reconnaissance-in-cyber-security/

Για παράδειγμα, οι συνδεδεμένες συσκευές άκρου τρέχουν διάφορες υπηρεσίες και οι Επόπτες που τις παρακολουθούν όπως είναι αναμενόμενο βρίσκονται όλα εκτεθειμένα στο διαδίκτυο. Επομένως, εάν αυτό το σημείο πρόσβασης παραμένει απροστάτευτο, ένας κακόβουλος χρήστης θα μπορούσε εύκολα να εκκινήσει σάρωση για ενεργές υπηρεσίες, ανοικτές πόρτες και ευπάθειες χωρίς να τραβήξει τη προσοχή ή να γίνει αντιληπτός από κάποιο σύστημα παρακολούθησης. Ο ΜΥΡΙΩΠΟΣ εξετάζει προσεκτικά αυτό το ζήτημα ασφαλείας προκειμένου να προσφέρει μηχανισμούς που ανιχνεύουν και αποτρέπουν τέτοιες ύποπτες ενέργειες συλλογής πληροφοριών, όπως επαναλαμβανόμενες προσπάθειες εισόδου στο σύστημα, πρόσβαση σε ώρες εκτός λειτουργίας και συμπεριφορικά πρότυπα που μπορούν να χαρακτηριστούν ως μη κανονικά. Συγκεκριμένα, θα εγκαταστήσουμε κατάλληλα διαμορφωμένα τείχη προστασίας που είναι σε θέση να ανιχνεύουν ανώμαλη κίνηση που προέρχεται από τέτοιες αναγνωριστικές επιθέσεις, όπως ο ασυνήθιστος όγκος πακέτων ICMP ή ατελείς συνδέσεις TCP και να ειδοποιούν έναν υπεύθυνο ασφαλείας ή να τερματίζουν / μπλοκάρουν συγκεκριμένες διευθύνσεις IP. Σημειώστε ότι, για να επιτευχθεί αυτό, ο ΜΥΡΙΩΠΟΣ θα αναπτύξει κατάλληλους Επόπτες παρακολούθησης καθώς και ευρετικούς κανόνες και πολιτικές ασφαλείας. Επίσης, στον ΜΥΡΙΩΠΟ θεωρούμε ότι μια αναγνωριστική επίθεση μπορεί να εξαπολυθεί σε διαφορετικά επίπεδα του μοντέλου αναφοράς OSI[4]. Για το λόγο αυτό οι Επόπτες παρακολούθησης θα είναι σε θέση να συλλάβουν αυτού του είδους τις επιθέσεις το συντομότερο δυνατό.

2.2 Επιθέσεις κωδικών

Είναι μια μέθοδος δοκιμής κάθε δυνατού κωδικού πρόσβασης μέχρι να βρεθεί ο σωστός. Αυτές οι επιθέσεις γίνονται με εξαντλητική αναζήτηση, δηλαδή με τη χρήση όλων των πιθανών συνδυασμών με σκοπό να εισέλθουν σε ιδιωτικούς λογαριασμούς. Αυτή η μέθοδος επίθεσης είναι παλιά αλλά εξακολουθεί να είναι αποτελεσματική και δημοφιλής στους κακόβουλους χρήστες, διότι η απόκτηση πρόσβασης σε έναν έγκυρο λογαριασμό μπορεί να σημαίνει την παραβίαση ολόκληρου του ιστότοπου καθώς και των εκάστοτε υποδομών. Σε αντίθεση με πολλές άλλες τακτικές που χρησιμοποιούν οι επιτιθέμενοι, αυτές οι επιθέσεις δεν βασίζονται σε ευπάθειες εντός των ιστοτόπων, χαρακτηριστικό που τις καθιστά αρκετά αποτελεσματικές. Επίσης, οι επιτιθέμενοι έχουν βρει τρόπους να βελτιώσουν τις μεθόδους τους εισάγοντας κάποιο είδος νοημοσύνης, όπως για παράδειγμα η ιεράρχηση των κωδικών που έχουν ήδη βρεθεί. Για παράδειγμα, κάποιος θα μπορούσε να δοκιμάσει πρώτα τις λίστες με τους παραβιασμένους κωδικούς, στη συνέχεια τις λίστες με κοινούς κωδικούς πρόσβασης, στη συνέχεια τις λίστες με κοινές λέξεις, μεταθέσεις και συνδυασμούς λέξεων κ.λπ. για να αυξήσει τις πιθανότητες επιτυχούς παραβίασης, μειώνοντας έτσι τις απαραίτητες προσπάθειες.

2.3 Επιθέσεις Δικαιωμάτων Χρήσης

Οι επιθέσεις τύπου *Privilege Escalation*[5] αποτελούνται από τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να αποκτήσουν δικαιώματα υψηλότερου επιπέδου σε ένα σύστημα ή δίκτυο. Οι επιτιθέμενοι συχνά εισέρχονται σε ένα δίκτυο έχοντας μη εξουσιοδοτημένη πρόσβαση, όμως για την επίτευξη των στόχων τους απαιτούνται αυξημένα δικαιώματα εντός του δικτύου. Συνήθεις προσεγγίσεις είναι η εκμετάλλευση αδυναμιών, λανθασμένων ρυθμίσεων στους κωδικούς πρόσβασης και ευπαθειών του συστήματος, οι οποίες θα μπορούσαν να οδηγήσουν σε τέτοιου είδους πρόσβαση. Χαρακτηριστικά παραδείγματα είναι τα

[4] https://en.wikipedia.org/wiki/OSI_model
[5] https://www.cynet.com/network-attacks/privilege-escalation/

δικαιώματα του διαχειριστή, πρόσβαση σε ομάδες που έχουν τα δικαιώματα για την εκτέλεση συγκεκριμένων λειτουργιών σε επίπεδο συστήματος, βάσεων δεδομένων κοκ. Ένας από τους κύριους τρόπους για την επίτευξη κλιμάκωσης προνομίων είναι η εκμετάλλευση ευπάθειας λογισμικού. Αυτό συμβαίνει όταν ένας αντίπαλος εκμεταλλεύεται ένα προγραμματιστικό σφάλμα σε ένα πρόγραμμα, μια υπηρεσία ή στο ίδιο το λογισμικό του λειτουργικού συστήματος ή τον πυρήνα για να εκτελέσει κώδικα. Μπορεί να υπάρχουν ευπάθειες, συνήθως σε στοιχεία του λειτουργικού συστήματος και σε λογισμικό που συνήθως εκτελείται με υψηλότερα δικαιώματα, οι οποίες μπορούν να αξιοποιηθούν για να αποκτήσουν υψηλότερα επίπεδα πρόσβασης στο σύστημα. Αυτό θα μπορούσε να επιτρέψει σε κάποιον να μεταβεί από μη προνομιούχα δικαιώματα ή δικαιώματα επιπέδου χρήστη σε δικαιώματα επιπέδου συστήματος ή διαχειριστή, ανάλογα με το στοιχείο που είναι ευάλωτο. Αυτό θα μπορούσε επίσης να επιτρέψει σε έναν αντίπαλο να μετακινηθεί από ένα εικονικό περιβάλλον, όπως μέσα σε μια εικονική μηχανή, στον επικείμενο κεντρικό υπολογιστή.

Τα λειτουργικά συστήματα που βασίζονται σε Unix/Linux αποτελούν τους κύριους στόχους αυτών των επιθέσεων, καθώς συνήθως φιλοξενούν τις δημόσιες υπηρεσίες των περισσότερων επιχειρήσεων, ενώ ακολουθούν οι κεντρικοί υπολογιστές που βασίζονται σε Windows. Αυτά από κοινού συμβάλλουν στο 99,8% των λειτουργικών συστημάτων που χρησιμοποιούνται για σκοπούς φιλοξενίας υπηρεσιών, επομένως, κάθε επιτυχής παραβίαση μπορεί να οδηγήσει σε σοβαρές επιπτώσεις στον οργανισμό-θύμα, είτε μέσω κάποιας λειτουργικής ζημιάς, οικονομικού κόστους (π.χ. κλοπή / κλείδωμα ιδιωτικών δεδομένων και αποζημίωση για την επιστροφή στην κανονικότητα), ή και απώλειας της φήμης μιας εταιρίας, επομένως είναι υποχρεωτικό να συμπεριληφθούν οι τεχνικές κλιμάκωσης προνομίων στη συνολική διαδικασία αξιολόγησης κινδύνων που προσφέρει ο ΜΥΡΙΩΠΟΣ στους τελικούς χρήστες του. Για το σκοπό αυτό, το ΜΥΡΙΩΠΟΣ θα εφαρμόσει υπηρεσίες πιστοποίησης και διασφάλισης εμπιστοσύνης συσκευών άκρου για την προστασία από αυτού του είδους τις επιθέσεις [15].

2.4 Επιθέσεις Απομακρυσμένης Πρόσβασης

Ο όρος *Remote Access Exploitation*[6] αναφέρεται σε μια ομάδα επιθέσεων που στοχεύουν σε τεχνολογίες απομακρυσμένης πρόσβασης, οι οποίες επιτρέπουν την πρόσβαση σε προστατευόμενους πόρους από εξωτερικά δίκτυα και συχνά από εξωτερικά ελεγχόμενους κεντρικούς υπολογιστές. Πρόσφατα, οι τεχνολογίες απομακρυσμένης πρόσβασης απέκτησαν εκτενή χρήση, καθώς υιοθετήθηκαν ευρέως ακόμη και από μικρές επιχειρήσεις, κυρίως λόγω του ξεσπάσματος της πανδημίας COVID-19 και της απομακρυσμένης εργασίας, ενώ παράλληλα αυξήθηκαν και τα σχετικά περιστατικά κυβερνοασφάλειας. Γενικά, οι τεχνολογίες απομακρυσμένης πρόσβασης χρειάζονται συχνά πρόσθετη προστασία λόγω της φύσης τους, η οποία τις θέτει σε μεγαλύτερη έκθεση σε εξωτερικές απειλές σε σύγκριση με τις τεχνολογίες στις οποίες η πρόσβαση γίνεται μόνο εσωτερικά. Οι σημαντικότερες ανησυχίες για την ασφάλεια των τεχνολογιών απομακρυσμένης πρόσβασης περιλαμβάνουν: α) μη ασφαλή δίκτυα, καθώς σχεδόν όλες οι προσπάθειες απομακρυσμένης πρόσβασης πραγματοποιούνται μέσω του Διαδικτύου και οι οργανισμοί δεν έχουν συνήθως ούτε τον έλεγχο της ασφάλειας των εξωτερικών δικτύων που χρησιμοποιούν οι εργαζόμενοι τηλεργασίας, ούτε τους πόρους για την ανάπτυξη υφιστάμενων λύσεων ασφαλείας στο πρόβλημα αυτό, β) την εξωτερική πρόσβαση σε πόρους που είναι αποκλειστικά εσωτερικοί, όπως ευαίσθητοι διακομιστές, οι οποίοι μπορούν δυνητικά να εκτεθούν σε νέες απειλές και να αυξήσουν σημαντικά την πιθανότητα παραβίασης, και γ) το πρόβλημα των μολυσμένων συσκευών που συνδέονται σε εσωτερικά δίκτυα, ιδίως των συσκευών άκρου, USB και

[6] https://www.extrahop.com/resources/attacks/remote-services-exploitation/

περιφερειακών συσκευών τύπου Bluetooth, οι οποίες συχνά χρησιμοποιούνται σε εξωτερικά δίκτυα και στη συνέχεια εισάγονται στον οργανισμό και συνδέονται απευθείας σε εσωτερικά μη προσβάσιμα δίκτυα. Ένας επιτιθέμενος με φυσική πρόσβαση σε τέτοιες συσκευές μπορεί να εγκαταστήσει κακόβουλο λογισμικό σε αυτές και να το χρησιμοποιήσει αργότερα για να συλλέξει δεδομένα από τα δίκτυα και τα συστήματα στα οποία συνδέονται.

Οι κύριες απειλές που θα ληφθούν υπόψιν είναι οι εξής: α) επιθέσεις υποκλοπής εναντίον κακώς σχεδιασμένων ή ρυθμισμένων λύσεων VPN, οι οποίες οδηγούν σε μη ασφαλή κανάλια επικοινωνίας, β) επιθέσεις εναντίον VPN που είτε είναι κακώς ρυθμισμένα όσον αφορά στους μηχανισμούς ελέγχου ταυτότητας είτε δεν υποστηρίζουν προηγμένες τεχνικές ελέγχου ταυτότητας (π.χ. 2FA[7]) και γ) υφιστάμενες ευπάθειες λογισμικού, ευπάθειες από παλιές εφαρμογές και προηγούμενες εκδόσεις λογισμικού που δεν έχουν ενημερωθεί για να μετριάσουν τα γνωστά ζητήματα και τις ανησυχίες για την ασφάλεια [18].

2.5 Επιθέσεις Υποκλοπής

Οι επιθέσεις Man-in-the-Middle (MITM)[8], επίσης γνωστές ως επιθέσεις υποκλοπής, συμβαίνουν όταν οι επιτιθέμενοι παρεμβάλλονται στη μέση μιας επικοινωνίας μεταξύ δύο μερών. Μόλις οι επιτιθέμενοι διακόψουν την κυκλοφορία, μπορούν να υποκλέψουν τι επικοινωνούν οι κεντρικοί υπολογιστές, να διαβάσουν τα δεδομένα που ανταλλάσσουν, να συλλέξουν ευαίσθητες πληροφορίες, να τις τροποποιήσουν και να στείλουν τα παραποιημένα δεδομένα πίσω στον παραλήπτη και αντίστροφα. Υπάρχουν δύο κύριες φάσεις για την επιτυχή εκτέλεση μιας επίθεσης Man-in-the-Middle, η υποκλοπή και η αποκρυπτογράφηση. Η υποκλοπή αναφέρεται όταν ο επιτιθέμενος παραμένει ανάμεσα στη ροή δεδομένων και είναι έτοιμος να κλέψει τα δεδομένα που λαμβάνει με σκοπό να τα επαναχρησιμοποιήσει ή και να χειραγωγήσει το θύμα προς όφελος του. Ομοίως, η φάση της αποκρυπτογράφησης αναφέρεται στη προσπάθεια του επιτιθέμενου να αναλύει τη μέθοδο κρυπτογράφησης που έχει χρησιμοποιηθεί στο κανάλι με σκοπό να αποκρυπτογραφήσει τα δεδομένα.

Τα δημόσια δίκτυα αποτελούν το καλύτερο πεδίο δράσης για τους επιτιθέμενους προκειμένου να πραγματοποιήσουν μια επίθεση υποκλοπής. Τον τελευταίο καιρό, παρατηρείται κατακόρυφη αύξηση της συχνότητας αλλά και της σοβαρότητας τέτοιων επιθέσεων. Τα τελευταία δύο χρόνια, ο αριθμός υπαλλήλων των επιχειρήσεων που χρησιμοποιεί δημόσια δίκτυα για να έχει απομακρυσμένη πρόσβαση στην υποδομή της επιχείρησης ή/και σε ευαίσθητα αρχεία αυξάνεται συνεχώς. Αν συνδυάσουμε την πιθανότητα επιτυχούς υποκλοπής της πληροφορίας σε ένα δημόσιο, απροστάτευτο σημείο πρόσβασης δικτύου και τις ευπάθειες των υπηρεσιών απομακρυσμένης πρόσβασης και απομακρυσμένης επιφάνειας εργασίας, όπως αναφέρθηκε προηγουμένως, οι επιτιθέμενοι μπορούν εύκολα να παρακολουθούν πληροφορίες που ανταλλάσσονται μεταξύ εργαζομένων και επιχείρησης χωρίς να γίνει αντιληπτό. Ο ΜΥΡΙΩΠΟΣ θα περιορίσει τέτοιου είδους επιθέσεις μέσω υπηρεσιών αυθεντικοποίησης, δημιουργίας ισχυρών κωδικών και έκθεσης μόνο απαραίτητων υπηρεσιών στο διαδίκτυο μέσα από συγκεκριμένες IP/ports που θα παρακολουθούνται από τους Επόπτες.

[7] https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa
[8] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

2.6 Επιθέσεις μέσω Δομημένων Επερωτήσεων

Μια επίθεση *SQL Injection*[9] βασίζεται στην εισαγωγή ειδικά διαμορφωμένων εντολών SQL μέσω των δεδομένων εισόδου σε μια εφαρμογή, προκειμένου να εξαπατηθεί το σύστημα και να κάνει απροσδόκητα και ανεπιθύμητες ενέργειες. Μια επιτυχημένη επίθεση SQL [19], [20] μπορεί να διαβάσει ευαίσθητα δεδομένα από τη βάση δεδομένων, να χειριστεί τα δεδομένα με διάφορους τρόπους (π.χ. να τα συμπληρώσει με νέα δεδομένα, να τροποποιήσει υπάρχουσες καταχωρήσεις, να αφαιρέσει υπάρχοντα δεδομένα, κ.λπ.), να εκτελέσει λειτουργίες διαχείρισης στη βάση δεδομένων, να ανακτήσει το περιεχόμενο ενός συγκεκριμένου αρχείου που υπάρχει στο σύστημα αρχείων της βάσης δεδομένων (π.χ. backup αρχείο που αποθηκεύεται καθημερινά) και, σε ορισμένες περιπτώσεις, να δώσει ακόμη και εντολές στο λειτουργικό σύστημα. Για παράδειγμα, ένας κακόβουλος χρήστης θα μπορούσε να εκμεταλλευτεί μια ευπάθεια κάποιας συνδεδεμένης συσκευής άκρου και να εισάγει δεδομένα που θα μπορούσαν να χειραγωγήσουν μια βάση δεδομένων με κακόβουλο και ανεπιθύμητο τρόπο. Για να εξαλείψουμε αυτά τα προβλήματα, θα εξετάσουμε τις επιθέσεις SQL κατά των βάσεων δεδομένων και του συστήματος που είναι εγκατεστημένες στη διαδικασία αξιολόγησης κινδύνων.

2.7 Ψάρεμα Κωδικών και Προσωπικών Στοιχείων

Οι επιθέσεις ηλεκτρονικού "ψαρέματος" (phising) χρησιμοποιούνται με σκοπό να πείσουν τα πιθανά θύματα να αποκαλύψουν ευαίσθητες πληροφορίες, όπως διαπιστευτήρια ή στοιχεία τραπεζικών και πιστωτικών καρτών. Συνήθως, περιλαμβάνουν μηχανισμούς κοινωνικής εξαπάτησης. Για το λόγο αυτό, η επίθεση λαμβάνει τόπο συνήθως μέσα από μηνύματα ηλεκτρονικού ταχυδρομείου, κακόβουλων ιστοτόπων ή και ακόμα και άμεσων μηνυμάτων, τα οποία εμφανίζονται ως προερχόμενα από νόμιμη και αξιόπιστη πηγή, όπως μια τράπεζα ή ένα κοινωνικό δίκτυο. Μια στοχευμένη μορφή ψαρέματος που ονομάζεται spear phishing βασίζεται στην εκ των προτέρων έρευνα, ώστε η απάτη να φαίνεται πιο αυθεντική και στοχεύει συνήθως θύματα υψηλών βαθμίδων ενός οργανισμού, καθιστώντας την έτσι, έναν από τους πιο επιτυχημένους τύπους επιθέσεων στα δίκτυα των επιχειρήσεων. Το ηλεκτρονικό ταχυδρομείο συνεχίζει να είναι ο νούμερο ένα μηχανισμός για το phishing, αλλά όχι για πολύ, καθώς οι οργανισμοί και οι επιχειρήσεις έχουν ήδη αρχίσει να υιοθετούν το πρότυπο DMARC (Domain-based message authentication, reporting, and conformance) [21], το οποίο διασφαλίζει ότι το ηλεκτρονικό ταχυδρομείο από δόλιους τομείς αποκλείεται, μειώνοντας το ποσοστό επιτυχίας των συγκεκριμένων επιθέσεων. Επίσης τα τελευταία χρόνια, παρατηρούμε αύξηση της χρήσης μηνυμάτων από τα μέσα κοινωνικής δικτύωσης για τη διεξαγωγή αυτών των επιθέσεων. Η πιο σημαντική αλλαγή αφορά στις μεθόδους που χρησιμοποιούνται για την αποστολή μηνυμάτων, οι οποίες θα γίνουν πιο εξελιγμένες μέσω της υιοθέτησης τεχνικών τεχνητής νοημοσύνης για την προετοιμασία και την αποστολή των μηνυμάτων.

Σε αυτό το σημείο, η κατάλληλη εκπαίδευση του προσωπικού ώστε να αναγνωρίζει τα ψεύτικα και κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου, καθώς και το μη ελεγχόμενο κλικ σε τυχαίους συνδέσμους, ιδίως αυτούς που λαμβάνονται από τα μέσα κοινωνικής δικτύωσης κρίνεται απαραίτητη. Ωστόσο, η ανθρώπινη ευαισθητοποίηση δεν είναι η μόνη δράση μετριασμού. Συμπεριλαμβάνουμε το ψάρεμα στη μεθοδολογία αξιολόγησης κινδύνου που εφαρμόζουμε, προκειμένου να είμαστε σε θέση να αναγνωρίζουμε και να μετριάζουμε την απειλή με πιο αυτοματοποιημένο τρόπο, κυρίως με τη δυνατότητα να επιλέγουμε και να

[9] https://www.w3schools.com/sql/sql_injection.asp

αναπτύσσουμε λύσεις κυβερνοασφάλειας από ένα προκαθορισμένο σύνολο, όταν και όπου είναι απαραίτητο. Στα πλαίσια του ΜΥΡΙΩΠΟΣ, οι λύσεις κυβερνοασφάλειας είναι πύλες ασφαλείας ηλεκτρονικού ταχυδρομείου με τακτική συντήρηση των φίλτρων, αυτόματο μπλοκάρισμα της εκτέλεσης κώδικα και μακροεντολών, καθώς εφαρμογή προτύπων για τη μείωση των μηνυμάτων ψαρέματος (DMARC [21], DKIM [22]), και αναλυτικές για την ανίχνευση απάτης και ανωμαλιών σε επίπεδο δικτύου για εισερχόμενα / εξερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου.

2.8 Επιθέσεις σε Υπηρεσίες και Εφαρμογές Ιστού

Οι επιθέσεις σε υπηρεσίες και εφαρμογές ιστού είναι μια ελκυστική μέθοδος με την οποία οι επιτιθέμενοι μπορούν να εξαπατούν τα θύματα χρησιμοποιώντας διαδικτυακά συστήματα και υπηρεσίες ως τον κύριο φορέα απειλής, καλύπτοντας ένα πολύ ευρύ φάσμα επιθέσεων. Κατά συνέπεια, οι επιθέσεις μέσω διαδικτύου μπορούν να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα δεδομένων, υπηρεσιών και συστημάτων. Οι πιο δημοφιλείς επιθέσεις που εμπίπτουν σε αυτή την κατηγορία είναι ορισμένες από τις παραπάνω επιθέσεις καθώς και η εκτέλεση κακόβουλου λογισμικού (malware / ransomware), ή η παραβίαση φορμών για την εισαγωγή κακόβουλου κώδικα JavaScript σε δικτυακούς τόπους-στόχους.

Οι εφαρμογές ιστού αποτελούν επίσης βασικό μέρος του σύγχρονου διαδικτύου, προσφέροντας περισσότερα χαρακτηριστικά, λειτουργίες, υπηρεσίες και χρήσεις πάνω στον ιστό. Η πλειονότητα αυτών των εφαρμογών εξαρτάται από διάφορα συστήματα, όπως βάσεις δεδομένων για την αποθήκευση και την παροχή των απαραίτητων πληροφοριών, διακομιστές ιστού για τη διαχείριση των αιτημάτων, APIs για τη σύνδεση και την επικοινωνία με άλλες υπηρεσίες ή συνδυασμό αυτών. Όπως είναι επόμενο υπάρχει μια μεγάλη ποικιλία επιθέσεων που μπορεί να χρησιμοποιήσει κάποιος επιτιθέμενος. Συγκεκριμένα, το SQL Injection είναι ένα γνωστό παράδειγμα και η πιο κοινή απειλή κατά των βάσεων δεδομένων, καθώς ευθύνεται για πάνω από το 70% όλων των περιστατικών εναντίον των εφαρμογών ιστού, με το Local File Inclusion (LFI)[10] να έρχεται δεύτερο και το Cross-Site Scripting (XSS) τρίτο, με συνολικό ποσοστό 95% [23].

Δεδομένου ότι πολλές από αυτές τις επιθέσεις επηρεάζουν συστήματα και υπηρεσίες που υιοθετούνται ευρέως από το οικοσύστημα των επιχειρήσεων (π.χ. συστήματα διαχείρισης περιεχομένου, ιστότοποι με φόρμες ελέγχου ταυτότητας, διαδικτυακές εφαρμογές), ο δυνητικός αντίκτυπος από περιστατικά που προέρχονται από επιθέσεις αυτής της ευρείας κατηγορίας θα μπορούσε να είναι σοβαρός. Επιπλέον, ο αριθμός αυτών των επιθέσεων αυξάνεται συνεχώς χρόνο με το χρόνο. Συγκεκριμένα, σύμφωνα με πρόσφατη έκθεση του ENISA [24], το 40% όλων των περιστατικών κυβερνοασφάλειας αναφέρεται σε επιθέσεις ιστού, ενώ μια άλλη έκθεση [25], αποκαλύπτει μια αύξηση της τάξης του 52% στον αριθμό των επιθέσεων σε διαδικτυακές εφαρμογές. Για τους λόγους αυτούς, η κατηγορία αυτή θα πρέπει οπωσδήποτε να θεωρηθεί ως βασικό μέρος της μεθοδολογίας μοντελοποίησης απειλών και αξιολόγησης κινδύνων του συστήματος ΜΥΡΙΩΠΟΣ.

