



ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Σχεδίαση και Ανάπτυξη Συστήματος Διαχείρισης
Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού»



Του φοιτητή
Αϊβαζίδη Δαμιανού
Αρ. Μητρώου: 103624

Επιβλέπων
Χαράλαμπος Μπράτσας
Επίκουρος Καθηγητής

Ημερομηνία 9/9/2025

Τίτλος Π.Ε.: Σχεδίαση και Ανάπτυξη Συστήματος Διαχείρισης Πρόσβασης Εργαζομένων και
Εταιρικού Εξοπλισμού
Κωδικός Π.Ε.: 25185

Όνοματεπώνυμο φοιτητή: Δαμιανός Αϊβαζίδης
Όνοματεπώνυμο εισηγητή: Χαράλαμπος Μπράτσας
Ημερομηνία ανάληψης Π.Ε.: 14/3/2025
Ημερομηνία περάτωσης Π.Ε. 9/9/2025

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως πτυχιακή εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή Δαμιανού Αϊβαζίδη που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης, ο συγγραφέας/δημιουργός εκχωρεί στο Διεθνές Πανεπιστήμιο της Ελλάδος άδεια χρήσης του δικαιώματος αναπαραγωγής, δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσης της εργασίας διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος. Η ανοικτή πρόσβαση στο πλήρες κείμενο της εργασίας, δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού, ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, πώληση, εμπορική χρήση, διανομή, έκδοση, μεταφόρτωση (downloading), ανάρτηση (uploading), μετάφραση, τροποποίηση με οποιοδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού.

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραίτητα και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

«Σε αυτούς που με ενέπνευσαν»

Πρόλογος

Ο λόγος που διάλεξα αυτό το θέμα για την πτυχιακή μου προέρχεται από την εμπειρία μου στην εταιρεία όπου εργάζομαι. Έχω αναλάβει το κομμάτι του ISO compliance και μέσα από αυτό είδα από πρώτο χέρι πόσο δύσκολο και κουραστικό είναι να καταχωρείς χειροκίνητα όλες τις εγγραφές σε αρχεία Excel. Κάθε φορά που χρειαζόταν να περάσω στοιχεία για εργαζόμενους ή εξοπλισμό, υπήρχε πάντα ο κίνδυνος για λάθη και χαμένο χρόνο. Ήταν μια διαδικασία πραγματικά απαιτητική και πολλές φορές αγχωτική.

Αυτό με έκανε να σκεφτώ πόσο πιο εύκολα θα ήταν τα πράγματα αν υπήρχε ένα σύστημα που θα μπορούσε να οργανώνει και να αυτοματοποιεί αυτές τις διαδικασίες. Έτσι αποφάσισα να ασχοληθώ με την ανάπτυξη μιας εφαρμογής για τη διαχείριση πρόσβασης και εταιρικού εξοπλισμού, με σκοπό να μειωθεί η χειροκίνητη εργασία, να υπάρχει περισσότερη ακρίβεια και να γίνεται πιο εύκολη η παρακολούθηση.

Μέσα από αυτή την πτυχιακή κατάφερα να συνδέσω τις γνώσεις των σπουδών μου με μια πραγματική ανάγκη που είχα ήδη συναντήσει στη δουλειά. Το σημαντικότερο για μένα είναι ότι αυτή η εργασία δεν έμεινε απλά σε θεωρητικό επίπεδο, αλλά μου έδωσε την ευκαιρία να δουλέψω πάνω σε κάτι που έχει άμεση πρακτική αξία και μπορεί να φανεί χρήσιμο σε έναν οργανισμό.

Περίληψη

Η παρούσα πτυχιακή εργασία έχει ως αντικείμενο την ανάπτυξη ενός Συστήματος Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού. Η ανάγκη για μια τέτοια εφαρμογή προκύπτει από το γεγονός ότι πολλές εταιρείες δυσκολεύονται να ελέγξουν με αποτελεσματικό τρόπο ποιος έχει πρόσβαση σε συστήματα και ποιος διαχειρίζεται τον εξοπλισμό, ειδικά όταν οι διαδικασίες γίνονται χειροκίνητα. Στόχος του συστήματος είναι να βελτιώσει την οργάνωση, να μειώσει τα λάθη και να προσφέρει μεγαλύτερη διαφάνεια και ασφάλεια.

Η αρχιτεκτονική του βασίζεται στο μοντέλο client-server, με διαχωρισμό μεταξύ διεπαφής χρήστη, επιχειρησιακής λογικής και βάσης δεδομένων. Το frontend προσφέρει εύχρηστο περιβάλλον για HR και IT, ενώ το backend υλοποιεί τη λογική των λειτουργιών και τη σύνδεση με τη βάση δεδομένων. Η ασφάλεια αποτελεί κεντρικό άξονα, με χρήση HTTPS, ελέγχου πρόσβασης βάσει ρόλων και κατακερματισμού κωδικών πρόσβασης.

Η υλοποίηση περιλαμβάνει διεπαφές για τη διαχείριση προσωπικού και εξοπλισμού, αυτοματισμούς για ειδοποιήσεις και ελέγχους ανωμαλιών, λειτουργίες CRUD και λεπτομερή καταγραφή ενεργειών. Οι δοκιμές που πραγματοποιήθηκαν επιβεβαίωσαν τη σταθερότητα, την ασφάλεια και τη χρηστικότητα του συστήματος, με θετική αποδοχή από τους τελικούς χρήστες.

Ωστόσο, αναγνωρίστηκαν ορισμένοι περιορισμοί, όπως η έλλειψη 2FA, η χειροκίνητη εισαγωγή εξοπλισμού και οι προκαθορισμένοι ρόλοι. Για το μέλλον προτείνονται βελτιώσεις όπως ενσωμάτωση με LDAP ή Azure AD, χρήση RFID/barcode, mobile εφαρμογή και πιο εξελιγμένες αναφορές.

Συνολικά, η εργασία αποδεικνύει ότι ένα τέτοιο εργαλείο μπορεί να ενισχύσει σημαντικά την καθημερινή λειτουργία μιας επιχείρησης, προσφέροντας ασφάλεια, ευελιξία και καλύτερο έλεγχο στη διαχείριση πόρων και προσβάσεων.

«Design and Development of an Employee and Corporate Equipment Access Management System»

Damianos Aivazidis

Abstract

This thesis focuses on the development of an Employee Access and Equipment Management System. The need for such a solution arises from the fact that many companies struggle to effectively monitor who has access to systems and who manages equipment, especially when these processes are carried out manually. The goal of the system is to improve organization, reduce errors, and provide greater transparency and security.

The architecture follows a client–server model, separating the user interface, business logic, and database. The frontend provides a user-friendly environment for HR and IT teams, while the backend handles business operations and database communication. Security is a central element of the design, with the use of HTTPS, role-based access control, and password hashing.

The implementation includes dedicated interfaces for managing employees and equipment, automation for notifications and anomaly detection, CRUD operations, and detailed logging of all user actions. Testing confirmed the system’s stability, security, and usability, with positive feedback from end users.

Nevertheless, some limitations were identified, such as the lack of two-factor authentication, manual entry of equipment data, and predefined user roles. Future improvements could include integration with LDAP or Azure AD, the use of RFID/barcodes, the development of a mobile application, and more advanced reporting tools.

Overall, the thesis demonstrates that such a tool can significantly enhance a company’s daily operations by offering security, flexibility, and better control over resource and access management.

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στους γονείς και τους φίλους μου για την αμέριστη ψυχολογική στήριξη καθ' όλη τη διάρκεια της εκπόνησης αυτής της εργασίας. Ευχαριστώ θερμά τους καθηγητές μου και τη Σχολή γενικότερα για τις γνώσεις και τις ευκαιρίες που μου προσέφεραν, καθώς και τον επιβλέποντα καθηγητή μου, κ. Χαράλαμπο Μπράτσα, για την πολύτιμη καθοδήγηση και υποστήριξή του καθ' όλη τη διάρκεια της πτυχιακής μου. Ιδιαίτερες ευχαριστίες οφείλω στο εργασιακό μου περιβάλλον και στους συναδέλφους μου, οι οποίοι με στήριξαν πρακτικά, παρέχοντάς μου το περιβάλλον φιλοξενίας (server) και χρήσιμες συμβουλές για τη σωστή λειτουργία του συστήματος. Λόγω των καθηκόντων που έχω στην εταιρεία, είχα την ευκαιρία να διαπιστώσω από πρώτο χέρι την ανάγκη για ένα σύστημα όπως αυτό που ανέπτυξα στην πτυχιακή μου, το οποίο πλέον με βοηθά σημαντικά στην καθημερινή μου εργασία. Η συμβολή όλων αυτών ήταν καθοριστική για την ολοκλήρωση της εργασίας μου, και τους είμαι ευγνώμων.

Περιεχόμενα

Πρόλογος.....	v
Περίληψη.....	vi
Abstract	vii
Ευχαριστίες	viii
Περιεχόμενα	ix
Κατάλογος Σχημάτων	xii
Κατάλογος Πινάκων.....	xii
Συνομογραφίες.....	xiii
Κεφάλαιο 1ο: Εισαγωγή	1
1.1 Ιστορικό.....	1
1.2 Ανάδειξη του Προβλήματος.....	1
1.3 Στόχοι	2
1.4 Σημασία της Μελέτης.....	2
1.5 Δομή Πτυχιακής Εργασίας.....	3
Κεφάλαιο 2ο: Πεδίο εφαρμογής του συστήματος	5
2.1 Διαχείριση Εργαζομένων	5
2.2 Έλεγχος Πρόσβασης	5
2.3 Παρακολούθηση Εξοπλισμού	6
2.4 Σύστημα ειδοποιήσεων	6
2.5 Διαχείριση Αδειών Προσωπικού.....	6
2.6 Υποβολή Αναφορών	7
2.7 Καταγραφή Ελέγχου	7
2.8 Άλλα Συστήματα	8
2.9 Σύνοψη	8
Κεφάλαιο 3ο: Μεθοδολογία.....	9
3.1 Στοιβα Τεχνολογίας.....	9
3.1.1 Backend	9
3.1.2 Frontend.....	9
3.1.3 Deployment και Υποδομή	10
3.1.4 Συνολική Αρχιτεκτονική	10
3.2 Διαδικασία Σχεδιασμού.....	11
3.2.1 Προσέγγιση Σχεδιασμού με επίκεντρο τον χρήστη.....	11

3.2.2	Συγκέντρωση Απαιτήσεων	12
3.2.3	Ανάπτυξη διαγραμμάτων UML.....	13
3.2.4	Διάγραμμα Οντότητας-Σχέσης (ER)	15
3.2.5	Σχέδια καλωδίων και πρωτότυπα UI.....	15
3.2.6	Σύνοψη	16
3.3	Προσέγγιση Ανάπτυξης.....	16
3.3.1	Επαναληπτική Ανάπτυξη Βασισμένη σε Ευέλικτο Σύστημα	16
3.3.2	Δομή και τεκμηρίωση αρθρωτής κωδικοποίησης	17
3.4	Μεθοδολογία Δοκιμών	17
3.4.1	Δοκιμή μονάδας.....	17
3.4.2	Δοκιμή ολοκλήρωσης.....	17
3.4.3	Δοκιμές ασφαλείας	17
3.5	Σύνοψη	18
Κεφάλαιο 4ο:	Αρχιτεκτονική Συστήματος	19
4.1	Τι είναι η Αρχιτεκτονική Χρήστη-Διακομιστή;.....	19
4.2	Επίπεδο Backend και Βάσης Δεδομένων	19
4.2.1	Λειτουργικότητες του backend.....	20
4.2.2	Βάση Δεδομένων	20
4.2.3	Απόδοση και κλιμάκωση	20
4.3	Μηχανισμοί ασφαλείας	20
4.3.1	Δικτυακή ασφάλεια	21
4.3.2	Έλεγχος ταυτότητας και πρόσβασης	21
4.3.3	Προστασία κωδικών και δεδομένων	21
4.3.4	Audit και λογοδοσία	21
4.4	Σύνοψη	22
Κεφάλαιο 5ο:	Υλοποίηση	23
5.1	Διεπαφές χρήστη για διαχειριστές ανθρώπινου δυναμικού και πληροφορικής	24
5.2	Λογική αυτοματισμού για ειδοποιήσεις και ανίχνευση ανωμαλιών	24
5.3	Λειτουργίες CRUD για Χρήστες, Συστήματα και Εξοπλισμό	25
5.4	Ασφαλής καταγραφή ιχνών ελέγχου	27
Κεφάλαιο 6ο:	Δοκιμές και Αξιολόγηση	29
6.1	Στόχοι Δοκιμών	29
6.2	Μεθοδολογία Δοκιμών	29
6.3	Λειτουργικές δοκιμές	29
6.4	Δοκιμές απόδοσης και φορτίου	30

6.5	Δοκιμές ασφαλείας.....	30
6.6	Αξιολόγηση Χρηστικότητας	31
6.7	Αποτελέσματα Αξιολόγησης.....	31
6.8	Σύνοψη	31
Κεφάλαιο 7ο: Παρουσίαση Εφαρμογής.....		33
7.1	Είσοδος στο σύστημα.....	33
7.2	Οργάνωση Επιχείρησης.....	34
7.3	Παραμετροποίηση Assets.....	38
7.4	Διαδικασία απόδοσης εξοπλισμού	40
7.4.1	Μέσω των members	40
7.4.2	Μέσω των items	41
7.5	Παρακολούθηση και Διαχείριση rentals	41
7.5.1	Συνολικά rentals	42
7.5.2	Rentals ανά member	42
7.5.3	Ιστορικό rentals ανά item	43
7.6	Σύνοψη	43
Κεφάλαιο 8ο: Περιορισμοί		45
8.1	Έλλειψη άμεσης ενσωμάτωσης αποθέματος υλικού.....	45
8.2	Απουσία Διπαραγοντικής Ταυτοποίησης (2FA)	46
8.3	Ανάληψη Ομοιόμορφων Ορισμών Ρόλων σε Όλα τα Τμήματα	46
8.4	Περιορισμένη Προσαρμογή Αναφορών.....	47
8.5	Σύνοψη	48
Κεφάλαιο 9ο: Μελλοντικές βελτιώσεις		49
Κεφάλαιο 10ο: Συμπέρασμα.....		51
ΒΙΒΛΙΟΓΡΑΦΙΑ.....		53

Κατάλογος Σχημάτων

Σχήμα 3.1 Αρχιτεκτονική Συστήματος	11
Σχήμα 3.2 Διάγραμμα περίπτωσης χρήσης του Συστήματος Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού	12
Σχήμα 3.3 Διάγραμμα κλάσης UML για το Σύστημα Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού	13
Σχήμα 3.4 Διάγραμμα δραστηριότητας για τη ροή εργασίας ένταξης υπαλλήλων	14
Σχήμα 3.5 Διάγραμμα Οντότητας-Σχέσης (ER) του Σχήματος Βάσης Δεδομένων Συστήματος	15
Σχήμα 5.1 Γενική ροή εργασίας του Συστήματος Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού	23
Σχήμα 5.2 Διάγραμμα ροής για συμβάντα αυτοματισμού	25
Σχήμα 7.1 Login συστήματος.....	33
Σχήμα 7.2 Μενού πλοήγησης.....	34
Σχήμα 7.3 Δημιουργία Department.....	35
Σχήμα 7.4 Departments view	35
Σχήμα 7.5 Προσθήκη member	36
Σχήμα 7.6 Προσθήκη member σε department.....	37
Σχήμα 7.7 Λίστα προσωπικού (members).....	38
Σχήμα 7.8 Asset groups.....	38
Σχήμα 7.9 Items - Εξοπλισμός & Συστήματα	39
Σχήμα 7.10 Items - Φιλτράρισμα	39
Σχήμα 7.11 Απόδοση εξοπλισμού σε άτομο	40
Σχήμα 7.12 Απόδοση εξοπλισμού σε άτομο – 2	41
Σχήμα 7.13 Λίστα ενεργών rentals.....	42
Σχήμα 7.14 Ιστορικό rentals ανά member.....	43
Σχήμα 7.15 Ιστορικό rentals ανά item.....	43

Κατάλογος Πινάκων

Πίνακας 5.1 Πίνακας CRUD με οντότητες και λειτουργίες.....	26
--	----

Συντομογραφίες

ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
Π.Ε.	Πτυχιακή Εργασία
2FA	Two-Factor Authentication (Διπλή/Διπαραγοντική Ταυτοποίηση)
AD	Active Directory (Υπηρεσία Καταλόγου)
API	Application Programming Interface (Διεπαφή Προγραμματισμού Εφαρμογών)
CISA	Cybersecurity and Infrastructure Security Agency (Υπηρεσία Κυβερνοασφάλειας και Ασφάλειας Υποδομών)
CRUD	Create, Read, Update, Delete (Δημιουργία, Ανάγνωση, Ενημέρωση, Διαγραφή)
CSRF Ιστότοπου)	Cross-Site Request Forgery (Πλαστογράφηση Αιτημάτων Διασταυρούμενου Ιστότοπου)
CSV	Comma-Separated Values (Τιμές Διαχωρισμένες με Κόμμα)
ERP	Enterprise Resource Planning (Σχεδιασμός Επιχειρησιακών Πόρων)
ER	Entity-Relationship (Διάγραμμα Οντοτήτων-Συσχετίσεων)
GDPR	General Data Protection Regulation (Γενικός Κανονισμός Προστασίας Δεδομένων)
HIPAA Ιατρικών Δεδομένων, ΗΠΑ)	Health Insurance Portability and Accountability Act (Νομοθεσία για την Ασφάλεια Ιατρικών Δεδομένων, ΗΠΑ)
HR	Human Resources (Ανθρώπινοι Πόροι)
HRIS Δυναμικού)	Human Resource Information System (Σύστημα Πληροφόρησης Ανθρώπινου Δυναμικού)
HTTPS Υπερκειμένου)	Hypertext Transfer Protocol Secure (Πρωτόκολλο Ασφαλούς Μεταφοράς Υπερκειμένου)
IAM	Identity and Access Management (Διαχείριση Ταυτότητας και Πρόσβασης)
IA	Information Architecture (Πληροφοριακή Αρχιτεκτονική)
ISO/IEC 27001	Διεθνές Πρότυπο Διαχείρισης Ασφάλειας Πληροφοριών
IT	Information Technology (Πληροφορική)
ITSM	IT Service Management (Διαχείριση Υπηρεσιών Πληροφορικής)
LDAP Καταλόγου)	Lightweight Directory Access Protocol (Ελαφρύ Πρωτόκολλο Πρόσβασης Καταλόγου)
MDM	Mobile Device Management (Διαχείριση Κινητών Συσκευών)
NIS2 και Πληροφοριών 2, Ευρωπαϊκή Ένωση)	Network and Information Security Directive 2 (Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών 2, Ευρωπαϊκή Ένωση)
OWASP Ιστού)	Open Web Application Security Project (Ανοικτό Έργο Ασφάλειας Εφαρμογών Ιστού)
PDF	Portable Document Format (Φορητή Μορφή Εγγράφου)

RBAC	Role-Based Access Control (Έλεγχος Πρόσβασης Βάσει Ρόλων)
REST	Representational State Transfer (Μεταφορά Αναπαράστασης Κατάστασης)
RFID	Radio Frequency Identification (Αναγνώριση μέσω Ραδιοσυχνοτήτων)
SIEM	Security Information and Event Management (Διαχείριση Πληροφοριών και Συμβάντων Ασφαλείας)
SMTP	Simple Mail Transfer Protocol (Απλό Πρωτόκολλο Μεταφοράς Αλληλογραφίας)
SQL	Structured Query Language (Δομημένη Γλώσσα Ερωτημάτων)
SSO	Single Sign-On (Ενιαία Σύνδεση)
UAT	User Acceptance Testing (Δοκιμή Αποδοχής Χρηστών)
UI	User Interface (Διεπαφή Χρήστη)
UML	Unified Modeling Language (Ενοποιημένη Γλώσσα Μοντελοποίησης)
VPN	Virtual Private Network (Εικονικό Ιδιωτικό Δίκτυο)
XSS	Cross-Site Scripting (Εισαγωγή Κακόβουλου Κώδικα στον Ιστότοπο)
ZAP	Zed Attack Proxy (Εργαλείο Ελέγχου Ασφάλειας)

Κεφάλαιο 1ο: Εισαγωγή

1.1 Ιστορικό

Σήμερα, οι οργανισμοί, προκειμένου να διασφαλίσουν την ομαλή εκτέλεση των βασικών επιχειρησιακών διαδικασιών τους, χρησιμοποιούν μια σειρά από συστήματα πληροφορικής. Σε αυτά περιλαμβάνονται εργαλεία όπως τα VPN για ασφαλή σύνδεση, τα ERP για τον προγραμματισμό πόρων και διάφορες εφαρμογές λογισμικού που υποστηρίζουν την καθημερινή λειτουργία. Δεδομένου ότι η κυβερνοασφάλεια αποτελεί πλέον κρίσιμο ζήτημα σε διεθνές επίπεδο — με πιο πρόσφατο παράδειγμα την Οδηγία NIS2 της Ευρωπαϊκής Ένωσης που επιβάλλει αυστηρότερους κανόνες ασφάλειας και διαχείρισης κινδύνων, αλλά και αντίστοιχες πρωτοβουλίες όπως η CISA (Cybersecurity and Infrastructure Security Agency) στις Ηνωμένες Πολιτείες [1] — οι διαχειριστές συστημάτων πρέπει να δίνουν ιδιαίτερη προσοχή στα δικαιώματα πρόσβασης των χρηστών, καθώς οι διαδικτυακές απειλές εντείνονται και το θεσμικό πλαίσιο γίνεται ολοένα πιο απαιτητικό. Ταυτόχρονα, οι εταιρείες παρέχουν στους εργαζομένους φορητούς υπολογιστές, smartphones και άλλα χρήσιμα εργαλεία για καλύτερη εργασία. Παρόλο που υπάρχουν πρότυπα όπως το ISO/IEC 27001 που ορίζουν διαδικασίες για την παρακολούθηση της πρόσβασης και τη διαχείριση περιουσιακών στοιχείων, στην πράξη πολλοί οργανισμοί δεν εφαρμόζουν καθολικά αυτές τις πρακτικές. Ως αποτέλεσμα, υπάρχει κίνδυνος να προκύψουν επιθέσεις ή παραβιάσεις κανόνων λόγω κενών στον έλεγχο [2][3].

Στα πρώτα στάδια, πολλές εταιρείες διαχειρίζονταν την ένταξη και την αποχώρηση εργαζομένων μέσω email και υπολογιστικών φύλλων, μια πρακτική που δεν εξασφάλιζε πάντα την προστασία των λογαριασμών και του εταιρικού εξοπλισμού. Σύμφωνα με το Υπουργείο Άμυνας των ΗΠΑ [4], περισσότερες από τις μισές απειλές από εσωτερικούς παράγοντες προκύπτουν επειδή τα δικαιώματα πρόσβασης σε ευαίσθητα δεδομένα δεν ανακαλούνται άμεσα. Αυτή η κατάσταση οδηγεί επίσης σε υψηλότερο κόστος και περισσότερα λάθη στους ελέγχους όταν τα περιουσιακά στοιχεία δεν παρακολουθούνται σωστά, όπως περιγράφεται λεπτομερώς στους Roberts και Ekstrom [5] και υποστηρίζεται από τα Real Time Networks [6].

Επομένως, χρειαζόμαστε μια λύση που να προστατεύει ταυτόχρονα τόσο τα ψηφιακά όσο και τα φυσικά μας περιουσιακά στοιχεία. Ένα καλό σύστημα είναι εξοπλισμένο για καθημερινές εργασίες, επιτρέπει διαφορετικές λειτουργίες ανά ρόλο, παρέχει ουσιαστικές αναφορές και καταγράφει κάθε δραστηριότητα για ελέγχους συμμόρφωσης [7].

1.2 Ανάδειξη του Προβλήματος

Επειδή οι εταιρείες συνήθως χρησιμοποιούν διαφορετικά συστήματα για την IAM (Identity and Access Management) και την παρακολούθηση περιουσιακών στοιχείων, τα δεδομένα τους χωρίζονται σε πολλά συστήματα. Δεδομένου ότι είναι σημαντικό να ενσωματώνονται, να παρέχονται και να διαχειρίζονται οι λογαριασμοί των εργαζομένων τόσο στην αρχή όσο και στο τέλος της εργασίας τους, τα λάθη είναι συνηθισμένα για τις ομάδες HR και IT που εκτελούν τις ίδιες εργασίες επανειλημμένα [8]. Ο μεγαλύτερος χρόνος ενσωμάτωσης, η πρόσβαση περισσότερων μη εξουσιοδοτημένων χρηστών και οι καθυστερήσεις στην απόκτηση επαγγελματικών συσκευών είναι όλα αποτέλεσμα αναποτελεσματικότητας και αυτά τα προβλήματα μπορούν να διαρκέσουν πολύ και να προσθέσουν επιπλέον κόστος [9].

Όταν οι οργανισμοί επεκτείνονται ή επιλέγουν απομακρυσμένη ή υβριδική εργασία, η εκτεταμένη διαχείριση των καταγραφών με το χέρι καθίσταται σχεδόν αδύνατη. Δεδομένου ότι η παροχή χρηστών

απαιτεί ενορχήστρωση, τα χρονικά πλαίσια για τη δημιουργία πολλαπλών συστημάτων για νέους χρήστες μπορεί να είναι ημέρες ή εβδομάδες, γεγονός που επηρεάζει την παραγωγικότητά τους και επίσης ενέχει τον κίνδυνο να μείνουν ανενεργοί ευαίσθητοι λογαριασμοί [10]. Όσον αφορά τα περιουσιακά στοιχεία, επειδή τα αποκεντρωμένα υπολογιστικά φύλλα δεν είναι συγχρονισμένα, ο εξοπλισμός μπορεί να καταγραφεί δύο φορές ή να χαθεί, γεγονός που μειώνει την ακρίβεια των ελέγχων απογραφής και τον έλεγχο των κεφαλαιουχικών δαπανών [3].

Η ύπαρξη ξεχωριστών πλατφορμών μειώνει την κυβερνοασφάλεια, καθώς τα δικαιώματα πρόσβασης δεν επιβλέπονται και καθιστά τις λειτουργίες πιο ακριβές επειδή τα περιουσιακά στοιχεία δεν διαχειρίζονται μαζί. Η ύπαρξη τόσο του IAM όσο και της διαχείρισης περιουσιακών στοιχείων σε ένα ενιαίο σύστημα διευκολύνει τη συμμόρφωση με κανόνες όπως το ISO/IEC 27001, καθώς επιβάλλει την προσεκτική παρακολούθηση της πρόσβασης και του αποθέματος. Έτσι, η εξομάλυνση αυτού του κενού είναι απαραίτητη όχι μόνο για λόγους ευκολίας, αλλά και επειδή υποστηρίζει την ισχυρή διακυβέρνηση, τη διαχείριση κινδύνων και τη συμμόρφωση.

