ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μια Εφαρμογή Ιστού για τη Δημοσίευση και Επιλογή Προϊόντων Ασφάλειας-ως-Υπηρεσία (Security-as-a-Service)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Παναγιώτη Πλιάτσικα

Επιβλέπων: Κυριάκος Κρητικός

Μέλη εξεταστικής επιτροπής: Δημήτριος Σκούτας, Παναγιώτης Συμεωνίδης

Σάμος, Φεβρουάριος 2025

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος της Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων, του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου. Με την ολοκλήρωση της, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους και όλες που με υποστήριξαν και συνέβαλαν στην πραγματοποίησή της.

Πρώτα και κύρια, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, Κυριάκο Κρητικό, για την καθοδήγηση, τη συνεχιζόμενη υποστήριξη και την ανεκτίμητη βοήθεια που μου προσέφερε καθ' όλη τη διάρκεια της έρευνάς μου. Οι πολύτιμες παρατηρήσεις και συμβουλές του αποτέλεσαν τη βασική πυξίδα για την ολοκλήρωση της εργασίας αυτής.

Ευχαριστώ θερμά την οικογένειά μου για την αγάπη και την υποστήριξη τους κατά τη διάρκεια αυτής της απαιτητικής περιόδου. Η υποστήριξή τους ήταν ανεκτίμητη και χωρίς αυτούς δεν θα είχα καταφέρει να φτάσω ως εδώ.

Τέλος, θα ήθελα να ευχαριστήσω την Ανθή για τη στήριξη της καθ' όλη τη διάρκεια της εκπόνησης αυτής της εργασίας.

Παναγιώτη Πλιάτσικα
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Πίνακας περιεχομένων

Λίστα Σχημάτων

Λίστα Πινάκων

Ακρωνύμια

API	Application Programming Interface
CPU	Central Process Unit
DNS	Domain Name System
DoS	Denial of Service
ER	Entity Relationship
IaaS	Infrastructure as a Service
JVM	Java Virtual Machine
PaaS	Platform as a Service
REPL	Read Eval Print Loop
SaaS	Software as a Service
SecaaS	Security as a Service
SQL	Structured Query Language
URI	Universal Resource Identifier
WAF	Web Application Firewall
XSS	Cross-site scripting

Περίληψη

Η παρούσα διπλωματική εργασία αφορά την ανάπτυξη μιας μοντέρνας εφαρμογής ιστού που θα επιτρέπει σε παρόχους τη δημοσίευση των προϊόντων Ασφάλειας-ως-Υπηρεσία (SecaaS) τους, αλλά και σε χρήστες την ανακάλυψη και ταξινόμηση των προϊόντων αυτού του είδους που ικανοποιούν τις σχετικές απαιτήσεις και προτιμήσεις τους.

Για τη δημοσίευση, ανακάλυψη και ταξινόμηση αυτών των προϊόντων αναπτύχθηκε κατάλληλο μοντέλο περιγραφής τους, το οποίο καλύπτει τόσο λειτουργικά όσο και μη λειτουργικά χαρακτηριστικά τους. Η ανακάλυψη των προϊόντων Ασφάλειας-ως-Υπηρεσία βασίζεται στις απαιτήσεις του χρήστη όσον αφορά τα προαναφερόμενα χαρακτηριστικά. Από την άλλη μεριά, η ταξινόμηση τους γίνεται με βάση το σκορ αξιολόγησης, το οποίο υπολογίζεται με βάση την απόδοση του εκάστοτε προϊόντος σε μη λειτουργικά χαρακτηριστικά και στις προτιμήσεις του χρήστη, οι οποίες παρέχονται με τη μορφή σχετικών βαρών στα μη λειτουργικά αυτά χαρακτηριστικά.

Οι λειτουργίες της ανακάλυψης ως προς τα λειτουργικά χαρακτηριστικά και της ταξινόμησης ως προς τα μη λειτουργικά χαρακτηριστικά των προϊόντων Ασφάλειας-ως-Υπηρεσία (SecaaS), αποτελούν καινοτομίες που εισάγει η εφαρμογή μας, επιτρέποντας σε έναν οργανισμό ή ιδιώτη να εντοπίσει προϊόντα αυτού του είδους με βάση τις απαιτήσεις και προτιμήσεις του.

Λέξεις Κλειδιά: *ασφάλεια, ανακάλυψη, ταξινόμηση, υπολογιστικό νέφος, προϊόντα ασφάλειας ως υπηρεσία, μηχανισμοί ασφάλειας, εφαρμογή ιστού*

Abstract

This thesis focuses on the development of a modern web application that will allow providers to publish their Security-as-a-Service (SecaaS) products, as well as users to discover and rank such products that meet their relevant requirements and preferences.

A suitable model for describing these products was developed for their publication, discovery, and ranking, covering both functional and non-functional characteristics. The discovery of Security-as-a-Service products is based on user requirements concerning the aforementioned characteristics. On the other hand, their ranking relies on the computation of their score, which is determined by the performance of each SecaaS on the non-functional characteristics and the user preferences, where the latter are supplied in the form of relevant weights mapping to these non-functional characteristics.

The discovery functions regarding the functional characteristics and the classification functions regarding the non-functional characteristics of Security-as-a-Service (SecaaS) products are innovations introduced by our application, allowing an organization or individual to identify such products based on their requirements and preferences.

Keywords: *security, discovery, ranking, cloud computing, security as a service products, security mechanisms, web application*

1

Εισαγωγή

1.1 Προϊόντα Ασφάλειας-ως-Υπηρεσία

Η ραγδαία αύξηση της χρήσης του διαδικτύου από όλο και μεγαλύτερο μέρος του πληθυσμού και η μεταφορά όλο και περισσότερων υπηρεσιών στον ψηφιακό κόσμο, προϋποθέτει τη δημιουργία πλατφόρμων τροφοδοσίας υπηρεσιών, όπως το υπολογιστικό νέφος, τις οποίες οι χρήστες θα μπορούν να χρησιμοποιούν με ασφάλεια. Τα πληροφοριακά συστήματα εξελίσσονται τόσο σε όγκο όσο και σε πολυπλοκότητα, ενώ ταυτόχρονα βλέπουμε να αυξάνεται σημαντικά και ο όγκος των αναφορών που παράγονται από αυτά. Αυτό καθιστά ιδιαίτερα δύσκολη την παρακολούθηση και αναγνώριση των συμβάντων ασφαλείας που θέτουν σε κίνδυνο την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητα των πληροφοριακών συστημάτων. Τα παραπάνω δυσκολεύουν ακόμα περισσότερο για τις επιχειρήσεις, καθώς συνήθως δεν διαθέτουν προσωπικό με την κατάλληλη τεχνογνωσία και εμπειρία ώστε να διαχειριστεί αυτές τις καταστάσεις. Επιπλέον, οι επιθέσεις στο διαδίκτυο είναι πιο οργανωμένες καθώς και οι επιτιθέμενοι πιο επιδέξιοι, με αποτέλεσμα να μπορούν να εκμεταλλευτούν τις ευπάθειες των πληροφοριακών αυτών συστημάτων, προκαλώντας με αυτόν τον τρόπο προβλήματα σε αυτά, όπως να τα βγάλουν εκτός λειτουργίας ή να κλέψουν ευαίσθητα προσωπικά δεδομένα των χρηστών.

Για τον σκοπό αυτό δημιουργήθηκαν τα προϊόντα Ασφάλειας-ως-Υπηρεσίας (SecaaS). Ένα προϊόν SecaaS αναφέρεται σε λύσεις ασφάλειας που προσφέρονται ως υπηρεσία μέσω του διαδικτύου και ειδικότερα του υπολογιστικού νέφους. Οπότε, δεν αφορά ένα προϊόν που εγκαθίσταται και διαχειρίζεται τοπικά από τον χρήστη ή από τον διαχειριστή των πληροφοριακών συστημάτων μιας επιχείρησης [1]. Αυτό σημαίνει, ότι οι χρήστες ή οι επιχειρήσεις δεν χρειάζεται να αγοράσουν και να έχουν οι ίδιοι την ευθύνη για τη συντήρηση των συστημάτων ασφάλειας, αλλά μπορούν να αποκτήσουν αυτές τις υπηρεσίες από τρίτους παρόχους μέσω συνδρομής ή πληρωμής

κατά τη χρήση. Επίσης, οι χρήστες ή οι επιχειρήσεις δεν χρειάζεται να επενδύσουν σε επιπλέον υποδομή ή εξοπλισμό για την λειτουργία συστημάτων ασφαλείας διότι αυτά θα προσφέρονται ως υπηρεσία από τρίτα μέρη. Αυτό σημαίνει ότι οι επιχειρήσεις γλυτώνουν κόστος και χρόνο, ενώ απλοποιείται σε μεγάλο βαθμό η διαχείριση της ασφάλειας. Προφανώς τους παρόχους τους βαραίνει η σωστή διαμόρφωση των υπηρεσιών αυτών ώστε αυτές να λειτουργούν με τον αναμενόμενο τρόπο και να ικανοποιούν τους στόχους ασφάλειας της επιχείρησης ή του μεμονωμένου χρήστη. Οι υπηρεσίες αυτές είναι αρκετά ολοκληρωμένες με τεχνολογίες τελευταίας γενιάς και παρέχονται από αξιόπιστα τρίτα μέρη που έχουν εξειδίκευση στην παροχή προϊόντων ασφαλείας. Ένα ακόμα πλεονέκτημα των SecaaS είναι ότι διασφαλίζουν ότι οι πιο πρόσφατες ενημερώσεις ασφαλείας εφαρμόζονται σε όλα τα προστατευόμενα μέρη, μόλις αυτές γίνουν διαθέσιμες. Επιπλέον, παρέχουν παρακολούθηση και ειδοποιήσεις για συμβάντα ασφαλείας όλο το 24ωρο, όλες τις ημέρες χρόνου και έτσι η επιχείρηση διαθέτει έναν μηχανισμό ταχείας απόκρισης συμβάντων, μειώνοντας τον χρόνο διακοπής της λειτουργίας της.

1.2 Αντικείμενο Διπλωματικής

Πλέον, υπάρχουν αρκετά προϊόντα SecaaS με το καθένα να έχει διαφορετικά χαρακτηριστικά και δυνατότητες που μπορεί να προσφέρει. Έτσι, γίνεται κατανοητή η ανάγκη ύπαρξης πλατφόρμων, οι οποίες θα μπορούν να περιγράφουν με ακριβή και εκτεταμένο τρόπο αυτά τα προϊόντα και να προσφέρουν κατάλληλες υπηρεσίες δημοσίευσης, ανακάλυψης και ταξινόμησης τους σύμφωνα με τις ανάγκες του εκάστοτε χρήστη ή οργανισμού. Όμως, παρατηρήθηκε ότι υπάρχει έλλειψη τέτοιων πλατφόρμων στο διαδίκτυο. Έτσι, η παρούσα διπλωματική εργασία προσπαθεί να συμβάλει στη λύση αυτού του προβλήματος μέσω της ανάπτυξης σχετικής πλατφόρμας που παίρνει τη μορφή μιας εφαρμογής ιστού.

Τα πλεονεκτήματα και βασικά χαρακτηριστικά της πλατφόρμας που αναπτύχθηκε είναι ότι επιτρέπει στους παρόχους τη δημοσίευση των προϊόντων SecaaS που προσφέρουν, δίνοντας τους τη δυνατότητα να παρέχουν πλήρη περιγραφή των χαρακτηριστικών, λειτουργικών & μη λειτουργικών, των προϊόντων τους. Επιπλέον, οι χρήστες μπορούν μέσω της πλατφόρμας να ανακαλύπτουν αυτά τα προϊόντα με βάση τις ανάγκες τους ενώ παράλληλα μπορούν να τα ταξινομούν με βάση προτιμήσεις που οι ίδιοι έχουν ως προς ορισμένα κριτήρια που θεωρούν οι ίδιοι πιο σημαντικά. Οι ανάγκες των χρηστών εκφράζονται ως περιορισμοί στα λειτουργικά και μη λειτουργικά χαρακτηριστικά των προϊόντων SecaaS ενώ οι προτιμήσεις τους εκφράζονται με τη μορφή σχετικών βαρών στα μη λειτουργικά χαρακτηριστικά αυτών των προϊόντων.

Ουσιαστικά, μέσω της πλατφόρμας δημιουργείται ένα είδος αγοράς (marketplace) που επιτρέπει την έμμεση επικοινωνία ανάμεσα σε παρόχους και χρήστες/επιχειρήσεις, όπου οι πρώτοι δημοσιεύουν τα προϊόντα SecaaS τους με τα χαρακτηριστικά τους ενώ οι δεύτεροι επιλέγουν εκείνο το προϊόν SecaaS από τα προσφερόμενα που χρειάζονται ως λύση για την ασφάλεια των συστημάτων τους. Η δημοσίευση, δηλαδή η περιγραφή, και η ανακάλυψη αυτών των προϊόντων μέσω της προτεινόμενης εφαρμογής γίνονται μέσω μιας σημασιολογικής προσέγγισης, όπου τέτοιες προσεγγίσεις έχουν αποδειχθεί πως οδηγούν σε μεγαλύτερη ακρίβεια στην ανακάλυψη υπηρεσιών/προϊόντων [2].

1.3 Δομή της Διπλωματικής

Το υπόλοιπο της αναφοράς της διπλωματικής μας εργασίας δομείται ως εξής. Στο Κεφάλαιο 2 παρουσιάζονται και αναλύονται βασικές έννοιες, όπως το υπολογιστικό νέφος και τα προϊόντα ασφάλειας ως υπηρεσία, για την καλύτερη κατανόηση του υπολειπόμενου περιεχομένου της αναφοράς αλλά και την συνεισφοράς της διπλωματικής. Στο Κεφάλαιο 3 γίνεται μια ανάλυση σχετικών, με την παρούσα, εργασιών. Στο Κεφάλαιο 4 αναλύεται η διαδικασία ανάπτυξης της προτεινόμενης εφαρμογής ιστού και παρουσιάζονται τα βασικά αποτελέσματα της διαδικασίας αυτής. Στο Κεφάλαιο 5 παρουσιάζεται ο τρόπος εγκατάστασης και εκτέλεσης της εφαρμογής, ενώ παράλληλα γίνεται και επίδειξη της εφαρμογής μέσω σεναρίων χρήσης. Τέλος, στο Κεφάλαιο 6 ανακεφαλαιώνεται η συνεισφορά της παρούσας εργασίας και τα πλεονεκτήματα της ενώ παρέχονται μελλοντικές κατευθύνσεις για την επέκταση και βελτίωσή της.

2

Υπόβαθρο

Σε αυτό το κεφάλαιο παρέχεται το θεωρητικό υπόβαθρο της εργασίας. Αρχικά, θα αναφερθούμε στο υπολογιστικό νέφος παρέχοντας έναν ακριβή ορισμό του, τα βασικά χαρακτηριστικά του, τα πλεονεκτήματα του και τα είδη υπηρεσιών που προσφέρει. Έπειτα, θα μιλήσουμε για τα προϊόντα Ασφάλεια-ως-Υπηρεσία (SecaaS) δίνοντας τον ορισμό τους, τα πλεονεκτήματα και τα μειονεκτήματά τους και αναλύοντας τις κατηγορίες τους.

2.1 Υπολογιστικό Νέφος

2.1.1 Ορισμός Υπολογιστικού Νέφους

Ως υπολογιστικό νέφος ορίζουμε την κατ'απαίτηση, πανταχού παρούσα και βολική δικτυακή πρόσβαση σε μία κοινόχρηστη δεξαμενή διαμορφώσιμων υπολογιστικών πόρων (π.χ. δίκτυα, διακομιστές, αποθηκευτικοί χώροι, υπηρεσίες και εφαρμογές), που μπορούν να παρέχονται και να απελευθερώνονται γρήγορα με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδρασης με τον πάροχο υπηρεσιών [3]. Με το υπολογιστικό νέφος οι χρήστες και οι οργανισμοί μπορούν να έχουν πρόσβαση σε υπολογιστικούς πόρους, όπως αποθηκευτικό χώρο, λογισμικό και εφαρμογές, χωρίς να χρειάζεται να τους διαχειρίζονται τοπικά. Όλα αυτά παρέχονται ως υπηρεσίες, απαλλάσσοντας έτσι τους οργανισμούς από την ανάγκη συντήρησης υποδομών και εξοπλισμού.

2.1.2 Βασικά Χαρακτηριστικά

Παρακάτω αναφέρονται τα βασικά χαρακτηριστικά του υπολογιστικού νέφους:

- *Αυτοεξυπηρέτηση κατά παραγγελία*: οι χρήστες μπορούν να καταναλώνουν μονομερώς υπολογιστικές δυνατότητες, όπως χρόνος διακομιστή και αποθηκευτικό χώρο, αυτόματα χωρίς να απαιτείται η ανθρώπινη αλληλεπίδραση με κάθε πάροχο υπηρεσίας.
- *Απανταχού πρόσβαση (ubiquitous access)*: οι δυνατότητες είναι διαθέσιμες μέσω του δικτύου και η πρόσβαση σε αυτές γίνεται μέσω τυποποιημένων μηχανισμών που επιτρέπουν τη χρήση από ετερογενείς πλατφόρμες πελατών (π.χ., κινητά τηλέφωνα, ταμπλέτες, φορητοί υπολογιστές και σταθμοί εργασίας).

- *Πολλαπλή μίσθωση*: οι υπολογιστικοί πόροι του παρόχου συγκεντρώνονται για να εξυπηρετήσουν πολλούς χρήστες χρησιμοποιώντας ένα μοντέλο πολλαπλής μίσθωσης (multi-tenant model) με διαφορετικούς φυσικούς και εικονικούς πόρους, οι οποίοι εκχωρούνται και ανακατανέμονται ανάλογα με τη ζήτηση των χρηστών. Σημειώνεται πως αν και ο χρήστης δεν έχει έλεγχο ούτε γνώση της θέσης στην οποία βρίσκονται οι παρεχόμενοι πόροι, ίσως να μπορεί να καθορίσει τη θέση τους σε υψηλότερο επίπεδο αφαίρεσης (π.χ. χώρα, πολιτεία ή κέντρο δεδομένων). Παραδείγματα πόρων περιλαμβάνουν την αποθήκευση, επεξεργασία, μνήμη και εύρος ζώνης δικτύου.
- *Ταχεία ελαστικότητα*: οι δυνατότητες μπορούν να δεσμεύονται και να αποδεσμεύονται ελαστικά, σε ορισμένες περιπτώσεις αυτόματα, ώστε να κλιμακώνονται γρήγορα προς τα έξω (scale-out) και προς τα μέσα (scale-in) ανάλογα με τη ζήτηση. Στον χρήστη, οι δυνατότητες που είναι διαθέσιμες για παροχή συχνά φαίνονται απεριόριστες και μπορούν να ιδιοποιηθούν σε οποιαδήποτε ποσότητα ανά πάσα στιγμή.
- *Μετρούμενη υπηρεσία*: τα συστήματα νέφους ελέγχουν και βελτιστοποιούν αυτόματα τη χρήση των πόρων αξιοποιώντας μια δυνατότητα μέτρησης σε ένα επίπεδο αφαίρεσης κατάλληλο για τον τύπο της υπηρεσίας (π.χ. αποθήκευση, επεξεργασία, εύρος ζώνης και λογαριασμοί ενεργών χρηστών). Η χρήση των πόρων μπορεί να παρακολουθείται, ελέγχεται και αναφέρεται, παρέχοντας διαφάνεια τόσο για τον πάροχο όσο και για τον καταναλωτή της χρησιμοποιούμενης υπηρεσίας.

2.1.3 Βασικά Πλεονεκτήματα

Με βάση τα παραπάνω χαρακτηριστικά του υπολογιστικού νέφους, μπορούμε να συμπεράνουμε ότι τα βασικά πλεονεκτήματα του είναι τα παρακάτω:

- *Μείωση κόστους*: οι χρήστες και οι οργανισμοί, οι πελάτες δηλ. του υπολογιστικού νέφους, δεν χρειάζεται να επενδύσουν σε ακριβό εξοπλισμό ή υποδομές και πληρώνουν μόνο για τους πόρους που χρησιμοποιούν.
- *Ευκολία στην κλιμάκωση*: το υπολογιστικό νέφος επιτρέπει στους χρήστες να αυξάνουν ή να μειώνουν τους πόρους που δεσμεύουν κατ'απαίτηση ανάλογα με τις εκάστοτε ανάγκες τους. Ειδικότερα, οι μεγάλοι πάροχοι νέφους δίνουν την ψευδαίσθηση της διάθεσης άπειρων πόρων στους πελάτες τους, πράγμα που σημαίνει πως οι εφαρμογές των πελατών αυτών μπορούν να κλιμακώνονται σε έναν υπέρτατο βαθμό.
- *Πρόσβαση σε προηγμένη τεχνολογία*: οι χρήστες μπορούν να αποκτήσουν πρόσβαση σε υψηλής τεχνολογίας εφαρμογές, εργαλεία και υπηρεσίες χωρίς να χρειάζεται να τις αναπτύξουν οι ίδιοι ή να τις συντηρήσουν τοπικά.
- *Αυξημένη ευελιξία και αξιοπιστία*: οι υπηρεσίες νέφους προσφέρουν τη δυνατότητα για καλύτερη διαχείριση και ικανοποίηση των απαιτήσεων των χρηστών καθώς και για συνεχιζόμενη λειτουργία άνευ διακοπής (πχ. εφαρμογών που εκτελούνται στο νέφος).
- *Διαχείριση ενημερώσεων και συντηρήσεων*: οι πάροχοι νέφους αναλαμβάνουν τη διαχείριση των ενημερώσεων και της συντήρησης των υποδομών και εν γένει των προσφερόμενων πόρων, εξοικονομώντας με αυτόν τον τρόπο πόρους και χρόνο για τους χρήστες, οι οποίοι δεν χρειάζεται πλέον να προχωρήσουν σε τέτοιες ενέργειες διαχείρισης, που μπορεί να οδηγήσουν και σε σφάλματα αν δεν υπάρχει η αντίστοιχη εμπειρία στον οργανισμό τους.

- *Ασφάλεια δεδομένων & αγαθών*: οι πάροχοι νέφους προσφέρουν προηγμένα χαρακτηριστικά ασφαλείας για την προστασία των δεδομένων και οποιονδήποτε άλλων αγαθών μεταφέρονται στο νέφος από τους πελάτες τους.

2.1.4 Είδη Υπηρεσιών Νέφους

Τα είδη υπηρεσιών νέφους είναι τα εξής: Λογισμικό-ως-Υπηρεσία (Software-as-a-Service), Υποδομή-ως-Υπηρεσία (Infrastructure-as-a-Service) και Πλατφόρμα-ως-Υπηρεσία (Platform-as-a-Service).

Με το Λογισμικό-ως-Υπηρεσία (SaaS) παρέχεται η δυνατότητα στον χρήστη να χρησιμοποιεί απομακρυσμένα τις εφαρμογές του παρόχου, οι οποίες τρέχουν σε υποδομή νέφους. Οι εφαρμογές είναι προσβάσιμες είτε μέσω μιας διεπαφής χρήστη, όπως ένα πρόγραμμα περιήγησης ιστού, είτε μέσω μιας προγραμματιστικής διεπαφής (πχ. API). Ο χρήστης δεν διαχειρίζεται ούτε ελέγχει την υποδομή του νέφους, συμπεριλαμβανομένου το δίκτυο, τους διακομιστές, τα λειτουργικά συστήματα, τους αποθηκευτικούς χώρους, ακόμα και τις δυνατότητες μεμονωμένων εφαρμογών, με μια πιθανή εξαίρεση σε περιορισμένες ρυθμίσεις εφαρμογών που αφορούν συγκεκριμένους χρήστες. Συνεπώς, ένα βασικό πλεονέκτημα των υπηρεσιών αυτών είναι πως δεν εγκαθίσταται το λογισμικό τους στους υπολογιστές των χρηστών, επιβαρύνοντας τους με τακτικές επιδιορθώσεις και συχνές εκδόσεις. Αντ' αυτού, οι υπηρεσίες αυτές εκτελούνται στο νέφος και διατίθενται μέσω του διαδικτύου, με τον πάροχο να είναι υπεύθυνος για την τροφοδοσία και συντήρησή τους. Εκτός από τα ευέλικτα μοντέλα χρέωσής τους, οι υπηρεσίες αυτές έχουν την ικανότητα να κλιμακώνονται ανάλογα με το φόρτο εργασίας ώστε να εξασφαλίσουν ένα κατάλληλο και σταθερό επίπεδο υπηρεσίας προς τους χρήστες τους.

Δημοφιλή παραδείγματα υπηρεσιών SaaS είναι τα: Google Workspace, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting.

Με την Πλατφόρμα-ως-Υπηρεσία (PaaS) παρέχεται η δυνατότητα στον χρήστη να αναπτύξει στην υποδομή νέφους εφαρμογές που δημιούργησε ο ίδιος, ή απέκτησε από τρίτο μέρος και έχουν υλοποιηθεί χρησιμοποιώντας γλώσσες προγραμματισμού, βιβλιοθήκες και υπηρεσίες που υποστηρίζει ο πάροχος. Ο χρήστης δεν διαχειρίζεται ούτε ελέγχει την υποκείμενη υποδομή νέφους, συμπεριλαμβανομένων του δικτύου, των διακομιστών, λειτουργικά συστήματα ή αποθήκευση, αλλά έχει τον έλεγχο των εφαρμογών που αναπτύσσονται και ενδεχομένως των ρυθμίσεων διαμόρφωσης για το περιβάλλον φιλοξενίας εφαρμογών. Το προσφερόμενο περιβάλλον ανάπτυξης, το οποίο ελέγχει και συντηρεί ο πάροχος, μπορεί να περιλαμβάνει λειτουργικά συστήματα, βάσεις δεδομένων, μεσισμικό καθώς και εργαλεία ανάπτυξης εφαρμογών. Έτσι, ο χρήστης δεν χρειάζεται να πληρώσει τις άδειες για όλα τα παραπάνω και χρεώνεται μόνο με βάση τη χρήση του διατιθέμενου περιβάλλοντος. Επιπλέον, το συγκεκριμένο είδος υπηρεσίας νέφους παρέχει αυξημένη ασφάλεια, καθώς οι πάροχοι επενδύουν αρκετά σε αυτόν τον τομέα. Ακόμη, μπορεί να αυξήσει γρήγορα τις δυνατότητες του συστήματος σε περιόδους αιχμής (μέσω κλιμάκωσης) και να τις μειώσει αντίστοιχα ανάλογα με τις εκάστοτε ανάγκες. Δίνει πρόσβαση σε υπερσύγχρονο υλικό και λειτουργικά συστήματα, αλλά και σε εργαλεία ανάπτυξης εφαρμογών, ώστε οι προγραμματιστές να δημιουργούν τις δικές τους εφαρμογές. Τέλος, παρέχει κατάλληλη υποστήριξη για την συνεργατική ανάπτυξη λογισμικού ενώ επιτρέπει τη διασύνδεση με τοπικά εργαλεία

ανάπτυξης με δυνατότητα offline εργασίας και μετέπειτα συγχρονισμού σε περιπτώσεις καλής διαδικτυακής συνδεσιμότητας.

Παραδείγματα υπηρεσιών PaaS είναι τα: Amazon Web Services (AWS) Elastic Beanstalk, Windows Azure App Service, Heroku, Force.com, Google App Engine, Apache Stratos, Red Hat OpenShift

Με την Υποδομή-ως-Υπηρεσία (IaaS) έχουμε την παροχή επεξεργασίας, αποθήκευσης, δικτύων και άλλων βασικών υπολογιστικών πόρων με βάση τους οποίους ο χρήστης είναι σε θέση να αναπτύσσει και να εκτελεί λογισμικό, το οποίο μπορεί να περιλαμβάνει λειτουργικά συστήματα και εφαρμογές. Ο χρήστης δεν διαχειρίζεται ούτε ελέγχει την υποδομή νέφους, αλλά έχει τον έλεγχο των λειτουργικών συστημάτων, της αποθήκευσης και των εφαρμογών που αναπτύσσονται, και ενδεχομένως περιορισμένο έλεγχο επιλεγμένων στοιχείων δικτύωσης (π.χ. τείχη προστασίας του κεντρικού υπολογιστή). Έτσι παρέχονται και συνδυάζονται βασικοί πόροι υποδομής, όπως εικονικές μηχανές, αποθηκευτικοί χώροι, δίκτυα και διακομιστές, τους οποίους ο χρήστης μπορεί να χρησιμοποιήσει απομακρυσμένα μέσω διαδικτύου από οποιοδήποτε τερματικό ή κινητή συσκευή. Με αυτόν τον τρόπο ο χρήστης αποφεύγει το κόστος αγοράς και συντήρησης αυτών των πόρων, όπως ειπώθηκε και προηγουμένως. Όπως η υπηρεσία PaaS, έτσι και η υπηρεσία παρέχει αυξημένη ασφάλεια στους χρήστες της και δίνει πρόσβαση σε υπερσύγχρονο υλικό και λειτουργικά συστήματα. Ακόμη, παρέχει ένα μεγάλο εύρος πόρων με διαφορετικές δυνατότητες για να καλύψει τις ευρείες ανάγκες των οργανισμών για οποιοδήποτε φόρτο εργασίας. Επιπλέον, μειώνει τον χρόνο διακοπής λειτουργίας και επιτρέπει την άμεση αποκατάσταση από διακοπές λειτουργίας. Τέλος, για την πρόσβαση σε αυτήν την υπηρεσία αρκεί μια απλή σύνδεση στο διαδίκτυο.

Παραδείγματα υπηρεσιών IaaS είναι: DigitalOcean, Linode, Rackspace, AWS EC2, Microsoft Azure, Google Compute Engine (GCE)

Τα παραπάνω είδη υπηρεσιών καθιστούν το υπολογιστικό νέφος ένα ισχυρό εργαλείο για χρήστες και επιχειρήσεις με βάση τη λειτουργικότητα και τα πλεονεκτήματα που προσφέρουν, ικανοποιώντας μια μεγάλη γκάμα απαιτήσεων και προτιμήσεων των δυνητικών πελατών του νέφους.

2.2 Ασφάλεια-ως-Υπηρεσία (SecaaS)

2.2.1 Ορισμός SecaaS

Ως Ασφάλεια-ως-Υπηρεσία (SecaaS) ορίζουμε ένα μοντέλο παροχής υπηρεσιών ασφαλείας μέσω του διαδικτύου, το οποίο επιτρέπει στους χρήστες και τις επιχειρήσεις να αποκτούν και να χρησιμοποιούν λύσεις ασφαλείας χωρίς να χρειάζεται να διατηρούν ή να διαχειρίζονται τοπικά συστήματα ασφάλειας και υποδομές. Στην ουσία, οι λύσεις SecaaS παρέχονται ως εξωτερική υπηρεσία από τρίτους παρόχους, επιτρέποντας την απομακρυσμένη προστασία των δεδομένων και των συστημάτων από απειλές, χωρίς την ανάγκη εσωτερικής υποδομής ή εξειδικευμένου προσωπικού, το οποίο θα επιβαρύνεται με έξτρα εργασίες, όπως είναι η εγκατάσταση και συντήρηση των προϊόντων ασφαλείας σε τοπική υποδομή [1].

2.2.2 Πλεονεκτήματα SecaaS

Τα προϊόντα SecaaS παρέχουν μια σειρά από πλεονεκτήματα στους χρήστες, τα οποία αναλύονται παρακάτω:

- *Οικονομία κλίμακας*: αυτό σημαίνει ότι οι επιχειρήσεις χρησιμοποιούν υπηρεσίες ασφάλειας μέσω συνδρομής ή πληρωμής, χωρίς να απαιτείται επένδυση σε υποδομές ασφαλείας ή εξοπλισμό, μειώνοντας το κόστος. Επιπλέον, η κλιμάκωση της υπηρεσίας είναι υπό την ευθύνη του παρόχου, πράγμα το οποίο δίνει ακόμα ένα συγκριτικό πλεονέκτημα στις επιχειρήσεις-πελάτες, με βάση το γεγονός πως οι υπηρεσίες ασφάλειας θα κλιμακώνονται με βάση την ανάπτυξη (growth) ενός οργανισμού καθώς και την επέκταση και μεγέθυνση των βασικών του workloads. Και σε αυτή την περίπτωση, η κλιμάκωση πραγματοποιείται χωρίς την ανάγκη επένδυσης σε κάποια υποδομή από την πλευρά του πελάτη.
- *Ευκολία και ευελιξία*: ένα προϊόν SecaaS επιτρέπει στους χρήστες να προσθέτουν ή να αφαιρούν υπηρεσίες ασφάλειας ανάλογα με τις ανάγκες τους. Είναι επίσης εύκολο να προσαρμοστεί στις αλλαγές του οργανισμού ή της επιχείρησης καθώς και να διαμορφωθεί με βάση τις ανάγκες του/της.
- *Αναβάθμιση και συντήρηση*: η παρακολούθηση, αναβάθμιση και βελτίωση των λύσεων ασφαλείας αναλαμβάνονται από τον πάροχο της υπηρεσίας, μειώνοντας το φόρτο εργασίας των εσωτερικών ομάδων της επιχείρησης.
- *Αναγνωρισμένα επίπεδα ασφάλειας*: οι πάροχοι SecaaS συχνά παρέχουν προηγμένα επίπεδα ασφαλείας που ίσως να είναι δύσκολο ή ακριβό να αναπτυχθούν εσωτερικά σε έναν οργανισμό, ειδικότερα όταν αυτός δεν έχει τον απαιτούμενο προϋπολογισμό και ικανότητες. Αυτό δικαιολογείται από το γεγονός πως οι ενσωματωμένοι μηχανισμοί και υπηρεσίες ασφάλειας υλοποιούνται με αυστηρά πρότυπα και χρησιμοποιούν cutting-edge τεχνολογίες και μεθόδους ενώ ο πλουραλισμός των διαφορετικών λειτουργιών ασφάλειας που παρέχονται οδηγεί πράγματι σε υψηλά επίπεδα ασφάλειας καλύπτοντας οποιαδήποτε περίπτωση ή περιστατικό.
- *Παγκόσμια κάλυψη και διαθεσιμότητα*: οι υπηρεσίες ασφαλείας είναι διαθέσιμες παγκοσμίως και μπορούν να προστατεύουν δεδομένα και συστήματα από οποιαδήποτε γεωγραφική τοποθεσία.
- *Συμμόρφωση*: οι πάροχοι SecaaS συνήθως συμμορφώνονται με διεθνείς κανονισμούς και πρότυπα ασφαλείας, προσφέροντας εγγυήσεις συμμόρφωσης χωρίς πρόσθετο φόρτο για τον πελάτη.

2.2.3 Μειονεκτήματα SecaaS

Εκτός από πλεονεκτήματα όμως, τα προϊόντα SecaaS έχουν και κάποια μειονεκτήματα, τα οποία αναλύονται παρακάτω:

- *Ασφάλεια δεδομένων και απόρρητο*: παρόλο που αυτό αποτελεί και πλεονέκτημα, η αποθήκευση δεδομένων σε τρίτους δεν παύει να ενέχει τον κίνδυνο παραβίασης ή υποκλοπής αυτών. Εκτός από τα προηγούμενα, οι χρήστες δεν μπορούν να είναι σίγουροι για το ποιοι έχουν πρόσβαση σε αυτά τα δεδομένα, αν και οι σοβαροί πάροχοι εφαρμόζουν αυστηρά μέτρα ασφαλείας. Σε αυτό το σημείο θα πρέπει να αναφερθεί πως είναι αρκετά

πιθανό κάποιοι πάροχοι να μην εφαρμόζουν αυστηρά μέτρα ασφαλείας στο εσωτερικό τους και έτσι να θέτουν σε κίνδυνο τα δεδομένα των χρηστών τους.

- *Εξάρτηση από τον πάροχο*: η επιχείρηση εξαρτάται πλήρως από τον πάροχο για τη λειτουργία των υπηρεσιών ασφαλείας. Αν ο πάροχος έχει προβλήματα ή διακοπεί η υπηρεσία, τότε μπορεί να επηρεαστεί σε κριτικό επίπεδο η ασφάλεια της επιχείρησης, ειδικότερα αν στηρίζεται εξ ολοκλήρου στην παρεχόμενη υπηρεσία ασφαλείας.
- *Περιορισμένη εξατομίκευση*: παρόλο που οι υπηρεσίες SecaaS παρέχουν γενικές λύσεις ασφαλείας, μπορεί να μην είναι πλήρως προσαρμοσμένες στις ιδιαίτερες ανάγκες κάθε επιχείρησης.
- *Προβλήματα σύνδεσης*: η ασφάλεια της επιχείρησης μπορεί να επηρεαστεί από διακοπές της σύνδεσης της στο διαδίκτυο καθώς η κατανάλωση των προϊόντων SecaaS βασίζεται σε αυτό.
- *Αναγνώριση και αντιμετώπιση σύνθετων απειλών*: σε ορισμένες περιπτώσεις η αντιμετώπιση πολύπλοκων ή νέων τύπων επιθέσεων μπορεί να είναι λιγότερο αποτελεσματική, δεδομένου ότι οι πάροχοι προσφέρουν έτοιμες λύσεις που δεν μπορούν πάντα να προσαρμοστούν άμεσα στις εξελισσόμενες απειλές. Αυτό βέβαια εξαρτάται από το είδος της λύσης και τις τεχνολογίες στις οποίες στηρίζεται. Επίσης, θα πρέπει να ληφθεί υπόψιν πως οι πάροχοι συνήθως ανιχνεύουν συνεχώς την εξέλιξη των απειλών αυτών ή νέες απειλές ώστε να βελτιώνουν τα προϊόντα ασφαλείας τους.

2.2.4 Κατηγορίες SecaaS

Σύμφωνα με την Cloud Security Alliance (CSA) [4] οι κατηγορίες των προϊόντων SecaaS είναι οι εξής:

- *Διαχείριση Πληροφοριών και Συμβάντων Ασφαλείας (Security Information & Event Management (SIEM)):* η κατηγορία αυτή προσφέρει ένα σύνολο εργαλείων και υπηρεσιών που επιτρέπουν στις επιχειρήσεις να συλλέγουν, να αναλύουν και διαχειρίζονται δεδομένα σχετικά με την ασφάλειά τους σε πραγματικό χρόνο. Οι λειτουργίες αυτών των προϊόντων περιλαμβάνουν τη συλλογή δεδομένων, την κατηγοριοποίηση και κανονικοποίηση δεδομένων, την ανάλυση, διαχείριση και αντιμετώπιση συμβάντων και απειλών, την ανίχνευση απειλών σε πραγματικό χρόνο, την αναφορά και καταγραφή των συμβάντων και τη διαχείριση ειδοποιήσεων σε περίπτωση κάποιου συμβάντος. Οι μηχανισμοί ασφάλειας που προσφέρει περιλαμβάνουν την αναγνώριση και αποτροπή επιθέσεων, την αυθεντικοποίηση και τον έλεγχο πρόσβασης, την ενσωμάτωση με άλλες λύσεις ασφαλείας, τη παροχή αναφορών συμμόρφωσης και αρχείων ελέγχου καθώς και την κρυπτογράφηση των δεδομένων που συλλέγονται από αυτό.
- *Συνέχιση Επιχειρησιακής Λειτουργίας και Ανάκτηση από Καταστροφή (Business Continuity and Disaster Recovery (BCDR)):* η κατηγορία αυτή προσφέρει ένα σύνολο υπηρεσιών και εργαλείων που επιτρέπουν στις επιχειρήσεις να διασφαλίσουν τη συνέχεια των επιχειρηματικών τους λειτουργιών και την αποκατάσταση των δεδομένων και υπηρεσιών τους σε περίπτωση καταστροφών ή σημαντικού προβλήματος (όπως φυσικές καταστροφές, κυβερνοεπιθέσεις, αποτυχίες υποδομών κλπ.). Οι λειτουργίες των προϊόντων αυτής της κατηγορίας περιλαμβάνουν την ανάκτηση δεδομένων, τη διαχείριση αντιγράφων

ασφαλείας, την αποκατάσταση εφαρμογών και υπηρεσιών, τον εντοπισμό καταστροφών και τη διασφάλιση της συνεχούς λειτουργίας της επιχείρησης. Οι μηχανισμοί ασφαλείας που προσφέρει περιλαμβάνουν την κρυπτογράφηση δεδομένων, την αυθεντικοποίηση και έλεγχο πρόσβασης, τις δοκιμές ανάκτησης, την ανάκτηση απώλειας δεδομένων, την απομόνωση δεδομένων, τα τείχη προστασίας και τη συμμόρφωση με τους κανονισμούς.

- *Διαχείριση Ταυτοτήτων και Πρόσβασης (Identity and Access Management):* η κατηγορία αυτή διασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε συγκεκριμένα δεδομένα και πόρους. Οι λειτουργίες της περιλαμβάνουν τη διαχείριση ταυτοτήτων, τις πολιτικές πρόσβασης, τον έλεγχο ταυτότητας και την εξουσιοδότηση, τον έλεγχος πρόσβασης, τη διαχείριση δικαιωμάτων χρηστών και ομάδων καθώς και την επαλήθευση πολιτικών πρόσβασης. Οι μηχανισμοί ασφάλειας που προσφέρει περιλαμβάνουν την κρυπτογράφηση και διαχείριση των διαπιστευτηρίων πρόσβασης, την αυθεντικοποίηση χρηστών, τον έλεγχο πρόσβασης, και την καταγραφή (logging) κάθε προσπάθειας πρόσβασης είτε είναι επιτυχημένη, είτε αποτυχημένη.
- *Πρόληψη Απώλειας Δεδομένων (Data Loss Prevention):* η κατηγορία αυτή αφορά τη χρήση εργαλείων και πολιτικών που βοηθούν στην αποφυγή της διαρροής, διαγραφής ή κλοπής δεδομένων. Οι λειτουργίες της περιλαμβάνουν την αναγνώριση ευαίσθητων δεδομένων, τις πολιτικές πρόληψης απώλειας δεδομένων, τη προστασία δεδομένων, την αποτροπή αποστολής ευαίσθητων δεδομένων, τη καταγραφή και την ανάλυση συμβάντων καθώς και τη συμμόρφωση με τα πρότυπα. Οι μηχανισμοί ασφάλειας περιλαμβάνουν την κρυπτογράφηση δεδομένων, την επιβολή πολιτικών πρόσβασης, την προστασία εξωτερικών συσκευών καθώς και την αναγνώριση ευαίσθητου περιεχομένου και μη εξουσιοδοτημένων προσπαθειών πρόσβασης σε δεδομένα.
- *Κρυπτογράφηση (Encryption):* η κατηγορία αυτή εξασφαλίζει ότι τα δεδομένα παραμένουν εμπιστευτικά, αποτρέποντας τη μη εξουσιοδοτημένη ανάγνωση και αποκάλυψή τους και διασφαλίζοντας τη συμμόρφωση με κανονιστικά πρότυπα. Οι λειτουργίες της περιλαμβάνουν την κρυπτογράφηση των δεδομένων, των αρχείων και των αντίγραφων ασφάλειας και τη διαχείριση των κλειδιών κρυπτογράφησης. Οι μηχανισμοί ασφάλειας περιλαμβάνουν αλγόριθμους κρυπτογράφησης, χρήση συστημάτων διαχείρισης κλειδιών για την ασφαλή αποθήκευση και διαχείριση των κρυπτογραφικών κλειδιών και ανάπτυξη και διαχείριση ψηφιακών πιστοποιητικών που επιτρέπουν την αυθεντικοποίηση και την ασφαλή ανταλλαγή κλειδιών
- *Ασφάλεια Ηλεκτρονικού Ταχυδρομείου (Email Security):* η κατηγορία αυτή αφορά την προστασία των επιχειρήσεων από απειλές που σχετίζονται με τα email, όπως κακόβουλα συνημμένα & ιοί, phishing & spam email, και άλλες επιθέσεις που εκμεταλλεύονται το ηλεκτρονικό ταχυδρομείο ως μέσο εξάπλωσης κακόβουλης δραστηριότητας. Οι λειτουργίες της περιλαμβάνουν το φιλτράρισμα ανεπιθύμητης αλληλογραφίας, την κρυπτογράφηση email, την ανίχνευση και πρόληψη phishing και social engineering, την ανίχνευση κακόβουλων συνημμένων και την αυθεντικοποίηση χρηστών για είσοδο στην υπηρεσία email. Οι μηχανισμοί ασφάλειας περιλαμβάνουν κρυπτογράφηση των email, την εκπαίδευση προσωπικού, την ανίχνευση phishing και κακόβουλου περιεχομένου και την καραντίνα.