[10] https://www.invicti.com/learn/local-file-inclusion-lfi/

2.9 Κακόβουλο Λογισμικό

Το κακόβουλο λογισμικό (malware) είναι ένας γενικός όρος που αναφέρεται σε κάθε τύπο κακόβουλου λογισμικού που έχει σχεδιαστεί για να βλάψει ή να εκμεταλλευτεί οποιαδήποτε προγραμματιζόμενη συσκευή, υπηρεσία ή δίκτυο. Οι εγκληματίες του κυβερνοχώρου το χρησιμοποιούν συνήθως για να αποσπάσουν δεδομένα από τις μολυσμένες συσκευές με σκοπό την άμεση ή έμμεση οικονομική εκμετάλλευση. Τα δεδομένα αυτά μπορεί να κυμαίνονται από οικονομικά δεδομένα έως αρχεία υγειονομικής περίθαλψης, προσωπικά μηνύματα ηλεκτρονικού ταχυδρομείου και κωδικούς πρόσβασης (οι δυνατότητες για το είδος των πληροφοριών που μπορούν να παραβιαστούν έχουν γίνει ατελείωτες). Επιπλέον, σε αυτά περιλαμβάνεται η κατασκοπεία και η διατάραξη της ακεραιότητας ή της διαθεσιμότητας συστημάτων και υπηρεσιών. *Με άλλα λόγια, το λογισμικό αναγνωρίζεται ως κακόβουλο λογισμικό με βάση την προβλεπόμενη χρήση του και όχι με βάση μια συγκεκριμένη τεχνική ή τεχνολογία που χρησιμοποιείται για την κατασκευή του.* Από την άποψη των εταιριών, καθώς αυξάνεται η εξάρτηση από τους υπολογιστές και το διαδίκτυο γενικότερα, αυξάνονται και τα περιστατικά ασφάλειας που βασίζονται σε κακόβουλο λογισμικό. Ενδεικτικά αναφέρουμε ότι το κακόβουλο λογισμικό αποτελεί την προέλευση έως και του 39% των συμβάντων ασφάλειας στον κυβερνοχώρο [25].

Υπάρχουν διάφορες κοινές οικογένειες κακόβουλου λογισμικού, συμπεριλαμβανομένων των κλασικών και καλά μελετημένων όπως οι ιοί, τα warms, τα trojans, τα rootkits, τα adware και τα spyware. Εκτός από εκτεταμένες αναλύσεις για κάθε κατηγορία κακόβουλου λογισμικού, στη βιβλιογραφία έχουν προταθεί πολλαπλές τεχνικές μετριασμού. Μερικές από αυτές είναι τα διάφορα συστήματα ανίχνευσης κακόβουλου λογισμικού με βάση υπογραφές σε πολλαπλά επίπεδα παρακολούθησης (π.χ. δίκτυο, κεντρικός υπολογιστής, εφαρμογή), η χρήση ειδικών εργαλείων για την ανάλυση κακόβουλου λογισμικού, ο μετριασμός κακόβουλου λογισμικού και η ανταλλαγή πληροφοριών σχετικά με τις τακτικές των επιτιθέμενων και τις απειλές (π.χ. MISP[11]), το φιλτράρισμα αλληλογραφίας και η αφαίρεση εκτελέσιμων συνημμένων αρχείων. Ωστόσο, υπάρχουν ορισμένες ειδικές οικογένειες, όπως τα memory-scraping malware και τα ransomware, που χρειάζονται πρόσθετη προσοχή.

Επιπρόσθετα, υπάρχουν malware που δεν έχουν εκτελέσιμα αρχεία, καθιστώντας ευκολότερη την παράκαμψη των τεχνικών ασφαλείας που εφαρμόζονται. Συγκεκριμένα, αντί για ένα εκτελέσιμο αρχείο, αυτός ο τύπος κακόβουλου λογισμικού επιτρέπει σε έναν επιτιθέμενο να εισάγει κακόβουλο κώδικα σε ήδη εγκατεστημένο και αξιόπιστο λογισμικό, είτε εξ αποστάσεως είτε με την λήψη αρχείων ή εγγράφων (π.χ. εγγράφων MS Word) με κακόβουλες μακροεντολές. Ως αποτέλεσμα, τα συγκεκριμένα malware εμφανίζουν υψηλότερα ποσοστά επιτυχίας σε σύγκριση με άλλους τύπους κακόβουλου λογισμικού καθώς οι τελικοί χρήστες είναι απροετοίμαστοι και ανυποψίαστοι.

Επίσης, το κακόβουλο λογισμικό memory-scraping είναι ένας τύπος κακόβουλου λογισμικού που βοηθά τους επιτιθέμενους να βρουν προσωπικά δεδομένα. Εξετάζει τη μνήμη για να αναζητήσει ευαίσθητα δεδομένα που δεν είναι διαθέσιμα μέσω άλλων διεργασιών. Αν και η κρυπτογράφηση δεδομένων χρησιμοποιείται ευρέως για την ασφάλεια των δεδομένων, το memory-scraping βρίσκει αδύναμες περιοχές από τις οποίες μπορεί να κλέψει δεδομένα. Για παράδειγμα, ορισμένα κακόβουλα λογισμικά memory-scraping κλέβουν κρυπτογραφημένα δεδομένα από εφαρμογές μέσω των οποίων τα δεδομένα πέρασαν χωρίς

[11] https://www.misp-project.org/

κρυπτογράφηση. Αυτό καθιστά πολλές τυπικές προσπάθειες ασφάλειας αναποτελεσματικές και μπορεί να οδηγήσει σε μεγάλες επιπτώσεις στην εμπιστευτικότητα ενός συστήματος ή των δεδομένων του.

Τέλος, το ransomware είναι μια συνεχώς εξελισσόμενη μορφή κακόβουλου λογισμικού που σχεδιάστηκε ειδικά για να κρυπτογραφεί αρχεία σε μια συσκευή, καθιστώντας τα αρχεία και τα συστήματα που βασίζονται σε αυτά μη χρησιμοποιήσιμα. Στη συνέχεια, οι κακόβουλοι χρήστες απαιτούν λύτρα σε αντάλλαγμα για τα κλειδιά αποκρυπτογράφησης. Πρόσφατα, τα περιστατικά ransomware έχουν γίνει όλο και πιο διαδεδομένα μεταξύ επιχειρήσεων, κυβερνητικών οργανισμών και οργανισμών υποδομών ζωτικής σημασίας, παράγοντας δισεκατομμύρια δολάρια σε πληρωμές σε εγκληματίες του κυβερνοχώρου και προκαλώντας σημαντικές ζημιές και έξοδα για τα συμβαλλόμενα μέρη που έχουν εκτεθεί. Οι δράστες που χρησιμοποιούν αυτήν την τακτική συχνά απειλούν να πουλήσουν ή να διαρρεύσουν τα εξαχθέντα δεδομένα ή τις πληροφορίες ελέγχου ταυτότητας εάν δεν καταβληθούν τα λύτρα, επηρεάζοντας έτσι την εμπιστευτικότητα των πληροφοριών και τη συνολική φήμη ενός οργανισμού. Ταυτόχρονα, όσο δεν καταβάλλονται τα λύτρα, το επηρεαζόμενο μέρος δεν μπορεί να έχει πρόσβαση σε δεδομένα που μπορεί να είναι ζωτικής σημασίας για τις λειτουργικές του διαδικασίες, επομένως δεν μπορεί να διασφαλιστεί η διαθεσιμότητα των πληροφοριών. Για το σκοπό αυτό, είναι απαραίτητο να λάβουμε υπόψη μας και αυτό το είδος απειλής στη μεθοδολογία αξιολόγησης κινδύνου, ώστε να είμαστε σε θέση να προτείνουμε αργότερα κατευθυντήριες γραμμές και δράσεις μετριασμού.

2.10 Επιθέσεις Πλημμύρας / Τερματισμού Υπηρεσίας

Η επίθεση Denial of Service (DoS)[12] είναι μια επίθεση που αποσκοπεί στο να τερματίσει ένα μηχάνημα, μια εφαρμογή διαδικτύου, μια υπηρεσία ή ένα δίκτυο, καθιστώντας το απρόσιτο στους χρήστες που το χρησιμοποιούν. Οι επιθέσεις DoS το επιτυγχάνουν αυτό κατακλύζοντας τον στόχο με κίνηση ή στέλνοντάς του πληροφορίες που προκαλούν κατάρρευση της εφαρμογής. Και στις δύο περιπτώσεις, η επίθεση DoS στερεί από τους νόμιμους χρήστες την υπηρεσία ή τον πόρο που περίμεναν. Ένας βελτιωμένος τύπος επίθεσης DoS είναι η Distributed Denial of Service (DDoS)[13] που συμβαίνει όταν πολλά συστήματα ενορχηστρώνουν μια συγχρονισμένη επίθεση DoS σε έναν μόνο στόχο ή σε ένα σύνολο στόχων. Η ουσιαστική διαφορά είναι ότι αντί να επιτίθεται ο στόχος από μία τοποθεσία, επιτίθεται από πολλές τοποθεσίες ταυτόχρονα. Διαισθητικά, θα μπορούσε κανείς να υποθέσει ότι οι επιτιθέμενοι δεν ενδιαφέρονται να εξαπολύουν επιθέσεις DoS εναντίον μικρών εταιριών ή οργανισμών. Ωστόσο, αυτό δεν ισχύει καθώς τέτοιου μεγέθους επιχειρήσεις δεν διαθέτουν χρήματα για μέτρα αντιμετώπισης των κυβερνοεπιθέσεων και ως εκ τούτου αποτελούν εύκολο στόχο.

Αν και η πλειονότητα των επιθέσεων DoS εξακολουθεί να πραγματοποιείται με καλά μελετημένες τεχνικές πλημμύρας (μέσω των πρωτοκόλλων SYN, UDP, TCP, ICMP), οι εγκληματίες του κυβερνοχώρου αναζητούν ενεργά νέες υπηρεσίες και πρωτόκολλα για την ενίσχυση αυτών των επιθέσεων. Για παράδειγμα, η έκθεση της Kaspersky για το πρώτο τρίμηνο του 2022 [26], σχετικά με τις επιθέσεις DDoS αναφέρει ότι το τοπίο διαμορφώθηκε από τη συνεχιζόμενη σύγκρουση μεταξύ Ρωσίας και Ουκρανίας όπου η πλειοψηφία των συμβάντων DDoS αφορούσαν αυτές τις χώρες και υφιστάμενες διαδικτυακές εφαρμογές.

Τέλος, η πανδημία COVID-19 χρησιμοποιήθηκε ως έμμεσος ενισχυτής για επιθέσεις DDoS. Συγκεκριμένα, κατά τη διάρκεια αυτής της περιόδου, κορυφώθηκε η χρήση εργαλείων τηλεδιάσκεψης και λύσεων

[12] https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
[13] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

απομακρυσμένης συνεργασίας. Επομένως, στη περίπτωση αυτή, οι επιθέσεις DDoS πραγματοποιούνται εισάγοντας υπερβολική πίεση στο δίκτυο όσον αφορά στις απαιτήσεις εύρους ζώνης, δυσκολεύοντας έτσι την απομακρυσμένη εργασία. Αυτό οδηγεί σε μειωμένη ικανότητα ενός οργανισμού να αμύνεται έναντι επιθέσεων DDoS.

Στο πλαίσιο του έργου ΜΥΡΙΩΠΟΣ, θα παρακολουθούμε συνεχώς τις υφιστάμενες εφαρμογές μέσω των Εποπτών και συνδυαστικά με τον Ενορχηστρωτή θα μετράμε σε πραγματικό χρόνο την υπολογιστική ισχύ, μνήμη και δίσκο που πιθανώς να εξαντλούνται σε μια επικείμενη DDoS επίθεση κατά τη διαδικασία αξιολόγησης κινδύνων. Τέλος, μέσω ανάλυσης κειμένων από το Σκοτεινό Δίκτυο θα αναζητούμε σε καθημερινή βάση μαζικές κλήσεις μεταξύ χρηστών σε forums για το συγχρονισμό τους σε DDoS επιθέσεις.

2.11 Ευπάθειες Πρωτοκόλλων και Επιθέσεις

Οι επιθέσεις κατά των υφιστάμενων ευπαθειών των ευρέως αποδεκτών πρωτοκόλλων συνήθως εκμεταλλεύονται συγκεκριμένα χαρακτηριστικά ή σφάλματα υλοποίησης ενός ή περισσότερων πρωτοκόλλων που χρησιμοποιούνται από τις υπηρεσίες ή τις εφαρμογές που τα χρησιμοποιούν. Στόχος είναι η κατανάλωση των διαθέσιμων πόρων ή ο επηρεασμός της ακεραιότητας των διαθέσιμων στοιχείων, με απώτερο σκοπό τη διατάραξη της κανονικής λειτουργίας μιας εφαρμογής / υπηρεσίας.

Για παράδειγμα, θα μπορούσε κανείς να εκμεταλλευτεί τα καλά χαρακτηριστικά του πρωτοκόλλου ICMP για κακόβουλους σκοπούς και να εξαπολύσει μια DDoS επίθεση ή να εκμεταλλευτεί τα υπάρχοντα σφάλματα της απομακρυσμένης πρόσβασης επιφάνειας εργασίας για να αποκτήσει πρόσβαση σε ένα σύστημα. Επιπλέον, όταν βρίσκεται κανείς σε κοντινή απόσταση, θα μπορούσε να κάνει κατάχρηση των καλών χαρακτηριστικών των πρωτοκόλλων που χρησιμοποιούνται στις ασύρματες συνδέσεις για να αποκτήσει πρόσβαση σε ένα υποσύνολο συσκευών από ένα κοντινό σημείο πρόσβασης ή να εκμεταλλευτεί πρόσφατα ανακαλυφθείσες ευπάθειες του WPA[14], όπως αναφέρει ο ENISA [27]. Επιπλέον, οι επιτιθέμενοι μπορούν να κάνουν κατάχρηση των χαρακτηριστικών των πρωτοκόλλων ARP[15] και DNS[16] για να εξαπολύσουν σχετικές επιθέσεις poisoning, spoofing, hijacking και να διαταράξουν την κανονική λειτουργία ενός τοπικού δικτύου. Τέλος, κάποιος θα μπορούσε να στέλνει επανειλημμένα άκυρες υπογραφές για να αναγκάσει έναν διακομιστή ελέγχου ταυτότητας να καταναλώσει τους πόρους του και να τους καταστήσει μη διαθέσιμους σε άλλους χρήστες. Ο κατάλογος των πιθανών επιθέσεων κατάχρησης πρωτοκόλλων είναι ατελείωτος και θα μπορούσε να επηρεάσει την εύρυθμη λειτουργία ενός οργανισμού με πολλούς διαφορετικούς τρόπους. Προσπαθούμε να εξετάσουμε τουλάχιστον τις γνωστές επιθέσεις κατά ευρέως αποδεκτών πρωτοκόλλων στη διαδικασία εκτίμησης κινδύνου, ώστε να είμαστε σε θέση να προσφέρουμε κατάλληλη παρακολούθηση, πρόληψη και μετριασμό τέτοιων επιθέσεων.

[14] https://www.krackattacks.com/
[15] https://www.imperva.com/learn/application-security/arp-spoofing/
[16] https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/

2.12 Μοντελοποίηση Πόρων στο Οικοσύστημα του ΜΥΡΙΩΠΟΣ

3 Απαιτήσεις ασφάλειας, ιδιωτικότητας, ανθεκτικότητας και υψηλής διαθεσιμότητας

Το κεφάλαιο αυτό συγκεντρώνει το σύνολο των απαιτήσεων ασφάλειας, ιδιωτικότητας και διαθεσιμότητας που καθορίζουν τις προδιαγραφές του συστήματος. Οι απαιτήσεις ασφαλείας χωρίζονται σε υποχρεωτικές απαιτήσεις και σε επιθυμητές απαιτήσεις. Το κίνητρο για τον καθορισμό των απαιτήσεων ασφαλείας, ιδιωτικότητας, ανθεκτικότητας και υψηλής διαθεσιμότητας είναι να προσδιοριστούν οι λειτουργικές και μη λειτουργικές απαιτήσεις που θα καθορίσουν τις προδιαγραφές του συστήματος καθώς και οι ποσοτικές και ποιοτικές απαιτήσεις των χρηστών που μπορούν να υλοποιηθούν σε έργα έρευνας και καινοτομίας και ως εκ τούτου σε έργα ανάπτυξης λογισμικού. Το παρόν κεφάλαιο παρέχει μια **περιεκτική περιγραφή της μεθοδολογίας για την εξαγωγή και ικανοποίηση των απαιτήσεων των χρηστών** σε ένα καθορισμένο περιβάλλον, και της **διαδικασίας που υιοθετήθηκε στο πλαίσιο του έργου ΜΥΡΙΩΠΟΣ**.
Η πλήρης εικόνα του ΜΥΡΙΩΠΟΣ αναπτύχθηκε με τη μεθοδολογία για τον καθορισμό του Ελάχιστου Βιώσιμου Προϊόντος (ΕΒΠ) η οποία απαιτεί τον καθορισμό των **λειτουργικών απαιτήσεων και τεχνικών προδιαγραφών** για τον ορισμό της Ελάχιστης Βιώσιμης Αρχιτεκτονικής (ΕΒΑ)[17]. Η μεθοδολογία αυτή μας επέτρεψε να εξαγάγουμε τις **λειτουργικές απαιτήσεις και τεχνικές προδιαγραφές του ΜΥΡΙΩΠΟΣ** που περιγράφονται σε αυτό το κεφάλαιο. Η χρήση αυτής της μεθοδολογίας μας επέτρεψε επίσης να χαρτογραφήσουμε αυτές τις διαφορετικές λειτουργικές και τεχνικές απαιτήσεις μέσα από συγκεκριμένες ανάγκες περιπτώσεων χρήσης και σεναρίων που εξάγονται. Οι λειτουργίες που απορρέουν επιτρέπουν στη συνέχεια το σχεδιασμό του Ελάχιστου Βιώσιμου Προϊόντος του έργου[18]. Το ΕΒΠ αφορά στη δημιουργία ενός προϊόντος που περιλαμβάνει μια σειρά θεμελιωδών χαρακτηριστικών για την αποτελεσματική και γρήγορη εισαγωγή στην αγορά στην οποία κατευθύνεται. Επομένως, στη περίπτωση μας το ΕΒΠ αποτελείται από τις βασικές υπηρεσίες ασφαλείας, ιδιωτικότητας, ανθεκτικότητας και υψηλής διαθεσιμότητας συμπεριλαμβανομένης της διαχείρισης **της ασφάλειας των υποδομών δικτύων και υπηρεσιών υπολογιστικού νέφους καθώς και της δυναμικής εκτίμησης κινδύνου σε πραγματικό χρόνο.**

3.1 Μεθοδολογία Εξαγωγής Απαιτήσεων

Αναλυτικά, το Ελάχιστο Βιώσιμο Προϊόν (ΕΒΠ), όσον αφορά στις λειτουργικές απαιτήσεις, είναι ένας όρος που επινοήθηκε από τον Frank Robinson το 2001 και περιγράφει μια ευέλικτη και λιτή προσέγγιση στον προγραμματισμό και το σχεδιασμό προϊόντων που αντανακλώνται από την προτεινόμενη Αρχιτεκτονική Λύση. Το ελάχιστο βιώσιμο προϊόν είναι συνήθως μια έκδοση ενός προϊόντος με αρκετά χαρακτηριστικά για να ικανοποιήσει τους βασικούς χρήστες, ενώ ο κύριος στόχος του είναι να παρέχει ανατροφοδότηση για μελλοντική βελτίωση και ανάπτυξη προϊόντων. **Μπορεί να χρησιμοποιηθεί για τη συλλογή πληροφοριών νωρίς κατά τη διάρκεια της ανάπτυξης προϊόντων**. Αυτό είναι συχνά λιγότερο δαπανηρό από την ανάπτυξη ενός προϊόντος με περισσότερες δυνατότητες και επιτρέπει την αναπροσαρμογή και βελτίωσή του στην πορεία. Επειδή το ΕΒΠ δοκιμάζει πιθανά επιχειρηματικά μοντέλα σε πελάτες για να δει πώς αντιδρά η αγορά, η διαδικασία είναι ιδιαίτερα χρήσιμη για νέες / νεοσύστατες εταιρείες που ενδιαφέρονται περισσότερο να ανακαλύψουν που υπάρχουν πιθανές επιχειρηματικές ευκαιρίες παρά να εκτελέσουν ένα προκατασκευασμένο, απομονωμένο επιχειρηματικό μοντέλο. Για το έργο ΜΥΡΙΩΠΟΣ, που αναμένεται να

[17] https://www.infoq.com/articles/minimum-viable-architecture/
[18] https://www.techopedia.com/definition/27809/minimum-viable-product-mvp

φτάσει στο Επίπεδο Τεχνολογικής Ετοιμότητας (ΕΤΤ) 6 στο τέλος του που σχετίζεται με το επίπεδο Επίδειξης της Τεχνολογίας, η ανάγκη πίσω από το σχεδιασμό ενός ΕΒΠ είναι διαφορετική από εκείνη μιας νεοσύστατης εταιρείας. Με άλλα λόγια, ο ορισμός του **ΕΒΠ του ΜΥΡΙΩΠΟΣ διευκολύνει το κοινό όραμα της κοινοπραξίας.** Η κοινοπραξία έχει παρουσιάσει τους σαφείς στόχους του έργου από τα πρώιμα κιόλας στάδια καθώς υπήρξε επιπλέον και ρητή συναίνεση σχετικά με τα βασικά χαρακτηριστικά του συστήματος ΜΥΡΙΩΠΟΣ. Σε αυτό το πλαίσιο, η δημιουργία ενός αρχικού ΕΒΠ είναι απαραίτητη για την ομαλή ανάπτυξη και υλοποίηση του έργου. Το γεγονός αυτό δεν απορρέει μόνο από τους πόρους και τους χρονικούς περιορισμούς για την εφαρμογή του συνολικού πλαισίου, αλλά συνδέεται άμεσα με τη γενική έννοια του ΜΥΡΙΩΠΟΣ που απαιτεί την συμμετοχή όλων των εταίρων στα παραδοτέα. Ως εκ τούτου, η επιλογή της κατάλληλης **στρατηγικής για τη δημιουργία του ΕΒΠ θα δοκιμάζει συνεχώς τα αποτελέσματα έναντι των απαιτήσεων του πελάτη και του τελικού χρήστη.**

Οι δύο προβλεπόμενες περιπτώσεις επίδειξης χρήσης διαδραματίζουν κρίσιμο ρόλο στη διαδικασία ορισμού ενός επιτυχημένου ΕΒΠ καθώς περιγράφουν λεπτομερώς ποιες διαδικασίες χρησιμοποιούνται σήμερα και τυχόν προκλήσεις που ενδέχεται να αντιμετωπιστούν και χρειάζεται να προστατεύονται από τη μεθοδολογία ΜΥΡΙΩΠΟΣ. Η αλληλεπίδραση με τον πιλότο επίδειξης συμβάλει στη δημιουργία ενός σαφούς πεδίου εφαρμογής καθώς και του σκοπού του έργου, εμπλουτίζοντας την **πραγματική αξία της προτεινόμενης λύσης** για τους τελικούς χρήστες. Μέσω αυτής της διαδικασίας διαμοιρασμού του πιλότου, των χρηστών, των τεχνικών και των ερευνητών της κοινοπραξίας απαντάμε στην ερώτηση "*Ποιο πρόβλημα επιλύετε;*".

Το ΕΒΠ του συστήματος ΜΥΡΙΩΠΟΣ περιλαμβάνει όλες τις υποχρεωτικές και επιθυμητές απαιτήσεις που καλύπτονται από τις περιπτώσεις χρήσης και προκύπτει μέσω της διαδικασίας που απεικονίζεται στην Εικόνα 1. Η διαδικασία αυτή επιτρέπει τον καθορισμό των αρχικών λειτουργικών απαιτήσεων και τεχνικών προδιαγραφών ως υποχρεωτικών και επιθυμητών χαρακτηριστικών του συστήματος και τη χαρτογράφηση των εν λόγω τεχνικών απαιτήσεων στις ανάγκες των περιπτώσεων χρήσης.

Εικόνα 1. Μεθοδολογία για τον καθορισμό των λειτουργικών απαιτήσεων του ΜΥΡΙΩΠΟΣ

3.1.1 Μεθοδολογία Καθορισμού Απαιτήσεων

Η συλλογή του αρχικού συνόλου των απαιτήσεων που ικανοποιεί το έργο ΜΥΡΙΩΠΟΣ στους χρήστες θέτει τα θεμέλια για το σχεδιασμό και την ανάπτυξη των τεχνικών δραστηριοτήτων του. Η κοινοπραξία,

ακολουθώντας το αρχικό όραμα που είχε ήδη συζητηθεί κατά τη διάρκεια της προετοιμασίας της περιγραφής των απαιτήσεων του έργου, εργάστηκε για **την καλύτερη διαμόρφωση των προσφερόμενων υπηρεσιών του έργου ΜΥΡΙΩΠΟΣ**. Επιπλέον, πραγματοποιήθηκε *ανάλυση των μεθόδων και τεχνολογιών αιχμής για κάθε μία από τις καινοτομίες του έργου.* Δεδομένης της ερευνητικής και καινοτόμου φύσης του έργου ΜΥΡΙΩΠΟΣ, μια τέτοια ανάλυση επιτρέπει στην κοινοπραξία να "*Καταλάβει τους Ανταγωνιστές*" και να "*Κατανοήσει την Τρέχουσα Κατάσταση της Αγοράς*". Το υλικό αυτό θα αξιοποιηθεί περεταίρω από την Ενότητα Εργασίας 6 (ΕΕ6) που σχετίζεται με τη διάδοση, την επικοινωνία και την εκμετάλλευση του έργου.

Ως επόμενο βήμα στον ορισμό των λειτουργιών και των υπηρεσιών του ΜΥΡΙΩΠΟΣ, η κοινοπραξία προσδιόρισε τα **ενδιαφερόμενα μέρη** - στο πλαίσιο του επιχειρηματικού οικοσυστήματος της κυβερνοασφάλειας καθώς και τον **ενδιαφερόμενο πιλότο και φορείς** για την κατανόηση του «*Για ποιον*» αναπτύσσονται.