1.3 Στόχοι

Στόχος της παρούσας πτυχιακής εργασίας είναι η δημιουργία και η εφαρμογή ενός διαδικτυακού συστήματος που συνδυάζει τη διαχείριση της πρόσβασης των εργαζομένων με την παρακολούθηση όλου του εταιρικού εξοπλισμού. Οι κύριοι στόχοι του συστήματος είναι οι εξής:

1. Να διασφαλίζεται ότι, όταν ένας εργαζόμενος εντάσσεται ή αποχωρεί, εφαρμόζονται αυτόματα διαδικασίες που ενημερώνουν το τμήμα IT για την ανάθεση ή την αφαίρεση ρόλων πρόσβασης σε VPN, ERP και άλλα εταιρικά συστήματα [1][11].
2. Να υποστηρίζεται η παρακολούθηση περιουσιακών στοιχείων, δίνοντας στους χρήστες τη δυνατότητα να αντιστοιχίζουν, να επιστρέφουν και να διαχειρίζονται εταιρικό εξοπλισμό — όπως φορητούς υπολογιστές και κινητά τηλέφωνα— ενώ παράλληλα ενημερώνονται τα αρχεία αποθεμάτων σε πραγματικό χρόνο [2][6].
3. Να καταγράφεται κάθε ενέργεια που αφορά χρήστες και περιουσιακά στοιχεία, ώστε να καλύπτονται οι ανάγκες συμμόρφωσης και να υποστηρίζονται οι έρευνες, διασφαλίζοντας έτσι διαφάνεια και λογοδοσία [12][13].
4. Να παρέχεται ένα ευέλικτο front-end, το οποίο διευκολύνει τους διευθυντές HR, IT και τμημάτων να εξοικειωθούν με το λογισμικό χωρίς να απαιτείται εκτεταμένη εκπαίδευση [14].
5. Να υποστηρίζεται η αποστολή ειδοποιήσεων μέσω email προς τις ομάδες IT και η δημιουργία προσαρμοσμένων αναφορών, ώστε τα ενδιαφερόμενα μέρη να ενημερώνονται εγκαίρως για αναμενόμενες εργασίες, εξερχόμενο εξοπλισμό και ασυνήθιστες προσπάθειες πρόσβασης [7][9].

Όταν επιτευχθούν αυτοί οι στόχοι, το σύστημα θα διευκολύνει το έργο των ομάδων HR, IT και των προϊσταμένων τμημάτων, θα μειώσει τον χρόνο ένταξης και αποχώρησης προσωπικού, θα βελτιώσει τα μέτρα ασφαλείας και θα διασφαλίσει ότι όλα τα περιουσιακά στοιχεία καταγράφονται και ελέγχονται με συνέπεια.

1.4 Σημασία της Μελέτης

Η πλατφόρμα θα ενδιέφερε σε μεγάλο βαθμό τόσο τις μεγάλες εταιρείες όσο και τις μικρότερες επιχειρήσεις. Η αναστολή των λογαριασμών χρηστών σε πραγματικό χρόνο μειώνει τον κίνδυνο ύπαρξης ενεργών δικαιωμάτων σε υποσυστήματα που δεν έχουν αφαιρεθεί εγκαίρως, κάτι που αποτελεί γνωστή απειλή για την ασφάλεια εμπιστευτικών πληροφοριών (όπως υποστηρίζεται από το Υπουργείο Άμυνας των ΗΠΑ [4] και την Tenna [3]). Επίσης, η αυτοματοποίηση της παρακολούθησης των περιουσιακών στοιχείων βοηθά τις εταιρείες να ανακτήσουν τον χαμένο εξοπλισμό και να ελέγξουν τους κύκλους αγοράς αποθεμάτων τους, γεγονός που μειώνει το κόστος αντικατάστασης [5][15]. Η

ύπαρξη τόσο του IAM όσο και της διαχείρισης περιουσιακών στοιχείων σε ένα μέρος διευκολύνει τη συμμόρφωση με κανόνες όπως το ISO/IEC 27001, καθώς επιβάλλει την προσεκτική παρακολούθηση της πρόσβασης και του αποθέματος [1][13].

Εκτός από το ότι κάνει πιο εύκολες διαδικασίες όπως η πρόσληψη, η αποχώρηση ή η διαχείριση εξοπλισμού, η πλατφόρμα βοηθά και τα τμήματα της εταιρείας να συνεργάζονται πιο ομαλά μεταξύ τους. Το τμήμα HR μπορεί να παρακολουθεί τον φόρτο εργασίας εντός του τμήματος IT, γεγονός που τους βοηθά να οργανώνουν το εργατικό δυναμικό με μεγαλύτερη ακρίβεια. Υπάρχουν λιγότερα αιτήματα και σαφέστεροι τρόποι για τους διαχειριστές IT να επιλύουν προβλήματα, επειδή όλες οι πληροφορίες για πρόσβαση και εξοπλισμό συγκεντρώνονται σε ένα κεντρικό σημείο αντί να είναι διασκορπισμένες σε υπολογιστικά φύλλα ή διαφορετικά συστήματα. Οι διευθυντές των τμημάτων μπορούν να επιβεβαιώσουν ότι οι εργαζόμενοι διαθέτουν τα απαραίτητα δικαιώματα και τους απαραίτητους πόρους πριν από τις ημερομηνίες των σημαντικών έργων. Με αυτές τις βελτιώσεις, οι νέοι εργαζόμενοι ξεκινούν τη δουλειά τους πιο γρήγορα, τα προβλήματα ασφαλείας γίνονται λιγότερα και οι υπάλληλοι μπορούν να παίρνουν πιο σωστές αποφάσεις στην καθημερινή τους εργασία.

1.5 Δομή Πτυχιακής Εργασίας

Η πτυχιακή εργασία αποτελείται συνολικά από δέκα κεφάλαια, τα οποία ακολουθούν μια λογική ακολουθία ώστε να παρουσιαστεί τόσο το θεωρητικό υπόβαθρο όσο και η υλοποίηση του συστήματος. Στο πρώτο κεφάλαιο γίνεται η εισαγωγή, όπου παρουσιάζεται το αντικείμενο της εργασίας, οι στόχοι της και η μεθοδολογία που ακολουθήθηκε. Στο δεύτερο κεφάλαιο αναλύεται το θεωρητικό υπόβαθρο, με αναφορές σε βασικές έννοιες γύρω από τη διαχείριση προσβάσεων, τα πληροφοριακά συστήματα και τις σχετικές τεχνολογίες. Το τρίτο κεφάλαιο επικεντρώνεται στις τεχνολογίες και τα εργαλεία που χρησιμοποιήθηκαν, τόσο στο κομμάτι του frontend όσο και στο backend.

Στο τέταρτο κεφάλαιο περιγράφεται αναλυτικά η αρχιτεκτονική του συστήματος, τα επίπεδα λειτουργίας του και οι μηχανισμοί ασφαλείας που ενσωματώθηκαν. Στη συνέχεια, το πέμπτο κεφάλαιο παρουσιάζει την υλοποίηση, όπου οι προδιαγραφές σχεδιασμού μετατρέπονται σε λειτουργική εφαρμογή. Το έκτο κεφάλαιο αφορά τις δοκιμές και την αξιολόγηση, περιγράφοντας τη μεθοδολογία ελέγχου, τα σενάρια δοκιμών και τα αποτελέσματα.

Στο έβδομο κεφάλαιο δίνεται μια αναλυτική παρουσίαση της εφαρμογής μέσα από πρακτικά παραδείγματα και screenshots, ώστε να καταδειχθεί η λειτουργικότητα του συστήματος. Το όγδοο κεφάλαιο ασχολείται με τους περιορισμούς της παρούσας έκδοσης, ενώ το ένατο αναφέρεται σε μελλοντικές βελτιώσεις που μπορούν να ενισχύσουν τη λειτουργικότητα και την ασφάλεια της πλατφόρμας. Τέλος, το δέκατο κεφάλαιο συνοψίζει τα συμπεράσματα της εργασίας, καταγράφοντας τις βασικές συμβολές και την αξία του συστήματος για έναν σύγχρονο οργανισμό.

Με αυτόν τον τρόπο, η εργασία ακολουθεί μια ολοκληρωμένη πορεία, ξεκινώντας από το θεωρητικό πλαίσιο, συνεχίζοντας με τον σχεδιασμό και την υλοποίηση, και καταλήγοντας στην αξιολόγηση, τις μελλοντικές προοπτικές και τα τελικά συμπεράσματα.

Κεφάλαιο 2ο: Πεδίο εφαρμογής του συστήματος

Όταν ένας οργανισμός μεγαλώνει και η δομή του γίνεται πιο περίπλοκη, γίνεται πιο δύσκολο να διαχειριστεί τι μπορούν να κάνουν οι εργαζόμενοι και σε τι τους δίνεται πρόσβαση. Το κεφάλαιο αυτό εξηγεί τι θα περιλαμβάνει το σύστημα και τις κύριες λειτουργικές του μονάδες. Καθιστώντας το αρθρωτό, επεκτάσιμο και κλιμακωτό, το σύστημα ασχολείται με ζητήματα όπως η ασφάλεια και η ευθύνη των λειτουργιών. Η χρήση μιας ενοποιημένης πλατφόρμας για τα αρχεία των εργαζομένων, τον έλεγχο των ταυτοτήτων και την παρακολούθηση των φυσικών περιουσιακών στοιχείων βοηθά έναν οργανισμό να διατηρεί ορθή παρακολούθηση και να είναι έτοιμος να συμμορφωθεί με τους κανόνες [1][12].

2.1 Διαχείριση Εργαζομένων

Στην καρδιά της πλατφόρμας βρίσκεται μια ισχυρή διαδικασία διαχείρισης εργαζομένων, η οποία είναι το πρώτο σημείο από το οποίο οι χρήστες ξεκινούν την εργασία τους. Με αυτήν τη λειτουργία, τα άτομα που είναι εξουσιοδοτημένα να χρησιμοποιούν το σύστημα μπορούν να προσθέσουν νέο προσωπικό, συλλέγοντας το πλήρες όνομά τους, το τμήμα, τη θέση, τον τύπο απασχόλησης και την ημερομηνία έναρξης [14]. Επιπλέον, εκχωρεί αριθμούς εργαζομένων μοναδικούς σε κάθε άτομο για να συνδέσει την πρόσβαση και την κατανομή ιδιοκτησίας του.

Οι προκαθορισμένες φόρμες και τα μενού βοηθούν στη μείωση του χρόνου που απαιτείται κατά την ενσωμάτωση, καθώς και της πιθανότητας σφαλμάτων [11]. Αυτή η ενότητα μπορεί να χρησιμοποιηθεί για την πραγματοποίηση αλλαγών προφίλ σε περίπτωση αλλαγών στο τμήμα ή σε περίπτωση προαγωγής. Καθώς οι έλεγχοι και η πρόσβαση θα αντικατοπτρίζουν πάντα τις πιο πρόσφατες πληροφορίες, μπορεί να επιβεβαιωθεί η κατάσταση κάθε υπαλλήλου στο σύστημα.

Ως αποτέλεσμα, η βάση δεδομένων του συστήματος έχει ρυθμιστεί με σχεσιακό τρόπο, έτσι ώστε κάθε αρχείο υπαλλήλου να συνδέεται με συνέπεια με τις πληροφορίες στους πίνακες πρόσβασης και εξοπλισμού [16]. Όταν τα δεδομένα είναι οργανωμένα σε δομή, οι χρήστες μπορούν να τα αναζητήσουν εύκολα και να παράγουν αναφορές γρήγορα, κάτι που είναι απαραίτητο τόσο για τα τμήματα Ανθρώπινου Δυναμικού όσο και για τα τμήματα συμμόρφωσης.

2.2 Έλεγχος Πρόσβασης

Η διατήρηση της πρόσβασης σε δεδομένα και συστήματα είναι πολύ σημαντική για την ασφάλεια των επιχειρήσεων. Ο έλεγχος πρόσβασης βάσει ρόλων (RBAC) αποτελεί μέρος του συστήματος, διασφαλίζοντας ότι τα μέλη της ομάδας ανάπτυξης, το προσωπικό οικονομικών και το προσωπικό του τμήματος ανθρώπινου δυναμικού έχουν διαφορετικά δικαιώματα, ανάλογα με τις ανάγκες [7]. Ο τρόπος με τον οποίο έχει σχεδιαστεί σημαίνει ότι τα δικαιώματα εκδίδονται γρήγορα και με ασφάλεια.

Όλοι οι τύποι πρόσβασης σε συστήματα (VPN και ERP, CRM και διακομιστές αρχείων) ορίζονται για κάθε εργαζόμενο, μαζί με τον βαθμό ή τη διάρκεια της εξουσιοδότησής του [4]. Κάθε φορά που κάποιος αποχωρεί από την εταιρεία ή αλλάζει ρόλους, το σύστημα ενημερώνει αυτόματα τα δικαιώματά του, αποτρέποντας την απειλή αδρανών «λογαριασμών ζόμπι» που μπορούν να χρησιμοποιηθούν σε κυβερνοεπιθέσεις [9].

Μια ροή εργασίας έγκρισης είναι ένα σημαντικό μέρος της μονάδας ελέγχου πρόσβασης. Όταν κάποιος ζητά πρόσβαση, το σύστημα δρομολογεί το αίτημα στον επικεφαλής του τμήματος ή στον διαχειριστή IT, ο οποίος πρέπει να εξετάσει και να επιβεβαιώσει το αίτημα πριν από την έγκρισή του [12].

Διασφαλίζει ότι τα άτομα μπορούν να θεωρηθούν υπεύθυνα και η κλιμάκωση προνομίων πραγματοποιείται μόνο όταν επιτρέπεται.

2.3 Παρακολούθηση Εξοπλισμού

Εκτός από τα ψηφιακά δικαιώματα, οι περισσότεροι εργαζόμενοι χρησιμοποιούν αντικείμενα όπως φορητούς υπολογιστές, κινητά τηλέφωνα, θόνες, μονάδες USB και εξωτερικές συσκευές αποθήκευσης. Αυτή η ενότητα στο σύστημα καταγράφει κάθε διανομή, επιστροφή και τρέχουσα κατάσταση κάθε αντικειμένου [2][5]. Κάθε αντικείμενο αναγνωρίζεται με μια μοναδική ετικέτα (είτε σειριακό αριθμό είτε ετικέτα περιουσιακού στοιχείου) και τα αρχεία για τον τρόπο με τον οποίο αντιστοιχίστηκε κάθε αντικείμενο διατηρούνται για έλεγχο κατά τη διάρκεια των ελέγχων.

Όλα τα εργαλεία παρακολουθούνται από την εκχώρηση έως την επιστροφή τους, ώστε να αποτραπεί η πιθανότητα απώλειας ή κακής χρήσης τους. Δεδομένου ότι η κατάσταση διαθεσιμότητας είναι σε πραγματικό χρόνο, οι ομάδες IT μπορούν να σχεδιάσουν καλά την προμήθεια υλικού και να παρακολουθούν ποιοι διακομιστές χρησιμοποιούνται [6]. Σε περίπτωση που κάποιος απομακρυνθεί από την εταιρεία, το σύστημα εμφανίζει μια λίστα εργασιών για να επιβεβαιώσει ότι όλα τα εργαλεία εργασίας έχουν επιστραφεί πριν κλείσει ο λογαριασμός του.

Εναλλακτικά, όταν εισαχθεί η τεχνολογία barcode ή RFID (σε μεταγενέστερα στάδια), η παρακολούθηση περιουσιακών στοιχείων για check-in και check-out μπορεί να γίνει πιο αυτοματοποιημένη, μειώνοντας τόσο την προσπάθεια όσο και τον κίνδυνο απώλειας πραγμάτων [3].

2.4 Σύστημα ειδοποιήσεων

Η χρήση αυτοματοποιημένων συστημάτων βοηθά στη μείωση του φόρτου εργασίας που απαιτείται στη διοίκηση. Ειδοποιήσεις σε πραγματικό χρόνο αποστέλλονται μέσω email ή εφαρμογών ανταλλαγής μηνυμάτων όταν συμβαίνει κάτι σημαντικό, όπως νέες εγγραφές προσωπικού, αιτήματα πρόσβασης που εξακολουθούν να είναι ανοιχτά και υπενθυμίσεις για την επιστροφή εξοπλισμού [8]. Με αυτές τις ειδοποιήσεις, οι αρμόδιοι διαχειριστές ενημερώνονται αμέσως για συμβάντα που απαιτούν την ενέργειά τους.

Οι διαχειριστές μπορούν να δημιουργήσουν τα δικά τους πρότυπα και χρονοδιαγράμματα ειδοποιήσεων για να υπενθυμίζουν σε όλους διάφορες ενημερώσεις, για παράδειγμα, αδειών χρήσης ή περιουσιακών στοιχείων. Με την προληπτική επικοινωνία, οι άνθρωποι μπορούν να αποφύγουν να ξεχνούν σημαντικές λεπτομέρειες και να συνεργάζονται πιο αποτελεσματικά [10].

Το σύστημα περιλαμβάνει ένα αρχείο καταγραφής όλων των ειδοποιήσεων, με χρονική σήμανση, το οποίο μπορεί να ελεγχθεί στο μέλλον από όσους διερευνούν περιστατικά ή από ομάδες αξιολόγησης [1].

2.5 Διαχείριση Αδειών Προσωπικού

Η σωστή διαχείριση αδειών αποτελεί κρίσιμο κομμάτι για την εύρυθμη λειτουργία ενός οργανισμού, καθώς επηρεάζει άμεσα τον προγραμματισμό εργασιών και τη διαθεσιμότητα προσωπικού. Η πλατφόρμα παρέχει ειδική λειτουργία καταχώρησης και έγκρισης αδειών, η οποία απεικονίζεται σε μορφή ημερολογίου (calendar view), ώστε να είναι κατανοητή και εύκολη στη χρήση από όλους τους εμπλεκόμενους [17].

Οι εργαζόμενοι μπορούν να υποβάλουν αιτήματα για ημέρες απουσίας, επιλέγοντας τα επιθυμητά διαστήματα μέσα από το ημερολόγιο. Τα αιτήματα αυτά αποστέλλονται αυτόματα στον προϊστάμενο

του τμήματος, ο οποίος είναι υπεύθυνος για την έγκριση ή απόρριψή τους. Με τον τρόπο αυτό, η διαδικασία γίνεται τυποποιημένη και διαφανής, ενώ μειώνεται ο κίνδυνος παραλείψεων ή λαθών [11].

Παράλληλα, η απεικόνιση σε ημερολογιακή μορφή δίνει στους διαχειριστές μια συνολική εικόνα των αδειών και της παρουσίας του προσωπικού, διευκολύνοντας τον σχεδιασμό βαρδιών και την κάλυψη αναγκών σε ανθρώπινο δυναμικό. Επιπλέον, όλες οι εγκρίσεις ή απορρίψεις αποθηκεύονται στο ιστορικό ενεργειών, γεγονός που ενισχύει τη λογοδοσία και τη συμμόρφωση με τις εσωτερικές πολιτικές [8].

Η ενότητα αυτή ενισχύει τον κεντρικό στόχο του συστήματος, που είναι η πλήρης εποπτεία και ο έλεγχος όλων των διαδικασιών που σχετίζονται με το προσωπικό.

2.6 Υποβολή Αναφορών

Το σύστημα συνοδεύεται από μια λεπτομερή ενότητα αναφοράς τόσο για τους διαχειριστές όσο και για τους ελεγκτές, ώστε να βλέπουν πώς χρησιμοποιείται το σύστημα και πώς κατανέμονται οι πόροι του. Το φιλτράρισμα των αναφορών ανά υπάλληλο, τμήμα, τον τρόπο παροχής πρόσβασης ή ανά εξοπλισμό διευκολύνει την υποστήριξη τόσο των ελέγχων λειτουργίας όσο και των ελέγχων συμμόρφωσης [15].

Μια αναφορά καλύπτει μια ποικιλία παραδειγμάτων.

- Αναζητήστε εγγραφές ελέγχου για αλλαγές δικαιωμάτων ανά χρήστη με την πάροδο του χρόνου.
- Λίστα εξοπλισμού που έχει διατεθεί ανά τμήμα.
- Η προβολή συμμόρφωσης κατά την ενσωμάτωση θα πρέπει να υποδεικνύει εάν ο εξοπλισμός έχει επιστραφεί ή εάν εξακολουθεί να περιμένει να επιστραφεί.
- Αναφορές γήρανσης που απαριθμούν εξοπλισμό που σύντομα θα πρέπει να επισκευαστεί ή να αντικατασταθεί.

Το εργαλείο αναφοράς επιτρέπει στους χρήστες να κατεβάζουν τα δεδομένα τους ως αρχεία CSV ή PDF για χρήση σε άλλα προγράμματα ή συστήματα ERP [18]. Οι αυτόματες αναφορές μπορούν να οργανωθούν και να αποσταλούν μέσω email στους προβλεπόμενους χρήστες σε συγκεκριμένα χρονικά διαστήματα, διατηρώντας τη διοίκηση ενημερωμένη.

2.7 Καταγραφή Ελέγχου

Όλες οι δραστηριότητες που πραγματοποιούνται χρησιμοποιώντας το σύστημα, όπως η δημιουργία υπαλλήλων, η αλλαγή πρόσβασης, η έκδοση περιουσιακών στοιχείων ή η δημιουργία αναφορών, σφραγίζονται αυτόματα με την τρέχουσα ημερομηνία και το αναγνωριστικό χρήστη. Η διαδρομή ελέγχου διευκολύνει τη συμμόρφωση με τους κανονισμούς ISO 27001, HIPAA και GDPR και είναι χρήσιμη για εγκληματολογική ανάλυση [1].

Λόγω της καταγραφής, οι χρήστες δεν μπορούν να αρνηθούν τίποτα από όσα έκαναν στο σύστημα. Κάθε καταχώρηση καταγράφει τι συνέβη, τι εμπλέκεται (για παράδειγμα, αναγνωριστικό χρήστη, αναγνωριστικό συσκευής) και ποιος ήταν υπεύθυνος [9]. Η διεπαφή του συστήματος σας επιτρέπει να ελέγξετε αυτά τα αρχεία καταγραφής ή μπορείτε να τα εξαγάγετε για να τα ελέγξετε με εργαλεία ελέγχου τρίτων.

Όταν συμβαίνουν περιστατικά ασφαλείας, τα αρχεία καταγραφής ελέγχου είναι πολύ χρήσιμα για την ανακάλυψη λεπτομερειών όπως οι μέθοδοι παραβίασης, οι επηρεαζόμενοι λογαριασμοί και τα συστήματα που χρησιμοποιούνται [12]. Επομένως, η ύπαρξη στέρεης καταγραφής ελέγχου είναι απαραίτητη για να είναι αξιόπιστο οποιοδήποτε σύστημα διαχείρισης σε επίπεδο επιχείρησης.

2.8 Άλλα Συστήματα

Πέρα από τις λύσεις που αναφέρθηκαν παραπάνω, υπάρχουν και άλλα συστήματα που σχετίζονται με τη διαχείριση χρηστών και εξοπλισμού, έστω και έμμεσα. Για παράδειγμα, συστήματα διαχείρισης έργων όπως το Jira ή το Trello χρησιμοποιούνται ευρέως σε επιχειρήσεις και δίνουν τη δυνατότητα οργάνωσης ομάδων και ρόλων μέσα από την καθημερινή ροή εργασιών. Επίσης, εργαλεία τύπου helpdesk ή ITSM, όπως το ServiceNow, συχνά αξιοποιούνται για αιτήματα πρόσβασης και υποστήριξης, λειτουργώντας παράλληλα με τα συστήματα IAM. Σε κάποιες περιπτώσεις, οργανισμοί εφαρμόζουν και Mobile Device Management (MDM) εργαλεία, όπως το Intune, για να έχουν έλεγχο στις φορητές συσκευές και στις πολιτικές ασφαλείας που τις συνοδεύουν. Αν και δεν αποτελούν τον βασικό κορμό της παρούσας πτυχιακής, αξίζει να σημειωθεί ότι αυτά τα συστήματα συνήθως συνεργάζονται με λύσεις διαχείρισης ταυτότητας και εξοπλισμού, δημιουργώντας ένα πιο ολοκληρωμένο πλαίσιο για την ασφάλεια και την ομαλή λειτουργία της επιχείρησης

2.9 Σύνοψη

Δεδομένου ότι περιλαμβάνει Διαχείριση Εργαζομένων, Έλεγχο Πρόσβασης, Παρακολούθηση Εξοπλισμού, Ειδοποιήσεις, Αναφορές και Καταγραφή Ελέγχων, το προτεινόμενο σύστημα μπορεί να χειριστεί τη σχέση μεταξύ των ανθρώπων, την πρόσβαση στο σύστημα και τους φυσικούς πόρους σε μία μόνο μονάδα. Η χρήση μιας ενιαίας προσέγγισης διευκολύνει τους οργανισμούς να συμμορφωθούν, διασφαλίζει καλύτερη αποτελεσματικότητα και προσθέτει την ευελιξία που απαιτείται για την αναβάθμιση της υποδομής και του προσωπικού τους ανάλογα [4][13]. Όλες οι ενότητες έχουν ρυθμιστεί ώστε να ταιριάζουν ομαλά με την κύρια αρχιτεκτονική, επιτρέποντας μελλοντικές συνδέσεις με πλατφόρμες HRIS, IAM και ITSM. Με τον τρόπο αυτό, το προτεινόμενο σύστημα προσφέρει μια ολοκληρωμένη λύση για την καθημερινή διαχείριση ανθρώπινου δυναμικού και εξοπλισμού.

Κεφάλαιο 3ο: Μεθοδολογία

Η τεχνική αρτιότητα, η επεκτασιμότητα, η χρηστικότητα και η συντηρησιμότητα επιτεύχθηκαν κατά την ανάπτυξη του Συστήματος Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού χρησιμοποιώντας αυστηρά μια δομημένη μέθοδο. Το κεφάλαιο παρουσιάζει τα εργαλεία, τις προσεγγίσεις και τα βήματα ανάλυσης, σχεδιασμού, υλοποίησης και δοκιμών του συστήματος. Η χρήση γνωστών μεθόδων μηχανικής λογισμικού, όπως η αρθρωτή δομή, η επαναληπτική κατασκευή και η συμπερίληψη των ενδιαφερόμενων μερών, βοηθά το τελικό προϊόν να καλύψει τις ανάγκες του οργανισμού.

3.1 Στοιβα Τεχνολογίας

Η επιλογή της στοιβας τεχνολογίας αποτελεί κρίσιμο βήμα για την επιτυχή ανάπτυξη και συντήρηση κάθε πληροφοριακού συστήματος. Στην παρούσα εργασία, δόθηκε ιδιαίτερη έμφαση στη χρήση σύγχρονων, ανοιχτών και ευρέως υποστηριζόμενων τεχνολογιών, ώστε να εξασφαλιστεί τόσο η τεχνική αρτιότητα όσο και η δυνατότητα μελλοντικής επεκτασιμότητας.

Η συνολική αρχιτεκτονική βασίζεται στο μοντέλο client–server, με το frontend να υλοποιεί τη διεπαφή χρήστη, το backend να αναλαμβάνει την επιχειρησιακή λογική και τη διασύνδεση με τη βάση δεδομένων, ενώ η διαχείριση ταυτοποίησης/εξουσιοδότησης και το deployment υλοποιούνται με εξειδικευμένες τεχνολογίες. Η επικοινωνία μεταξύ frontend και backend γίνεται μέσω GraphQL API, που εξασφαλίζει αποδοτική και στοχευμένη ανάκτηση δεδομένων.