- *Ασφάλεια Δικτύου (Network Security):* η κατηγορία αυτή δίνει τη δυνατότητα στις επιχειρήσεις να διασφαλίσουν την ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των δεδομένων και της επικοινωνίας τους στο δίκτυο, χρησιμοποιώντας προηγμένες τεχνολογίες και μηχανισμούς ασφαλείας. Οι λειτουργίες της περιλαμβάνουν το τείχος προστασίας, τη πρόληψη και αντιμετώπιση επιθέσεων, τη χρήση ιδιωτικών δικτύων (VPN), την ασφάλεια DNS, τον έλεγχος πρόσβασης στο δίκτυο, τη προστασία των εφαρμογών που εκτελούνται στο δίκτυο μέσω WAF (Web Application Firewalls) και τη παρακολούθηση του δικτύου. Οι μηχανισμοί ασφάλειας περιλαμβάνουν την ανίχνευση κακόβουλης κίνησης, την κρυπτογράφηση της δικτυακής κίνησης και την αυτοματοποιημένη αντίδραση σε επιθέσεις
- *Αποτίμηση Ασφάλειας (Security Assessment):* η κατηγορία αυτή βοηθά τις επιχειρήσεις να αξιολογήσουν και να εντοπίσουν τις αδυναμίες, τα κενά και τις ευπάθειες στις υποδομές και τις πολιτικές ασφαλείας τους. Οι λειτουργίες της περιλαμβάνουν τη σάρωση των συστημάτων και των δικτύων για εντοπισμό ευπαθειών, την αξιολόγηση πολιτικών, διαδικασιών ασφαλείας και της συμμόρφωσης σε κανονισμούς και κινδύνους, την αξιολόγηση ασφάλειας υποδομών και δικτύου καθώς και τις δοκιμές διείσδυσης. Οι μηχανισμοί ασφάλειας περιλαμβάνουν την ύπαρξη αυτόματων εργαλείων σάρωσης ευπαθειών, τη διαχείριση και παρακολούθηση συμβάντων και δραστηριότητας στο δίκτυο καθώς και στρατηγικές για τη διαχείριση του κινδύνου.
- *Ασφάλεια Ιστού (Web Security)*: η κατηγορία αυτή αφορά την προστασία των διαδικτυακών εφαρμογών, ιστοσελίδων και των υποδομών που συνδέονται με αυτές από διάφορες απειλές και επιθέσεις. Καθώς οι περισσότερες σύγχρονες εφαρμογές και υπηρεσίες λειτουργούν μέσω του διαδικτύου, η ασφάλεια του ιστού είναι απαραίτητη για την προστασία των χρηστών, των δεδομένων τους και των εταιρικών υποδομών από απειλές, όπως η κλοπή δεδομένων, οι επιθέσεις Denial of Service (DoS), η έκχυση SQL, το cross-site scripting (XSS) και άλλες ευπάθειες/απειλές. Οι λειτουργίες της περιλαμβάνουν την πρόληψη και την αντιμετώπιση επιθέσεων, τη χρήση ιδιωτικών δικτύων (VPN), την ασφάλεια DNS, τον έλεγχο πρόσβασης στο δίκτυο, τη προστασία των εφαρμογών που εκτελούνται στο δίκτυο μέσω WAF (Web Application Firewalls), την ασφάλεια API, το φιλτράρισμα διαδικτυακής κίνησης, τη παρακολούθηση δικτύου και την ανίχνευση κακόβουλης κίνησης. Οι μηχανισμοί ασφάλειας περιλαμβάνουν τη σάρωση των συστημάτων και του δικτύου για ανίχνευση ευπαθειών, την ανίχνευση μη τυπικής δραστηριότητας, την επαναφορά υπηρεσιών, τις αναφορές καθώς και την ανάκτηση και την ανάλυση δεδομένων.
- *Διαχείριση Παραβιάσεων (Intrusion Management):* η κατηγορία αυτή αναφέρεται στην ικανότητα να εντοπίζονται, να αναλύονται, να καταγράφονται και να υπάρχει απόκριση σε εισβολές ή ύποπτες δραστηριότητες που ενδέχεται να παραβιάσουν την ασφάλεια ενός οργανισμού. Οι παραβιάσεις μπορεί να περιλαμβάνουν επιθέσεις από εξωτερικούς ή εσωτερικούς κακόβουλους χρήστες. Οι λειτουργίες της περιλαμβάνουν την ανίχνευση εισβολής και παραβίασης κάποιου συστήματος, την ανάλυση παραβιάσεων, την ανίχνευση κακόβουλης κίνησης στο δίκτυο, την αυτόματη απάντηση στις παραβιάσεις, την αναφορά και καταγραφή περιστατικών, την ανάκτηση και επαναφορά από κάποια παραβίαση ή καταστροφή, τη συμμόρφωση με κανονισμούς ασφάλειας, την εκπαίδευση χρηστών και τη ανάλυση της στρατηγικής ασφάλειας ώστε να αξιολογηθεί η αποτελεσματικότητα της. Οι μηχανισμοί ασφάλειας περιλαμβάνουν την ανάλυση συμπεριφοράς των χρηστών, την

αποστολή ειδοποιήσεων μετά από την ανίχνευση παραβίασης και την ενημέρωση με νέες απειλές.

3

Σχετικές Εργασίες

Σε αυτό το κεφάλαιο θα αναφερθούμε σε σχετικές ερευνητικές εργασίες και σημεία αγοράς (marketplaces) προϊόντων SecaaS. Για κάθε σχετική εργασία ή σημείο αφοράς θα δοθεί μια σύντομη περιγραφή, τα θετικά και αρνητικά, ενώ θα γίνει και μια σύγκριση της/του με την παρούσα εργασία.

3.1 Ερευνητικές Εργασίες

Σε αυτή την ενότητα αναλύονται ερευνητικές εργασίες που ασχολούνται με τη μοντελοποίηση και κατηγοριοποίηση των προϊόντων SecaaS διότι θεωρούνται σχετικές με την παρούσα εργασία. Επίσης, θεωρούνται σχετικές και αναλύονται εργασίες που εστιάζουν στη χρήση σημασιολογικών προσεγγίσεων για περιγραφή και ανακάλυψη διαφόρων οντοτήτων (όπως υπηρεσίες ιστού).

3.1.1 A Taxonomy of Security as a Service

Η εργασία 'A Taxonomy of Security as a Service' (Ταξινόμηση Υπηρεσιών Security as a Service) των Marwa Elsayed and Mohammad Zulkernine [5] , παρουσιάζει μια ολοκληρωμένη ταξινόμηση των προϊόντων SecaaS και αναλύει το πόσο σημαντική είναι αυτή. Σύμφωνα με τους συγγραφείς της εργασίας, η ταξινόμηση επιτρέπει την κατανόηση της εξέλιξης και των τάσεων σε αυτόν τον ερευνητικό τομέα, καθώς και την εξαγωγή συμπερασμάτων σχετικά με την υπάρχουσα εργασία σε σχέση με τρεις κύριες διαστάσεις: λειτουργία υπηρεσίας, λύση ασφάλειας και απειλή. Υπό αυτή την έννοια, η προτεινόμενη ταξινόμηση βοηθά τους χρήστες SecaaS και τους ερευνητές να αποκτήσουν σαφή και ολοκληρωμένη εικόνα σχετικά με τη λειτουργία και το σχεδιασμό κάθε εργασίας/προτεινόμενης υπηρεσίας που περιλαμβάνει το μοντέλο παράδοσης, το μοντέλο ανάπτυξης και τις υπεύθυνες οντότητες για τη λειτουργία της προτεινόμενης υπηρεσίας. Βοηθά επίσης τους χρήστες να αντιληφθούν τον μηχανισμό ασφάλειας και το σχέδιο άμυνας που χρησιμοποιεί κάθε προσέγγιση για την επίτευξη συγκεκριμένης απαίτησης ασφάλειας. Τέλος, η ταξινόμηση προσδιορίζει την επιφάνεια επίθεσης και τις μεθόδους των απειλών ασφαλείας που στοχεύει να μετριάσει η κάθε εργασία.

Η ταξινόμηση γίνεται με βάση 3 διαστάσεις: τη λειτουργία της υπηρεσίας, τη λύση ασφάλειας που προσφέρει και την απειλή ασφάλειας που αντιμετωπίζει. Επίσης, αναφέρεται στις τάσεις που

παρατηρούνται στην έρευνα πάνω στον τομέα της ασφάλειας ως υπηρεσία. Αυτό γίνεται από την άποψη των απειλών που στοχεύουν να μετριάσουν οι υπηρεσίες αυτές και τους μηχανισμούς ασφάλειας που υιοθετούν.

Τα θετικά της παραπάνω εργασίας είναι η λεπτομερέστατη ανάλυση της ταξινόμησης των προϊόντων SecaaS με βάση τα χαρακτηριστικά τους που επιδεικνύει διάφορες πλευρές που κάποιος πρέπει να εστιάσει για την επιλογή τους. Επιπλέον, η ταξινόμηση αυτή θεωρητικά καλύπτει όλα τα προϊόντα SecaaS που υπήρχαν μέχρι την περίοδο δημοσίευσης της εργασίας. Ως αρνητικό θα μπορούσαμε να αναφέρουμε ότι η παραπάνω εργασία δεν ασχολείται με τη δημοσίευση τέτοιων προϊόντων. Αντιθέτως, η παρούσα εργασία (της διπλωματικής) ασχολείται, εκτός από την ταξινόμηση, και με τη δημοσίευση και την ανακάλυψη των υπηρεσιών SecaaS.

3.1.2 Towards Security as a Service (SecaaS): on the modeling of Security Services for Cloud Computing

Η εργασία ‘Towards Security as a Service (SecaaS): on the modeling of Security Services for Cloud Computing’ (Προς τις Υπηρεσίες Security as a Service: Μοντελοποίηση των Υπηρεσιών Ασφάλειας για το Υπολογιστικό Νέφος) των Angelo Furfaro, Alfredo Garro, Andrea Tundis [6] ασχολείται με τη μοντελοποίηση των υπηρεσιών ασφαλείας. Συγκεκριμένα, η εργασία αυτή προτείνει μια διαδικασία για τον σχεδιασμό προϊόντων SecaaS που βασίζεται σε 3 φάσεις:

- *εντοπισμός υπηρεσιών ασφαλείας*, η οποία ασχολείται με τον εντοπισμό εννοιολογικών μοντέλων υπηρεσιών ασφαλείας,
- *ορισμός λύσεων σχεδιασμού*, η οποία αφορά τον ορισμό υποψήφιων λύσεων σχεδιασμού και
- *ανάλυση λύσεων σχεδιασμού*, η οποία προσανατολίζεται στην ανάλυση, σύγκριση και επιλογή λύσεων που ενδέχεται να ληφθούν υπόψη για τις επόμενες φάσεις αναλυτικού σχεδιασμού και υλοποίησης ενός προϊόντος SecaaS.

Με αυτόν τον τρόπο, η εργασία αυτή προτείνει κάποια βασικά χαρακτηριστικά των προϊόντων SecaaS, τα οποία χρησιμοποιεί και η παρούσα διπλωματική εργασία. Τα χαρακτηριστικά τα οποία προτείνει η εξεταζόμενη εργασία είναι: μοντέλο διάταξης, μοντέλο παράδοσης, πάροχος υπηρεσίας, μηχανισμοί ασφάλειας, μοντέλο κόστους και κατηγορία προϊόντος.

Η δική μας εργασία χρησιμοποιεί όλα τα παραπάνω χαρακτηριστικά, αλλά χρησιμοποιεί και επιπλέον χαρακτηριστικά για να καλύψει και άλλες σχετικές πλευρές. Αυτά τα χαρακτηριστικά είναι: μη λειτουργικές εγγυήσεις, είδη προσφερόμενης προστασίας, ιδιότητες ασφάλειας, αντικείμενα που προστατεύονται, απειλές που αντιμετωπίζονται, περιορισμοί, πληροφορίες για το αν το προϊόν διατίθεται δωρεάν και για πόσο χρονικό διάστημα, τρόπος χρήσης προϊόντος, τρόπος χρήσης προϊόντος, σημεία αγοράς και υποστήριξη. Όπως είναι φανερό, η παρούσα εργασία υπερτερεί σε αυτόν τον τομέα.

Τα θετικά της αναλυόμενης εργασίας είναι το μοντέλο περιγραφής προϊόντων SecaaS που αυτή προσφέρει. Έτσι μιλάμε για ένα μοντέλο περιγραφής των προϊόντων αυτών που μπορεί να χρησιμοποιηθεί για τη δημοσίευση τους, δηλαδή παράγονται προσδιορισμοί των προϊόντων που έπειτα δημοσιεύονται σε κάποιο αποθετήριο. Δεν ασχολείται καθόλου με την ταξινόμηση των

προϊόντων SecaaS. Αντιθέτως, η παρούσα διπλωματική εργασία ασχολείται και με την ταξινόμηση και με την ανακάλυψη προϊόντων SecaaS, εκτός από τη δημοσίευσή τους.

3.1.3 Σημασιολογική προσέγγιση

Ένα ακόμα σημαντικό θέμα με το οποίο ασχολείται η παρούσα διπλωματική σε πρακτικό επίπεδο είναι η σημασιολογική προσέγγιση για περιγραφή και ανακάλυψη διαφόρων οντοτήτων, μέσω της οποίας γίνεται η ανακάλυψη των προϊόντων SecaaS [7] [8]. Στον τομέα αυτόν έχει γίνει πολύ μεγάλη έρευνα όλα τα προηγούμενα χρόνια [9] [10]. Η σημασιολογική αναζήτηση είναι μια τεχνολογία ανάκτησης πληροφοριών που ερμηνεύει τη σημασία των λέξεων και των φράσεων και αποτελεί ένα σύνολο δυνατοτήτων των μηχανών αναζήτησης, που περιλαμβάνει την κατανόηση των λέξεων με βάση την πρόθεση του χρήστη και το πλαίσιο της αναζήτησης. Τα αποτελέσματα μιας σημασιολογικής αναζήτησης επιστρέφουν περιεχόμενο που ταιριάζει με τη σημασία ενός αιτήματος, σε αντίθεση με μια (δομική – structural) προσέγγιση που κοιτάει μόνο τη δομή και το κυριολεκτικό ταίριασμα του περιεχομένου. Αυτός ο τύπος αναζήτησης έχει σκοπό να βελτιώσει την ποιότητα των αποτελεσμάτων αναζήτησης, ερμηνεύοντας τη φυσική γλώσσα ακριβώς και στο πλαίσιο της αναζήτησης. Η σημασιολογική αναζήτηση επιτυγχάνει αυτόν τον στόχο, αντιστοιχώντας την πρόθεση αναζήτησης με τη σημασιολογική έννοια, με τη βοήθεια τεχνολογιών, όπως η μηχανική μάθηση (machine learning), η τεχνητή νοημοσύνη (artificial intelligence), η επεξεργασία φυσικής γλώσσας (natural language processing) και ο σημασιολογικός ιστός (semantic web).

Τα αρνητικά αυτής της προσέγγισης είναι ότι αυξάνουν την πολυπλοκότητα της υλοποίησης, καθώς ναι μεν μειώνεται η πολυπλοκότητα και η ακρίβεια που απαιτείται από τη μεριά του χρήστη, όμως η σημασιολογική ανάλυση και επέκταση των ερωτημάτων καθώς και το σημασιολογικό τους ταίριασμα θα πρέπει να γίνει στη μεριά του προγράμματος που θα κληθεί να απαντήσει σε αυτά. Επίσης, λόγω του προηγούμενου μπορούμε να πούμε ότι αυξάνεται ο χρόνος απόκρισης και η κατανάλωση υπολογιστικών πόρων.

Η παρούσα διπλωματική εργασία έχει υιοθετήσει την προσέγγιση αυτή για να επιτύχει καλύτερη ακρίβεια στην ανακάλυψη των προϊόντων SecaaS.

3.2 Σημεία Αγοράς

Υπάρχουν σημεία αγοράς προϊόντων SecaaS, τα οποία είναι τα παρακάτω:

- AWS - https://aws.amazon.com/marketplace/search?FULFILLMENT_OPTION_TYPE=SAAS&filters=FULFILLMENT_OPTION_TYPE (Ημερομηνία πρόσβασης: 15/1/2025): Η Amazon προσφέρει δυνατότητα δημοσίευσης προϊόντων, αναζήτησης με βάση αρκετά κριτήρια, όπως εκδότης, ύπαρξη δοκιμαστικής έκδοσης κ.α. και ταξινόμησης με περιορισμένη λίστα κριτηρίων.
- GCP - https://console.cloud.google.com/marketplace/browse?filter=solution-type:saas&inv=1&invt=Abm7LA (Ημερομηνία πρόσβασης: 15/1/2025): Η Google προσφέρει δυνατότητα φιλτραρίσματος προϊόντων με βάση μόνο 3 κριτήρια (κατηγορία, τύπος και τιμή) και δυνατότητα αναζήτησης με λέξεις-κλειδιά. Επιπλέον,

παρέχει δυνατότητα δημοσίευσης ενός προϊόντος, αλλά δεν παρέχει δυνατότητα ταξινόμησης.

- Microsoft Azure - https://azuremarketplace.microsoft.com/en-us/marketplace/apps?page=1&filters=saas (Ημερομηνία πρόσβασης: 15/1/2025): Η Microsoft προσφέρει δυνατότητα δημοσίευσης και αναζήτησης προϊόντων με βάση συγκεκριμένα κριτήρια, όπως λειτουργικό σύστημα, εκδότης, ύπαρξη δοκιμαστικής έκδοσης κ.α.

Οι ιστότοποι που αναφέρονται παραπάνω προσφέρουν μια μεγάλη ποικιλία από SecaaS προϊόντα, τα οποία μπορεί να ανακαλύψει ένας χρήστης, όμως δεν προσφέρουν στον χρήστη τη δυνατότητα να αναζητήσει προϊόντα με βάση κάποια συγκεκριμένα χαρακτηριστικά του ίδιου του προϊόντος. Επιπλέον, θα πρέπει να πούμε ότι στα σημεία αγοράς που αναφέρονται παραπάνω, έχουμε να κάνουμε με γενικά προϊόντα και όχι εξειδικευμένα προϊόντα SecaaS. Οπότε, ο χρήστης θα πρέπει να επιλέξει την κατηγορία της ασφάλειας για να τα εντοπίσει. Τέλος, τα φίλτρα για το ταίριασμα είναι αρκετά περιορισμένα και η ταξινόμηση γίνεται με βάση περιορισμένο αριθμό κριτηρίων. Επισημαίνουμε ακόμα πως δεν υποστηρίζεται σημασιολογική αναζήτηση των προϊόντων SecaaS.

Η παρούσα εργασία δεν δίνει τη δυνατότητα στον χρήστη να αναζητήσει προϊόντα με βάση το λειτουργικό σύστημα, όπως η Microsoft Azure π.χ. που αναφέρθηκε παραπάνω, όμως ο χρήστης μπορεί να αναζητήσει προϊόντα με βάση με όλα τα χαρακτηριστικά των SecaaS προϊόντων, όπως αυτά αναφέρθηκαν στο υπό-κεφάλαιο 3.1.1 και φυσικά περιλαμβάνουν το μοντέλο κόστους, τον εκδότη, και την ύπαρξη ελεύθερων εκδόσεων. Επιπλέον, η παρούσα εργασία υπερτερεί των παραπάνω καθώς δίνει τη δυνατότητα στον χρήστη να ταξινομεί προϊόντα SecaaS με βάση πολλά κριτήρια, που περιλαμβάνουν τα μη λειτουργικά τους χαρακτηριστικά και περιορισμούς. Τέλος, υποστηρίζεται σημασιολογική αναζήτηση, η οποία οδηγεί στην παραγωγή πιο ακριβών αποτελεσμάτων.

Παρακάτω είναι ιστότοποι που παρέχουν μια αναφορά σε ένα περιορισμένο σύνολο από παρόχους SecaaS και τα προϊόντα τους:

- Straits Research - https://straitsresearch.com/report/security-as-a-service-market (Ημερομηνία πρόσβασης: 15/1/2025)
- Technology Advice - https://technologyadvice.com/blog/information-technology/security-as-a-service-saas-software-providers/ (Ημερομηνία πρόσβασης: 15/1/2025)
- Mordor Intelligence - https://www.mordorintelligence.com/industry-reports/security-as-a-service-market/companies (Ημερομηνία πρόσβασης: 15/1/2025)
- Market Research Future - https://www.marketresearchfuture.com/reports/security-as-a-service-market-6709 (Ημερομηνία πρόσβασης: 15/1/2025)

Οι παραπάνω ιστότοποι δεν προσφέρουν δυνατότητες δημοσίευσης, ανακάλυψης και ταξινόμησης προϊόντων SecaaS. Οπότε, αυτό είναι ένα κομμάτι στο οποίο υστερούν σε σχέση με την παρούσα εργασία.

Προσφέρουν όμως, σημαντικές πληροφορίες για την παγκόσμια αγορά των προϊόντων SecaaS και τους πιο σημαντικούς παρόχους αυτών. Όπως φαίνεται στις διαδικτυακές σελίδες τους, η αγορά των SecaaS προϊόντων αναμένεται να αναπτυχθεί ακόμη περισσότερο την επόμενη δεκαετία,

φθάνοντας από 15-16 δισεκατομμύρια δολάρια το 2024 σε 46,42 με 81,3 το 2032, έχοντας ένα ρυθμό ανάπτυξης που κυμαίνεται από 15,02 έως 19%. Μάλιστα, αυτό αναμένεται να γίνει σε όλες τις ηπείρους. Με αυτά τα δεδομένα, μπορούμε να πούμε ότι ο τομέας αυτός αλλά και γενικά της ασφάλειας, θα προσφέρει σημαντικές ευκαιρίες τα επόμενα χρόνια, καθώς θα γνωρίσει μεγάλη ανάπτυξη.

Επιπλέον, βλέπουμε ότι κατά την περίοδο της πανδημίας COVID-19, ενώ όλοι οι βιομηχανικοί τομείς παγκοσμίως επηρεάστηκαν αρνητικά, στον συγκεκριμένο τομέα δεν ίσχυσε κάτι τέτοιο. Αυτό εξηγείται λόγω της αύξησης της τηλεργασίας και άρα της απομακρυσμένης πρόσβασης αλλά και του διαμοιρασμού αρχείων μέσω του διαδικτύου. Έτσι οι μεγάλες εταιρίες και επιχειρήσεις αναγκάστηκαν να βελτιώσουν την κυβερνοασφάλεια σε μικρό χρονικό διάστημα. Αυτό είχε ως αποτέλεσμα να καταφύγουν σε λύσεις έτοιμων προϊόντων SecaaS.

3.3 Σύγκριση

Στις 2 προηγούμενες ενότητες του τρέχοντος κεφαλαίου έγινε μια ανάλυση σχετικών εργασιών και σημείων αγοράς προϊόντων SecaaS. Η παρούσα εργασία προσφέρει στους χρήστες τη δυνατότητα της δημοσίευσης και της εξεζητημένης ταξινόμησης αυτών των προϊόντων, κάτι το οποίο δεν είχε πραγματοποιηθεί μέχρι και σήμερα. Επιπλέον, προσφέρει στους χρήστες τη δυνατότητα της σημασιολογικής ανακάλυψης των προϊόντων αυτών. Η δυνατότητα αναζήτησης/ανακάλυψης υπάρχει ήδη σε ορισμένα σημεία αγοράς, όπως αναφέρθηκε, όμως είναι αρκετά περιορισμένη και μη σημασιολογική, προσφέροντας πολύ λίγα κριτήρια ή φίλτρα αναζήτησης. Αντίθετα, η παρούσα εργασία δίνει στον χρήστη τη δυνατότητα να ανακαλύψει με σημασιολογικό τρόπο προϊόντα SecaaS με βάση κριτήρια που περιλαμβάνουν όλα τα χαρακτηριστικά τους.

4

Ανάπτυξη Εφαρμογής

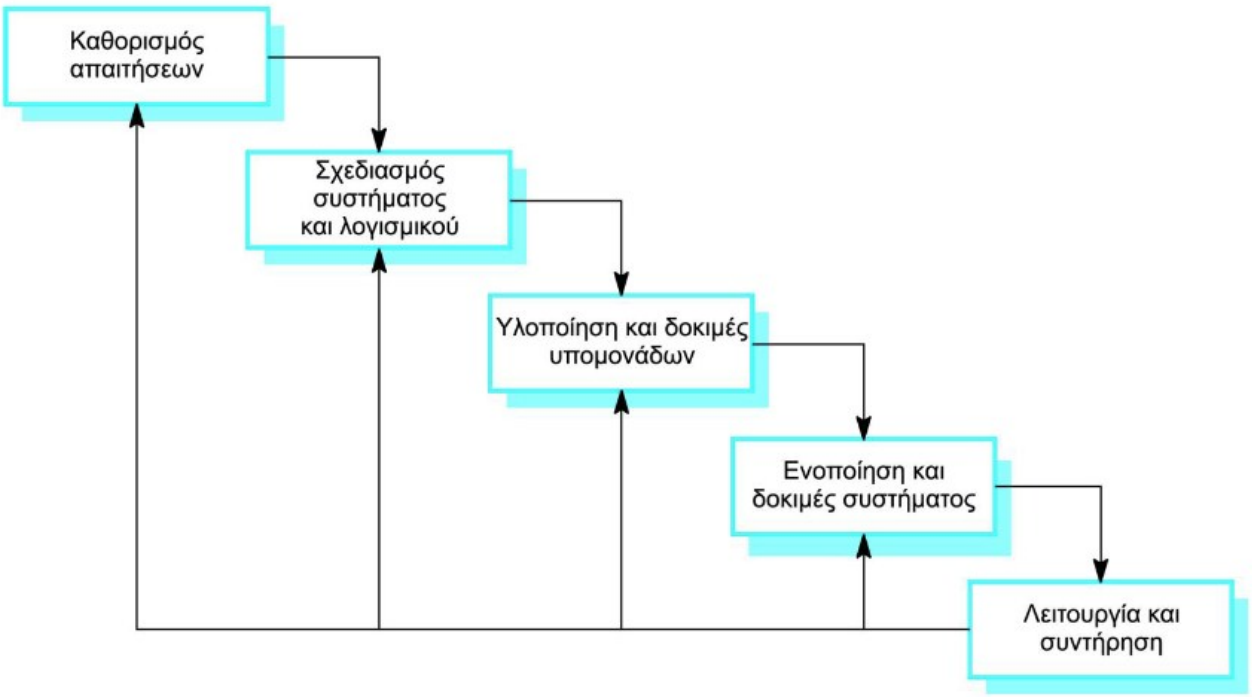
Στο κεφάλαιο αυτό θα συζητηθεί το μοντέλο ανάπτυξης της εφαρμογής μας. Στη συνέχεια θα γίνει ανάλυση των απαιτήσεων της εφαρμογής και καθώς και της σχεδίασής της μέσω διαγραμμάτων και επεξήγησης αυτών. Έπειτα, θα αναφερθούμε σε τεχνικές λεπτομέρειες που αφορούν την υλοποίηση της εφαρμογής, όπως τη γλώσσα προγραμματισμού, τα πλαίσια και τις βιβλιοθήκες που χρησιμοποιήθηκαν για την ανάπτυξη της. Τέλος, θα προσδιοριστεί ο βαθμός ικανοποίησης της κάθε απαίτησης που τέθηκε για την εφαρμογή, με αιτιολόγηση όταν αυτός δεν είναι άριστος.

4.1 Μοντέλο Καταρράκτη

Η ανάπτυξη της εφαρμογής έγινε σύμφωνα με το μοντέλο του καταρράκτη. Αυτό το μοντέλο ορίζει ότι οι φάσεις της ανάπτυξης ενός λογισμικού (όπως ανάλυση απαιτήσεων και σχεδίαση) είναι ξεχωριστές και εκτελούνται η μία μετά την άλλη. Στις περιπτώσεις όπου οι απαιτήσεις και οι στόχοι του έργου είναι καλά καθορισμένοι από την αρχή καθώς και έχουμε την ανάπτυξη μεγάλων έργων με κατανεμημένες ομάδες εργασίας, αυτό το μοντέλο είναι αρκετά χρήσιμο. Η σταθερότητα απαιτήσεων είναι απαραίτητο να υπάρχει διότι το μοντέλο αυτό είναι δύσκαμπτο και αντιδρά σε αλλαγές μόνο μετά από τον εκάστοτε κύκλο ανάπτυξης. Ενώ η δυνατότητα χρήσης τους σε μεγάλα έργα έγκειται στο γεγονός πως απαιτείται κατάλληλος συντονισμός της εργασίας σε αυτά τα έργα που μπορεί να υποστηριχθεί από ένα μοντέλο που οδηγείται από πλάνα (plan-based development), όπως είναι το μοντέλο του καταρράκτη. Το μοντέλο του καταρράκτη συνολικά αποτελείται από 5 φάσεις [11].

Στην πρώτη φάση γίνεται ανάλυση και καθορισμός των απαιτήσεων, που σημαίνει ότι ορίζονται οι προδιαγραφές, η λειτουργικότητα, οι περιορισμοί και οι στόχοι του έργου λογισμικού. Στη δεύτερη φάση γίνεται ο σχεδιασμός του συστήματος λογισμικού, το οποίο σημαίνει ότι καθορίζεται η δομή καθώς και η συμπεριφορά του. Στην τρίτη φάση γίνεται η υλοποίηση και οι δοκιμές των ξεχωριστών μονάδων (unit testing), όπου συγγράφεται ο κώδικας και επαληθεύεται η λειτουργία της κάθε μονάδας. Στην τέταρτη φάση γίνεται η ενοποίηση και δοκιμές του συστήματος, κατά την οποία τα συστατικά ενοποιούνται μεταξύ τους και δοκιμάζονται ως ένα ενιαίο σύστημα. Τέλος, στην πέμπτη φάση έχουμε τη παράδοση του λογισμικού στους πελάτες του καθώς και τη λειτουργία και συντήρησή του, κατά την οποία γίνεται η διόρθωση σφαλμάτων και η βελτιστοποίηση υπηρεσιών.

Στην παρακάτω εικόνα παρουσιάζονται σχηματικά τα βήματα που αναλύθηκαν προηγουμένως. Παρατηρήστε πως η εκτέλεση των βημάτων-δραστηριοτήτων ανάπτυξης γίνεται με σειριακό τρόπο και μόνο όταν ολοκληρωθεί ένας κύκλος (ανάπτυξης) μπορούμε να γυρίζουμε πίσω σε κάποια φάση δραστηριότητας για να διορθώσουμε σφάλματα ή να κάνουμε αλλαγές. Στη συνέχεια, θα αναλύσουμε τα αποτελέσματα ξεχωριστών δραστηριοτήτων του μοντέλου του καταρράκτη σε ξεχωριστές ενότητες.



Εικόνα 1. Μοντέλο καταρράκτη

4.2 Ανάλυση Απαιτήσεων

Έπειτα από την σχετική ανάλυση που πραγματοποιήθηκε, οριστικοποιήθηκαν οι απαιτήσεις του συστήματος, τόσο οι λειτουργικές όσο και οι μη λειτουργικές.

4.2.1 Λειτουργικές Απαιτήσεις

Οι λειτουργικές απαιτήσεις του συστήματος σχετίζονται με τις δυο βασικές οντότητες του συστήματος που είναι οι χρήστες και τα προϊόντα SecaaS. Αρχικά, θα δούμε στη πρώτη οντότητα (χρήστης) και έπειτα στην δεύτερη (προϊόντα SecaaS).

4.2.1.1 Λειτουργικές Απαιτήσεις Διαχείρισης Χρηστών

Εγγραφή χρήστη

Η πρώτη απαίτηση είναι η εγγραφή χρήστη. Κάθε επισκέπτης θα πρέπει να μπορεί να εγγραφεί στο σύστημα. Για την εγγραφή του θα πρέπει να παρέχει την ακόλουθη πληροφορία: ονοματεπώνυμο, όνομα χρήστη, κωδικό και διεύθυνση ηλεκτρονικού ταχυδρομείου. Στο όνομα χρήστη ο πρώτος χαρακτήρας θα πρέπει να είναι γράμμα και οι υπόλοιποι αλφαριθμητικοί ή ο χαρακτήρας '_'. Ο κωδικός θα πρέπει να έχει τουλάχιστον 8 χαρακτήρες, να περιέχει αλφαριθμητικούς και τουλάχιστον έναν από τους εξής ειδικούς χαρακτήρες: @, $, !, %, *, ?, &, #. Επίσης θα πρέπει να αποθηκεύεται στη βάση σε κατακερματισμένη μορφή και να ελέγχεται δυο φορές κατά την εγγραφή. Το ονοματεπώνυμο θα πρέπει να περιέχει μόνο αλφαριθμητικούς χαρακτήρες και η ηλεκτρονική διεύθυνση να είναι έγκυρη. Σημειώνεται ότι το όνομα χρήστη και το email έχουν περιορισμό μοναδικότητας. Επιπλέον, σε περίπτωση λάθους θα πρέπει να εμφανίζεται κατάλληλο μήνυμα στον χρήστη.

Ενεργοποίηση λογαριασμών (από διαχειριστή/χρήστη)

Εφόσον η εγγραφή πετύχει, ο λογαριασμός του χρήστη θα είναι ανενεργός. Η ενεργοποίηση του θα γίνεται με δυο τρόπους. Είτε χειρωνακτικά όπου ο διαχειριστής αναλαμβάνει την ενεργοποίηση, είτε μέσω του email του χρήστη. Ο δεύτερος τρόπος είναι πιο ασφαλής, καθώς έτσι μπορεί να επιβεβαιωθεί το email του χρήστη. Για να γίνει αυτό, ένας σύνδεσμος θα στέλνεται στην ηλεκτρονική διεύθυνση του χρήστη. Έπειτα ο χρήστης θα έχει διορία ένα συγκεκριμένο χρονικό διάστημα να ακολουθήσει τον σύνδεσμο και έτσι να επιβεβαιώσει το email του και άρα να ενεργοποιήσει τον λογαριασμό του.

Τροποποίηση στοιχείων

Ο ίδιος ο χρήστης θα μπορεί να τροποποιεί τα στοιχεία του και να αυτό-διαγράφεται. Η πληροφορία που μπορεί να αλλάξει είναι το ονοματεπώνυμο και το email του χρήστη. Αν ο λογαριασμός του χρήστη ενεργοποιήθηκε μέσω email και ο χρήστης το αλλάξει, τότε θα πρέπει να επιβεβαιώσει το νέο email με τον τρόπο που αναλύθηκε πιο πάνω. Σε αυτήν την περίπτωση θα απενεργοποιείται ο λογαριασμός και θα πρέπει να ενεργοποιηθεί εκ νέου με την επιβεβαίωση του καινούριου email. Ο διαχειριστής του συστήματος θα μπορεί να τροποποιεί χρήστες κατά βούληση.

Αλλαγή κωδικού

Ο χρήστης θα μπορεί να αλλάζει τον κωδικό του. Για να το κάνει αυτό θα πρέπει πρώτα να εισάγει τον παλιό κωδικό του και στη συνέχεια τον καινούριο. Ο καινούριος κωδικός θα πρέπει να εισαχθεί ξανά για επιβεβαίωση. Σε περίπτωση που ο παλιός κωδικός είναι λάθος, ή τα δυο πεδία

που περιέχουν τον καινούριο κωδικό δεν είναι ίδια, τότε θα εμφανίζεται κατάλληλο μήνυμα λάθους στον χρήστη. Ο καινούριος κωδικός θα πρέπει να ακολουθεί τους κανόνες που αναφέρθηκαν στη λειτουργία της Εγγραφής χρήστη για τον κωδικό. Και σε αυτήν την περίπτωση, αν ο κωδικός δεν ακολουθεί τους κανόνες θα εμφανιστεί μήνυμα λάθους στον χρήστη. Ο διαχειριστής δεν έχει το δικαίωμα να αλλάξει τον κωδικό ενός χρήστη.

Διαγραφή λογαριασμού

Ο ίδιος ο χρήστης θα μπορεί να αυτό-διαγράφεται. Ο διαχειριστής του συστήματος θα μπορεί να διαγράφει χρήστες κατά βούληση. Για την αποφυγή λανθασμένων ενεργειών θα πρέπει να πραγματοποιείται επιβεβαίωση της διαγραφής.

Επαναφορά κωδικού

Ακόμα, ο χρήστης έχει τη δυνατότητα επαναφοράς του κωδικού του σε περίπτωση που τον ξέχασε. Σε αυτή την περίπτωση, ο χρήστης, που δεν θα μπορεί να εισέλθει στο σύστημα, θα αιτείται την επαναφορά ως επισκέπτης δίνοντας το email του. Έπειτα, το σύστημα θα υπολογίζει έναν ισχυρό και έγκυρο κωδικό, ο οποίος θα στέλνεται στο email του χρήστη σε μη κρυπτογραφημένη μορφή.

Αυθεντικοποίηση χρήστη

Τέλος, ένας χρήστης θα μπορεί να δώσει τα διαπιστευτήρια του (όνομα χρήστη, κωδικό) και εφόσον αυτά είναι σωστά, να εισέλθει στο σύστημα. Σε αυτήν την περίπτωση θα λάβει ένα token, το οποίο μπορεί να χρησιμοποιήσει για την συνέχιση της περιήγησης στην εφαρμογή ως ταυτοποιημένος χρήστης. Ο φυλλομετρητής θα το εισάγει αυτόματα στις σελίδες που ο χρήστης επισκέπτεται. Σε περίπτωση που ο χρήστης αποτύχει 3 συνεχόμενες φορές να διαπιστευθεί, τότε ο λογαριασμός του θα απενεργοποιείται. Για να ενεργοποιήσει ξανά τον λογαριασμό του, ο χρήστης θα πρέπει να επικοινωνήσει με τον διαχειριστή. Στη συνέχεια, αν ο διαχειριστής ενεργοποιήσει τον λογαριασμό του, ο χρήστης θα μπορεί να αιτηθεί την επαναφορά του κωδικού του.

4.2.1.2 Λειτουργικές Απαιτήσεις Διαχείρισης Προϊόντων SecaaS

Δημιουργία

Η πρώτη απαίτηση που αφορά τα προϊόντα SecaaS είναι η δημιουργία τους. Ένας ταυτοποιημένος χρήστης θα μπορεί να εισάγει την πληροφορία για ένα νέο SecaaS προϊόν. Η πληροφορία αυτή θα πρέπει να συνάδει με το πληροφοριακό μοντέλο περιγραφής προϊόντων SecaaS του συστήματος. Επίσης, θα πρέπει να ελέγχεται η εγκυρότητα των παρεχόμενων τιμών και η ύπαρξη του ίδιου προϊόντος στο σύστημα. Στις περιπτώσεις που το προϊόν υπάρχει ήδη, ή έχει γίνει κάποιο λάθος

στις παρεχόμενες τιμές του χρήστη, τότε θα εμφανίζεται κατάλληλο μήνυμα λάθους. Επιπλέον, θα μηδενίζονται τα πεδία εισαγωγής προϊόντος. Ένα προϊόν SecaaS που δημιουργείται επιτυχώς δεν είναι αρχικά δημοσιευμένο.

Δημοσίευση/Αποδημοσίευση

Επιπλέον, ένα προϊόν μπορεί να δημοσιεύεται και να αποδημοσιεύεται μόνο από τον δημιουργό του. Από τη στιγμή που ένα προϊόν δημοσιευτεί, τότε οι πληροφορίες του θα είναι διαθέσιμες προς ανακάλυψη από τους υπόλοιπους χρήστες.

Εμφάνιση

Κάθε χρήστης θα μπορεί να δει όλες τις πληροφορίες που συνοδεύουν ένα δημοσιευμένο προϊόν. Αυτή η λειτουργία της εμφάνισης προϊόντων SecaaS θα είναι διαθέσιμη και για τους επισκέπτες.

Διαγραφή

Μία ακόμα απαίτηση είναι η διαγραφή ενός προϊόντος, η οποία μπορεί να πραγματοποιηθεί είτε από τον δημιουργό του προϊόντος, είτε από τον διαχειριστή. Για την αποφυγή λανθασμένων διαγραφών, θα πρέπει να πραγματοποιείται επιβεβαίωση της διαγραφής.

Ταίριασμα

Το ταίριασμα είναι άλλη μια απαίτηση. Ο χρήστης θα πρέπει να παρέχει στον σύστημα μια σειρά από απαιτήσεις και έπειτα το σύστημα θα του επιστρέφει μια μη ταξινομημένη λίστα με τα ταιριασμένα SecaaS προϊόντα. Τονίζεται πως αν δεν δοθούν απαιτήσεις από το χρήστη, τότε επιστρέφονται όλα τα προϊόντα SecaaS. Κάθε απαίτηση είναι ένας περιορισμός ως προς τα χαρακτηριστικά των SecaaS προϊόντων. Προκαθορισμένα ο συνδυασμός των απαιτήσεων είναι συζευκτικός οπότε όλοι οι περιορισμοί θα πρέπει να ικανοποιούνται από την περιγραφή ενός SecaaS προϊόντος ώστε αυτό να καταστεί ταιριασμένο. Αλλά θα είναι στην ευχέρεια του χρήστη να χρησιμοποιεί και να συνδυάζει τους περιορισμούς του και με άλλους λογικούς τελεστές (εκτός του AND - σύζευξης), όπως OR (διάζευξης), XOR (αποκλειστικής διάζευξης) και NOT (λογικής άρνησης).

Ένας περιορισμός είναι μια συνθήκη που αφορά ένα χαρακτηριστικό ενός SecaaS προϊόντος. Περιλαμβάνει το όνομα του χαρακτηριστικού, έναν τελεστή σύγκρισης/ισότητας (πχ. <, ==) και μια τιμή. Αυτό ισχύει για μονότιμα χαρακτηριστικά. Σημειώνεται εδώ πως οι τελεστές σύγκρισης (<, >= κλπ.) έχουν νόημα να παρέχονται για μονότιμα χαρακτηριστικά μόνο όταν αυτά είναι αριθμητικά. Σε περίπτωση που τα χαρακτηριστικά είναι πολλαπλών τιμών, τότε η συνθήκη εκτός από το όνομα του χαρακτηριστικού μπορεί να περιλαμβάνει τελεστές σύγκρισης/ισότητας συνόλων

(μπορεί να είναι οι ίδιοι με τους απλούς τελεστές σύγκρισης/ισότητας για λόγους απλότητας αλλά προφανώς με διαφορετική σημασιολογία) και ένα σύνολο ως την τιμή της συνθήκης (με τη μορφή πολλαπλών τιμών μέσα σε άγκιστρα). Για παράδειγμα, έχουμε τη συνθήκη region >= {“Europe”, “Asia”} που προσδιορίζει πως η περιοχή διάθεσης του προϊόντος πρέπει να είναι τουλάχιστον η Ευρώπη και η Ασία. Για τους επισκέπτες της εφαρμογής όμως θα υπάρχουν κάποιοι περιορισμοί. Έτσι, ένας επισκέπτης θα μπορεί να χρησιμοποιεί μόνο συζευκτικούς λογικούς τελεστές και θα υπάρχει περιορισμός ως προς τον αριθμό των αποτελεσμάτων που θα του επιστρέφονται. Ο αριθμός αυτός θα ρυθμίζεται από μια σχετική παράμετρο διαμόρφωσης του συστήματος.

Ταξινόμηση

Μία βασική λειτουργική απαίτηση είναι αυτή της ταξινόμησης. Η ταξινόμηση μπορεί να πραγματοποιείται σε μια λίστα από προϊόντα SecaaS που είτε έχουν ταιριαστεί ήδη με βάση τις απαιτήσεις του χρήστη ή όχι. Στη δεύτερη περίπτωση, θα αφορά επομένως όλα τα διαθέσιμα/δημοσιευμένα SecaaS προϊόντα ή προϊόντα SecaaS που έχουν επιλεγεί χειρωνακτικά από τον ίδιο. Για να πραγματοποιηθεί η ταξινόμηση, ο χρήστης θα πρέπει να παρέχει μια σειρά από σχετικά βάρη, όπου έκαστο τοποθετείται σε κάποιο μη λειτουργικό χαρακτηριστικό των SecaaS προϊόντων. Το άθροισμα των βαρών αυτών θα πρέπει να ισούται με 1.0 ενώ κάθε βάρος θα είναι μια τιμή στο σύνολο [0.0, 1.0].