Προς αυτή την κατεύθυνση, απαραίτητη προϋπόθεση είναι η συλλογή, ορισμός και προτεραιοποίηση των απαιτήσεων. Οι απαιτήσεις του ΜΥΡΙΩΠΟΣ συλλέγονται (αφενός) με τη μορφή **λειτουργικών απαιτήσεων και τεχνικών προδιαγραφών** που απορρέουν από τους τεχνικούς εταίρους της κοινοπραξίας, οι οποίοι είναι υπεύθυνοι για το σχεδιασμό και την ανάπτυξη της συνολικής λύσης. Από την άλλη, ο ορισμός των απαιτήσεων καθοδηγείται επίσης από τον πιλότο του έργου με τη μορφή **περιπτώσεων χρήσης.** Μετά τη συλλογή όλων των απαιτήσεων, ο εταίρος που είναι υπεύθυνος για την εξαγωγή των απαιτήσεων (MAGGIOLI) θα τις ιεραρχήσει με τη βοήθεια και τη συγκατάθεση της κοινοπραξίας στο σύνολό της.

Αργότερα κατά τη διάρκεια του έργου, αλλά αναπόσπαστο μέρος του ορισμού του ΕΒΠ, είναι ο κύκλος «Σχεδιασμός, Υλοποίηση & Βελτίωση» που έχει προβλεφθεί κατά την ανάπτυξη των τεχνικών Ενοτήτων Εργασίας 2, 3, 4 και 5, καθώς και της ενοποιημένης λύσης του ΜΥΡΙΩΠΟΣ στο σύνολό της. Όλοι οι τεχνικοί συνεργάτες έχουν την ευκαιρία να αναπτύξουν τις ενότητες τους ακολουθώντας μια επαναληπτική διαδικασία, καθώς και να δοκιμάσουν τις ενότητες τους σε πρώιμους και ώριμους χώρους δοκιμών, προκειμένου να μεγιστοποιηθεί η προστιθέμενη αξία σε κάθε ενότητα, καθώς και στο σύστημα ΜΥΡΙΩΠΟΣ. Η εταιρία UBITECH για το σκοπό αυτό διαθέτει στο έργο το υπολογιστικό περιβάλλον για τις δοκιμές και την τελική υλοποίηση της ενοποιημένης λύσης.

Συνολικά, η διαδικασία καθορισμού των απαιτήσεων, όπως περιγράφεται στην παρούσα ενότητα, αναμένεται να καταλήξει σε μια **συγκεκριμένη και ολιστική περιγραφή της κύριας λύσης του ΜΥΡΙΩΠΟΣ σε συνδυασμό με μια λεπτομερή αναγνώριση και ανάλυση των τεχνικών, λειτουργικών και υφιστάμενων αρχιτεκτονικών στοιχείων**. Αυτό το σύνολο λειτουργικών απαιτήσεων, στον πυρήνα του, είναι προσανατολισμένο στην αναπαράσταση του συνολικού οράματος της κοινοπραξίας και της διαδικασίας που υιοθετήθηκε για την ανάπτυξη του προϊόντος, λαμβάνοντας επίσης υπόψη τις προσδοκίες των χρηστών προσφέροντάς τους υπηρεσίες προστιθέμενης αξίας.

Δεδομένου των σαφών στόχων του έργου στο στάδιο της πρότασης, υπήρξε σταθερή συναίνεση ως προς τα ουσιώδη χαρακτηριστικά του ΜΥΡΙΩΠΟΣ - με βάση έναν συνδυασμό εξατομικευμένων λειτουργιών ασφάλειας στον κυβερνοχώρο, βελτιωμένων δυνατοτήτων επιχειρησιακής ασφάλειας και αυτοματοποιημένης ενορχήστρωσης προηγμένων υπηρεσιών κυβερνοασφάλειας. Οι υπηρεσίες εμπλουτίζονται με συστήματα δυναμικής εκτίμησης κινδύνου και λήψης αποφάσεων σε πραγματικό χρόνο. Αυτό το κοινό όραμα βοήθησε στον εντοπισμό των επιθυμητών χαρακτηριστικών που οργανώθηκαν σε λειτουργικές απαιτήσεις, τεχνικές προδιαγραφές και απαιτήσεις ασφάλειας / απορρήτου.

Ως προς τον ορισμό των απαιτήσεων, «Απαίτηση» είναι μια δήλωση που εκφράζει μια ανάγκη και τους σχετικούς περιορισμούς της καθώς και τις συνθήκες με σκοπό τη μετατροπή (μέσω ανάλυσής) των ενδιαφερόμενων μερών σε μια τεχνική λύση ενός προϊόντος που υποστηρίζει αυτές τις υπηρεσίες. Η σωστή περιγραφή των απαιτήσεων είναι ύψιστης σημασίας για την παραγωγή ενός σωστού προϊόντος, καθώς περιγράφουν συγκεκριμένες ανάγκες. Για το λόγο αυτό, είναι σημαντικό να είναι **πλήρεις, σαφείς, σωστές και συνεπείς**.

3.1.2 Εξαγωγή Τεχνικών Απαιτήσεων

Η μεθοδολογία που χρησιμοποιείται στο έργο ΜΥΡΙΩΠΟΣ είναι **μια ευέλικτη μεθοδολογία**, η οποία καταρχήν είναι **επαναληπτική** για να ενσωματώνει αλλαγές και βελτιώσεις, ενώ ορισμένες από τις βασικές έννοιες στις οποίες βασίζεται προάγουν την κατανόηση μεταξύ των επιχειρηματικών, τεχνικών και επιστημονικών αναγκών του έργου, θέτοντας σαφείς προσδοκίες στην αρχή και στις διαφορετικές εκδόσεις του λογισμικού. Στα πλαίσια του έργου ΜΥΡΙΩΠΟΣ προβλέπονται δυο (2) εκδόσεις λογισμικού, η μία στο 24^{ο} μήνα του έργου (Q8) και η δεύτερη στον 30^{ο} μήνα του έργου (Q10) [16].

Αρχικά, ο καθορισμός των απαιτήσεων του συστήματος ξεκίνησε με τη συνέντευξη των αρμόδιων τεχνικών συνεργατών της κοινοπραξίας και των τελικών χρηστών. Συγκεκριμένα, οι κατ' *ιδίαν συνεντεύξεις* πραγματοποιήθηκαν με τη χρήση διαδικτυακών εργαλείων και παρήγαγαν τις εκάστοτε ακατέργαστες απαιτήσεις του συστήματος. Οι ακατέργαστες απαιτήσεις είναι απαιτήσεις που δεν έχουν αναλυθεί και δεν έχουν ακόμη καταγραφεί σε μια καλά διαμορφωμένη μορφή απαιτήσεων [17]. Έπειτα, οι πρώτες απαιτήσεις συλλέχθηκαν και μια επαναληπτική εσωτερική διαδικασία εκτελέστηκε προκειμένου να παραχθούν σαφέστερα αποτελέσματα. Σε αυτό το σημείο η τεχνική που χρησιμοποιήθηκε ήταν οι ανοιχτές συζητήσεις χρησιμοποιώντας εργαλεία όπως το Miro[19] και οι βίντεο-κλήσεις. Στη συνέχεια, τα αποτελέσματα που συλλέχθηκαν συγκρίθηκαν με την τεχνική φύση του συστήματος και συνδέθηκαν με έναν από τους Στόχους 1 - 4 του έργου.

Ωστόσο, οι απαιτήσεις που προκύπτουν από τις συνεντεύξεις μπορεί μερικές φορές να είναι διφορούμενες, καθώς ενδέχεται να παρερμηνεύσουν τις ανάγκες των ενδιαφερόμενων μερών. **Για το λόγο αυτό, εκτός από τη συλλογή απαιτήσεων,** διεξήχθη επίσης ***ανάλυση των ληφθέντων δεδομένων*** **μέσω διεξοδικής ανασκόπησης της βιβλιογραφίας από τους εταίρους του ΜΥΡΙΩΠΟΣ**, προκειμένου να επικυρωθούν οι απαιτήσεις, καθώς και να εντοπιστούν τα πρότυπα και οι περιορισμοί που αφορούν στην ποιότητα των παραγόμενων απαιτήσεων.

Η συλλογή απαιτήσεων μέσα στο διάστημα των πρώτων 9 μηνών του έργου αναθεωρήθηκε συνεχώς και εξεταζόταν από την αντίστοιχη ομάδα του ΕΕ1. Οι συναντήσεις της ομάδας της ΕΕ1 πραγματοποιήθηκαν με τη μορφή ειδικών τηλεδιασκέψεων μεταξύ συγκεκριμένων συνεργατών του ΜΥΡΙΩΠΟΣ. Μεταξύ των καθηκόντων τους ήταν επίσης να παρέχουν πολύτιμη ανατροφοδότηση στους συμμετέχοντες, καθώς η εκμαίευση των απαιτήσεων των χρηστών εξαρτάται σε μεγάλο βαθμό από τις γνώσεις και την ωριμότητα των ενδιαφερόμενων μερών.

Με γνώμονα τη **διασφάλιση των επιχειρηματικών οικοσυστημάτων των εταιριών, των κατόχων υποδομών δικτύου και υπηρεσιών υπολογιστικού νέφους** οι πρόσθετες απαιτήσεις βασίζονται στον πιλότο επίδειξης του έργου και σε τυχόν πρόσθετα χαρακτηριστικά που οι συνεργάτες θα προσθέσουν σε μια τέτοια αρχιτεκτονική ασφάλειας στη φάση του σχεδιασμού. Ενώ οι «επιθυμητές» απαιτήσεις ενδέχεται να μην αποτελούν βασικό μέρος του έργου, συμπεριλήφθηκαν για λόγους πληρότητας, για να ενθαρρύνουν τα ανοικτά ερευνητικά ερωτήματα και να οδηγήσουν σε περαιτέρω ανεξάρτητη ή συνεργατική εργασία από τους εταίρους, η οποία θα μπορούσε αργότερα να συμβάλει στην καλύτερη διάχυση των αποτελεσμάτων του έργου.

Ο δεύτερος διαχωρισμός είναι για λόγους σαφήνειας στην κατανομή των απαιτήσεων μεταξύ των λειτουργικών πτυχών του ΜΥΡΙΩΠΟΣ ως λύσης και των υπηρεσιών ασφάλειας, προστασίας και απορρήτου. Αυτά χωρίστηκαν περαιτέρω σε κατηγορίες ανάλογα με το τεχνολογικό επίπεδο. Στη συνέχεια, οι κατηγορίες των απαιτήσεων συγκεντρώθηκαν και επισημοποιήθηκαν, ώστε να μπορούν να αντιστοιχιστούν συστηματικά στις απαιτήσεις των περιπτώσεων χρήσης που πρέπει να επιδειχθούν.

[19] https://miro.com/

3.2 Χρήστες και Ρόλοι του ΜΥΡΙΩΠΟΥ

Ένας από τους πρωταρχικούς στόχους του ΜΥΡΙΩΠΟΣ επικεντρώνεται στη διάδοση της επιστημονικής και τεχνολογικής γνώσης που παράγεται στο πλαίσιο του έργου και στη διασφάλιση τόσο μιας μεσοπρόθεσμης όσο και μακροπρόθεσμης σχέσης με τα ενδιαφερόμενα μέρη. Τα ενδιαφερόμενα μέρη εντάσσονται στην συλλογή των απαιτήσεων για να διασφαλιστεί ότι όλοι οι σχετικοί φορείς συμμετέχουν στη συν δημιουργία, σχεδιασμό και υλοποίηση ενός ανοικτού, ανθεκτικού και συνεργατικού οικοσυστήματος καινοτομίας στον κυβερνοχώρο.

Ως ενδιαφερόμενο μέρος σε οποιοδήποτε έργο έρευνας και καινοτομίας ορίζεται ο χρήστης και ο ρόλος που ενδιαφέρεται για την επιτυχία του έργου και των αποτελεσμάτων του και εισπράττει αξία από τη χρήση των υφιστάμενων υπηρεσιών. Αξίζει να σημειωθεί ότι, παρόλο που κάθε ενδιαφερόμενος μοιράζεται το κοινό όραμα όπως ορίζεται από το εκάστοτε έργο, ενδέχεται να έχει ελαφρώς διαφορετικούς στόχους και προσδοκίες από αυτό. Ο Πίνακας 1 παρουσιάζει τα πολλαπλά κοινά, χρήστες και τους πιθανούς πελάτες που ενδεχομένως ενδιαφέρονται για τις υπηρεσίες που αναπτύσσει και υλοποιεί το έργο ΜΥΡΙΩΠΟΣ.

Πίνακας 1. Κοινό και Πιθανοί Πελάτες του έργου ΜΥΡΙΩΠΟΣ

Όνομα ενδιαφερομένου	Περιγραφή των ενδιαφερομένων μερών
Επιχειρήσεις, Βιομηχανικοί Σύλλογοι & Τεχνολογικοί Φορείς	Περιλαμβάνει ιδιωτικές επιχειρήσεις που δραστηριοποιούνται στον τομέα της ασφάλειας στον κυβερνοχώρο, των οποίων οι δραστηριότητες ταιριάζουν με τους στόχους του ΜΥΡΙΩΠΟΣ: ✓ Οι Βιομηχανικοί Σύλλογοι είναι οργανισμοί που υποστηρίζουν τις εταιρείες και τους εργοδότες ενός συγκεκριμένου τύπου βιομηχανίας και προστατεύουν τα δικαιώματά τους. ✓ Οι τεχνολογικοί φορείς είναι κοινοπραξίες ή ιδιωτικές πρωτοβουλίες που ασκούν επιχειρηματικές και τεχνολογικές δραστηριότητες.
Πάροχος υπηρεσιών ασφαλείας	Αναπτύσσουν, επεκτείνουν και παρέχουν καινοτόμες υπηρεσίες κυβερνοασφάλειας. Συμβουλεύουν τους πελάτες τους σχετικά με εξελιγμένους μηχανισμούς ασφάλειας, μετριασμού επιθέσεων και εφαρμογών υποστήριξης αποφάσεων. Ανήκουν στους άμεσα προβλεπόμενους δικαιούχους του ΜΥΡΙΩΠΟΣ, καθώς φιλοδοξούν να αναπτύξουν τις δικές τους υπηρεσίες που εντάσσονται στη συνολική αγορά υπηρεσιών ασφαλείας του ΜΥΡΙΩΠΟΣ.
Ερευνητική και επιστημονική κοινότητα	Περιλαμβάνει πανεπιστήμια, σχολές μηχανικών πληροφορικής, ερευνητικά κέντρα, και βιομηχανικά τμήματα, κ.λπ. Εκτελούν έρευνα και καινοτομία τελευταίας τεχνολογίας και δημοσιεύουν τα αποτελέσματά τους στην ευρύτερη κοινότητα. Στοχεύουν στη συνέχιση της έρευνας και της καινοτομίας και μπορούν επίσης να αξιοποιήσουν τα αποτελέσματα σε δραστηριότητες κατάρτισης και καθοδήγησης. Είναι άμεσοι συντελεστές των δράσεων του ΜΥΡΙΩΠΟΣ.

Διαχειριστής συστήματος	Ο διαχειριστής συστήματος είναι υπεύθυνος για τη συντήρηση, τη διαμόρφωση και την αξιόπιστη λειτουργία των υπηρεσιών του ΜΥΡΙΩΠΟΣ. Ο διαχειριστής συστήματος προσπαθεί να διασφαλίσει την απόδοση και την ασφάλεια του συστήματος που διαχειρίζεται.
Επαγγελματίες ασφαλείας στον κυβερνοχώρο	Οι επαγγελματίες ασφαλείας στον κυβερνοχώρο δημιουργούν και εφαρμόζουν ελέγχους ασφαλείας στα συστήματα υλικού και λογισμικού των υφιστάμενων συστημάτων. Διασφαλίζουν επίσης ότι τα συστήματα λειτουργούν όπως πρέπει και ότι είναι ασφαλή από επιθέσεις.
Πάροχος δικτυακών και υπολογιστικών υποδομών	Οι πάροχοι δικτυακών και υπολογιστικών υποδομών παρέχουν το εικονικό και φυσικό υλικό που μπορεί να αξιοποιηθεί από την εκάστοτε εφαρμογή. Παρέχουν επίσης την υπολογιστική ισχύ, τη μνήμη και τα μέσα σταθερής αποθήκευσης για την παροχή εφαρμογών.

Ο προσδιορισμός των ενδιαφερομένων μερών του έργου συνδέεται στενά με τις δραστηριότητες διάδοσης που προγραμματίζονται στο πλαίσιο της ΕΕ6, καθώς οι ενδιαφερόμενοι φορείς θεωρούνται ως επιδιωκόμενος στόχος για τη διεύρυνση της κοινότητας που πιθανώς την ενδιαφέρουν οι υπηρεσίες που υλοποιούνται στο έργο ΜΥΡΙΩΠΟΣ. Τα μέλη της κοινοπραξίας στοχεύουν να προωθήσουν εγκαίρως τα αποτελέσματα του έργου στους ενδιαφερόμενους φορείς με κατάλληλους μηχανισμούς, διασφαλίζοντας ότι οι κοινοί στόχοι για την αξιοποίηση του έργου και η απορρόφηση από την αγορά θα πραγματοποιηθεί το συντομότερο δυνατό.

Η παρούσα ενότητα συνεχίζει με τον προσδιορισμό των φορέων που προβλέπεται να αλληλεπιδρούν και να επωφελούνται από την αγορά των διαφορετικών υπηρεσιών ασφαλείας ΜΥΡΙΩΠΟΣ. Στο πλαίσιο του ΜΥΡΙΩΠΟΣ εντοπίζονται **τρεις τύποι δραστηριοτήτων αλληλεπίδρασης**, όσον αφορά στους διάφορους φορείς και τον τρόπο με τον οποίο μπορούν να χρησιμοποιήσουν τη λύση ΜΥΡΙΩΠΟΣ, ως ακολούθως.

- **Άμεση αλληλεπίδραση με το ΜΥΡΙΩΠΟΣ που επιτρέπει σε μια ιδιωτική επιχείρηση να αλληλεπιδρά άμεσα με τα στοιχεία και τις υπηρεσίες του συστήματος ΜΥΡΙΩΠΟΣ.** Θα μπορούσε να είναι το πρόσωπο που είναι υπεύθυνο για τον καθορισμό των κρίσιμων (περιουσιακών) στοιχείων του επιχειρηματικού οικοσυστήματος-στόχου (π.χ., υπηρεσίες, δεδομένα, βάσεις δεδομένων, δικτυακές υποδομές, λογαριασμοί χρηστών), έτσι ώστε στη συνέχεια να αναπτυχθούν τα κατάλληλα στοιχεία και υπηρεσίες του ΜΥΡΙΩΠΟΣ. Ή μπορεί να είναι το πρόσωπο (π.χ. ο διαχειριστής συστήματος) που ζητά πληροφορίες, αναλύσεις ή / και προβλέψεις προερχόμενες από τα στοιχεία του συστήματος ΜΥΡΙΩΠΟΣ.

- **Η έμμεση αλληλεπίδραση μπορεί να χωριστεί σε δύο περαιτέρω υποκατηγορίες: τελικός δικαιούχος και παρατηρητής.** Από τη μία πλευρά, ο τελικός δικαιούχος είναι ένα άτομο που με τον ρόλο του εργάζεται ή αλληλεπιδρά με το επιχειρηματικό οικοσύστημα στο οποίο αναπτύσσεται η λύση ΜΥΡΙΩΠΟΣ. Στην περίπτωση αυτή, το άτομο δεν έρχεται σε άμεση αλληλεπίδραση με τις υπηρεσίες του ΜΥΡΙΩΠΟΣ, ωστόσο επωφελείται από τα χαρακτηριστικά της λύσης με έμμεσο τρόπο. Από την άλλη πλευρά, ο παρατηρητής είναι ένας εξωτερικός ωφελούμενος ο οποίος ως προς το ρόλο

του παρατηρεί ή / και μετρά τα αποτελέσματα των εργασιών ή / και τα αποτελέσματα που παράγονται από τις υπηρεσίες του ενοποιημένου συστήματος ΜΥΡΙΩΠΟΣ.

Λαμβάνοντας υπόψη αυτούς τους τύπους αλληλεπιδράσεων και τις ομάδες-στόχους των ιδιωτικών επιχειρήσεων ως τους κύριους φορείς και δικαιούχους των υπηρεσιών ασφαλείας του ΜΥΡΙΩΠΟΣ, αυτές μπορούν να αλληλοεπιδράσουν με τη λύση ΜΥΡΙΩΠΟΣ μέσω των ακόλουθων ρόλων:

- Οι **ιδιωτικές επιχειρήσεις και πάροχοι υποδομών** παρέχουν πληροφορίες σχετικά με τα περιουσιακά στοιχεία του δικτύου τους (υλικό / λογισμικό / εταιρικά δεδομένα / λογαριασμοί χρηστών), καθώς και του περιβάλλοντος του δικτύου.
- Ο **υπεύθυνος ασφαλείας** υπολογίζει τη βέλτιστη πολιτική ασφάλειας (υπηρεσίες / λογισμικό ασφάλειας, κανόνες και βέλτιστες διαμορφώσεις).
- Ο **διαχειριστής συστήματος και εγκατάστασης** εγκαθιστά τις κατάλληλες υπηρεσίες (Επόπτες παρακολούθησης σε συσκευές άκρου και κεντρικές υποδομές, τείχη προστασίας, κ.λπ.).
- Ο **τελικός χρήστης / πελάτης** έχει πρόσβαση σε διάφορες πληροφορίες σχετικά με την ασφάλεια μέσω της κεντρικής διεπαφής χρήστη και των αναφορών ποσοτικοποίησης.

Στην περίπτωση αυτή, οι πελάτες των επιχειρήσεων και των οργανισμών έχουν πρόσβαση σε:

- Όλες οι λειτουργίες, την κεντρική διεπαφή και τις μεθόδους ΜΥΡΙΩΠΟΣ.
- Στις διάφορες υπηρεσίες ασφάλειας που παρέχονται μέσω της λύσης ΜΥΡΙΩΠΟΣ.

3.3 Λειτουργικές Απαιτήσεις και Τεχνικές Προδιαγραφές ΜΥΡΙΩΠΟΥ

Η παρούσα ενότητα συγκεντρώνει το σύνολο των λειτουργικών απαιτήσεων του ΜΥΡΙΩΠΟΣ με σκοπό την ενίσχυση της κυβερνοασφάλειας ενός επιχειρηματικού οικοσυστήματος, επιτρέποντας στους χρήστες να παρακολουθούν, αξιολογούν και να διαχειρίζονται δυναμικά τους κινδύνους. Ο απώτερος στόχος είναι να δοθεί η δυνατότητα στις επιχειρήσεις με υποδομές υπολογιστικού νέφους, να αυξήσουν την εκπαίδευση και ευαισθητοποίησή τους στον τομέα της κυβερνοασφάλειας μέσω της αποτελεσματικής συγκέντρωσης και επεξεργασίας ετερογενών ροών πληροφορίας, που συλλέγονται από εγκατεστημένους και κατανεμημένους Επόπτες και γίνονται αποτέλεσμα επεξεργασίας σε πραγματικό χρόνο προσφέροντας αυξημένα επίπεδα προστασίας. Οι απαιτήσεις αυτές ομαδοποιούνται ανά κατηγορία των βασικών λειτουργιών και υπηρεσιών και βρίσκονται σε συμφωνία με τους στόχους του έργου ΜΥΡΙΩΠΟΣ στους ακόλουθους τομείς: **διαχείριση της ασφάλειας δικτύων, δυναμική αξιολόγηση κινδύνων και λήψη αποφάσεων σε πραγματικό χρόνο, καθώς και ενισχυμένη και υπεύθυνη ανταλλαγή τακτικών και πληροφορίας που σχετίζονται με επικείμενες απειλές.**

Σε αυτό το πλαίσιο, το ΜΥΡΙΩΠΟΣ θα διερευνήσει την υιοθέτηση βασικών τεχνολογιών στην **ασφάλεια συσκευών και υπηρεσιών άκρου μέσω εγκατάστασης εποπτών παρακολούθησης κίνησης και υφιστάμενων υπηρεσιών νέφους.** Οι Επόπτες στο άκρο και στην κεντρική υποδομή θα **ενορχηστρώνονται και θα ενοποιούνται από έναν έξυπνο ενορχηστρωτή ο οποίος με βάση την κατηγορία των καταγραφών** (π.χ. ποσοτικοποιημένες σε μια κλίμακα χαμηλού ως υψηλού κινδύνου) **θα εφαρμόζει τις αντίστοιχες πολιτικές καταστολής και αντιμετώπισης** (π.χ. από τερματισμό λειτουργίας, επανεκκίνησης, απόρριψη

πακέτων δεδομένων, έως αντιγραφή κίνησης για περεταίρω επεξεργασία, κ.α.). Το σύστημα ΜΥΡΙΩΠΟΣ **θα υιοθετήσει αλγόριθμους κατανεμημένης βαθιάς μηχανικής μάθησης και νοημοσύνης μέσω κατηγοριοποίησης κυβερνο-απειλών με σκοπό την εξαγωγή συμπερασμάτων και την αυτοματοποιημένη λήψη αποφάσεων.** Οι πληροφορίες προέρχονται από την **παρακολούθηση και την καταγραφή κίνησης και ενεργειών που εκτελείται από τους Επόπτες, την ανάλυση και εμπλουτισμό της πληροφορίας,** με πληροφορίες για ευπάθειες στις τρέχουσες ροές εργασιών, εγκατεστημένου λογισμικού και υπηρεσιών, ελέγχου φόρτου εργασίας και διεργασιών που οδηγούνται σε λιμοκτονία (starvation), ασφάλειας περιβάλλοντος, συμπεριφορικών προτύπων κατά της σύνδεση με υφιστάμενα συστήματα (π.χ. ώρες της ημέρας, προσπάθειες αποτυχημένης / πετυχημένης εισόδου, αλλαγή κωδικών, κτλ.). Όλες αυτές οι λειτουργίες θα υλοποιηθούν μέσω της ανάπτυξης **προγραμματιζόμενων μηχανισμών που αλληλεπιδρούν με τους Επόπτες για την ασφαλή παρακολούθηση, συλλογή, συγκέντρωση, επεξεργασία, επαύξηση και υπολογισμό τέτοιων ετερογενών ροών πληροφοριών.** Το παρών παραδοτέο συγκεντρώνει ένα βασικό σύνολο τεχνικών απαιτήσεων που πρέπει να πληροί η λύση ΜΥΡΙΩΠΟΣ. Οι πίνακες που ακολουθούν παρουσιάζουν την αντιστοίχιση μεταξύ των απαιτήσεων, των χρηστών και το σκοπό που εκπληρώνουν. Παράλληλα, παρέχεται σύντομη περιγραφή κάθε λειτουργικής απαίτησης.