3.1.1 Backend

Το backend αποτελεί την “καρδιά” του συστήματος, υπεύθυνη για την επεξεργασία των αιτημάτων, την επιχειρησιακή λογική και την αλληλεπίδραση με τη βάση δεδομένων.

- Node.js & TypeScript: προσφέρει ασύγχρονη εκτέλεση και υψηλή απόδοση. Η TypeScript προσθέτει στατική τυποποίηση, μειώνοντας σφάλματα κατά την ανάπτυξη.
- Koa (Web Server): ελαφρύς server που παρέχει απλότητα και ευελιξία στη διαχείριση HTTP αιτημάτων.
- Apollo GraphQL Module: ενσωματώνει το GraphQL, το οποίο επιτρέπει στον client να λαμβάνει μόνο τα απαραίτητα δεδομένα, βελτιστοποιώντας την επικοινωνία.
- Class-validator: εξασφαλίζει την εγκυρότητα των εισόδων, βελτιώνοντας την ασφάλεια του συστήματος.
- Mikro-ORM: υλοποιεί την αντικειμενοστραφή αντιστοίχιση με τη MySQL, διευκολύνοντας την ανάπτυξη και διαχείριση migrations.
- MySQL: επιλέχθηκε ως σχεσιακή βάση δεδομένων, γνωστή για τη σταθερότητα, την ευρεία υποστήριξη και την αποδοτικότητά της.
- Keycloak (OAuth2): αναλαμβάνει τον μηχανισμό αυθεντικοποίησης και εξουσιοδότησης, υποστηρίζοντας πρότυπα όπως OpenID Connect.
- Nodemailer: επιτρέπει την αυτοματοποίηση ειδοποιήσεων μέσω email (π.χ. ενημέρωση για παραχώρηση ή επιστροφή asset).
- Jest: παρέχει ισχυρό πλαίσιο δοκιμών για επαλήθευση της ορθής λειτουργίας.

3.1.2 Frontend

Το frontend αναπτύχθηκε με γνώμονα την ευχρηστία, την ταχύτητα και την προσαρμοστικότητα, ώστε να εξασφαλίζεται θετική εμπειρία χρήστη.

- JavaScript: κύρια γλώσσα υλοποίησης.
- Vue.js 2 με Composition API: προσφέρει αρχιτεκτονική βασισμένη σε components, διευκολύνοντας την οργάνωση και επαναχρησιμοποίηση κώδικα. Το Composition API προσθέτει μεγαλύτερη ευελιξία στη διαχείριση κατάστασης.
- Quasar UI Framework: παρέχει πλήρη βιβλιοθήκη έτοιμων, responsive στοιχείων για ταχύτερη ανάπτυξη UI.
- Vuex: αναλαμβάνει την κεντρική διαχείριση της κατάστασης, διασφαλίζοντας συνέπεια δεδομένων σε όλη την εφαρμογή.
- Apollo Client (GraphQL): λειτουργεί ως client-side layer για τη διαχείριση queries και mutations προς το backend.
- OAuth OpenID Connect Client: επιτρέπει ασφαλή είσοδο/έξοδο χρηστών μέσω των μηχανισμών του Keycloak.
- FullCalendar: χρησιμοποιείται για την οπτικοποίηση χρονοδιαγραμμάτων και προσβάσεων.

3.1.3 Deployment και Υποδομή

Για την ορθή λειτουργία του συστήματος στο παραγωγικό περιβάλλον αξιοποιήθηκαν σύγχρονες τεχνολογίες containerization και web serving.

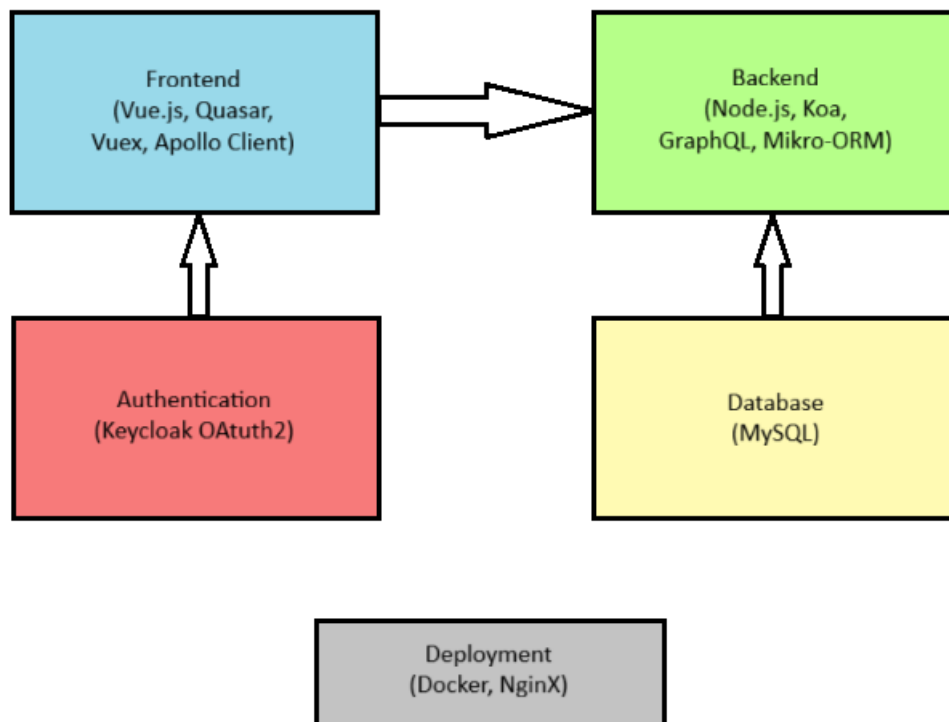
- Docker: παρέχει απομόνωση υπηρεσιών και φορητότητα. Το Keycloak εκτελείται σε ξεχωριστό container για καλύτερη διαχείριση.
- Nginx Proxy: προωθεί αιτήματα προς το backend, βελτιώνοντας την ασφάλεια και την απόδοση.
- Nginx Static File Server: εξυπηρετεί τα στατικά αρχεία του frontend με ταχύτητα και αξιοπιστία.

3.1.4 Συνολική Αρχιτεκτονική

Συνοπτικά, η στοίβα τεχνολογίας οργανώνεται ως εξής:

- Το **frontend** χειρίζεται την αλληλεπίδραση με τον χρήστη.
- Το **backend** επεξεργάζεται αιτήματα και συνδέεται με τη βάση δεδομένων.
- Η **ασφάλεια** διασφαλίζεται από το Keycloak με OAuth2 και OpenID Connect.
- Το **deployment** υλοποιείται μέσω Docker και Nginx, παρέχοντας σταθερότητα και κλιμακωσιμότητα.

Η παρακάτω εικόνα (Σχήμα 3.1) απεικονίζει τη συνολική αρχιτεκτονική του συστήματος:



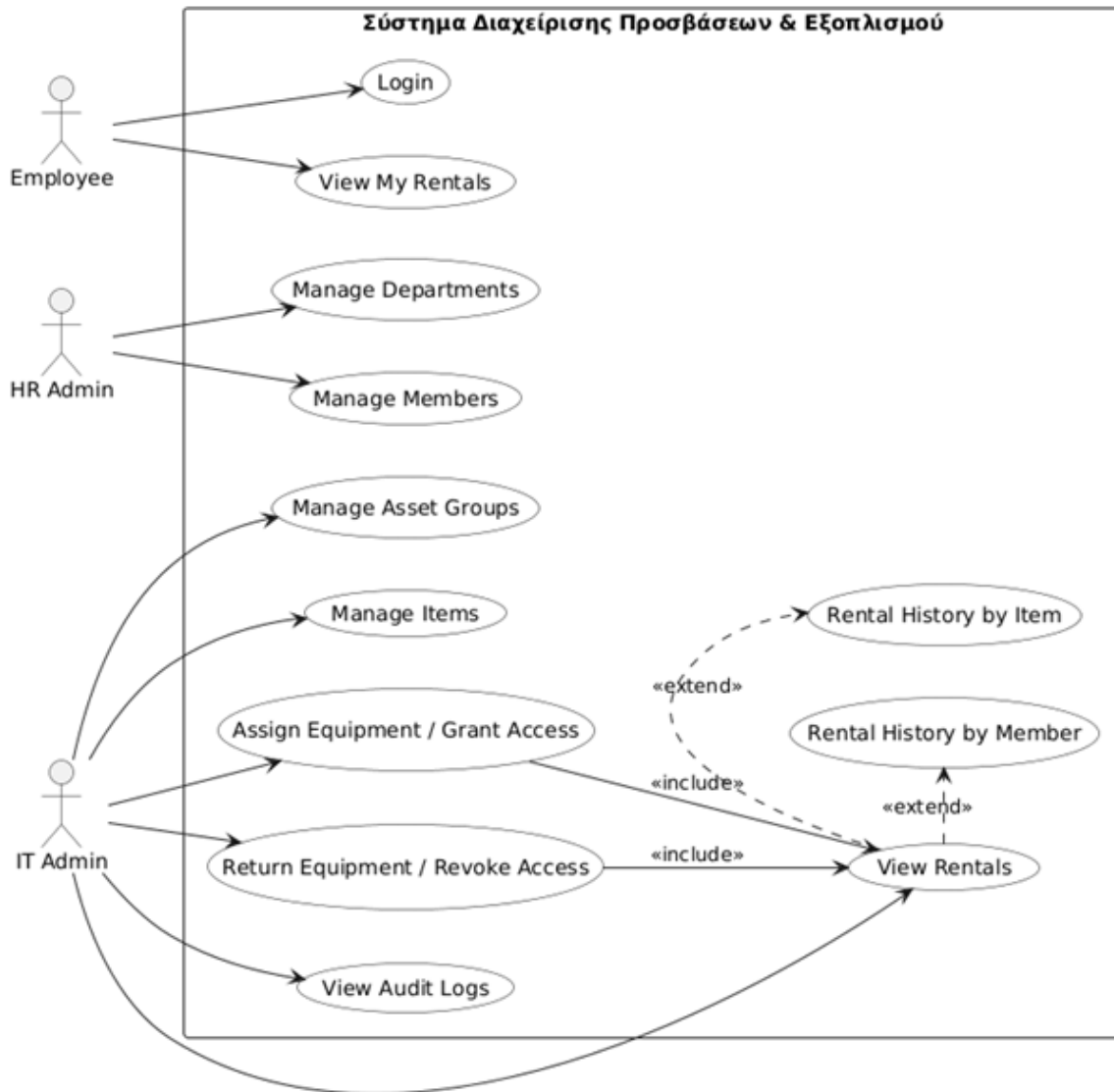
Σχήμα 3.1 Αρχιτεκτονική Συστήματος

3.2 Διαδικασία Σχεδιασμού

3.2.1 Προσέγγιση Σχεδιασμού με επίκεντρο τον χρήστη

Η ομάδα σχεδιασμού επικεντρώθηκε στους χρήστες, διασφαλίζοντας ότι το τελικό σύστημα θα μπορούσε να λύσει προβλήματα που αντιμετωπίζουν οι χειριστές. Οι υπεύθυνοι HR και IT συμμετείχαν στο έργο από την αρχή, συνεισφέροντας ανατροφοδότηση στον σχεδιασμό του συστήματος. Χάρη στη συμμετοχή τους, ο σχεδιασμός μπόρεσε να υλοποιηθεί αποτελεσματικά και να ενταχθεί στις τακτικές εργασίες και τα προβληματικά σημεία της ομάδας.

Παρακάτω γίνεται αναφορά στο Σχήμα 3.2, όπου απεικονίζεται διάγραμμα με τους κύριους παράγοντες (HR, IT Admin και Υπάλληλο) και τις αλληλεπιδράσεις τους με το σύστημα μέσω κύριων περιπτώσεων χρήσης, όπως η προσθήκη χρηστών, η εκχώρηση ή η ανάκληση πρόσβασης, η υποβολή αιτημάτων για συσκευές και η δημιουργία αναφορών.

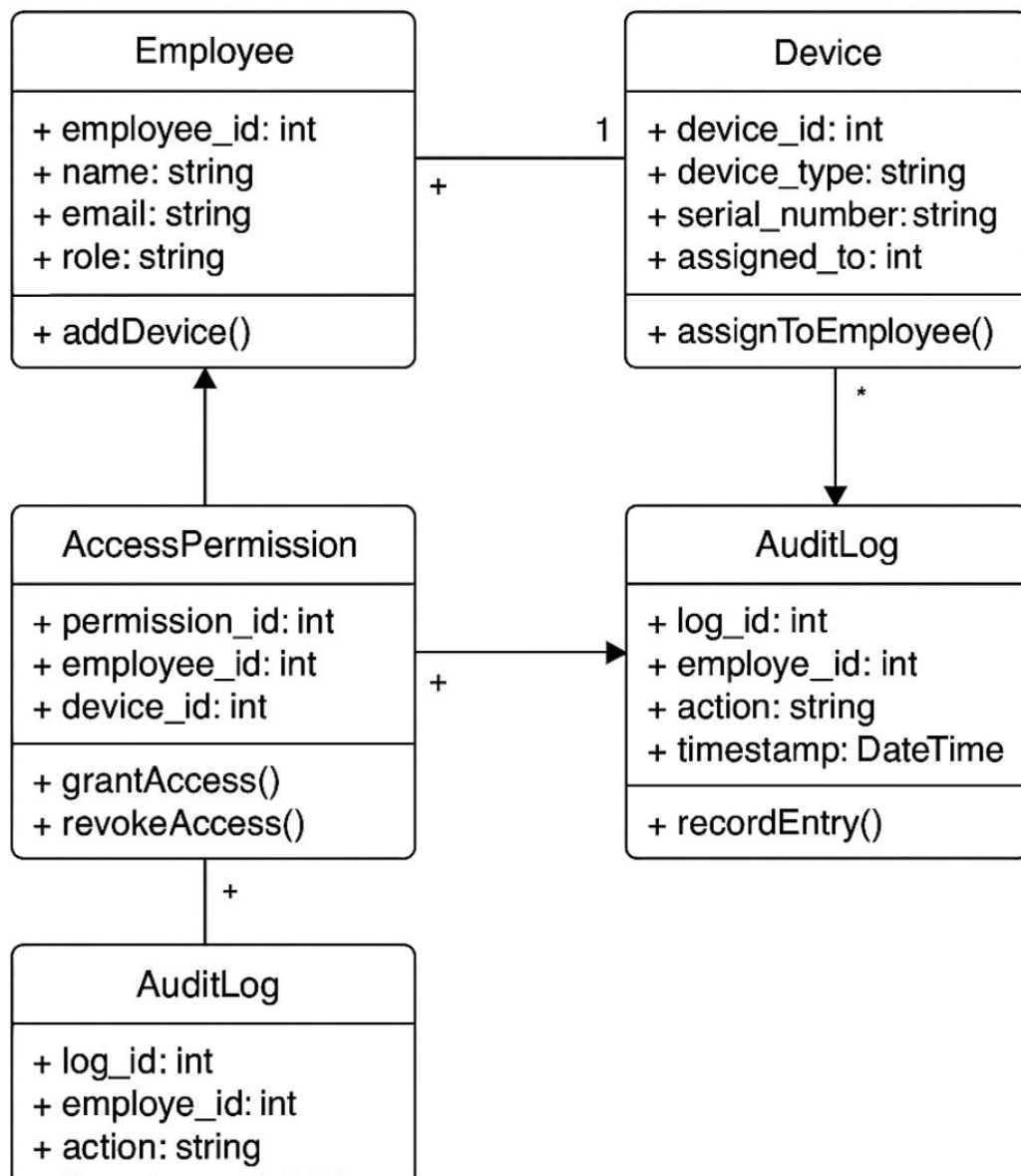


Σχήμα 3.2 Διάγραμμα περίπτωσης χρήσης του Συστήματος Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού

3.2.2 Συγκέντρωση Απαιτήσεων

Πραγματοποιήθηκαν συνεδρίες με μέλη του τμήματος Ανθρώπινου Δυναμικού, της Πληροφορικής και διαφόρων τμημάτων για να κατανοηθούν τα προβλήματα που αντιμετωπίζουν και τι αναμένεται από αυτά. Μερικές από τις βασικές ανησυχίες ήταν ότι οι μηχανές των εργαζομένων εξακολουθούσαν να παρακολουθούνται χειροκίνητα, η απενεργοποίηση της πρόσβασης καθυστερούσε κατά τις αναχωρήσεις και ο κατάλογος ενεργειών δεν ήταν απολύτως σαφής. Όλες αυτές οι πληροφορίες οργανώθηκαν σε μια πλήρη λίστα λειτουργικών και μη λειτουργικών απαιτήσεων. Οι βασικές λειτουργίες που χειρίζονταν τον εξοπλισμό, η κατανομή και η είσοδος και τα μη λειτουργικά στοιχεία έδιναν έμφαση στη διατήρηση της ασφάλειας, της καλής ταχύτητας και της ευκολίας χρήσης.

Παρακάτω γίνεται αναφορά στο Σχήμα 3.3, όπου απεικονίζεται διάγραμμα με τις δομικές σχέσεις μεταξύ των βασικών κλάσεων: Employee (Υπάλληλος), Device (Συσκευή), AccessPermission (Άδεια Πρόσβασης) και AuditLog (Λογιστικό Αρχείο). Ορίζει τα χαρακτηριστικά και τις μεθόδους κάθε κλάσης και δείχνει πώς στους υπαλλήλους εκχωρούνται συσκευές, παρέχεται πρόσβαση και καταγράφονται μέσω καταχωρίσεων ελέγχου για λόγους λογοδοσίας και ιχνηλασιμότητας.



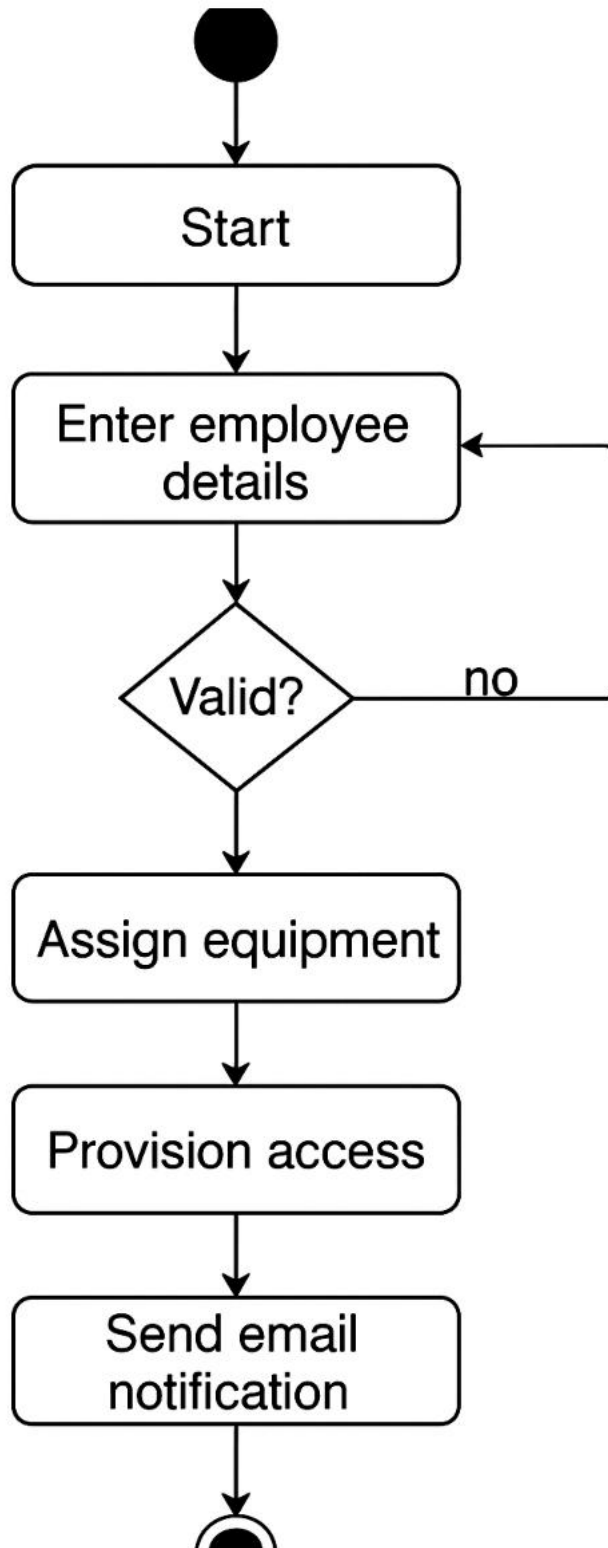
Σχήμα 3.3 Διάγραμμα κλάσης UML για το Σύστημα Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού

3.2.3 Ανάπτυξη διαγραμμάτων UML

Η λειτουργικότητα και η δομή του συστήματος έγιναν σαφείς με μια σειρά από διαγράμματα UML. Η εγγραφή νέων υπαλλήλων, η παροχή και η αφαίρεση πρόσβασης, η ανάθεση τεχνολογικού εξοπλισμού στο προσωπικό και η εκτέλεση αναφορών ήταν μερικές από τις βασικές ενέργειες των χρηστών που παρουσιάζονται στα διαγράμματα περιπτώσεων χρήσης. Τα διαγράμματα δραστηριοτήτων έδειχναν με σαφήνεια κάθε βήμα στην ένταξη, την αποχώρηση και την παράδοση εξοπλισμού, γεγονός που επέτρεψε τον εντοπισμό των σημείων στα οποία οι εργαζόμενοι ενδέχεται να αντιμετωπίσουν δυσκολίες. Επιπλέον, χρησιμοποιήθηκαν διαγράμματα κλάσεων για τη δημιουργία της κύριας δομής του λογισμικού, δείχνοντας πώς αλληλεπιδρούν μεταξύ τους ο Υπάλληλος, η Συσκευή και η Πρόσβαση.

Παρακάτω γίνεται αναφορά στο Σχήμα 3.4, όπου απεικονίζεται διάγραμμα που περιγράφει τη διαδικασία ένταξης, ξεκινώντας με την εισαγωγή των στοιχείων του υπαλλήλου, την επικύρωση των

δεδομένων, την ανάθεση εξοπλισμού, την παροχή πρόσβασης και ολοκληρώνοντας με μια αυτοματοποιημένη ειδοποίηση μέσω email στα αρμόδια τμήματα.



Σχήμα 3.4 Διάγραμμα δραστηριότητας για τη ροή εργασίας ένταξης υπαλλήλων

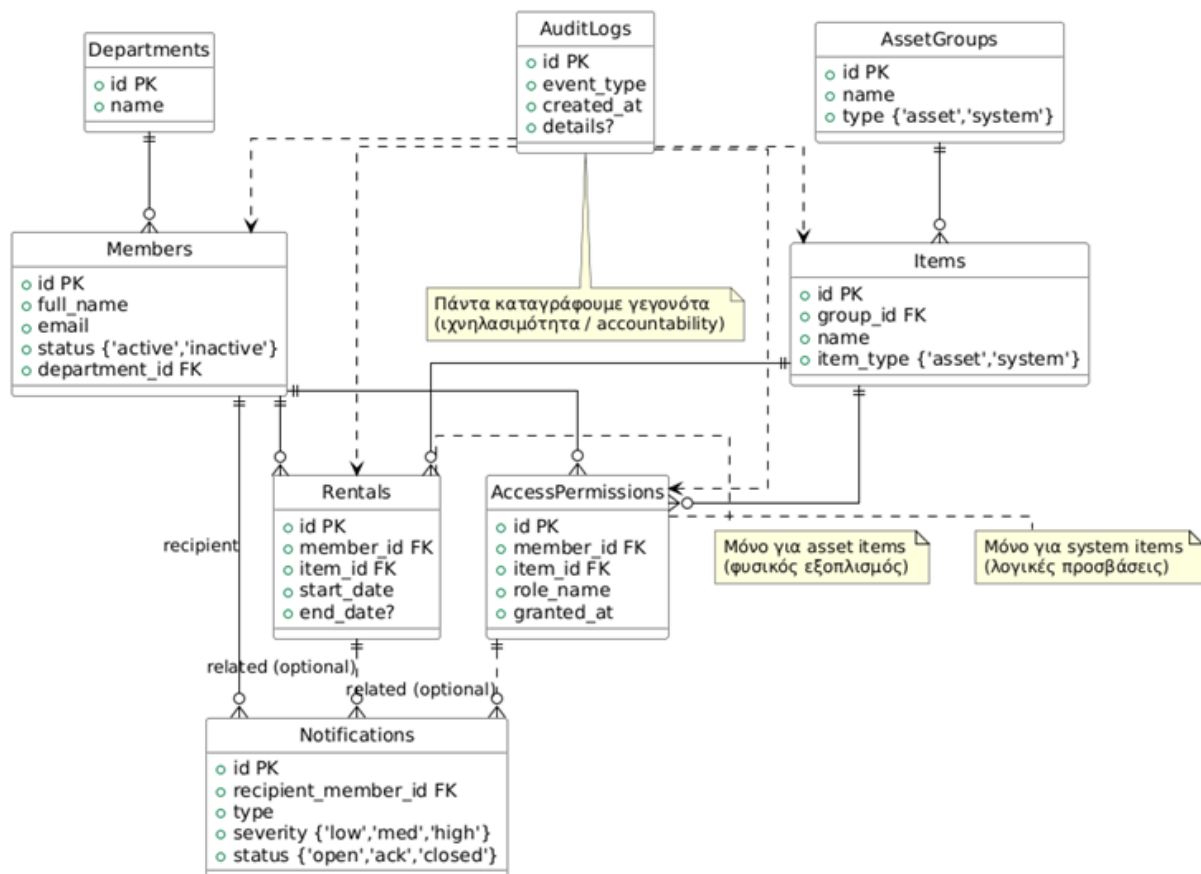
3.2.4 Διάγραμμα Οντότητας-Σχέσης (ER)

Δημιουργήθηκε ένα κανονικοποιημένο διάγραμμα ER για τον σχεδιασμό της βάσης δεδομένων, με στόχο την αποφυγή πλεονασμών και τη διατήρηση της συνέπειας. Ο πίνακας Members (Υπάλληλοι) αποτελεί τον κεντρικό κόμβο και συνδέεται με τα Departments για την οργάνωση της εταιρικής δομής, καθώς και με τους πίνακες Items και AssetGroups για την καταγραφή εξοπλισμού και συστημάτων.

Η εκχώρηση φυσικού εξοπλισμού καταγράφεται στον πίνακα Rentals, ενώ τα δικαιώματα πρόσβασης σε λογικά συστήματα αποτυπώνονται στον πίνακα AccessPermissions. Με αυτόν τον τρόπο διαχωρίζεται σαφώς η διαχείριση υλικών πόρων από τη διαχείριση λογικών προσβάσεων. Ο πίνακας AuditLogs καταγράφει όλες τις ενέργειες που εκτελούνται, ώστε να εξασφαλίζεται ασφάλεια, ιχνηλασιμότητα και συμμόρφωση.