Η ταξινόμηση πραγματοποιείται με βάση ένα σκορ που θα πρέπει να παραχθεί για κάθε SecaaS προϊόν στη λίστα, το οποίο υπολογίζεται λαμβάνοντας υπόψιν τα βάρη του χρήστη και την απόδοση του προϊόντος σε σχέση με τα χαρακτηριστικά που αντιστοιχούν στα βάρη αυτά. Το σκορ αυτό υπολογίζεται με βάση την εξής φόρμουλα: $\text{score}_j = \sum_i (w_i * score_{ij})$, όπου w_i είναι το βάρος για το κριτήριο/χαρακτηριστικό *i* και $score_{ij}$ είναι το τοπικό σκορ για το χαρακτηριστικό *i* όσον αφορά το προϊόν *j*. Το τοπικό σκορ για ένα μονότιμο χαρακτηριστικό υπολογίζεται με βάση την κατεύθυνση των τιμών για αυτό το χαρακτηριστικό. Η θετική κατεύθυνση σημαίνει πως όσο πιο μεγάλη είναι η τιμή του χαρακτηριστικού, τόσο το καλύτερο ενώ αρνητική σημαίνει πως όσο πιο μεγάλη είναι η τιμή, τόσο το χειρότερο. Σημειώνουμε εδώ πως θεωρούμε πως αν ένα μονότιμο χαρακτηριστικό δεν είναι αριθμητικό αλλά παίρνει τιμές από ένα σύνολο διαβαθμισμένων τιμών (πχ. τύπου String), τότε εσωτερικά το σύστημα γνωρίζει πως να αντιστοιχεί κάθε τιμή του συνόλου σε μια αριθμητική τιμή (θεωρούμε πως είναι μη αρνητική αυτή τη τιμή).

Αν το μονότιμο χαρακτηριστικό i έχει θετική κατεύθυνση τιμών, τότε το τοπικό σκορ για αυτό υπολογίζεται ως εξής:

$$\frac{x_{ij} - \min_k(x_{ik})}{\max_k(x_{ik}) - \min_k(x_{ik})},$$

- όπου x_{ij} είναι η τιμή για το χαρακτηριστικό για το προϊόν SecaaS *j*,
- $\max_k(x_{ik})$ είναι η μέγιστη τιμή για αυτό το χαρακτηριστικό κατά μήκος όλων των προϊόντων
- $\min_k(x_{ik})$ είναι η ελάχιστη τιμή για αυτό το χαρακτηριστικό κατά μήκος όλων των προϊόντων SecaaS.

Αν το μονότιμο χαρακτηριστικό i έχει αρνητική κατεύθυνση τιμών, τότε το τοπικό σκορ για αυτό υπολογίζεται ως εξής:

$$\frac{\max_k(x_{ik}) - x_{ij}}{\max_k(x_{ik}) - \min_k(x_{ik})}$$

Εδώ θα πρέπει να τονίσουμε πως δεν έχει νόημα να υπολογίσουμε το τοπικό σκορ για χαρακτηριστικά πολλαπλών τιμών, οπότε αυτά θα χρησιμοποιούνται μόνο για την έκφραση περιορισμών χρήστη. Αυτό σημαίνει πως μπορούν να παρέχονται βάρη μόνο σε μονότιμα χαρακτηριστικά.

Ανακάλυψη

Η τελευταία απαίτηση είναι αυτή της ανακάλυψης. Ουσιαστικά είναι συνδυασμός των δύο προηγούμενων λειτουργιών (ταριάσματος & ταξινόμησης). Ο χρήστης θα πρέπει να παρέχει την είσοδο που αφορά και τις 2 λειτουργίες (δηλ. απαιτήσεις και προτιμήσεις) και έπειτα το σύστημα θα φιλτράρει τα SecaaS προϊόντα με βάση τις απαιτήσεις του χρήστη και θα τα ταξινομεί με βάση τις προτιμήσεις του. Το αποτέλεσμα είναι να εμφανίζεται στον χρήστη μια ταξινομένη λίστα με τα ταιριασμένα SecaaS προϊόντα σε φθίνουσα σειρά ως προς το σκορ αξιολόγησής τους.

4.2.2 Μη Λειτουργικές Απαιτήσεις

Οι μη λειτουργικές απαιτήσεις της εφαρμογής περιλαμβάνουν:

- *Καλό επίπεδο απόδοσης*
    - Κάθε λειτουργία δεν μπορεί να παίρνει πάνω από 5 δευτερόλεπτα προς εκτέλεση
    - Θα πρέπει να υποστηρίζονται τουλάχιστον 50 ταυτόχρονοι χρήστες
- *Καλό επίπεδο χρηστικότητας*
    - Η διεπαφή χρήσης πρέπει να είναι χρηστική κατά μήκος διαφορετικών συσκευών
    - Η διεπαφή χρήσης πρέπει να έχει ενιαίο look-n-feel
    - Το επίπεδο navigability και user-orientation πρέπει να είναι καλό
- *Αρθρωτότητα & Ωριμότητα*
    - Διαχωρισμένο API (Back-End) και Front-End
    - Υλοποίηση backend σε REST με επίπεδο ωριμότητας 3
- *Καλό επίπεδο δυναμικότητας*
    - Ισορροπημένη χρήση Ajax και δυναμικής HTML
- *Επικύρωση & χειρισμός λαθών*
    - Κατάλληλος χειρισμός λαθών/εξαιρέσεων με παροχή αυτό-επεξηγούμενων μηνυμάτων (και άλλων μέσων οπτικοποίησης)
    - Κατάλληλη επικύρωση φορμών/δεδομένων τόσο στην πλευρά του πελάτη όσο και του εξυπηρετητή
- *Καλό επίπεδο ασφάλειας*
    - Ταυτοποίηση με βάση token

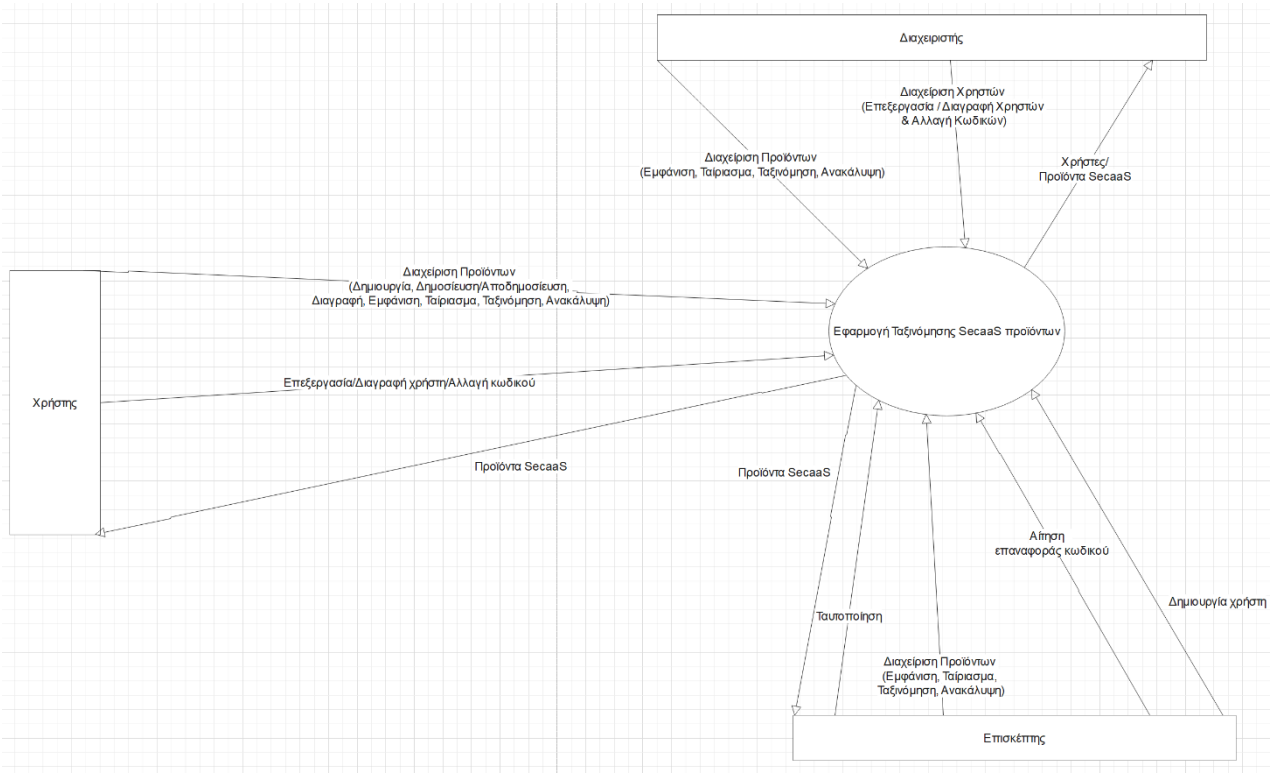
- Χρήση μοντέλου πρόσβασης RBAC ή ABAC
- Υποστήριξη TLS
- Προστασία CSRF
- Κατακερματισμός κωδικών

4.3 Σχεδίαση

Η προσπάθεια που καταναλώθηκε κατά τη δραστηριότητα της σχεδίασης της εφαρμογής αποτυπώνεται στο τελικό αποτέλεσμα που αφορά την δημιουργία των εξής διαγραμμάτων: διάγραμμα περιβάλλοντος, διάγραμμα συστατικών, διάγραμμα περιπτώσεων χρήσης, διαγράμματα δραστηριοτήτων (όπου έκαστο καλύπτει μια περίπτωση χρήσης από το προηγούμενο διάγραμμα) και διαγράμματα κλάσεων για την περιγραφή των κύριων οντοτήτων της εφαρμογής μας. Τα διαγράμματα αυτά θα παρουσιαστούν στη συνέχεια.

4.3.1 Διάγραμμα Περιβάλλοντος

Το διάγραμμα περιβάλλοντος που φαίνεται στην παρακάτω εικόνα περιλαμβάνει το σύστημα λογισμικού (δηλ. την εφαρμογή μας) και τον τρόπο που αυτό επικοινωνεί με το περιβάλλον του, το οποίο αποτελείται αποκλειστικά από εξωτερικές οντότητες / είδη χρηστών, οι οποίες είναι ο διαχειριστής, οι χρήστες και οι επισκέπτες.



Εικόνα 2. Διάγραμμα περιβάλλοντος

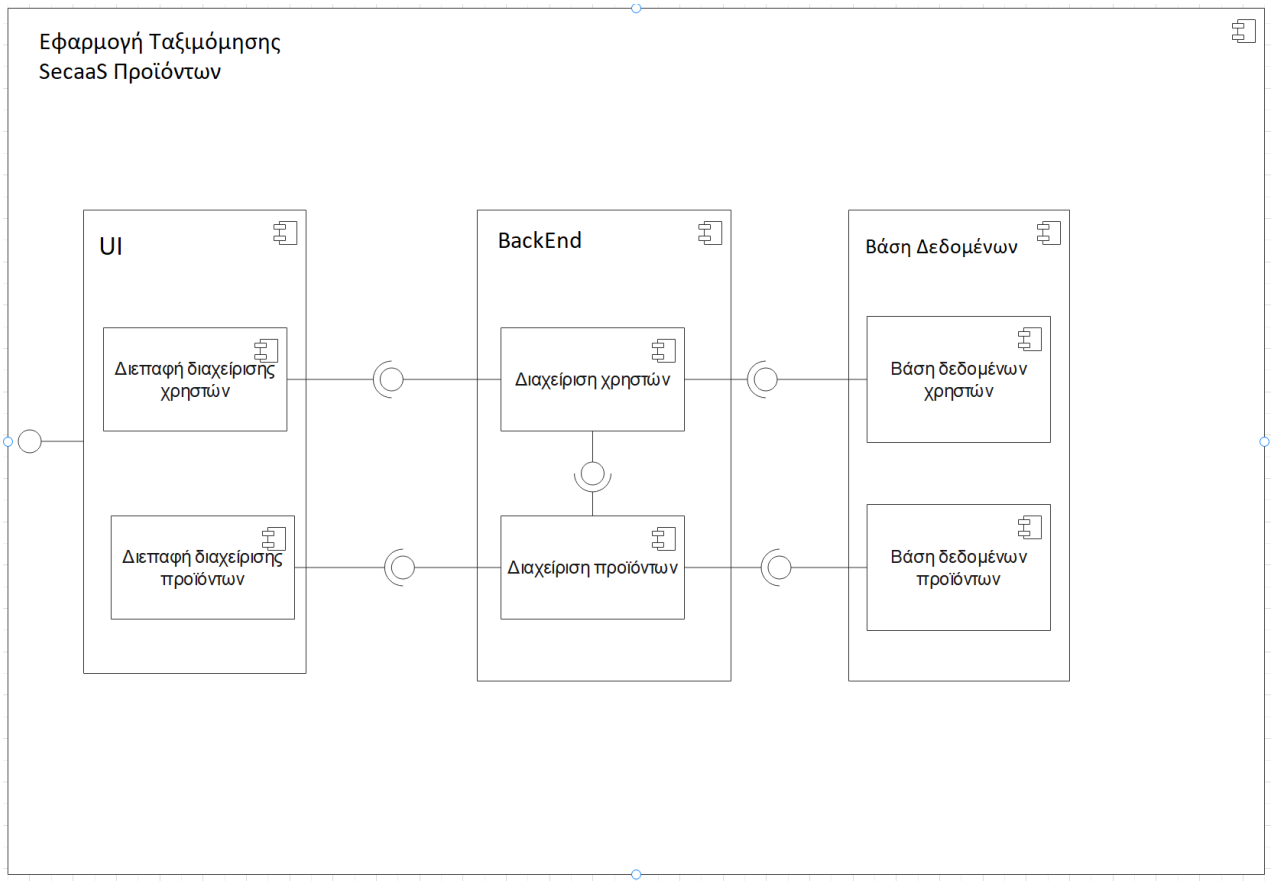
4.3.2 *Διάγραμμα Συστατικών*

Το διάγραμμα συστατικών της Εικόνας 3 παρουσιάζει την αρχιτεκτονική της εφαρμογής, η οποία περιλαμβάνει τα κύρια συστατικά της: το UI, το Backend και την βάση δεδομένων.

Το UI χωρίζεται σε 2 μέρη: τη διεπαφή διαχείρισης χρηστών και τη διεπαφή διαχείρισης προϊόντων. Το πρώτο μέρος καλύπτει όλες τις ενέργειες που μπορεί να κάνει ένας χρήστης της εφαρμογής και αφορούν τον λογαριασμό του, είτε τον λογαριασμό και άλλων στην περίπτωση που ο χρήστης είναι διαχειριστής. Το δεύτερο μέρος καλύπτει όλες τις ενέργειες που μπορεί να κάνει ένας χρήστης και αφορούν τα προϊόντα.

Το Backend της εφαρμογής επίσης ακολουθεί παρόμοιο σχεδιασμό με το UI. Αποτελείται από δυο βασικά μέρη, τα οποία καλύπτουν τη διαχείριση των χρηστών και των προϊόντων αντίστοιχα. Σε αυτό το συστατικό έχουμε την υλοποίηση του API της εφαρμογής, δηλαδή όλων των μεθόδων, οι οποίες εκτελούν τις ενέργειες και αιτήματα του χρήστη.

Τέλος, το συστατικό της βάσης δεδομένων περιλαμβάνει 2 βάσεις δεδομένων. Στη μια βάση δεδομένων αποθηκεύονται τα δεδομένα των χρηστών. Οπότε, όλες οι ενέργειες που τους αφορούν έχουν τη βάση αυτή ως σημείο αναφοράς (για την διαχείριση των δεδομένων τους). Στη δεύτερη βάση αποθηκεύονται τα δεδομένα των προϊόντων (SecaaS). Όπως και στην περίπτωση των χρηστών, έτσι και εδώ όλες οι ενέργειες που αφορούν τα προϊόντα έχουν την δεύτερη αυτή βάση ως σημείο αναφοράς (για την διαχείριση των δεδομένων τους).



Εικόνα 3. Διάγραμμα συστατικών

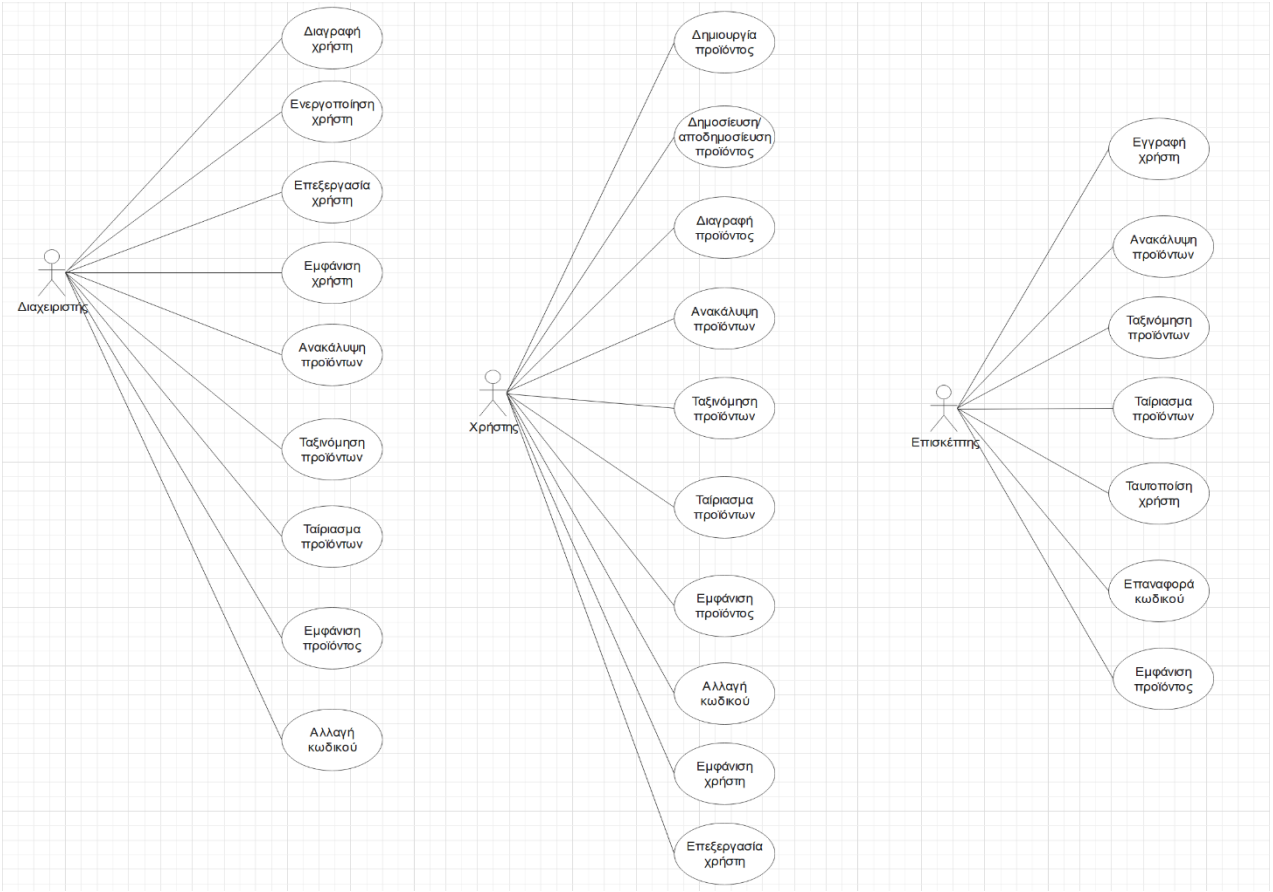
4.3.3 Διάγραμμα Περιπτώσεων Χρήσης

Το διάγραμμα περιπτώσεων χρήσης (Εικόνα 4) περιλαμβάνει συνοπτικά τις περιπτώσεις χρήσης για τις 3 εξωτερικές οντότητες που επικοινωνούν με την εφαρμογή, δηλαδή τον διαχειριστή, τους χρήστες και τους επισκέπτες. Ουσιαστικά κάθε περίπτωση χρήσης αντιστοιχεί σε μια βασική λειτουργία του συστήματος. Στο διάγραμμα υπάρχει επανάληψη ορισμένων περιπτώσεων χρήσης διότι η παρουσίαση των περιπτώσεων χρήσης πραγματοποιείται με βάση την εκάστοτε κύρια οντότητα που τις εκκινεί. Με αυτή τη λογική, μπορούμε να δούμε πως το διάγραμμα αποτελείται από 3 μέρη, όπου κάθε ένα είναι αφιερωμένο στην κάλυψη των αλληλεπιδράσεων και σχετικών περιπτώσεων χρήσης με μια από τις 3 (προαναφερόμενες) βασικές εξωτερικές οντότητες του συστήματος.

Η οντότητα διαχειριστής μπορεί να κάνει τις εξής ενέργειες στο σύστημα: να διαγράψει έναν χρήστη, να ενεργοποιήσει έναν χρήστη, να επεξεργαστεί έναν χρήστη (συμπ. του εαυτού του), να εμφανίσει τα στοιχεία ενός χρήστη (συμπ. του εαυτού του), να ανακαλύψει προϊόντα SecaaS, να ταξινομήσει προϊόντα SecaaS, να ταιριάξει προϊόντα SecaaS, να εμφανίσει τα στοιχεία ενός προϊόντος SecaaS και να αλλάξει τον κωδικό του.

Η οντότητα χρήστης μπορεί να κάνει τις εξής ενέργειες στο σύστημα: να δημιουργήσει ένα προϊόν SecaaS, να δημοσιεύσει ή αποδημοσιεύσει ένα δικό του προϊόν SecaaS, να διαγράψει ένα δικό του προϊόν SecaaS, να ανακαλύψει προϊόντα SecaaS, να ταξινομήσει προϊόντα SecaaS, να ταιριάξει προϊόντα SecaaS, να εμφανίσει τα στοιχεία ενός προϊόντος SecaaS, να αλλάξει τον κωδικό του, να εμφανίσει τα στοιχεία του και να τα επεξεργαστεί.

Η οντότητα επισκέπτης μπορεί να κάνει τις εξής ενέργειες στο σύστημα: να εγγραφεί, να ανακαλύψει προϊόντα SecaaS, να ταξινομήσει προϊόντα SecaaS, να ταιριάξει προϊόντα SecaaS, να ταυτοποιηθεί στο σύστημα (να κάνει είσοδο με τα διαπιστευτήρια του), να επαναφέρει τον κωδικό του και να εμφανίσει τα στοιχεία ενός προϊόντος SecaaS.



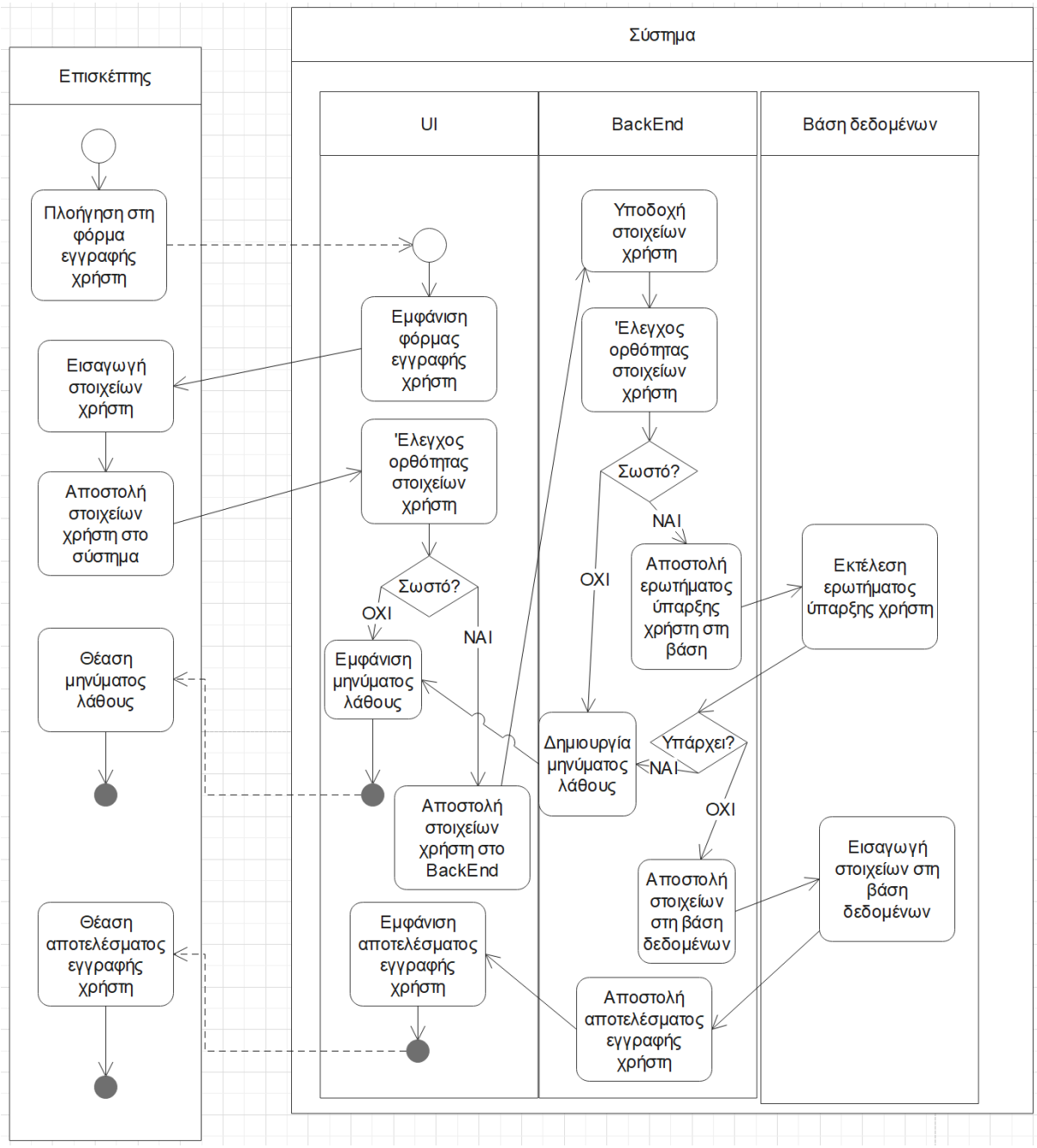
Εικόνα 4. Διάγραμμα περιπτώσεων χρήσης

4.3.4 Διαγράμματα Δραστηριοτήτων

Για κάθε περίπτωση χρήσης έχουμε αφιερώσει ένα διάγραμμα δραστηριοτήτων, το οποίο προσδιορίζει με περισσότερες λεπτομέρειες τις ενέργειες που πραγματοποιούνται για την υλοποίηση της εκάστοτε βασικής λειτουργίας που καλύπτεται από την περίπτωση αυτή.

4.3.4.1 Διάγραμμα Περίπτωσης Εγγραφής Επισκέπτη

Το διάγραμμα περίπτωσης εγγραφής επισκέπτη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για την εγγραφή ενός επισκέπτη στο σύστημα. Όπως φαίνεται και στην εικόνα, ο επισκέπτης θα πρέπει να πλοηγηθεί στη φόρμα εγγραφής, να εισάγει τα στοιχεία του και να τα στείλει στο σύστημα. Στη συνέχεια, το σύστημα θα ελέγξει αν τα στοιχεία είναι ορθά και σε περίπτωση που είναι, θα αποθηκεύσει τον χρήστη στη βάση. Σε αντίθετη περίπτωση, θα εμφανίσει στον χρήστη ένα μήνυμα λάθους. Ο έλεγχος ορθότητας των στοιχείων γίνεται και στο UI και στο BackEnd (για λόγους περισσότερης ασφάλειας).

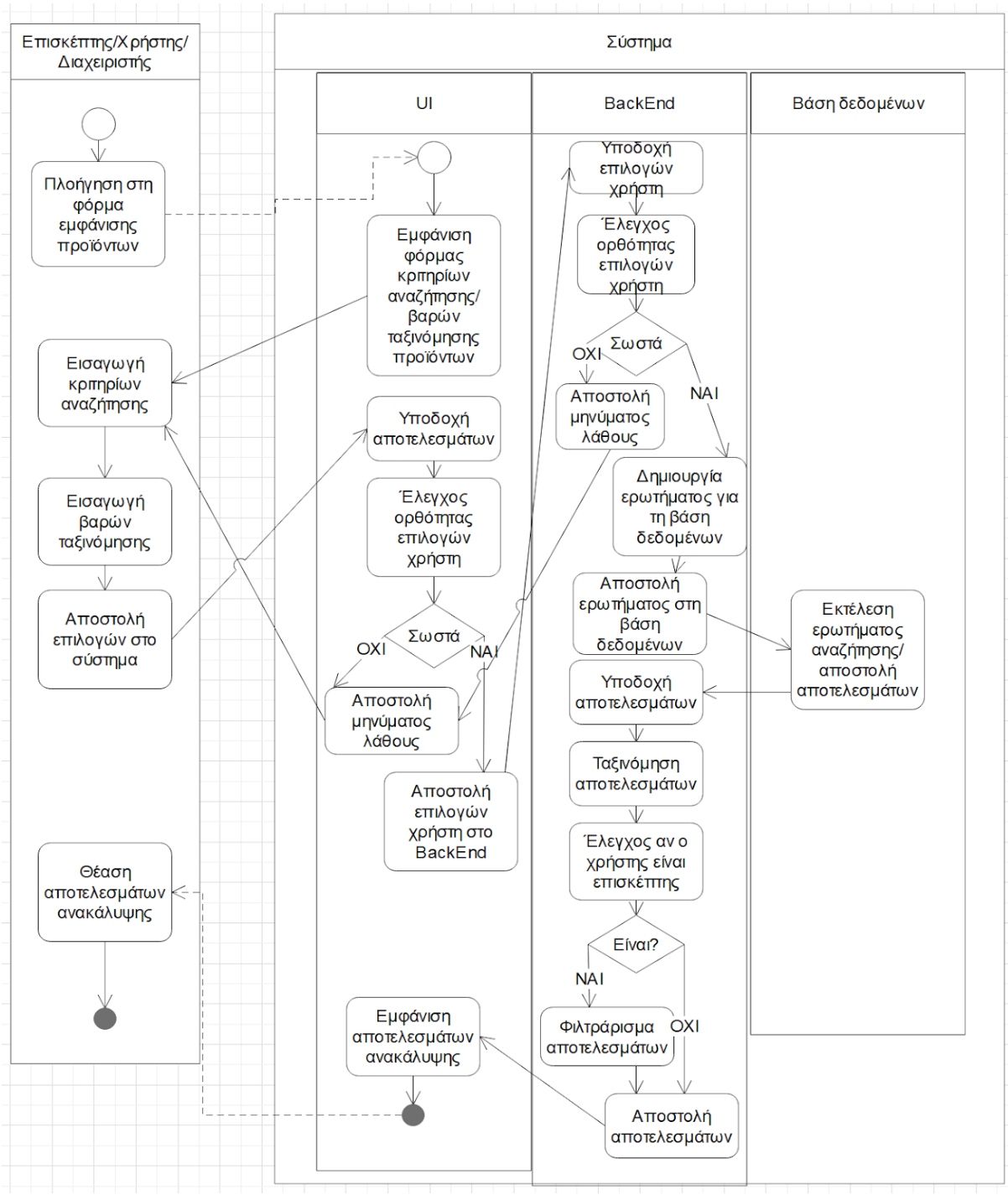


Εικόνα 5. Διάγραμμα περίπτωσης εγγραφής επισκέπτη

4.3.4.2 Διάγραμμα Περίπτωσης Ανακάλυψης

Το διάγραμμα περίπτωσης ανακάλυψης προϊόντων SecaaS της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για τη λειτουργία της ανακάλυψης. Αρχικά ο χρήστης θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης προϊόντων. Εκεί θα δει όλα τα κριτήρια αναζήτησης που προσφέρει η εφαρμογή και εισόδους κειμένου για τα βάρη. Μόλις ο χρήστης συμπληρώσει τα πεδία που επιθυμεί, θα προχωρήσει στην υποβολή των τιμών τους στο σύστημα. Το UI θα ελέγξει πρώτα την ορθότητα των τιμών που έδωσε ο χρήστης και αν δεν είναι σωστές, θα εμφανίσει κατάλληλο

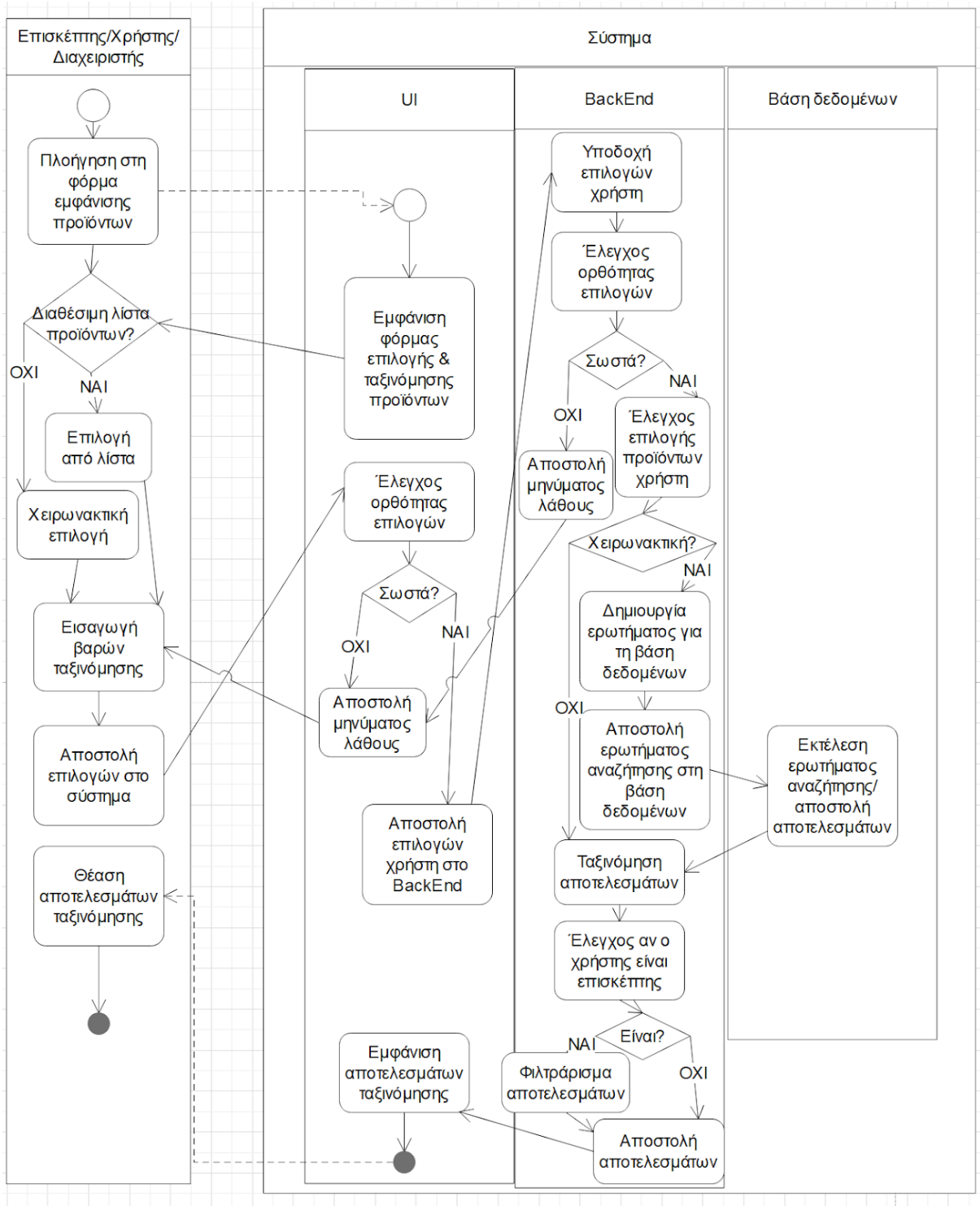
μήνυμα λάθους. Αν είναι σωστές, θα τις στείλει στο BackEnd. Εκεί θα γίνει ξανά έλεγχος ορθότητας των τιμών, όπου πάλι σε περίπτωση σφάλματος, θα σταλθεί μήνυμα λάθους στον χρήση. Αν οι τιμές είναι σωστές, το BackEnd θα δημιουργήσει ένα κατάλληλο ερώτημα με βάση τις τιμές του χρήστη, θα το στείλει στη βάση δεδομένων και έπειτα θα ταξινομήσει τα αποτελέσματα που θα λάβει πίσω από αυτήν. Έπειτα, θα γίνει έλεγχος αν ο χρήστης είναι επισκέπτης. Εφόσον κάτι τέτοιο ισχύει, τότε το BackEnd θα φιλτράρει τα αποτελέσματα που θα στείλει στο UI προς θέαση από τον χρήστη. Διαφορετικά, αυτά θα αποσταλούν ως έχουν.



Εικόνα 6. Διάγραμμα περίπτωσης ανακάλυψης

4.3.4.3 Διάγραμμα Περίπτωσης Ταξινόμησης

Το διάγραμμα περίπτωσης ταξινόμησης προϊόντων SecaaS της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για τη λειτουργία της ταξινόμησης. Ο χρήστης αρχικά θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης προϊόντων. Εκεί μπορεί να υπάρχει ήδη μια λίστα με προϊόντα από προηγούμενη αναζήτηση ή ο χρήστης μπορεί να προχωρήσει σε χειρωνακτική επιλογή κάποιων προϊόντων από τα συνολικά. Στη συνέχεια θα πρέπει να δώσει τις τιμές που επιθυμεί στα βάρη και να τις στείλει στο σύστημα ώστε αυτό να προχωρήσει στην ταξινόμηση των επιλεγμένων προϊόντων. Το UI θα κάνει έναν πρώτο έλεγχο για την ύπαρξη λαθών σε αυτές τις τιμές και σε περίπτωση που υπάρχουν, θα εμφανίσει μήνυμα λάθους χωρίς να στείλει το αίτημα στο Back|End. Αν οι τιμές είναι σωστές, θα στείλει το σχετικό αίτημα. Το BackEnd θα κάνει και αυτό έλεγχο ορθότητας των τιμών. Αν οι τιμές δεν είναι ορθές, θα στείλει μήνυμα λάθους στο UI. Στην περίπτωση που είναι ορθές, θα ελέγξει αν ο χρήστης επέλεξε χειρωνακτική αναζήτηση προϊόντων ή όχι. Αν η επιλογή είναι χειρωνακτική, το BackEnd θα στείλει ερώτημα στη βάση για να αναζητήσει τα προϊόντα που ζητήθηκαν και έπειτα θα προχωρήσει σε ταξινόμηση των αποτελεσμάτων που θα ληφθούν από αυτήν. Αλλιώς θα ταξινομήσει τα προϊόντα που του έχουν ήδη σταλεί. Τέλος, θα γίνει έλεγχος αν ο χρήστης είναι επισκέπτης. Εφόσον αυτό ισχύει, το BackEnd θα φιλτράρει τα αποτελέσματα που θα στείλει στο UI προς θέαση από τον χρήστη. Διαφορετικά, θα τα στείλει ως έχουν.

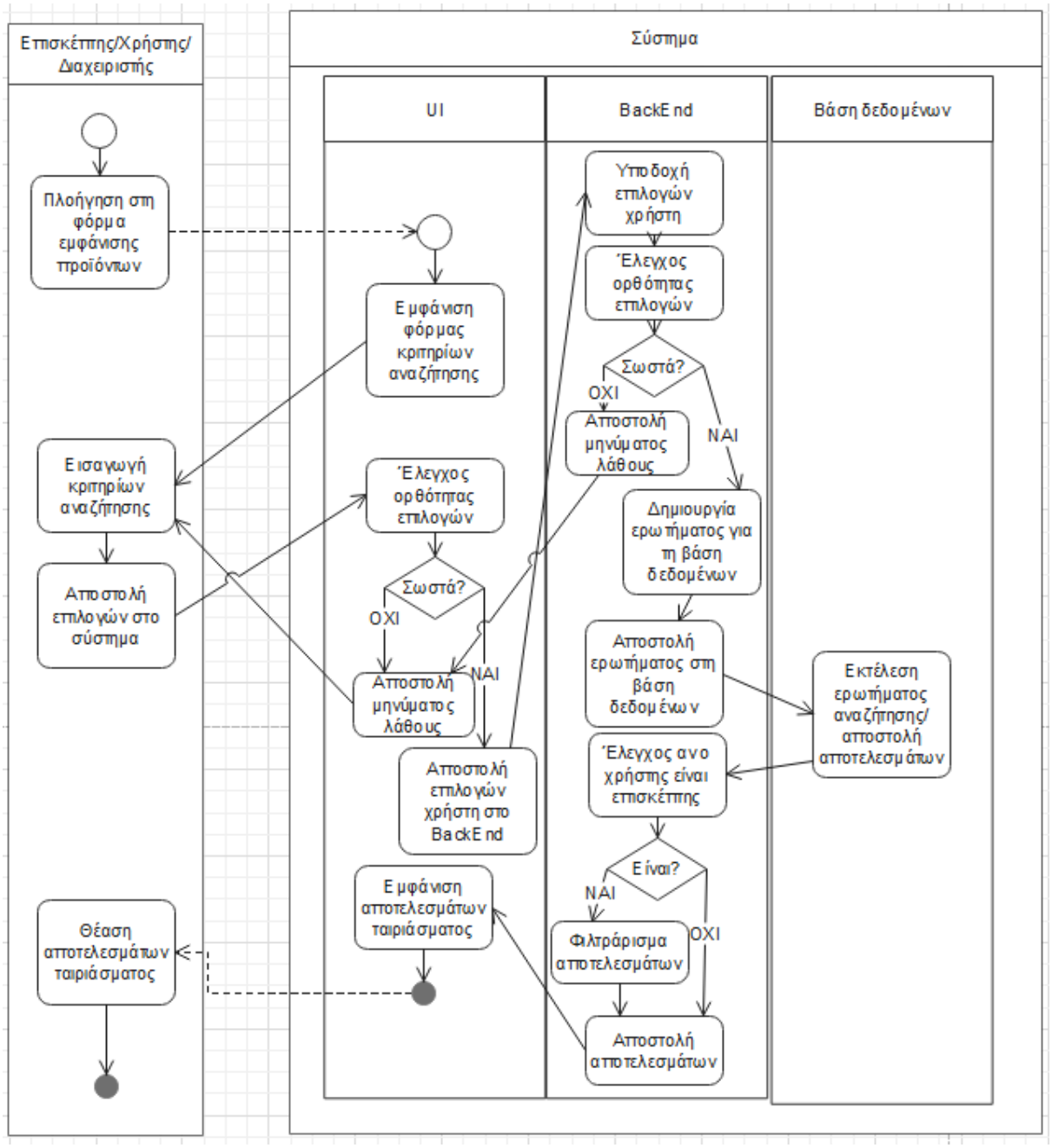


Εικόνα 7. Διάγραμμα περίπτωσης ταξινόμησης

4.3.4.4 Διάγραμμα Περίπτωσης Ταιριάσματος

Το διάγραμμα περίπτωσης ταιριάσματος προϊόντων SecaaS της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που πραγματοποιούνται για τη λειτουργία του ταιριάσματος. Ο χρήστης θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης προϊόντων. Εκεί, θα εισάγει τα κριτήρια αναζήτησης που επιθυμεί και θα στείλει τις επιλογές του στο σύστημα. Μπορεί να μην εισάγει κανένα κριτήριο οπότε το

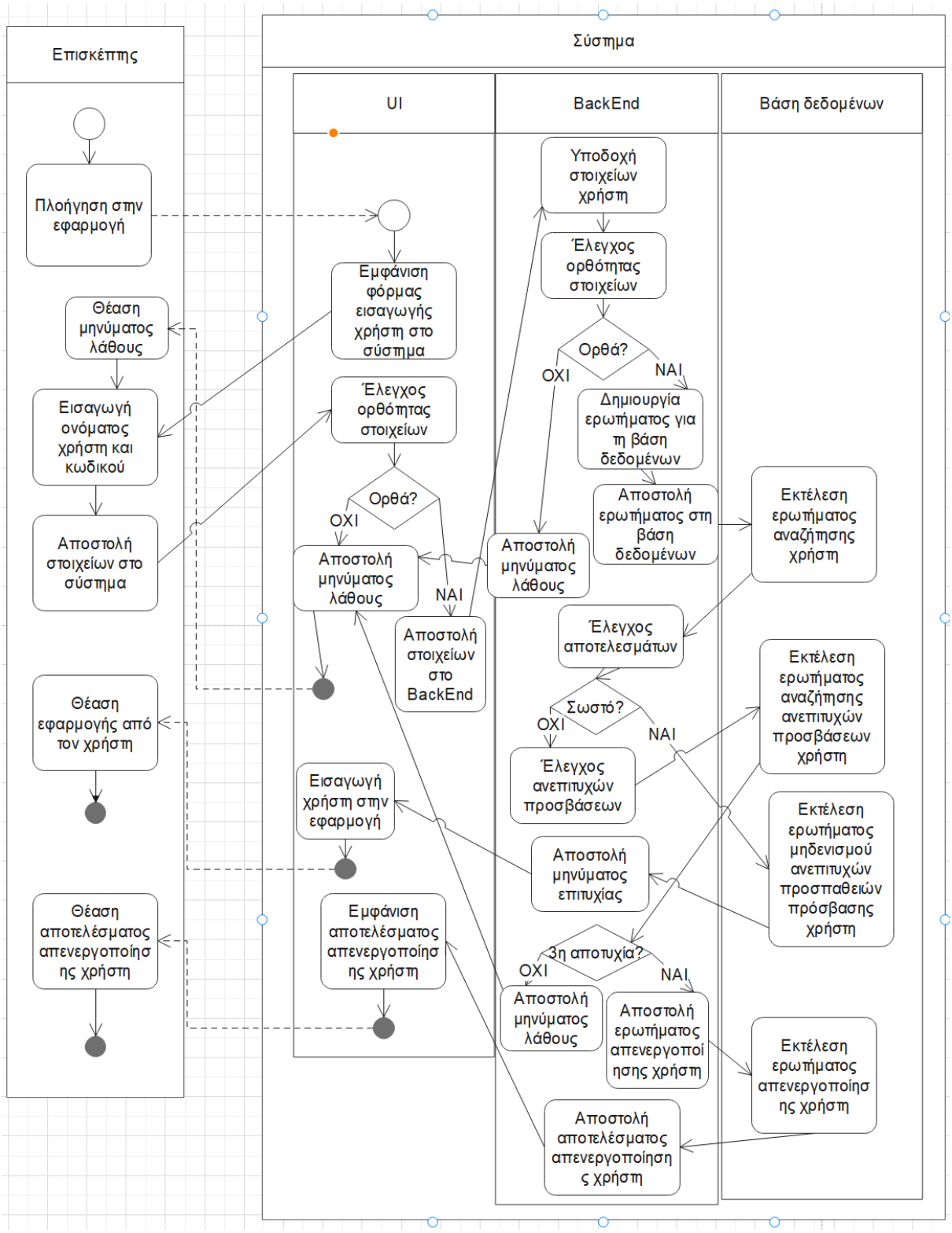
σύστημα θα του εμφανίσει όλα τα διαθέσιμα προϊόντα. Στη συνέχεια το UI θα κάνει έναν πρώτο έλεγχο ορθότητας των επιλογών του χρήστη. Στην περίπτωση που είναι σωστές, θα τις στείλει στο BackEnd, αλλιώς θα εμφανίσει μήνυμα λάθους. Έπειτα, το BackEnd θα ελέγξει ξανά την ορθότητα των επιλογών του χρήστη και στην περίπτωση λάθους θα στείλει κατάλληλο μήνυμα στο UI προς εμφάνιση. Αν όλες οι επιλογές είναι ορθές, τότε θα δημιουργήσει το ερώτημα για τη βάση δεδομένων σύμφωνα με τα κριτήρια του χρήστη και θα στείλει τα λαμβανόμενα αποτελέσματα στο UI προς θέαση από τον χρήστη. Σημειώνεται πως το BackEnd θα φιλτράρει τα αποτελέσματα που θα στείλει στο UI εφόσον ο χρήστης είναι επισκέπτης.