Πίνακας 2. Γενικές Λειτουργικές και Τεχνικές Απαιτήσεις

Α/Α	**ΑΠ1 (Υποχρεωτικό)**
Τίτλος	**Επεξεργασία ετερογενών ροών πληροφοριών (Στόχος 1)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Το ΜΥΡΙΩΠΟΣ πρέπει να **επεξεργάζεται και να αναλύει ετερογενείς ροές πληροφοριών σε διαφορετικά επίπεδα** (π.χ. επίπεδο συσκευής, δικτύου και εφαρμογής) και σε διαφορετικές μορφές (π.χ. CSV, JSON, PCAP αρχεία, αρχεία καταγραφής εφαρμογών και συστημάτων). **Αυτό καθιστά δυνατή την προηγμένη ανίχνευση εισβολών σε πραγματικό χρόνο, την ταξινόμηση ροών και τον εντοπισμό κακόβουλης συμπεριφοράς** και θα επιτρέψει την ακριβέστερη ανίχνευση παραβιάσεων της ασφάλειας και τη μείωση του αριθμού των ψευδώς θετικών αποτελεσμάτων. Η καταγραφή κίνησης και η επεξεργασία θα πραγματοποιείται από αναπτυγμένους και έξυπνους Επόπτες και ανιχνευτές ασφαλείας, οι οποίοι θα μπορούν να διεξάγουν πολυεπίπεδη λεπτομερή παρακολούθηση και ανίχνευση.

Α/Α	**ΑΠ2 (Υποχρεωτικό)**
Τίτλος	**Ανταλλαγή πληροφοριών για την ασφάλεια στον κυβερνοχώρο (Στόχος 3)**
Ρόλος χρήστη	Υπεύθυνος ασφαλείας
Περιγραφή	Η ανταλλαγή πληροφοριών για την ασφάλεια στον κυβερνοχώρο θα βελτιώσει τη συνεργασία και θα αυξήσει την έγκαιρη ενημέρωση για την κατάσταση κινδύνου και κυβερνοαπειλών.

Α/Α	ΑΠ3 (Υποχρεωτικό)
Τίτλος	**Ημιαυτόματη απάντηση σε επιθέσεις και ενέργειες μετριασμού (Στόχος 2 & 3)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Υπεύθυνος ασφαλείας Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Το ΜΥΡΙΩΠΟΣ θα πρέπει να διευκολύνει την έγκαιρη και αποτελεσματική αντιμετώπιση περιστατικών. Το περιστατικό πρέπει να αξιολογηθεί για να προσδιοριστεί η σημαντικότητα του. Το ΜΥΡΙΩΠΟΣ θα συμπεραίνει έναν (κατά το δυνατόν) αυτοματοποιημένο τρόπο υπολογισμού των αλυσιδωτών επιπτώσεων σε περίπτωση παραβίασης κάποιου περιουσιακού στοιχείου.

Α/Α	ΑΠ4 (Υποχρεωτικό)
Τίτλος	**Παροχή ειδοποιήσεων κυβερνοασφάλειας σε πραγματικό χρόνο (Στόχος 3)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Υπεύθυνος ασφαλείας Διαχειριστής συστήματος και εγκατάστασης Τελικός χρήστης / πελάτης
Περιγραφή	Για να είναι σε θέση να ανταποκριθούν στις επιθέσεις, **θα πρέπει να δημιουργούνται ειδοποιήσεις / συναγερμοί ασφαλείας που θα παρέχουν τις πληροφορίες που απαιτούνται για τον ημιαυτόματο καθώς και αυτόματο μετριασμό και την πρόληψη των επιθέσεων στον κυβερνοχώρο.** Ο χρόνος απόκρισης σε περιστατικά είναι συχνά κρίσιμος παράγοντας και απαιτούνται άμεσες ειδοποιήσεις που περιλαμβάνουν όλες τις απαραίτητες πληροφορίες για την αποτελεσματική απόκριση.

Α/Α	ΑΠ5 (Υποχρεωτικό)
Τίτλος	**Υπηρεσίες για προστασία από ύποπτη / κακόβουλη συμπεριφορά δικτύου (Στόχος 1)**
Ρόλος χρήστη	Υπεύθυνος ασφαλείας Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Θα πρέπει να παρέχονται υπηρεσίες για την προστασία του δικτύου του οργανισμού. Αυτό θα εξασφαλίσει την προστασία του δικτύου σε θεμελιώδες επίπεδο. Η απαίτηση αυτή περιλαμβάνει τις ακόλουθες υπηρεσίες που μπορεί να παρέχονται από το ΜΥΡΙΩΠΟΣ: • Τείχος προστασίας και Τείχος προστασίας εφαρμογών ιστού • Σύστημα ανίχνευσης / πρόληψης εισβολών Ως σημείο εκκίνησης, οι υπηρεσίες προστασίας του δικτύου θα πρέπει να **βασίζονται σε ευρετικούς κανόνες** που αντιστοιχούν σε κακόβουλη συμπεριφορά. **Τα δεδομένα**

	εισόδου σε αυτές τις υπηρεσίες παρέχονται από τους Επόπτες παρακολούθησης του συστήματος ΜΥΡΙΩΠΟΣ. Επιπλέον, οι υπηρεσίες αυτές θα πρέπει να ενισχύονται από τους μηχανισμούς τεχνητής νοημοσύνης και βαθιάς μηχανικής μάθησης που εκπαιδεύονται στο υπολογιστικό νέφος. Αυτό θα οδηγήσει σε σημαντικά πιο εξελιγμένες λύσεις που θα μπορούν να αναλύουν, να ανιχνεύουν και να αναγνωρίζουν τα πρότυπα πιο σύνθετων ύποπτων και δυνητικά κακόβουλων συμπεριφορών.

Α/Α	**ΑΠ6 (Υποχρεωτικό)**
Τίτλος	**Υπηρεσίες Κατανεμημένης Ευφυίας Ιστού & Σκοτεινού Δικτύου (Στόχος 1 & 2)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Διαχειριστής συστήματος και εγκατάστασης Τελικός χρήστης / πελάτης
Περιγραφή	Το ΜΥΡΙΩΠΟΣ θα αναζητεί πληροφορίες που σχετίζονται με ζητήματα κυβερνοασφάλειας στο σκοτεινό δίκτυο. Στις υπηρεσίες αυτές συμπεριλαμβάνεται η συλλογή και αποθήκευση ετερογενών σχετικών ροών δεδομένων που σχετίζονται με το υποκείμενο στοχευμένο επιχειρηματικό οικοσύστημα (emails, εταιρικά δεδομένα για υποκλοπής τους). Οι λειτουργίες αυτές περιλαμβάνουν: ● Πολύτροπη Ειδοποίηση ● Εξαγωγή Γνώσης από Ιστό & Σκοτεινό Δίκτυο ● Διαδικτυακή Ανίχνευση & Συλλογή Αποδείξεων ● Μηχανική & Βαθιά Μάθηση σε Μη Αξιόπιστα Δεδομένα από το Σκοτεινό Δίκτυο ● Στατιστική Πραγματικού Χρόνου

3.3.1 Επόπτες Καταγραφής, Αναζήτησης και Επεξεργασίας Δεδομένων

Πίνακας 3. Απαιτήσεις Πρακτόρων

Α/Α	**ΑΠ7 (Υποχρεωτικό)**
Τίτλος	**Ανατροφοδότηση σχετικά με τη συλλογική πληροφόρηση για απειλές (Στόχος 1, 2 & 3)**
Ρόλος χρήστη	Υπεύθυνος ασφαλείας Διαχειριστής συστήματος και εγκατάστασης

Περιγραφή	Οι υπηρεσίες ΜΥΡΙΩΠΟΣ θα πρέπει να επιτρέπουν στους προηγμένους χρήστες να παρέχουν ανατροφοδότηση σχετικά με την ποιότητα των πληροφοριών που ανακτώνται. Για παράδειγμα, οι ειδοποιήσεις παραβίασης και οι σχετικές πληροφορίες που εμφανίζονται στην κεντρική διεπαφή χρήστη θα μπορούσαν να κατηγοριοποιηθούν ως χρήσιμες, εσφαλμένες (δηλ. ψευδείς συναγερμοί) ή ελλιπείς (δηλ. λείπουν σημαντικά στοιχεία) μαζί με το επίπεδο εμπιστοσύνης τους. **Η ανταλλαγή αυτών των πληροφοριών μπορεί να είναι ζωτικής σημασίας για την αξιολόγηση της αξιοπιστίας και της καταλληλότητας των ψευδώς θετικών ειδοποιήσεων.**

Α/Α	**ΑΠ8 (Υποχρεωτικό)**
Τίτλος	**Προγραμματισμός Πρακτόρων (Στόχος 2 & 3)**
Ρόλος χρήστη	Υπεύθυνος ασφαλείας Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Το σύστημα ΜΥΡΙΩΠΟΣ πρέπει να είναι ευέλικτο ώστε να υποστηρίζει διαφορετικά σενάρια, καθώς και να μπορεί να αντιμετωπίσει και να ανιχνεύσει ένα ευρύ φάσμα πιθανών τύπων επίθεσης. **Αυτό απαιτεί την ανάπτυξη προγραμματιζόμενων πρακτόρων παρακολούθησης και ανάλυσης κίνησης που μπορούν να διαμορφώνονται και να ενημερώνονται κατά τη διάρκεια της εκτέλεσης**. Οι Επόπτες πρέπει να είναι σε θέση να προσαρμόζουν (κατά τον χρόνο εκτέλεσης) τις διαδικασίες παρακολούθησης και επιθεώρησης στις τρέχουσες ανάγκες ανίχνευσης, αποθήκευσης και μετάδοσης. Για παράδειγμα, όταν εντοπίζονται πρώιμα σημάδια επιθέσεων ή ανακαλύπτονται νέες απειλές, μπορεί να είναι απαραίτητη η ανάλυση λεπτομερέστερων πληροφοριών από ό,τι κατά τη διάρκεια της κανονικής λειτουργίας. Οι λεπτομερέστερες πληροφορίες μπορεί να συνίστανται σε συχνότερες τιμές δειγματοληψίας ή σε πρόσθετα δεδομένα παρακολούθησης (για παράδειγμα, στην περίπτωση πακέτων δικτύου μπορεί να ελέγχονται τα επιμέρους πρωτοκόλλα εκτός από τις τυπικές επικεφαλίδες TCP/IP). Ο προγραμματισμός πρακτόρων αναμένεται να υποστηρίζει τα ακόλουθα χαρακτηριστικά: ➢ Να διαχειρίζεται τη διαμόρφωση των τοπικών εποπτών παρακολούθησης. ➢ Να εισάγει απλά προγράμματα επεξεργασίας σε τοπικούς Επόπτες ασφαλείας για παρακολούθηση, επιθεώρηση, συγχώνευση δεδομένων, συνάθροιση και φιλτράρισμα. ➢ Να υποστηρίζει κάποιο είδος προσαρμοστικής παρακολούθησης, το οποίο επιτρέπει την παρακολούθηση σε καθολικό επίπεδο (αλλά με αποδοτική χρήση της CPU) είτε τη δυνατότητα να γίνεται μια πιο λεπτομερής παρακολούθηση όταν εντοπίζονται κάποια ύποπτα συμβάντα μόνο όταν αυτό είναι πραγματικά απαραίτητο. Συνολικά, για να λειτουργήσει αξιόπιστα το ΜΥΡΙΩΠΟΣ, πρέπει να είναι ικανό να παρακολουθεί ένα ευρύ φάσμα στοιχείων, όπως πρωτόκολλα δικτύου, λειτουργικά

	συστήματα, εφαρμογές, υπηρεσίες, διακομιστές ιστού, ενδιάμεσο λογισμικό, κ.λπ., και όλα αυτά καταναλώνοντας όσο το δυνατόν λιγότερους πόρους.

Α/Α	**ΑΠ9 (Υποχρεωτικό)**
Τίτλος	**Βελτιστοποίηση της παρακολούθησης και της επεξεργασίας με βάση προγραμματιζόμενους μηχανισμούς ασφάλειας δικτύου και επιτάχυνση υλικού (π.χ. προγραμματιζόμενο μονοπάτι δεδομένων) (Στόχος 1 & 2)**
Ρόλος χρήστη	Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Θα πρέπει να εξεταστούν νέοι μηχανισμοί βελτιστοποίησης για τη βελτίωση της απόδοσης και της αποτελεσματικότητας της παρακολούθησης της κίνησης στο δίκτυο σε θέματα ασφάλειας και επεξεργασίας δεδομένων συσκευής και εκτέλεσης σε πραγματικό χρόνο. Αυτές οι λειτουργίες ανίχνευσης θα είναι πλήρως προγραμματιζόμενες, επιτρέποντας την προτεραιοποίηση προς τη δυναμική προσαρμογή της ανίχνευσης.

Α/Α	**ΑΠ10 (Υποχρεωτικό)**
Τίτλος	**Βελτιστοποίηση της παρακολούθησης και της επεξεργασίας στο άκρο (Στόχος 1 & 2)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Η βελτιστοποίηση των λειτουργιών ασφαλείας πρέπει να εξετάζει την κατανομή της επεξεργασίας στις συσκευές άκρου, ώστε να αποφεύγεται η αποκλειστικά συγκεντρωτική ανάλυση σε αυτές. Επιπλέον, η από άκρη σε άκρη ασφάλεια απαιτεί παρακολούθηση και εντοπισμό περιστατικών ασφαλείας σε επίπεδο άκρου.

Α/Α	**ΑΠ11 (Υποχρεωτικό)**
Τίτλος	**Βελτιστοποίηση της παρακολούθησης και της επεξεργασίας με βάση τις υπηρεσίες νέφους και τη σύνθεση υπηρεσιών (Στόχος 1 & 2)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Για να βελτιωθεί η δυναμική και η απόδοση των λειτουργιών ασφαλείας σε εικονικά περιβάλλοντα, πρέπει να αναπτυχθούν και να συνδυαστούν τόσο κεντρικά όσο και τοπικά στοιχεία υπηρεσιών (π.χ. με τη μορφή πρακτόρων που παρακολουθούν υπηρεσίες νέφους ή με τη χρήση σύνθεσης υπηρεσιών).

Α/Α	ΑΠ12 (Υποχρεωτικό)
Τίτλος	**Μηχανισμοί αντιμετώπισης παραβιάσεων ασφαλείας (Στόχος 1, 2 & 3)**
Ρόλος χρήστη	Υπεύθυνος ασφαλείας
Περιγραφή	Οι υπηρεσίες ΜΥΡΙΩΠΟΣ θα πρέπει να περιλαμβάνουν ταχείς και αξιόπιστους μηχανισμούς αντιμετώπισης παραβιάσεων ασφάλειας, οι οποίοι θα παρέχουν αποτελεσματικά βήματα προς την αποκατάσταση της παραβίασης. Πιο συγκεκριμένα, σκοπός των μηχανισμών αυτών είναι να παρέχουν: • Όλες τις πληροφορίες που είναι απαραίτητες για την ορθή και πλήρη κατανόηση της παραβίασης της ασφάλειας (ακολουθούμενη πορεία επίθεσης, πληροφορίες/στοιχεία/συσκευές που έχουν παραβιαστεί). • Όλες τις απαραίτητες πληροφορίες σε πραγματικό ή σχεδόν πραγματικό χρόνο. • Προτάσεις για το περιστατικό ασφαλείας. Οι Επόπτες παρακολούθησης του συστήματος ΜΥΡΙΩΠΟΣ θα πρέπει να παρέχουν τα απαραίτητα ακατέργαστα δεδομένα από τις συσκευές, τα οποία θα πρέπει να είναι επαρκή για να υποδεικνύουν την παραβίαση της ασφάλειας. Τα ακατέργαστα δεδομένα πρέπει να χρησιμοποιούνται από τις μηχανές ανάλυσης του συστήματος ΜΥΡΙΩΠΟΣ προκειμένου να υποδεικνύουν τυχόν παραβιάσεις ασφαλείας που είναι πιο δύσκολο να εντοπιστούν. Επιπλέον, θα πρέπει να παρέχονται έγκαιρες προειδοποιήσεις σχετικά με δυνητικά επερχόμενες απειλές.

Α/Α	ΑΠ13 (Υποχρεωτικό)
Τίτλος	**Ειδοποίηση για συμβάντα ασφαλείας (Στόχος 3)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Υπεύθυνος ασφαλείας Διαχειριστής συστήματος και εγκατάστασης Τελικός χρήστης / πελάτης
Περιγραφή	Η διεπαφή χρήστη είναι υπεύθυνη για την αναφορά της τρέχουσας κατάστασης του συστήματος και των παρεχόμενων γραφημάτων ασφαλείας. **Για το λόγο αυτό, θα παρέχει ένα μεγάλο σύνολο οπτικών στοιχείων (π.χ. ανάλυση χρονοσειρών, γράφημα δικτύου, κυκλικά διαγράμματα, κ.λπ.) για την εμφάνιση πληροφοριών σχετικά με τις ευπάθειες, τους εντοπισμένους κινδύνους, τα μοτίβα επιθέσεων και τις απειλές.** Επιπλέον, θα πρέπει να επιτρέπει στους χρήστες να αναλαμβάνουν δράση και να αντιδρούν σε κάθε εντοπισμένη ευπάθεια ή εξωτερική ένδειξη παραβίασης, ρυθμίζοντας τα στοιχεία του συστήματός τους αποδεχόμενοι / απορρίπτοντας τις συστάσεις που δίνονται από το ΜΥΡΙΩΠΟΣ. Μέσω της διεπαφής χρήστη και με τη χρήση του κατάλληλου πίνακα ελέγχου θα πρέπει επίσης να δίνεται η δυνατότητα στους χρήστες να μπορούν να εξατομικεύουν τον πίνακα ελέγχου προσθέτοντας, αφαιρώντας και μετακινώντας παράθυρα ανάλογα

	με το ρόλο τους και την εκάστοτε εργασία. Επιπλέον, θα πρέπει να μπορούν να χειρίζονται τα οπτικά στοιχεία, π.χ. μετακίνηση, αλλαγή μεγέθους, μεγέθυνση / σμίκρυνση, κ.λπ. Άλλες λειτουργίες θα πρέπει επίσης να περιλαμβάνουν: ➢ **Διαδραστικές προβολές:** Ο πίνακας ελέγχου θα πρέπει να συλλέγει και να παρουσιάζει στοιχεία ιστορικά καθώς και πραγματικού χρόνου που σχετίζονται με την ασφάλεια. ➢ **Φιλτράρισμα πληροφοριών:** Ο πίνακας ελέγχου θα πρέπει να επιτρέπει στους χρήστες να μειώνουν τον όγκο των δεδομένων που παρουσιάζονται και να περιορίζουν την ανάλυση σε συγκεκριμένο τμήμα του συστήματος, χρονικό παράθυρο, τύπο απειλής, πηγή πληροφοριών, κ.λπ. ➢ **Αναζήτηση πληροφοριών:** Ο πίνακας ελέγχου θα πρέπει να επιτρέπει στους χρήστες να βρίσκουν συγκεκριμένες πληροφορίες αναζητώντας μια συγκεκριμένη λέξη-κλειδί ή όρο σε τμήμα κειμένου. ➢ **Σύγκριση πληροφοριών:** Ο πίνακας ελέγχου θα πρέπει να επιτρέπει στους χρήστες να συγκρίνουν πληροφορίες σχετικά με το σύστημα σε διαφορετικές χρονικές περιόδους, προκειμένου να εντοπίζουν / επιβεβαιώνουν τυχόν μοτίβα σε αυτά. ➢ **Δυνατότητες υποβολής αναφορών:** Ο πίνακας ελέγχου θα πρέπει να συντάσσει μια αναφορά σχετικά με την κατάσταση ασφάλειας του συστήματος, τις ευπάθειες που εντοπίστηκαν, τις απειλές και τους κινδύνους.

Α/Α	**ΑΠ14 (Επιθυμητό)**
Τίτλος	**Χρήση ανοικτών προγραμματιστικών διεπαφών (APIs) (Στόχος 1 - 3)**
Ρόλος χρήστη	Διαχειριστής συστήματος και εγκατάστασης Τελικός χρήστης / πελάτης
Περιγραφή	Η χρήση ανοικτού API με βάση τα εκάστοτε πρότυπα ασφαλείας διευκολύνει: ➢ Τους παρόχους τεχνολογίας ως τελικούς χρήστες του συστήματος ΜΥΡΙΩΠΟΣ που θέλουν να ενσωματώσουν τα εργαλεία τους με τις υπάρχουσες υπηρεσίες. ➢ Τους τελικούς χρήστες των οργανισμών που θέλουν να χρησιμοποιήσουν τις υπηρεσίες του ΜΥΡΙΩΠΟΣ. Προσφέρει ανοικτές προγραμματιστικές διεπαφές χωρίς τεχνικές ιδιαιτερότητες επιτρέποντας την κατανόηση των δυνατοτήτων της προσφερόμενης υπηρεσίας χωρίς την εξέταση του πηγαίου κώδικα της. Επιτρέπει επιπλέον την εξ αποστάσεως κατανόηση και αλληλεπίδραση με την υπηρεσία με ελάχιστη τεχνική εφαρμογή ή γνώση επάνω σε αυτή.

3.3.2 Απαιτήσεις Ασφάλειας

Πίνακας 4. Απαιτήσεις Ασφαλείας

Α/Α	**ΑΠ15 (Υποχρεωτικό)**
Τίτλος	**Έλεγχος πρόσβασης (Στόχος 4)**
Ρόλος χρήστη	Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Ο έλεγχος αφορά στη δυνατότητα πρόσβασης σε εξουσιοδοτημένα μέρη του συστήματος, και μόνο σε αυτά, με δικαιώματα πρόσβασης, ανάγνωσης, τροποποίησης και διαγραφής των πληροφοριών που λαμβάνονται, συλλέγονται ή παράγονται. Κατά τη λήψη ενός αιτήματος, η **μονάδα ελέγχου πρόσβασης θα καθορίσει αν ο εκάστοτε αιτών έχει πρόσβαση στα δεδομένα.** Συγκεκριμένα, αν είναι εξουσιοδοτημένος να υποβάλει αυτό το είδος αιτήματος, για αυτό το είδος και αυτόν τον όγκο δεδομένων, αυτή τη στιγμή, χρησιμοποιώντας το κανάλι επικοινωνίας μέσω του οποίου έφτασε το αίτημα. Αφού διαπιστώσει η εγκυρότητα του αιτήματος, **η μονάδα ελέγχου πρόσβασης καθορίζει το απαιτούμενο επίπεδο πρόσβασης (π.χ. ανάγνωση, τροποποίηση, διαγραφή, κ.α.) και δίνει εντολή στις σχετικές μονάδες του συστήματος να εκτελέσουν το αίτημα.**

Α/Α	**ΑΠ16 (Υποχρεωτικό)**
Τίτλος	**Απόρρητο χρήστη (Στόχος 4)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Διαχειριστής συστήματος και εγκατάστασης Τελικός χρήστης / πελάτης
Περιγραφή	Το ΜΥΡΙΩΠΟΣ απευθύνεται σε επιχειρηματικά οικοσυστήματα που μπορεί να περιλαμβάνουν πολλαπλούς χρήστες, διαχειριστές και πελάτες. Λόγω των διαφορετικών τύπων δεδομένων του κάθε οικοσυστήματος, επιβάλλεται η θέσπιση της κατάλληλης πολιτικής σχεδιασμού έτσι ώστε να διασφαλίζεται ότι μόνο **ηθικά αποδεκτά, νομικά επιτρεπόμενα και ελάχιστα απαιτούμενα δεδομένα συλλέγονται, υποβάλλονται σε επεξεργασία και διαδίδονται από το σύστημα ΜΥΡΙΩΠΟΣ** με απώτερο σκοπό τον εντοπισμού οποιασδήποτε παραβατικής πολιτικής και πιθανής ευπάθειας.

Α/Α	**ΑΠ17 (Υποχρεωτικό)**
Τίτλος	**Ασφαλή κανάλια επικοινωνίας (Στόχος 4)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Διαχειριστής συστήματος και εγκατάστασης Τελικός χρήστης / πελάτης

Περιγραφή	Το ΜΥΡΙΩΠΟΣ θα συλλέγει δεδομένα και μετρήσεις από εικονικές υπηρεσίες και συσκευές άκρου με **προγραμματιστικό τρόπο. Οι εικονικές υπηρεσίες εκτελούνται συνήθως σε απομονωμένα περιβάλλοντα και επιτρέπεται μόνο περιορισμένη πρόσβαση στις κύριες λειτουργίες.** Ο πάροχος υποδομών πρέπει να παρέχει ένα ασφαλές και αξιόπιστο κανάλι επικοινωνίας για τη σύνδεση των λειτουργικών στοιχείων του έργου και τον έλεγχό τους κατά το χρόνο εκτέλεσης. Το σύστημα ΜΥΡΙΩΠΟΣ πρέπει να είναι σε θέση να: ➢ Συλλέγει δεδομένα από κάθε τοπικό Επόπτη ασφαλείας. ➢ Να έχει πρόσβαση και να διαμορφώνει οποιοδήποτε τοπικό Επόπτη ασφαλείας ανεξάρτητα από την τοποθέτησή του στο γράφημα.