Επιπλέον, ο πίνακας Notifications αποθηκεύει τις ειδοποιήσεις που παράγονται αυτόματα από το σύστημα. Κάθε ειδοποίηση συνδέεται με συγκεκριμένο παραλήπτη και μπορεί να σχετίζεται με μια εγγραφή σε rental ή access. Η παράδοσή της πραγματοποιείται μέσω email ή/και του dashboard, ενώ οι σχετικές ενέργειες καταγράφονται επίσης στο AuditLogs.

Στο Σχήμα 3.5 παρουσιάζεται το ER διάγραμμα με τις βασικές σχέσεις ανάμεσα στους πίνακες και τον κανονικοποιημένο σχεδιασμό τους.



Σχήμα 3.5 Διάγραμμα Οντότητας-Σχέσης (ER) του Σχήματος Βάσης Δεδομένων Συστήματος

3.2.5 Σχέδια καλωδίων και πρωτότυπα UI

Όλος ο σχεδιασμός της διεπαφής χρήστη έγινε στο Figma και χρησιμοποιήσαμε wireframes και πρωτότυπα για να δείξουμε τη δομή και την πλοήγηση του ιστότοπου. Ένας απλός και σαφής

σχεδιασμός ήταν η κύρια εστίαση στην αποστολή της εταιρείας. Μια μεγάλη οθόνη εμφάνιζε σημαντικές μετρήσεις και ειδοποιήσεις και επίσης τακτοποιούσε τις λειτουργίες σε ξεχωριστές ενότητες για χρήστες, στοιχεία και αναφορές. Μετά την παρουσίαση αυτών των πρωτοτύπων στα ενδιαφερόμενα μέρη, έγιναν επαναληπτικές αλλαγές στην ΙΑ και τον οπτικό σχεδιασμό. Η παρακολούθηση των σχολίων επέτρεψε στους σχεδιαστές να διευκολύνουν όλους τους τύπους χρηστών να χρησιμοποιούν το σύστημα σωστά.

3.2.6 Σύνοψη

Ως αποτέλεσμα της χρήσης αυτής της βασισμένης σε πρότυπα και ενδιαφέρουσας διαδικασίας, το σύστημα αναπτύχθηκε από γενικές ανάγκες σε ένα ολοκληρωμένο σχέδιο σχεδιασμού. Συγκεντρώνοντας προτάσεις χρηστών, δοκιμάζοντας πρωτότυπα και μοντελοποιώντας το λογισμικό, η ομάδα διασφάλισε ότι η υλοποίηση ακολουθούσε τόσο τους στόχους της εταιρείας όσο και τις προσδοκίες των χρηστών.

3.3 Προσέγγιση Ανάπτυξης

3.3.1 Επαναληπτική Ανάπτυξη Βασισμένη σε Ευέλικτο Σύστημα

Το σύστημα δημιουργήθηκε χρησιμοποιώντας μια ευέλικτη μέθοδο, δίνοντας ιδιαίτερη σημασία στην ευελιξία, επιτρέποντας τη συνεργασία και την εργασία σε μικρά στάδια. Προτιμήθηκε να διασφαλιστεί ότι οι νέες απαιτήσεις θα μπορούσαν να εισαχθούν ομαλά και ότι οι συνεχείς προτάσεις από τα ενδιαφερόμενα μέρη θα επηρέαζαν την εξέλιξη του προϊόντος. Το έργο αναπτύχθηκε και δόθηκε σε όλους όσους εμπλέκονταν στο HR και την IT η ευκαιρία να εξετάσουν τη νέα λειτουργικότητα. Ο τακτικός σχεδιασμός, η εκτέλεση εργασιών και η αναθεώρηση της εργασίας τους βοήθησε στο να λυθούν γρήγορα τα προβλήματα, να βελτιωθούν οι λειτουργίες και να διατηρηθεί μια ισχυρή αίσθηση του τι ήθελαν οι χρήστες.

Το πρώτο στάδιο περιλάμβανε κυρίως τη δημιουργία της υποδομής ανάπτυξης. Αυτό περιλάμβανε τη διαμόρφωση της πλατφόρμας ανάπτυξης, τον σχεδιασμό της δομής της βάσης δεδομένων σύμφωνα με το διάγραμμα ER και τη δημιουργία βασικών τρόπων για την ασφαλή σύνδεση και πρόσβαση των χρηστών στο σύστημα. Ο δεύτερος κύκλος εργασίας επικεντρώθηκε στην εγγραφή των εργαζομένων στο σύστημα και στη λογική που ελέγχει την πρόσβασή τους, η οποία απαιτούσε την ανάθεση ρόλων, τη διαχείριση των δικαιωμάτων τους και την προσθήκη νέων χρηστών στην πλατφόρμα. Το τρίτο στάδιο αφορά στη δημιουργία ενός συστήματος τόσο για τον εξοπλισμό όσο και για τους ανατεθειμένους ρόλους στο σύστημα. Οι χρήστες μπορούσαν να συνδέσουν τον εξοπλισμό με τους υπαλλήλους και να έχουν πρόσβαση σε πληροφορίες σχετικά με την κατάσταση της συσκευής τους όποτε το χρειαζόνταν.

Στη συνέχεια, ενσωματώνονται νέες λειτουργίες, όπως αυτόματα email και ποικίλες αναφορές δεδομένων. Βελτίωσαν την ικανότητα του συστήματος να ενημερώνει τους χρήστες για την κατάργηση πρόσβασης ή τις λανθασμένες επιστροφές και να παρέχει τις απαραίτητες αναφορές για αξιολογήσεις και ελέγχους. Κατά τη διάρκεια του πέμπτου και τελευταίου σταδίου, πραγματοποιήθηκαν πλήρεις δοκιμές ενσωμάτωσης, επιλύθηκαν σφάλματα, βελτιστοποιήθηκε η απόδοση του συστήματος και ετοιμάστηκαν όλα τα απαραίτητα έγγραφα για την ανάπτυξη και την εκπαίδευση του συστήματος. Ελέγχθηκαν διεξοδικά διαφορετικές ενότητες για να βεβαιωθεί ότι δεν υπήρξε απώλεια δεδομένων, ότι η διεπαφή φαινόταν η ίδια και ότι όλα τα μέρη επικοινωνούσαν με ασφάλεια.

3.3.2 Δομή και τεκμηρίωση αρθρωτής κωδικοποίησης

Για μεγάλο μέρος της διαδικασίας ανάπτυξης χρησιμοποιήθηκε μια αρθρωτή αρχιτεκτονική προσέγγιση για τη συγγραφή του κώδικα. Ο διαχωρισμός του συστήματος σε μονάδες, ιδιαίτερα για τον έλεγχο ταυτότητας, τη διαχείριση χρηστών και τη διαχείριση πόρων, διευκόλυνε τη διαχείριση και τη χρήση του. Όλα τα σενάρια και τα αρχεία διαμόρφωσης φυλάσσονταν στους δικούς τους φακέλους μέσα σε κάθε ενότητα. Με μια αρθρωτή προσέγγιση, ο κώδικας παρέμεινε οργανωμένος και εύκολος στην ανάπτυξη, επομένως ελαχιστοποιήθηκε η πιθανότητα σημαντικών διακοπών από ενημερώσεις ή συγχώνευση με εξωτερικά συστήματα.

Η τεκμηρίωση χειριζόταν παράλληλα με άλλες λειτουργίες. Προστέθηκαν σχόλια δίπλα σε κάθε συνάρτηση, μέθοδο και κλάση για να γίνει ο κώδικας πιο σαφής για τους προγραμματιστές τώρα και στο μέλλον. Κάθε ενότητα περιείχε ένα αρχείο README που εξηγούσε την εργασία της, τον τρόπο λειτουργίας της στο εσωτερικό της και τυχόν βιβλιοθήκες που χρειαζόταν για να λειτουργήσει. Επειδή όλα ήταν καλά τεκμηριωμένα, οι νέοι υπάλληλοι μπορούσαν να αναλάβουν την εργασία πιο γρήγορα και η διόρθωση σφαλμάτων και η συντήρηση ήταν πιο απλές.

3.4 Μεθοδολογία Δοκιμών

Οι δοκιμές είναι σημαντικές για να επιβεβαιωθεί ότι η εφαρμογή θα είναι αξιόπιστη και θα έχει καλή απόδοση. Στο πλαίσιο αυτό ελέγχθηκε τόσο η επιχειρησιακή λογική όσο και η διεπαφή χρήστη (UI).

Η διεπαφή εξετάστηκε χειροκίνητα αλλά και με τη χρήση του Selenium, ώστε να διασφαλιστεί ότι όλα τα κουμπιά, οι φόρμες και τα αναπτυσσόμενα μενού λειτουργούν σωστά. Παράλληλα ελέγχθηκε η ταχύτητα φόρτωσης των σελίδων σε διαφορετικούς φυλλομετρητές (Chrome, Firefox) καθώς και σε πολλούς τύπους συσκευών, όπως επιτραπέζιοι υπολογιστές, tablet και κινητά τηλέφωνα. Οι δοκιμές αυτές βοήθησαν να επιβεβαιωθεί ότι η εμπειρία χρήστη παραμένει σταθερή, ανεξάρτητα από το περιβάλλον πρόσβασης

3.4.1 Δοκιμή μονάδας

Κάθε διαδικασία «Προσθήκη Υπαλλήλου», «Ανάθεση Εξοπλισμού» και «Αποστολή Ειδοποίησης» δοκιμάστηκε με το Jest της JavaScript. Οι δοκιμές unit έλεγξαν ότι ο κώδικας συμπεριφέρθηκε σωστά σε κάθε περίπτωση.

3.4.2 Δοκιμή ολοκλήρωσης

Οι επιμέρους ενότητες υλοποιήθηκαν διαδοχικά και, σε κάθε στάδιο, ελέγχθηκε ότι τα δεδομένα μεταφέρονταν σωστά μεταξύ του χρήστη, του backend και της βάσης δεδομένων. Για παράδειγμα, μια δοκιμαστική κατάσταση επιβεβαίωσε ότι ένας νέος χρήστης μπορούσε να προσθέσει τα στοιχεία του, να αποκτήσει πρόσβαση στο VPN, να λάβει έναν φορητό υπολογιστή και να δημιουργήσει σωστά όλα τα αρχεία και τα email του.

3.4.3 Δοκιμές ασφαλείας

Το RBAC διασφαλίστηκε ότι κάθε χρήστης μπορεί να εκτελεί μόνο ενέργειες που επιτρέπουν οι κανόνες. Ελέγχθηκαν όλες οι μέθοδοι για την επικύρωση των δεδομένων εισόδου, την προστασία από επιθέσεις CSRF και τους κωδικούς πρόσβασης hash.

3.5 Σύνοψη

Η μεθοδολογία συνδύασε σύγχρονα εργαλεία web, συμμετοχικό σχεδιασμό με επίκεντρο τον χρήστη και ευέλικτες (agile) πρακτικές, παράγοντας ένα σταθερό και ασφαλές σύστημα διαχείρισης προσβάσεων και εξοπλισμού. Η εκτενής μοντελοποίηση (UML, ER), η αρθρωτή υλοποίηση και οι συστηματικές δοκιμές (unit, integration, UI, security) ενόησαν τη συντηρησιμότητα, την επεκτασιμότητα και την ποιότητα. Χάρη στην καθαρή διάκριση επιπέδων (frontend, backend, δεδομένα, έλεγχος ταυτότητας) και στη στοιβα που επιλέχθηκε, η εφαρμογή παραμένει φορητή και εύκολα εξελίξιμη, καλύπτοντας τις επιχειρησιακές ανάγκες HR και IT..

Κεφάλαιο 4ο: Αρχιτεκτονική Συστήματος

Το Σύστημα Διαχείρισης Πρόσβασης Εξοπλισμού Εργαζομένων και Εταιρικής Χρήσης είναι κατασκευασμένο με μια ισχυρή και ευέλικτη αρχιτεκτονική client-server, υποστηρίζοντας τον σαφή διαχωρισμό μεταξύ διεπαφής χρήστη (UI), επιχειρησιακών λειτουργιών και αποθήκευσης δεδομένων. Αυτή η δομή εξασφαλίζει αρθρωτότητα, βιωσιμότητα και επεκτασιμότητα — στοιχεία απαραίτητα για την επεξεργασία ευαίσθητων εταιρικών δεδομένων.

4.1 Τι είναι η Αρχιτεκτονική Χρήστη-Διακομιστή;

Η αρχιτεκτονική client-server είναι ένα καθιερωμένο μοντέλο στον χώρο της πληροφορικής, όπου το frontend (πελάτης) αναλαμβάνει την αλληλεπίδραση με τον χρήστη, ενώ το backend (διακομιστής) χειρίζεται την επιχειρησιακή λογική, τις διαδικασίες ασφαλείας και την πρόσβαση στη βάση δεδομένων.

Ο συγκεκριμένος διαχωρισμός προσφέρει σημαντικά πλεονεκτήματα [19]:

- **Αρθρωτότητα:** οι αλλαγές στη βάση δεδομένων ή στην επιχειρησιακή λογική δεν επηρεάζουν το UI.
- **Κλιμάκωση:** το backend μπορεί να επεκταθεί με περισσότερους πόρους χωρίς να αλλάξει το frontend.
- **Ασφάλεια:** το frontend δεν έχει άμεση πρόσβαση στα δεδομένα, αλλά επικοινωνεί μόνο μέσω API.

Το UI μπορεί να υλοποιηθεί με HTML, CSS και JavaScript, ή με σύγχρονα frameworks όπως Vue ή React, προσφέροντας προσαρμοσμένη εμπειρία για κάθε ρόλο. Έτσι, το HR βλέπει εργαλεία για διαχείριση προσωπικού, οι IT admins χειρίζονται δικαιώματα πρόσβασης, ενώ οι επικεφαλής τμημάτων έχουν οπτικοποίηση για τις ομάδες τους.

Η επικοινωνία με το backend γίνεται αποκλειστικά μέσω RESTful ή GraphQL API, που λειτουργούν ως ενδιάμεσο επίπεδο. Έτσι εξασφαλίζεται ότι τα δεδομένα είναι προσβάσιμα με ελεγχόμενο και ασφαλές τρόπο.

Τα APIs μπορούν να υλοποιηθούν με frameworks όπως Flask/Django (Python) ή Node.js. Αναλαμβάνουν:

- προσθήκη/τροποποίηση/διαγραφή εργαζομένων,
- ανάθεση και επιστροφή εξοπλισμού,
- διαχείριση δικαιωμάτων πρόσβασης.

Η αρχιτεκτονική αυτή διευκολύνει και τη διασύνδεση με εξωτερικά συστήματα, όπως:

- HRIS (Human Resource Information Systems),
- LDAP (Lightweight Directory Access Protocol),
- IAM (Identity and Access Management).

Η δυνατότητα ενοποίησης με τέτοιες πλατφόρμες είναι κρίσιμη σε μεγάλους οργανισμούς όπου η κεντρική διαχείριση ταυτοτήτων και η συμμόρφωση με κανονισμούς (GDPR, ISO 27001) είναι απαραίτητη.

4.2 Επίπεδο Backend και Βάσης Δεδομένων

Το backend είναι το κομβικό σημείο του συστήματος, υπεύθυνο για την εκτέλεση όλων των επιχειρησιακών διαδικασιών, την επικύρωση δεδομένων, την εφαρμογή πολιτικών ασφαλείας και τη

διασύνδεση με τη βάση δεδομένων. Κάθε αίτημα που φτάνει από το frontend περνά μέσα από το backend, το οποίο:

- ελέγχει την εγκυρότητά του,
- εφαρμόζει κανόνες που σχετίζονται με τον ρόλο του χρήστη,
- ενημερώνει ή ανακτά δεδομένα από τη βάση,
- και καταγράφει την ενέργεια σε audit logs.

4.2.1 Λειτουργικότητες του backend

Το backend καλύπτει βασικές διαδικασίες όπως:

- Ενσωμάτωση εργαζομένων (onboarding): καταχώρηση νέων χρηστών με τα προσωπικά και εργασιακά στοιχεία τους.
- Διαχείριση πρόσβασης: ανάθεση ή αφαίρεση δικαιωμάτων σε συστήματα (π.χ. ERP, VPN).
- Διαχείριση εξοπλισμού: παραχώρηση, παρακολούθηση και επιστροφή περιουσιακών στοιχείων.
- Απενεργοποίηση λογαριασμών: κατά την αποχώρηση υπαλλήλου, εξασφαλίζεται η αφαίρεση προσβάσεων και η επιστροφή συσκευών.
- Αναφορές και auditing: δημιουργία εκθέσεων χρήσης για HR, IT και compliance.

4.2.2 Βάση Δεδομένων

Η βάση δεδομένων υλοποιείται σε σχεσιακό μοντέλο, συνήθως με MySQL ή PostgreSQL, και έχει κανονικοποιημένη δομή (ER schema). Κύριοι πίνακες:

- Employees: προσωπικά στοιχεία, ρόλοι, τμήμα.
- Devices/Assets: καταγραφή φυσικού εξοπλισμού με μοναδικά IDs (serial number, asset tag).
- Access: δικαιώματα ανά χρήστη και σύστημα.
- AuditLogs: πλήρης καταγραφή ενεργειών με χρονική σήμανση.
- Notifications: ειδοποιήσεις που έχουν σταλεί ή εκκρεμούν.

Η κανονικοποίηση εξασφαλίζει συνέπεια και αποτρέπει διπλοεγγραφές. Για παράδειγμα, όταν διαγραφεί ένας εργαζόμενος, όλες οι σχετιζόμενες εγγραφές του (πρόσβαση, εξοπλισμός, ειδοποιήσεις) απενεργοποιούνται ή ενημερώνονται αυτόματα, αποφεύγοντας τα λεγόμενα «ορφανά δεδομένα».

4.2.3 Απόδοση και κλιμάκωση

Σε περιβάλλον με χιλιάδες εργαζόμενους και assets, η απόδοση της βάσης είναι κρίσιμη. Για τον λόγο αυτό:

- εφαρμόζονται ευρετήρια (indexes) σε πεδία που αναζητούνται συχνά,
- χρησιμοποιούνται βελτιστοποιημένα queries,
- υλοποιείται connection pooling ώστε πολλαπλά αιτήματα να εξυπηρετούνται χωρίς καθυστερήσεις.

Έτσι, ακόμη και σε μεγάλους οργανισμούς, οι αναφορές και οι έλεγχοι συμμόρφωσης εκτελούνται σε πραγματικό χρόνο.

4.3 Μηχανισμοί ασφαλείας

Δεδομένου ότι το σύστημα διαχειρίζεται ευαίσθητα δεδομένα προσωπικού και στοιχεία εταιρικού εξοπλισμού, η ασφάλεια είναι ενσωματωμένη σε όλα τα επίπεδα σχεδιασμού. Οι μηχανισμοί ασφαλείας χωρίζονται σε τέσσερις βασικές κατηγορίες: δικτυακή ασφάλεια, έλεγχος ταυτότητας και πρόσβασης, προστασία δεδομένων και auditing.

4.3.1 Δικτυακή ασφάλεια

Όλη η επικοινωνία μεταξύ frontend και backend γίνεται μέσω HTTPS με χρήση πρωτοκόλλων SSL/TLS. Έτσι προστατεύονται:

- τα διαπιστευτήρια χρηστών,
- τα tokens πρόσβασης,
- τα δεδομένα εργαζομένων και assets.

Με αυτόν τον τρόπο αποτρέπονται επιθέσεις τύπου man-in-the-middle, υποκλοπή δεδομένων ή αλλοίωση πακέτων κατά τη μεταφορά.

4.3.2 Έλεγχος ταυτότητας και πρόσβασης

Για την αυθεντικοποίηση και εξουσιοδότηση χρηστών χρησιμοποιείται Keycloak σε συνδυασμό με τα πρωτόκολλα OAuth2 και OpenID Connect.

- Μετά το login, ο χρήστης λαμβάνει access token, το οποίο καθορίζει τις ενέργειες που μπορεί να εκτελέσει.
- Η πρόσβαση ελέγχεται βάσει ρόλων (Role-Based Access Control – RBAC). Έτσι, οι HR managers μπορούν να δημιουργούν/τροποποιούν εργαζόμενους, οι IT admins να διαχειρίζονται ρυθμίσεις, αλλά κανένας δεν αποκτά δικαιώματα πέρα από τα καθορισμένα.

Αυτό μειώνει τον κίνδυνο προνομιακής κλιμάκωσης και εξασφαλίζει ότι κάθε ενέργεια αντιστοιχεί σε συγκεκριμένο ρόλο.

4.3.3 Προστασία κωδικών και δεδομένων

Οι κωδικοί πρόσβασης αποθηκεύονται μόνο σε μορφή κατακερματισμού (bcrypt ή PBKDF2), με χρήση μοναδικού salt για κάθε εγγραφή. Αυτό αποτρέπει:

- την ανάκτηση κωδικών σε περίπτωση παραβίασης βάσης,
- την εφαρμογή rainbow tables,
- επιθέσεις brute-force.

Επιπλέον, τα δεδομένα της βάσης μπορούν να προστατεύονται με κρυπτογράφηση σε επίπεδο δίσκου (disk-level encryption) ή ακόμη και σε επίπεδο πεδίου (field-level encryption) για κρίσιμες πληροφορίες.

4.3.4 Audit και λογοδοσία

Όλες οι ενέργειες χρηστών καταγράφονται σε audit logs, με:

- user ID,
- ημερομηνία/ώρα,
- τύπο ενέργειας (π.χ. «Απόδοση laptop σε υπάλληλο»),
- αποτέλεσμα (επιτυχία ή αποτυχία).

Τα logs είναι αδιάβλητα και προστατεύονται από μη εξουσιοδοτημένες τροποποιήσεις. Αυτό εξασφαλίζει:

- δυνατότητα ιχνηλασιμότητας σε περίπτωση παραβίασης,
- υποστήριξη για συμμόρφωση με πρότυπα όπως ISO 27001, GDPR και HIPAA,
- ύπαρξη αποδεικτικών στοιχείων για ελέγχους και εσωτερικές έρευνες.

4.4 Σύνοψη

Η αρχιτεκτονική του συστήματος βασίζεται σε ένα σαφές και ευέλικτο μοντέλο client–server, το οποίο διαχωρίζει λειτουργικά επίπεδα και διευκολύνει τόσο τη διαχείριση όσο και τη μελλοντική επέκταση. Ο διαχωρισμός μεταξύ διεπαφής χρήστη (frontend), επιχειρησιακής λογικής (backend) και αποθήκευσης δεδομένων (βάση) δημιουργεί ένα περιβάλλον όπου κάθε επίπεδο μπορεί να βελτιστοποιείται ή να αναβαθμίζεται ανεξάρτητα, χωρίς να επηρεάζεται η συνολική λειτουργία.

Η χρήση τεχνολογιών όπως το Keycloak για την αυθεντικοποίηση/εξουσιοδότηση, η MySQL για τη σταθερή και κανονικοποιημένη διαχείριση δεδομένων, καθώς και η επικοινωνία μέσω GraphQL API προσφέρουν:

- ενισχυμένη ασφάλεια,
- υψηλή ακεραιότητα δεδομένων,
- εγγυημένη διαθεσιμότητα.

Οι μηχανισμοί ασφαλείας έχουν ενσωματωθεί σε όλα τα επίπεδα:

- HTTPS για την προστασία των δικτυακών επικοινωνιών,
- RBAC και tokens για τον έλεγχο ταυτότητας,
- hashing με salt για την προστασία κωδικών,
- audit logs για πλήρη ιχνηλασιμότητα.

Έτσι το σύστημα ανταποκρίνεται στις ανάγκες συμμόρφωσης με διεθνή πρότυπα (GDPR, ISO 27001, HIPAA), καθιστώντας το κατάλληλο για χρήση ακόμη και σε περιβάλλοντα υψηλής ευαισθησίας.

Επιπλέον, η αρχιτεκτονική είναι αρθρωτή και επεκτάσιμη, κάτι που επιτρέπει την εύκολη ενσωμάτωση νέων λειτουργιών στο μέλλον. Για παράδειγμα, μπορούν να προστεθούν:

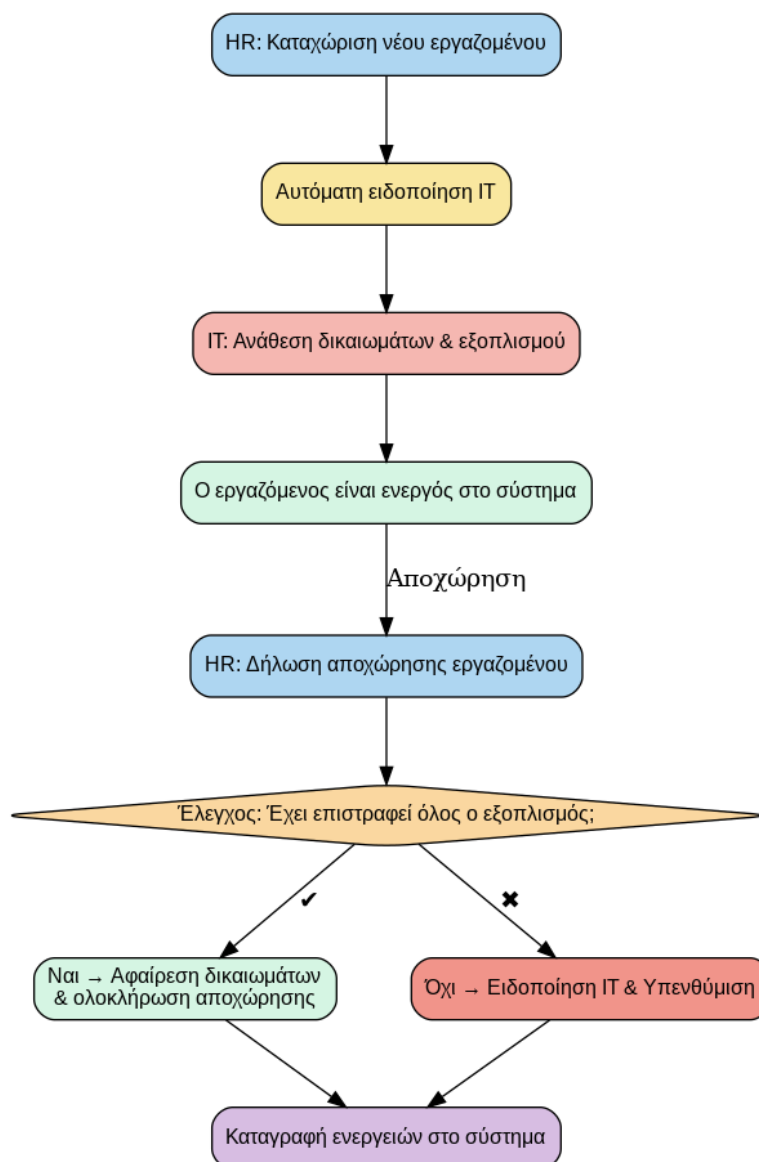
- επιπλέον μέθοδοι αυθεντικοποίησης (π.χ. SSO, 2FA),
- διασύνδεση με πλατφόρμες HRIS ή ITSM,
- αυτοματοποιημένοι μηχανισμοί provisioning για μεγαλύτερη κλίμακα.