Εικόνα 8. Διάγραμμα περίπτωσης ταιριάσματος

4.3.4.5 Διάγραμμα Περίπτωσης Ταυτοποίησης Επισκέπτη

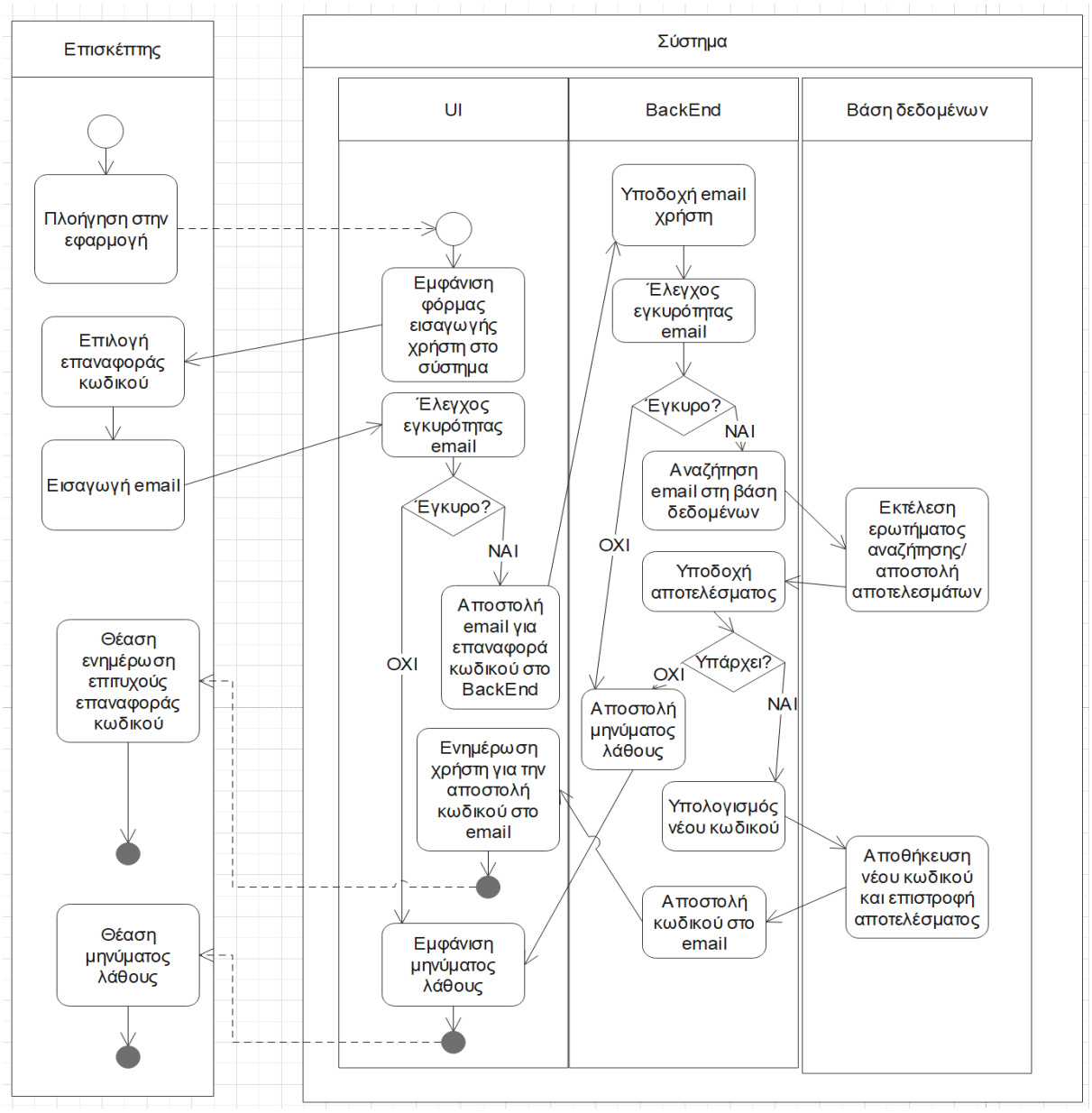
Το διάγραμμα περίπτωσης ταυτοποίησης ενός επισκέπτη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που πραγματοποιούνται για την ταυτοποίηση του στο σύστημα. Ο χρήστης θα πρέπει να πλοηγηθεί στην εφαρμογή, στη σελίδα της σύνδεσης. Έπειτα, θα πρέπει να εισάγει το όνομα χρήστη και τον κωδικό του και να τα στείλει στο σύστημα. Το UI θα κάνει έναν πρώτο έλεγχο ορθότητας των στοιχείων. Αυτός ο έλεγχος έχει να κάνει μόνο με το αν τα στοιχεία που θα δώσει ο χρήστης πληρούν τους κανόνες για τα αντίστοιχα πεδία. Αν δεν είναι ορθά. θα στείλει μήνυμα λάθους στον χρήστη, αλλιώς θα στείλει τα στοιχεία στο BackEnd. Εκεί, θα γίνει ξανά έλεγχος ορθότητας των στοιχείων όμοιος με αυτόν που γίνεται στο UI. Αν τα παρεχόμενα στοιχεία δεν περάσουν τον έλεγχο, το Backend θα στείλει μήνυμα λάθους στο UI. Αν περάσουν τον έλεγχο, τότε θα φτιάξει το ερώτημα για την αναζήτηση του χρήστη με βάση το όνομα και τον κωδικό. Αν υπάρχει ο χρήστης που ζητήθηκε, το Backend θα μηδενίσει τις ανεπιτυχείς προσπάθειες πρόσβασης του χρήστη και ο χρήστης θα εισέλθει στο σύστημα ως διαπιστευμένος χρήστης. Στην περίπτωση που δεν εντοπιστεί χρήστης με βάση τα παρεχόμενα στοιχεία, θα σταλθεί μήνυμα αποτυχίας στο UI. Αν το όνομα χρήστη υπάρχει αλλά είναι λάθος ο κωδικός, το Backend θα αυξήσει τον αριθμό των ανεπιτυχών προσβάσεων για τον συγκεκριμένο χρήστη και θα στείλει μήνυμα αποτυχίας στο UI. Όταν ο αριθμός των ανεπιτυχών προσβάσεων γίνει 3, τότε το σύστημα θα απενεργοποιήσει τον λογαριασμό του χρήστη και θα στείλει το αντίστοιχο μήνυμα στο UI προς θέαση από τον χρήστη.



Εικόνα 9. Διάγραμμα περίπτωσης ταυτοποίησης επισκέπτη

4.3.4.6 Διάγραμμα Περίπτωσης Επαναφοράς Κωδικού Επισκέπτη

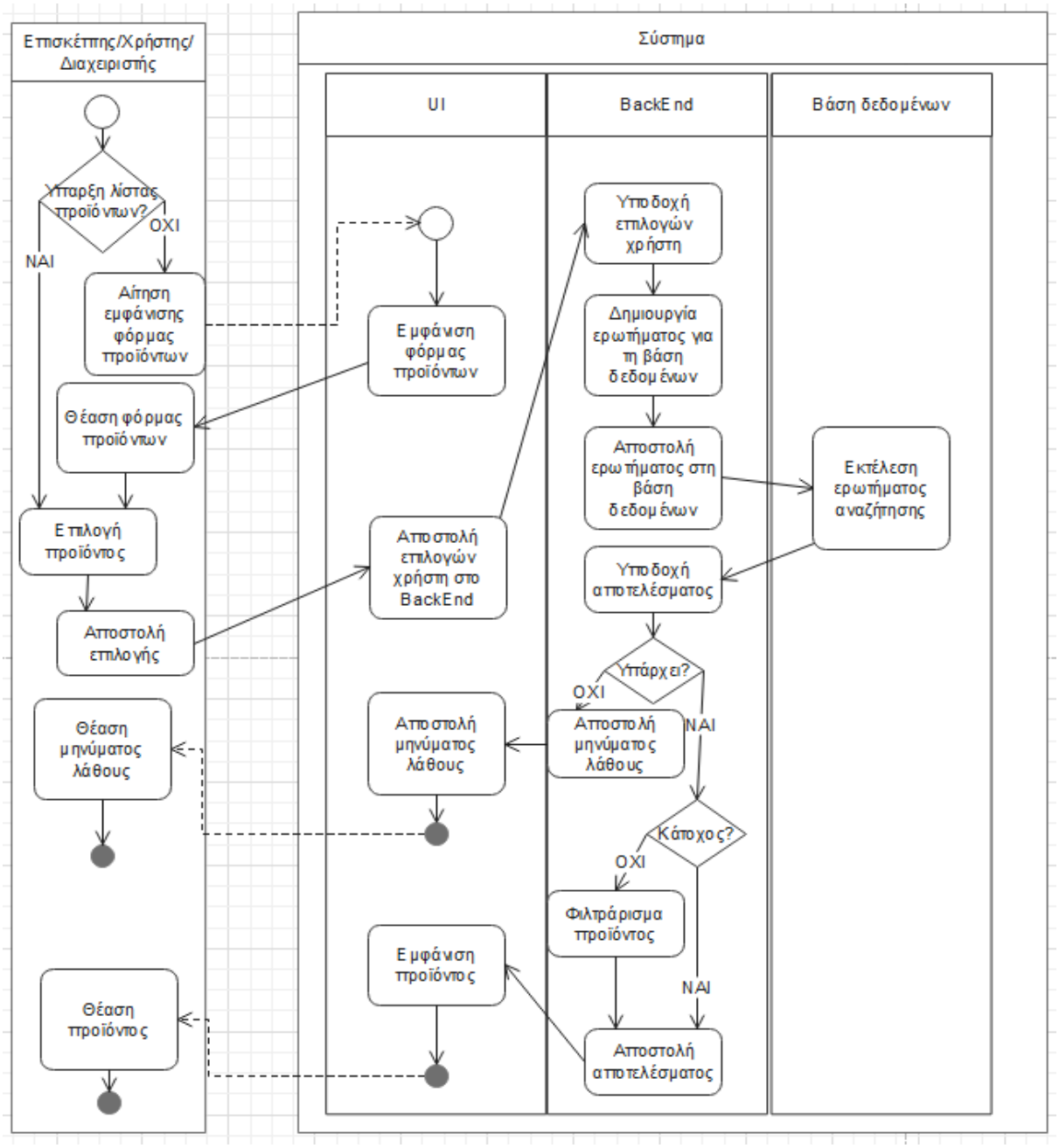
Το διάγραμμα περίπτωσης επαναφοράς κωδικού επισκέπτη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για την επαναφορά του κωδικού του. Αρχικά ο χρήστης θα πρέπει να πλοηγηθεί στην εφαρμογή και να επιλέξει την επαναφορά κωδικού. Εκεί, θα του ζητηθεί να εισάγει το email του και να το στείλει στο σύστημα. Το UI θα κάνει έναν πρώτο έλεγχο εγκυρότητας του email. Αν δεν είναι έγκυρο, θα εμφανίσει μήνυμα λάθους στον χρήστη, αλλιώς θα το στείλει στο BackEnd. Το BackEnd με τη σειρά του θα ελέγξει ξανά την εγκυρότητα του email. Αν είναι λάθος. θα στείλει αντίστοιχο μήνυμα στο UI. Αν είναι σωστό, θα αναζητήσει το email στη βάση δεδομένων. Στην περίπτωση που δεν υπάρχει, το Backend θα στείλει μήνυμα λάθους στο UI, αλλιώς θα υπολογίσει έναν καινούριο κωδικό για τον χρήστη, θα τον αποθηκεύσει στη βάση δεδομένων και θα τον στείλει στο email του χρήστη που δόθηκε.



Εικόνα 10. Διάγραμμα περίπτωσης επαναφοράς κωδικού επισκέπτη

4.3.4.7 Διάγραμμα Περίπτωσης Εμφάνισης Προϊόντος

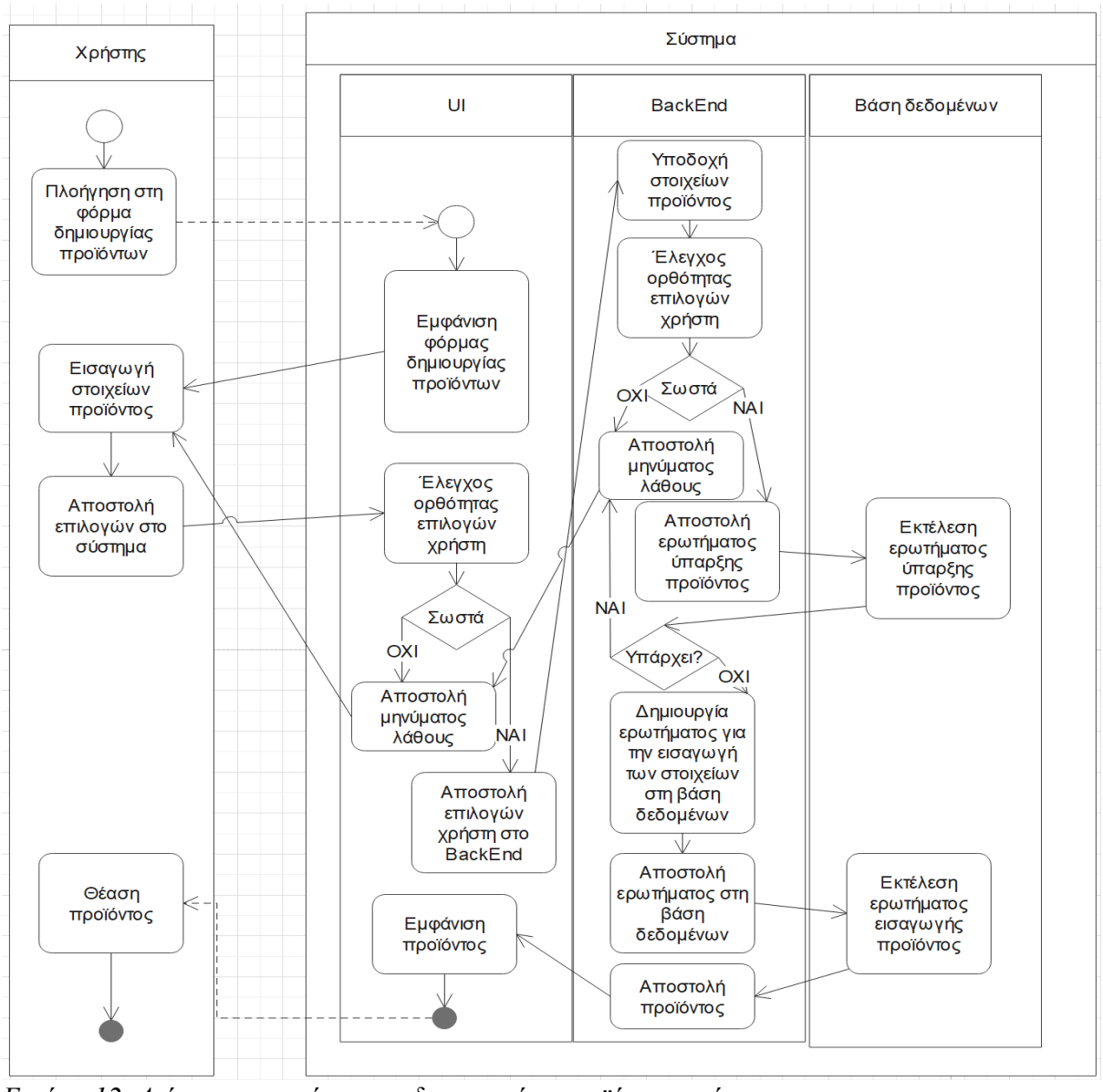
Το διάγραμμα περίπτωσης εμφάνισης προϊόντος της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για την εμφάνιση ενός προϊόντος. Ο χρήστης θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης προϊόντων. Εκεί, θα πρέπει να επιλέξει το προϊόν που επιθυμεί και το UI θα στείλει την επιλογή στο BackEnd. Το BackEnd θα ελέγξει την ύπαρξη του προϊόντος που ζητήθηκε. Αν αυτό δεν υπάρχει, θα στείλει κατάλληλο μήνυμα λάθους στο UI. Αν όμως υπάρχει, τότε το BackEnd θα στείλει τις πληροφορίες του προϊόντος στο UI προς εμφάνισή τους στον χρήστη. Σημειώνεται πως στην περίπτωση που ο χρήστης δεν είναι κάτοχος του προϊόντος, τότε οι πληροφορίες του προϊόντος θα φιλτραριστούν πριν αποσταλούν στο UI.



Εικόνα 11. Διάγραμμα περίπτωσης εμφάνισης προϊόντος

4.3.4.8 Διάγραμμα Περίπτωσης Δημιουργίας Προϊόντος Χρήστη

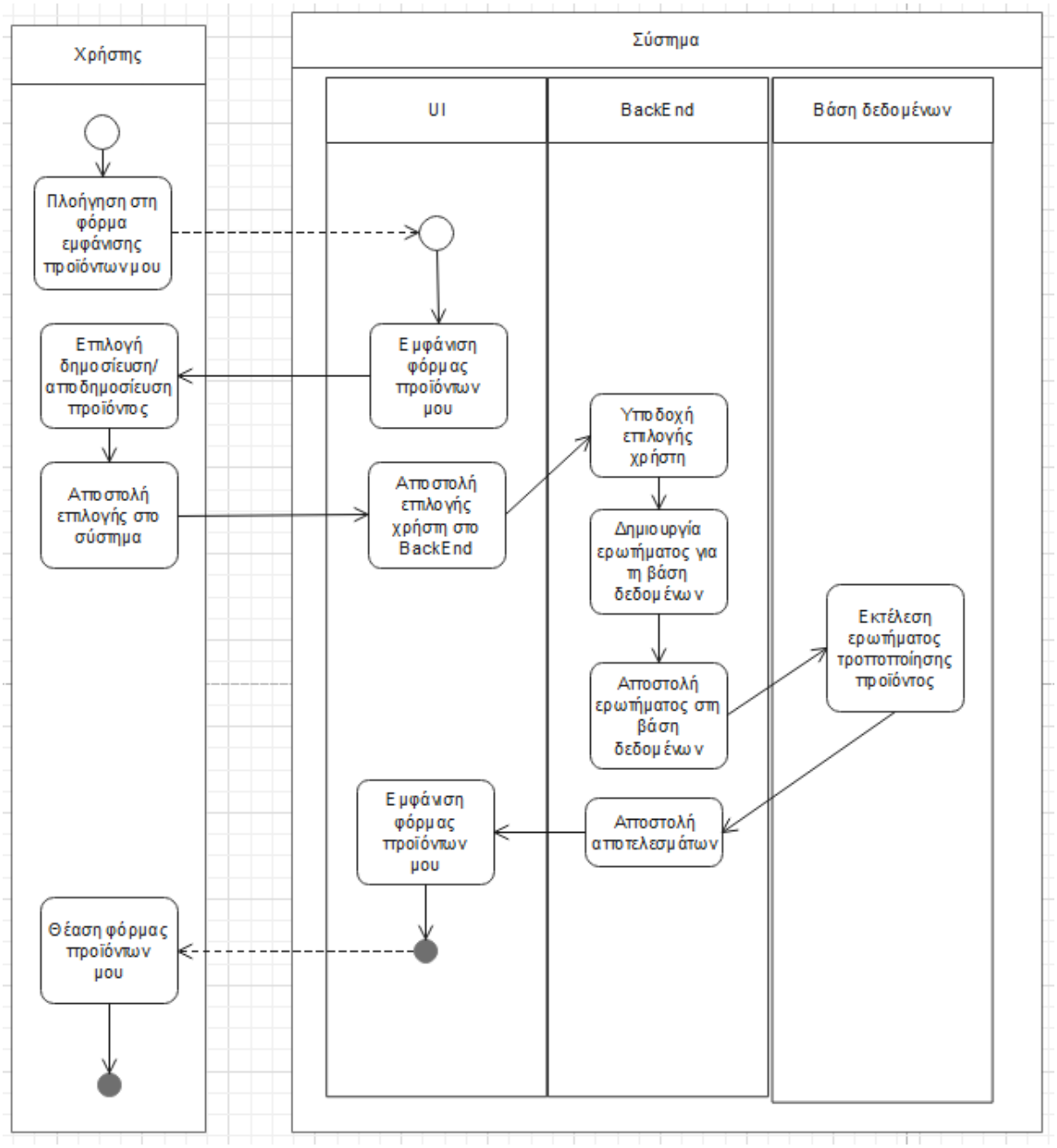
Το διάγραμμα περίπτωσης δημιουργίας προϊόντος χρήστη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που πραγματοποιούνται για τη δημιουργία ενός προϊόντος από τον χρήστη. Αρχικά, ο χρήστης θα πρέπει να πλοηγηθεί στη φόρμα δημιουργίας προϊόντος και εκεί να εισάγει τα στοιχεία που επιθυμεί και να τα στείλει στο σύστημα. Το UI θα λάβει τα στοιχεία και θα ελέγξει την ορθότητά τους. Αν αυτά δεν είναι έγκυρα, θα εμφανίσει μήνυμα λάθους στον χρήστη, διαφορετικά θα τα στείλει στο BackEnd. Το BackEnd θα ελέγξει ξανά την ορθότητα των στοιχείων. Αν αυτά είναι λάθος, θα στείλει μήνυμα σφάλματος στο UI. Αν όχι, θα ελέγξει αν το προϊόν που δίδεται από τον χρήστη υπάρχει ήδη στη βάση δεδομένων. Και σε αυτήν την περίπτωση, αν υπάρχει ήδη το προϊόν, θα στείλει κατάλληλο μήνυμα λάθους στο UI. Αν το προϊόν δεν υπάρχει, τότε θα το αποθηκεύσει στη βάση δεδομένων. Έπειτα, θα στείλει τις πληροφορίες για αυτό το καινούριο προϊόν στο UI προς θέαση από τον χρήστη.



Εικόνα 12. Διάγραμμα περίπτωσης δημιουργίας προϊόντος χρήστη

4.3.4.9 Διάγραμμα Περίπτωσης Δημοσίευσης/Αποδημοσίευσης Προϊόντος Χρήστη

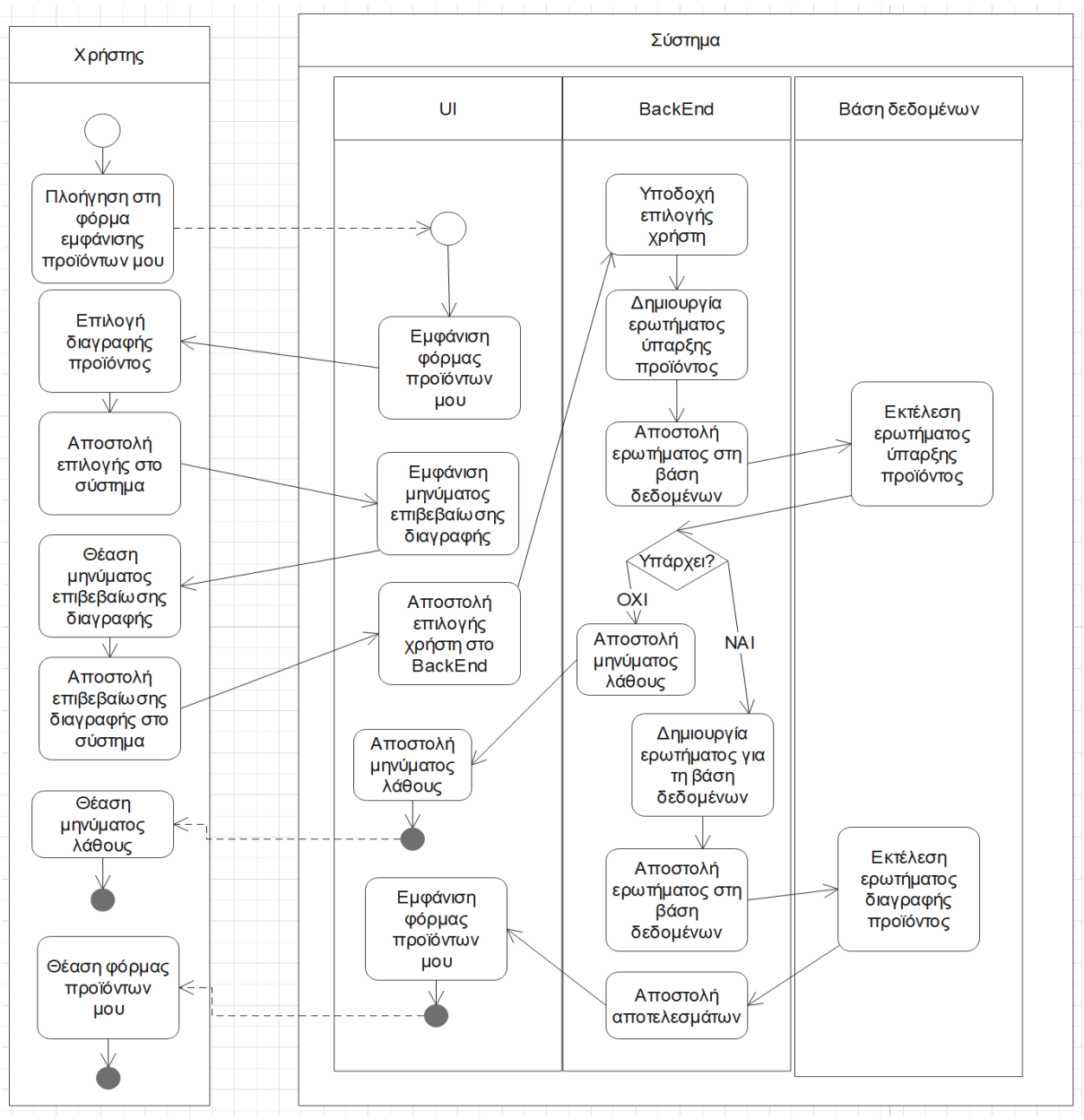
Το διάγραμμα περίπτωσης δημοσίευσης/αποδημοσίευσης προϊόντος χρήστη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που πραγματοποιούνται για αυτήν τη λειτουργία. Ο χρήστης θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης των προϊόντων του. Εκεί, θα πρέπει να επιλέξει το προϊόν που θέλει και στη συνέχεια να πατήσει δημοσίευση/αποδημοσίευση του προϊόντος. Το UI θα πάρει την επιλογή και θα τη στείλει στο BackEnd και αυτό με τη σειρά του θα εκτελέσει την ενέργεια. Τέλος, το UI θα εμφανίσει ξανά στον χρήστη την φόρμα των προϊόντων του, όπου η κατάσταση του αρχικώς επιλεγμένου προϊόντος θα έχει αλλάξει.



Εικόνα 13. Διάγραμμα περίπτωσης δημοσίευσης/αποδημοσίευσης προϊόντος χρήστη

4.3.4.10 Διάγραμμα Περίπτωσης Διαγραφής Προϊόντος Χρήστη

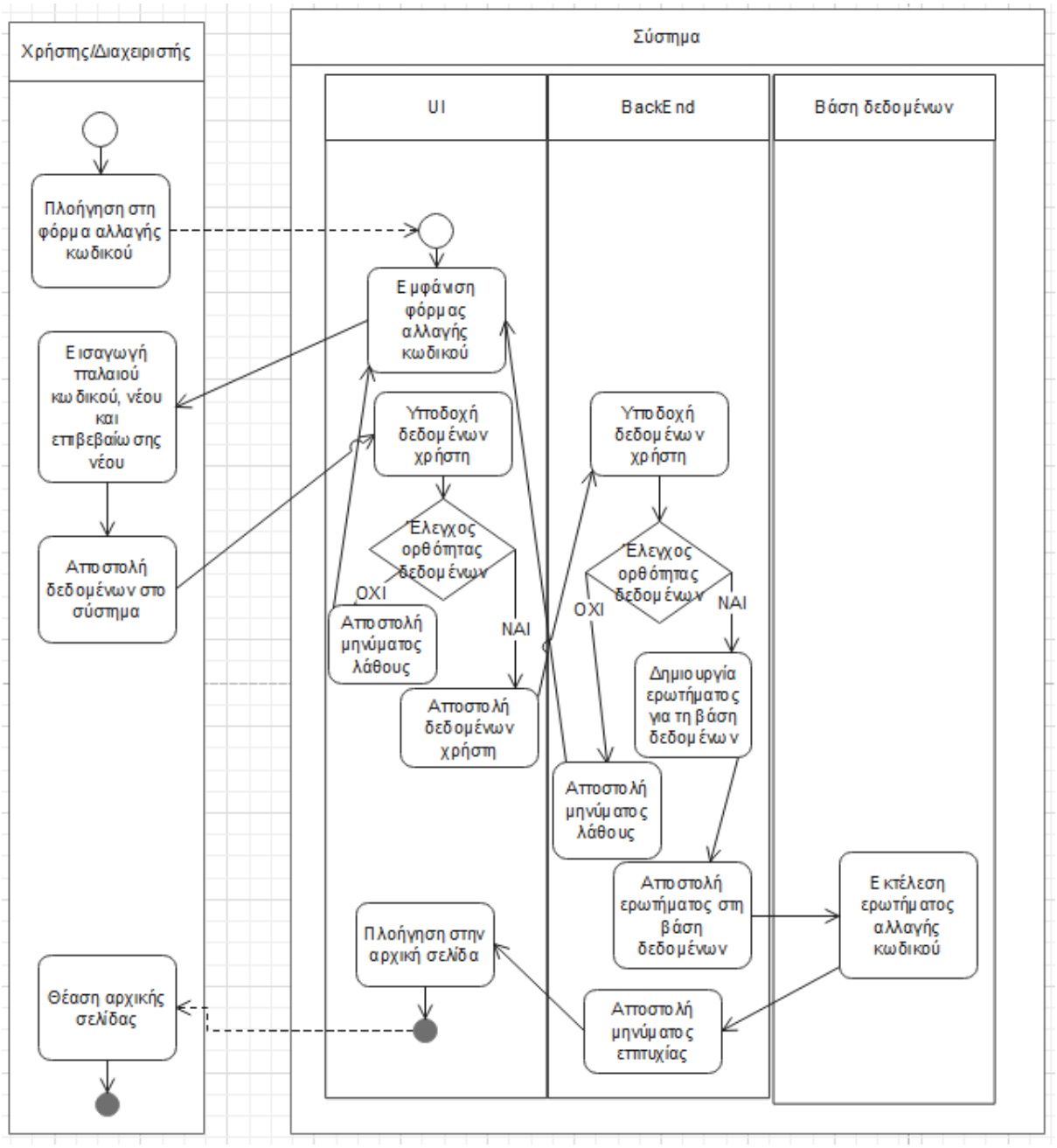
Το διάγραμμα περίπτωσης διαγραφής προϊόντος χρήστη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που πραγματοποιούνται για τη διαγραφή ενός προϊόντος. Αρχικά, ο χρήστης θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης των προϊόντων του, να επιλέξει το προϊόν που επιθυμεί και στη συνέχεια να πατήσει διαγραφή. Έπειτα, στο μήνυμα επιβεβαίωσης που θα του εμφανιστεί θα πρέπει να πατήσει ξανά επιβεβαίωση. Κατόπιν, το UI θα στείλει την επιλογή του χρήστη στο BackEnd. Το τελευταίο θα ελέγξει την ύπαρξη του προϊόντος στη βάση δεδομένων. Αν το προϊόν δεν υπάρχει, θα στείλει κατάλληλο μήνυμα λάθους στο UI, αλλιώς θα το διαγράψει. Στην τελευταία περίπτωση, η φόρμα των προϊόντων του εμφανίζεται στο χρήστη όπου το αρχικώς επιλεγμένο προϊόν πλέον δεν υπάρχει.



Εικόνα 14. Διάγραμμα περίπτωσης διαγραφής προϊόντος χρήστη

4.3.4.11 Διάγραμμα Περίπτωσης Αλλαγής Κωδικού Χρήστη

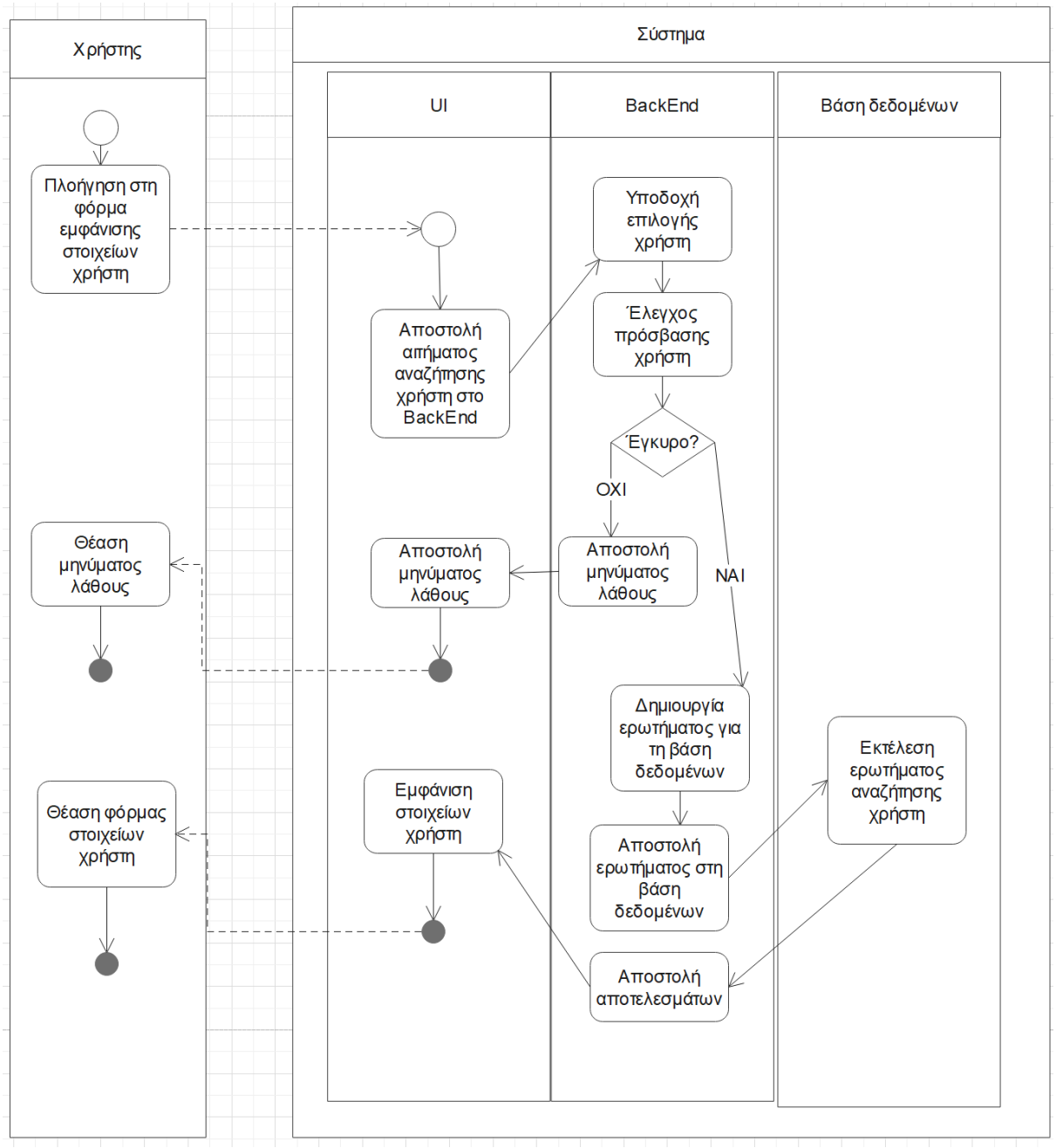
Το διάγραμμα περίπτωσης αλλαγής κωδικού χρήστη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για την αλλαγή του κωδικού. Ο χρήστης θα πρέπει να πλοηγηθεί στη φόρμα αλλαγής κωδικού, να εισάγει τα στοιχεία που θα του ζητηθούν και να τα στείλει στο σύστημα. Το UI αρχικά θα ελέγξει την ορθότητα των δεδομένων του χρήστη. Αν υπάρχει κάποιο σφάλμα θα εμφανίσει μήνυμα λάθους στον χρήστη, αλλιώς θα τα στείλει στο BackEnd. Εκεί, θα γίνει ξανά έλεγχος ορθότητας των δεδομένων. Αν υπάρχει λάθος, το BackEnd θα στείλει κατάλληλο μήνυμα στο UI, αλλιώς θα προχωρήσει σε αλλαγή κωδικού του χρήστη και θα στείλει μήνυμα επιτυχίας στο UI.



Εικόνα 15. Διάγραμμα περίπτωσης αλλαγής κωδικού χρήστη

4.3.4.12 Διάγραμμα Περίπτωσης Εμφάνισης Χρήστη

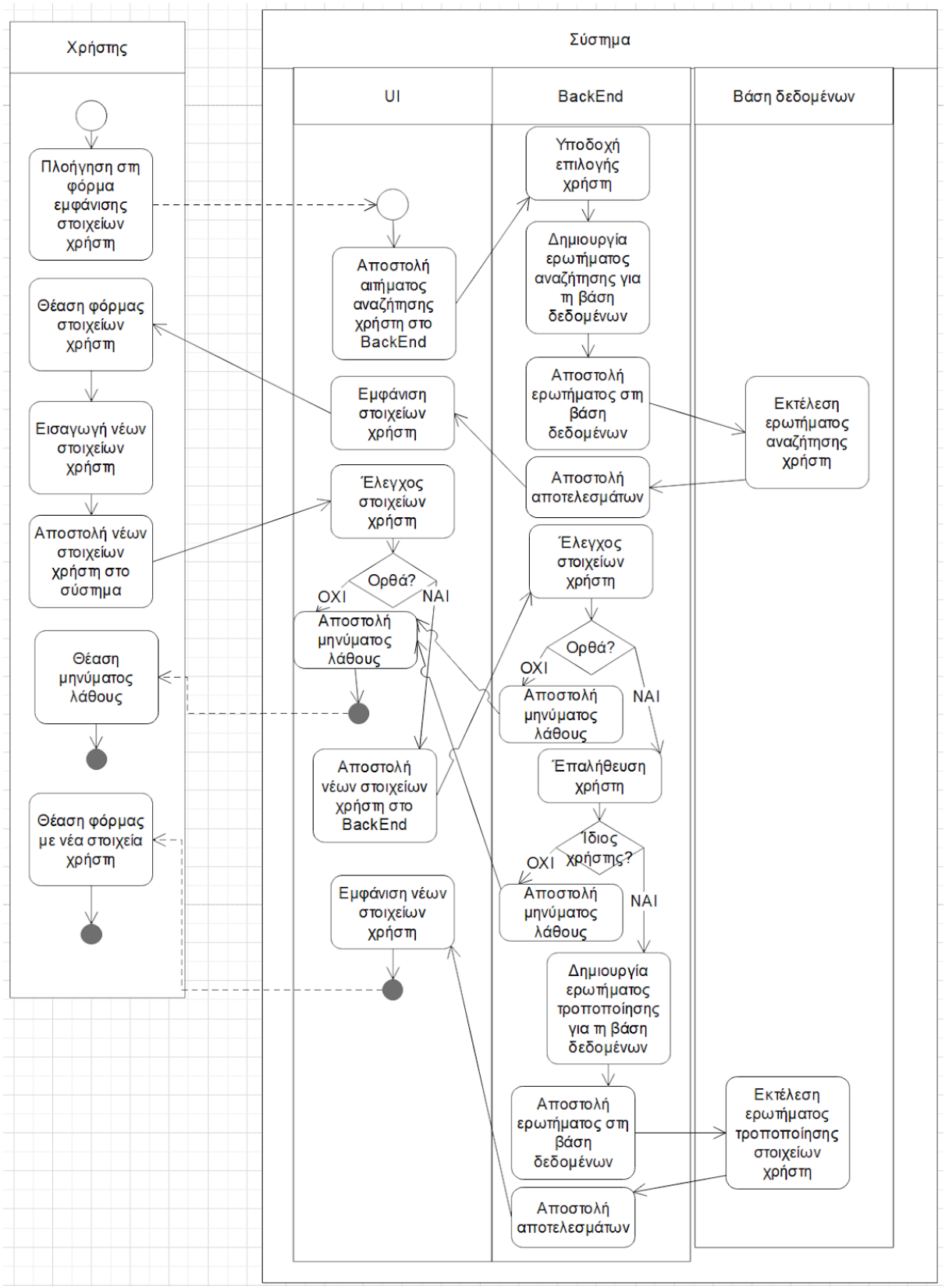
Το διάγραμμα περίπτωσης εμφάνισης χρήστη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για την εμφάνιση των στοιχείων ενός χρήστη. Ο χρήστης θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης των στοιχείων χρήστη. Στη συνέχεια το UI θα στείλει το αίτημα αναζήτησης χρήστη στο BackEnd, το οποίο θα ελέγξει αν ο χρήστης έχει πρόσβαση σε αυτά τα δεδομένα. Σε περίπτωση που έχει, το BackEnd θα στείλει τα δεδομένα που ζητήθηκαν στο UI, αφού τα λάβει από τη βάση δεδομένων. Αλλιώς, θα στείλει μήνυμα λάθους.