3.3.3 Απαιτήσεις Απορρήτου και Ακεραιότητας Δεδομένων

Πίνακας 5. Απαιτήσεις Απορρήτου και Ακεραιότητας Δεδομένων

Α/Α	**ΑΠ18 (Υποχρεωτικό)**
Τίτλος	**Εγγυήσεις ακεραιότητας και αυθεντικότητας δεδομένων (Στόχος 4)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Διαχειριστής συστήματος και εγκατάστασης Τελικός χρήστης / πελάτης
Περιγραφή	Η ακεραιότητα των δεδομένων (μερικές φορές ονομάζεται επίσης αυθεντικότητα των δεδομένων και δεν πρέπει να συγχέεται με την αυθεντικοποίηση του χρήστη). Επίσης αφορά στην εμπιστοσύνη ενός μέρους ότι τα δεδομένα που έλαβε ή παρείχε δεν τροποποιήθηκαν από μη εξουσιοδοτημένα μέρη. Η ακεραιότητα των δεδομένων θα διασφαλίζεται μέσω αποτελεσματικών μηχανισμών προσαρμοσμένων στον τύπο των παρακολουθούμενων δεδομένων, που προβλέπονται στα επιχειρηματικά οικοσυστήματα των εμπλεκόμενων μερών. Στο πλαίσιο αυτό, **θα πρέπει επίσης να παρέχεται ακεραιότητα και αυθεντικότητα όλων των ανταλλασσόμενων πληροφοριών (συμπεριλαμβανομένων των αρχείων καταγραφής των εφαρμογών, των πακέτων δικτύου καθώς και των πληροφοριών πιστοποίησης).**

Α/Α	**ΑΠ19 (Υποχρεωτικό)**
Τίτλος	**Ασφαλής παράδοση δεδομένων (Στόχος 4)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Διαχειριστής συστήματος και εγκατάστασης Τελικός χρήστης / πελάτης

Περιγραφή	Το σύστημα ΜΥΡΙΩΠΟΣ πρέπει να συλλέγει δεδομένα καταγραφής κίνησης και συμβάντων στο σκοτεινό δίκτυο και να τροφοδοτεί τον κεντρικό μηχανισμό ανίχνευσης εισβολών. Πολλαπλοί αλγόριθμοι θα αναπτυχθούν για την ανάλυση και τη συσχέτιση των δεδομένων, οπότε το σύστημα ΜΥΡΙΩΠΟΣ θα πρέπει να φροντίζει για την αποστολή του σωστού συνόλου δεδομένων σε καθέναν από τα επιμέρους συστήματα. Υπάρχουν δύο κύριες μέθοδοι παράδοσης που θα πρέπει να υποστηρίζονται από το πλαίσιο: ➢ **Πραγματικός χρόνος:** τα δεδομένα παραδίδονται σε πραγματικό χρόνο, αφού έχουν πιστοποιηθεί. Αυτό επιτρέπει τη συλλογή δεδομένων των οποίων η ακεραιότητα έχει επαληθευτεί, ενώ παράλληλα υποστηρίζεται μειωμένη καθυστέρηση και επιβάρυνση των αλγορίθμων κατά την ανάκτηση δεδομένων. ➢ **Ιστορικά:** τα δεδομένα αποθηκεύονται στη σταθερή μονάδα αποθήκευσης. Η μέθοδος αυτή προσφέρει τη δυνατότητα για περαιτέρω ανάλυση, διερεύνηση και εντοπισμό πιθανών μοτίβων επιθέσεων.

3.3.4 Εκτίμηση Κινδύνων και Επιβολή Πολιτικών

Πίνακας 6. Απαιτήσεις Εκτίμησης Κινδύνου

Α/Α	**ΑΠ20 (Υποχρεωτικό)**
Τίτλος	**Δυνατότητα επιβολής πολιτικών μέσω της έκφρασης πολιτικών ασφάλειας, εμπιστοσύνης και επιχειρησιακής διασφάλισης (Στόχος 3)**
Ρόλος χρήστη	Διαχειριστής συστήματος και εγκατάστασης

Περιγραφή	Ο διαχειριστής θα πρέπει να είναι σε θέση να εκφράζει πολιτικές που ρυθμίζουν τη λειτουργική συμπεριφορά του ΜΥΡΙΩΠΟΣ και να διασφαλίζει τη σωστή εκτέλεση και την ανταλλαγή δεδομένων κατά τη διάρκεια εκτέλεσης. Αυτό θα επιτευχθεί μέσω του ορισμού ενός μέτα-μοντέλου πολιτικής που διευκολύνει την έκφραση των στόχων ασφαλείας και την επιβολή μέτρων μέσω **των πρακτόρων και του ενορχηστρωτή ασφάλειας**. Ο ορισμός της πολιτικής θα αποτελεί μέρος του πλαισίου αξιολόγησης κινδύνων και θα απαιτεί τη συμμετοχή του διαχειριστή, ο οποίος θα είναι σε θέση να λάβει τεκμηριωμένες αποφάσεις για τις πολιτικές που θα επιβληθούν με βάση τα αποτελέσματα της αξιολόγησης κινδύνων. Οι πολιτικές ασφαλείας αντικατοπτρίζουν ουσιαστικά το σύνολο των ιδιοτήτων διαμόρφωσης και συμπεριφοράς που πρέπει να πιστοποιούνται και να επαληθεύονται κατά τη διάρκεια του χρόνου εκτέλεσης. Είναι αναγκαίο να είναι δυνατή η έκφραση πολιτικών που: (i) όταν επιβάλλονται, μετριάζουν τους κρίσιμους κινδύνους που σχετίζονται με την ασφάλεια και την προστασία των εκάστοτε συστημάτων που επιθυμούν να συνθέσουν, (ii) λαμβάνουν υπόψη ιδιότητες που μπορούν να διασφαλιστούν από τα ενσωματωμένα στοιχεία με περιορισμένους πόρους, (iii) διασφαλίζουν την ιδιωτικότητα των συσκευών που πιστοποιούν, καθορίζοντας τις γενικές αρχές για την προστασία των δεδομένων πιστοποίησης, και (iv) καθορίζουν τον τύπο των αποδεικτικών στοιχείων που πρέπει να συλλέγονται από ένα σύστημα, σε περίπτωση που αυτό δεν πιστοποιεί ορισμένες από τις ιδιότητές του. Οι **καθορισμένες πολιτικές πρέπει να είναι ξεκάθαρες και εφαρμόσιμες ώστε να μπορούν να ενημερώνονται δυναμικά και να προσαρμόζονται στους διάφορους τύπους ευπαθειών**.

3.3.5 Ενορχήστρωση Υπηρεσιών και Εφαρμογή Πολιτικών Ασφαλείας

Πίνακας 7. Απαιτήσεις Ενορχήστρωσης και Εφαρμογής Πολιτικών Ασφαλείας

Α/Α	**ΑΠ21 (Υποχρεωτικό)**
Τίτλος	**Εργαλεία ενορχήστρωσης (Στόχος 3 & 4)**
Ρόλος χρήστη	Υπεύθυνος ασφαλείας Διαχειριστής συστήματος και εγκατάστασης

Περιγραφή	**Ο ΜΥΡΙΩΠΟΣ θα υιοθετήσει εργαλεία ενορχήστρωσης για τις λειτουργίες διαχείρισης.** Τα εν λόγω εργαλεία πρέπει να είναι σε θέση να εκτελούν ενέργειες διαχείρισης του κύκλου ζωής των αναπτυγμένων υπηρεσιών, καθώς και να αναφέρουν την τρέχουσα τοπολογία και θέση των υπηρεσιών. Η υιοθέτηση ενός αφηρημένου επιπέδου είναι προτιμότερη για τη σωστή διαχείριση των ακόλουθων λειτουργιών: ➢ **Παροχή υπηρεσιών ισχυρής αυθεντικοποίησης, εξουσιοδότησης και διαχείρισης πολιτικών ελέγχου πρόσβασης.** Ο χρήστης θα πρέπει να χρησιμοποιεί ένα ολοκληρωμένο στοιχείο ελέγχου πρόσβασης βάσει ρόλων (RBAC) που αντιστοιχίζει έναν εισερχόμενο χρήστη ή μια ομάδα σε ένα σύνολο δικαιωμάτων που είναι συγκεντρωμένα στους αντίστοιχους ρόλους. ➢ **Παροχή αυτοματοποιημένων ιεραρχικών πιστοποιητικών.** Οι συσκευές άκρου θα πρέπει να ρυθμίζονται έτσι ώστε να μην μοιράζονται έμπιστες πληροφορίες με άλλους κόμβους και αντίστοιχους φόρτους εργασίας.

Α/Α	**ΑΠ22 (Υποχρεωτικό)**
Τίτλος	**Ασφαλής πρόσβαση σε υπολογιστικούς κόμβους (Στόχος 3 & 4)**
Ρόλος χρήστη	Υπεύθυνος ασφαλείας Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Οι κόμβοι θα πρέπει να ρυθμιστούν ώστε να δέχονται συνδέσεις από τον ενορχηστρωτή ασφαλείας των υπηρεσιών ελέγχου στις καθορισμένες θύρες και να δέχονται συνδέσεις για τις εκάστοτε υπηρεσίες. Εάν είναι δυνατόν, οι κόμβοι αυτοί δεν θα πρέπει να εκτίθενται εξ ολοκλήρου στο δημόσιο διαδίκτυο.

Α/Α	**ΑΠ23 (Υποχρεωτικό)**
Τίτλος	**Ανάπτυξη εποπτών ασφαλείας και ασφαλής παρακολούθηση (Στόχος 3 & 4)**
Ρόλος χρήστη	Υπεύθυνος ασφαλείας Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Όπως προαναφέρθηκε, ο ενορχηστρωτής ασφάλειας είναι υπεύθυνος (μεταξύ άλλων) για τη διαχείριση των υπηρεσιών. Οι Επόπτες ασφαλείας πρέπει να συνδεθούν εικονικά και να παρακολουθούν τις υπηρεσίες και συσκευές του επιχειρηματικού οικοσυστήματος-στόχου, ώστε να μπορούν να αναλυθούν περεταίρω οι διάφορες ροές πληροφοριών. Η λειτουργία αυτή θα πραγματοποιηθεί από τον ενορχηστρωτή, ανάλογα με τον συγκεκριμένο φορμαλισμό που θα χρησιμοποιήσει το εργαλείο ενορχήστρωσης. Τέλος, οι Επόπτες ασφαλείας μπορούν να απενεργοποιηθούν προσωρινά κατόπιν συγκεκριμένου αιτήματος από τον διαχειριστή συστήματος του ΜΥΡΙΩΠΟΣ, π.χ. για εξοικονόμηση πόρων, εάν αυτό κρίνεται σημαντικό. Επιπλέον, το σύστημα ΜΥΡΙΩΠΟΣ θα πρέπει να υποστηρίζει τον ορισμό εργασιών παρακολούθησης και ανάλυσης κατά τον χρόνο εκτέλεσης, δημιουργώντας και φορτώνοντας δυναμικά νέες διεργασίες επεξεργασίας. Το πρόσθετο λογισμικό που βρίσκεται μαζί με τις εικονικές λειτουργίες και συσκευές, που αποτελούν το επιχειρηματικό οικοσύστημα, δεν πρέπει να εισάγει ευπάθειες σε ολόκληρη την

	υπηρεσία. Επιπλέον, ο αριθμός των τοπικών πρακτόρων πρέπει να είναι όσο το δυνατόν μικρότερος και η υλοποίησή τους όσο το δυνατόν απλούστερη.

Α/Α	**ΑΠ24 (Επιθυμητό)**
Τίτλος	**Επεκτάσιμοι αλγόριθμοι ανίχνευσης και ανάλυσης (Στόχος 3 & 4)**
Ρόλος χρήστη	Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών Διαχειριστής συστήματος και εγκατάστασης
Περιγραφή	Το ΜΥΡΙΩΠΟΣ σχεδιάζει ένα ευέλικτο σύστημα που μπορεί να χρησιμοποιηθεί για οποιαδήποτε εικονική υπηρεσία (που λειτουργεί σε ένα επιχειρηματικό οικοσύστημα). Ο προγραμματισμός των μηχανισμών του ΜΥΡΙΩΠΟΥ θα προσαρμόζει το βάθος του ελέγχου ανάλογα με τις πραγματικές ανάγκες. Για το λόγο αυτό, η ποσότητα των πληροφοριών μπορεί να ποικίλλει σε ένα ευρύ φάσμα, ανάλογα με τον αριθμό των εικονικών λειτουργιών και τον τρέχοντα φόρτο εργασίας. Συνεπώς, είναι δύσκολο να **κατανεμηθούν εκ των προτέρων υπολογιστικοί πόροι για την ανάλυση και την ανίχνευση.** Οι προγραμματιστές εφαρμογών κυβερνοασφάλειας καλούνται να **αναπτύξουν κλιμακούμενους αλγορίθμους, οι οποίοι μπορούν εύκολα να εκτελεστούν με κατανεμημένο ή παράλληλο τρόπο ανάλογα με την ποσότητα των πληροφοριών που πρέπει να επεξεργαστούν, χωρίς την εκ των προτέρων ανάγκη κατανομής πόρων**.

3.4 Μη Λειτουργικές Απαιτήσεις

Οι πίνακες που ακολουθούν δημιουργούν μια συγκεκριμένη αντιστοίχιση μεταξύ των βασικών χαρακτηριστικών του συστήματος του ΜΥΡΙΩΠΟΥ με το μοντέλο ποιότητας υπηρεσίας που θέλουμε να πετύχουμε. Επομένως, κάθε τεχνική ή λειτουργική απαίτηση θα ελέγχεται ώστε να πληροί και τις αντίστοιχες ποιοτικές απαιτήσεις, ως ακολούθως.

Πίνακας 8. Μη Λειτουργικές Απαιτήσεις

Α/Α	**ΜΑΠ1**
Τίτλος	**Αποδοτικότητα (Στόχος 1 - 4)**
Περιγραφή	Αυτό το χαρακτηριστικό αντιπροσωπεύει την απόδοση σε σχέση με την ποσότητα των πόρων που χρησιμοποιούνται υπό τις καθορισμένες συνθήκες. Το χαρακτηριστικό αυτό αποτελείται από τα ακόλουθα επιμέρους χαρακτηριστικά: ➢ **Χρονική συμπεριφορά**. Βαθμός στον οποίο οι χρόνοι απόκρισης και επεξεργασίας και οι ρυθμοί απόδοσης ενός προϊόντος ή συστήματος, κατά την εκτέλεση των λειτουργιών του, ανταποκρίνονται στις απαιτήσεις. ➢ **Χρήση πόρων**. Ο βαθμός στον οποίο οι ποσότητες και οι τύποι των πόρων που χρησιμοποιούνται από ένα προϊόν ή σύστημα, κατά την εκτέλεση των λειτουργιών του, ανταποκρίνονται στις απαιτήσεις.

	➢ **Χωρητικότητα**. Βαθμός στον οποίο τα μέγιστα όρια μιας παραμέτρου ενός προϊόντος ή συστήματος ανταποκρίνονται στις απαιτήσεις.
Λειτουργικές απαιτήσεις	**ΑΠ1: Επεξεργασία ετερογενών ροών πληροφοριών** **ΑΠ2: Ανταλλαγή πληροφοριών για την ασφάλεια στον κυβερνοχώρο** **ΑΠ4: Παροχή ειδοποιήσεων κυβερνοασφάλειας σε πραγματικό χρόνο** **ΑΠ6: Υπηρεσίες Κατανεμημένης Ευφυίας Ιστού & Σκοτεινού Δικτύου** **ΑΠ9: Βελτιστοποίηση της παρακολούθησης και της επεξεργασίας με βάση προγραμματιζόμενους μηχανισμούς ασφάλειας δικτύου και επιτάχυνση υλικού (π.χ. προγραμματιζόμενο μονοπάτι δεδομένων).** **ΑΠ11: Βελτιστοποίηση της παρακολούθησης και της επεξεργασίας με βάση τις μικρουπηρεσίες και τη σύνθεση υπηρεσιών.**

Α/Α	**ΜΑΠ2**
Τίτλος	**Συμβατότητα (Στόχος 1 - 4)**
Περιγραφή	Βαθμός στον οποίο ένα προϊόν ή σύστημα μπορεί να ανταλλάσσει, πληροφορίες με άλλα προϊόντα και συστήματα καθώς και να εκτελεί τις απαιτούμενες λειτουργίες του, ενώ μοιράζεται το ίδιο περιβάλλον υλικού ή λογισμικού. Το χαρακτηριστικό αυτό αποτελείται από τα ακόλουθα επιμέρους χαρακτηριστικά: ➢ **Συνύπαρξη.** Ο βαθμός στον οποίο ένα προϊόν μπορεί να εκτελεί αποτελεσματικά τις απαιτούμενες λειτουργίες του, ενώ μοιράζεται ένα κοινό περιβάλλον και πόρους με άλλα προϊόντα, χωρίς να επιβαρύνει οποιοδήποτε άλλο εμπλεκόμενο προϊόν. ➢ **Διαλειτουργικότητα.** Ο βαθμός στον οποίο δύο ή περισσότερα συστήματα, προϊόντα ή στοιχεία μπορούν να ανταλλάσσουν πληροφορίες και να χρησιμοποιούν τις πληροφορίες που έχουν ανταλλαχθεί. Η ανάγκη εφαρμογής νέων προτύπων μηχανισμών ασφάλειας για περιορισμένα επιχειρηματικά οικοσυστήματα δεν μπορεί να παρακάμψει τις υπάρχουσες πρακτικές και διαδικασίες (ασφάλειας). Από την άποψη αυτή, είναι σημαντικό να διευκολυνθεί η διαλειτουργικότητα και, κυρίως, η ενσωμάτωση με τα υπάρχοντα εργαλεία. Τα στοιχεία χρόνου εκτέλεσης του ΜΥΡΙΩΠΟΣ θα πρέπει να είναι, από άποψη αρχιτεκτονικής και υλοποίησης, κοντά στη βιομηχανία. Για το λόγο αυτό, το ΜΥΡΙΩΠΟΣ θα παρέχει υποστήριξη σε ορισμένα ευρέως χρησιμοποιούμενα πρότυπα, προγραμματιζόμενες διεπαφές (APIs), ευρέως διαθέσιμα εργαλεία, τεχνολογίες, μεθοδολογίες και βέλτιστες πρακτικές. Επιπλέον, αξίζει να σημειωθεί ότι υπάρχουν ήδη διαθέσιμα διάφορα πλαίσια συλλογής δεδομένων και μετρήσεων, τόσο για την παρακολούθηση των πόρων όσο και για την ανίχνευση επιθέσεων. Συγκεκριμένα, τα πλαίσια αυτά επιτρέπουν την ενοποιημένη διαχείριση των αρχείων καταγραφής από διαφορετικές εφαρμογές. Επομένως, το σύστημα ΜΥΡΙΩΠΟΣ θα πρέπει να διατηρεί συμβατότητα με

	υπάρχοντα εργαλεία (π.χ. Στοίβα Elasticsearch - ELK[20], Prometheus[21]), με σκοπό την περαιτέρω ενοποίηση του με παρεμφερή πλαίσια και εφαρμογές.
Λειτουργικές απαιτήσεις	**ΑΠ2: Ανταλλαγή πληροφοριών για την ασφάλεια στον κυβερνοχώρο**

[20] https://www.elastic.co/what-is/elk-stack
[21] https://prometheus.io/

4 Στοιχεία Αρχιτεκτονικής

Το ΜΥΡΙΩΠΟΣ στοχεύει στην παροχή ενός εξαιρετικά εύχρηστου συστήματος διαχείρισης της ασφάλειας στον κυβερνοχώρο, το οποίο εστιάζει στις επιχειρηματικές ιδιαιτερότητες των υπολογιστικών συστημάτων και υπηρεσιών νέφους, εισάγοντας καινοτομίες στις υπηρεσίες ασφάλειας στον κυβερνοχώρο, στην ανάλυση δεδομένων καθώς και την αυτοματοποιημένη δημιουργία ειδοποιήσεων και λήψη αποφάσεων πραγματικού χρόνου.

Οι αποφάσεις που θα ληφθούν από την ανάλυση των δεδομένων διαχωρίζονται στις αποφάσεις Χαμηλού και Υψηλού επιπέδου. Οι πρώτες αναφέρονται σε αποφάσεις που εφαρμόζονται και λαμβάνονται σε χαμηλό επίπεδο και περιλαμβάνουν τις διεπαφές δικτύου, τα τείχη προστασίας, και μπορούν να αφορούν στην απόρριψη συγκεκριμένων πιθανών κακόβουλων πακέτων μέσω ντετερμινιστικών κανόνων εξόρυξης πληροφορίας. Αντιθέτως, οι αποφάσεις Υψηλού επιπέδου αναφέρονται σε αποφάσεις που θα ληφθούν σε κάποιον εξωτερικό διακομιστή ή κεντρικά στην υποδομή του υπολογιστικού νέφους και αφορούν στη δημιουργία ειδοποιήσεων και στα αποτελέσματα αναλυτικής μέσω της χρήσης και εκπαίδευσης μοντέλων βαθιάς μηχανικής μάθησης. Λόγω της πολυπλοκότητας και του απαιτητικού υλικοτεχνικού εξοπλισμού αυτών των αλγορίθμων, η εκτέλεση τους σε ξεχωριστό υλικό κρίνεται απαραίτητη. Η εταιρία UBITECH για το σκοπό αυτό διαθέτει στο έργο το υπολογιστικό περιβάλλον για τις δοκιμές και την τελική υλοποίηση της ενοποιημένης λύσης.

4.1 Εννοιολογική Αρχιτεκτονική

Η Εννοιολογική Αρχιτεκτονική όπως παρουσιάζεται στην Εικόνα 2 αφορά στον καθορισμό των τεχνικών εννοιών του ΜΥΡΙΩΠΟΣ και παρουσιάζει με αφηρημένο τρόπο τα στοιχεία του συστήματος δίχως να παρέχονται λεπτομέρειες. Τα εννοιολογικά αρχιτεκτονικά διαγράμματα λειτουργούν ουσιαστικά ως δομικά μοντέλα, οπότε (ιδανικά θα πρέπει να) αναδεικνύουν τις σχέσεις μεταξύ των βασικών εννοιών και όχι τον τρόπο λειτουργίας τους. Αυτό σημαίνει ότι δεν ασχολούνται με την αποκάλυψη της ροής/διαδοχής διαδικασιών [28]. Περισσότερες λεπτομέρειες δίνονται στην Αρχιτεκτονική Συστήματος της ενότητας 4.2.

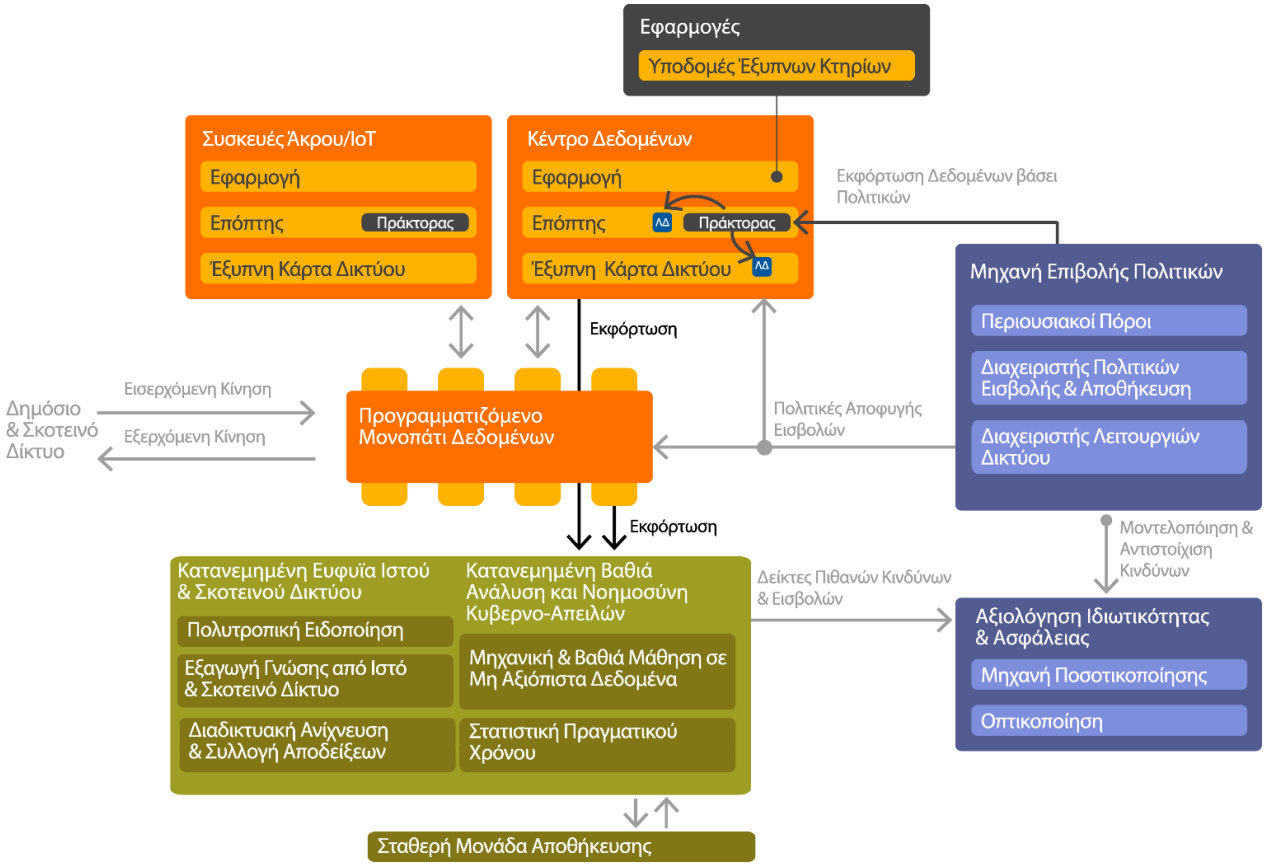
Η μοντελοποίηση σε αυτό το αφαιρετικό επίπεδο συνιστάται για τη δημιουργία μιας συνοπτικής, σαφούς και ξεκάθαρης εικόνας της οργάνωσης του συστήματος παρουσιάζοντας μόνο τις θεμελιώδεις έννοιες του. Δεδομένου ότι η Εννοιολογική Αρχιτεκτονική δεν υπεισέρχεται σε τεχνικές λεπτομέρειες, είναι κατάλληλη για την επικοινωνία με τους ενδιαφερόμενους που έχουν εμπορικό ενδιαφέρον και επιχειρηματικό υπόβαθρο, επομένως μπορεί να χρησιμοποιηθεί ακόμη και για σκοπούς επικοινωνίας και διάδοσης.