Συνολικά, η παρούσα αρχιτεκτονική συνδυάζει ασφάλεια, αξιοπιστία και ευελιξία, προσφέροντας ένα ολοκληρωμένο εργαλείο για την αποτελεσματική διαχείριση προσβάσεων εργαζομένων και εταιρικού εξοπλισμού. Εξασφαλίζει ότι το σύστημα όχι μόνο καλύπτει τις ανάγκες του οργανισμού σήμερα, αλλά είναι και τεχνολογικά προετοιμασμένο να ανταποκριθεί σε μελλοντικές προκλήσεις, αλλαγές κανονισμών και αυξημένες απαιτήσεις κλιμάκωσης.

Κεφάλαιο 5ο: Υλοποίηση

Σε αυτό το στάδιο, οι προδιαγραφές σχεδιασμού μετατράπηκαν σε μια πλήρως λειτουργική εφαρμογή που συνδυάζει το front-end, το back-end, την επιχειρησιακή λογική, τον αυτοματισμό και την ασφαλή διαχείριση δεδομένων. Αναπτύχθηκε το σύστημα χρησιμοποιώντας ενότητες, ελέγχοντας την πρόσβαση ανά ρόλο και δοκιμάζοντας σε κάθε στάδιο. Τα κύρια σημεία του θέματος αναλύονται σε ξεχωριστές ενότητες σχετικά με τον τρόπο με τον οποίο εκτελείται το καθένα.

Παρακάτω γίνεται αναφορά στο Σχήμα 5.1, όπου απεικονίζεται διάγραμμα ροής με την πλήρη ροή εργασίας ενσωμάτωσης: Το τμήμα HR ξεκινά την εγγραφή των εργαζομένων, το σύστημα ειδοποιεί αυτόματα το τμήμα IT, το οποίο εκχωρεί δικαιώματα συσκευής και πρόσβασης. Όλες οι ενέργειες καταγράφονται και ενεργοποιούνται αυτοματοποιημένες ειδοποιήσεις για εκκρεμείς επιστροφές και ύποπτες δραστηριότητες.



Σχήμα 5.1 Γενική ροή εργασίας του Συστήματος Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού

5.1 Διεπαφές χρήστη για διαχειριστές ανθρώπινου δυναμικού και πληροφορικής

Η εφαρμογή περιλαμβάνει δύο ξεχωριστά συστήματα dashboard, ένα για το HR και το άλλο για το IT, τα οποία προσφέρουν λειτουργικότητα που ταιριάζει σε κάθε τμήμα.

Οι διευθυντές μπορούν να δημιουργούν, να προσαρμόζουν και να διαχειρίζονται τα αρχεία των εργαζομένων της εταιρείας μέσω του πίνακα ελέγχου HR. Κατά την εγγραφή, το τμήμα HR φροντίζει να σημειώνει το πλήρες όνομα κάθε εργαζομένου, σε ποιο τμήμα έχει ανατεθεί, τον ρόλο που έχει και τότε ξεκίνησε η απασχόλησή του. Μετά την υποβολή, το αίτημα τοποθετείται σε μια ουρά για να εκχωρήσει πρόσβαση το τμήμα IT και να διαχειριστεί τα περιουσιακά στοιχεία, γεγονός που μειώνει την απαιτούμενη χειροκίνητη βοήθεια. Έχουν χρησιμοποιηθεί αναπτυσσόμενα μενού, συμβουλές επικύρωσης και αυτόματης συμπλήρωσης στη διεπαφή για την αποτροπή σφαλμάτων.

Ο πίνακας ελέγχου IT επιτρέπει στους διαχειριστές να διαχειρίζονται ποιος έχει πρόσβαση και να παρακολουθούν τις εταιρικές συσκευές. Χρησιμοποιώντας αυτόν τον πίνακα, η ομάδα IT μπορεί να βλέπει όλους τους υπαλλήλους, να ελέγχει ποια δικαιώματα έχει κάθε άτομο και να αλλάζει αυτά τα δικαιώματα, εάν χρειάζεται. Ομοίως, τα βήματα για την ανάθεση συσκευών στο προσωπικό είναι διαθέσιμα στην εφαρμογή, ώστε η ομάδα IT να μπορεί να καταγράφει προσθήκες, να τις διανέμει και να παρακολουθεί τη χρήση τους μέχρι τη συνταξιοδότησή τους. Το περιβάλλον χρήστη διευκολύνει επίσης τον εντοπισμό καθυστερημένης υποβολής περιουσιακών στοιχείων και ατόμων που προσπαθούν να εισέλθουν σε συστήματα χωρίς έγκριση, ώστε οι διαχειριστές να μπορούν να ενεργούν άμεσα.

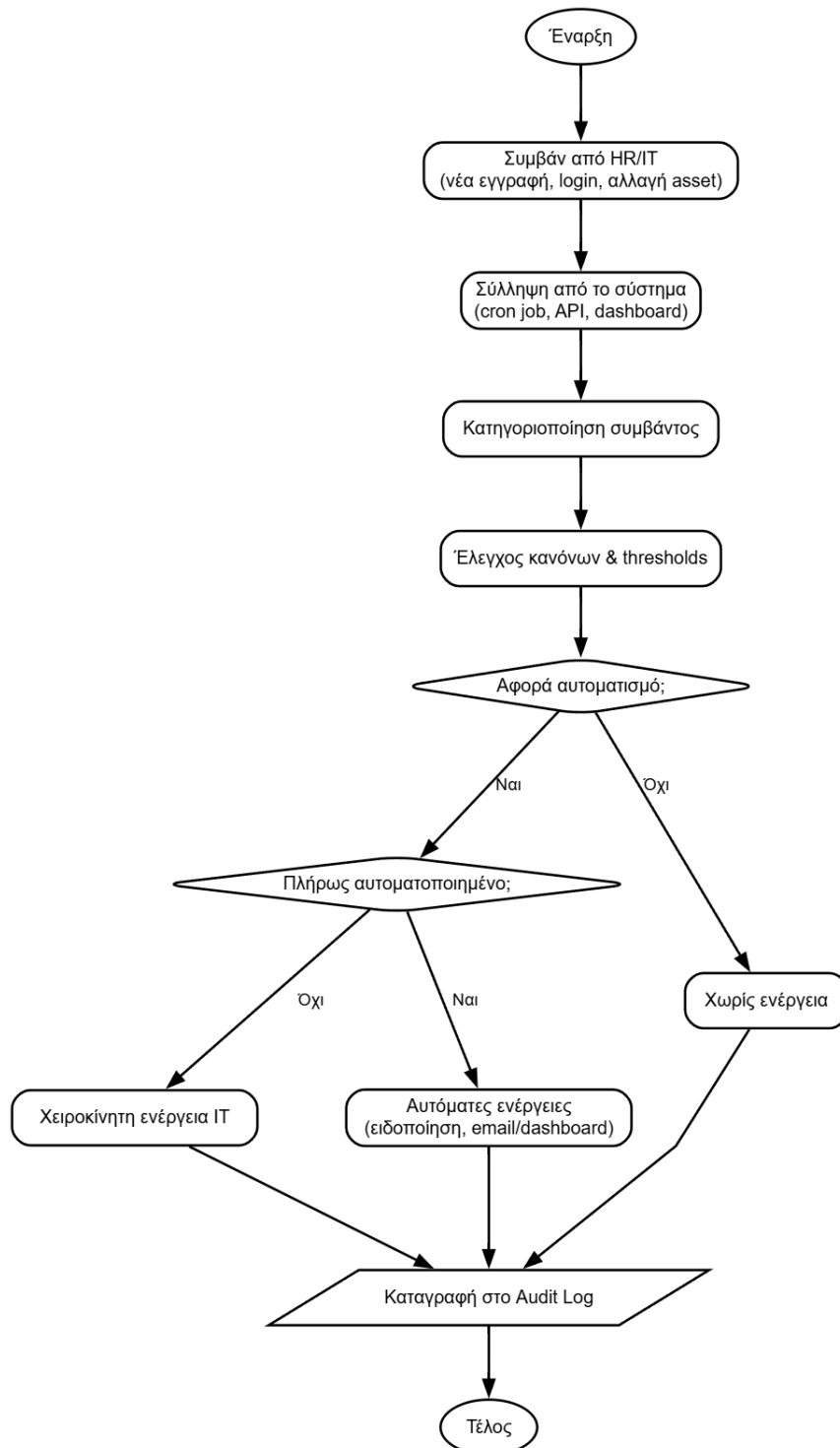
5.2 Λογική αυτοματισμού για ειδοποιήσεις και ανίχνευση ανωμαλιών

Ο αυτοματισμός ήταν ένας σημαντικός παράγοντας που βοήθησε στη μείωση του όγκου εργασίας που έπρεπε να κάνουν τα μέλη της ομάδας χειροκίνητα. Για να γίνει αυτό, χρησιμοποιήθηκε scripting από την πλευρά του διακομιστή με κανονικές εργασίες που εκτελούνταν μέσω cron και τα email αποστέλλονταν χρησιμοποιώντας το λογισμικό και τη διεπαφή προγραμματισμού εφαρμογών (API) του SendGrid.

Το τμήμα Ανθρώπινου Δυναμικού εγγράφει κάθε νέο υπάλληλο και αυτό ενεργοποιεί αυτόματα ένα email για το τμήμα IT που περιέχει τον ρόλο και τα στοιχεία πρόσβασης του νέου υπαλλήλου. Δεν υπάρχουν πλέον καθυστερήσεις μεταξύ της ένταξης ενός υπαλλήλου και της παροχής πρόσβασης.

Αφού ένας εργαζόμενος επισημανθεί ότι έχει αποχωρήσει ή είναι ανενεργός, το σύστημα στέλνει αυτές τις πληροφορίες αμέσως στο τμήμα IT, το οποίο στη συνέχεια αφαιρεί τα διαπιστευτήρια πρόσβασης και ξεκινά την ανάκτηση του εξοπλισμού IT. Οι εταιρείες στέλνουν email υπενθύμισης τόσο στα μέλη του προσωπικού τους όσο και στους προϊσταμένους τους, εάν ορισμένα περιουσιακά στοιχεία δεν έχουν επιστραφεί εντός της καθορισμένης προθεσμίας.

Τα σενάρια ανωμαλιών παρακολουθούν τι συμβαίνει στο σύστημα και εκδίδουν σημαίες όταν εντοπίζουν ασυνήθιστες ενέργειες, όπως χρήστες που προσπαθούν να συνδεθούν παρά το γεγονός ότι είναι ανενεργοί, κλιμακώσεις ρόλων που πραγματοποιούνται χωρίς βάσιμο λόγο ή πάρα πολλές προσπάθειες σύνδεσης που δεν ολοκληρώνονται με επιτυχία. Αυτά παρατίθενται στον πίνακα ελέγχου διαχειριστή και διατηρούνται επίσης ως αρχείο για ελέγχους αργότερα. Το σύστημα ειδοποιήσεων σημαίνει ότι οι οργανισμοί είναι ασφαλέστεροι και πιο προστατευμένοι, ακόμη και όταν η παρακολούθηση από ανθρώπους δεν είναι δυνατή όλη την ώρα.



Σχήμα 5.2 Διάγραμμα ροής για συμβάντα αυτοματισμού

5.3 Λειτουργίες CRUD για Χρήστες, Συστήματα και Εξοπλισμό

Το σύστημα βασίζεται κυρίως στην ικανότητά του να χειρίζεται λειτουργίες όπως Δημιουργία, Ανάγνωση, Ενημέρωση, Διαγραφή (CRUD). Η πρόσβαση βάσει ρόλων είναι στενά ενσωματωμένη με αυτές τις λειτουργίες, οι οποίες εκτίθενται ως RESTful API.

Το προσωπικό του τμήματος ανθρώπινου δυναμικού μπορεί να προσθέσει και να διαχειριστεί εύκολα προφίλ υπαλλήλων στη μονάδα διαχείρισης χρηστών. Οι πληροφορίες που εισάγονται στα αρχεία των

υπαλλήλων καλύπτουν το όνομα, το τμήμα, το email, την επαγγελματική ιδιότητα και τη θέση του εργαζομένου. Οι υπάλληλοι μπορούν να απενεργοποιηθούν αντί να διαγραφούν, για να διασφαλιστεί ότι τα αρχεία καταγραφής τους διατηρούνται. Αυτό σημαίνει ότι τα ίχνη ελέγχου διατηρούνται ασφαλή ακόμη και όταν η πρόσβαση στο σύστημα έχει χαθεί.

Οι διαχειριστές μπορούν να χρησιμοποιήσουν τη μονάδα πρόσβασης συστήματος, που προορίζεται για το τμήμα IT, για να παραχωρήσουν συγκεκριμένα συστήματα στους υπαλλήλους (VPN, ERP, εσωτερικές πύλες) ανάλογα με τα καθήκοντά τους. Οι ρόλοι μπορούν να αλλάξουν ανάλογα με τις ανάγκες, πράγμα που σημαίνει ότι τα δικαιώματα πρόσβασης ενδέχεται να τροποποιηθούν ή να αφαιρεθούν αμέσως σε περίπτωση κακής χρήσης τους ή ενεργοποίησης συναγερμού. Οι διοικητικές αναφορές δείχνουν τις ενημερώσεις και τον τρόπο με τον οποίο επηρεάζουν την επιχείρηση.

Το προσωπικό IT μπορεί να χρησιμοποιήσει τη μονάδα παρακολούθησης εξοπλισμού για να εισάγει στοιχεία για κάθε νέα συσκευή, συμπεριλαμβανομένου του σειριακού αριθμού της. Οι εργαζόμενοι παραλαμβάνουν τα περιουσιακά τους στοιχεία κατά την έναρξη της εργασίας τους και καταγράφεται η ώρα παραλαβής και επιστροφής τους. Η παρακολούθηση συντήρησης και αποκατάστασης είναι δυνατή επιτρέποντας στο προσωπικό IT να παρακολουθεί την κατάσταση κάθε περιουσιακού στοιχείου και να ελέγχει ολόκληρο το ιστορικό του.

Όλες οι ενέργειες CRUD προστατεύονται από επαλήθευση στον διακομιστή και έλεγχο ταυτότητας διακριτικών, επομένως μόνο οι εξουσιοδοτημένοι χρήστες μπορούν να ενεργήσουν σε αυτές σύμφωνα με τους ρόλους τους.

Πίνακας 5.1 Πίνακας CRUD με οντότητες και λειτουργίες

Οντότητα	Create	Read	Update	Delete
Υπάλληλος	✓	✓	✓	✗(Απενεργοποίηση)
Εξοπλισμός	✓	✓	✓	✓
Δικαιώματα πρόσβασης	✓	✓	✓	✓
Ειδοποιήσεις	✓	✓	✗	✓

5.4 Ασφαλής καταγραφή ιχνών ελέγχου

Ένα σημαντικό μέρος της χρήσης του συστήματος είναι η συμπερίληψη ενός ασφαλούς και λεπτομερούς μηχανισμού καταγραφής. Αυτό βοηθά την πλατφόρμα να παραμένει υπόλογη, διαφανής και εντός των κανονισμών. Καθώς η πρόσβαση στα δικαιώματα των εργαζομένων και η έκδοση ή ο τερματισμός της χρήσης της συσκευής μπορεί να είναι ευαίσθητα ζητήματα, το σύστημα θα πρέπει να δημιουργεί ένα λεπτομερές αρχείο όλων των σημαντικών ενεργειών που πραγματοποιούνται από τους χρήστες.

Επίσης, οποιαδήποτε αλλαγή στο σύστημα καταγράφεται αμέσως με μια εκτενή λίστα λεπτομερειών σχετικά με την αλλαγή. Τέτοιες ενέργειες καλύπτουν την εγγραφή και τις συνδέσεις για τους χρήστες, τις αλλαγές στο ποιος έχει πρόσβαση στα δεδομένα, τη διανομή και την απόσυρση συσκευών και τις διαγραφές κύριων αρχείων. Κάθε στοιχείο στο αρχείο καταγραφής ελέγχου περιλαμβάνει την ακριβή ώρα που έλαβε χώρα η ενέργεια για να διασφαλιστεί ότι το αρχείο καταγραφής είναι εντάξει. Όλα τα συμβάντα καταγράφουν το όνομα του ατόμου που εκτελεί την ενέργεια και κάθε ενέργεια συνδέεται με μια επαληθευμένη συνεδρία στο σύστημα. Επειδή ο χρήστης και η ενέργεια συνδέονται, αυτό υποστηρίζει τους κατάλληλους ελέγχους εντός του οργανισμού, καθώς και τους ελέγχους από εξωτερικούς ρυθμιστικούς φορείς.

Εκτός από την καταγραφή ενεργειών όπως η δημιουργία, η ενημέρωση ή η διαγραφή, το σύστημα παρακολουθεί επίσης τον συγκεκριμένο στόχο. Ας υποθέσουμε ότι ένας υπάλληλος λαμβάνει έναν νέο φορητό υπολογιστή από τον διαχειριστή και το αρχείο καταγραφής θα καταγράφει το αναγνωριστικό του υπαλλήλου, το αναγνωριστικό περιουσιακού στοιχείου και τον τύπο της αλλαγής. Όποτε είναι δυνατόν, η δραστηριότητα καταγράφει μαζί τόσο τη διεύθυνση IP όσο και το διακριτικό περιόδου σύνδεσης. Με αυτές τις πληροφορίες, είναι ευκολότερο να αποκαλυφθεί η πηγή τυχόν πιθανών προβλημάτων, κάτι που είναι χρήσιμο για τη διερεύνηση συμβάντων.

Για να διασφαλιστεί η σωστή καταγραφή ελέγχου, κάθε καταχώρηση καταγραφής μεταφέρεται σε έναν ξεχωριστό πίνακα βάσης δεδομένων μόνο για εγγραφή, ο οποίος είναι λογικά και φυσικά ξεχωριστός από άλλους πίνακες ημερήσιας βάσης δεδομένων. Εξαιτίας αυτού, τόσο οι τυπικοί χρήστες όσο και όσοι έχουν εκτεταμένο έλεγχο δεν μπορούν να τροποποιήσουν, να αντικαταστήσουν ή να διαγράψουν πληροφορίες καταγραφής ελέγχου. Η δυσκολία τροποποίησης των καταχωρίσεων καταγραφής προστατεύει την ακεραιότητα όλων των δεδομένων και εγγυάται την ακρίβειά τους. Ο αυστηρός διαχωρισμός καθηκόντων είναι το κλειδί για την εναρμόνιση με πολλούς κανονισμούς, όπως αυτούς του ISO, του GDPR και των εταιρικών κανόνων.

Μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στα αρχεία καταγραφής ελέγχων μέσω μιας διεπαφής με εργαλεία προηγμένης αναζήτησης. Οι χρήστες με άδεια αναθεώρησης αρχείων καταγραφής, όπως οι υπεύθυνοι συμμόρφωσης ή οι επικεφαλής στην τεχνολογία πληροφοριών, μπορούν να χρησιμοποιήσουν παραμέτρους όπως το εύρος ημερομηνιών, το ποιος εκτέλεσε τη δραστηριότητα, τον τύπο ενέργειας ή τον συγκεκριμένο στόχο για να αναζητήσουν τα αρχεία καταγραφής. Ως ένα άλλο παράδειγμα, ένας διαχειριστής μπορεί να βρει όλες τις ανακλήσεις πρόσβασης από τον τελευταίο μήνα ή να ελέγξει όλες τις συσκευές που εκδόθηκαν από ένα δεδομένο μέλος του προσωπικού IT. Λόγω αυτών των λειτουργιών, τα εργαλεία SIEM είναι χρήσιμα τόσο για την παρακολούθηση των τρεχουσών δραστηριοτήτων όσο και για τη διερεύνηση προηγούμενων συμβάντων που σχετίζονται με περιστατικά ασφαλείας ή ελέγχους συμμόρφωσης.

Η ασφαλής καταγραφή της διαδρομής ελέγχου βοηθά το σύστημα να παραμένει διαφανές και αξιόπιστο και παρέχει επίσης στους οργανισμούς ένα αξιόπιστο σύστημα διαχείρισης κινδύνων. Συνδυάζει την

κατάλληλη τεχνική ρύθμιση με κορυφαία πρότυπα κυβερνοασφάλειας και διακυβέρνησης δεδομένων, γεγονός που το καθιστά κατάλληλο για χρήση σε χώρους που επικεντρώνονται στην λογοδοσία και τη συμμόρφωση. Καθώς είναι σταθερό και παρακολουθεί τα πάντα στενά, η διαδρομή ελέγχου επιτρέπει στους οργανισμούς να τηρούν τις πολιτικές, να εντοπίζουν τυχόν καταχρήσεις και να παραμένουν συμμορφούμενες με τους κανονισμούς. Κατά την υλοποίηση, οι μηχανικοί συστήματος μετέτρεψαν την ιδέα σε κάτι που οι άνθρωποι θα μπορούσαν πραγματικά να χρησιμοποιήσουν. Οι διεπαφές για συγκεκριμένους ρόλους, οι μηχανές αυτοματισμού, η ασφαλής διαχείριση δεδομένων και οι λεπτομερείς διαδρομές ελέγχου δημιουργήθηκαν χρησιμοποιώντας την τρέχουσα, κλιμακούμενη ανάπτυξη ιστού. Επειδή η εφαρμογή είναι αρθρωτή, οι ενημερώσεις ή οι αλλαγές σε διαφορετικά μέρη δεν επηρεάζουν τη λειτουργία άλλων στοιχείων. Χρησιμοποιώντας αυτήν την υλοποίηση, οι ομάδες HR και IT μπορούν να έχουν ομαλότερες ροές εργασίας, βελτιωμένη ασφάλεια και να ελέγχουν όλες τις απαιτήσεις ελέγχου. Σε αυτό το σημείο, οι αρχιτεκτονικές αποφάσεις επηρεάζουν πιθανές αναβαθμίσεις, όπως εφαρμογές για κινητά, ασφαλέστερη σύνδεση δύο παραγόντων ή εργαλεία παρακολούθησης.

Κεφάλαιο 6ο: Δοκιμές και Αξιολόγηση

Η διαδικασία δοκιμών και αξιολόγησης αποτελεί κρίσιμο στάδιο σε κάθε πληροφοριακό σύστημα, καθώς μέσω αυτής επιβεβαιώνεται η αξιοπιστία, η σταθερότητα και η ασφάλεια της λύσης πριν τεθεί σε παραγωγική λειτουργία. Το Σύστημα Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού δοκιμάστηκε εκτενώς, προκειμένου να διασφαλιστεί ότι ανταποκρίνεται στις απαιτήσεις που τέθηκαν στα προηγούμενα στάδια σχεδιασμού και υλοποίησης. Οι δοκιμές εστίασαν τόσο στην ορθότητα και πληρότητα της λειτουργικότητας όσο και στην απόδοση, την ασφάλεια και τη χρηστικότητα για τους τελικούς χρήστες.

6.1 Στόχοι Δοκιμών

Οι στόχοι των δοκιμών επικεντρώθηκαν σε τέσσερις βασικούς άξονες. Πρώτον, στην επαλήθευση ότι όλες οι βασικές λειτουργίες του συστήματος, όπως η εγγραφή νέου προσωπικού, η εκχώρηση δικαιωμάτων πρόσβασης και η διαχείριση εξοπλισμού, εκτελούνται σωστά και χωρίς σφάλματα. Δεύτερον, στη διασφάλιση ότι η πλατφόρμα παραμένει σταθερή και αποδοτική ακόμη και σε περιόδους υψηλού φόρτου, όπως κατά την ταυτόχρονη ένταξη πολλών υπαλλήλων ή την εκτέλεση μαζικών αναφορών. Τρίτον, στην εξέταση της ασφάλειας και της προστασίας των δεδομένων, με έμφαση στους μηχανισμούς αυθεντικοποίησης, εξουσιοδότησης και καταγραφής. Τέταρτον, στην αξιολόγηση της εμπειρίας χρήσης από την πλευρά του HR και του IT, ώστε να διαπιστωθεί αν το εργαλείο είναι πράγματι φιλικό και αποδοτικό στην καθημερινή εργασία.

6.2 Μεθοδολογία Δοκιμών

Η μεθοδολογία που ακολουθήθηκε ήταν πολυεπίπεδη και συνδύασε διαφορετικά είδη ελέγχων. Στο πρώτο στάδιο πραγματοποιήθηκαν δοκιμές μονάδων, οι οποίες στόχευαν στον έλεγχο μεμονωμένων λειτουργιών και μεθόδων. Εξετάστηκε, για παράδειγμα, αν η διαδικασία δημιουργίας υπαλλήλου επιστρέφει το σωστό αναγνωριστικό και αν οι μηχανισμοί επικύρωσης αποτρέπουν ελλιπή ή εσφαλμένα δεδομένα.

Στη συνέχεια ακολούθησαν δοκιμές ενσωμάτωσης, που έλεγξαν την αλληλεπίδραση μεταξύ διαφορετικών ενοτήτων. Ένα χαρακτηριστικό σενάριο ήταν η προσθήκη υπαλλήλου από το HR, η αυτόματη ειδοποίηση του IT και η εκχώρηση εξοπλισμού και δικαιωμάτων, με παράλληλη ενημέρωση του συστήματος ειδοποιήσεων.

Έπειτα, οι δοκιμές συστήματος εστίασαν στο σύνολο της εφαρμογής, αναπαράγοντας πλήρεις ροές εργασίας όπως η αποχώρηση υπαλλήλου και η επιστροφή συσκευών. Σε αυτό το στάδιο ελέγχθηκε ότι δεν δημιουργούνται ασυνέπειες στα δεδομένα, ότι τα αρχεία καταγραφής ενημερώνονται σωστά και ότι η αλληλουχία των ενεργειών ανταποκρίνεται στις προδιαγραφές.

Τέλος, υλοποιήθηκαν δοκιμές αποδοχής χρηστών (User Acceptance Testing – UAT), στις οποίες συμμετείχαν στελέχη HR και IT. Οι χρήστες κλήθηκαν να χρησιμοποιήσουν την πλατφόρμα σε σενάρια καθημερινής εργασίας, ώστε να αξιολογηθεί η ευχρηστία, η σαφήνεια της διεπαφής και η συνολική εμπειρία.

6.3 Λειτουργικές δοκιμές

Οι λειτουργικές δοκιμές έδειξαν στην πράξη πώς ανταποκρίνεται το σύστημα στις επιχειρησιακές ανάγκες. Η ενότητα διαχείρισης υπαλλήλων δοκιμάστηκε με σενάρια προσθήκης νέου προσωπικού,

ενημέρωσης υπαρχόντων στοιχείων και αλλαγής της κατάστασης απασχόλησης. Ελέγχθηκε επίσης η δυνατότητα αναζήτησης με βάση το τμήμα ή την κατάσταση (ενεργός, ανενεργός).

Στην ενότητα ελέγχου πρόσβασης εξετάστηκαν περιπτώσεις εκχώρησης νέων δικαιωμάτων, τροποποίησης υπαρχόντων και ανάκλησης όταν εργαζόμενος αποχωρεί. Παράλληλα, πραγματοποιήθηκαν δοκιμές απόπειρας μη εξουσιοδοτημένης πρόσβασης, οι οποίες απέτυχαν όπως αναμενόταν, αποδεικνύοντας την ορθότητα της λογικής RBAC.