Εικόνα 16. Διάγραμμα περίπτωσης εμφάνισης χρήστη

4.3.4.13 Διάγραμμα Περίπτωσης Επεξεργασίας Χρήστη

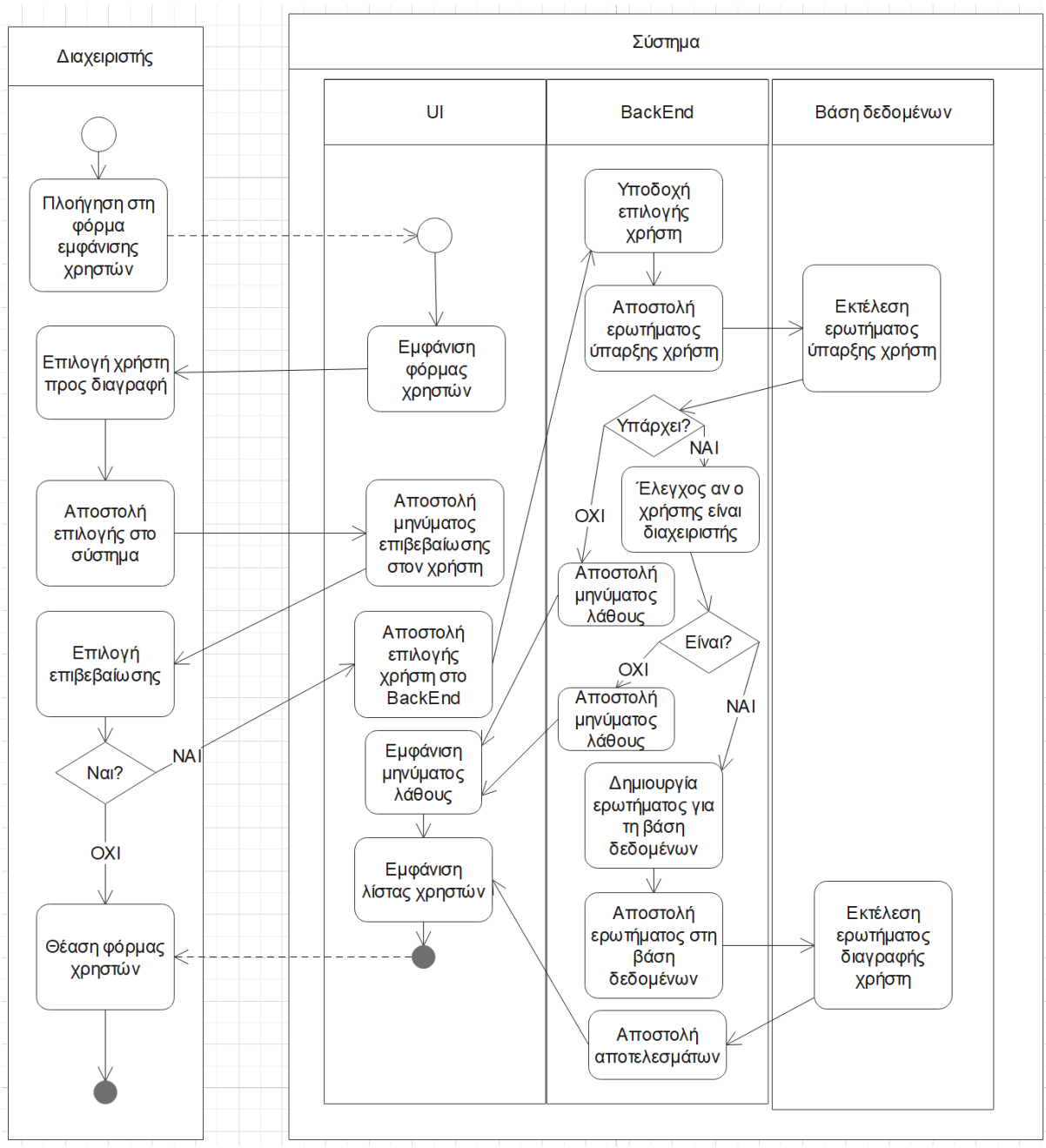
Το διάγραμμα περίπτωσης επεξεργασίας χρήστη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που πραγματοποιούνται για την επεξεργασία των στοιχείων ενός χρήστη. Για να γίνει αυτό, ο χρήστης θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης στοιχείων χρήστη, να εισάγει τα νέα στοιχεία που επιθυμεί και να τα στείλει στο σύστημα. Το UI αφού κάνει έναν πρώτο έλεγχο ως προς την ορθότητα των στοιχείων, θα τα στείλει στο BackEnd εφόσον είναι σωστά, αλλιώς θα εμφανίσει μήνυμα λάθους στον χρήστη. Το BackEnd θα ελέγξει ξανά την ορθότητα των στοιχείων που θα του δοθούν. Αν αυτά είναι ορθά και ο χρήστης που αιτείται την επεξεργασία είναι ίδιος με τον χρήστη για τον οποίο θα πραγματοποιηθεί η επεξεργασία καθώς και ο χρήστης υπάρχει στη βάση δεδομένων, τότε θα προχωρήσει στις αλλαγές που ζητήθηκαν. Διαφορετικά, θα στείλει ένα μήνυμα λάθους στο UI.



Εικόνα 17. Διάγραμμα περίπτωσης επεξεργασίας χρήστη

4.3.4.14 Διάγραμμα Περίπτωσης Διαγραφής Χρήστη από Διαχειριστή

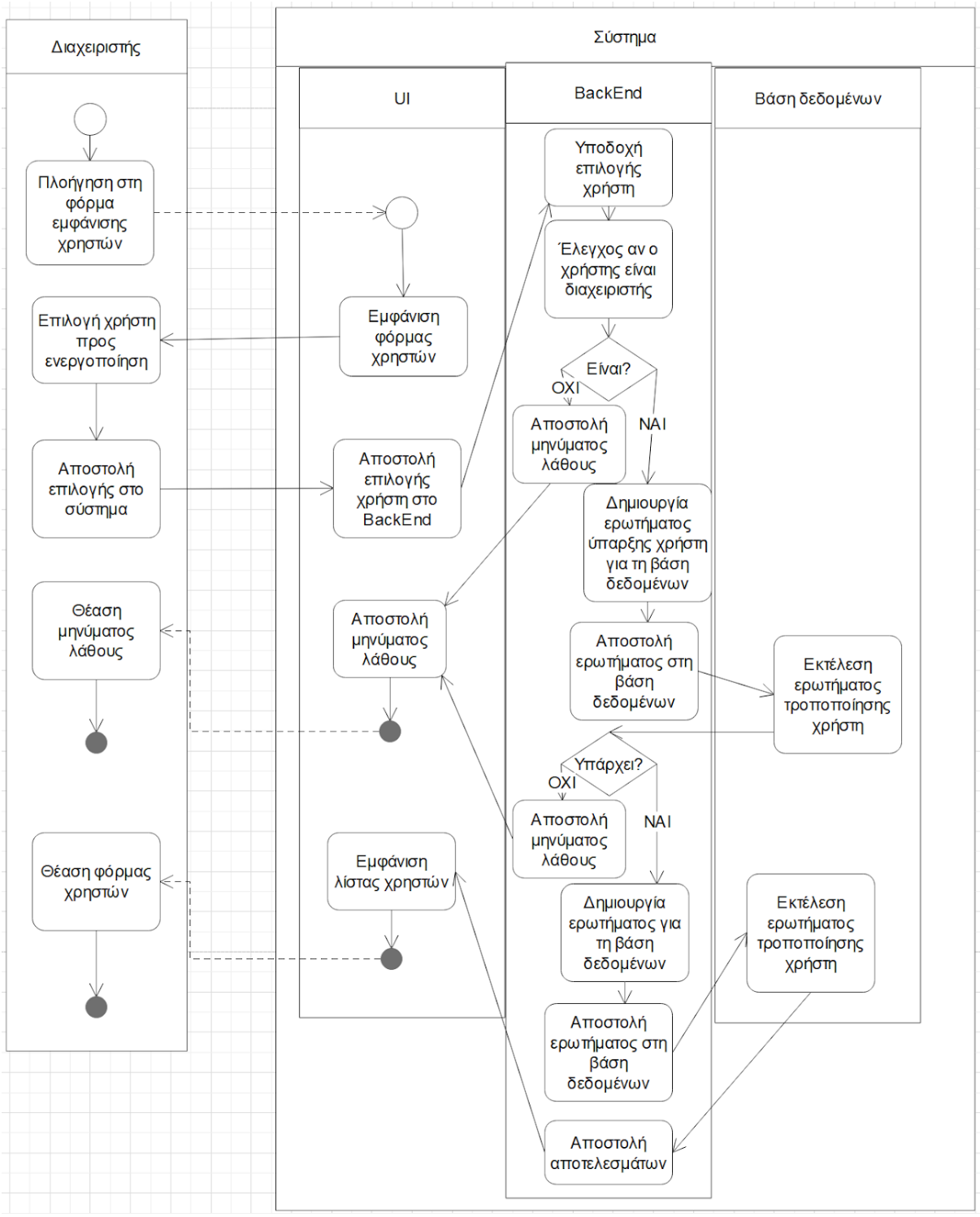
Το διάγραμμα περίπτωσης διαγραφής χρήστη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που πραγματοποιούνται για τη διαγραφή ενός χρήστη από τον διαχειριστή. Ο διαχειριστής θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης χρηστών και να επιλέξει τον χρήστη προς διαγραφή, πατώντας ξανά επιβεβαίωση της επιλογής του στο μήνυμα που θα του εμφανιστεί. Το UI αφού υποδεχθεί την επιλογή, θα τη στείλει στο BackEnd. Εκεί, θα γίνει έλεγχος ύπαρξης του χρήστη και αν ο χρήστης που αιτείται τη διαγραφή είναι ο διαχειριστής. Εφόσον ισχύουν και τα δυο, το BackEnd θα προχωρήσει σε διαγραφή του χρήστη. Διαφορετικά, θα στείλει μήνυμα λάθους στο UI.



Εικόνα 18. Διάγραμμα περίπτωσης διαγραφής χρήστη διαχειριστή

4.3.4.15 Διάγραμμα Περίπτωσης Ενεργοποίησης Χρήστη από Διαχειριστή

Το διάγραμμα περίπτωσης ενεργοποίησης χρήστη της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για την ενεργοποίηση ενός χρήστη από τον διαχειριστή. Ο διαχειριστής θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης χρηστών και να επιλέξει τον επιθυμητό χρήστη προς ενεργοποίηση. Το UI στη συνέχεια θα αποστείλει την επιλογή στο BackEnd, το οποίο θα ελέγξει αν ο χρήστης που αιτείται την ενεργοποίηση είναι διαχειριστής. Στην περίπτωση που αυτό ισχύει, το BackEnd θα ενεργοποιήσει τον χρήστη εφόσον αυτός υπάρχει. Αν ο χρήστης προς ενεργοποίηση δεν υπάρχει ή ο χρήστης που αιτείται την ενεργοποίηση δεν είναι διαχειριστής, το BackEnd θα στείλει κατάλληλο μήνυμα λάθους στο UI προς θέαση από τον χρήστη.

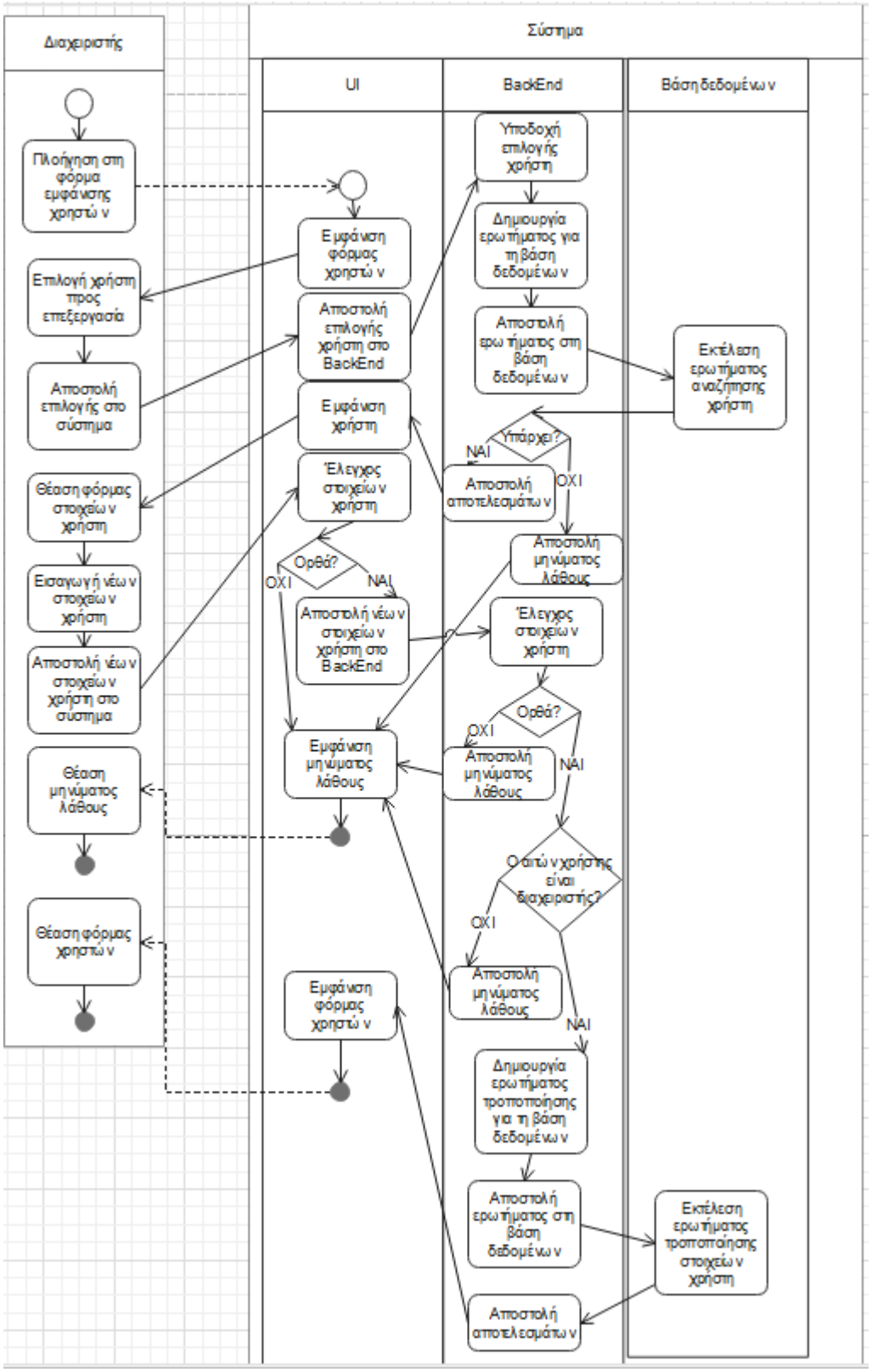


Εικόνα 19. Διάγραμμα περίπτωσης ενεργοποίησης χρήστη από διαχειριστή

4.3.4.16 Διάγραμμα Περίπτωσης Επεξεργασίας Χρήστη από Διαχειριστή

Το διάγραμμα περίπτωσης επεξεργασίας χρήστη από τον διαχειριστή της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για την επεξεργασία των στοιχείων ενός χρήστη (από τον διαχειριστή). Ο διαχειριστής θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης χρηστών και εκεί να επιλέξει τον χρήστη προς επεξεργασία. Στη συνέχεια το UI θα στείλει την επιλογή του διαχειριστή

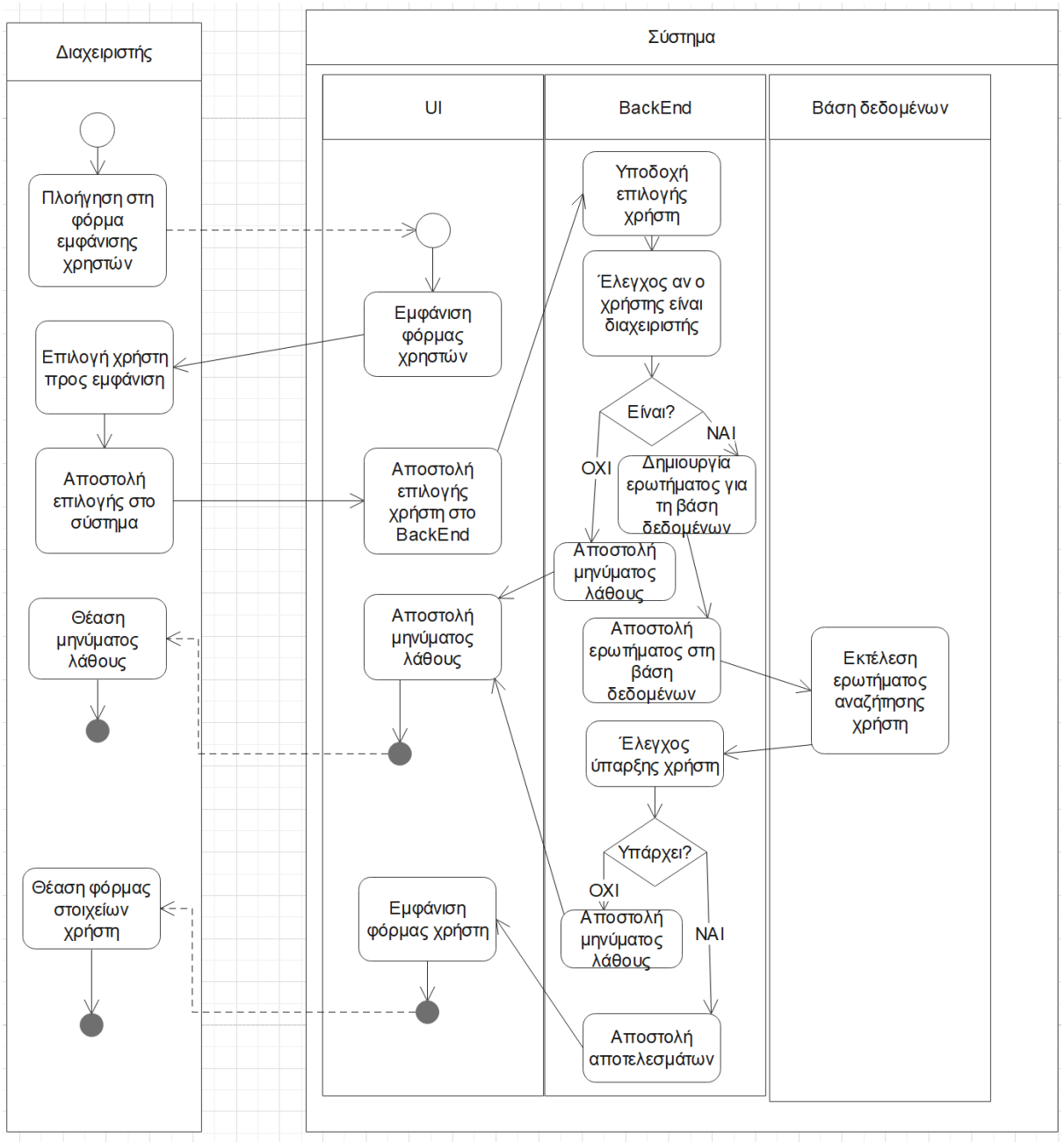
στο BackEnd και αυτό θα ελέγξει αν ο χρήστης προς επεξεργασία υπάρχει. Αν αυτός δεν υπάρχει, το BackEnd θα στείλει μήνυμα λάθους, αλλιώς θα στείλει τα στοιχεία του χρήστη στο UI για να τα εμφανίσει στον διαχειριστή. Έπειτα, ο διαχειριστής θα εισάγει τα νέα στοιχεία που επιθυμεί και θα τα στείλει στο UI, το οποίο θα κάνει έναν πρώτο έλεγχο ορθότητας αυτών. Αν δεν υπάρχει σφάλμα, θα στείλει τα στοιχεία αυτά στο BackEnd, αλλιώς θα εμφανίσει μήνυμα λάθους. Έπειτα, το BackEnd θα ελέγξει εκ νέου την ορθότητα των δεδομένων που θα λάβει και αν ο χρήστης που πραγματοποιεί την αίτηση είναι όντως διαχειριστής. Εφόσον ισχύουν και τα δυο, τότε θα πραγματοποιήσει τις αλλαγές που ζητήθηκαν και θα στείλει τα αποτελέσματα στο UI προς θέαση από τον χρήστη. Σε αντίθετη περίπτωση, το BackEnd θα στείλει το κατάλληλο μήνυμα λάθους στο UI.



Εικόνα 20. Διάγραμμα περίπτωσης επεξεργασίας χρήστη από διαχειριστή

4.3.4.17 Διάγραμμα Περίπτωσης Εμφάνισης Χρήστη από Διαχειριστή

Το διάγραμμα περίπτωσης εμφάνισης χρήστη από τον διαχειριστή της παρακάτω εικόνας περιλαμβάνει τις ενέργειες που γίνονται για την εμφάνιση των στοιχείων ενός χρήστη (από τον διαχειριστή). Αρχικά, ο διαχειριστής θα πρέπει να πλοηγηθεί στη φόρμα εμφάνισης χρηστών και να επιλέξει τον χρήστη που επιθυμεί προς εμφάνιση. Το UI θα λάβει την επιλογή και θα τη στείλει στο BackEnd, το οποίο θα ελέγξει αν ο χρήστης από τον οποίον προήλθε το αίτημα είναι ο διαχειριστής. Αν δεν είναι, θα στείλει μήνυμα λάθους. Διαφορετικά, θα ελέγξει αν υπάρχει ο χρήστης προς εμφάνιση. Στην περίπτωση που ο χρήστης υπάρχει, το BackEnd θα στείλει τα αποτελέσματα στο UI προς εμφάνιση, αλλιώς θα στείλει μήνυμα λάθους.



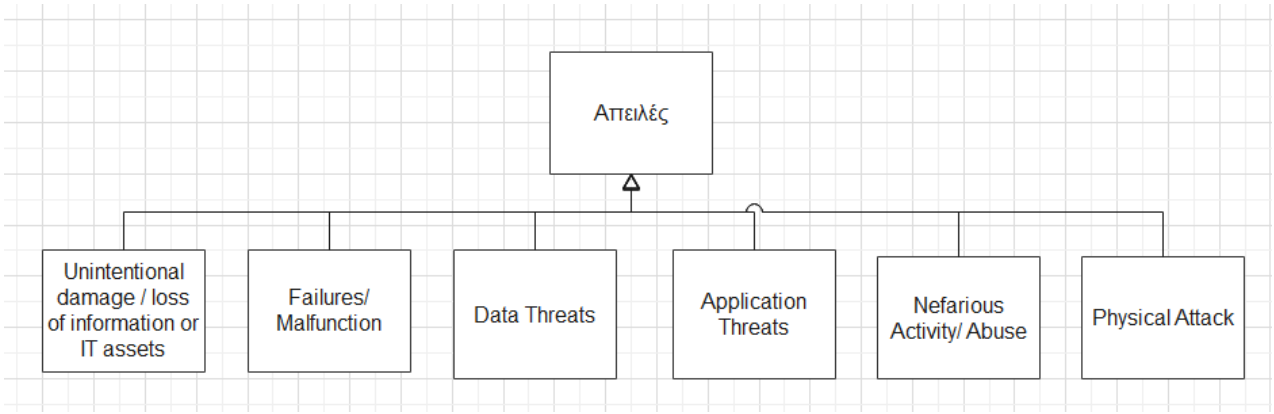
Εικόνα 21. Διάγραμμα περίπτωσης εμφάνισης χρήστη από διαχειριστή

4.3.5 Διαγράμματα Κλάσεων

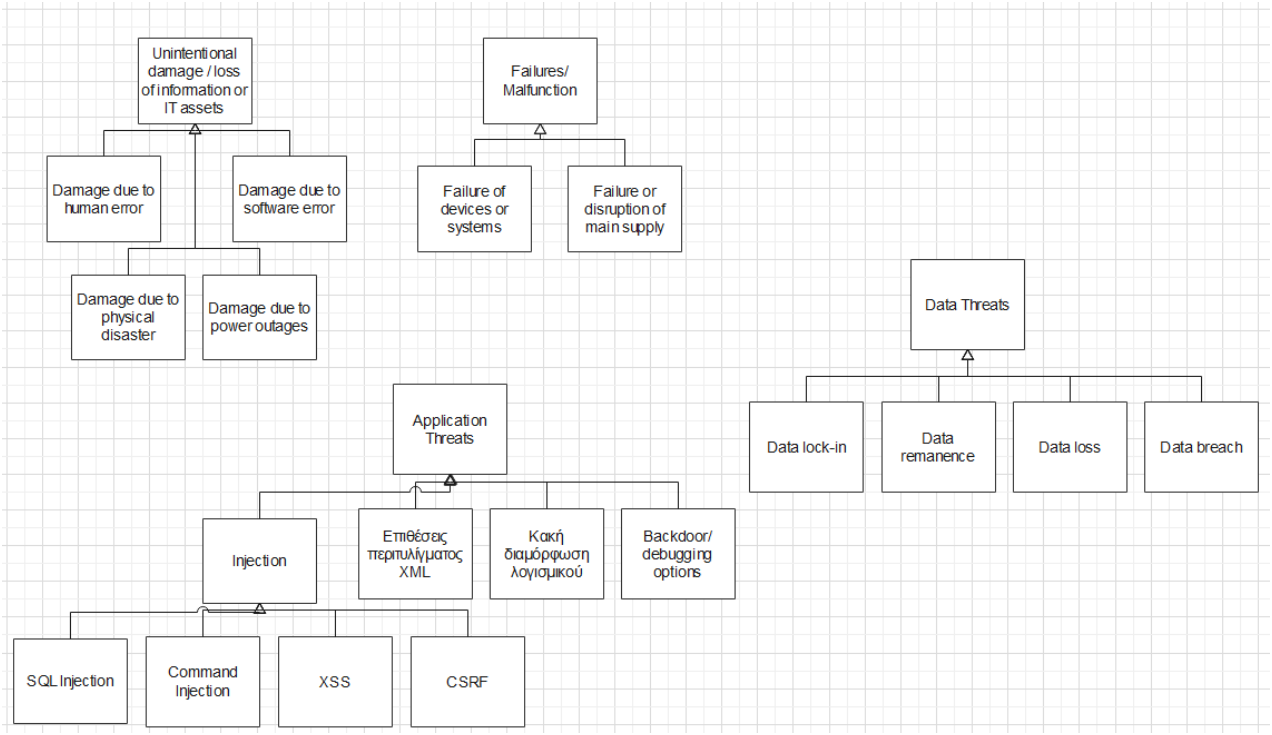
Αφιερώσαμε ένα σύνολο από διαγράμματα κλάσεων για να καλύψουμε τη μοντελοποίηση των βασικών οντοτήτων του συστήματός μας. Τα πρώτα διαγράμματα παρουσιάζουν ιεραρχίες οντοτήτων για τις βασικές οντότητες των απειλών και των μηχανισμών ασφάλειας. Συνεπώς, παρέχουν μια ευρεία ταξινόμηση τόσο για απειλές που ενδέχεται να αντιμετωπίζουν τα προϊόντα SecaaS όσο και για μηχανισμούς ασφάλειας που μπορεί να ενσωματώνουν αυτά. Το τελευταίο διάγραμμα καλύπτει τις υπόλοιπες βασικές οντότητες του συστήματος, που είναι οι χρήστες και τα προϊόντα SecaaS, τις δευτερεύοντες οντότητες, καθώς και τις συσχετίσεις μεταξύ όλων αυτών των οντοτήτων.

4.3.5.1 Απειλές

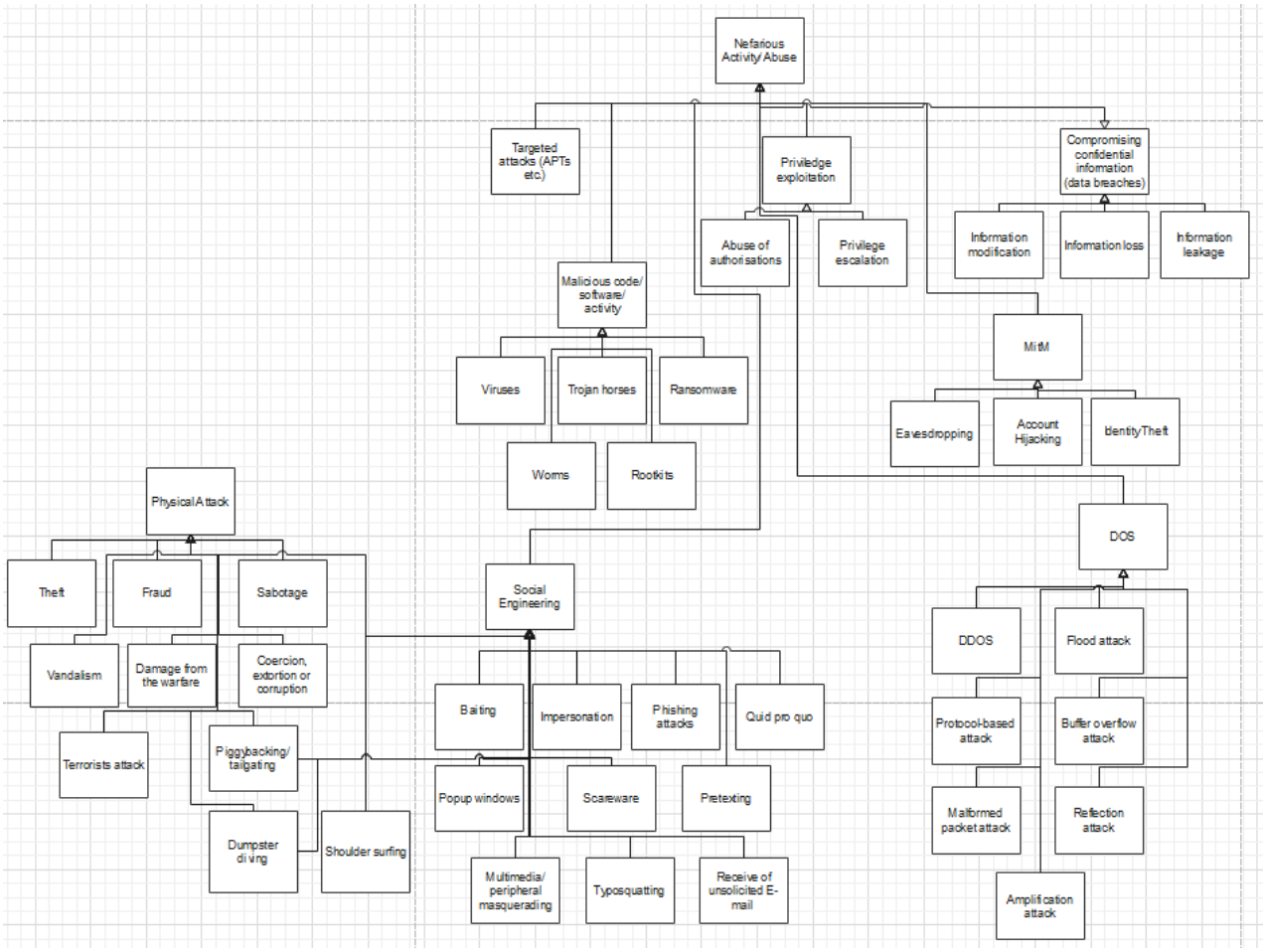
Λόγω της βαθιάς ιεράρχησης των απειλών, που αντιμετωπίζουν τα προϊόντα SecaaS, στην οποία έχουμε προχωρήσει, αποφασίστηκε η τμηματική παρουσίασή της με τη μορφή τριών διαγραμμάτων κλάσεων. Στην Εικόνα 22 βλέπουμε ένα διάγραμμα κλάσεων που απεικονίζει τις βασικές κατηγορίες των απειλών, ενώ στις Εικόνες 23 και 24 βλέπουμε δύο αντίστοιχα διαγράμματα κλάσεων που αναλύουν τις κατηγορίες αυτές στις υποκατηγορίες τους.



Εικόνα 22. Διάγραμμα κλάσεων για την ιεραρχία απειλών (μέρος Α)



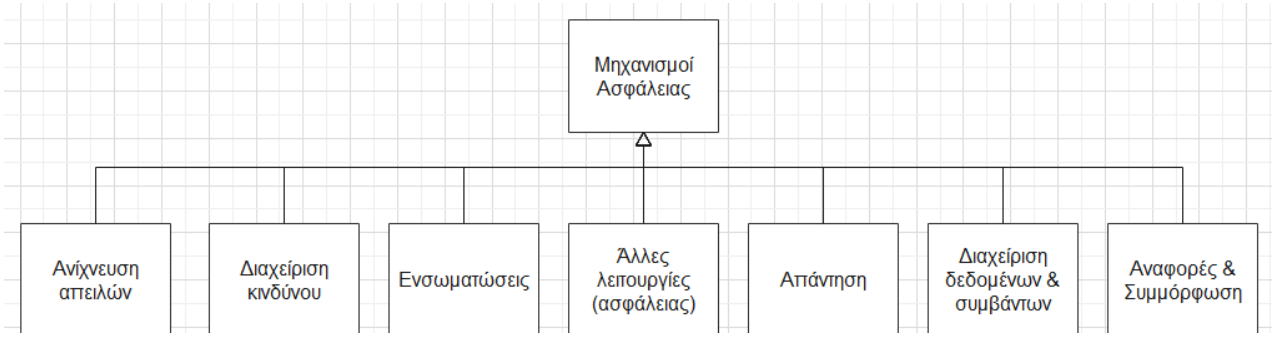
Εικόνα 23. Διάγραμμα κλάσεων για την ιεραρχία απειλών (μέρος Β)



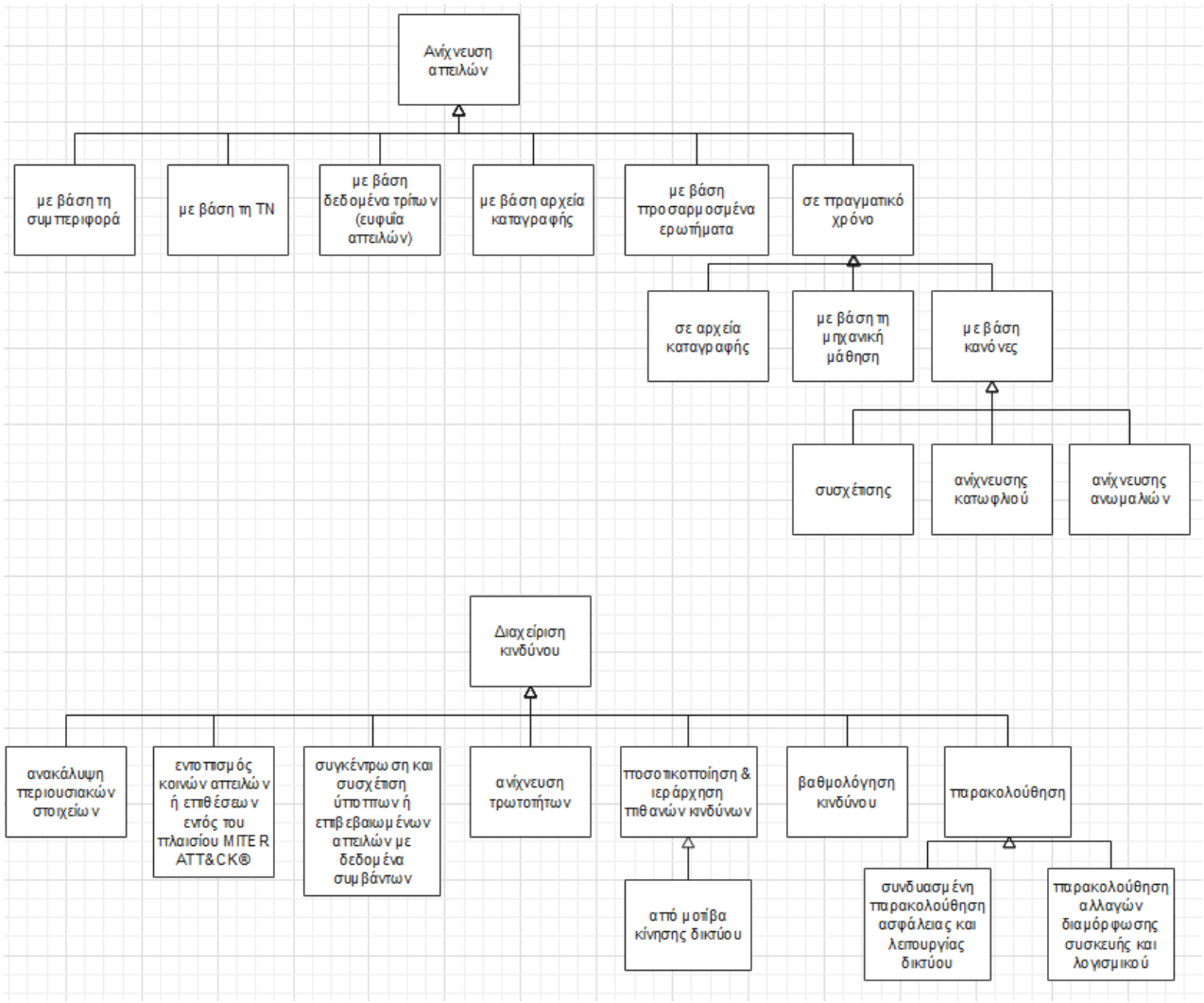
Εικόνα 24. Διάγραμμα κλάσεων για την ιεραρχία απειλών (μέρος Γ)

4.3.5.2 Μηχανισμοί Ασφάλειας για την SIEM Κατηγορία των Προϊόντων SecaaS

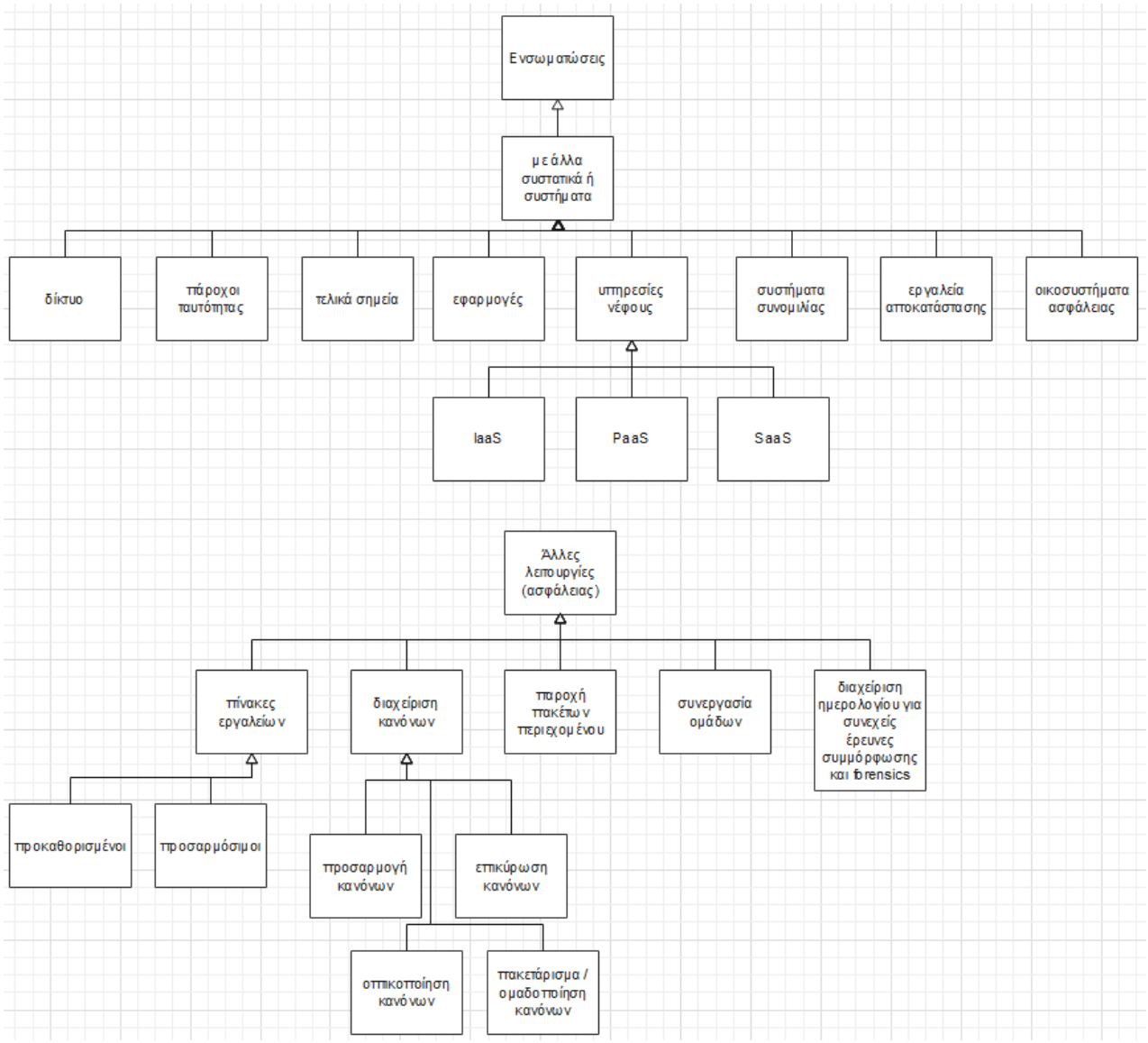
Τα διαγράμματα ER για τους μηχανισμούς ασφαλείας περιλαμβάνουν μια εκτεταμένη ιεραρχία των μηχανισμών ασφαλείας που μπορεί να ενσωματώνουν τα προϊόντα SecaaS της κατηγορίας SIEM. Ουσιαστικά έχουμε μια σειρά από διαγράμματα λόγω περιορισμών στην παρουσίαση ενός σύνθετου διαγράμματος που να καλύπτει πλήρως την εκτεταμένη ιεραρχία. Στην Εικόνα 25 βλέπουμε τις βασικές κατηγορίες των μηχανισμών ασφάλειας, ενώ στις Εικόνες 26 με 30 βλέπουμε την ανάλυση των βασικών κατηγοριών στις υποκατηγορίες τους.