Η Εννοιολογική Αρχιτεκτονική καταγράφει όλα τα επίπεδα στο περιβάλλον υποδομής, από τις Συσκευές Άκρου, τις κεντρικές υπηρεσίες στο Κέντρο Δεδομένων που φιλοξενούνται στο υπολογιστικό νέφος ως την Μηχανή Επιβολής Πολιτικών. Η αρχιτεκτονική αποτελείται από διάφορα λειτουργικά μέρη, και συγκεκριμένα:

- Τις Συσκευές Άκρου,
- Το Κέντρο Δεδομένων,
- Το Προγραμματιζόμενο Μονοπάτι Δεδομένων,
- Την Κατανεμημένη Ευφυία Ιστού & Σκοτεινού Δικτύου,
- Τις μεθόδους που υποστηρίζουν την Κατανεμημένη Βαθιά Ανάλυση και Νοημοσύνη Κυβερνοαπειλών,
- Τη Μηχανή Επιβολής Πολιτικών,

- Τις μεθόδους για την Αξιολόγηση Ιδιωτικότητας & Ασφαλείας,
- Τη Σταθερή Μονάδα Αποθήκευσης.

Καθένα από τα επίπεδα είναι ικανό να εκτελεί ένα συγκεκριμένο σύνολο λειτουργιών κυβερνοασφάλειας, να ικανοποιεί ένα συγκεκριμένο σύνολο απαιτήσεων και να υποστηρίζει τις αντίστοιχες δράσεις και ενότητες εργασίας του ΜΥΡΙΩΠΟΣ. Στην Εικόνα 2 απεικονίζεται το διάγραμμα της Εννοιολογικής Αρχιτεκτονικής ΜΥΡΙΩΠΟΣ, συμπεριλαμβανομένων των κύριων στοιχείων και των βασικών αλληλεπιδράσεων μεταξύ τους.



Εικόνα 2. Εννοιολογική Αρχιτεκτονική ΜΥΡΙΩΠΟΣ

Τα επιμέρους εννοιολογικά στοιχεία των λειτουργιών του ΜΥΡΙΩΠΟΣ είναι τα εξής:

- Επόπτης που προγραμματίζεται και εφαρμόζει κανόνες για να παρακολουθεί και να καταγράφει πακέτα και κίνηση από το δίκτυο
- Έξυπνη Κάρτα Δικτύου που προγραμματίζεται για να επιτρέπει ή να αποτρέπει κίνηση πακέτων με βάσει κάποια κριτήρια
- Διαδικτυακή Ανίχνευση & Συλλογή Αποδείξεων που αφορά στην εκπαίδευση μοντέλων και στην εκτέλεση των αντίστοιχων μεθόδων τεχνητής νοημοσύνης και βαθιάς μηχανικής μάθησης που υποβοηθούν στην εξαγωγή γνώσης

- Εξαγωγή Γνώσης από Ιστό & Σκοτεινό Δίκτυο που αφορά στην κειμενική ανάλυση, δημιουργία γράφων και στον εντοπισμό επικίνδυνων δραστηριοτήτων στον ιστό (π.χ. μαζική κλήση για DDoS επιθέσεις, υποκλοπή δεδομένων, κ.α.)
- Πολυτροπική Ειδοποίηση που αφορά σε μηχανισμούς ενημέρωσης του τελικού χρήστη σχετικά με σημαντικά γεγονότα ως αποτέλεσμα ανάλυσης και το αποτέλεσμά τους παρουσιάζεται στη Μηχανή Οπτικοποίησης
- Μηχανική & Βαθιά Μάθηση σε δεδομένα καταγραφής και παρακολούθησης κίνησης καθώς και της κειμενικής συλλογής από τον Ιστό που αφορά στις μεθόδους και στα μοντέλα εκπαίδευσης πάνω από δεδομένα πραγματικού χρόνου και σταθερά δεδομένα που βρίσκονται στη Σταθερή Μονάδα Αποθήκευσης
- Στατιστική Πραγματικού Χρόνου σε δεδομένα καταγραφής και παρακολούθησης κίνησης καθώς και της κειμενικής συλλογής που αφορά στην εκτέλεση στατιστικών μεθόδων συνάθροισης, υπολογισμού μεγίστου / ελαχίστου / μέσου όρου κ.τ.λ. που υποβοηθούν στη δημιουργία επερωτήσεων πάνω από τα δεδομένα της Σταθερής Μονάδας Αποθήκευσης
- Διαχειριστής Επιβολής Πολιτικών αφορά στη μηχανή που προτεραιοποιεί και υπολογίζει τη βέλτιστη πολιτική που εφαρμόζεται στο σύστημα για την αποφυγή εισβολών και την αποτροπή επιθέσεων
- Περιουσιακοί Πόροι και η Διαχείριση Λειτουργιών Δικτύου αφορούν στα υπολογιστικά στοιχεία που χρειάζονται (π.χ. εικονικά δίκτυα, ευρετήρια και σταθερά δεδομένα καταγραφής από τους Επόπτες, Ενορχηστρωτής που διαχειρίζεται τη μνήμη, το σταθερό δίσκο, κ.α.) για τη βέλτιστη διαλειτουργικότητα του συστήματος ΜΥΡΙΩΠΟΣ
- Αναφορές Ποσοτικοποίησης που αφορούν στην κατάλληλη οργάνωση όλων των δεδομένων του συστήματος για τη δημιουργία αναφορών και περιγραφικής αναλυτικής μέσα από ένα πλήθος επερωτήσεων με κριτήριο την κατηγορία, το χρόνο, το πλήθος, κ.α.
- Διεπαφή Χρήστη που αφορά στη διασύνδεση όλων των λειτουργιών και οπτικοποίησή τους μέσα από φιλικές και διαδραστικές προς τον τελικό χρήστη διεπαφές

Ο τρόπος που αλληλοεπιδρούν τα λειτουργικά συστατικά του ΜΥΡΙΩΠΟΣ μέσω προγραμματιστικών διεπαφών παρουσιάζονται στη συνέχεια. Πιο συγκεκριμένα, οι Συσκευές Άκρου και το Κέντρο Δεδομένων λειτουργούν ως αισθητήρες εποπτείας και καταγραφής κίνησης για το σύστημα ΜΥΡΙΩΠΟΣ. Το Προγραμματιζόμενο Μονοπάτι Δεδομένων είναι η κύρια Διεπαφή επικοινωνίας για κάθε εισερχόμενη και εξερχόμενη ροή κίνησης του συστήματος ΜΥΡΙΩΠΟΣ. Όπως απεικονίζεται στην Εικόνα 2, το Προγραμματιζόμενο Μονοπάτι Δεδομένων είναι υπεύθυνο για όλες τις ενέργειες φόρτωσης και εκφόρτωσης, απόρριψης και επανάληψης σε άλλη υπηρεσία ή πόρτα για περεταίρω επεξεργασίας της εισερχόμενης και εξερχόμενης κίνησης των δεδομένων από και προς το Δημόσιο & Σκοτεινό Δίκτυο. Επιπλέον, είναι υπεύθυνο για την επιβολή των πολιτικών στις συσκευές άκρου και στις κεντρικές υπηρεσίες που υπολογίζονται από τη Μηχανή Επιβολής Πολιτικών. Η εκφόρτωση δεδομένων πραγματοποιείται είτε σε δεδομένα καταγραφής κίνησης μέσω του Προγραμματιζόμενου Μονοπατιού Δεδομένων είτε από το Κέντρο Δεδομένων για την

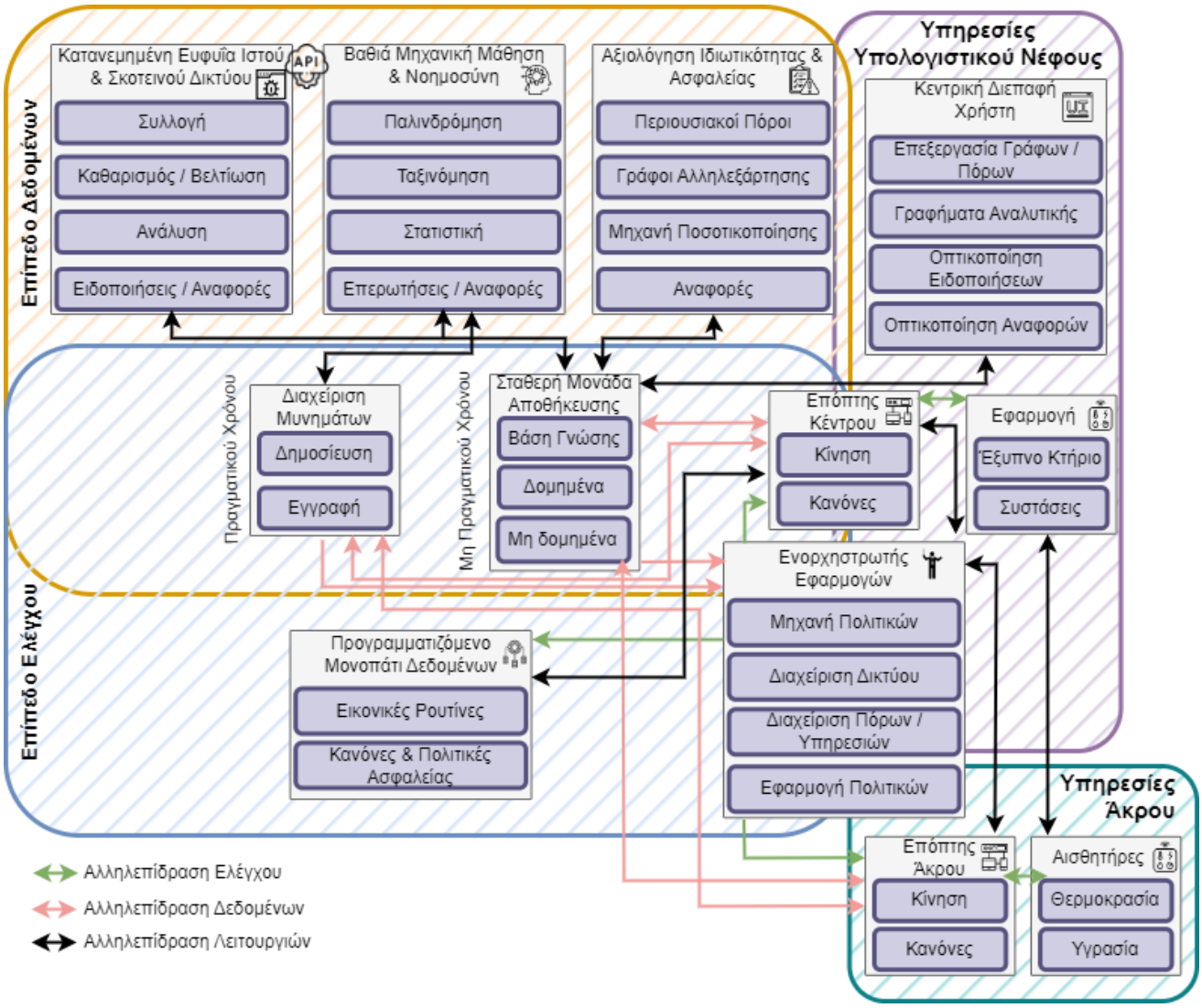
εκπαίδευση προηγμένων μοντέλων βαθιάς μηχανικής μάθησης. Η Κατανεμημένη Ευφυΐα Ιστού διαθέτει τη δική της εσωτερική στοίβα υπηρεσιών για τη στοχευμένη συλλογή πληροφορίας, ανάλυσης και δημιουργία ειδοποιήσεων και αλληλεπιδρά με τη Σταθερή Μονάδα Αποθήκευσης και με τη μηχανή Οπτικοποίησης. Η Κατανεμημένη Βαθιά Ανάλυση έχει τους αλγορίθμους για τα μοντέλα εκπαίδευσης, αλληλεπιδρά με τη Σταθερή Μονάδα Αποθήκευσης και είναι υπεύθυνη για την εκπαίδευση των μοντέλων, την παραγωγή διαφορετικών κατηγοριών αναλυτικής (π.χ. παλινδρόμηση για προβλέψεις επικείμενων εισβολών ή ταξινόμηση για κατηγοριοποίηση επιθέσεων) και για την εξαγωγή γνώσης. Η Μηχανή Επιβολής Πολιτικών αποτελεί τον εγκέφαλο του ΜΥΡΙΩΠΟΣ, λειτουργεί ως ο Ενορχηστρωτής του συστήματος καθώς συγκεντρώνει όλη τη γνώση που εξάγεται, υπολογίζει τις βέλτιστες πολιτικές και τις εφαρμόζει στα επιμέρους λειτουργικά στοιχεία, όπως είναι οι Συσκευές Άκρου ή το Κέντρο Δεδομένων. Η Μηχανή Ποσοτικοποίησης υλοποιεί μεθόδους για την ποσοτικοποίηση του κινδύνου από ευπάθειες, επιθέσεις και τη συνέπεια που μπορεί να έχουν σε διασυνδεδεμένα και διαλειτουργικά συστήματα. Τέλος, η Σταθερή Μονάδα Αποθήκευσης είναι υπεύθυνη για τη αποθήκευση των δεδομένων που έχουν συλλεχθεί και πρόκειται να επεξεργαστούν σε μετέπειτα χρόνο καθώς και όλων των αποτελεσμάτων μη πραγματικού χρόνου που υπολογίζονται. Τα δεδομένα και τα αποτελέσματα πραγματικού χρόνου τα διαχειρίζεται ένα υποσύστημα μηνυμάτων που λειτουργεί με τη λογική παραγωγού / καταναλωτή γεγονότων ως δημοσίευση / εγγραφή κατόπιν σχετικής ρύθμισης.

4.2 Αρχιτεκτονική Συστήματος

Η Αρχιτεκτονική Συστήματος περιγράφει τον τρόπο λειτουργίας ενός συστήματος από την άποψη της λειτουργίας και των λογικών πληροφοριών. Αντιπροσωπεύει ένα ενδιάμεσο επίπεδο, που βρίσκεται μεταξύ της εννοιολογικής και της φυσικής αρχιτεκτονικής. Ωστόσο, σε αντίθεση με αυτές, η Αρχιτεκτονική Συστήματος έχει αρκετά ευρύ πεδίο εφαρμογής. Στην πραγματικότητα, επιτρέπει τη μοντελοποίηση τόσο σε υψηλό όσο και σε χαμηλό επίπεδο, ανάλογα με τις απαιτήσεις, γεγονός που την καθιστά αναπόσπαστο κομμάτι της διαδικασίας. Σε αυτή την ενότητα θα παρουσιάσουμε τις λειτουργίες και τις λογικές πληροφορίες του ΜΥΡΙΩΠΟΣ και θα συνδέσουμε τις απαιτήσεις που εισήχθησαν στις Ενότητες 3.3 και 3.4 με τα λειτουργικά μέρη του ΜΥΡΙΩΠΟΣ.

Συγκεκριμένα, για τη δημιουργία της Αρχιτεκτονικής Συστήματος οι κύριες αλληλεπιδράσεις που προσδιορίστηκαν ως μέρος της Εννοιολογικής Αρχιτεκτονικής στην Ενότητα 4.1 εμπλουτίστηκαν με τα επιμέρους επίπεδα και τις λογικές πληροφορίες Άκρου, Υπολογιστικού Νέφους καθώς και των επιπέδων Ελέγχου που είναι απαραίτητο για την ενορχήστρωση των υπηρεσιών, την εξαγωγή γνώσης και εφαρμογής των πολιτικών και των Δεδομένων που είναι απαραίτητο για όλη τη ροή της πληροφορίας από τη συλλογή ως την ανάλυση και αποθήκευση.

Η Αρχιτεκτονική Συστήματος του ΜΥΡΙΩΠΟΣ απεικονίζεται στην Εικόνα 3.



Εικόνα 3. Αρχιτεκτονική Συστήματος ΜΥΡΙΩΠΟΣ

Η αλληλεπίδραση μεταξύ διαφορετικών υποσυστημάτων παρουσιάζεται με μαύρα βέλη και υποδεικνύει τη διαλειτουργικότητά τους. Η αλληλεπίδραση σε Επίπεδο Ελέγχου, υπολογισμού και επιβολής των πολιτικών ασφαλείας παρουσιάζεται με πράσινα βέλη και η αλληλεπίδραση μεταξύ διαφορετικών υποσυστημάτων κατά τη συλλογή, αποθήκευση, ανάγνωση δεδομένων σε πραγματικό και μη πραγματικό χρόνο για την εξυπηρέτηση των ίδιων των υποσυστημάστων παρουσιάζεται με ροζ βέλη.

Το έργο ΜΥΡΙΩΠΟΣ στοχεύει στην παροχή ενός ολιστικού συστήματος ασφαλείας σε εφαρμογές που εκτελούνται στο άκρο και σε υπολογιστικά συστήματα νέφους. Περίπτωση χρήσης του ΜΥΡΙΩΠΟΣ αποτελεί μια εφαρμογή έξυπνου κτηρίου που διαθέτει κατανεμημένους αισθητήρες υγρασίας και θερμοκρασίας (υπηρεσίες άκρου) και υπηρεσίες αναλυτικής και συστάσεων στο νέφος (υπηρεσίες υπολογιστικού νέφους)

που παρακολουθούνται από έξυπνους Επόπτες για εισβολές. Οι έξυπνοι Επόπτες καταγράφουν όλη τη δραστηριότητα των κατανεμημένων αισθητήρων και κεντρικοποιημένων υπηρεσιών στη Σταθερή Μονάδα Αποθήκευσης και τροφοδοτούν τον Ενορχηστρωτή Εφαρμογών για τον υπολογισμό των κατάλληλων Πολιτικών Ασφαλείας με δεδομένα πραγματικού και μη πραγματικού χρόνου ως αποτέλεσμα ανάλυσης από τη Βαθιά Μηχανική Μάθηση ή ευρημάτων στο Σκοτεινό Δίκτυο. Το αποτέλεσμα υπολογισμού της βέλτιστης Πολιτικής κατόπιν εφαρμόζεται μέσω του Ενορχηστρωτή με τη μορφή Κανόνων στις Υπηρεσίες Άκρου ή Υπολογιστικού Νέφους. Οι Κανόνες ανάλογα την κρισιμότητα που ποσοτικοποιείται από την Αξιολόγηση Ιδιωτικότητας & Ασφαλείας μπορεί να διακόψουν μια υπηρεσία, να εκφορτώσουν για περεταίρω επεξεργασία και ανάλυση τα δεδομένα ή να απορρίψουν πακέτα. Ως εκ τούτου, το έργο ΜΥΡΙΩΠΟΣ παραδίδει ένα προγραμματιζόμενο Επίπεδο Ελέγχου για την επιβολή των Κανόνων Ασφαλείας και ένα Επίπεδο Δεδομένων που διασφαλίζει ότι τα διαφορετικά γεγονότα που προκύπτουν από την καταγραφή της κίνησης μέσων των Εποπτών μπορούν να εμπλουτίζονται απρόσκοπτα και να τροφοδοτούν περεταίρω αναλύσεις, προβλέψεις και επιβολή νέων Ενεργειών μέσω Κανόνων. Για το λόγο αυτό, το ΜΥΡΙΩΠΟΣ έχει σχεδιαστεί με διαλειτουργικό τρόπο που δεν επηρεάζει την ενορχήστρωση. Αυτό σημαίνει ότι δεν θα εξαρτάται οργανικά από τις εκάστοτε βιβλιοθήκες ή οποιοδήποτε συγκεκριμένο συστατικό του κάθε ενορχηστρωτή που βρίσκεται στη βιβλιογραφία με τη μορφή ανοικτού κώδικα.

Πριν εμβαθύνουμε στις λεπτομέρειες της Αρχιτεκτονικής Συστήματος, είναι εξαιρετικά σημαντικό να συζητήσουμε και να αναλύσουμε τις προϋποθέσεις που πρέπει να πληρούνται προκειμένου να υλοποιηθεί η αρχιτεκτονική. Όπως έχει ήδη αναφερθεί, το έργο ΜΥΡΙΩΠΟΣ στοχεύει στην ανάπτυξη ενός *"προγραμματιζόμενου επιπέδου ελέγχου και δεδομένων"*. Στο σημείο αυτό τονίζεται ότι ενώ το Επίπεδο Ελέγχου έχει μηδενικές προϋποθέσεις, το Επίπεδο Δεδομένων θέτει κάποιες ελάχιστες απαιτήσεις. Πιο συγκεκριμένα, ο Ενορχηστρωτής Εφαρμογών που αξιοποιείται από το ΜΥΡΙΩΠΟΣ επιτρέπει τη βαθιά ανάλυση και διαχείριση πακέτων από εξωτερικές οντότητες λογισμικού. Μια άλλη απαίτηση που ικανοποιείται είναι η ικανότητα του προγραμματιζόμενου μονοπατιού δεδομένων μέσω εικονικών οντοτήτων λογισμικού και έξυπνων καρτών δικτύου να υποστηρίζουν άμεση εκφόρτωση δεδομένων στο άκρο μιας υποδομής δίχως να επιτρέπουν σε ένα πακέτο να περάσει και να επεξεργαστεί κεντρικά (ενδεχομένως προσβάλοντας την υποδομή).

Όπως εύκολα συμπεραίνεται από την Εικόνα 3, η Αρχιτεκτονική Συστήματος χωρίζεται σε τέσσερα διακριτά "επίπεδα", με τις αντίστοιχες "ζώνες" οι οποίες περικλείουν τα διάφορα λειτουργικά συστατικά μέρη. Συγκεκριμένα, οι εν λόγω ζώνες περιλαμβάνουν:

- Το **Επίπεδο Ελέγχου** το οποίο υποστηρίζει ολόκληρο τον κύκλο διεργασιών από τη συλλογή και παρακολούθηση της κίνησης μέσω των Εποπτών ως τον υπολογισμό των Πολιτικών Ασφαλείας και την επιβολή των Κανόνων αποφυγής ή περιορισμού των κυβερνοαπειλών.

- Το **Επίπεδο Δεδομένων** το οποίο υποστηρίζει τον κύκλο της Κατανεμημένης Ευφυΐας από την αποθήκευση των δεδομένων, τον υπολογισμό των διαφορετικών μεθόδων αναλυτικής μέσω βαθιάς μηχανικής μάθησης και την παραγωγή αναφορών προς Οπτικοποίηση ή ενδείξεων που πυροδοτούν τον υπολογισμό βέλτιστων Πολιτικών Αποφυγής.
- Οι **Υπηρεσίες Άκρου** αφορούν στην εγκατάσταση και παραμετροποίηση του λογισμικού των Εποπτών που παρακολουθούν την κίνηση που παράγουν ασύρματοι αισθητήρες.
- Οι **Υπηρεσίες Υπολογιστικού Νέφους** αφορούν στην εγκατάσταση και παραμετροποίηση του λογισμικού των Εποπτών που παρακολουθούν την κίνηση που υποστηρίζει την κεντρική Εφαρμογή Έξυπνου Κτηρίου, περιλαμβάνει τον Ενορχηστρωτή που έχει γνώση όλου του οικοσυστήματος και της Κεντρικής Διεπαφής Χρήστη που παρουσιάζει τα αποτελέσματα, τις αναφορές και τις ειδοποιήσεις που υπολογίζονται από την Κατανεμημένη Ευφυΐα Ιστού, τη Μηχανή Αξιολόγησης της Ιδιωτικότητας και Ασφάλειας, τους Γράφους Αλληλεπίδρασης των υφιστάμενων συσκευών, υπηρεσιών και εφαρμογών.

Τα συγκεκριμένα επίπεδα αποτελούν μια "εννοιολογική ομαδοποίηση" των λειτουργικών συστατικών του συστήματος ΜΥΡΙΩΠΟΣ και αφορούν στην εγγύτητα και τον τρόπο αλληλεπίδρασης των υπηρεσιών του συστήματος. Για παράδειγμα, τα επιμέρους λειτουργικά συστατικά του Επιπέδου Ελέγχου είναι σε θέση να απορρίπτουν, προωθούν ή να τερματίζουν μια υπηρεσία βάσει Κανόνων μέσω του Ενορχηστρωτή. Αντιθέτως, τα λειτουργικά συστατικά του Επιπέδου Δεδομένου είναι σε θέση να συλλέγουν, επεξεργάζονται, αναλύουν σε μεγαλύτερο βάθος τις εκάστοτε πληροφορίες που ταξιδεύουν εντός του συστήματος και να παράγουν αναφορές μέσω επερωτήσεων ή ως αποτέλεσμα βαθιάς μάθησης και ειδοποιήσεις. Επιπλέον, όπως είναι εύλογο, πολλά λειτουργικά στοιχεία ανήκουν στην τομή των επιπέδων καθώς έχουν διττό ρόλο στο σύστημα ΜΥΡΙΩΠΟΣ. Τέλος, πριν δώσουμε μια σύντομη περιγραφή του κάθε λειτουργικού συστατικού στην επόμενη ενότητα, γίνεται μια συνοπτική αναφορά που αφορά στη ροή των πληροφοριών εντός της προτεινόμενης αρχιτεκτονικής.