Για την παρακολούθηση εξοπλισμού, ελέγχθηκαν η καταχώρηση νέων συσκευών, η εκχώρησή τους σε υπαλλήλους, η επισήμανση καθυστερημένων επιστροφών και η απεικόνιση της κατάστασης κάθε αντικειμένου.

Τέλος, εξετάστηκε η ενότητα καταγραφής ελέγχου. Επιβεβαιώθηκε ότι όλες οι κρίσιμες ενέργειες, από τις συνδέσεις χρηστών μέχρι τις αλλαγές πρόσβασης και τη διαχείριση εξοπλισμού, αποθηκεύονται με λεπτομέρειες, χρονοσήμανση και συσχέτιση με τον χρήστη που τις εκτέλεσε.

6.4 Δοκιμές απόδοσης και φορτίου

Η απόδοση και η αντοχή του συστήματος αξιολογήθηκαν μέσω προσομοιώσεων με αυξημένο φόρτο. Σε σενάριο μαζικής ένταξης, καταχωρήθηκαν περισσότερα από 200 νέα προφίλ υπαλλήλων σε σύντομο χρονικό διάστημα. Όλες οι ενέργειες εκτελέστηκαν ομαλά: δημιουργήθηκαν δικαιώματα, καταχωρήθηκε εξοπλισμός και στάλθηκαν ειδοποιήσεις χωρίς καθυστερήσεις.

Για να αξιολογηθεί η αντοχή υπό ταυτόχρονες προσβάσεις, χρησιμοποιήθηκε το Apache JMeter. Προσομοιώθηκαν 1.000 ταυτόχρονες λειτουργίες, οι οποίες περιλάμβαναν αιτήματα για εκχώρηση εξοπλισμού, ανάκτηση δεδομένων και ελέγχους πρόσβασης. Το σύστημα ανταποκρίθηκε ικανοποιητικά, χωρίς να προκύψουν σφάλματα ή σημαντικές καθυστερήσεις.

Η μόνη βελτίωση που κρίθηκε απαραίτητη αφορούσε τις ρυθμίσεις pooling συνδέσεων της βάσης δεδομένων, οι οποίες προσαρμόστηκαν ώστε να αποφευχθεί υπερφόρτωση σε ακραίες περιπτώσεις. Είναι σημαντικό να τονιστεί ότι στην πράξη δεν αναμένεται το σύστημα να λειτουργεί σε τόσο απαιτητικές συνθήκες, καθώς πρόκειται για υποστηρικτικό εργαλείο και όχι για core επιχειρησιακό σύστημα. Παρ' όλα αυτά, τα αποτελέσματα δείχνουν ότι διαθέτει αξιόλογες δυνατότητες κλιμάκωσης.

6.5 Δοκιμές ασφαλείας

Δεδομένης της φύσης των δεδομένων, οι δοκιμές ασφαλείας είχαν ιδιαίτερη βαρύτητα. Ελέγχθηκε ότι όλες οι συνδέσεις πραγματοποιούνται μέσω πρωτοκόλλου HTTPS, με χρήση SSL/TLS, εξασφαλίζοντας την προστασία από υποκλοπές και επιθέσεις man-in-the-middle.

Οι μηχανισμοί RBAC επιβεβαιώθηκαν με σενάρια μη εξουσιοδοτημένων ενεργειών: HR που προσπαθεί να αλλάξει δικαιώματα συστήματος ή IT που επιχειρεί να τροποποιήσει προσωπικά δεδομένα. Σε όλες τις περιπτώσεις, οι προσπάθειες απορρίφθηκαν.

Δοκιμάστηκαν επίσης σενάρια SQL Injection, Cross-Site Scripting (XSS) και Cross-Site Request Forgery (CSRF) με τη βοήθεια εργαλείων όπως το OWASP ZAP. Τα εντοπισμένα ζητήματα διορθώθηκαν πριν από την παραγωγική χρήση.

Τέλος, επιβεβαιώθηκε ότι οι κωδικοί πρόσβασης αποθηκεύονται μόνο σε κατακερματισμένη μορφή με χρήση αλγορίθμου bcrypt και μοναδικά salts, χωρίς να είναι ποτέ διαθέσιμοι σε απλό κείμενο.

6.6 Αξιολόγηση Χρηστικότητας

Η αξιολόγηση χρηστικότητας πραγματοποιήθηκε μέσω δοκιμών αποδοχής χρηστών. Στελέχη HR και IT χρησιμοποίησαν την πλατφόρμα για καθημερινές εργασίες όπως η ένταξη νέου προσωπικού, η εκχώρηση εξοπλισμού και η διαχείριση αποχωρήσεων.

Η γενική εικόνα ήταν ιδιαίτερα θετική. Οι χρήστες εκτίμησαν τη σαφήνεια του συστήματος, τη λογική ροή των εργασιών και την ταχύτητα απόκρισης. Παράλληλα, διατυπώθηκαν προτάσεις βελτίωσης, όπως η προσθήκη συμβουλών (tooltips) σε κρίσιμα πεδία, η ύπαρξη έτοιμων επιλογών για συχνές εργασίες και η εντονότερη επισήμανση σε περιπτώσεις επειγόντων ειδοποιήσεων. Οι παρατηρήσεις αυτές δύνανται να ενσωματωθούν πριν από την τελική διάθεση.

Η χρηστικότητα επιβεβαιώθηκε και με αντικειμενικά κριτήρια, όπως ο χρόνος ολοκλήρωσης εργασιών, ο αριθμός λαθών κατά την εισαγωγή και το επίπεδο εμπιστοσύνης που δήλωσαν οι χρήστες. Σε όλα τα σημεία τα αποτελέσματα ήταν ικανοποιητικά.

6.7 Αποτελέσματα Αξιολόγησης

Τα συνολικά αποτελέσματα των δοκιμών ήταν ιδιαίτερα θετικά. Όλες οι βασικές λειτουργίες λειτούργησαν χωρίς σφάλματα, το σύστημα απέδωσε σταθερά ακόμη και σε απαιτητικές συνθήκες, οι μηχανισμοί ασφαλείας αποδείχθηκαν αποτελεσματικοί και η εμπειρία χρήσης κρίθηκε θετική από τους τελικούς χρήστες. Δεν εντοπίστηκαν σοβαρά προβλήματα και τα μικρότερα ζητήματα διορθώθηκαν πριν την τελική διάθεση. Το σύστημα θεωρείται έτοιμο για χρήση σε οργανισμούς μεσαίου και μεγάλου μεγέθους.

6.8 Σύνοψη

Συνοψίζοντας, οι δοκιμές και η αξιολόγηση κατέδειξαν ότι το Σύστημα Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού είναι ένα ολοκληρωμένο, αξιόπιστο και ασφαλές εργαλείο. Η πλατφόρμα απέδειξε ότι μπορεί να χειριστεί μαζικές διαδικασίες, να προστατεύσει αποτελεσματικά τα δεδομένα και να προσφέρει ένα φιλικό και κατανοητό περιβάλλον εργασίας. Η ευελιξία της αρχιτεκτονικής και η επιτυχής ανταπόκριση στις δοκιμές δημιουργούν στέρεες βάσεις για μελλοντική επέκταση και προσαρμογή σε νέες ανάγκες, ενώ η θετική αποδοχή από τους τελικούς χρήστες επιβεβαιώνει ότι το σύστημα ανταποκρίνεται στις πραγματικές απαιτήσεις του οργανισμού.

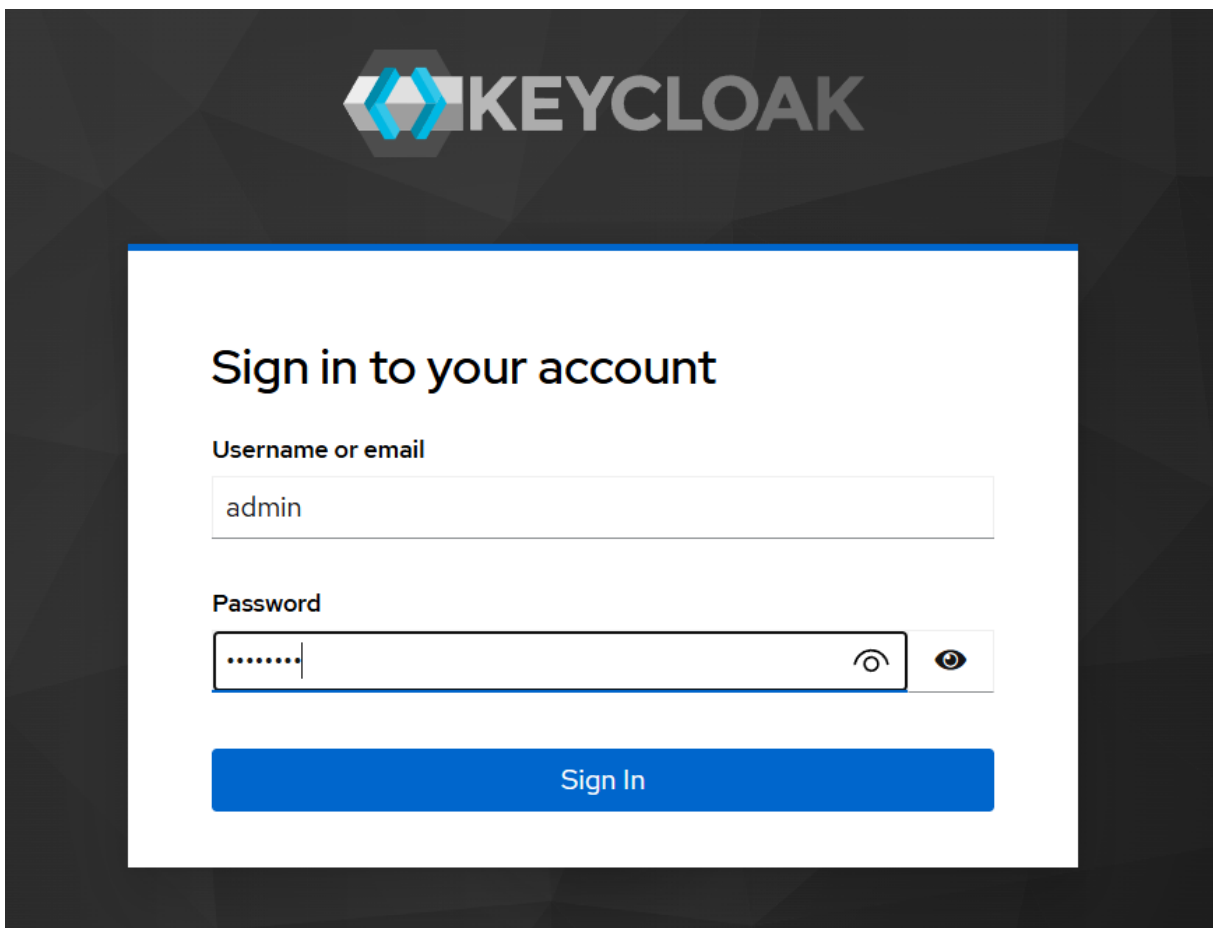
Κεφάλαιο 7ο: Παρουσίαση Εφαρμογής

Στο κεφάλαιο αυτό παρουσιάζεται αναλυτικά η λειτουργικότητα της εφαρμογής που αναπτύχθηκε. Στόχος είναι να αναδειχθεί πώς οι θεωρητικές προδιαγραφές και ο σχεδιασμός που περιγράφηκαν στα προηγούμενα κεφάλαια εφαρμόζονται σε ένα πραγματικό σύστημα, το οποίο μπορεί να χρησιμοποιηθεί από μια επιχείρηση για τη διαχείριση εξοπλισμού και προσβάσεων.

Η παρουσίαση γίνεται με πρακτικά παραδείγματα, μέσα από στιγμιότυπα οθόνης (screenshots), τα οποία απεικονίζουν τις κύριες διαδικασίες της εφαρμογής. Παρουσιάζονται οι δυνατότητες του διαχειριστή (administrator), καθώς από αυτόν εξαρτάται η αρχική παραμετροποίηση και η συνολική εποπτεία.

7.1 Είσοδος στο σύστημα

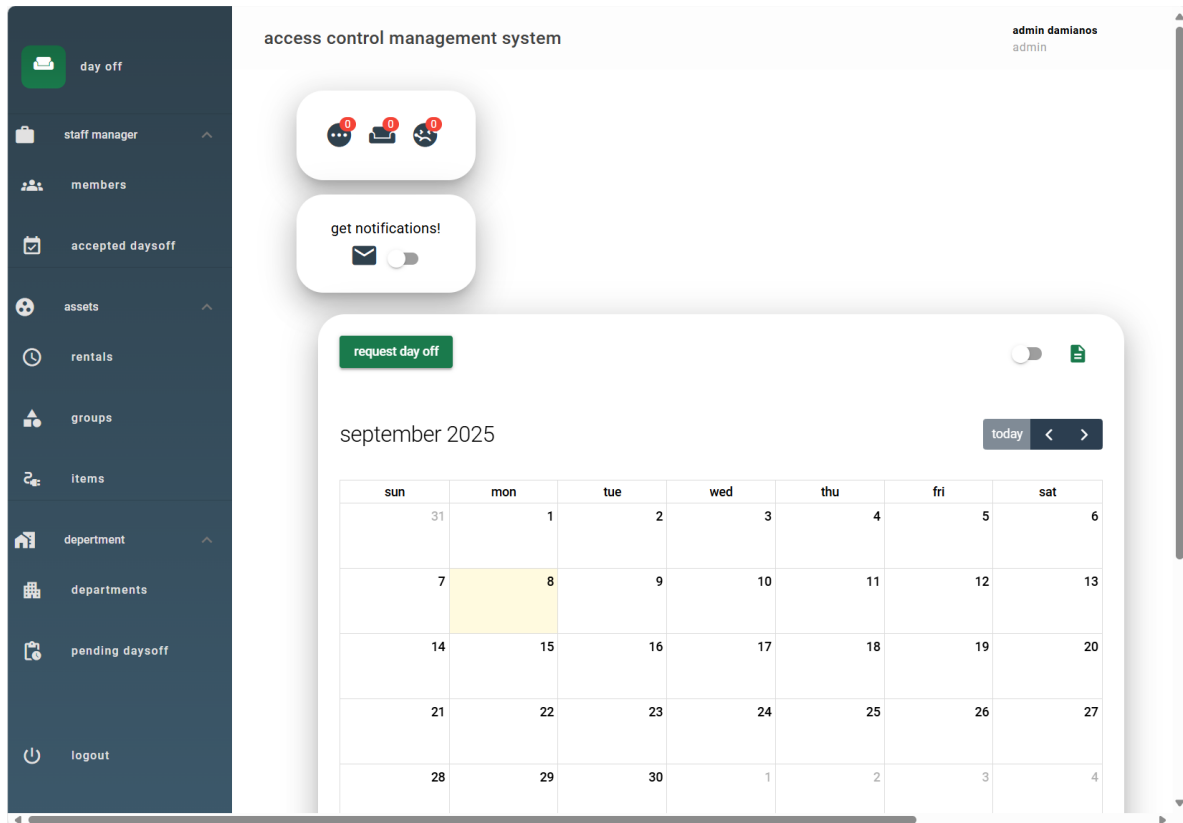
Η πρώτη επαφή με την εφαρμογή ξεκινά από την οθόνη σύνδεσης. Ο χρήστης καλείται να εισαγάγει τα στοιχεία του (username και password), τα οποία ελέγχονται από το σύστημα αυθεντικοποίησης Keycloak. Στο παράδειγμα που ακολουθεί (Σχήμα 7.1), η είσοδος πραγματοποιείται με τα στοιχεία του admin, έτσι ώστε να φανούν οι δυνατότητες διαχείρισης.



Σχήμα 7.1 Login συστήματος

Στη συνέχεια με το επιτυχές login ανακατευθυνόμαστε στο dashboard του συστήματος, στο Σχήμα 7.2 φαίνεται το μενού πλοήγησης. Στην κορυφή υπάρχει η ενότητα “Days Off” η οποία αφορά την λειτουργία αίτησης ανάληψης ημερών αδειών από το προσωπικό. Στη συνέχεια υπάρχει η κατηγορία

“Staff Manager” με τις ενότητες “Members” και “Accepted Days Off” όπου αφορούν λειτουργίες προοριζόμενες για το τμήμα ανθρώπινου δυναμικού μιας επιχείρησης. Έπειτα στην κατηγορία “Assets” υπάρχουν οι ενότητες “Rentals”, “Groups” και “Items” τα οποία αφορούν κατανομή προσβάσεων και εξοπλισμού στο προσωπικό. Μετά στην κατηγορία “Department” υπάρχουν οι ενότητες “Departments” και “Pending Days Off”, και τέλος η επιλογή για logout από το σύστημα.



Σχήμα 7.2 Μενού πλοήγησης

7.2 Οργάνωση Επιχείρησης

Το σύστημα για να λειτουργήσει και να αποδώσει στην επιχείρηση την προστιθέμενη αξία για την οποία σχεδιάστηκε και δημιουργήθηκε, προϋποθέτει την κατάλληλη ενσωμάτωση πληροφοριών της εταιρίας. Έτσι, σαν πρώτο βήμα είναι η δημιουργία “Departments” τα οποία αντικατοπτρίζουν τα διακριτά τμήματα (οργανωτική δομή) που έχει η εταιρία. Από το μενού πλοήγησης επιλέγουμε “Departments” και επιλέγουμε “Create Department”. Οι πληροφορίες που ζητούνται (Σχήμα 7.3) είναι το όνομα του department και ο σχετικός υπεύθυνος (πληροφορία η οποία μπορεί να αλλάξει σε μετέπειτα χρόνο).

Σχήμα 7.3 Δημιουργία Department

Στην παρούσα υλοποίηση έχουμε ήδη δημιουργήσει οκτώ διαφορετικά τμήματα (Σχήμα 7.4).

Σχήμα 7.4 Departments view

Επόμενο βήμα είναι η δημιουργία των χρηστών και ο κατάλληλος καταμερισμός τους στα τμήματα (departments) που έχουν δημιουργηθεί. Από το αρχικό μενού πλοήγησης επιλέγουμε “Members” και στη συνέχεια κάνουμε κλικ στο κουμπί «+» για δημιουργία χρήστη (Σχήμα 7.5). Θα ανοίξει ένα pop-up window στο οποίο εισάγουμε τα στοιχεία του ατόμου, τα οποία είναι ονοματεπώνυμο, διεύθυνση e-mail, ημερομηνία πρόσληψης, τμήμα στο οποίο ανήκει καθώς και ρόλος στο σύστημα (απλός χρήστης,

πλήρης διαχειριστής ή διαχειριστής προσωπικού). Το πεδίο “end deployment date” συμπληρώνεται μόνο στο ενδεχόμενο που αποχωρήσει το εν λόγω άτομο από την εταιρία.

add member

fullname

email

hired date

end employment date

department

role
user

admin

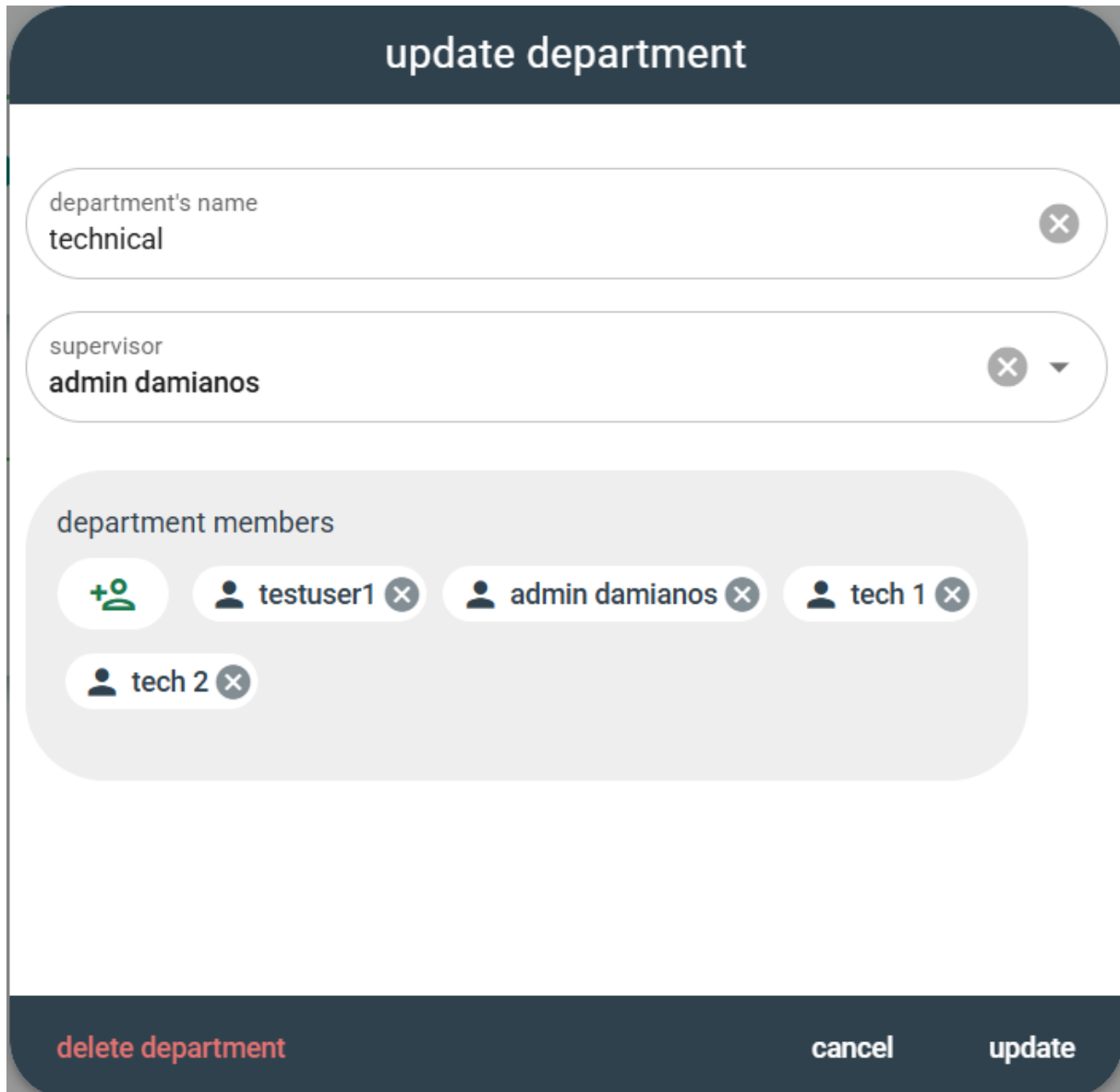
user

staffmanager

cancel save

Σχήμα 7.5 Προσθήκη member

Επίσης, ο ορισμός ενός εργαζομένου κάτω από ένα department δύναται να πραγματοποιηθεί απευθείας μέσω της επεξεργασίας του ίδιου department, προσθέτοντας το άτομο στη σχετική λίστα όπως αυτή φαίνεται στο Σχήμα 7.6 παρακάτω.



The screenshot displays a form titled "update department". It features three main input areas: a text field for "department's name" containing "technical", a dropdown menu for "supervisor" containing "admin damianos", and a "department members" section. The members section includes a "+o" icon for adding members and a list of existing members: "testuser1", "admin damianos", "tech 1", and "tech 2", each with a removal "x" icon. At the bottom, there are three buttons: "delete department" (in red), "cancel", and "update".

Σχήμα 7.6 Προσθήκη member σε department

Στο Σχήμα 7.7 παρακάτω απεικονίζεται ενδεικτική λίστα προσωπικού το οποίο έχει προστεθεί στο σύστημα. Με μια ματιά έχουμε όλες τις σημαντικές πληροφορίες συγκεντρωτικά για κάθε εργαζόμενο. Παρατηρήστε τη στήλη "actions" με το αντίστοιχο εικονίδιο, δίνονται επιλογές για άμεσες ενέργειες οι οποίες θα αναλυθούν στη συνέχεια.

full name	email	role	hire date	end employment date	department	supervisor	days off	actions
accounting manager	accmgr@company.gr	staffmanager	19-06-2019		accounting	accounting manager	0 holidays, 0 sickdays	edit rent item rental history update days off days off history
admin 2	admin2@test.user	admin					0 holidays, 0 si	
admin damianos	admin@company.gr	admin	01-01-1970		technical	admin damianos	0 holidays, 0 si	
admin damianos	admin@damin.gr	admin					0 holidays, 0 si	
dev 1	dev1@company.gr	user	10-09-2024		development		0 holidays, 0 sickdays	
hr manager	hr@company.gr	staffmanager	21-06-2022		hr	hr manager	0 holidays, 0 sickdays	
infrastructure mgr	infra@company.gr	user	21-09-2016		infrastructure	infrastructure mgr	0 holidays, 0 sickdays	
marketing 2	marketing2@company.gr	user	06-09-2023	08-09-2025	marketing	marketing1	0 holidays, 0 sickdays	
marketing1	marketing1@company.gr	user	15-09-2021		marketing	marketing1	0 holidays, 0 sickdays	
procurement manager	procurement@company.gr	user	06-08-2025		procurement	procurement manager	0 holidays, 0 sickdays	

Σχήμα 7.7 Λίστα προσωπικού (members)

7.3 Παραμετροποίηση Assets

Αφού έχουν δημιουργηθεί τα κατάλληλα τμήματα (departments) και έχει εισαχθεί το προσωπικό (members) στο σύστημα, σειρά έχει η εισαγωγή των assets. Τα assets χωρίζονται σε groups (Σχήμα 7.8), όπου το κάθε ένα group πρακτικά αφορά έναν και μόνο τύπο εξοπλισμού ή συστήματος.

title	group manager	no items	actions
erp	tech 1	1	
laptops	procurement manager	5	
mails	admin damianos	1	
vpn	tech 1	1	
crm	sales 1	1	
phones	procurement manager	3	

Σχήμα 7.8 Asset groups

Στο παράδειγμα ανωτέρω έχουμε δημιουργήσει 6 διαφορετικά asset groups. Κατά τη δημιουργία ενός group ορίζεται το όνομα και ο σχετικός υπεύθυνος διαχείρισης, ο οποίος είναι ένας εκ των members.