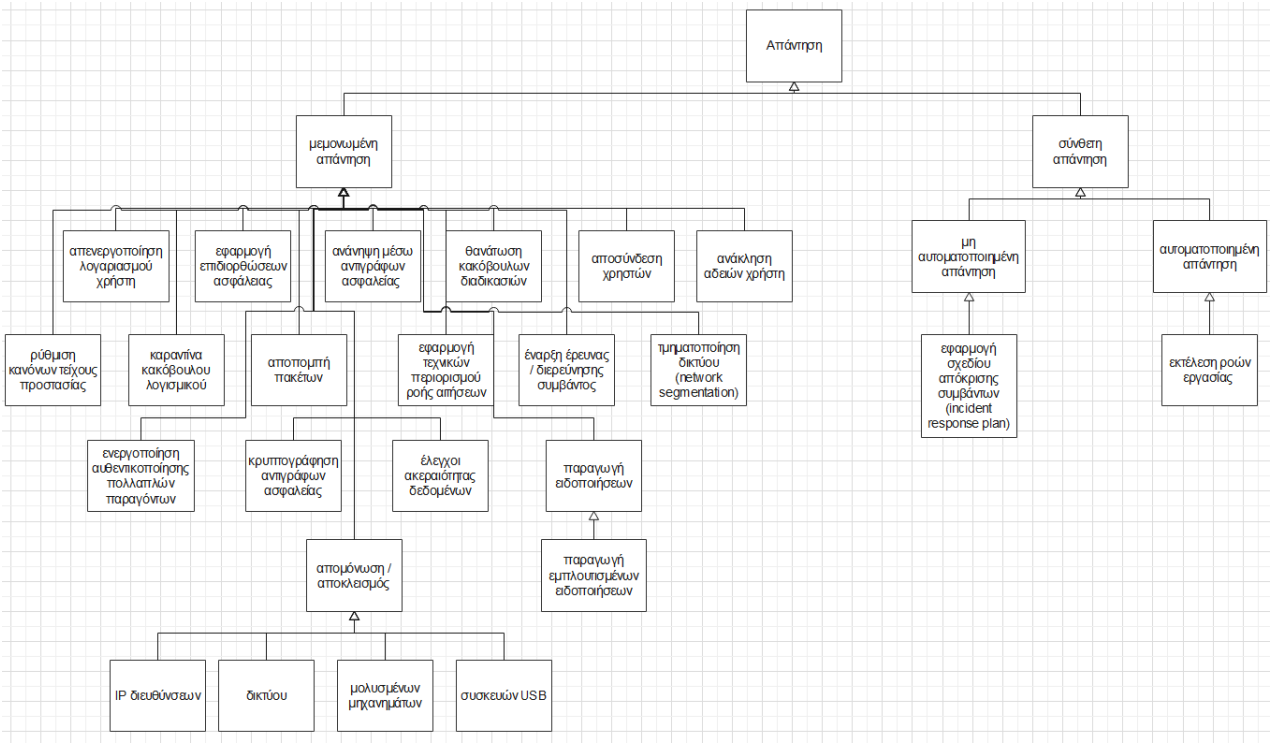
Εικόνα 25. Διάγραμμα κλάσεων για την ιεραρχία μηχανισμών ασφαλείας (μέρος Α)



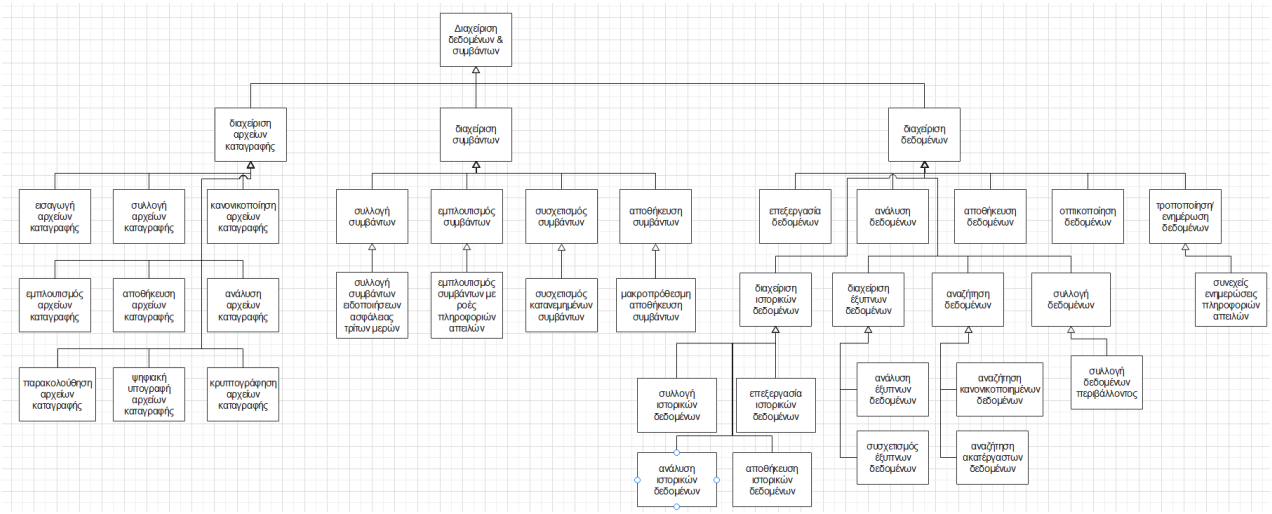
Εικόνα 26. Διάγραμμα κλάσεων για την ιεραρχία μηχανισμών ασφαλείας (μέρος Β)



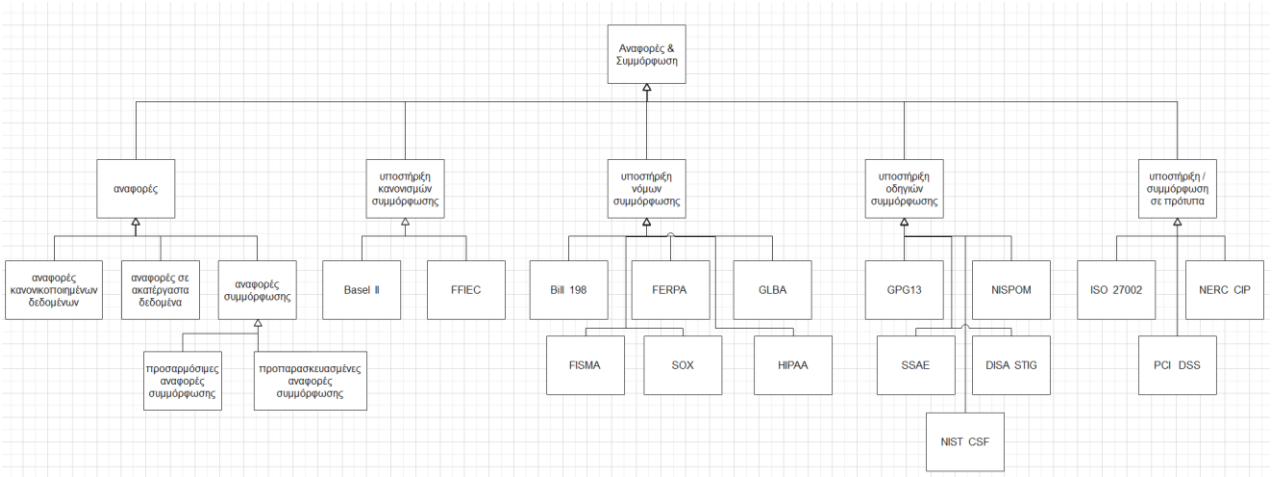
Εικόνα 27. Διάγραμμα κλάσεων για την ιεραρχία μηχανισμών ασφαλείας (μέρος Γ)



Εικόνα 28. Διάγραμμα κλάσεων για την ιεραρχία μηχανισμών ασφαλείας (μέρος Δ)



Εικόνα 29. Διάγραμμα κλάσεων για την ιεραρχία μηχανισμών ασφαλείας (μέρος Ε)



Εικόνα 30. Διάγραμμα κλάσεων για την ιεραρχία μηχανισμών ασφαλείας (μέρος ΣΤ)

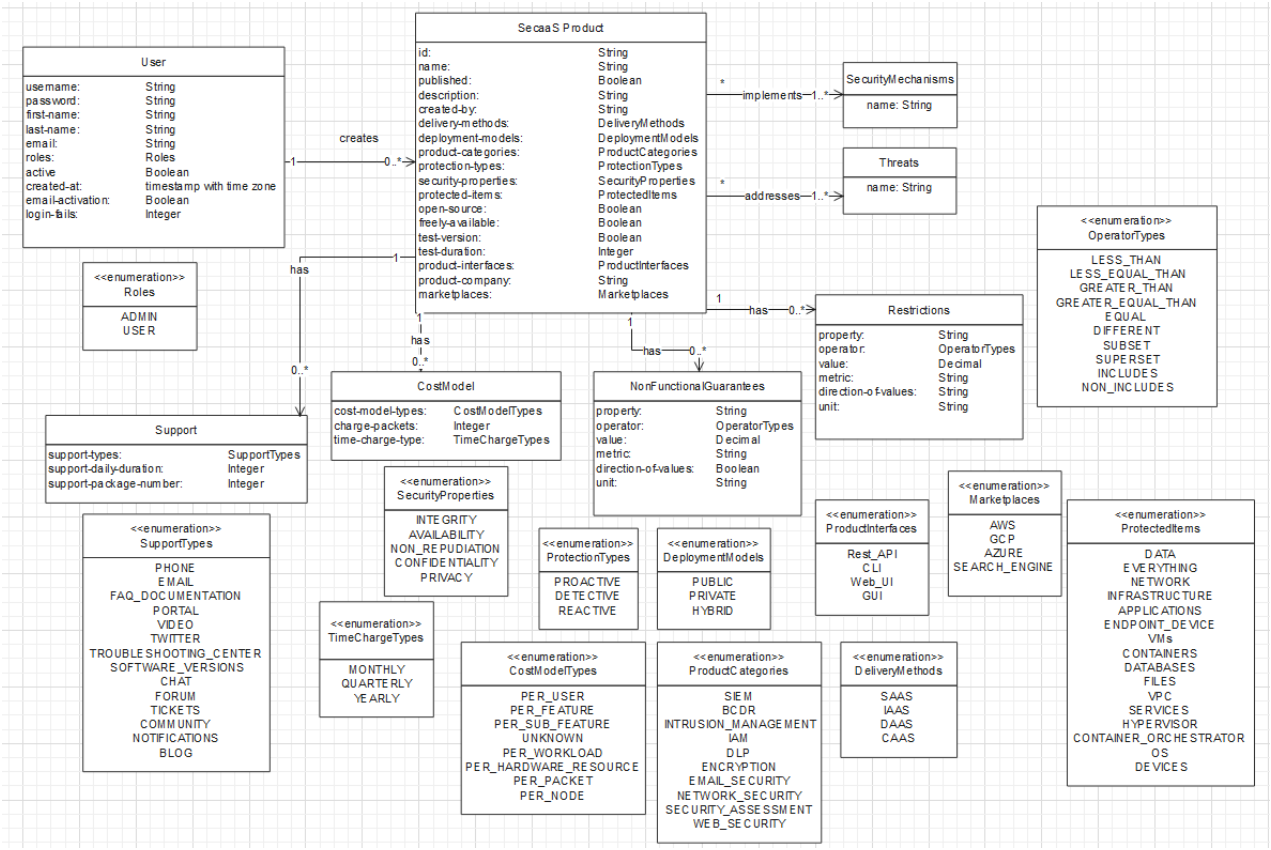
4.3.5.3 Χρήστες και Προϊόντα SecaaS

Το διάγραμμα κλάσεων λογισμικού/εφαρμογής που φαίνεται στην Εικόνα 31, περιλαμβάνει τις δυο βασικές οντότητες του συστήματος, οι οποίες είναι οι χρήστες και τα προϊόντα, τις δευτερεύουσες οντότητες (όπως το μοντέλου κόστους και οι μη λειτουργικές εγγυήσεις), τις ιδιότητες όλων αυτών των οντοτήτων καθώς και τις συσχετίσεις μεταξύ τους.

Η οντότητα χρήστης, όπως βλέπουμε στην παρακάτω εικόνα, περιλαμβάνει τις εξής ιδιότητες: όνομα χρήστη, κωδικό, όνομα, επώνυμο, διεύθυνση ηλεκτρονικού ταχυδρομείου, ρόλους, ένδειξη αν είναι ενεργός, ημερομηνία δημιουργίας, ένδειξη αν ο χρήστης έχει ενεργοποιηθεί μέσω email και αριθμό αποτυχημένων προσπαθειών σύνδεσης. Το όνομα χρήστη αποτελεί και το αναγνωριστικό του κάθε χρήστη, που σημαίνει ότι είναι μοναδικό. Η διεύθυνση ηλεκτρονικού ταχυδρομείου, επίσης είναι μοναδική για κάθε χρήστη. Επιπλέον, ένας χρήστης μπορεί να έχει πάνω από έναν ρόλο. Προς το παρόν οι δυο ρόλοι που υποστηρίζει η εφαρμογή μας είναι: ADMIN και USER, δηλαδή διαχειριστής και απλός χρήστης.

Η οντότητα προϊόν, όπως βλέπουμε στην παρακάτω εικόνα, περιλαμβάνει τις εξής ιδιότητες: μοντέλο διάταξης, μοντέλο παράδοσης, πάροχος υπηρεσίας, μηχανισμοί ασφάλειας, μοντέλο κόστους, κατηγορία προϊόντος, μη λειτουργικές εγγυήσεις, είδη προσφερόμενης προστασίας, ιδιότητες ασφάλειας, αντικείμενα που προστατεύονται, απειλές που αντιμετωπίζονται, περιορισμοί, πληροφορίες για το αν το προϊόν διατίθεται δωρεάν και για πόσο χρονικό διάστημα, τρόπος χρήσης προϊόντος, σημεία αγοράς, όνομα προϊόντος, ένδειξη αν είναι δημοσιευμένο, αναγνωριστικό, περιγραφή και υποστήριξη. Ένα προϊόν μπορεί να έχει από 0 έως πολλά μοντέλα κόστους, τύπους υποστήριξης, μη λειτουργικές εγγυήσεις και περιορισμούς.

Οι δυο οντότητες που αναφέρθηκαν παραπάνω συνδέονται με τη σχέση ένα προς πολλά, που σημαίνει ότι ένας χρήστης μπορεί να δημιουργήσει πολλά προϊόντα.



Εικόνα 31. Διάγραμμα κλάσεων για τις βασικές & δευτερεύοντες οντότητες της εφαρμογής

4.4 Υλοποίηση

4.4.1 Λεπτομέρειες Υλοποίησης

Για την υλοποίηση της εφαρμογής χρησιμοποιήθηκε η γλώσσα προγραμματισμού Clojure στην έκδοση 1.10.0 για το Backend και η γλώσσα προγραμματισμού ClojureScript στην έκδοση 1.10.914 για το Frontend. Η Clojure είναι συναρτησιακή γλώσσα που ανήκει στην οικογένεια της Lisp.

Το API της εφαρμογής υλοποιήθηκε με χρήση του πλαισίου Reitit (https://github.com/metosin/reitit), το οποίο ουσιαστικά δρομολογεί τα αιτήματα στο κατάλληλο endpoint/URI. Στο Frontend χρησιμοποιήθηκαν τα πλαίσια Reagent (https://reagent-project.github.io/) και re-frame (https://github.com/day8/re-frame). Το πλαίσιο Reagent αποτελεί μια πολύ ελαφριά διεπαφή μεταξύ ClojureScript και React. Το πλαίσιο re-frame είναι κατάλληλο για τη δημιουργία single-page εφαρμογών.

Επίσης, χρησιμοποιήθηκε το Migratus (https://github.com/yogthos/migratus), το οποίο είναι ένα πλαίσιο κατάλληλο για τη δημιουργία των πινάκων της βάσης δεδομένων και τη διαχείριση των αλλαγών στο σχήμα της. Κάθε αλλαγή στο σχήμα αποθηκεύεται σε ξεχωριστό αρχείο, το οποίο περιλαμβάνει στο όνομά του τη χρονοσφραγίδα της στιγμής που δημιουργήθηκε, η οποία αποτελείται από 14 ψηφία με ακρίβεια δευτερολέπτου. Με αυτόν τον τρόπο, το πλαίσιο αυτό καταφέρνει να μειώσει σημαντικά την πιθανότητα να έρθουν σε σύγκρουση δυο ή περισσότερες αλλαγές στο σχήμα της βάσης δεδομένων. Η χρονοσφραγίδα που αναφέρθηκε πιο πριν, είναι της

μορφής '20241115091201', δηλαδή καλύπτει την ημερομηνία και ώρα που δημιουργήθηκε η κάθε αλλαγή.

Η Clojure, ως συναρτησιακή γλώσσα, δεν περιέχει κλάσεις αλλά namespaces (χώρους ονομάτων) στους οποίους γίνεται η υλοποίηση των απαιτούμενων συναρτήσεων. Για το UI της εφαρμογής μας, όπως ειπώθηκε πιο πριν, χρησιμοποιήθηκαν οι βιβλιοθήκες Reagent και re-frame και αποτελεί single-page εφαρμογή. Κάθε διαφορετική φόρμα αποτελείται από δυο namespaces, το view και το model. Το view είναι υπεύθυνο για την εμφάνιση της διεπαφής χρήστη, όπως τα κουμπιά, το μενού και τα πεδία εισόδου. Το model είναι υπεύθυνο για την εκτέλεση όλων των Ajax αιτημάτων προς το BackEnd της εφαρμογής, τα οποία πυροδοτούνται είτε κατά την φόρτωση της φόρμας, είτε μετά από κάποια είσοδο του χρήστη, είτε μετά από αίτημα του χρήστη, όπως π.χ. με το πάτημα ενός κουμπιού. Επιπλέον, το model είναι υπεύθυνο για τη διατήρηση όλων των δεδομένων που έχει φορτωμένα η κάθε φόρμα.

Το BackEnd της εφαρμογής, όπως επίσης ειπώθηκε πιο πριν, είναι ένα API που εξυπηρετεί όλες τις λειτουργίες που προσφέρει η εφαρμογή μας και είναι χωρισμένο σε δυο μέρη, τα οποία αντικατοπτρίζουν τις δυο οντότητες που περιέχει η εφαρμογή μας, τους χρήστες και τα προϊόντα SecaaS. Στο ένα μέρος υπάρχουν όλα τα namespaces που αφορούν τους χρήστες και τις λειτουργίες διαχείρισής τους και στο άλλο τα namespaces που αφορούν τα προϊόντα SecaaS και τις λειτουργίες διαχείρισής τους. Το κάθε μέρος με τη σειρά του χωρίζεται σε τρία υπό-μέρη. Το πρώτο περιλαμβάνει τα namespaces που περιέχουν όλα τα URIs διαχείρισης (προϊόντων ή χρηστών) που εκθέτει το API μας. Το δεύτερο αποτελείται από τα namespaces που χειρίζονται τα αιτήματα προς τα URIs διαχείρισης και υλοποιούν όλη τη λειτουργικότητα που περιγράφεται σε αυτό το κεφάλαιο. Τέλος, το τρίτο αποτελείται από τα namespaces που είναι υπεύθυνα για τη διασύνδεση με τη βάση, εκτελώντας τις λειτουργίες της αναζήτησης, της εισαγωγής, της διαγραφής και της ενημέρωσης εγγραφών (προϊόντων ή χρηστών) σε αυτήν.

4.4.2 Υλοποίηση Ταιριάσματος Προϊόντων SecaaS

Για το ταίριασμα των προϊόντων SecaaS η εφαρμογή αρχικά παίρνει τα χαρακτηριστικά και τις τιμές αυτών, τις οποίες ο χρήστης θέλει να ταιριάξει. Ο χρήστης μπορεί να έχει δώσει παραπάνω πληροφορίες για το κάθε χαρακτηριστικό, οι οποίες αφορούν τον τελεστή σύγκρισης με τον οποίον επιθυμεί να γίνει το ταίριασμα. Για το ταίριασμα ο προεπιλεγμένος τελεστής σύγκρισης είναι η ισότητα, ο χρήστης όμως μπορεί να επιλέξει την ανισότητα. Αν η παρεχόμενη τιμή είναι αριθμός, μπορεί να επιλέξει επιπλέον από τους τελεστές: μεγαλύτερο, μεγαλύτερο ή ίσο, μικρότερο και μικρότερο ή ίσο. Αν η τιμή είναι μια λίστα, τότε οι επιπλέον της ισότητας και της ανισότητας επιλογές τελεστών είναι: «υποσύνολο», «υπερσύνολο», «περιέχει οποιαδήποτε από τις τιμές» και «δεν περιέχει καμία από τις τιμές». Τέλος, ο χρήστης μπορεί να δώσει τον λογικό τελεστή με τον οποίο θα συνδυαστούν όλοι οι παρεχόμενοι περιορισμοί των χαρακτηριστικών. Ο προεπιλεγμένος είναι ο AND (σύζευξη), μπορεί όμως να επιλέξει τον OR (διάζευξη) ή τον XOR (αποκλειστική διάζευξη). Με βάση τα παραπάνω, το BackEnd θα συνθέσει το σχετικό ερώτημα που θα σταλεί στη βάση δεδομένων για να πραγματοποιηθεί το ταίριασμα των προϊόντων SecaaS. Παρακάτω δίνουμε ένα παράδειγμα SQL ερωτήματος που μπορεί να δημιουργηθεί στο πλαίσιο 2 περιορισμών που παρέχει ο χρήστης για 2 χαρακτηριστικά, οι οποίες συνδυάζονται με τον τελεστή σύζευξης (AND).

```
select p.* from products p
where published = true
   AND ANY y IN $marketplaces SATISFIES ARRAY_CONTAINS(`marketplaces`,y) END
   AND EVERY j IN $deliveryMethods SATISFIES j IN `delivery-methods` END,
   ...
params={"deliveryMethods":["CAAS"],
          "marketplaces":["AWS","SEARCH_ENGINE"
          ...]}
```

Όπως βλέπουμε στο ερώτημα, επιλέγουμε από τον κουβά (η Couchbase χρησιμοποιεί αυτόν τον όρο για έναν πίνακα) 'products' όλα τα πεδία με το '*' και με τον προεπιλεγμένο περιορισμό τα προϊόντα να είναι δημοσιευμένα. Στη συνέχεια βάζουμε τους περιορισμούς που έχει δώσει ο χρήστης και πχ. αφορούν τα πεδία σημεία αγοράς (marketPlaces) και τρόποι παράδοσης (deliveryMethods). Για τον πρώτο περιορισμό το προϊόν θα πρέπει να περιέχει οποιαδήποτε από τις τιμές "AWS" και "SEARCH_ENGINE" ως προς το χαρακτηριστικό των σημείων αγοράς, ενώ για τον δεύτερο θα πρέπει να έχει μόνο την τιμή "CAAS" ως προς το χαρακτηριστικό του τρόπου παράδοσης.

Παρακάτω εξηγούμε τον τρόπο που γίνεται το ταίριασμα χαρακτηριστικών μεταξύ των αποθηκευμένων περιγραφών προϊόντων SecaaS και των περιορισμών του χρήστη ανάλογα με το πεδίο τιμών τους.

Όταν το χαρακτηριστικό που θέλουμε να συγκρίνουμε έχει αριθμητικό πεδίο τιμών και έχει θετική κατεύθυνση τιμών, τότε έχουμε σχετικό ταίριασμα ενός προϊόντος και των απαιτήσεων του χρήστη αν το προϊόν υπόσχεται μια τιμή ν1 για το χαρακτηριστικό αυτό, ο χρήστης παρέχει έναν περιορισμό >= ν2 (μια άλλη τιμή) και ισχύει πως ν1 >= ν2. Από την άλλη πλευρά, αν το χαρακτηριστικό έχει αρνητική κατεύθυνση τιμών, τότε έχουμε ταίριασμα όταν το προϊόν υπόσχεται μια τιμή ν1, ο χρήστης παρέχει έναν περιορισμό <= ν2 και ισχύει πως ν1 <= ν2.

Στην περίπτωση που το χαρακτηριστικό είναι αλφαριθμητικό, θέλουμε απόλυτο ταίριασμα με βάση ισότητες ή ανισότητες που δίνει ο χρήστης. Αν το προϊόν έχει την τιμή ν1 και ο χρήστης παρέχει την ίδια τιμή ν1 για το χαρακτηριστικό αυτό με τελεστή ισότητας τότε έχουμε ταίριασμα. Όταν το προϊόν έχει την τιμή ν1 και ο χρήστης παρέχει μια άλλη τιμή ν2 με τελεστή ανισότητας, τότε πάλι έχουμε ταίριασμα.

Όταν το χαρακτηριστικό που θέλουμε να συγκρίνουμε έχει ως πεδίο τιμών ένα σύνολο τιμών, τότε ο έλεγχος για το ταίριασμα γίνεται βάσει των στοιχείων του συνόλου. Έστω ν1 το σύνολο τιμών που έχει το προϊόν για το συγκεκριμένο χαρακτηριστικό και ν2 το σύνολο τιμών που παρέχει ο χρήστης. Για να έχουμε ταίριασμα έχουμε τις εξής περιπτώσεις:

- Αν ο χρήστης παρέχει τον τελεστή της ισότητας, τότε θα πρέπει ν1 = ν2 ,
- Αν ο χρήστης παρέχει τον τελεστή «υποσύνολο», τότε θα πρέπει το ν2 να αποτελεί υποσύνολο του ν1,

- Αν ο χρήστης παρέχει τον τελεστή «υπερσύνολο», τότε θα πρέπει το ν2 να αποτελεί υπερσύνολο του ν1,
- Αν ο χρήστης παρέχει τον τελεστή «περιέχει οποιαδήποτε από τις τιμές», τότε θα πρέπει τουλάχιστον μια τιμή του ν2 να υπάρχει στο ν1,
- Αν ο χρήστης παρέχει τον τελεστή «δεν περιέχει καμία από τις τιμές», τότε δεν θα πρέπει οποιαδήποτε τιμή του ν2 να περιέχεται στο ν1.

Επίσης, όσον αφορά τους λογικούς τελεστές AND/OR/XOR για τον συνδυασμό των περιορισμών που μπορεί να δώσει ο χρήστης σε καθολικό επίπεδο και πάλι έχουμε ξεχωριστές περιπτώσεις. Αν ο χρήστης παρέχει το λογικό AND, τότε θα πρέπει όλοι οι περιορισμοί που παρείχε ο χρήστης να ικανοποιούνται. Αν παρέχει το λογικό OR, τότε θα πρέπει να ικανοποιείται τουλάχιστον ένας από τους περιορισμούς που παρείχε. Τέλος, αν παρέχει το λογικό XOR, θα πρέπει να ικανοποιείται αποκλειστικά μόνο ένας από τους περιορισμούς που παρείχε.

Είναι σημαντικό σε αυτό το σημείο να τονίσουμε ότι η εφαρμογή μας υποστηρίζει σημασιολογική αναζήτηση για τα χαρακτηριστικά των μηχανισμών ασφαλείας που υλοποιούνται και των απειλών που αντιμετωπίζονται από το εκάστοτε προϊόν SecaaS. Κάθε απειλή/μηχανισμός ασφαλείας αποτελεί υπέρ-κλάση ή υπό-κλάση μιας άλλης απειλής/μηχανισμού ασφαλείας. Κατά τη δημιουργία ενός προϊόντος SecaaS, όταν ο χρήστης επιλέξει τιμές για αυτά τα χαρακτηριστικά και τις στείλει στο σύστημα για αποθήκευση του προϊόντος, το σύστημα γνωρίζει ποιες από αυτές αποτελούν υπέρ-κλάσεις για άλλες τιμές που μπορεί να έχει αυτό το χαρακτηριστικό και αποθηκεύει μαζί και όλες τις υπό-κλάσεις της παρεχόμενης υπερ-κλάσης σε οποιοδήποτε βάθος της ιεραρχίας στις περιπτώσεις που αυτές όντως υπάρχουν.

Επίσης, ισχύει και η ανάποδη διαδρομή. Με άλλα λόγια, εφόσον η παρεχόμενη κλάση για τον μηχανισμό ασφάλειας ή την απειλή για ένα προϊόν SecaaS έχει προγονικές υπερ-κλάσεις, κι αυτές αποθηκεύονται μαζί με την κλάση για το προϊόν αυτό. Αυτό έχει ως τελικό αποτέλεσμα για την παρεχόμενη κλάση να αποθηκεύεται όλο το κλαδί με τις προγονικές κλάσεις καθώς και το υπο-δένδρο της με τις απογονικές της κλάσεις. Προφανώς, η αποθήκευση πραγματοποιείται εφόσον υπάρχει το προγονικό κλαδί ή το απογονικό υπο-δένδρο.

Η λογική για την αποθήκευση του προγονικού κλαδιού είναι πως με αυτό τον τρόπο εξασφαλίζεται πως όταν ο χρήστης παρέχει μια προγονική κλάση, τότε το προϊόν SecaaS, αν και αποτελεί ένα εν μέρει αποτέλεσμα του αιτήματος ταιριάσματος του χρήστη, θα πρέπει να επιστρέφεται. Ενώ για την αποθήκευση του απογονικού υπο-δένδρου είναι πως όταν ο χρήστης παρέχει μια απογονική κλάση, τότε το προϊόν SecaaS σίγουρα ικανοποιεί το αίτημα ταιριάσματός του διότι καλύπτει όχι μόνο αυτή αλλά όλο το απογονικό υπο-δένδρο.

Για την καλύτερη κατανόηση της λειτουργίας σημασιολογικής αναζήτησης θα δώσουμε το παρακάτω παράδειγμα. Έστω ότι ένας χρήστης δημιουργεί το προϊόν Α δίνοντας ως απειλή που αντιμετωπίζει την ‘Κακόβουλη δραστηριότητα / κατάχρηση (Nefarious Activity)’. Έπειτα δημιουργεί ένα δεύτερο προϊόν το Β, το οποίο αντιμετωπίζει την απειλή ‘Υποκλοπές (Eavesdropping)’. Όταν ο χρήστης ζητήσει τα προϊόντα που αντιμετωπίζουν την απειλή ‘Man-In-The-Middle’ θα του επιστραφούν τα προϊόντα Α και Β διότι βρίσκονται στο σχετικό κλαδί/υπό-δένδρο (Nefarious Activity - MiTM - Eavesdropping), όπως φαίνεται στην Εικόνα 24. Ειδικότερα, το προϊόν Α σίγουρα ταιριάζει με το αίτημα ταιριάσματος του χρήστη εφόσον καλύπτει όλες τις

κακόβουλες δραστηριότητες ενώ το προϊόν Β αποτελεί ένα εν μέρει αποτέλεσμα διότι καλύπτει μόνο μια από τις υπο-απειλές MiTM.

4.4.3 Υλοποίηση Ταξινόμησης Προϊόντων SecaaS

Για την ταξινόμηση των προϊόντων SecaaS, η εφαρμογή παίρνει τα βάρη και τα χαρακτηριστικά που αυτά αφορούν (όπως αυτά παρέχονται από τον χρήστη). Στη συνέχεια, βρίσκει τη μέγιστη και την ελάχιστη τιμή αυτών των χαρακτηριστικών μεταξύ των προϊόντων που θα ταξινομηθούν. Το σκορ της ταξινόμησης υπολογίζεται από τους 2 τύπους που υπάρχουν στην υπό-ενότητα 4.2.1.2 στην παράγραφο *Ταξινόμηση*. Η επιλογή του τύπου γίνεται με βάση την κατεύθυνση τιμών του συγκεκριμένου χαρακτηριστικού, η οποία υπάρχει ως πληροφορία στη βάση δεδομένων. Για τον υπολογισμό του εκάστοτε επιμέρους σκορ (δηλ. του σκορ για ένα χαρακτηριστικό) πολλαπλασιάζουμε το αποτέλεσμα που θα μας βγάλει ο μαθηματικός τύπος που αναφέρθηκε προηγουμένως με το βάρος που μας έδωσε ο χρήστης (για το αντίστοιχο χαρακτηριστικό). Αυτό γίνεται για κάθε παρεχόμενο χαρακτηριστικό και έπειτα γίνεται πρόσθεση των επιμέρους σκορ ώστε να παραχθεί το συνολικό για το προϊόν. Μόλις υπολογιστεί το σκορ του κάθε προϊόντος, γίνεται ταξινόμηση των προϊόντων με βάση το σκορ σε φθίνουσα σειρά χρησιμοποιώντας τον αλγόριθμο Timsort [12] (δηλ. έναν πολύ αποδοτικό αλγόριθμο που συνδυάζει τους πλέον γνωστούς Merge & Insertion Sort).

4.5 Ικανοποίηση Απαιτήσεων

Στον παρακάτω πίνακα φαίνονται οι απαιτήσεις του συστήματος, όπως αυτές αναλύθηκαν στην ενότητα 4.2, μαζί με τον βαθμό ικανοποίησης για κάθε μια από αυτές. Στις περιπτώσεις που ο βαθμός ικανοποίησης δεν είναι άριστος, στην τρίτη στήλη υπάρχει η σχετική αιτιολόγηση.

ΑΠΑΙΤΗΣΗ	**ΒΑΘΜΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ**	**ΑΙΤΙΟΛΟΓΗΣΗ**
Εγγραφή χρήστη	Άριστο	
Ενεργοποίηση λογαριασμού	Καλό	Ο λογαριασμός ενεργοποιείται κανονικά μέσω email, παρόλα αυτά το αίτημα για ενεργοποίηση αποστέλλεται 2 φορές όταν ο χρήστης επιλέξει τον σύνδεσμο ενεργοποίησης στο email του.
Τροποποίηση στοιχείων χρήστη	Άριστο	
Διαγραφή χρήστη	Άριστο	
Αλλαγή κωδικού	Άριστο	
Επαναφορά κωδικού	Άριστο	
Ταυτοποίηση χρήστη	Άριστο	

Δημιουργία SecaaS προϊόντος	Καλό	Υπάρχει ένα bug στο UI όταν ο χρήστης πατήσει πρώτη φορά να προσθέσει περιορισμούς, μη λειτουργικές εγγυήσεις, μοντέλα κόστους και λεπτομέρειες υποστήριξης και δεν μπορεί να γράψει στα αντίστοιχα πεδία που ανοίγουν. Αν ο χρήστης αφαιρέσει το προστιθέμενο στοιχείο και το προσθέσει ξανά, αυτό λειτουργεί κανονικά.
Δημοσίευση SecaaS προϊόντος	Άριστο	
Αποδημοσίευση SecaaS προϊόντος	Άριστο	
Ταίριασμα SecaaS προϊόντων	Άριστο	
Ταξινόμηση SecaaS προϊόντων	Άριστο	
Ανακάλυψη SecaaS προϊόντων	Άριστο	
< 5 δευτερόλεπτα κάθε αίτημα	Άριστο	
> 50 ταυτόχρονοι χρήστες	Άριστο	
Χρηστική διεπαφή χρήστη	Άριστο	
Ενιαίο look-n-feel διεπαφής	Άριστο	
Navigability and user orientation	Άριστο	
Διαχωρισμένο API / front end	Άριστο	
REST με επίπεδο ωριμότητας 3	Άριστο	
Χρήση Ajax και δυναμικής HTML	Άριστο	
Χειρισμός λαθών/εξαιρέσεων	Άριστο	
Επικύρωση δεδομένων	Άριστο	
Καλό επίπεδο ασφάλειας	Άριστο	

Πίνακας 1. Ικανοποίηση Απαιτήσεων

5

Εγκατάσταση και Επίδειξη Εφαρμογής

Σε αυτό το κεφάλαιο θα δοθούν τα προαπαιτούμενα καθώς και οδηγίες εγκατάστασης και εκτέλεσης της εφαρμογής. Τέλος, θα γίνει μια επίδειξη της εφαρμογής μέσω σεναρίων χρήσης, τα οποία θα συνοδεύονται από τα αντίστοιχα στιγμιότυπα οθόνης.

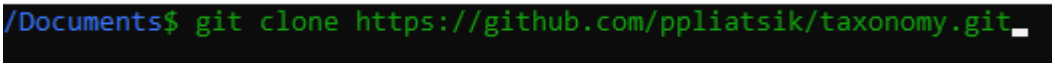
5.1 Εγκατάσταση και Εκτέλεση Εφαρμογής

Η ανάπτυξη της εφαρμογής μας έγινε σε περιβάλλον Microsoft Windows 10. Για την εκτέλεση των βημάτων που περιγράφονται στη συνέχεια εγκαταστάθηκε στο σύστημα η εφαρμογή των Windows, WSL (Windows Subsystem for Linux – Υπό-σύστημα των Windows για το Linux) και όλες οι εντολές εκτελέστηκαν στο περιβάλλον Linux που προσφέρει η εφαρμογή αυτή. Όπως γίνεται κατανοητό, όλες οι εντολές που εκτελούνται παρακάτω μπορούν να εκτελεστούν άμεσα και σε λειτουργικό σύστημα Linux. Άρα, η εφαρμογή μας μπορεί να εγκατασταθεί και να εκτελεστεί και σε Microsoft Windows και σε Linux λειτουργικά συστήματα.

Η εφαρμογή μας, όπως ειπώθηκε στην Ενότητα 4.4, υλοποιήθηκε με τη χρήση της γλώσσας προγραμματισμού Clojure. Η Clojure είναι μια γλώσσα που εκτελείται στη JVM και αυτό σημαίνει ότι αρχικά θα πρέπει να υπάρχει εγκατεστημένη η Java (ουσιαστικά το runtime περιβάλλον της). Μπορεί να χρησιμοποιηθεί οποιαδήποτε έκδοση της Java, με προτεινόμενη την τελευταία. Έπειτα, θα πρέπει να εγκατασταθεί η Clojure. Αναλυτικές πληροφορίες για το πώς μπορούν να γίνουν τα παραπάνω υπάρχουν στην επίσημη σελίδα της Clojure στο διαδίκτυο εδώ: https://clojure.org/guides/install_clojure. Ένα ακόμα προαπαιτούμενο είναι η ύπαρξη της μηχανής ενορχήστρωσης δοχείων Docker, καθώς αυτή είναι υπεύθυνη για την εκτέλεση των τριών εικόνων (δοχείων) που χρησιμοποιεί η εφαρμογή, οι οποίες είναι: Nginx, PostGis και Couchbase. Ο Nginx είναι διακομιστής ιστού, ενώ οι άλλες δυο εικόνες αντιστοιχούν σε δύο βάσεις δεδομένων, αντίστοιχα. Η PostGis είναι σχεσιακή βάση και χρησιμοποιείται για τη διαχείριση των χρηστών ενώ η Couchbase είναι μη σχεσιακή βάση και χρησιμοποιείται για τη διαχείριση των προϊόντων SecaaS. Πληροφορίες για την εγκατάσταση της μηχανής Docker μπορούν να βρεθούν εδώ: https://www.docker.com/.

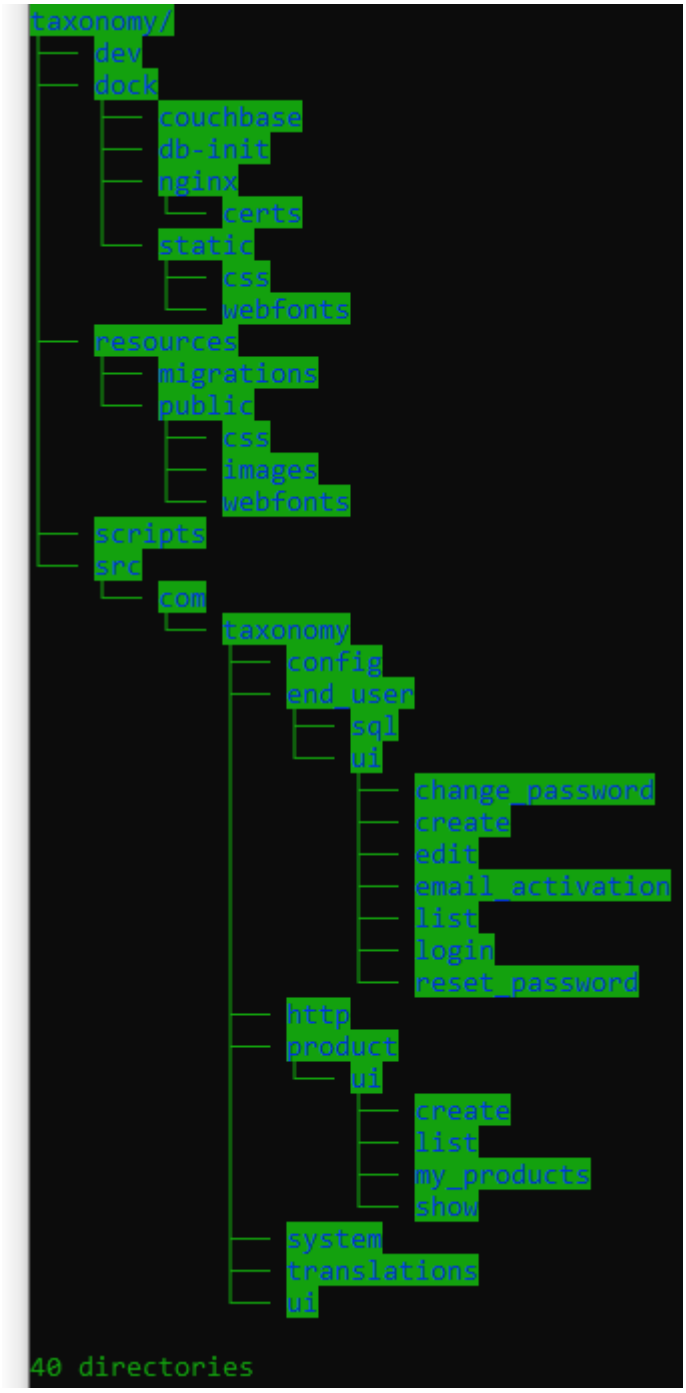
Στη συνέχεια θα πρέπει να γίνει η κλωνοποίηση του πηγαίου κώδικα της εφαρμογής από το GitHub. Η εφαρμογή είναι διαθέσιμη εδώ: https://github.com/ppliatsik/taxonomy. Η κλωνοποίηση

του πηγαίου κώδικα της εφαρμογής μπορεί να γίνει εκτελώντας την εντολή της Εικόνας 32. Προαπαιτούμενο είναι η εγκατάσταση του git στο σύστημα του χρήστη. Για την εγκατάσταση του git, πληροφορίες υπάρχουν εδώ: https://git-scm.com/book/en/v2/Getting-Started-Installing-Git.



Εικόνα 32. Κλωνοποίηση εφαρμογής από GitHub

Μόλις εκτελεστεί η εντολή της παραπάνω εικόνας θα εκφορτωθεί ο πηγαίος κώδικας της εφαρμογής στο σύστημα του χρήστη. Στην Εικόνα 33 φαίνεται η διάταξη σε μορφή δέντρου των φακέλων της εφαρμογής. Το όνομα του ριζικού φακέλου είναι *taxonomy*.



Εικόνα 33. Οργάνωση φακέλων της εφαρμογής

Το επόμενο βήμα είναι η δημιουργία του πιστοποιητικού και του ιδιωτικού κλειδιού, ώστε να μπορεί ο εξυπηρετητής Nginx να υποστηρίζει ασφαλείς συνδέσεις (https). Για να γίνει αυτό θα πρέπει να εκτελεστεί η εντολή που υπάρχει στο αρχείο *create-nginx-certs.sh* που βρίσκεται στον φάκελο *scripts* και φαίνεται στην παρακάτω εικόνα.

```
/scripts$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout certs/nginx-selfsigned.key -out certs/nginx-selfsigned.crt
```

Εικόνα 34. Δημιουργία πιστοποιητικού & ιδιωτικού κλειδιού Nginx

Η εφαρμογή μας, έχει τη δυνατότητα να στέλνει μηνύματα ηλεκτρονικού ταχυδρομείου στους χρήστες της. Για τις ανάγκες της υλοποίησης χρησιμοποιήθηκε η προσωπική email διεύθυνση του γράφοντος και ο αντίστοιχος κωδικός εφαρμογής από το Gmail. Για να μπορέσει να εκτελέσει κάποιος την εφαρμογή και να υποστηρίζει μηνύματα ηλεκτρονικού ταχυδρομείου, θα πρέπει να χρησιμοποιήσει έναν λογαριασμό Gmail και να δημιουργήσει έναν κωδικό εφαρμογής. Οι δυο αυτές τιμές θα πρέπει να μπουν στο αρχείο */resources/config.end* στο κλειδί *:email/host*. Εκεί η email διεύθυνση θα πρέπει να μπει στο πεδίο *user* και ο κωδικός εφαρμογής στο πεδίο *pass*. Πληροφορίες για το πώς μπορεί να παραχθεί αυτός ο κωδικός παρέχονται εδώ: https://support.google.com/mail/thread/205453566/how-to-generate-an-app-password?hl=en.

Μόλις πραγματοποιηθούν με επιτυχία τα παραπάνω μπορούμε να εκτελέσουμε την εφαρμογή μας. Αρχικά, θα πρέπει να ενορχηστρώσουμε την εκτέλεση των 3 προαναφερόμενων εικόνων δοχείων, υποθέτοντας πως η μηχανή Docker εκτελείται ήδη στο σύστημα. Συνεπώς, θα πρέπει να πάμε στον φάκελο όπου βρίσκεται η εφαρμογή μας και από εκεί να κατευθυνθούμε στον υπό-φάκελο *dock*. Σε αυτόν τον (υπό-)φάκελο θα εκτελέσουμε την εντολή της παρακάτω εικόνας για να αρχίσει η ενορχήστρωση.

```
/taxonomy/dock$ docker-compose up -d
```

Εικόνα 35. Εκτέλεση Docker

Όταν ολοκληρωθεί η εκτέλεση της προηγούμενης εντολής, θα πρέπει να πλοηγηθούμε στον φάκελο *taxonomy,* που είναι και ο ριζικός φάκελος, όπως είπαμε προηγουμένως – άρα πηγαίνουμε ένα φάκελο πάνω από τον τρέχοντα και από εκεί θα πρέπει να εκτελέσουμε όλες τις παρακάτω εντολές. Με τη βάση PostGis της εφαρμογής να τρέχει, μπορούμε να εκτελέσουμε την εντολή για τη δημιουργία των πινάκων σε αυτήν με την εντολή που φαίνεται στην παρακάτω εικόνα.

```
/taxonomy$ clj -A:dev:migrate init
```

Εικόνα 36. Αρχικοποίηση PostGis

Στη συνέχεια θα τρέξουμε το BackEnd της εφαρμογής εκτελώντας με τη σειρά τις εντολές των Εικόνων 37, 38 και 39. Μόλις εκτελεστεί η εντολή της Εικόνας 37 θα ανοίξει το REPL (Read Eval Print Loop) της Clojure και σε αυτό θα εκτελέσουμε τις εντολές που φαίνονται στις Εικόνες 38 και 39. Το REPL είναι ένα περιβάλλον προγραμματισμού, το οποίο μας επιτρέπει να

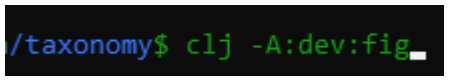
αλληλοεπιδράσουμε με ένα τρέχον πρόγραμμα Clojure και να το διαμορφώνουμε δυναμικά κατά την εκτέλεση του, εφαρμόζοντας μία έκφραση κώδικα κάθε φορά.