4.2.1 Ροή Πληροφοριών και Αρχικοποίηση Συστήματος

Το ΜΥΡΙΩΠΟΣ στοχεύει στην παροχή νέων τεχνικών και συνδυαστικών υπηρεσιών τόσο σε επίπεδο υλικού, όσο και σε επίπεδο λογισμικού για την έγκαιρη ανίχνευση εισβολών και παράνομου ηλεκτρονικού περιεχομένου, με στόχο την επίτευξη αυξημένης προστασίας σε υποδομές, υπηρεσίες και εφαρμογές εξελιγμένων υπηρεσιών ασφαλείας σε υποδομές υπολογιστικού νέφους. Προκειμένου να λειτουργήσει το ΜΥΡΙΩΠΟΣ εγκαθιστούμε ένα σύνολο εποπτών που παρακολουθούν υπηρεσίες άκρου (π.χ. κίνηση που παράγουν κατανεμημένοι ασύρματοι αισθητήρες) και κεντρικές υπηρεσίες υπολογιστικού νέφους. Αυτή η φάση ενεργοποίησης είναι ουσιαστική δεδομένου ότι:

- Εκκινεί τον Ενορχηστρωτή Εφαρμογών ο οποίος βρίσκεται στο Επίπεδο Ελέγχου, Δεδομένων και Υπολογιστικού Νέφους. Ο Ενορχηστρωτής διαχειρίζεται τους διάφορους Επόπτες που είναι εγκατεστημένοι είτε στο άκρο είτε στην υποδομή Υπολογιστικού Νέφους. Ο Ενορχηστρωτής αποτελεί τον ακρογωνιαίο λίθο της Διαχείρισης Εφαρμογών, Πόρων και Υπηρεσιών, της Διαχείρισης του

Δικτύου και της Μηχανής Υπολογισμού των Πολιτικών Ασφαλείας ολόκληρου του συστήματος. Επιπλέον είναι αυτός ο οποίος επιβάλει τις Πολιτικές στο Προγραμματιζόμενο Μονοπάτι Δεδομένων, στον Επόπτη Κέντρου και στον Επόπτη Άκρου και ως εκ τούτου στην τελική εφαρμογή.

- Εκκινεί τη Μηχανή Επιβολής Πολιτικών που λαμβάνει όλες τις πληροφορίες που σχετίζονται με το πλαίσιο ασφαλείας των εφαρμογών (π.χ. αρχεία καταγραφής, υπολογιζόμενες μέσω αξιολόγησης παραβίασης ιδιωτικότητας ή ασφάλειας, γεγονότα εντοπισμού κακόβουλων ενεργειών μέσω της υπηρεσίας «δημοσίευση / εγγραφή» του υποσυστήματος μηνυμάτων), να τις επεξεργάζεται μέσω ενός υποσυστήματος κανόνων[22] και να λαμβάνει αποφάσεις μετριασμού των πιθανών επιθέσεων σε όλο το εύρος του πλαισίου.
- Υποστηρίζει την Κεντρική Διεπαφή Χρήστη όπου οι χρήστες του συστήματος μπορούν να παραμετροποιήσουν διαφορετικές λειτουργίες όπως για παράδειγμα την αρχικοποίηση αναζητήσεων στο Σκοτεινό Δίκτυο, τις πολιτικές ασφαλείας, κ.α. Επίσης έχουν την πλήρη εποπτεία των αναφορών που παράγονται από τα επιμέρους συστήματα, των ειδοποιήσεων και των γραφημάτων αναλυτικής.

Το δεύτερο βήμα της ενεργοποίησης του συστήματος ΜΥΡΙΩΠΟΣ είναι η εγκατάσταση των τοπικών Εποπτών που επιτηρούν τις Υπηρεσίες Άκρου, συλλέγουν πληροφορίες παρακολούθησης κίνησης και εμπλουτίζουν τις καταγραφές με περεταίρω μέτα-πληροφορία. Ο κάθε τοπικός Επόπτης υποστηρίζει πέντε διακριτές λειτουργίες. Πιο συγκεκριμένα:

- Ανακοινώνει την παρουσία του στον Ενορχηστρωτή. Ο Ενορχηστρωτής έχει την εποπτική εικόνα ολόκληρου του Επιπέδου Ελέγχου και του Επιπέδου Δεδομένων. Επιπλέον, κάθε Επόπτης χρησιμοποιεί συγκεκριμένα πρωτόκολλα που ενισχύουν την ασφαλή μεταφορά των δεδομένων μέσω αυθεντικοποίησης και εξουσιοδότησης με τον Ενορχηστρωτή και το Προγραμματιζόμενο Μονοπάτι Δεδομένων.
- Επιτρέπει μέσω παραμετροποίησης τη διαχείριση της εξαγωγής αρχείων καταγραφής από οποιαδήποτε εφαρμογή. Δεδομένου ότι ο Επόπτης έχει ορατότητα σε επίπεδο πυρήνα, μπορεί να φιλτράρει τα δεδομένα προκειμένου να δημιουργήσει το πλήρες μονοπάτι που ταξιδεύει η πληροφορία και προωθείται από επίπεδο σε επίπεδο.
- Επιτρέπει μέσω παραμετροποίησης τη διαχείριση κανόνων σε επίπεδο πακέτων δικτύου σε πραγματικό χρόνο καθώς και περεταίρω ενέργειες όπως απόρριψη, προώθηση, επανάληψη, κ.λπ. για εύκολες συνθήκες εντοπισμού κακόβουλων πακέτων.

4.2.2 Λειτουργικά Στοιχεία Αρχιτεκτονικής

Στη συνέχεια παρουσιάζονται οι λειτουργίες των επιμέρους υποσυστημάτων του ΜΥΡΙΩΠΟΣ. Περισσότερες τεχνικές λεπτομέρειες θα δοθούν στα επιμέρους τεχνικά παραδοτέα του κάθε υποσυστήματος που περιγράφουν τις τεχνολογίες, τις μεθόδους και τον τρόπο διασύνδεσής τους. Τα υποσυστήματα είναι ως ακολούθως:

- Η Κατανεμημένη Ευφυία Ιστού και Σκοτεινού Δικτύου περιλαμβάνει την ανάπτυξη λογισμικού και την υποστήριξη υπηρεσιών για τη στοχευμένη συλλογή κειμενικών δεδομένων που αφορούν σε κυβερνοεπιθέσεις, μαζικές κλήσεις για DDoS επιθέσεις, διαρροή δεομένων που πωλούνται στο Σκοτεινό Δίκτυο. Η συλλογή υποστηρίζεται με αυτόματο τρόπο αλλά και μέσω της Κεντρικής Διεπαφής Χρήστη όπου ο τελικός χρήστης μπορεί να αρχικοποιήσει τις δικές του αναζητήσεις. Επίσης, περιλαμβάνει ένα σύνολο ενεργειών για τον καθαρισμό των δεδομένων, τον εμπλουτισμό τους με

[22] https://en.wikipedia.org/wiki/Forward_chaining

ανοικτές οντολογίες και τη διαχείριση μιας ουράς για την αποφυγή ανακάλυψης του ίδιου κειμένου / άρθρου που έχει ήδη ανακαλυφθεί εντός της ημέρας. Αν το περιεχόμενο ενός άρθρου αλλάξει μεταξύ διαφορετικών αναζητήσεων σε διαφορετικές μέρες, η διαφορά τους αποθηκεύεται ως ηλεκτρονικό τεκμήριο με χρονοσφραγίδα. Επίσης, περιλαμβάνει ένα σύνολο μεθόδων μηχανικής μάθησης για εξαγωγή γνώσης από κείμενα, ανάλυση κειμένων, δημιουργία γράφων δεικτοδότησης διαφορετικών ιστοσελίδων, καταμέτρησης συχνών όρων που υποβοηθούν τον υπολογισμό αναφορών και ειδοποιήσεων τα οποία παρουσιάζονται στην Κεντρική Διεπαφή Χρήστη.

- Βαθιά Μηχανική Μάθηση & Νοημοσύνη η οποία περιλαμβάνει τους αλγορίθμους κειμενικής ανάλυσης, ανάλυσης χρονοσειρών, τεχνητών νευρωνικών δικτύων (LSTM[23], RNN[24], κ.α.) και μεθόδων ενεργοποίησης (RELU[25], SoftMax[26], κ.α.) καθώς και στατιστικών μεθόδων για την ανάλυση των συλλεχθέντων δεδομένων από τις καταγραφές των Εποπτών και από δεδομένα Δημόσιου και Σκοτεινού Δικτύου. Τα δεδομένα είναι δομημένα και αδόμητα, αφορούν σε κείμενα, γράφους, κατηγορικά και χρονοσειρές καταγραφής, επομένως θα επιλεχθούν οι κατάλληλοι αλγόριθμοι για την εκπαίδευση των μοντέλων που ταιριάζουν στη φύση των δεδομένων. Η πληροφορία που εξάγεται ως αποτέλεσμα της ανάλυσης θα τροφοδοτήσει τον Ενορχηστρωτή για τη λήψη αποφάσεων και επιβολή της κατάλληλης πολιτικής είτε μέσω της Σταθερής Μονάδας Αποθήκευσης (για δεδομένα μη πραγματικού χρόνου) είτε το υποσύστημα Διαχείρισης Μηνυμάτων (για δεδομένα πραγματικού χρόνου)[27]. Ιδιαιτέρως οι αλγόριθμοι ανάλυσης κειμένου και γράφων χρησιμοποιούνται μέσω ειδικής προγραμματιστικής διεπαφής (API) από το υποσύστημα της Κατανεμημένης Ευφυΐας Ιστού & Σκοτεινού Δικτύου.
- Αξιολόγηση Ιδιωτικότητας και Ασφάλειας η οποία περιλαμβάνει μεθόδους και διεπαφές χρήστη για τη μοντελοποίηση των υφιστάμενων πόρων (υλικό, λογισμικό, εφαρμογές, βάσεις δεδομένων, διευθύνσεων IP και πόρτες) σε γράφους αλληλεξάρτησης προκειμένου να υπολογιστεί ο κίνδυνος από μια πιθανή κυβερνοεπίθεση. Ακριβώς από το γεγονός ότι οι υπηρεσίες και οι πόροι αλληλεπιδρούν μεταξύ τους, είναι πιθανό η συνέπεια από μια επίθεση να επηρεάσει κλιμακωτά κι άλλες υπηρεσίες και όχι απαραίτητα την άμεσα προσβεβλημένη. Ως εκ τούτου, οι υφιστάμενες υπηρεσίες μοντελοποιούνται σε γράφο αλληλεξάρτησης που περιέχει μέτα-πληροφορία για τον τρόπο που είναι συνδεδεμένες, χρησιμοποιούνται ή εκτίθενται δημόσια στον ιστό για τον υπολογισμό του ατομικού κινδύνου, του συναθροιστικού κινδύνου και κλιμακωτού κινδύνου μέσω άλλων υπηρεσιών / πόρων. Θα αξιοποιηθεί η Βάση Γνώσης που αποθηκεύει σε σχεσιακό μοντέλο τον τρόπο που σχετίζονται οι ευπάθειες[28] (Common Vulnerabilities Enumeration - CVE), οι κωδικοί γνωστών προϊόντων[29] (Common Platform Enumeration - CPE) και οι αδυναμίες των συστημάτων υλικού και λογισμικού (Common Weakness Enumeration - CWE)[30].
- Κέντρο Δεδομένων περιλαμβάνει τη Βάση Γνώσης για τον εμπλουτισμό των ευπαθειών του συστήματος ΜΥΡΙΩΠΟΣ με υπάρχουσες οντολογίες που μοντελοποιούν ευπάθειες, προϊόντα και αδυναμίες που μπορεί να γίνουν μέσο εκμετάλλευσης από εισβολείς, τη Σχεσιακή Βάση που

[23] https://en.wikipedia.org/wiki/Long_short-term_memory
[24] https://en.wikipedia.org/wiki/Recurrent_neural_network
[25] https://machinelearningmastery.com/rectified-linear-activation-function-for-deep-learning-neural-networks/
[26] https://developers.google.com/machine-learning/crash-course/multi-class-neural-networks/softmax
[27] https://kafka.apache.org/
[28] https://cve.mitre.org/
[29] https://cpe.mitre.org/
[30] https://cwe.mitre.org/

αποθηκεύει και υποστηρίζει επερωτήσεις σε δομημένα δεδομένα και τη Μη Σχεσιακή Βάση (NoSQL) που αποθηκεύει και υποστηρίζει όψεις, υπολογισμούς και επερωτήσεις σε αδόμητα δεδομένα. Χρησιμοποιείται και για την αποθήκευση των συλλεχθέντων δεδομένων, τα αποτελέσματα των υπολογισμών κυρίως για απαιτήσεις μη πραγματικού χρόνου. Αναφορικά με τις απαιτήσεις πραγματικού χρόνου τα δεδομένα ταξιδεύουν μέσω του υποσυστήματος Διαχείρισης Μηνυμάτων που υποστηρίζει το πρότυπο επικοινωνίας Δημοσίευσης / Εγγραφής.

- Η Κεντρική Διεπαφή Χρήστη αποτελεί το βασικό γραφικό περιβάλλον που επιτρέπει στο χρήστη να παρακολουθεί τα αποτελέσματα των αναφορών που παράγουν τα επιμέρους υποσυστήματα, της αναλυτικής από τους αλγορίθμους βαθιάς μηχανικής μάθησης, ποσοτικοποίησης του κινδύνου, γραφήματα σχετικά με την κειμενική ανάλυση από το Σκοτεινό Δίκτυο. Ο χρήστης έχει επίσης τη δυνατότητα παραμετροποίησης και αρχικοποίησης υπηρεσιών όπως η εκκίνηση αναζητήσεων στο Σκοτεινό Δίκτυο, μοντελοποίησης των Πόρων (υλικού και λογισμικού με όνομα/IP/port) σε γράφο αλληλεξάρτησης καθώς και των πολιτικών ελέγχου και επιβολής ασφάλειας.
- Οι Επόπτες παρακολούθησης αναφέρονται στο λογισμικό που εγκαθίσταται και αρχικοποιείται κεντρικά στις υπηρεσίες υπολογιστικού νέφους (βλέπε Επόπτης Κέντρου) και στις συσκευές άκρου (βλέπε Επόπτης Άκρου) με σκοπό την παρακολούθηση του δικτύου, των πακέτων κίνησης και της πληροφορίας που ανταλλάσσεται μεταξύ τους.
- Ο Ενορχηστρωτής Εφαρμογών αποτελεί τον κεντρικό εγκέφαλο του συστήματος ΜΥΡΙΩΠΟΣ καθώς συγκεντρώνει την απαιτούμενη γνώση από τη διαχείριση της υφιστάμενης υποδομής (εφαρμογές, υπηρεσίες, δίκτυο, μνήμη, επεξεργαστική ισχύς και σταθερός δίσκος ανά υπηρεσία), τους Επόπτες, τα υποσυστήματα της Κατανεμημένης Ευφυΐας, τα αποτελέσματα των αλγορίθμων Βαθιάς Μηχανικής Μάθησης και Ποσοτικοποίησης του Κινδύνου και μέσω της Μηχανής Πολιτικών υπολογίζει και εφαρμόζει τους Κανόνες αντιμετώπισης από μια πιθανή εισβολή. Οι Κανόνες αυτοί με τη μορφή του γραμμογραφημένου προτύπου YAML[31] είναι ικανοί όταν εκτελεστούν από τον Ενορχηστρωτή να επιβάλουν την επιθυμητή πολιτική καταστολής στον επιθυμητό πόρο. Ο πόρος μπορεί να είναι κεντρικά στα πλαίσια εφαρμογής που παρακολουθείται από τον / τους Επόπτη/ες Κέντρου ή στο άκρο στα πλαίσια κάποιας συσκευής / υπηρεσίας που παρακολουθείται από τον / τους Επόπτη/ες Άκρου.
- Προγραμματιζόμενο Μονοπάτι Δεδομένων αναφέρεται στη δυνατότητα προγραμματισμού της κίνησης και της έξυπνης διαχείρισης των δεδομένων κίνησης μέσα από εικονικές ρουτίνες λογισμικού. Δίνει τη δυνατότητα επεξεργασίας και λήψης αποφάσεων σε πραγματικό χρόνο δίχως την ανάγκη να προωθηθεί το πακέτο σε υψηλότερο επίπεδο ή να περάσει από τον κεντρικό επεξεργαστή καθώς και καθορισμού κανόνων (π.χ. προώθηση, τερματισμός, ανά-δρομολόγηση / απόρριψη πακέτου, κ.α.) για την αποτροπή κακόβουλων ενεργειών.
- Εφαρμογή η οποία αναφέρεται στην περίπτωση χρήσης ενός έξυπνου κτηρίου που θα χρησιμοποιηθεί ως πιλοτική επίδειξη στο έργο ΜΥΡΙΩΠΟΣ. Η εφαρμογή περιλαμβάνει καταγραφή συνθηκών θερμοκρασίας και υγρασίας με τη μορφή χρονοσειρών για τη δημιουργία συστάσεων βέλτιστης κατανάλωσης ενέργειας. Συνδυάζει συσκευές άκρου και κατανεμημένους ασύρματους αισθητήρες που μετρούν τις συνθήκες του κτηρίου, μια κεντρική βάση χρονοσειρών[32] και μια σχεσιακή βάση[33] για τον υπολογισμό συστάσεων. Οι υπηρεσίες των βάσεων (με όνομα/IP/port), οι

[31] https://yaml.org/
[32] https://www.influxdata.com/
[33] https://www.mysql.com/

ασύρματοι αισθητήρες (με όνομα/IP/port) και ο τρόπος που μοντελοποιούνται σε γράφο αλληλεξάρτησης αποτελούν το οικοσύστημα μελέτης των υπηρεσιών κυβερνοασφάλειας που υποστηρίζει ο ΜΥΡΙΩΠΟΣ.

4.2.3 Στοιχεία Αρχιτεκτονικής Και Απαιτήσεις

Στην ενότητα αυτή παρουσιάζουμε ένα πίνακα (βλέπε Πίνακας 9) αντιστοίχισης στον οποίο συνδέουμε τα διαφορετικά επίπεδα και στοιχεία της Αρχιτεκτονικής με τις Απαιτήσεις που ορίστηκαν στις ενότητες 3.4 και 3.4.

Πίνακας 9. Αντιστοίχιση Στοιχείων Αρχιτεκτονικής και Απαιτήσεων

Επίπεδο	Λειτουργικό Στοιχείο	Λειτουργικές Απαιτήσεις	Μη Λειτουργικές Απαιτήσεις
Δεδομένων	Κατανεμημένη Ευφυΐα Ιστού & Σκοτεινού Δικτύου	ΑΠ1, ΑΠ4, ΑΠ5, ΑΠ6, ΑΠ13, ΑΠ14, ΑΠ19	ΜΑΠ1, ΜΑΠ2
	Βαθιά Μηχανική Μάθηση & Νοημοσύνη	ΑΠ4, ΑΠ5, ΑΠ13, ΑΠ14, ΑΠ19, ΑΠ24	ΜΑΠ2
	Αξιολόγηση Ιδιωτικότητας & Ασφαλείας	ΑΠ3, ΑΠ4, ΑΠ5, ΑΠ12, ΑΠ14, ΑΠ19, ΑΠ20	ΜΑΠ2
	Σταθερή Μονάδα Αποθήκευσης	ΑΠ1, ΑΠ2, ΑΠ6, ΑΠ16, ΑΠ18, ΑΠ19	ΜΑΠ2
	Διαχείριση Μηνυμάτων	ΑΠ1, ΑΠ2, ΑΠ4, ΑΠ6, ΑΠ13, ΑΠ19	ΜΑΠ1, ΜΑΠ2
Ελέγχου	Προγραμματιζόμενο Μονοπάτι Δεδομένων	ΑΠ3, ΑΠ8, ΑΠ9, ΑΠ12	ΜΑΠ1, ΜΑΠ2
	Ενορχηστρωτής Εφαρμογών	ΑΠ3, ΑΠ5, ΑΠ12, ΑΠ19, ΑΠ20, ΑΠ21, ΑΠ22	ΜΑΠ1, ΜΑΠ2
Υπολογιστικού Νέφους	Κεντρική Διεπαφή Χρήστη	ΑΠ2, ΑΠ4, ΑΠ13, ΑΠ15, ΑΠ19	ΜΑΠ2
	Επόπτης Κέντρου	ΑΠ4, ΑΠ6, ΑΠ8, ΑΠ11, ΑΠ12, ΑΠ14, ΑΠ23	ΜΑΠ1, ΜΑΠ2
	Εφαρμογή Έξυπνου Κτηρίου	ΑΠ11, ΑΠ15, ΑΠ17, ΑΠ18, ΑΠ19	ΜΑΠ2
Υπηρεσιών & Συσκευών Άκρου	Επόπτης Άκρου	ΑΠ4, ΑΠ6, ΑΠ8, ΑΠ10, ΑΠ12, ΑΠ14, ΑΠ23	ΜΑΠ1, ΜΑΠ2
	Αισθητήρες	ΑΠ10, ΑΠ15, ΑΠ17, ΑΠ19	ΜΑΠ2

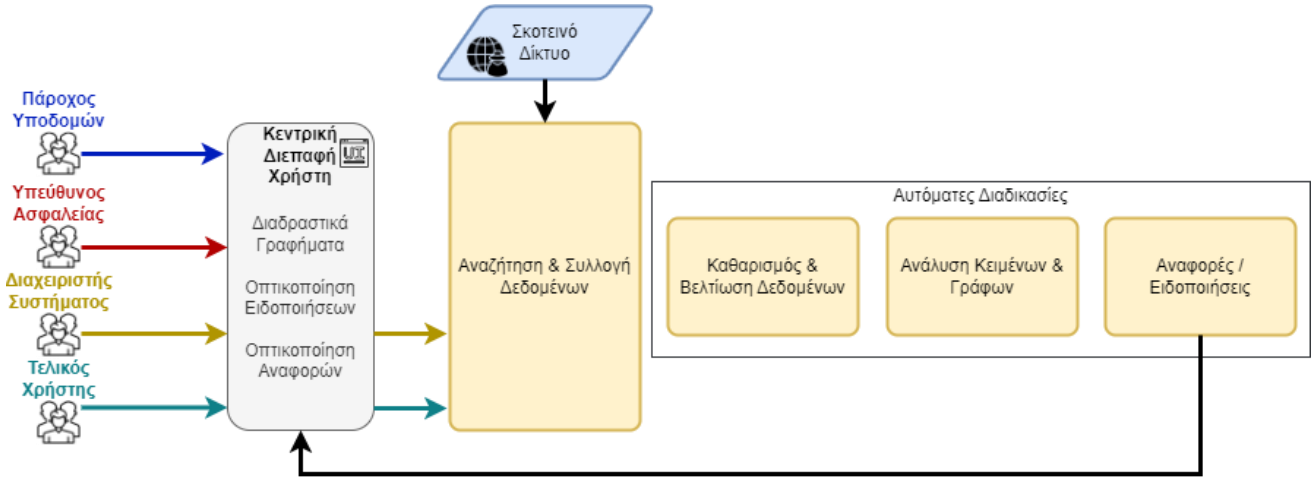
4.3 Διάγραμμα Ροής Χρηστών

Στη συγκεκριμένη υποενότητα παρουσιάζουμε τις αλληλεπιδράσεις των χρηστών του συστήματος ΜΥΡΙΩΠΟΣ με τα κύρια λειτουργικά μέρη της προτεινόμενης αρχιτεκτονικής. Συγκεκριμένα οι χρήστες του πλαισίου είναι, οι:

- Ιδιωτικές επιχειρήσεις και πάροχοι υποδομών

- Υπεύθυνος ασφαλείας
- Διαχειριστής συστήματος και εγκατάστασης
- Τελικός χρήστης / πελάτης

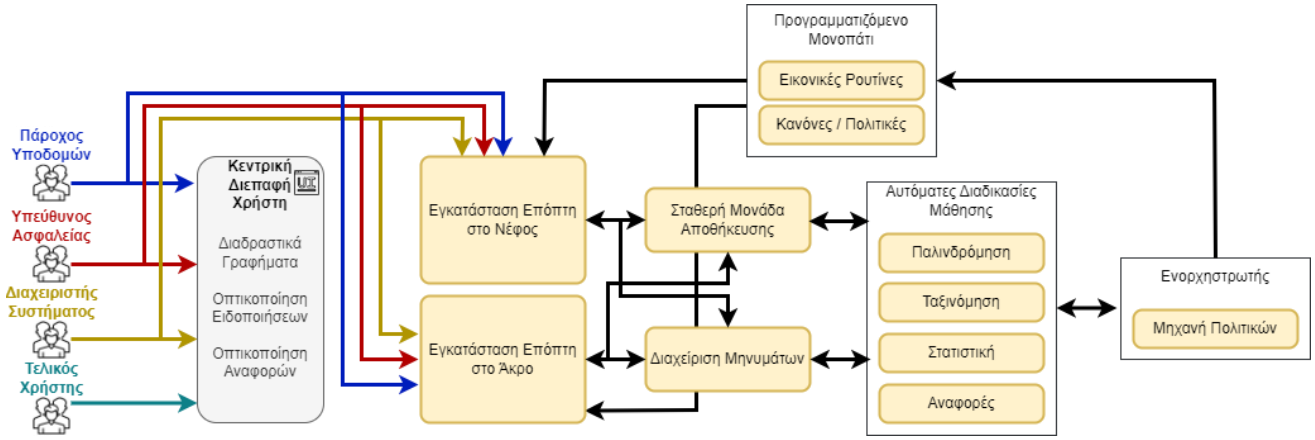
και για την απεικόνιση της αλληλεπίδρασης τους με τα κύρια λειτουργικά μέρη χρησιμοποιήθηκαν διαγράμματα UML[34], όπως αυτά παρουσιάζονται στα παρακάτω σχήματα. Συγκεκριμένα στην Εικόνα 4, παρουσιάζονται οι τέσσερις διαφορετικοί χρήστες του πλαισίου και ο τρόπος που αλληλεπιδρούν με τη Κατανεμημένη Ευφυΐα Ιστού και Σκοτεινού Δικτύου. Όπως φαίνεται, ο Διαχειριστής Συστήματος από τη διεπαφή χρήστη αλληλεπιδρά με όλα τα επιμέρους στοιχεία σε αντίθεση με τον Υπεύθυνο Ασφαλείας ο οποίος αλληλεπιδρά μόνο με τις αναφορές και τα γραφήματα. Επίσης, ο Πάροχος Υποδομών αλληλεπιδρά με τις αναφορές, τις ειδοποιήσεις και τα γραφήματα, ενώ ο Τελικός χρήστης αλληλεπιδρά με τις αναφορές, τα γραφήματα και τις μεθόδους αρχικοποίησης για την Αναζήτηση και Συλλογή περιεχομένου στο σκοτεινό δίκτυο. Οι διαδικασίες βελτίωσης και καθαρισμού των δεδομένων, κειμενικής ανάλυσης και ανάλυσης γράφων καθώς και οι αναφορές εκτελούνται και παράγονται αυτόματα από το υποσύστημα Κατανεμημένης Ευφυΐας Ιστού και Σκοτεινού Δικτύου. Ο προγραμματισμός των διαδικασιών και η δημιουργία επερωτήσεων για την παραγωγή αναφορών γίνεται από τον προγραμματιστή του υποσυστήματος.