Εφόσον έχουν δημιουργηθεί τα επιθυμητά groups, μπορούμε να ξεκινήσουμε την εισαγωγή των διαθέσιμων στοιχείων τα οποία θα είναι προς διαμοιρασμό στους εργαζομένους. Τα items μπορεί να είναι δύο διακριτών τύπων:

- Asset (εξοπλισμός)
- System (Σύστημα)

Ως “Asset” καταχωρείται οποιοδήποτε κομμάτι φυσικού εξοπλισμού, όπως για παράδειγμα laptops και κινητά τηλέφωνα. Ως “System” καταχωρείται το σύστημα στο οποίο ο εκάστοτε εργαζόμενος ενδέχεται να αποκτήσει δικαίωμα λογικής πρόσβασης, όπως είναι για παράδειγμα η πρόσβαση στο ERP της εταιρίας και το εταιρικό e-mail. Στο Σχήμα 7.9 παρουσιάζονται τα εισαχθέντα items.

item	group	rented by	type	availability	actions
crm	crm		system		
erp	erp		system		
laptop-1	laptops		asset		
laptop-2	laptops		asset		
laptop-3	laptops	tech 1	asset		
laptop-4	laptops	tech 2	asset		

Σχήμα 7.9 Items - Εξοπλισμός & Συστήματα

Τα items μπορούν να απεικονίζονται είτε όλα μαζί σε μια ενιαία λίστα, είτε να φιλτράρονται βάσει του group στο οποίο ανήκουν (Σχήμα 7.10).

item	group	rented by	type	availability	actions
mail	mails		system		
phone-1	phones	sales 1	asset		
phone-2	phones		asset		
phone-3	phones		asset		

Σχήμα 7.10 Items - Φιλτράρισμα

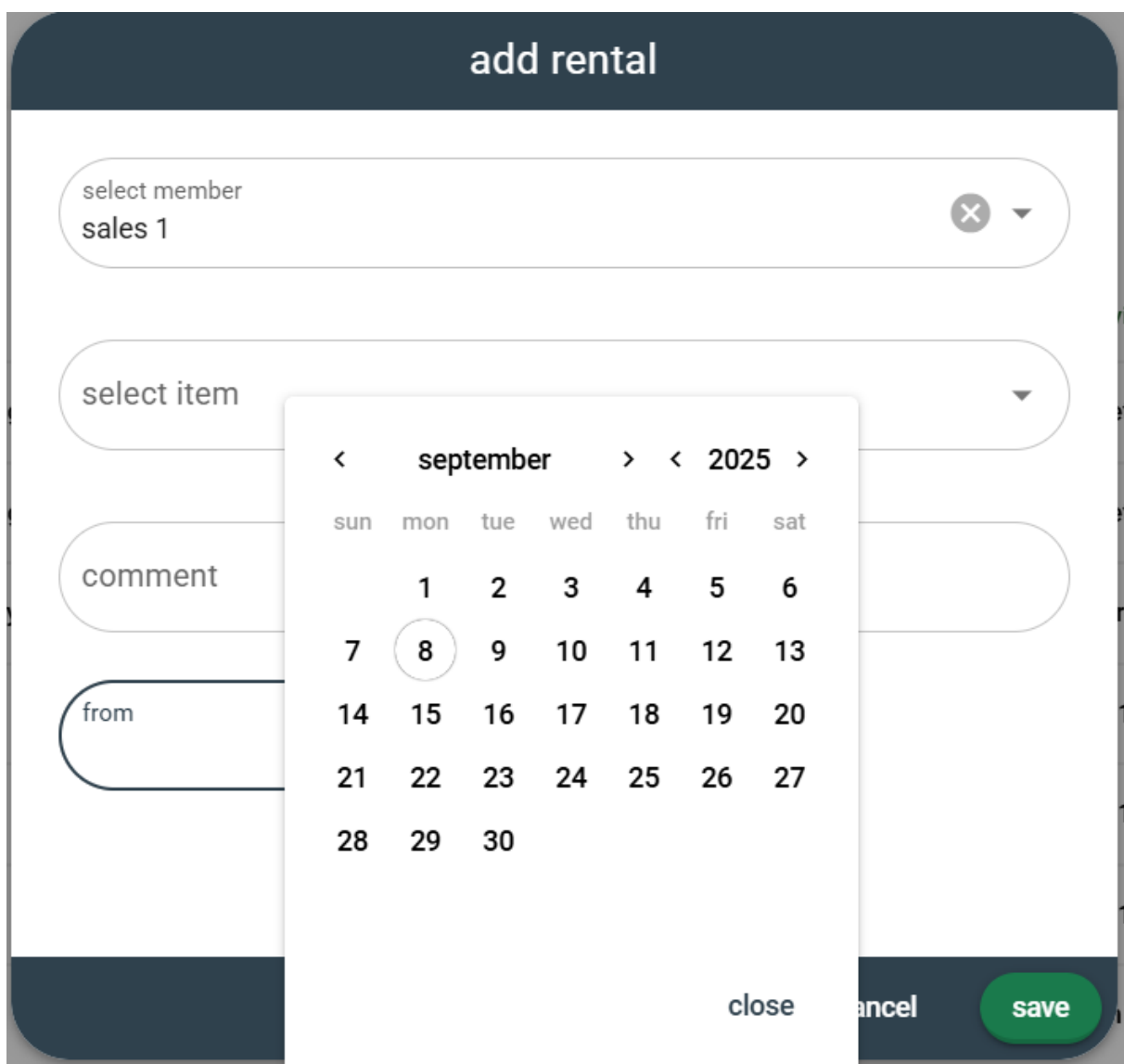
Με μια γρήγορη ματιά στα items έχουμε άμεση εποπτεία για το πλήθος του εξοπλισμού που διαθέτει η εταιρία. Παρατηρήστε τη στήλη “availability”, τα items τύπου asset παρουσιάζονται ως available ή unavailable ανάλογα αν έχουν αποδοθεί σε κάποιο άτομο. Αντιθέτως, τα items τύπου system, καθώς δεν πρόκειται για φυσικό εξοπλισμό αλλά για λογική παραχώρηση πρόσβασης με χρήση λογαριασμού, παρουσιάζονται με διαφορετικό εικονίδιο ως πάντα διαθέσιμα.

7.4 Διαδικασία απόδοσης εξοπλισμού

Έχοντας ολοκληρώσει την αρχική παραμετροποίηση με τα προαπαιτούμενα (δημιουργία departments, εισαγωγή members, καταχώρηση groups & items), μπορούμε να προχωρήσουμε σε απόδοση εξοπλισμού ή πρόσβασης σε σύστημα σε ένα άτομο της επιχείρησης.

7.4.1 Μέσω των members

Μπορούμε να αποδώσουμε απευθείας σε ένα άτομο της επιχείρησης ένα στοιχείο εξοπλισμού. Από το μενού πλοήγησης πηγαίνουμε στο “Members”, εντοπίζουμε το άτομο που μας ενδιαφέρει και από το κουμπί επιλογών επιλέγουμε “rent item” (Σχήμα 7.7). Αμέσως θα εμφανιστεί αντίστοιχο pop-up window (add rental) όπου επιλέγουμε από την drop down list το επιθυμητό item (δεν έχει σημασία αν είναι τύπου asset ή system) και ορίζουμε την ημερομηνία κτήσης (Σχήμα 7.11). Το άτομο στο οποίο πραγματοποιείται το rental συμπληρώνεται αυτόματα.



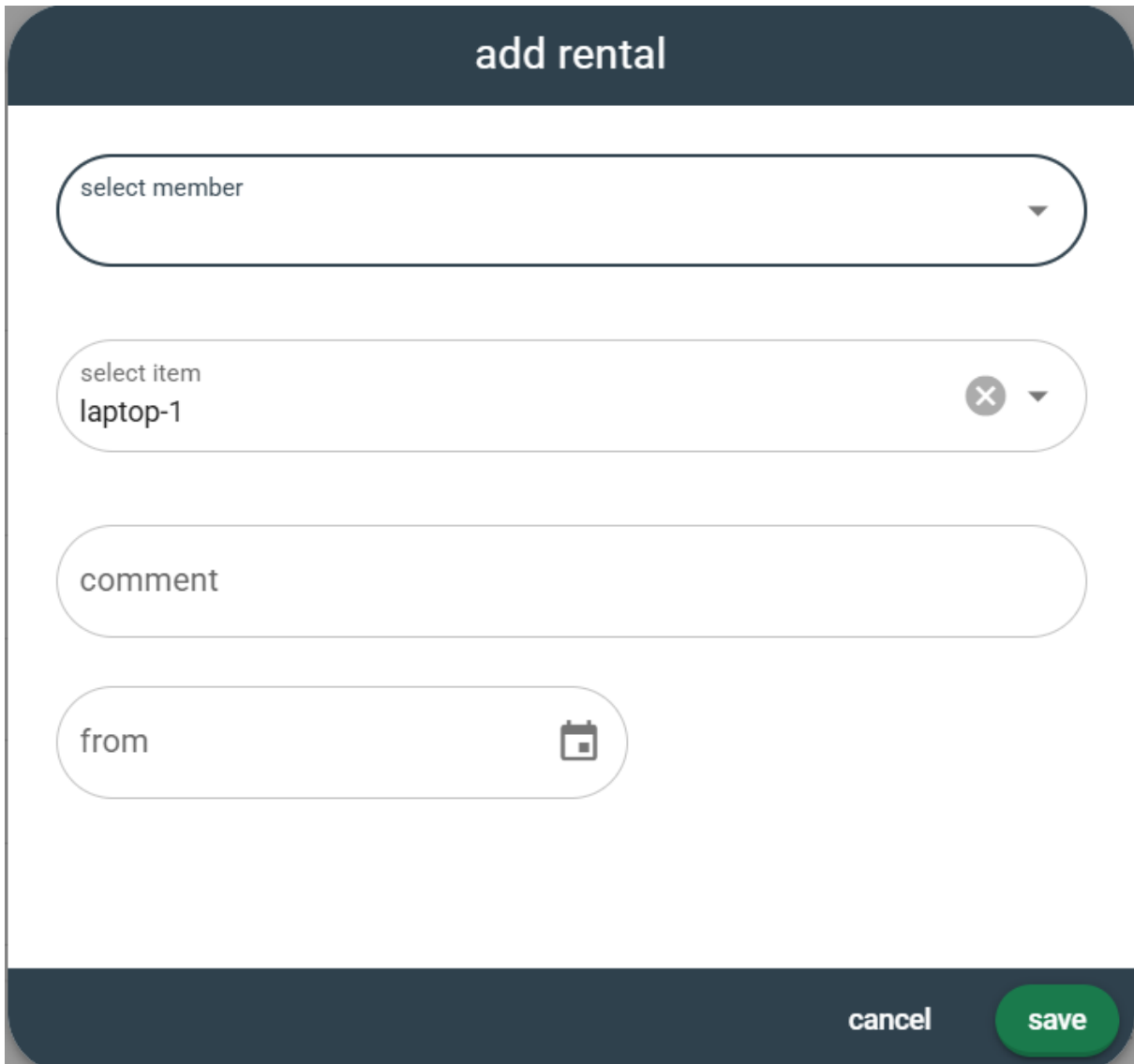
The screenshot shows a mobile application interface for adding a rental. The title is "add rental". There are four input fields: "select member" (with "sales 1" selected), "select item", "comment", and "from". A calendar is displayed over the "select item" field, showing the month of September 2025. The date "8" is selected. At the bottom, there are three buttons: "close", "cancel", and "save".

<	september	>	<	2025	>	
sun	mon	tue	wed	thu	fri	sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Σχήμα 7.11 Απόδοση εξοπλισμού σε άτομο

7.4.2 Μέσω των items

Μπορούμε να αποδώσουμε απευθείας ένα στοιχείο εξοπλισμού σε ένα άτομο της επιχείρησης. Από το μενού πλοήγησης πηγαίνουμε στο “Items”, εντοπίζουμε το item που μας ενδιαφέρει (δεν έχει σημασία αν είναι τύπου asset ή system) και από το κουμπί επιλογών επιλέγουμε “rent item” (Σχήμα 7.9). Αμέσως θα εμφανιστεί αντίστοιχο pop-up window (add rental) όπου επιλέγουμε από την drop down list τον επιθυμητό εργαζόμενο και ορίζουμε την ημερομηνία κτήσης (Σχήμα 7.12). Το item το οποίο δίνεται ως rental συμπληρώνεται αυτόματα.



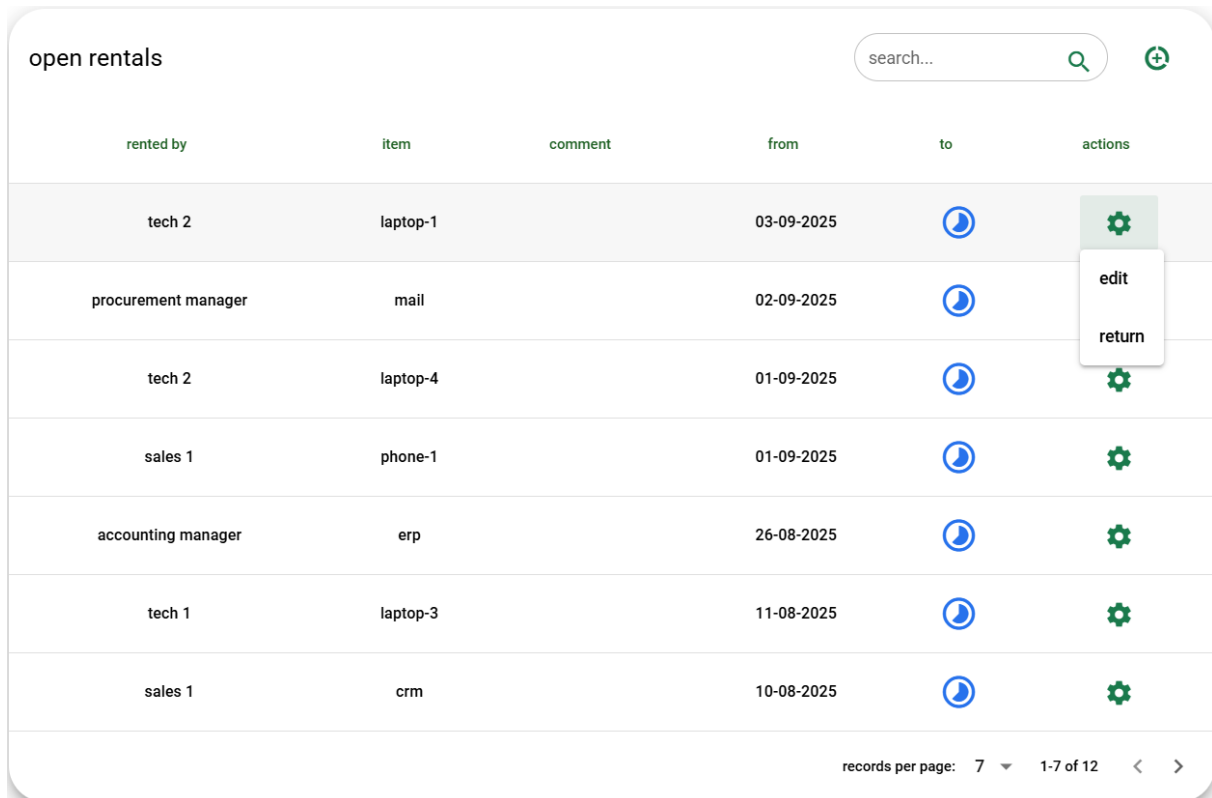
Σχήμα 7.12 Απόδοση εξοπλισμού σε άτομο – 2

7.5 Παρακολούθηση και Διαχείριση rentals

Έχοντας αποδώσει εξοπλισμό και προσβάσεις στο προσωπικό, θα πρέπει να είμαστε σε θέση ανά πάσα στιγμή να έχουμε την εποπτεία της υφιστάμενης κατάστασης. Για το λόγο αυτό έχει παραμετροποιηθεί στο σύστημα η δυνατότητα εμφάνισης του συνόλου των rentals προς το προσωπικό, όπως επίσης και το ιστορικό παράδοσης/επιστροφής.

7.5.1 Συνολικά rentals

Για να εμφανίσουμε το σύνολο των ενεργών rentals, από το κεντρικό μενού πλοήγησης θα επιλέξουμε “Rentals” (Σχήμα 7.13). Εμφανίζεται λίστα όλων των ενεργών rented items, συνοδευόμενα από το άτομο και την ημερομηνία κτήσης. Από το ίδιο περιβάλλον επίσης μπορούμε να κάνουμε «επιστροφή» του συγκεκριμένου εξοπλισμού εάν το θέλουμε (return από το μενού επιλογών του item), αποδεδεσμένοντας άμεσα το item και κάνοντάς το διαθέσιμο προς rent σε άλλο άτομο (για την περίπτωση που το item είναι τύπου asset).



rented by	item	comment	from	to	actions
tech 2	laptop-1		03-09-2025		edit return
procurement manager	mail		02-09-2025		
tech 2	laptop-4		01-09-2025		
sales 1	phone-1		01-09-2025		
accounting manager	erp		26-08-2025		
tech 1	laptop-3		11-08-2025		
sales 1	crm		10-08-2025		

records per page: 7 1-7 of 12 < >

Σχήμα 7.13 Λίστα ενεργών rentals

7.5.2 Rentals ανά member

Για κάθε άτομο που έχουμε δηλωμένο στο σύστημα, μπορούμε πολύ εύκολα να ανατρέξουμε και να ελέγξουμε το σύνολο των προσβάσεων/εξοπλισμού που διαθέτει την παρούσα στιγμή, όπως επίσης και να ανατρέξουμε στο ιστορικό παλαιότερων εγγραφών. Από το κεντρικό μενού πλοήγησης θα επιλέξουμε “Members”, θα εντοπίσουμε το άτομο που μας ενδιαφέρει και θα επιλέξουμε το “rental history” όπως φαίνεται στο Σχήμα 7.7. Αμέσως θα εμφανιστεί η λίστα με όλες τις εγγραφές που έχουν γίνει στο σύστημα και αφορούν τον συγκεκριμένο εργαζόμενο. Ο ενεργός εξοπλισμός/πρόσβαση σημειώνεται ως “renting is in progress”, ενώ για εξοπλισμό που έχει επιστραφεί αναγράφεται η ημερομηνία επιστροφής (Σχήμα 7.14).

rentals for member: **infrastructure mgr**

← back

item	from	to
phone-3	30-08-2023	renting is in progress
erp	10-06-2025	renting is in progress
laptop-2	10-07-2024	renting is in progress
laptop-1	01-09-2023	10-07-2024

records per page: 5 1-4 of 4

Σχήμα 7.14 Ιστορικό rentals ανά member

7.5.3 Ιστορικό rentals ανά item

Για κάθε item που έχουμε καταχωρημένο στο σύστημα, μπορούμε πολύ εύκολα να ανατρέξουμε στο ιστορικό παράδοσης και επιστροφής ανά των members. Από το κεντρικό μενού πλοήγησης θα επιλέξουμε “Items”, θα εντοπίσουμε το στοιχείο που μας ενδιαφέρει και θα επιλέξουμε το “rental history” όπως φαίνεται στο Σχήμα 7.9. Αμέσως θα εμφανιστεί η λίστα με όλο το ιστορικό κτήσης του συγκεκριμένου στοιχείου από όλα τα members του συστήματος. Φαίνεται η ημερομηνία κτήσης όπως επίσης και η ημερομηνία επιστροφής, και σε περίπτωση που την παρούσα στιγμή το στοιχείο χρησιμοποιείται από κάποιο άτομο θα αναγράφεται ως “renting is in progress” (Σχήμα 7.15).

rentals for item: **laptop-1**

rented by ↑	from	to
infrastructure mgr	01-09-2023	10-07-2024
tech 2	03-09-2025	renting is in progress
hr manager	12-08-2025	02-09-2025

records per page: 5 1-3 of 3

Σχήμα 7.15 Ιστορικό rentals ανά item

7.6 Σύνοψη

Με την παρουσίαση του συστήματος φάνηκε στην πράξη πώς οι θεωρητικοί στόχοι της εργασίας γίνονται λειτουργικό λογισμικό. Μέσα από τα screenshots και τις περιγραφές καλύφθηκαν όλα τα βασικά στάδια:

- Η αρχική παραμετροποίηση της εταιρείας με τμήματα και χρήστες.
- Η οργάνωση του εξοπλισμού και των συστημάτων σε groups και items.
- Η απόδοση assets ή προσβάσεων στο προσωπικό.
- Η εποπτεία σε πραγματικό χρόνο και η πρόσβαση σε πλήρες ιστορικό καταγραφών.

Η εφαρμογή δίνει στους διαχειριστές HR, IT αλλά και στους supervisors ένα εργαλείο που τους επιτρέπει να γνωρίζουν ανά πάσα στιγμή ποιος έχει ποια πρόσβαση και ποιον εξοπλισμό. Επιπλέον, προσφέρει απλότητα και σαφήνεια στη διαχείριση, μειώνοντας τον κίνδυνο λαθών.

Κεφάλαιο 7

Συνολικά, το κεφάλαιο αυτό απέδειξε ότι το σύστημα δεν είναι απλώς μια θεωρητική πρόταση αλλά ένα ολοκληρωμένο εργαλείο έτοιμο να υποστηρίξει την καθημερινή λειτουργία μιας επιχείρησης.

Την ίδια στιγμή, η παρουσίαση της εφαρμογής αναδεικνύει και ορισμένους τομείς που μπορούν να εξελιχθούν περαιτέρω. Η ενσωμάτωση πιο προηγμένων μηχανισμών ελέγχου, η ανάπτυξη mobile εφαρμογής ή η αξιοποίηση τεχνολογιών SSO (Single Sign-On) είναι ενδεικτικές κατευθύνσεις που θα μπορούσαν να βελτιώσουν ακόμη περισσότερο τη λειτουργικότητα και την εμπειρία των χρηστών.

Με βάση τα παραπάνω, το επόμενο κεφάλαιο εστιάζει στα συμπεράσματα της παρούσας εργασίας και στις μελλοντικές δυνατότητες ανάπτυξης, ώστε να δοθεί μια ολοκληρωμένη εικόνα για το πώς η εφαρμογή αυτή μπορεί να αποτελέσει θεμέλιο για επόμενες εκδόσεις και βελτιώσεις.

Κεφάλαιο 8ο: Περιορισμοί

Παρόλο που το Σύστημα Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού επιτυγχάνει τέλεια την ενσωμάτωση, τον έλεγχο και την παρακολούθηση, όλα τα συστήματα έχουν όρια που βασίζονται στον χρόνο, το πεδίο εφαρμογής, τις τεχνικές απαιτήσεις και τους πόρους. Ανεξάρτητα από αυτό, αυτά τα όρια δείχνουν πού πρέπει να αλλάξει η εφαρμογή για μελλοντικές ενημερώσεις. Η αναγνώριση αυτών των ορίων έχει σημασία για τα ενδιαφερόμενα μέρη, τους διαχειριστές και τους προγραμματιστές, επειδή τους καθοδηγεί στον καθορισμό στόχων και στον σχεδιασμό μελλοντικών βελτιώσεων. Το σύστημα χρησιμοποιείται αυτήν τη στιγμή, αλλά παρουσιάζει περιορισμένη λειτουργικότητα, η οποία περιγράφεται λεπτομερέστερα παρακάτω.

8.1 Έλλειψη άμεσης ενσωμάτωσης αποθέματος υλικού

Το σύστημα, στην τρέχουσα μορφή του, δεν προσφέρει δυνατότητα άμεσης διασύνδεσης με λογισμικό ή πλατφόρμες που παρακολουθούν το απόθεμα υλικού σε πραγματικό χρόνο. Αυτό σημαίνει ότι η καταγραφή και η συντήρηση εξοπλισμού, όπως φορητοί υπολογιστές, κινητά τηλέφωνα ή περιφερειακές συσκευές, δεν γίνεται αυτόματα αλλά απαιτεί χειροκίνητη εισαγωγή στοιχείων από τους διαχειριστές. Οι πληροφορίες για τα περιουσιακά στοιχεία πρέπει να εισάγονται από τους διαχειριστές IT, μία λεπτομέρεια κάθε φορά, όπως σειριακούς αριθμούς, λεπτομέρειες υλικού, τότε αγοράστηκε το περιουσιακό στοιχείο και αν έχει αντιστοιχιστεί. Αυτές οι εισροές ρυθμίζονται χρησιμοποιώντας φόρμες και πεδία στο δίκτυο. Ωστόσο, δεν υπάρχει αυτόματος τρόπος σύνδεσης με επιχειρηματικές βάσεις δεδομένων, ετικέτες περιουσιακών στοιχείων ή συστήματα API που εμπλέκονται στις προμήθειες.

Λόγω αυτού του περιορισμού, η ασφάλεια πλέον εξαρτάται από τους ανθρώπους για να εντοπίσουν οποιαδήποτε ύποπτη δραστηριότητα. Οι άνθρωποι μπορεί να πληκτρολογήσουν κάτι λανθασμένα, να παραλείψουν πεδία ή να αντιγράψουν υπάρχουσες καταχωρίσεις όταν εργάζονται με δεδομένα χειροκίνητα. Επίσης, η μη πρόσβαση σε συστήματα προμηθειών σημαίνει ότι κάθε φορά που αγοράζονται, αντικαθίστανται ή απορρίπτονται περιουσιακά στοιχεία, δεν υπάρχει αυτόματη ενημέρωση στο σύστημα ελέγχου πρόσβασης. Εξαιτίας αυτού, τα περιουσιακά στοιχεία ενδέχεται να μην αναφέρονται σωστά ή να προκύψουν σφάλματα στην αναφορά διαθεσιμότητας.

Σε μεγαλύτερους οργανισμούς που βασίζονται σε λογισμικό ERP ή παρακολούθησης υλικού, η μη άμεση σύνδεση με αυτά τα εργαλεία συνήθως έχει ως αποτέλεσμα οι άνθρωποι να κάνουν το ίδιο πράγμα δύο φορές. Είναι φυσιολογικό για τους διαχειριστές να παρακολουθούν πολλές πλατφόρμες ταυτόχρονα, όπως μία για τη διαχείριση περιουσιακών στοιχείων και μια άλλη για τη διαχείριση της πρόσβασης των χρηστών. Επειδή τα δεδομένα επαναλαμβάνονται, η διαχείρισή τους μπορεί να είναι λιγότερο αποτελεσματική και να οδηγήσει σε πιθανές ασυνέπειες σε όλα τα συστήματα.

Η έλλειψη αυτής της δυνατότητας καθιστά την παρακολούθηση σε επίπεδο υπαλλήλου απλή, αλλά εμποδίζει το σύστημα να αναπτυχθεί και να αυτοματοποιηθεί πλήρως. Εάν ενσωματωθούν τα Microsoft Intune, ServiceNow ή ο γραμμωτός κώδικας περιουσιακών στοιχείων, αυτό θα μπορούσε να διορθώσει το πρόβλημα σε μελλοντικές ενημερώσεις, έτσι ώστε τα αρχεία απογραφής να ενημερώνονται σε πραγματικό χρόνο.

8.2 Απουσία Διπαραγοντικής Ταυτοποίησης (2FA)

Ο έλεγχος ταυτότητας δύο παραγόντων δεν περιλαμβάνεται στο υπάρχον σύστημα. Ο έλεγχος ταυτότητας εξαρτάται μόνο από το όνομα χρήστη και τον κωδικό πρόσβασής σας, τα οποία προστατεύονται μόνο μέσω κατακερματισμού και κρυπτογράφησης HTTPS και, ως εκ τούτου, παρέχουν μόνο ένα εμπόδιο εισόδου. Με τις επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing), την παραποίηση διαπιστευτηρίων και τις συνδέσεις με βίαιη βία να συμβαίνουν όλο και πιο συχνά στις μέρες μας, η επιλογή του ελέγχου ταυτότητας ενός παράγοντα αφήνει το σύστημα εκτεθειμένο σε υψηλότερους κινδύνους.