Εικόνα 37. BackEnd command (μέρος Α)

Εικόνα 38. BackEnd command (μέρος Β)

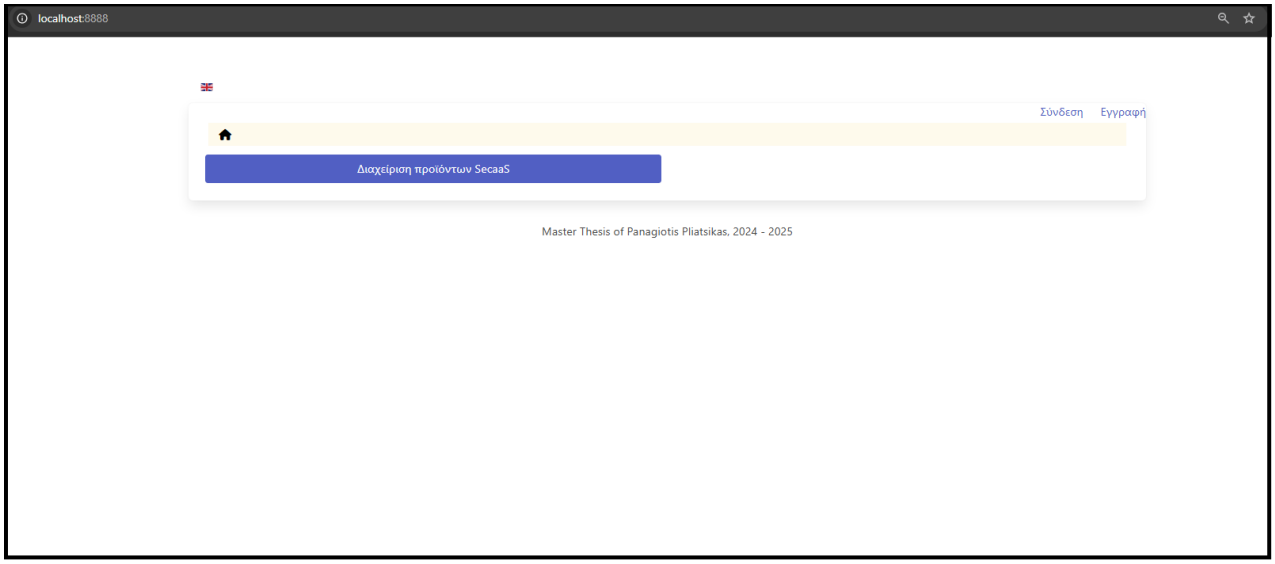
Εικόνα 39. BackEnd command (μέρος Γ)

Τέλος, εφόσον ολοκληρωθούν τα παραπάνω θα πρέπει να τρέξουμε το UI της εφαρμογής. Για τον σκοπό αυτόν θα πρέπει να ανοίξουμε καινούρια γραμμή εντολών και να πλοηγηθούμε στο ίδιο μονοπάτι με πριν στον φάκελο *taxonomy*. Εκεί, θα πρέπει να εκτελέσουμε την εντολή της παρακάτω εικόνας.



Εικόνα 40. UI command

Όταν και η παραπάνω εντολή εκτελεστεί με επιτυχία, θα ανοίξει στον φυλλομετρητή (browser) η αρχική σελίδα της εφαρμογής, όπως φαίνεται στην παρακάτω εικόνα. Υπάρχει περίπτωση να μην εκτελεστεί η παραπάνω εντολή με την πρώτη φορά. Σε αυτήν την περίπτωση θα πρέπει να κλείσει η γραμμή εντολών, να ανοίξει εκ νέου με πλοήγηση στον ίδιο φάκελο και να εκτελεστεί ξανά η εντολή της Εικόνας 40. Με αυτό τον τρόπο, εξασφαλίζουμε πως το front-end της εφαρμογής μας εν τέλει θα εκτελεστεί επιτυχώς.



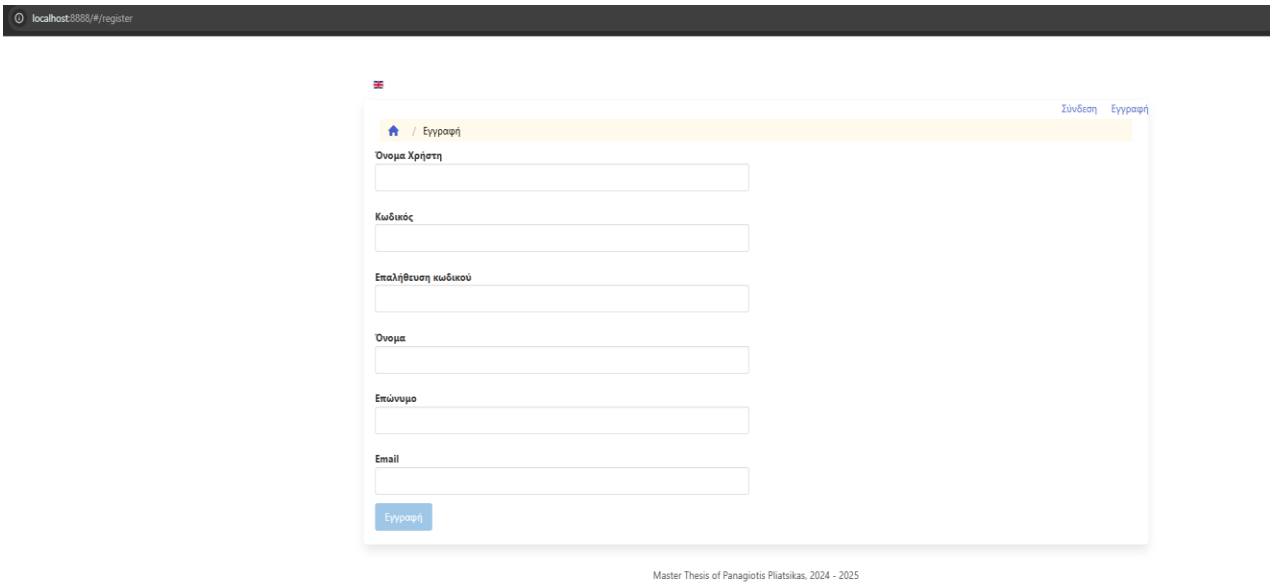
Εικόνα 41. Αρχική σελίδα εφαρμογής

5.2 Επίδειξη Εφαρμογής

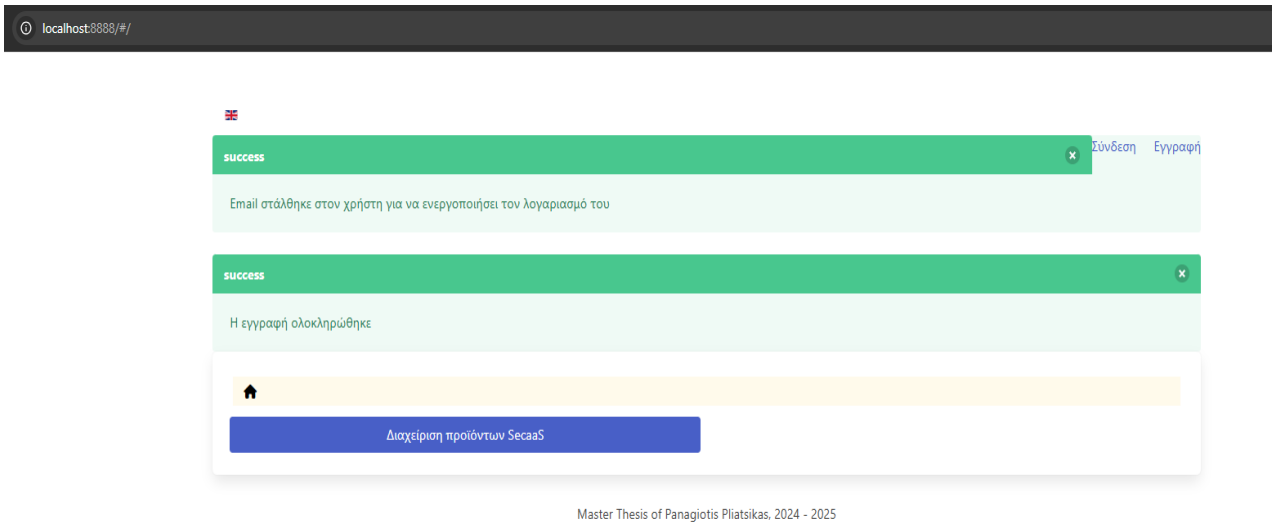
Σε αυτό την ενότητα θα παρουσιάσουμε 7 σενάρια χρήσης της εφαρμογής μας. Το πρώτο είναι η δημιουργία χρήστη, το δεύτερο η διαδικασία ενεργοποίησης του λογαριασμού του μέσω email, το τρίτο η επιτυχής σύνδεση στην εφαρμογή, το τέταρτο η δημιουργία προϊόντος, το πέμπτο η αναζήτηση προϊόντων με βάση κάποια κριτήρια, το έκτο η ταξινόμηση αυτών των προϊόντων πάλι βάσει δοθέντων κριτηρίων και το έβδομο η διαγραφή χρήστη από τον διαχειριστή.

5.2.1 Σενάριο Δημιουργίας Χρήστη

Το πρώτο σενάριο που θα παρουσιάσουμε είναι αυτό της εγγραφής ενός χρήστη. Στην Εικόνα 41 βλέπουμε στην αρχική σελίδα της εφαρμογής ότι ένας επισκέπτης της μπορεί να εγγραφεί σε αυτήν. Ειδικότερα, πατώντας τον σύνδεσμο Εγγραφή στο πάνω δεξιά μενού, ο επισκέπτης θα οδηγηθεί στη σελίδα της Εικόνας 42. Εκεί, θα πρέπει να συμπληρώσει όλα τα στοιχεία που του ζητούνται, σύμφωνα με τις προδιαγραφές που περιγράφονται για το καθένα στην Ενότητα 4.2.1.1. Μόλις τα συμπληρώσει σωστά και πατήσει το κουμπί ‘Εγγραφή’, θα δημιουργηθεί ένας καινούριος λογαριασμός για αυτόν, ο οποίος όμως θα είναι ανενεργός. Στην Εικόνα 43 φαίνεται η αρχική σελίδα της εφαρμογής μας στην οποία οδηγείται ο χρήστης μετά την επιτυχημένη δημιουργία του λογαριασμού του στην εφαρμογή αυτή.



Εικόνα 42. Σελίδα εγγραφής χρήστη

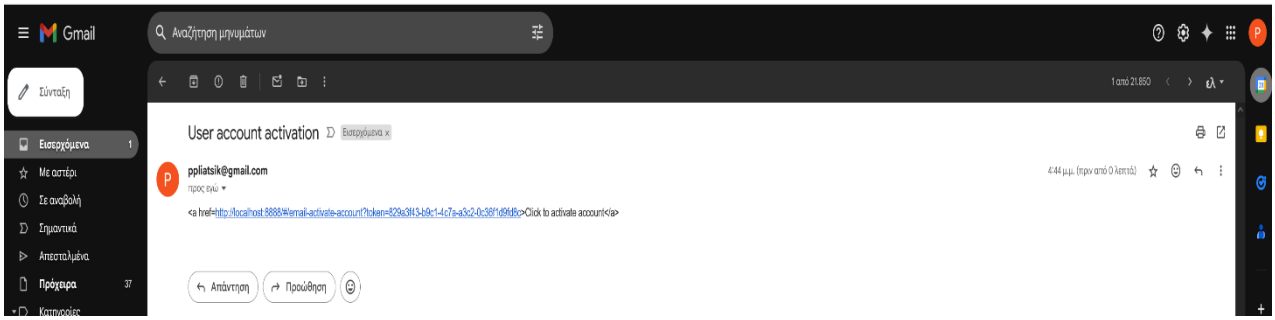


Εικόνα 43. Σελίδα επιτυχούς δημιουργίας χρήστη

5.2.2 Σενάριο Ενεργοποίησης Λογαριασμού Μέσω Email

Σε αυτή την ενότητα θα παρουσιάσουμε το δεύτερο σενάριο που αφορά την ενεργοποίηση του λογαριασμού ενός χρήστη, μετά τη δημιουργία του. Έχουμε ήδη πει ότι ο λογαριασμός του χρήστη όταν δημιουργείται είναι ανενεργός. Όπως βλέπουμε στην Εικόνα 43, η εφαρμογή έστειλε ένα μήνυμα ηλεκτρονικού ταχυδρομείου στον χρήστη για το λογαριασμό του που μόλις δημιουργήθηκε.

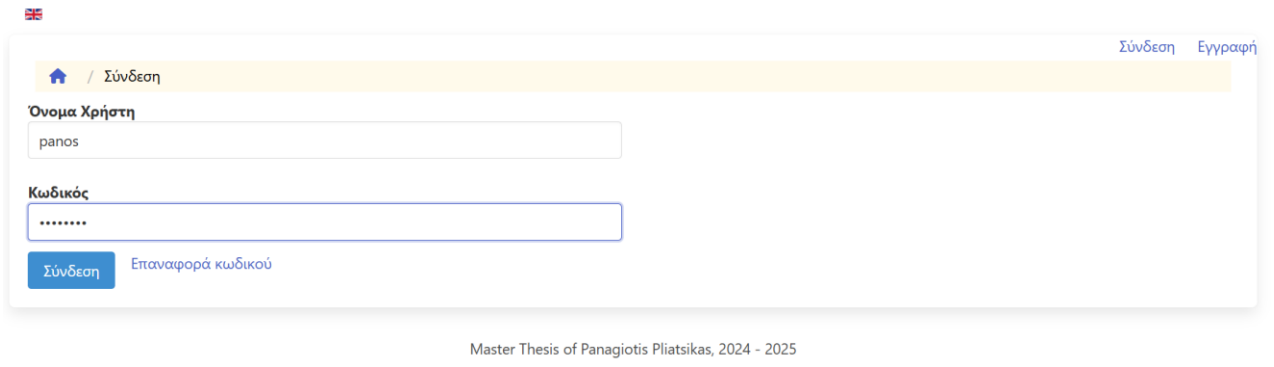
Σε αυτό το μήνυμα περιέχεται ένας σύνδεσμος τον οποίον ο χρήστης θα πρέπει να πατήσει. Μόλις τον πατήσει, θα σταλεί ένα αίτημα στην εφαρμογή για ενεργοποίηση του λογαριασμού του χρήστη. Στην παρακάτω εικόνα βλέπουμε το email που στάλθηκε στη διεύθυνση ηλεκτρονικού ταχυδρομείου που παρείχε ο χρήστης.



Εικόνα 44. Email ενεργοποίησης λογαριασμού

5.2.3 Σενάριο Επιτυχούς Σύνδεσης στην Εφαρμογή

Το τρίτο σενάριο που θα παρουσιάσουμε είναι η επιτυχής σύνδεση του χρήστη στην εφαρμογή. Όταν ολοκληρωθεί με επιτυχία το προηγούμενο σενάριο ενεργοποίησης του λογαριασμού του χρήστη, τότε αυτός θα μπορεί να συνδεθεί στην εφαρμογή. Για να το κάνει αυτό θα πρέπει αρχικά να πατήσει το κουμπί 'Σύνδεση' στο μενού πάνω δεξιά, όπως φαίνεται στην Εικόνα 41, και στη συνέχεια να εισάγει τα διαπιστευτήρια του και να πατήσει το κουμπί 'Σύνδεση', όπως φαίνεται στην Εικόνα 45. Στην Εικόνα 46 φαίνεται η αρχική σελίδα της εφαρμογής μετά την επιτυχή είσοδο του χρήστη.

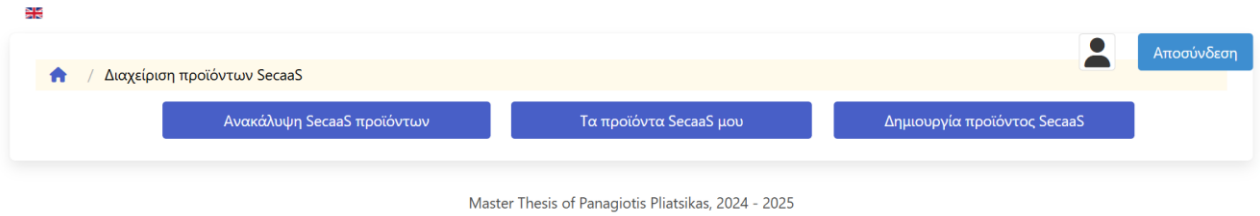


Εικόνα 45. Είσοδος χρήστη

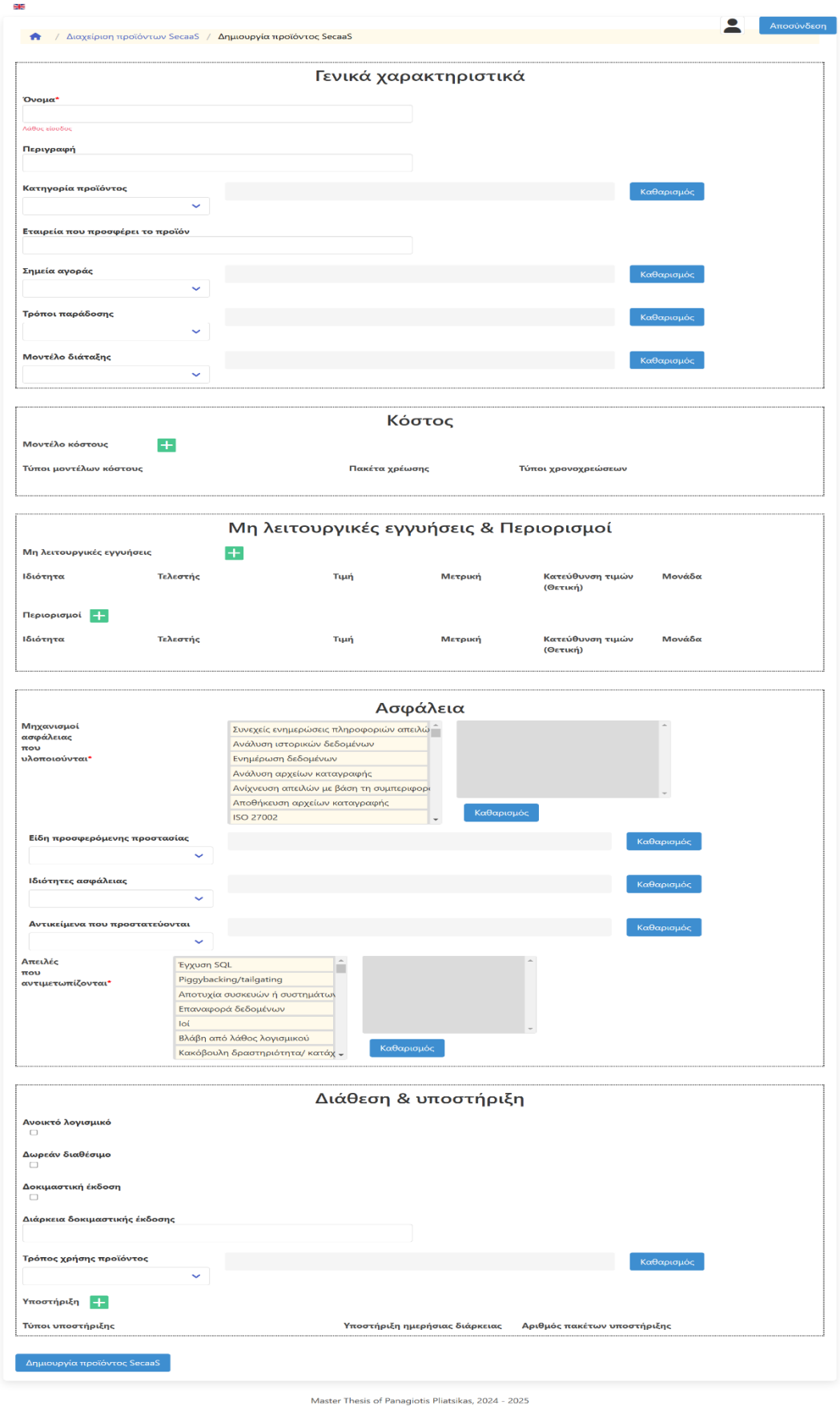
Εικόνα 46. Αρχική σελίδα χρήστη

5.2.4 Σενάριο Δημιουργία Προϊόντος

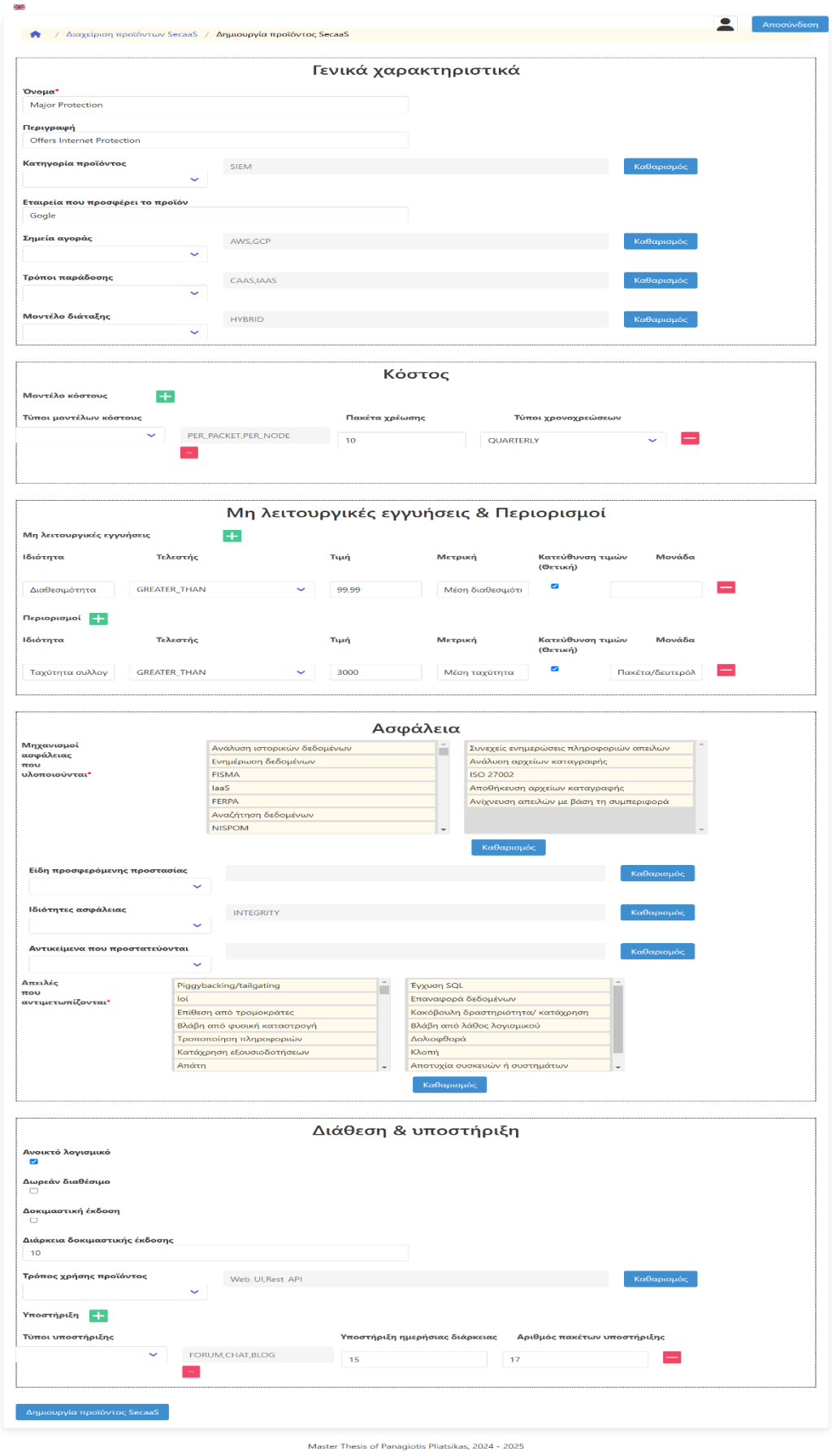
Εδώ θα περιγράψουμε το σενάριο δημιουργίας ενός προϊόντος SecaaS. Ο χρήστης, αφού συνδεθεί στην εφαρμογή, μπορεί να δημιουργήσει ένα προϊόν μεταβαίνοντας στην αντίστοιχη σελίδα που φαίνεται στην Εικόνα 48. Για να μεταβεί εκεί θα πρέπει να πατήσει το κουμπί 'Διαχείριση προϊόντων SecaaS' που φαίνεται στην Εικόνα 46 και στη συνέχεια το κουμπί 'Δημιουργία προϊόντος SecaaS' που φαίνεται στην Εικόνα 47. Εκεί, θα εμφανιστούν όλα τα χαρακτηριστικά που μπορεί να έχει ένα προϊόν SecaaS και οι πιθανές επιλογές αυτών. Ο χρήστης δεν είναι υποχρεωμένος να συμπληρώσει όλα τα πεδία – το αστεράκι δίπλα από το όνομα του εκάστοτε πεδίου προσδιορίζει πως αυτό είναι υποχρεωτικό. Όταν ο χρήστης συμπληρώσει τα πεδία που επιθυμεί, όπως φαίνεται στην Εικόνα 49, και πατήσει το κουμπί 'Δημιουργία προϊόντος SecaaS', θα δημιουργηθεί το καινούριο προϊόν και το σύστημα θα τον πλοηγήσει στην οθόνη με τα προϊόντα που έχει δημιουργήσει ο ίδιος, όπως φαίνεται στην Εικόνα 50.



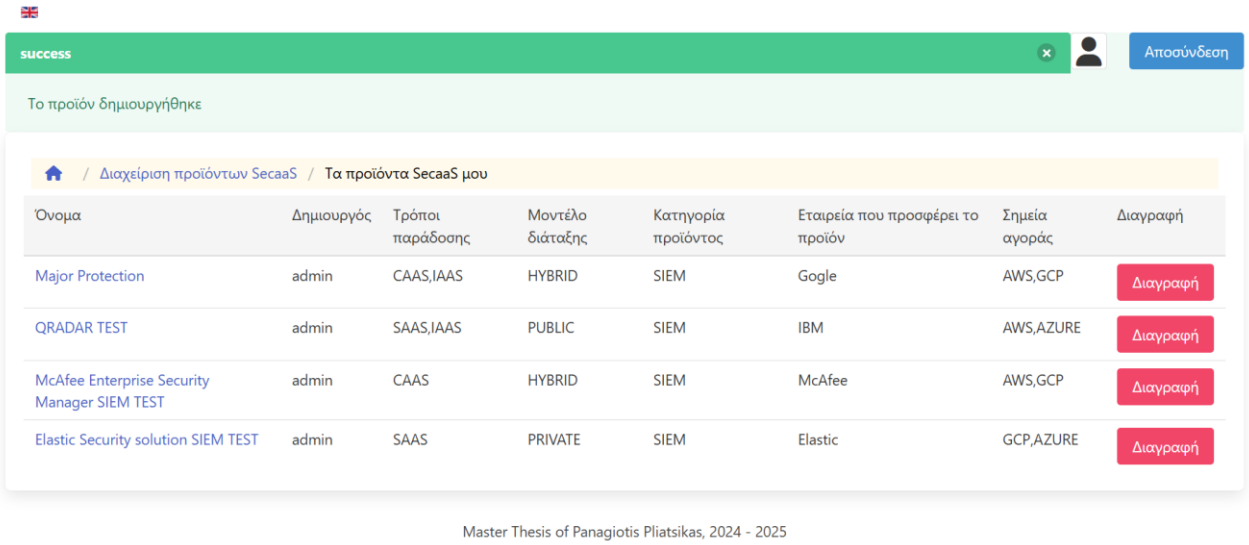
Εικόνα 47. Μενού διαχείρισης προϊόντων SecaaS



Εικόνα 48. Δημιουργία προϊόντος



Εικόνα 49. Στοιχεία νέου προϊόντος



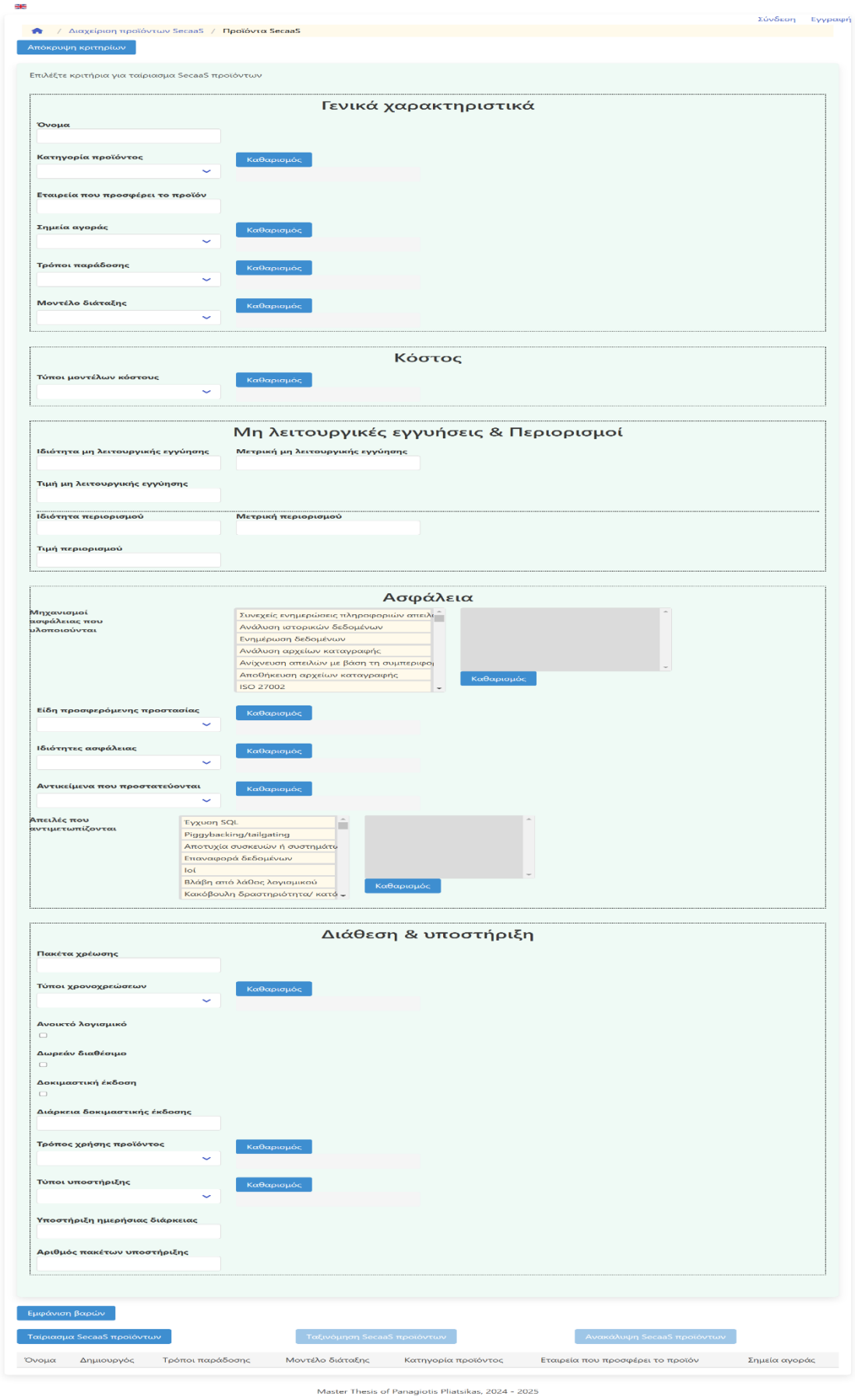
Εικόνα 50. Τα προϊόντα του χρήστη

5.2.5 Σενάριο Ταιριάσματος Προϊόντων

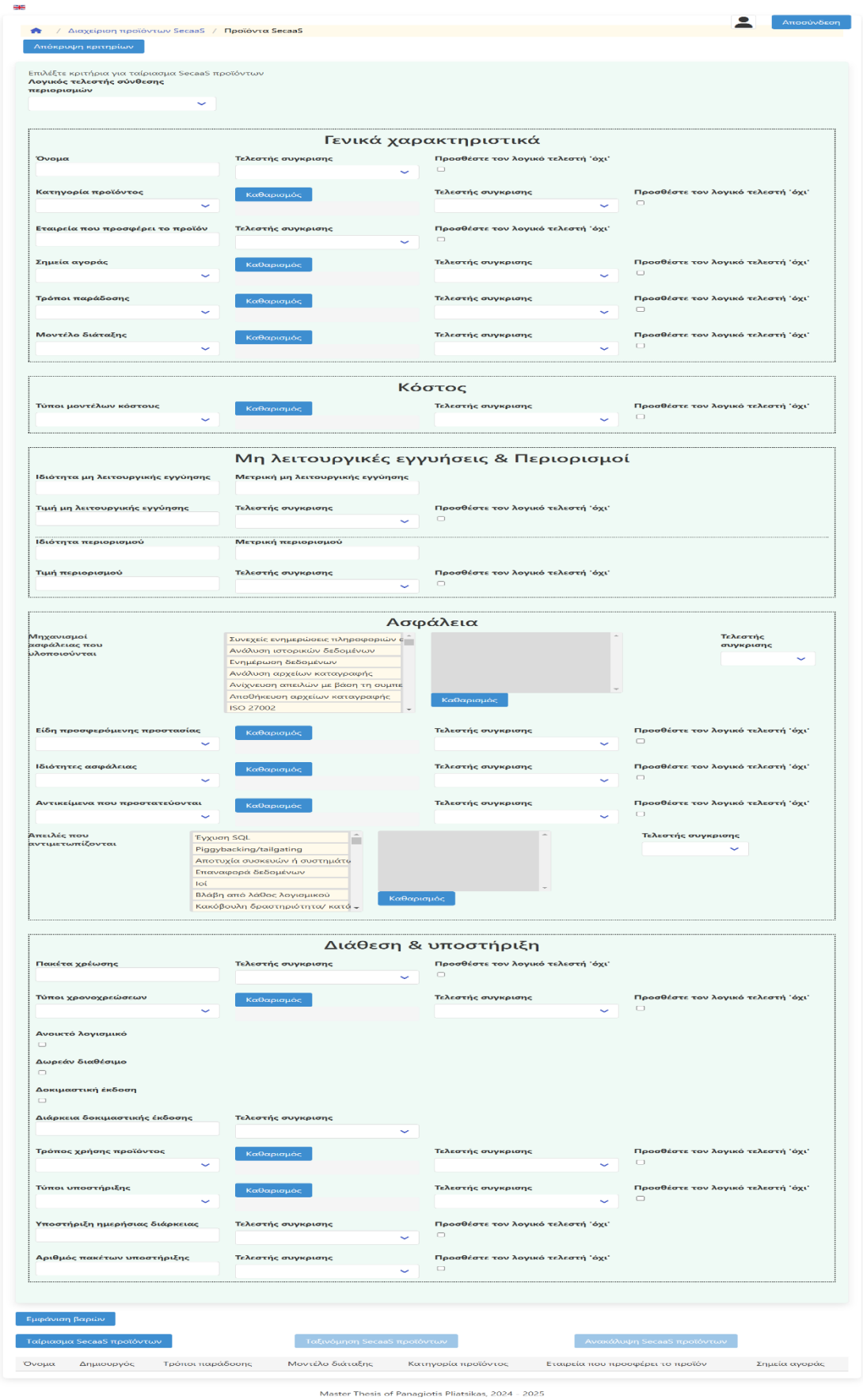
Σε αυτό την ενότητα θα παρουσιάσουμε ένα σενάριο ταιριάσματος προϊόντων. Για τις ανάγκες αυτού και του επόμενου σεναρίου, στην εφαρμογή μας έχουμε δημιουργήσει ήδη 3 προϊόντα SecaaS, τα οποία φαίνονται στην Εικόνα 51. Η λειτουργία του ταιριάσματος είναι διαθέσιμη όχι μόνο στους χρήστες της εφαρμογής, αλλά και στους επισκέπτες. Οι τελευταίοι μπορούν να συνδυάσουν τις απαιτήσεις τους μόνο με συζευκτικό τρόπο (λογικό AND), ενώ οι (εγγεγραμμένοι) χρήστες μπορούν να συνδυάζουν τις απαιτήσεις τους και με άλλους λογικούς τελεστές (εκτός του AND - σύζευξης), όπως OR (διάζευξης), XOR (αποκλειστικής διάζευξης) και NOT (λογικής άρνησης). Για να πάμε στην οθόνη ταιριάσματος προϊόντων θα πρέπει από την αρχική σελίδα να πατήσουμε το κουμπί ‘Διαχείριση προϊόντων SecaaS’ (Εικόνα 46) και στη συνέχεια, στο μενού που θα εμφανιστεί, το κουμπί ‘Ανακάλυψη SecaaS προϊόντων’ (Εικόνα 47). Στις Εικόνες 52 και 53 φαίνονται οι διαφορές στις οθόνες μεταξύ των επισκεπτών και εγγεγραμμένων χρηστών, αντίστοιχα. Στο σενάριο μας, θα βασιστούμε στην οθόνη της Εικόνας 53 (για να καλύψουμε την περίπτωση εγγεγραμμένου χρήστη). Συμπληρώνοντας τα κριτήρια που θέλουμε, όπως φαίνεται στην Εικόνα 54, και πατώντας το κουμπί ‘Ταίριασμα SecaaS προϊόντων’ θα εμφανιστούν τα αποτελέσματα της Εικόνας 55.