Εικόνα 4. Διάγραμμα Ροής της Κατανεμημένης Ευφυίας Ιστού και Σκοτεινού Δικτύου

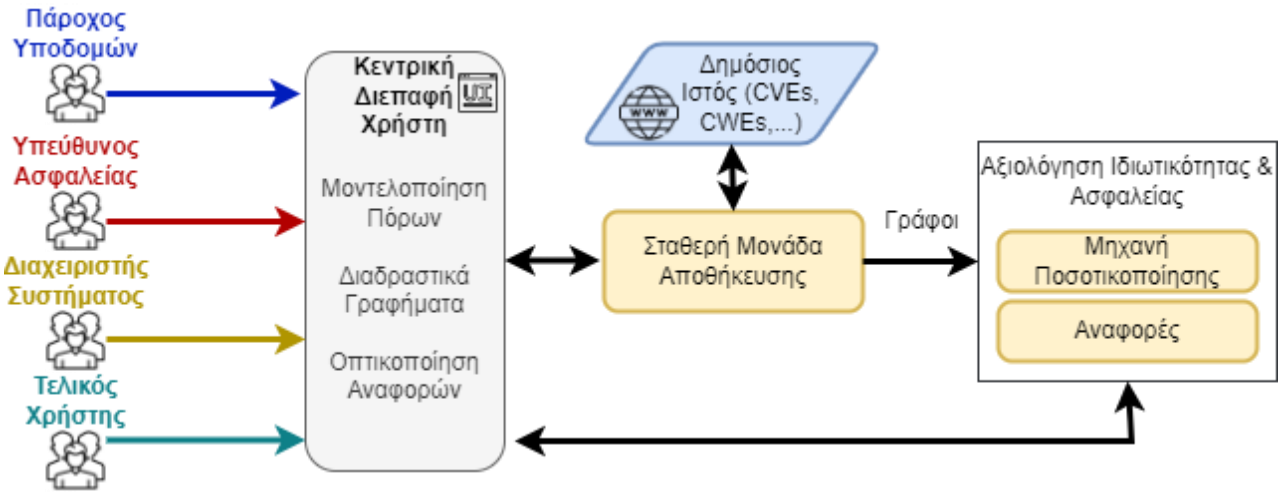
Με την ίδια λογική, στο διάγραμμα ροής στην Εικόνα 5, σχετικά με την αλληλεπίδραση των χρηστών του συστήματος ΜΥΡΙΩΠΟΣ με τον Ενορχηστρωτή και τη Μηχανή Επιβολής Πολιτικών παρατηρούμε τον Πάροχο Υποδομών, τον Υπεύθυνο Ασφαλείας και το Διαχειριστή Συστήματος να επιδρούν με όλα τα επιμέρους στοιχεία. Ο Τελικός Χρήστης έχει πρόσβαση στις αναφορές και ειδοποιήσεις μέσω της Κεντρικής Διεπαφής καθώς και με γραφήματα που παρουσιάζουν την κατάσταση της υποδομής με τη μορφή χρονοσειρών αναφορικά με τους υπολογιστικούς πόρους και τα αποτελέσματα της Βαθιάς Μηχανικής Μάθησης. Ο προγραμματισμός των διαδικασιών και η δημιουργία επερωτήσεων για την παραγωγή αναφορών γίνεται από τον προγραμματιστή του υποσυστήματος.

[34] https://en.wikipedia.org/wiki/Unified_Modeling_Language



Εικόνα 5. Διάγραμμα Ροής της Μηχανής Επιβολής Πολιτικών

Τέλος, στην Εικόνα 6 που αφορά το διάγραμμα ροής των χρηστών αναφορικά με τη Αξιολόγηση Ιδιωτικότητας και Ασφάλειας παρατηρείται και πάλι ο Υπεύθυνος Ασφαλείας και ο Διαχειριστής Συστήματος να έχουν πρόσβαση στη μοντελοποίηση της υφιστάμενης υποδομής υπό τη μορφή γράφου αλληλεξάρτησης. Κατόπιν, οι διαδικασίες ποσοτικοποίησης του κινδύνου παρουσιάζονται μέσω αναφορών και διαδραστικών γραφημάτων. Ο Πάροχος Υποδομών και ο Τελικός Χρήστης έχουν πρόσβαση στις αναφορές ποσοτικοποίησης του κινδύνου. Με ειδική εκπαίδευση μπορούν να είναι σε θέση να μοντελοποιήσουν τους πόρους με την προϋπόθεση ότι διαθέτουν σαφή γνώση και εποπτεία της υφιστάμενης υποδομής και του τρόπου που οι πόροι αλληλεπιδρούν και είμαι μεταξύ τους διασυνδεδεμένοι. Ο προγραμματισμός των διαδικασιών και η δημιουργία επερωτήσεων για την παραγωγή αναφορών γίνεται από τον προγραμματιστή του υποσυστήματος.



Εικόνα 6. Διάγραμμα Ροής της Αξιολόγησης Ιδιωτικότητας και Ασφαλείας

5 Καθορισμός Νέου Προϊόντος

Όπως αναφέρθηκε, το Ελάχιστο Βιώσιμο Προϊόν (ΕΒΠ) είναι μια ευέλικτη έννοια σχεδιασμού και προγραμματισμού των προϊόντων με στόχο την πρώιμη είσοδο στην αγορά, καθώς είναι μια έκδοση με αρκετά χαρακτηριστικά ώστε να ικανοποιεί τους πρώτους χρήστες. Ως αποτέλεσμα, πρόκειται για μια προσέγγιση που μπορεί να εξοικονομήσει χρόνο και προσπάθεια ελαχιστοποιώντας τις πιθανότητες δραστικού επανασχεδιασμού του προϊόντος στο τέλος της ανάπτυξης του, ώστε να ανταποκρίνεται στις πραγματικές ανάγκες των χρηστών. Σε αντίθεση με τον απομονωμένο σχεδιασμό, η έγκαιρη εμπλοκή των τελικών χρηστών κατά τη στιγμή του σχεδιασμού, αποκαλύπτει τις ανάγκες και τις ευκαιρίες βελτίωσης που υπάρχουν στις τρέχουσες διαδικασίες, αναδεικνύοντας τα σημεία παρέμβασης για το υπό εξέλιξη προϊόν.

Ωστόσο, στο πλαίσιο του ΜΥΡΙΩΠΟΣ, η μεθοδολογία σχεδιασμού του ΕΒΠ εξυπηρετεί έναν ελαφρώς διαφορετικό σκοπό από αυτόν της άμεσης εκκίνησης και σταδιακής ωρίμανσης του προϊόντος. Έχοντας ένα σαφές όραμα από την αρχή του έργου, που αντικατοπτρίζονται μέσω των τεχνικών απαιτήσεων του παρόντος παραδοτέου, το ΕΒΠ λειτουργεί ως συνεκτική διαδικασία και εργαλείο για την επικύρωση των προβλεπόμενων λειτουργιών, την ιεράρχηση των προτεραιοτήτων και τον ομαλό σχεδιασμό των δραστηριοτήτων ανάπτυξης λογισμικού. Στη συνέχεια, το ΕΒΠ αποτελεί το θεμέλιο για τη σταδιακή ωρίμανση του προϊόντος που βασίζεται σε επαναληπτικούς κύκλους ανάπτυξης και επικύρωσης, η οποία ανοίγει το δρόμο προς τη βέλτιστη συνεργασία μεταξύ των εταίρων και την παράδοση ενός προϊόντος πραγματικής αξίας για τους χρήστες, με σεβασμό στους υφιστάμενους περιορισμούς, όπως ο χρόνος, οι πόροι και οι τεχνικές προκλήσεις.

Η τελική έκδοση του ΕΒΠ αποτελείται από τη συνένωση του ενδιάμεσου και του τελικού ΕΒΠ. Καθώς το πλήρες σύνολο των υποχρεωτικών απαιτήσεων που πρέπει να πληρούνται μέχρι το τέλος του έργου έχει προσδιοριστεί στο συγκεκριμένο παραδοτέο μέσω της διαδικασίας εντοπισμού των εκάστοτε αναγκών κυβερνοασφάλειας. Το τελικό ΕΒΠ του ΜΥΡΙΩΠΟΣ θα λειτουργήσει ως το Πλέον Πολύτιμο Προϊόν, όσον αφορά στην παροχή όλων των απαιτήσεων και λειτουργιών που έχουν καθοριστεί στις ενότητες 3.3 και 3.4. Με βάση αυτή την προσέγγιση, η διαδικασία ιεράρχησης αποκαλύπτει τα χαρακτηριστικά της ενδιάμεσης έκδοσης του ΕΒΠ τα οποία θα πρέπει να προσφέρουν όλες τις απαιτούμενες λειτουργίες που θα ληφθούν υπόψη κατά τον σχεδιασμό των πρώτων εκδόσεων των λειτουργικών στοιχείων του ΜΥΡΙΩΠΟΣ και του ολοκληρωμένου συστήματος.

Επιπλέον, ο ρόλος της πιλοτικής εφαρμογής για τον ορισμό ενός επιτυχημένου ΕΒΠ είναι ουσιαστικός, καθώς παρέχει την απαιτούμενη γνώση και τις περιπτώσεις χρήσης που ενσωματώνουν τις προβλεπόμενες απαιτήσεις σε πραγματικές λειτουργίες. Αξίζει να σημειωθεί ότι, λόγω της υψηλής πολυπλοκότητάς των χαρακτηριστικών, ορισμένα από αυτά μπορεί να συμπεριληφθούν εν μέρει στο ενδιάμεσο ΕΒΠ και θα αναπτυχθούν περαιτέρω και θα υλοποιηθούν πλήρως στο τελικό ΕΒΠ. Όπως είναι επόμενο, το ενδιάμεσο ΕΒΠ είναι υποσύνολο του τελικού ΕΒΠ που προβλέπεται για την τελική έκδοση του πλαισίου.

5.1 Μεθοδολογία Καθορισμού και Προτεραιοποίησης Χαρακτηριστικών Νέου Προϊόντος

Ακολουθώντας την προσανατολισμένη στο χρήστη προσέγγιση της άμεσης εκκίνησης του έργου, η διαδικασία ανάπτυξης του ΕΒΠ του ΜΥΡΙΩΠΟΣ εξαρτάται σε μεγάλο βαθμό από τον σαφή και συνεκτικό ορισμό των περιπτώσεων χρήσης. Όπως φαίνεται στην Εικόνα 7, η λεπτομερής περιγραφή της τρέχουσας κατάστασης του οικοσυστήματος της πιλοτικής εφαρμογής, όσον αφορά στο επιχειρησιακό περιβάλλον των εφαρμογών, τις

διαδικασίες και το επιχειρηματικό πεδίο, παρέχουν ορισμένες πληροφορίες για την πραγματική υποδομή και λειτουργία τους. Επομένως, ο προσδιορισμός των κενών που σχετίζονται με την κυβερνοασφάλεια αποκαλύπτει τις πραγματικές ανάγκες τους. Οι διαπιστωθείσες ανάγκες μεταφράζονται σε σενάρια που θα εμπλουτίσουν τις εκάστοτε λειτουργικές ροές εργασίας μέσω της προσθήκης των λειτουργιών κυβερνοασφάλειας που υποστηρίζονται από το ΜΥΡΙΩΠΟΣ. Τα σενάρια αυτά ενσωματώνουν τις υπηρεσίες μέσω των απαιτήσεων όπως έχουν οριστεί στο παρόν παραδοτέο και παρέχουν μια πρώτη προσπάθεια αναπαράστασης των αλληλεπιδράσεων και της ανταλλαγής δεδομένων μεταξύ του συστήματος και των υποσυστημάτων του ΜΥΡΙΩΠΟΣ. Οι περιπτώσεις χρήσης, είναι ένα δημοφιλές εργαλείο που χρησιμοποιείται για τη περιγραφή των ροών εργασίας των διαφόρων χρηστών χρήσης.

Για να εξασφαλιστεί η ισχυρή σύνδεση με τις απαιτήσεις όπως ορίστηκαν στο συγκεκριμένο παραδοτέο μέσω του τελικού συνόλου υποχρεωτικών και επιθυμητών απαιτήσεων, οι εξαγόμενες περιπτώσεις χρήσης και τα χαρακτηριστικά αντιστοιχίζονται στις αντίστοιχες απαιτήσεις, προσδιορίζοντας τις ακριβείς ανάγκες κάθε περίπτωσης χρήσης και τις συγκεκριμένες λειτουργίες του ΜΥΡΙΩΠΟΣ που θα δοκιμαστούν σε κάθε σενάριο. Θα πρέπει να σημειωθεί ότι οι απαιτήσεις που παρουσιάστηκαν στο συγκεκριμένο παραδοτέο, όπως η ενορχήστρωση υπηρεσιών ή οι μη λειτουργικές απαιτήσεις, δεν μεταφράζονται σε ιστορίες χρηστών, καθώς δεν αποτελούν αντικείμενο άμεσης αλληλεπίδρασης με τους χρήστες. Ωστόσο, θα αποτελέσουν μέρος των λεπτομερών προδιαγραφών των συστατικών στοιχείων στα επόμενα παραδοτέα, καθώς υποδεικνύουν την υποκείμενη λειτουργικότητα που απαιτείται για την παροχή των πραγματικών χαρακτηριστικών του συστήματος ΜΥΡΙΩΠΟΣ.

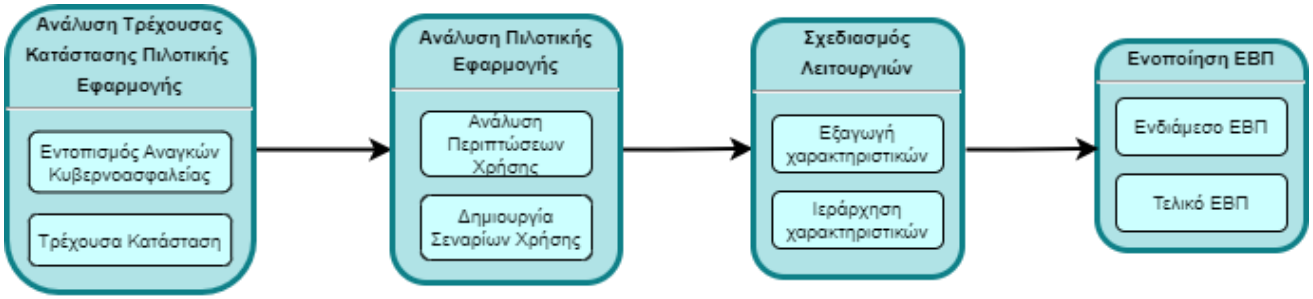
5.2 Μεθοδολογία Εξαγωγής Χαρακτηριστικών και Ιεράρχησης Προτεραιοτήτων

Οι περιπτώσεις χρήσης χρησιμεύουν ως βάση για την εξαγωγή του αρχικού καταλόγου των χαρακτηριστικών του συστήματος ΜΥΡΙΩΠΟΣ. Τα χαρακτηριστικά αυτά αποτελούν τα δομικά στοιχεία του ΕΒΠ, περιγράφοντας με επίσημο τρόπο τις λειτουργίες που θα παρέχει το ΜΥΡΙΩΠΟΣ στους τελικούς χρήστες. Η διαδικασία σχεδιασμού χαρακτηριστικών περιλαμβάνει την ανάλυση των λειτουργιών που βρίσκονται κάτω από κάθε περίπτωση χρήσης και την ευθυγράμμιση τους με τις απαιτήσεις του πλαισίου, ώστε να διασφαλιστεί ότι ο κατάλογος των χαρακτηριστικών εξυπηρετεί το αμοιβαία συμφωνημένο όραμα του ΜΥΡΙΩΠΟΣ. Το τελικό βήμα προς την παγίωση του ΕΒΠ είναι η ιεράρχηση των εξαχθέντων χαρακτηριστικών ακολουθώντας μια προσέγγιση ιεράρχησης με βάση τις λειτουργίες και τις υπηρεσίες που προσθέτους άμεσα αξία έναντι της πολυπλοκότητας ανάπτυξης. Για να διασφαλιστεί ότι η τελική λίστα προτεραιοτήτων συνδυάζει τόσο την επιχειρηματική όσο και την τεχνική προοπτική, η διαδικασία ιεράρχησης περιλαμβάνει όλους τους εταίρους του ΜΥΡΙΩΠΟΣ ώστε να συνεισφέρουν την εμπειρία τους από τον τομέα εξειδίκευσής τους και να διαμορφώσουν από κοινού ένα αμοιβαία αποδεκτό ΕΒΠ. Η ανάλυση των αποτελεσμάτων οδηγεί στην κατηγοριοποίηση των χαρακτηριστικών και στην ιεράρχησή τους με βάση τις επιθυμητές λειτουργίες που χρειάζεται να έχει άμεσα το σύστημα και προσφέρουν αξία στον τελικό χρήστη έναντι της πολυπλοκότητας. Η μεθοδολογία που ακολουθήθηκε για τον καθορισμό του ΕΒΠ παρουσιάζεται στην Εικόνα 7.

Στο πρώτο διάστημα του έργου θα εστιάσουμε στην εγκατάσταση των δομικών λειτουργικών στοιχείων του ΜΥΡΙΩΠΟΣ όπως είναι οι Επόπτες, η Σταθερή Μονάδα Αποθήκευσης, η Διαχείριση Μηνυμάτων, η Κατανεμημένη Ευφυΐα Ιστού και Σκοτεινού Δικτύου και η συλλογή δεδομένων παρακολούθησης για να υποβοηθήσουν την εκπαίδευση των μοντέλων της Βαθιάς Μηχανικής Μάθησης στη συνέχεια. Επίσης, θα δοθεί έμφαση στο σχεδιασμό και παροχή της Κεντρικής Διεπαφής Χρήστη η οποία στην αρχή θα παρουσιάσει

αναφορές και γραφήματα ως αποτέλεσμα του ενδιάμεσου ΕΒΠ και στη συνέχεια στο τελικό ΕΒΠ θα εμπλουτιστεί με διεπαφές που θα υποστηρίζουν την πλήρη λειτουργικότητα του συστήματος.

Θα πρέπει να σημειωθεί ότι κατά τη στιγμή του σχεδιασμού και της ανάπτυξης στοιχείων, τα χαρακτηριστικά και οι περιπτώσεις χρήσης αλληλοσυμπληρώνονται, καθώς τα τελευταία παρέχουν πολύτιμες λεπτομέρειες και το αναμενόμενο όφελος από την αναμενόμενη συμπεριφορά του συστήματος που δεν αποτυπώνεται στην επίσημη περιγραφή των χαρακτηριστικών.



Εικόνα 7. Μεθοδολογία ενοποίησης του τελικού ΕΒΠ

6 Επίλογος

Το παραδοτέο Π1.1 αποτελεί το παραδοτέο που προδιαγράφει τις απαιτήσεις και την Αρχιτεκτονική Συστήματος. Οι αναφορές σχετικά με τη μοντελοποίηση ασφαλείας, τις επικείμενες επιθέσεις και οι περιγραφές τους καλύπτουν μια αρχική διερεύνηση και περιγραφή της τρέχουσας τεχνολογικής κατάστασης που ανοίγουν το δρόμο για το καθορισμό των υποχρεωτικών και επιθυμητών απαιτήσεων του συστήματος. Η Αρχιτεκτονική Συστήματος του ΜΥΡΙΩΠΟΣ αποτελεί την προδιαγραφή μιας ενιαίας εφαρμογής ασφαλείας και προστασίας από κυβερνοαπειλές, με στόχο την προστασία διαφόρων οικοσυστημάτων που λειτουργούν σε υποδομές υπολογιστικού νέφους και διαθέτουν κατανεμημένες υπηρεσίες άκρου.

Επιπλέον, στο παραδοτέο περιγράφονται οι λειτουργικές και μη λειτουργικές απαιτήσεις της Αρχιτεκτονικής Συστήματος του ΜΥΡΙΩΠΟΣ καθώς και οι πληροφορίες που σχετίζονται με τη μοντελοποίησή τους, τη σύνδεσή τους με τα λειτουργικά στοιχεία του ΜΥΡΙΩΠΟΣ και τα επίπεδα εκτέλεσης. Επιπλέον, περιγράφηκε η Εννοιολογική Αρχιτεκτονική του ΜΥΡΙΩΠΟΣ για να υποβοηθήσει τον αναγνώστη αναφορικά με τη σύμβαση των εννοιών που υιοθετούμε στο συγκεκριμένο έργο, τα λειτουργικά στοιχεία που συναποτελούν το ενοποιημένο σύστημα καθώς και οι αλληλεπιδράσεις μεταξύ τους. Συγκεκριμένα, η Εννοιολογική Αρχιτεκτονική έθεσε τη βάση για τη δημιουργία της Αρχιτεκτονικής Συστήματος. Επιπρόσθετα, οι αλληλεπιδράσεις των χρηστών με τα επιμέρους λειτουργικά στοιχεία του συστήματος παρουσιάστηκαν με σαφήνεια, παράλληλα με τον καθορισμό του νέου προϊόντος μέσω της θέσπισης του ΕΒΠ.

Τέλος, στα επόμενα παραδοτέα θα δοθούν περισσότερες τεχνικές λεπτομέρειες σχετικά τα επιμέρους δομικά λειτουργικά στοιχεία του συστήματος ΜΥΡΙΩΠΟΣ, όπως της εξαγωγής γνώσης από το σκοτεινό δίκτυο, εκπαίδευσης μοντέλων ταξινόμησης και παλινδρόμησης με βαθιά μηχανική μάθηση και του μηχανισμού λήψης αποφάσεων και επιβολής πολιτικών έγκαιρου εντοπισμού κυβερνοαπειλών του ενοποιημένου συστήματος ΜΥΡΙΩΠΟΣ.

7 Αναφορές

[1] The Untold Story of NotPetya, the most Devastating Cyberattack in history. Available Online: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[2] Petya (malware). Available Online: https://en.wikipedia.org/wiki/Petya_(malware)
[3] Verizon 2018 Data Breach Investigations Report. Available Online: https://enterprise.verizon.com/resources/reports/dbir/
[4] Gartner Predicts for the Future of Privacy 2019. Available Online: https://www.gartner.com/smarterwithgartner/gartner-predicts-2019-for-the-future-of-privacy/
[5] Cloud hosting provider iNSYNQ hit by MegaCortex ransomware. Available Online: https://www.hackread.com/cloud-hosting-provider-insynq-hit-by-megacortex-ransomware/
[6] New trojan malware spreading through malicious Word documents. Available Online: https://gdpr.report/news/2019/08/09/new-trojan-malware-spreading-through-malicious-worddocuments/
[7] Saefko: new trojan being sold on the dark web. Available Online: https://gdpr.report/news/2019/08/09/saefkonew-trojan-being-sold-on-the-dark-web/
[8] Brown, A., Tuor, A., Hutchinson, B., & Nichols, N. (2018). Recurrent Neural Network Attention Mechanisms for Interpretable System Log Anomaly Detection. arXiv preprint arXiv:1803.04967.
[9] Radford, B. J., Apolonio, L. M., Trias, A. J., & Simpson, J. A. (2018). Network Traffic Anomaly Detection Using Recurrent Neural Networks. arXiv preprint arXiv:1803.10769.
[10] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: an ensemble of autoencoders for online network intrusion detection. arXiv preprint arXiv:1802.09089.
[11] Antonis Michalas and Ryan Murray. “Keep Pies Away from Kids: A Raspberry Pi Attacking Tool”. Proceedings of the 1st ACM CCS International Workshop on Internet of Things Security and Privacy (IoT S&P’17) in Conjunction with ACM CCS 2017, Dallas, USA, October 30 – November 03, 2017.
[12] ENISA, Methodologies for the identification of Critical Information Infrastructure assets and services, December 2014.
[13] PwC, The Global State of Information Security Survey 2018. Available Online: https://www.pwc.com/us/en/cybersecurity/information-security-survey.html
[14] General Data Protection Regulation (GDPR). Available Online: https://gdpr-info.eu/
[15] Grant, R. E., Rashti, M. J., Balaji, P., & Afsahi, A. (2015). Scalable Network Communication Using Unreliable RDMA. In Handbook on Data Centers (pp. 393-424). Springer, New York, NY.
[16] K. Beck, M. Beedle, A. Van Bennekum, A. Cockburn, W. Cunningham, M. Fowler, and D. Thomas, “The agile manifesto.,” 2001.
[17] D. S. U. Pandey and A. K. Ramani, “An effective requirement engineering process model for software development and requirements management,” in International Conference on Advances in Recent Technologies in Communication and Computing, 2010.
[18] R. Bansode and A. Girdhar, “Common Vulnerabilities Exposed in VPN – A Survey,” in *Journal of Physics: Conference Series 1714 012045*, 2021.
[19] A. Orso, W. G. J. Halfond and J. V. and, “A Classification of SQL Injection Attacks and Countermeasures,” 2006.
[20] D. A. Kindy and A.-S. K. Pathan, “A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques,” in *IEEE 15th International Symposium on Consumer Electronics (ISCE)*, 14-17 June 2011.
[21] “DMARC,” [Online]. Available: https://dmarc.org/

[22] "DKIM," [Online]. Available: http://www.dkim.org/
[23] Akamai, "Financial Services — Hostile Takeover Attempts, Volume 6, Issue 1," Akamai, 2020.
[24] ENISA, "Cybersecurity for SMEs Challenges and Recommendations," ENISA, June 2021.
[25] Sonicwall, "Sonicwall Cyber Threat Report," Sonicwall, 2020.
[26] Kaspersky, "DDoS attacks in Q1 2022," 2022. [Online]. Available: https://securelist.com/ddos-attacks-in-q1-2022/106358/
[27] ENISA, "Vulnerability of Wi-Fi WPA2 networks," 20 October 2017. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/vulnerability-of-wi-fi-wpa2-networks
[28] How to use architecture levels, Orbussoftware, https://www.orbussoftware.com/enterprisearchitecture/archimate/how-to-use-architecture-levels-effectively