Ο έλεγχος ταυτότητας δύο παραγόντων (2FA) απαιτεί από τους χρήστες να επιβεβαιώνουν την ταυτότητά τους όχι μόνο με το όνομα χρήστη και τον κωδικό πρόσβασής τους, αλλά και με μια δεύτερη μέθοδο, όπως έναν κωδικό πρόσβασης που αποστέλλεται μέσω SMS ή email ή μια εφαρμογή όπως το Google Authenticator. Επιπλέον, σύγχρονες μελέτες προτείνουν ακόμα και βιομετρικές μεθόδους, όπως αναγνώριση προσώπου και ομιλίας [20]. Δεδομένου ότι αυτό δεν ισχύει, εάν κακόβουλοι χρήστες αποκτήσουν πρόσβαση σε στοιχεία σύνδεσης, ενδέχεται να έχουν πρόσβαση σε σημαντικά δεδομένα, όπως αρχεία υπαλλήλων, κωδικούς πρόσβασης και πληροφορίες που καταγράφονται σχετικά με σημαντικά στοιχεία.

Δεδομένου ότι ο σκοπός της πλατφόρμας είναι ο έλεγχος της πρόσβασης στο διαδίκτυο και η παρακολούθηση σημαντικού εξοπλισμού, το 2FA θεωρείται απαραίτητο βιομηχανικό πρότυπο. Δεδομένου ότι η ομάδα αναγνωρίζει αυτό το πρόβλημα, η τελευταία έκδοση της εφαρμογής διαθέτει μια ευέλικτη μονάδα ελέγχου ταυτότητας, ώστε το 2FA να μπορεί να προστεθεί χωρίς σημαντικές αλλαγές στο λογισμικό. Παρ' όλα αυτά, μέχρι να έρθουν αυτές οι βελτιώσεις, οι διαχειριστές βασίζονται σε ασφαλείς κωδικούς πρόσβασης και σε τακτικούς ελέγχους των χρηστών για την ελαχιστοποίηση των κινδύνων.

8.3 Ανάλυση Ομοιόμορφων Ορισμών Ρόλων σε Όλα τα Τμήματα

Ένας άλλος σημαντικός περιορισμός είναι ότι το σύστημα υποθέτει ρόλους χρηστών και τα δικαιώματά τους είναι πάντα τα ίδια στον οργανισμό. Σε πολλές περιπτώσεις, αυτή η ιδέα δεν είναι ακριβής, ειδικά σε πολύπλοκες ή μητρικές επιχειρήσεις που διαθέτουν τμήματα που λειτουργούν ημι-αυτόνομα ή χρησιμοποιούν μεμονωμένες μεθόδους εργασίας.

Ένα παράδειγμα είναι ότι ένας «Διαχειριστής Πληροφορικής» σε ένα τμήμα θα μπορούσε να χειρίζεται όλα τα δικαιώματα πρόσβασης και τις κατανομές περιουσιακών στοιχείων, ενώ σε ένα άλλο τμήμα της εταιρείας, ο ρόλος επικεντρώνεται μόνο στον εξοπλισμό παρακολούθησης. Όπως και πριν, οι χρήστες στο HR μπορούν να επιβλέπουν τα καθήκοντα ένταξης σε μια ομάδα, αλλά να μην συμμετέχουν στην έξοδο από αυτήν οπουδήποτε αλλού. Προς το παρόν, ο έλεγχος πρόσβασης βάσει ρόλων (RBAC) είναι οργανωμένος σε μια απλή ιεραρχία και έχει ρυθμιστεί εκ των προτέρων. Δίνει σε σταθερούς ρόλους συγκεκριμένα δικαιώματα και αυτά τα δικαιώματα χρησιμοποιούνται σε όλα τα τμήματα με τον ίδιο τρόπο.

Λόγω αυτών των κανόνων, το σύστημα δεν είναι σε θέση να ανταποκριθεί καλά σε διαφορετικά πρότυπα σε οργανισμούς. Κάθε φορά που προκύπτουν εξαιρέσεις και απαιτούνται προσωρινά δικαιώματα διαχειριστή ή διαμορφώσεις ρόλων, αυτό πρέπει να γίνεται από έναν διαχειριστή συστήματος. Αυτό μπορεί να καταστήσει τη διαχείριση αναποτελεσματική και τα δικαιώματα μπορεί μερικές φορές να είναι πολύ χαλαρά ή πολύ αυστηρά.

Επιπλέον, η υπόθεση της ομοιομορφίας των ρόλων αποτελεί πρόκληση για τις επιχειρήσεις που λειτουργούν σε πολλαπλές γεωγραφικές τοποθεσίες, όπου οι κανονιστικές ή λειτουργικές απαιτήσεις ενδέχεται να απαιτούν τοπικούς ρόλους. Το τρέχον σύστημα δεν υποστηρίζει την προσαρμογή ρόλων σε επίπεδο τμήματος ή περιοχής, ούτε δέχεται δικαιώματα σε επίπεδα εντός ενός μόνο ρόλου.

Για να αντιμετωπιστεί αυτό, μια μελλοντική έκδοση του συστήματος θα μπορούσε να εφαρμόσει δυναμικό RBAC ή έλεγχο πρόσβασης βάσει χαρακτηριστικών (ABAC), ο οποίος επιτρέπει την εκχώρηση δικαιωμάτων με βάση πολλαπλά χαρακτηριστικά περιβάλλοντος, όπως τμήμα, τοποθεσία, ιεραρχία ή συσχέτιση έργου. Μέχρι τότε, οι διαχειριστές συστήματος πρέπει να παρακολουθούν προσεκτικά τις αναθέσεις ρόλων και ενδέχεται να χρειαστεί να δημιουργήσουν λύσεις μέσω σημαιών κατάστασης χρήστη ή χειροκίνητων παρακάμψεων.

8.4 Περιορισμένη Προσαρμογή Αναφορών

Παρόλο που το σύστημα παρέχει αναφορές, προς το παρόν οι χρήστες περιορίζονται στη χρήση προκαθορισμένων προτύπων και φίλτρων. Ο ιστότοπος προσφέρει αναφορές με τις ονομασίες «Σύνοψη Εκχώρησης Πόρων», «Δικαιώματα Πρόσβασης ανά Άτομο», αλλά οι χρήστες δεν μπορούν να δημιουργήσουν προσαρμοσμένες αναφορές ή να προσαρμόσουν τα φίλτρα μόνοι τους. Εξαιτίας αυτού, το λογισμικό ενδέχεται να μην καλύπτει πλήρως τις ανάγκες των οργανισμών που χρειάζονται αναφορές που να ταιριάζουν με τους εσωτερικούς τους κανόνες ή τις οδηγίες ελέγχου.

Για παράδειγμα, ένας υπεύθυνος συμμόρφωσης μπορεί να επιθυμεί να δημιουργήσει μια αναφορά με τα ονόματα όλων των ατόμων που εξακολουθούσαν να έχουν πρόσβαση στο σύστημα επτά ημέρες μετά την τελευταία ημερομηνία πρόσληψής τους. Για την τρέχουσα εφαρμογή, ο υπεύθυνος πρέπει να εξάγει ακατέργαστα δεδομένα και να εργαστεί για την ανάλυσή τους χρησιμοποιώντας υπολογιστικά φύλλα αντί για ένα πρότυπο αναφοράς. Ως αποτέλεσμα, οι άνθρωποι πρέπει να κάνουν επιπλέον εργασία, η οποία δεν συνάδει με τον στόχο του συστήματος για αποδοτικότητα.

Υπάρχει πιθανότητα οι περαιτέρω ενημερώσεις να προσφέρουν μια διεπαφή για τη δημιουργία αναφορών ή μια μηχανή εξαγωγής που θα επιτρέπει στους προχωρημένους χρήστες να καθορίζουν τις ρυθμίσεις για τις εξαγωγές καθώς και να χρησιμοποιούν το Power BI ή το Tableau με τα δεδομένα τους.

Οι άνθρωποι ενδέχεται να εξακολουθούν να χρησιμοποιούν χειροκίνητα μέσα για την αντιμετώπιση συγκεκριμένων διαδικασιών στην εταιρεία.

Παρόλο που ορισμένα πράγματα διεκπεραιώνονται με αυτοματοποιημένες ειδοποιήσεις, άλλα απαιτούν ανθρώπινη απόκριση. Η επιβεβαίωση της επιστροφής εξοπλισμού, η ενημέρωση των πληροφοριών των περιουσιακών στοιχείων και η αφαίρεση της πρόσβασης στο σύστημα συνήθως πρέπει να γίνονται χειροκίνητα. Παρόλα αυτά, η ύπαρξη ανθρώπου στον έλεγχο βοηθά σε επικίνδυνες εργασίες, αλλά μπορεί να οδηγήσει σε πιο αργές ενέργειες ή διακυμάνσεις στον χρόνο ολοκλήρωσης των εργασιών. Η αφαίρεση των ροών εργασίας καθιστά σαφές αυτό το ελάττωμα, καθώς το τμήμα IT πρέπει να βεβαιωθεί ότι έχει ανακληθεί κάθε πρόσβαση και ότι όλος ο εξοπλισμός έχει επιστραφεί πριν κλείσει ένα προφίλ χρήστη.

Οι ειδοποιήσεις και οι υπενθυμίσεις βοηθούν, αλλά οι διαχειριστές πρέπει να εκτελούν τις κύριες λειτουργίες χειροκίνητα. Για να είναι πλήρως αυτοματοποιημένο, το σύστημα πρέπει να επικοινωνεί με παρόχους ταυτοτήτων (όπως Azure AD και LDAP) και πλατφόρμες υλικού που υποστηρίζουν την παροχή εντολών μέσω του τερματικού για την εκτέλεση ανάπτυξης και αφαίρεσης. Προς το παρόν, η αρχιτεκτονική επιτρέπει αυτές τις επεκτάσεις, αλλά δεν υπάρχουν σε αυτήν την έκδοση.

8.5 Σύνοψη

Συνολικά, το τρέχον Σύστημα Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού καλύπτει τις βασικές ανάγκες μιας επιχείρησης, προσφέροντας οργάνωση και έλεγχο σε κρίσιμες διαδικασίες. Παρ' όλα αυτά, όπως κάθε πρώτη έκδοση, παρουσιάζει ορισμένους περιορισμούς που αξίζει να ληφθούν υπόψη. Η έλλειψη άμεσης διασύνδεσης με αποθέματα υλικού, η απουσία διπαραγοντικής ταυτοποίησης, οι σταθεροί και λιγότερο ευέλικτοι ρόλοι χρηστών και η περιορισμένη παραμετροποίηση αναφορών είναι σημεία που περιορίζουν την ευελιξία και τον βαθμό αυτοματοποίησης του συστήματος.

Οι αδυναμίες αυτές δεν αναιρούν τη χρησιμότητα της πλατφόρμας, αλλά λειτουργούν περισσότερο ως κατευθυντήριες γραμμές για τα επόμενα βήματα. Η καταγραφή τους βοηθά ώστε μελλοντικές βελτιώσεις να επικεντρωθούν σε σημεία με ουσιαστικό αντίκτυπο στην ασφάλεια, στην παραγωγικότητα και στη χρηστικότητα. Έτσι, το τρέχον σύστημα μπορεί να θεωρηθεί ως ένα ισχυρό πρώτο βήμα, πάνω στο οποίο θα «χτιστούν» πιο εξελιγμένες εκδόσεις, πιο κοντά στις πραγματικές ανάγκες των σύγχρονων επιχειρήσεων.

Κεφάλαιο 9ο: Μελλοντικές βελτιώσεις

Παρόλο που το τρέχον σύστημα ανταποκρίνεται στις σημερινές οργανωτικές ανάγκες, αρκετές βελτιώσεις μπορούν να γίνουν στο μέλλον για να βελτιωθεί η απόδοση, η ευελιξία και η συμμετοχή των χρηστών. Σκοπός τους είναι να αντιμετωπίσουν τις τρέχουσες προκλήσεις και να καλύψουν τις αυξανόμενες ανάγκες των εταιρειών που σχετίζονται με την ασφάλεια, τον αυτοματισμό, την κινητικότητα και την ανάλυση.

Η σύνδεση της πλατφόρμας με υπηρεσίες όπως το LDAP (Lightweight Directory Access Protocol) ή το Azure Active Directory (Azure AD) θα ήταν πολύ ωφέλιμη. Σε πολλές μεσαίες έως μεγάλες εταιρείες, αυτές οι πλατφόρμες αποτελούν τον κύριο τρόπο ελέγχου ταυτότητας των χρηστών. Η σύνδεση με το LDAP ή το Azure AD θα βοηθούσε στον συγχρονισμό των λογαριασμών χρηστών, επομένως δεν χρειάζεται να προσθέσετε υπαλλήλους στο σύστημα διαχείρισης πρόσβασης χειροκίνητα. Είναι καλύτερο να λαμβάνετε τόσο τους χρήστες όσο και τους ρόλους τους από τον κατάλογο, κάτι που βοηθά στη διασφάλιση τόσο της ακρίβειας όσο και της ασφάλειας στην επαλήθευση ταυτοτήτων. Επιπλέον, εάν ενσωματωθούν οι Identity Providers, καθίσταται δυνατή η Ενιαία Σύνδεση (SSO), η οποία καθιστά την σύνδεση πολύ πιο βολική, τηρώντας παράλληλα τα πρότυπα ελέγχου ταυτότητας του οργανισμού [1]. Θα διευκόλυνε πολύ τη διαχείριση των διαπιστευτηρίων ταυτότητας και την ανάθεση ρόλων σε διάφορα σημεία [4].

Ένα άλλο μεγάλο πλεονέκτημα είναι η παροχή υποστήριξης μέσω κινητού ή η δημιουργία μιας συγκεκριμένης εφαρμογής για κινητά. Αυτή τη στιγμή, το σύστημα λειτουργεί καλύτερα σε έναν επιτραπέζιο υπολογιστή και είναι προγραμματισμένο με responsive design. Στην πραγματικότητα, εάν θέλετε να είστε πραγματικά κινητοί, με εργασία πεδίου ή με περισσότερα από ένα γραφεία, η κατοχή μιας εφαρμογής για κινητά μπορεί να σας επιτρέψει να ελέγχετε την πρόσβαση και να είστε πιο αποτελεσματικοί ενώ βρίσκεστε στο πεδίο. Για παράδειγμα, οι τεχνικοί μπορούν να ελέγχουν τα δικαιώματα πρόσβασης, να ελέγχουν τα περιουσιακά στοιχεία και να καταγράφουν τις επιστροφές μέσω όλων των συσκευών τους κατά την επίσκεψη. Ομοίως, η εγγραφή νέων προσλήψεων, η διαχείριση των βημάτων ένταξης και η προειδοποίηση για εξόδους θα μπορούσαν να γίνουν οποιοδήποτε και οπουδήποτε. Όταν μια πλατφόρμα είναι κινητή, οι χρήστες μπορούν να έχουν πρόσβαση σε αυτήν οποιαδήποτε στιγμή και να λαμβάνουν αποφάσεις σε πραγματικό χρόνο, γεγονός που βελτιώνει την ανταπόκριση [7].

Η περαιτέρω ανάπτυξη του συστήματος θα μπορούσε να βασιστεί στην κωδικοποίηση με γραμμωτό κώδικα εξοπλισμού (barcode) ή στην RFID για τη βελτίωση και τον έλεγχο της διαχείρισης των περιουσιακών στοιχείων. Αυτή τη στιγμή, κάθε καταχώρηση στο σύστημα εξοπλισμού πρέπει να γίνεται χειροκίνητα, ακόμη και αν είναι βασική και τα σφάλματα και η σπατάλη χρόνου μπορούν να γίνουν μεγαλύτερα καθώς αυξάνονται οι όγκοι. Η προσθήκη barcode ή RFID επιτρέπει στους χρήστες να εγγράφονται και να βρίσκουν περιουσιακά στοιχεία αυτόματα. Για να το κάνετε αυτό, μπορείτε είτε να σαρώσετε τον barcode είτε την ετικέτα RFID κατά την έκδοση ή την επιστροφή, ώστε το σύστημα να μπορεί να καταγράψει άμεσα την αλλαγή. Ειδικά σε μεγάλες εγκαταστάσεις, η RFID βοηθά στην παρακολούθηση των αποθεμάτων σε πραγματικό χρόνο και στην αποτροπή της εσφαλμένης τοποθέτησης εξοπλισμού [2][6]. Τέτοια εργαλεία θα επέτρεπαν την προσθήκη χρονοσημασμένων σαρώσεων κάθε υλικού στα αρχεία καταγραφής, τα οποία αργότερα μπορούν να χρησιμοποιηθούν για τον έλεγχο των περιουσιακών στοιχείων.

Ένα ισχυρό χαρακτηριστικό που πρέπει να συμπεριληφθεί είναι ένας πίνακας ελέγχου που παρουσιάζει βασικές πληροφορίες σχετικά με το σύστημα και τον οργανισμό στο σύνολό του. Οι ομάδες HR, IT και συμμόρφωσης θα μπορούσαν να χρησιμοποιήσουν αυτόν τον πίνακα ελέγχου επειδή εμφανίζει γραφήματα και σύνολα για εκδοθέντα περιουσιακά στοιχεία, αλλαγές πρόσβασης, εκκρεμείς αποχωρήσεις, καθυστερημένες επιστροφές και παρόμοιες πληροφορίες. Εάν τα φίλτρα και τα εύρη ημερομηνιών μπορούν να προσαρμοστούν, οι ομάδες θα βρουν πιο εύκολο να χρησιμοποιήσουν τις πληροφορίες για δράση. Ένας διευθυντής HR μπορεί να σκεφτεί γιατί ορισμένα τμήματα αντιμετωπίζουν υψηλές αλλαγές προσωπικού και οι υπεύθυνοι ασφάλειας IT μπορούν να συλλέγουν δεδομένα σχετικά με ασυνήθιστες δραστηριότητες πρόσβασης για να δουν εάν αναπτύσσονται τάσεις. Η χρήση πινάκων ελέγχου στην υγειονομική περίθαλψη βοηθά τους γιατρούς να αποφασίζουν με δεδομένα, να διαχειρίζονται πόρους, να διαμορφώνουν πολιτικές και να επιβλέπουν τη συμμόρφωση με τους νόμους [12]. Η χρήση εργαλείων BI όπως το Power BI ή το Tableau εκτός από αυτήν τη λειτουργία είναι δυνατή, η οποία θα μπορούσε να παρέχει πιο εις βάθος ανάλυση [14].

Ένας άλλος τομέας στον οποίο μπορεί να αναπτυχθεί η πλατφόρμα είναι η βελτίωση του τρόπου με τον οποίο ανατίθενται ρόλοι στους χρήστες, ώστε να υποστηρίζεται μια καλύτερη εμπειρία και λιγότερα σφάλματα. Επειδή οι υπάρχοντες ορισμοί ρόλων δεν ανταποκρίνονται στις ανάγκες τους, δυσκολεύονται να ενταχθούν σε επιχειρήσεις με διαφορετικές μορφές λειτουργίας. Με τον έλεγχο πρόσβασης βάσει χαρακτηριστικών (ABAC), οι ρόλοι θα μπορούσαν να αλλάξουν για τους χρήστες σε πραγματικό χρόνο με βάση τον χώρο εργασίας, τον τόπο κατοικίας, τον βαθμό, το έργο ή άλλες παρόμοιες πτυχές. Μια τέτοια ευελιξία θα βοηθούσε στην ενίσχυση των πολιτικών εσωτερικής ασφάλειας και στην αποτροπή της διασποράς δικαιωμάτων, επιτρέποντας παράλληλα πιο ακριβή έλεγχο της πρόσβασης των χρηστών [7].

Η εισαγωγή ιδεών και αυτοματισμού Τεχνητής Νοημοσύνης θα μπορούσε να αυξήσει τη συνολική επιχειρησιακή νοημοσύνη της πλατφόρμας. Για παράδειγμα, θα μπορούσε να εξετάσει την προηγούμενη συμπεριφορά των χρηστών και να καθορίσει κατάλληλα δικαιώματα για τους νέους υπαλλήλους, καθώς και να επισημάνει προφίλ πρόσβασης που δεν συνάδουν με τους κανόνες του τμήματός τους. Η προγνωστική συντήρηση μπορεί επίσης να λειτουργήσει με μηχανήματα πληροφορικής, όπως φορητούς υπολογιστές και τηλέφωνα, ενημερώνοντας το προσωπικό πότε είναι ώρα να τα αντικαταστήσει λόγω της χρήσης τους και των ημερομηνιών εγγύησής τους [12]. Η ύπαρξη αυτών των έξυπνων λειτουργιών θα βοηθούσε στην αποφυγή προβλημάτων, στην ευκολία διαχείρισης και στον προγραμματισμό πόρων τόσο για τα τμήματα HR όσο και για τα τμήματα πληροφορικής.

Κεφάλαιο 10ο: Συμπέρασμα

Η ανάπτυξη του Συστήματος Διαχείρισης Πρόσβασης Εργαζομένων και Εταιρικού Εξοπλισμού ήταν ένα σημαντικό βήμα για την καλύτερη οργάνωση των διαδικασιών μιας επιχείρησης. Στόχος ήταν να συγκεντρωθούν όλα τα δεδομένα και οι λειτουργίες σε ένα ενιαίο και ασφαλές εργαλείο, ώστε να μειωθούν τα λάθη και να γίνουν πιο εύκολες οι καθημερινές εργασίες.

Με το σύστημα αυτό, πληροφορίες που μέχρι τώρα βρίσκονταν σε υπολογιστικά φύλλα, emails ή διαφορετικές εφαρμογές, μπαίνουν σε μια κοινή πλατφόρμα. Αυτό επιτρέπει καλύτερη εικόνα για το προσωπικό, τον εξοπλισμό και τις προσβάσεις, ενώ ταυτόχρονα μειώνει τον κίνδυνο κακής χρήσης ή παραλείψεων. Οι ροές εργασίας είναι πιο ξεκάθαρες, κάθε ενέργεια καταγράφεται και έτσι υπάρχει διαφάνεια και δυνατότητα ελέγχου.

Ένα από τα βασικά πλεονεκτήματα είναι ότι η πλατφόρμα είναι αρθρωτή, δηλαδή μπορεί να επεκταθεί μελλοντικά χωρίς να χρειάζεται να αλλάξει όλο το σύστημα. Αυτό δίνει τη δυνατότητα να προστεθούν νέες λειτουργίες, όπως έλεγχος ταυτότητας δύο παραγόντων (2FA), σύνδεση με εξωτερικά συστήματα, ή ακόμα και εφαρμογή για κινητά. Οι περιορισμοί που υπάρχουν σήμερα είναι αναμενόμενοι για μια πρώτη έκδοση και δεν μειώνουν την αξία της – απλώς δείχνουν πού μπορούν να γίνουν βελτιώσεις στο μέλλον.

Πέρα από τα τεχνικά στοιχεία, το σύστημα δείχνει και έναν πιο σύγχρονο τρόπο οργάνωσης. Δίνει τη δυνατότητα στα τμήματα HR και IT να συνεργάζονται καλύτερα, να έχουν κοινή εικόνα και να αποφεύγουν λάθη. Σε μια εποχή που οι επιχειρήσεις γίνονται όλο και πιο ψηφιακές και βασίζονται σε απομακρυσμένη εργασία, τέτοιου είδους εργαλεία βοηθούν όχι μόνο στην καθημερινότητα, αλλά και στη γενικότερη ασφάλεια και συνέπεια του οργανισμού [9][11].

Συνολικά, η εργασία αυτή έδειξε ότι με σωστό σχεδιασμό μπορούν να δημιουργηθούν εργαλεία που καλύπτουν πραγματικές ανάγκες. Το σύστημα που αναπτύχθηκε μπορεί να εξελιχθεί σε ένα βασικό εργαλείο για τη διαχείριση της πρόσβασης και του εξοπλισμού στις επιχειρήσεις, συμβάλλοντας σε πιο ασφαλείς, οργανωμένες και αποδοτικές λειτουργίες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] CISA, "Αρχιτεκτονική αναφοράς διαχείρισης ταυτοτήτων, διαπιστευτηρίων και πρόσβασης (ICAM)," 2023.
- [2] Camcode, "Τι είναι η Παρακολούθηση Περιουσιακών Στοιχείων; Πώς Λειτουργεί, Σκοπός, Οφέλη," 2025. [Online]. Available: <https://www.camera-code.gr>
- [3] Tenna, "Λύσεις Παρακολούθησης Εξοπλισμού στο Πεδίο," 2025.
- [4] U.S. Department of Defense, "Σχεδιασμός αναφοράς για τη διαχείριση εταιρικής ταυτότητας, διαπιστευτηρίων και πρόσβασης (ICAM) του Υπουργείου Άμυνας," 2020.
- [5] J. Roberts and J. Ekstrom, "Σύστημα Παρακολούθησης Περιουσιακών Στοιχείων," Επιθεώρηση Προπτυχιακής Έρευνας, vol. 1, άρθρο 2034, 2013.
- [6] Real Time Networks, "Όλα όσα πρέπει να γνωρίζετε για τα συστήματα παρακολούθησης φυσικών περιουσιακών στοιχείων," 2025.
- [7] A. S. M. Kayes, et al., "Ένα μοντέλο πολιτικής και ένα πλαίσιο για τον έλεγχο πρόσβασης σε πληροφοριακούς πόρους με επίγνωση του πλαισίου," 2017.
- [8] LogicManager, "Πώς να αυτοματοποιήσετε με ασφάλεια την ένταξη των εργαζομένων," 2025.
- [9] Keeper Security, "Βέλτιστες πρακτικές για την ασφαλή ένταξη των εργαζομένων," 2024.
- [10] Allwhere, "Τα πάντα για την ενσωμάτωση στην πληροφορική + Λίστα ελέγχου," 2025.
- [11] Secureframe, "Οδηγός για την Ένταξη και την Αποχώρηση Εργαζομένων για Διαχείριση Κινδύνων," 2024.
- [12] A. Chatterjee, et al., "Δυναμικός έλεγχος πρόσβασης βάσει ρόλων για αποκεντρωμένες εφαρμογές," 2020.
- [13] IJRTE, "Σύστημα Διαχείρισης Απογραφής Προμηθειών και Εξοπλισμού, Παρακολούθησης και Παρακολούθησης με Τεχνικές Εξόρυξης Δεδομένων," 2021.
- [14] GeeksforGeeks, "Σχεδιασμός Βάσεων Δεδομένων για Σύστημα Διαχείρισης Ανθρώπινου Δυναμικού," 2024. [Online]. Available: <https://www.geeksforgeeks.org>
- [15] GigaTrak, "Σύστημα Παρακολούθησης Εργαλείων | Λύσεις Λογισμικού Διαχείρισης Εργαλείων," 2025. [Online]. Available: <https://www.gigatrak.com>
- [16] Πανεπιστήμιο Λιναίος, "Σύστημα Διαχείρισης Εργαζομένων," 2009.
- [17] Guru, "Λογισμικό Ενσωμάτωσης Εργαζομένων: Ένας Πλήρης Οδηγός," 2025. [Online]. Available: <https://www.guru.com>
- [18] Creately, "6 Διαγράμματα ER για Σύστημα Διαχείρισης Εργαζομένων + Δωρεάν Πρότυπα," 2025.
- [19] ACM Digital Library, "Σχεδιασμός Συστήματος Διαχείρισης Εργαζομένων με βάση το SpringBoot," 2025. [Online]. Available: <https://dl.acm.org>
- [20] N. Tkauc, et al., "Αναγνώριση προσώπου και ομιλίας που βασίζεται στο cloud για εφαρμογές ελέγχου πρόσβασης," 2020.