Όνομα	Δημιουργός	Τρόποι παράδοσης	Μοντέλο διάταξης	Κατηγορία προϊόντος	Εταιρεία που προσφέρει το προϊόν	Σημεία αγοράς
McAfee Enterprise Security Manager SIEM TEST	admin	CAAS	HYBRID	SIEM	McAfee	AWS,GCP
Elastic Security solution SIEM TEST	admin	SAAS	PRIVATE	SIEM	Elastic	GCP,AZURE
QRADAR TEST	admin	SAAS,IAAS	PUBLIC	SIEM	IBM	AWS,AZURE

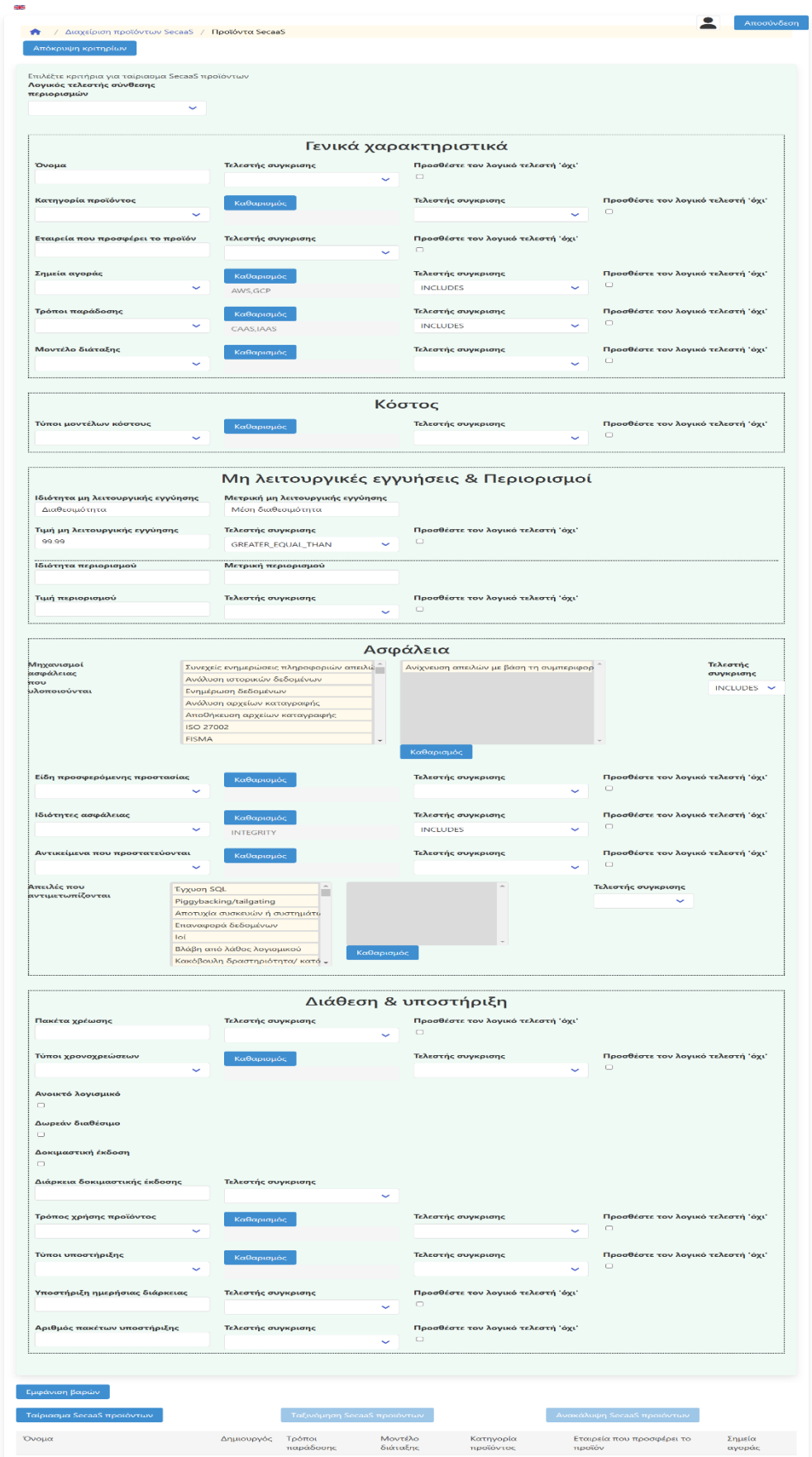
Εικόνα 51. Δημοσιευμένα προϊόντα SecaaS



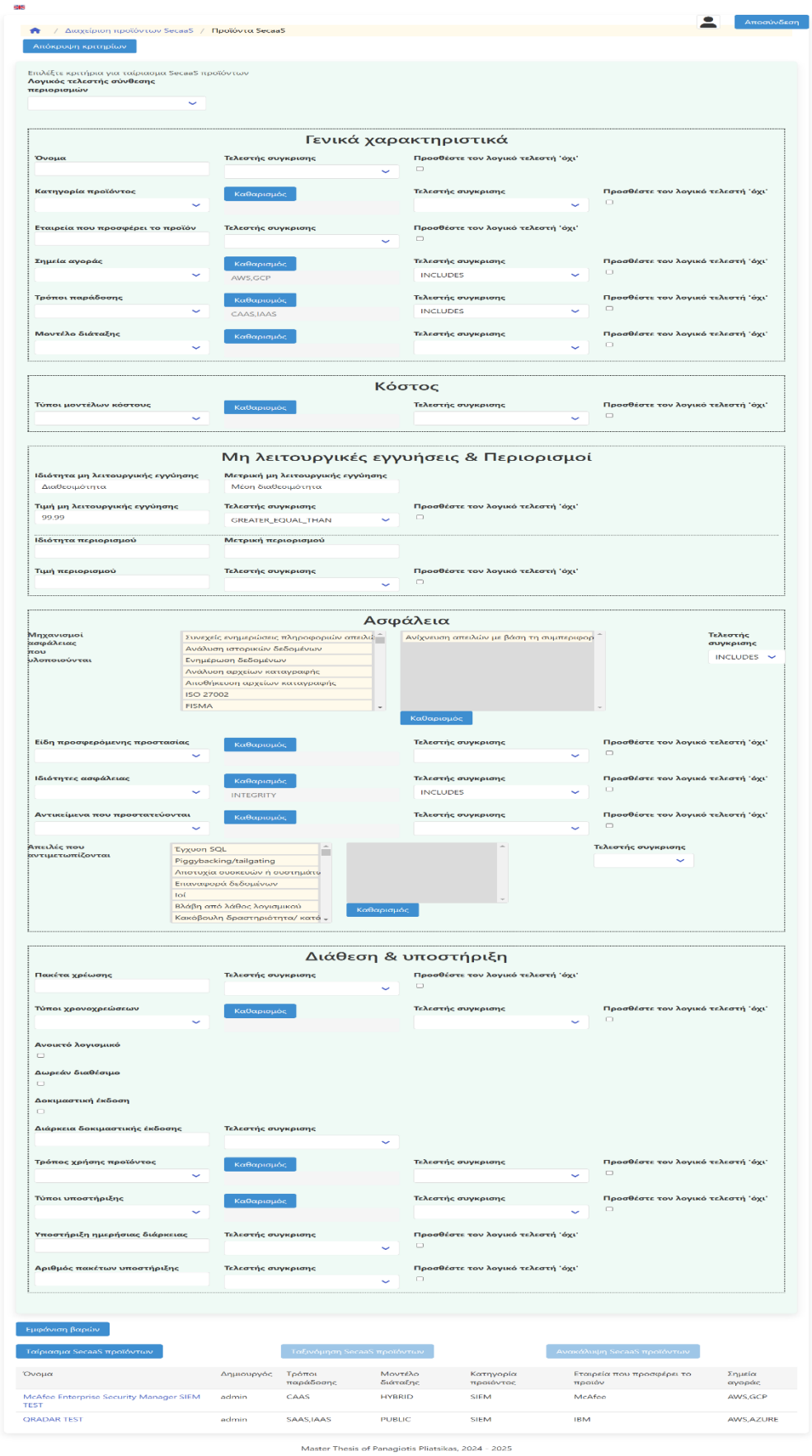
Εικόνα 52. Οθόνη ταιριάσματος για επισκέπτη



Εικόνα 53. Οθόνη ταιριάσματος για εγγεγραμμένο χρήστη



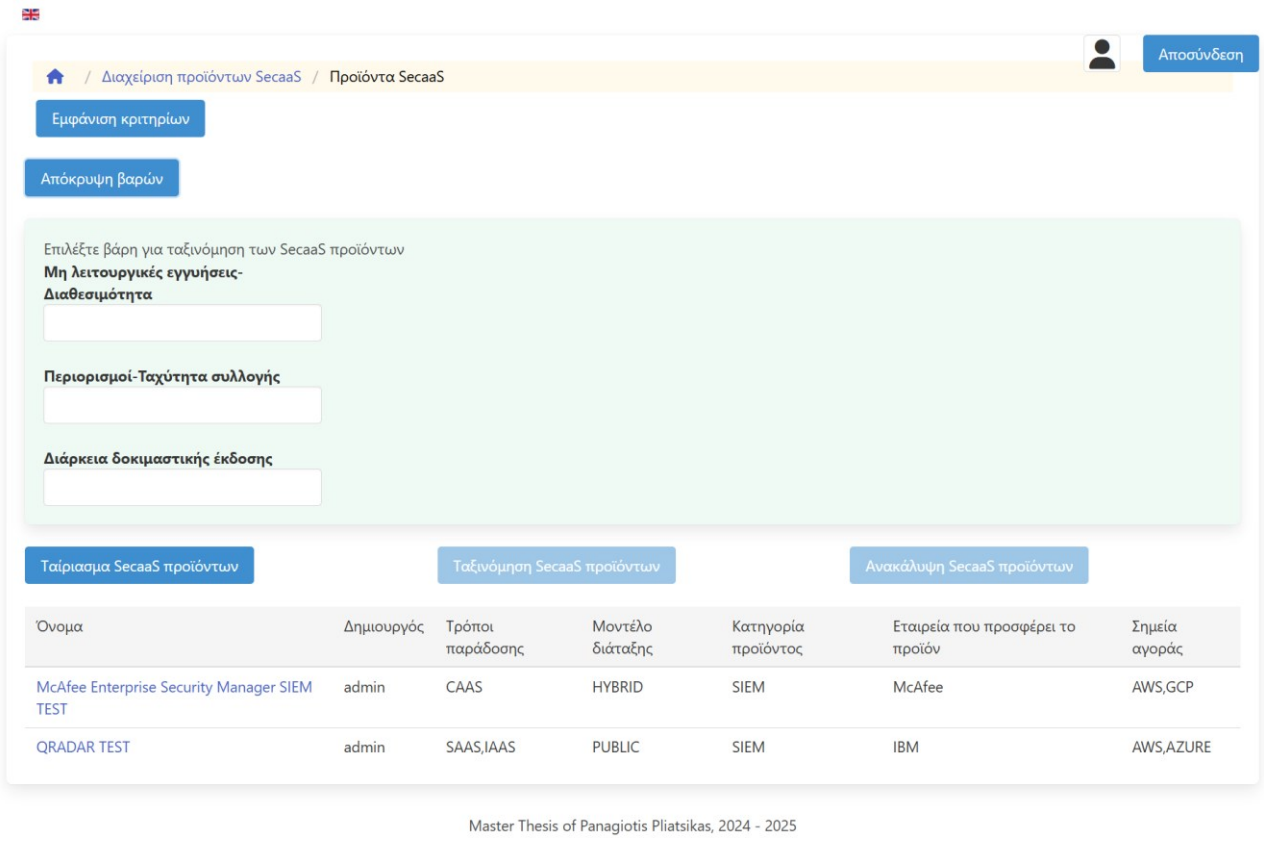
Εικόνα 54. Κριτήρια ταιριάσματος



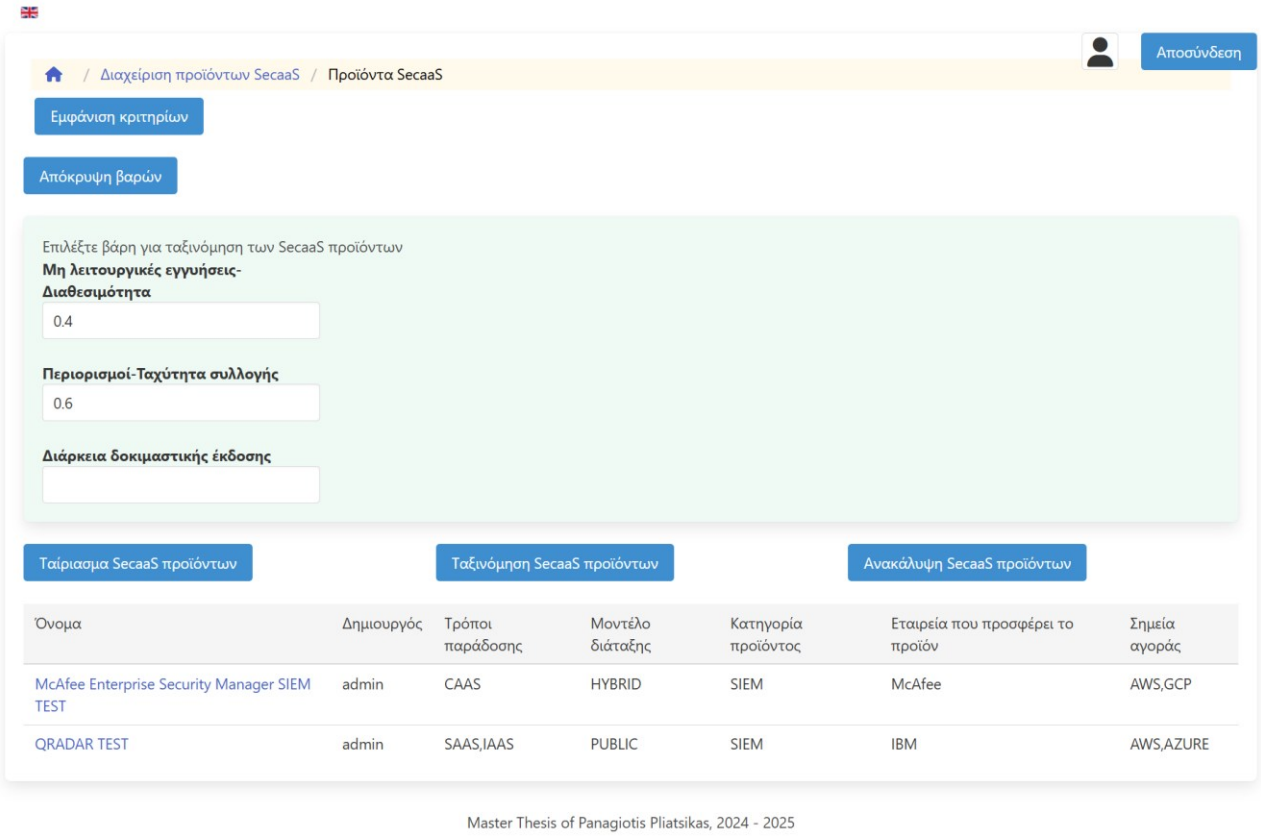
Εικόνα 55. Αποτελέσματα ταιριάσματος

5.2.6 Σενάριο Ταξινόμησης Προϊόντων

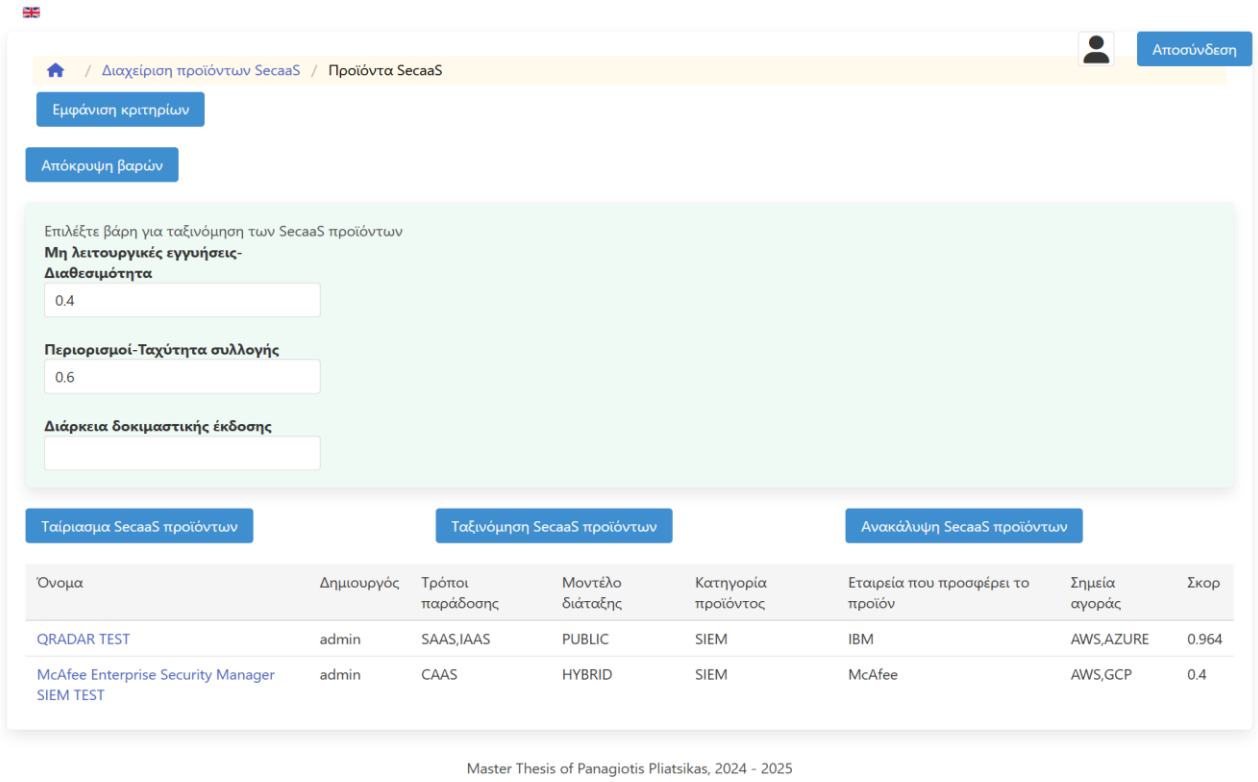
Το τελευταίο σενάριο που θα παρουσιάσουμε είναι αυτό της ταξινόμησης προϊόντων SecaaS. Έχοντας ολοκληρώσει την αναζήτηση βάσει του προηγούμενου σεναρίου, θα ταξινομήσουμε τα προϊόντα που προέκυψαν ως αποτέλεσμα. Για το σενάριο αυτό αρχικά θα παραμείνουμε στην ίδια σελίδα με το προηγούμενο σενάριο (Εικόνα 55) και ο χρήστης θα πρέπει να πατήσει το κουμπί 'Εμφάνιση βαρών' για να εμφανιστούν οι διαθέσιμες επιλογές βαρών που έχει ο χρήστης (Εικόνα 56). Συμπληρώνοντας τα, όπως φαίνεται στην Εικόνα 57 και πατώντας το κουμπί 'Ταξινόμηση SecaaS προϊόντων', θα εμφανιστεί η Εικόνα 58, στην οποία παρατηρούμε ότι έχει αλλάξει η σειρά των αποτελεσμάτων σε σχέση με αυτήν της Εικόνας 55 ενώ εμφανίζεται και το σκορ του κάθε προϊόντος. Αυτό σημαίνει ότι η ταξινόμηση άλλαξε τη σειρά των προϊόντων SecaaS, σύμφωνα με τα βάρη που δόθηκαν.



Εικόνα 56. Διαθέσιμες επιλογές βαρών



Εικόνα 57. Επιλογές βαρών χρήστη



Εικόνα 58. Αποτελέσματα ταξινόμησης

Για την τεκμηρίωση των αποτελεσμάτων του σεναρίου της ταξινόμησης, αλλά και του προηγούμενου σεναρίου του ταιριάσματος παραθέτουμε παρακάτω στις 3 επόμενες εικόνες (Εικόνα 59, Εικόνα 60 και Εικόνα 61) τα χαρακτηριστικά των 3 προϊόντων SecaaS που συμμετείχαν σε αυτά τα σενάρια. Για το ταίριασμα, όπως βλέπουμε στην Εικόνα 54, χρησιμοποιήσαμε ως περιορισμούς τα προϊόντα να έχουν ως σημεία αγοράς οποιοδήποτε από τα ΄AWS' και 'GCP', ως τρόπους παράδοσης οποιοδήποτε από τα 'CAAS' και 'IAAS', ως μηχανισμό ασφαλείας που υλοποιεί την 'Ανίχνευση απειλών με βάση τη συμπεριφορά', ως ιδιότητα ασφάλειας μόνο την 'INTEGRITY' ενώ ζητάμε η μέση διαθεσιμότητα να είναι μεγαλύτερη ή ίση από 99.99%.

Βλέποντας τις τρεις παρακάτω εικόνες, παρατηρούμε ότι τα προϊόντα μόνο των Εικόνων 59 (QRADAR TEST) και 60 (McAfee Enterprise Security Manager SIEM TEST) πληρούν όλα τα κριτήρια που δώσαμε, ενώ το προϊόν της Εικόνας 61 (Elastic Security solution SIEM TEST) δεν ικανοποιεί τον περιορισμό για το μοντέλο/τρόπο παράδοσης και για τη μη λειτουργική εγγύηση της μέσης διαθεσιμότητας. Συνεπώς, ορθώς οδηγηθήκαμε στο αποτέλεσμα της Εικόνας 55, με μόνο τα 2 πρώτα προϊόντα στην εμφανιζόμενη λίστα.

Για την ταξινόμηση δώσαμε βάρη στα χαρακτηριστικά της Διαθεσιμότητας που ανήκει στις μη λειτουργικές εγγυήσεις και στην ταχύτητα συλλογής που ανήκει στους περιορισμούς. Το προϊόν της Εικόνας 59 (QRADAR TEST) έχει τιμή 99.99 στη (μέση) Διαθεσιμότητα με θετική κατεύθυνση και 3000 στην (μέση) ταχύτητα συλλογής, ενώ το προϊόν της Εικόνας 60 (McAfee Enterprise Security Manager SIEM TEST) έχει τιμή 99.999 (με θετική κατεύθυνση) και 500 αντίστοιχα. Η μέγιστη τιμή για τη (μέση) Διαθεσιμότητα όλων των αποθηκευμένων προϊόντων SecaaS είναι 99.999 και η ελάχιστη 99.9. Αντίστοιχα, για τη (μέση) ταχύτητα συλλογής η μέγιστη τιμή είναι 3000 και η ελάχιστη 500. Στη συνέχεια θα εφαρμόσουμε τον τύπο για τον υπολογισμό του συνολικού σκορ για το κάθε προϊόν, ο οποίος θα βασιστεί στον τύπο υπολογισμού επιμέρους σκορ για μη λειτουργικές ιδιότητες θετικής κατεύθυνσης (επειδή και οι δύο ιδιότητες έχουν όντως θετική κατεύθυνση), πάνω στις παραπάνω τιμές των δυο προϊόντων για τις μετρικές της μέσης διαθεσιμότητας και μέσης ταχύτητας συλλογής. Οι δύο αυτοί τύποι αναφέρθηκαν στην Ενότητα 4.2.1.2 στην παράγραφο για την Ταξινόμηση.

Για το προϊόν QRADAR TEST έχουμε:

[((99.99 - 99.9) / (99.999 - 99.9)) * 0.4] + [((3000 – 500) / (3000 - 500)) * 0.6] = 0.364 + 0.6 = **0.964**

Για το προϊόν McAfee Enterprise Security Manager SIEM TEST έχουμε:

[((99.999 - 99.9) / (99.999 - 99.9)) * 0.4] + [((500 – 500) / (3000 - 500)) * 0.6] = 0.4 + 0 = **0.4**

Οπότε, βλέπουμε ότι εφαρμόζοντας τον τύπο για κάθε τιμή χαρακτηριστικού στην οποία δώσαμε βάρος και στη συνέχεια προσθέτοντας το αποτέλεσμα με βάση τα παρεχόμενα βάρη, επαληθεύουμε το αποτέλεσμα ταξινόμησης που βλέπουμε στην Εικόνα 58.

Εικόνα 59. Προϊόν QRADAR

Αποσύνδεση

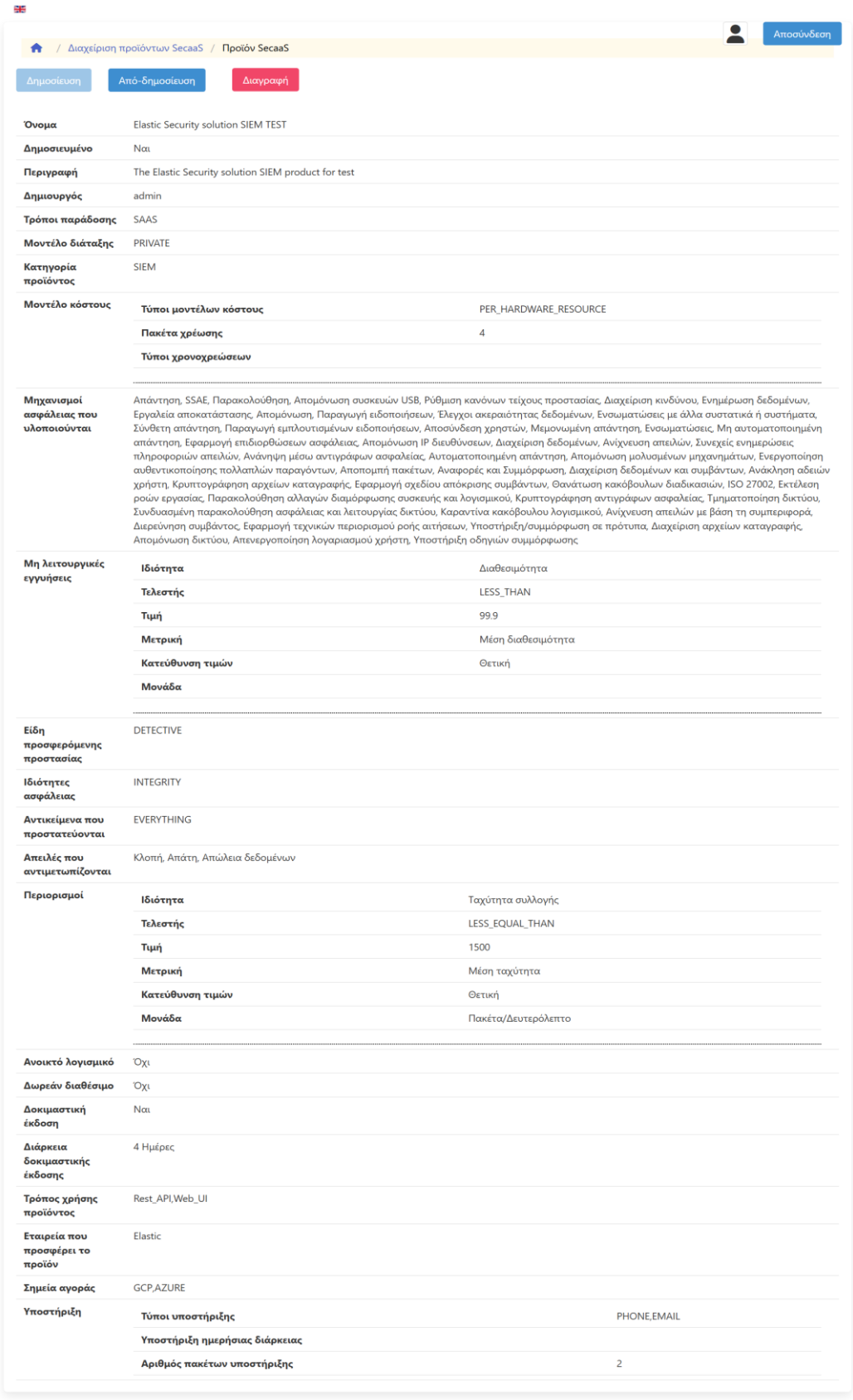
Διαχείριση προϊόντων SecaaS / Προϊόν SecaaS

Δημοσίευση | Από-δημοσίευση | Διαγραφή

Όνομα	McAfee Enterprise Security Manager SIEM TEST		
Δημοσιευμένο	Ναι		
Περιγραφή	The McAfee Enterprise Security Manager SIEM product for test		
Δημιουργός	admin		
Τρόποι παράδοσης	CAAS		
Μοντέλο διάταξης	HYBRID		
Κατηγορία προϊόντος	SIEM		
Μοντέλο κόστους	**Τύποι μοντέλων κόστους**	PER_WORKLOAD	
	Πακέτα χρέωσης	20	
	Τύποι χρονοχρεώσεων		
Μηχανισμοί ασφάλειας που υλοποιούνται	Ανίχνευση απειλών με βάση τη συμπεριφορά, Ανίχνευση απειλών με βάση τη TN, Ανίχνευση απειλών με βάση αρχεία καταγραφής, Ανίχνευση απειλών σε πραγματικό χρόνο, Ανίχνευση απειλών σε πραγματικό χρόνο σε αρχεία καταγραφής, Ανίχνευση απειλών σε πραγματικό χρόνο με βάση τη μηχανική μάθηση, Ανίχνευση απειλών σε πραγματικό χρόνο με βάση κανόνες, Ανίχνευση απειλών σε πραγματικό χρόνο με βάση κανόνες συσχέτισης, Ανίχνευση απειλών σε πραγματικό χρόνο με βάση κανόνες ανίχνευσης κατωφλιού, Ανίχνευση απειλών σε πραγματικό χρόνο με βάση κανόνες ανίχνευσης ανωμαλιών		
Μη λειτουργικές εγγυήσεις	**Ιδιότητα**	Διαθεσιμότητα	
	Τελεστής	LESS_THAN	
	Τιμή	99.999	
	Μετρική	Μέση διαθεσιμότητα	
	Κατεύθυνση τιμών	Θετική	
	Μονάδα		
Είδη προσφερόμενης προστασίας	DETECTIVE		
Ιδιότητες ασφάλειας	INTEGRITY		
Αντικείμενα που προστατεύονται	DATA		
Απειλές που αντιμετωπίζονται	Κλοπή, Απάτη, Απώλεια δεδομένων		
Περιορισμοί	**Ιδιότητα**	Ταχύτητα συλλογής	
	Τελεστής	LESS_EQUAL_THAN	
	Τιμή	500	
	Μετρική	Μέση ταχύτητα	
	Κατεύθυνση τιμών	Θετική	
	Μονάδα	Πακέτα/Δευτερόλεπτο	
Ανοικτό λογισμικό	Όχι		
Δωρεάν διαθέσιμο	Όχι		
Δοκιμαστική έκδοση	Ναι		
Διάρκεια δοκιμαστικής έκδοσης	14 Ημέρες		
Τρόπος χρήσης προϊόντος	CLI,Web_UI		
Εταιρεία που προσφέρει το προϊόν	McAfee		
Σημεία αγοράς	AWS,GCP		
Υποστήριξη	**Τύποι υποστήριξης**	PHONE,EMAIL,FAQ_DOCUMENTATION,NOTIFICATIONS,COMMUNITY	
	Υποστήριξη ημερήσιας διάρκειας		
	Αριθμός πακέτων υποστήριξης	4	

Master Thesis of Panagiotis Pliatsikas, 2024 - 2025

Εικόνα 60. Προϊόν McAfee

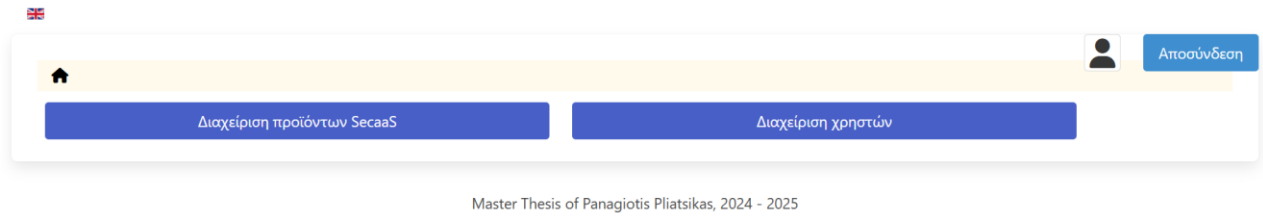


Εικόνα 61. Προϊόν Elastic

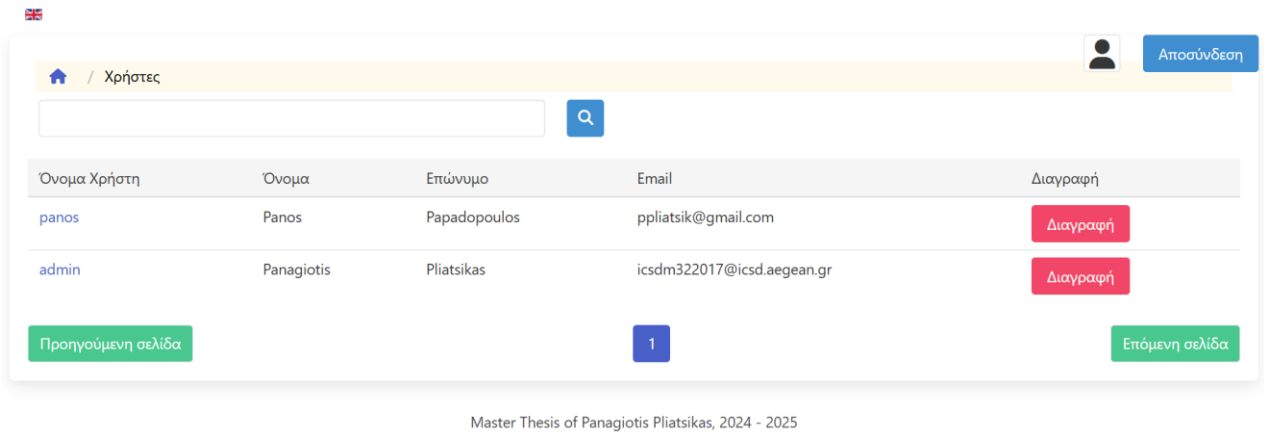
5.2.7 Σενάριο Διαγραφής Χρήστη από τον Διαχειριστή

Εδώ θα παρουσιάσουμε το σενάριο της διαγραφής ενός χρήστη από τον διαχειριστή. Αρχικά, θα πρέπει να συνδεθούμε στην εφαρμογή ως διαχειριστές του συστήματος. Αυτό φαίνεται στην Εικόνα 62. Μόλις γίνει αυτό θα εμφανιστεί στην οθόνη μας η Εικόνα 63, στην οποία θα πρέπει να πατήσουμε το κουμπί 'Διαχείριση χρηστών'. Όταν το πατήσουμε, θα μεταφερθούμε στην οθόνη της Εικόνας 64, στην οποία φαίνεται η λίστα με τους χρήστες που είναι εγγεγραμμένοι αυτή την στιγμή στην εφαρμογή και στην τελευταία κολώνα κάθε γραμμής του πίνακα υπάρχει το κουμπί 'Διαγραφή'. Για τις ανάγκες του σεναρίου θα πατήσουμε το κουμπί για να διαγράψουμε τον χρήστη με το όνομα χρήστη 'panos'. Πατώντας το, θα εμφανιστεί ένα παράθυρο επιβεβαίωσης της ενέργειας της διαγραφής, όπως φαίνεται στην Εικόνα 65 και αν πατήσουμε 'Ναι' τότε ο χρήστης θα διαγραφεί και θα εμφανιστεί η Εικόνα 66.

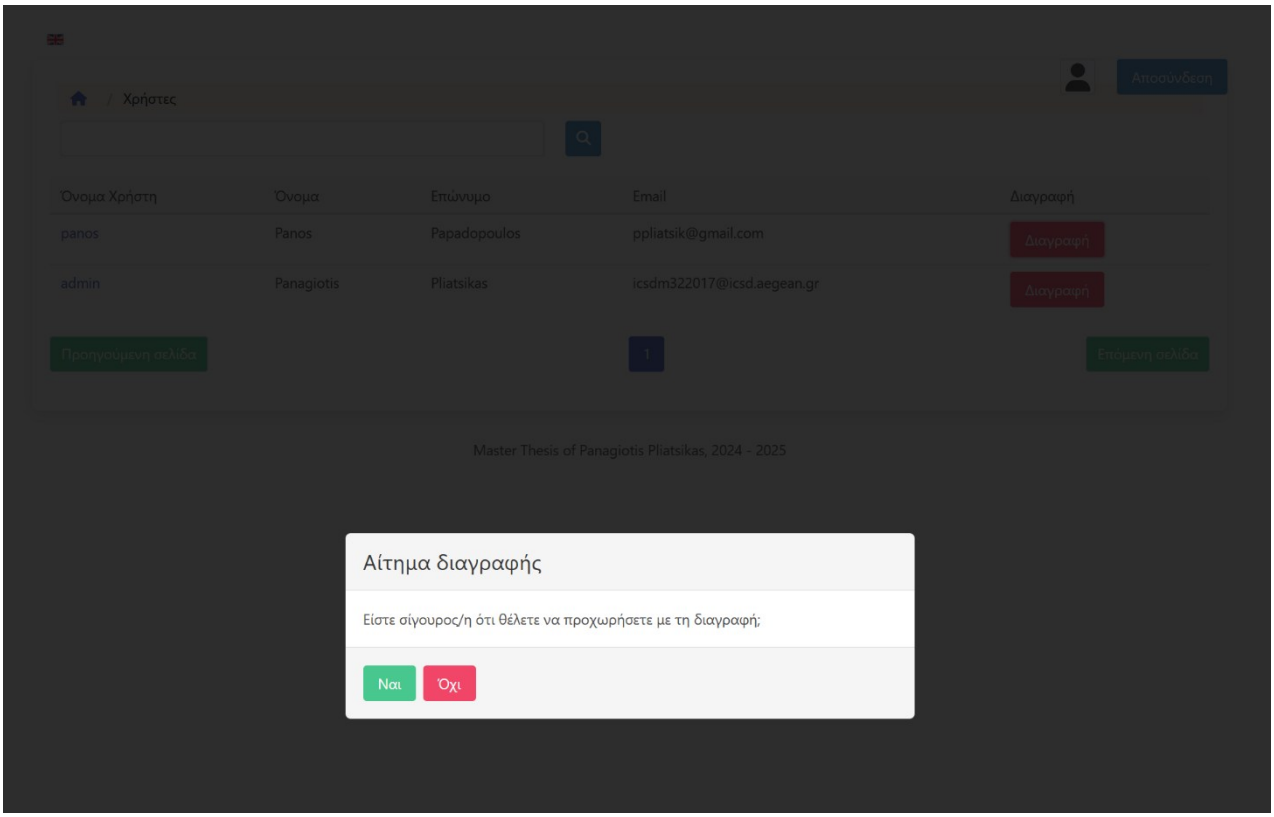
Εικόνα 62. Σύνδεση διαχειριστή στην εφαρμογή



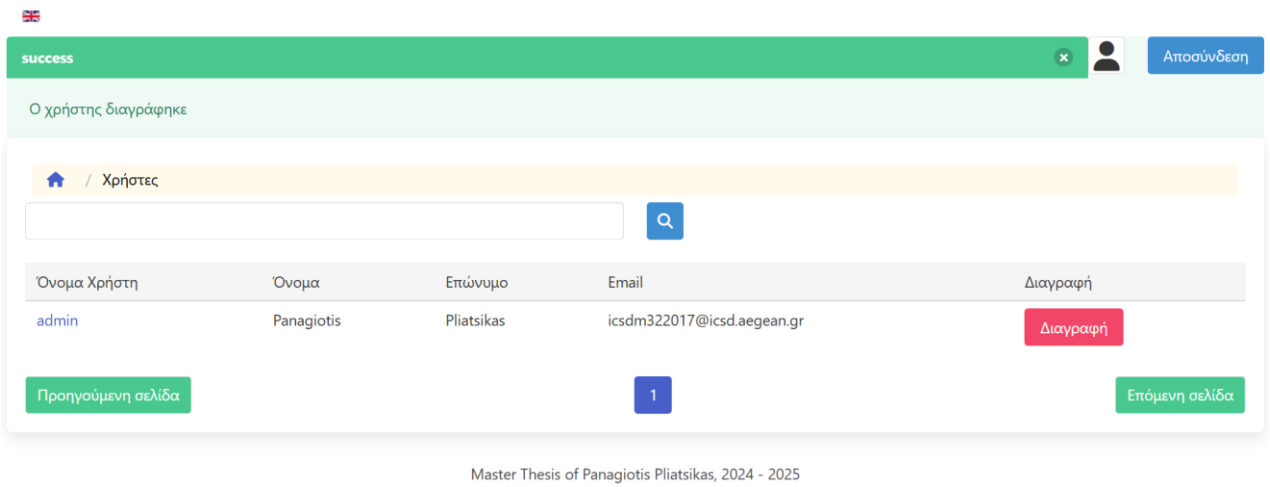
Εικόνα 63. Αρχική σελίδα διαχειριστή



Εικόνα 64. Λίστα χρηστών συστήματος



Εικόνα 65. Επιβεβαίωση διαγραφής χρήστη



Εικόνα 66. Επιτυχημένη διαγραφή χρήστη

6

Συμπεράσματα και Μελλοντική Εργασία

6.1 Συμπεράσματα

Στην παρούσα εργασία παρουσιάστηκε η έννοια του υπολογιστικού νέφους, ενώ αναλύθηκαν τα πλεονεκτήματα που αυτό προσφέρει και αναφέρθηκαν τα διαφορετικά είδη του. Επίσης, αναλύθηκε η έννοια της Ασφάλειας-ως-Υπηρεσίας, τα πλεονεκτήματα και τα μειονεκτήματα της, οι διάφορες κατηγορίες που έχει και η ανάγκη που οδήγησε στη δημιουργία προϊόντων που την υλοποιούν. Παρουσιάζοντας τις πιο σημαντικές εργασίες ανακάλυψης που έχουν γίνει μέχρι τη στιγμή που γράφεται αυτή η εργασία για αυτά τα προϊόντα και τα σημεία αγοράς τέτοιων προϊόντων, γίνεται αντιληπτό ότι αυτό που έλειπε είναι μια εφαρμογή που να μπορεί να συλλέξει όλες τις δυνατές και σχετικές πληροφορίες που αφορούν τα προϊόντα SecaaS και να προσφέρει στους χρήστες τη δυνατότητα να τα αναζητήσουν με σημασιολογικό τρόπο καθώς και να τα ταξινομήσουν με βάση συγκεκριμένα κριτήρια.

Η συνεισφορά αυτής της εργασίας έγκειται στην πλήρη κάλυψη της προαναφερόμενης έλλειψης. Ειδικότερα, δημιουργήσαμε μια εφαρμογή μέσω της οποίας μπορεί ο κάθε πάροχος προϊόντων SecaaS να τα δημοσιοποιήσει στο διαδίκτυο. Η εφαρμογή μας προσφέρει στους παρόχους τη δυνατότητα να αποθηκεύσουν τα προϊόντα τους χρησιμοποιώντας μια πληθώρα λειτουργικών και μη λειτουργικών χαρακτηριστικών, τα οποία μπορούν να καλύψουν πλήρως τις ανάγκες περιγραφής ενός οποιουδήποτε προϊόντος SecaaS. Επιπλέον, η εφαρμογή μας δίνει τη δυνατότητα στους καταναλωτές τέτοιων προϊόντων να τα αναζητήσουν σημασιολογικά με βάση τα κριτήρια που επιθυμούν, ώστε να βρουν ποια καλύπτουν τις απαιτήσεις τους. Η σημασιολογική αναζήτηση μπορεί να γίνει και στα λειτουργικά και στα μη λειτουργικά χαρακτηριστικά των προϊόντων SecaaS. Τέλος, κάτι πολύ σημαντικό που προσφέρει η εφαρμογή μας είναι η λειτουργία της ταξινόμησης προϊόντων SecaaS. Ο χρήστης αφού αναζητήσει και βρει κάποια προϊόντα σύμφωνα με ορισμένα κριτήρια, ή και χωρίς να έχει προηγηθεί η ενέργεια της αναζήτησης και δίνοντας σχετικά βάρη στα κριτήρια (ταξινόμησης) που επιθυμεί, μπορεί να ταξινομήσει τα αποτελέσματα. Η ταξινόμηση, σε αντίθεση με την αναζήτηση, μπορεί να γίνει μόνο στα μη λειτουργικά χαρακτηριστικά και στους περιορισμούς των προϊόντων SecaaS. Το προϊόν με το υψηλότερο σκορ εμφανίζεται πρώτο στη σχετική λίστα, δηλαδή η ταξινόμηση πραγματοποιείται σε φθίνουσα σειρά.

6.2 Μελλοντική Εργασία

Για τη δημιουργία της εφαρμογής, στα πλαίσια της εργασίας, αναλύθηκαν μόνο οι μηχανισμοί ασφάλειας που αφορούν τα προϊόντα SecaaS της κατηγορίας Διαχείριση Πληροφοριών και Συμβάντων Ασφαλείας (Security Information & Event Management (SIEM)). Συνεπώς, αυτοί χρησιμοποιήθηκαν και στην εφαρμογή ως τιμές του συγκεκριμένου χαρακτηριστικού. Ως μελλοντική εργασία που θα αποτελεί συνέχεια της παρούσας, θα μπορούσε να γίνει ανάλυση και των υπόλοιπων κατηγοριών προϊόντων SecaaS, ώστε να ενταχθούν και οι μηχανισμοί ασφάλειας που τις αφορούν.

Σε επόμενη φάση θα μπορούσε να γίνει πλήρης δοχειοποίηση της εφαρμογής, ώστε με την εντολή της Εικόνας 35 να εκτελείται άμεσα όλη η εφαρμογή. Επιπλέον, η εφαρμογή μας θα μπορούσε να συλλέγει αυτόματα πληροφορίες για προϊόντα SecaaS από σημεία αγοράς ή/και την επίσημη ιστοσελίδα τους.

Το ταίριασμα θα μπορούσε να επιτευχθεί και με εναλλακτικό τρόπο με βάση την παροχή προτάσεων ή λέξεων κλειδιών από τον χρήστη και την υποκείμενη χρήση τεχνικών μηχανικής μάθησης. Επίσης, για το ταίριασμα θα μπορούσε να υλοποιηθεί αλλιώς η διεπαφή χρήστη. Αντί να υπάρχουν διαθέσιμα όλα τα χαρακτηριστικά, όπως είναι τώρα, η εφαρμογή μας θα έδινε τη δυνατότητα στον χρήστη να επιλέξει δυναμικά το χαρακτηριστικό που επιθυμεί και την τιμή του. Όσον αφορά τους λογικούς τελεστές για κάθε περιορισμό, αυτοί θα μπορούσαν να επιλεγούν με τη βοήθεια ενός δένδρου. Το δένδρο μπορεί να έχει ως ριζικό κόμβο είτε έναν περιορισμό σε ένα πεδίο ή έναν λογικό τελεστή. Ανάλογα με τον τελεστή στην δεύτερη περίπτωση, ο ριζικός κόμβος μπορεί να έχει ένα ή δύο παιδιά-κόμβους. Οπότε, κατά την επιλογή ενός πατρικού κόμβου, θα υπάρχει ένα κουμπί '+' που θα επιτρέπει στον χρήστη να επιλέγει είτε ένα κόμβο περιορισμού είτε έναν κόμβο λογικού τελεστή. Αν έχουμε έναν κόμβο περιορισμού, έχουμε επιλογή πεδίου και της τιμής του. Αν έχουμε έναν κόμβο τελεστή, θα πρέπει να επιλέγεται ο επιθυμητός λογικός τελεστής. Στο δένδρο δεν θα μπορεί να υπάρχει κόμβος-φύλλο που να αντιστοιχεί σε λογικό τελεστή. Αν κάτι τέτοιο ισχύει, τότε η υποβολή δεν θα επιτρέπεται. Ακόμα για το ταίριασμα, σε μελλοντική φάση θα μπορούσε να δέχεται ως είσοδο από τον χρήστη πολλαπλές εγγυήσεις/περιορισμούς και όχι μόνο μια τιμή για το καθένα όπως συμβαίνει τώρα.

Τέλος, όπως φαίνεται στον Πίνακα 1 στην Ενότητα 4.5 υπάρχουν απαιτήσεις, οι οποίες δεν ικανοποιήθηκαν στον άριστο βαθμό. Αν και υπάρχει η αιτιολόγηση για αυτό στον ίδιο πίνακα, θα μπορούσε σε μελλοντικό χρόνο να γίνει προσπάθεια ώστε να επιτευχθεί και σε αυτές τις απαιτήσεις άριστος βαθμός ικανοποίησης.

Βιβλιογραφία

[1] Hussain, M., & Abdulsalam, H. (2011, April). SECaaS: security as a service for cloud-based applications. In *Proceedings of the Second Kuwait Conference on e-Services and e-Systems* (pp. 1-4).

[2] Guha, R., McCool, R., & Miller, E. (2003, May). Semantic search. In *Proceedings of the 12th international conference on World Wide Web* (pp. 700-709).

[3] Mell, P. (2011). *The NIST Definition of Cloud Computing*. *Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology – US Department of Commerce.

[4] Jaeger B. (2016). *Defined Categories of Security as a Service*. Cloud Security Alliance.

[5] Elsayed, M., & Zulkernine, M. (2018). A Taxonomy of Security as a Service. In *On the Move to Meaningful Internet Systems. OTM 2018 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2018, Valletta, Malta, October 22-26, 2018, Proceedings, Part II* (pp. 305-312). Springer International Publishing.

[6] Furfaro, A., Garro, A., & Tundis, A. (2014, October). Towards security as a service (secaas): On the modeling of security services for cloud computing. In *2014 international carnahan conference on security technology (ICCST)* (pp. 1-6). IEEE.

[7] Elastic Search Platform: https://www.elastic.co/platform (Ημερομηνία πρόσβασης: 15/1/2025)

[8] Google Enterprise Search: https://cloud.google.com/enterprise-search (Ημερομηνία πρόσβασης: 15/1/2025)

[9] Guha, R., McCool, R., & Miller, E. (2003, May). Semantic search. In *Proceedings of the 12th international conference on World Wide Web* (pp. 700-709).

[10] Mäkelä, E. (2005). Survey of semantic search research. In *Proceedings of the seminar on knowledge management on the semantic web*. Department of Computer Science, University of Helsinki, Helsinki.

[11] Adenowo, A. A., & Adenowo, B. A. (2013). Software engineering methodologies: a review of the waterfall model and object-oriented approach. *International Journal of Scientific & Engineering Research*, *4*(7), 427-434.

[12] T. Peters. Timsort description: http://svn.python.org/projects/python/trunk/Objects/listsort.txt (Ημερομηνία πρόσβασης: 15/1/2025)