Πανεπιστήμιο Αιγαίου
Σχολή Θετικών Επιστημών
Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων
Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΤΥΧΙΑΚΗ
«ΣΧΕΔΙΑΣΗ & ΥΛΟΠΟΙΗΣΗ ΑΣΦΑΛΟΥΣ ΣΥΣΤΗΜΑΤΟΣ ΑΙΤΗΜΑΤΩΝ ΠΡΟΣΒΑΣΗΣ ΣΕ ΕΦΑΡΜΟΓΕΣ & ΥΠΗΡΕΣΙΕΣ»

Μπούρα Χριστίνα – Κεσκεμπές Αθανάσιος

Σάμος
Ιούνιος 2016

Επιβλέπων
Δρ. Ριζομυλιώτης Παναγιώτης

Συμβουλευτική Επιτροπή
Δρ. Μήτρου Λίλιαν & Δρ. Κοκκολάκης Σπυρίδων

Πτυχιακή Εργασία

« Ανάπτυξη Συστήματος Διαχείρισης Authorization (Authorization Ticketing Management System) για την υποστήριξη των Πληροφοριακών Συστημάτων μιας Επιχείρησης»

Μπούρα Χριστίνα (ICSDM14018)
Κεσκεμπές Αθανάσιος (ICSDM14010)

Η παρούσα διατριβή, εκπονήθηκε στα πλαίσια του Μεταπτυχιακού «Ασφάλεια Πληροφοριακών και Επικοινωνιακών συστημάτων» της σχολής «Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων» του τμήματος Θετικών Επιστημών του Πανεπιστημίου Αιγαίου για διδακτικούς και ερευνητικούς σκοπούς.

Υπεύθυνη Δήλωση *: Βεβαιώνουμε ότι είμαστε οι συγγραφείς αυτής της Πτυχιακής Εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην Πτυχιακή Εργασία. Επίσης αναφέρουμε τις όποιες πηγές από τις οποίες κάναμε χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Βεβαιώνουμε ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε από εμάς προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος «Ασφάλεια Πληροφοριακών και Επικοινωνιακών συστημάτων» της σχολής «Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων» του Πανεπιστημίου Αιγαίου.*

Ανάπτυξη Ασφαλούς Συστήματος Αυτοματοποίησης και Διαχείρισης αιτημάτων πρόσβασης στα Πληροφοριακά Συστήματα μίας Επιχείρησης (Authorization Ticketing System)

Μπούρα Χριστίνα – Κεσκεμπές Αθανάσιος

Ονοματεπώνυμο Επιβλέποντα	Ονοματεπώνυμο Συμβούλου 1	Ονοματεπώνυμο Συμβούλου 2
Δρ.Ριζομιλιώτης Παναγιώτης	Δρ. Μήτρου Λίλιαν	Δρ. Κοκολάκης Σπύρος
Πανεπιστήμιο Αιγαίου	Πανεπιστήμιο Αιγαίου	Πανεπιστήμιο Αιγαίου

Περίληψη: Η πτυχιακή εργασία αφορά την δημιουργία Ασφαλούς συστήματος αυτοματοποίησης και διαχείρισης αιτημάτων πρόσβασης στα Πληροφοριακά συστήματα μίας Επιχείρησης. Κύρια σημεία είναι η αυτοματοποίηση, η κεντρική διαχείριση, η διασφάλιση των διαδικασιών, οι εγκρίσεις με χρήση τεχνικών μη αποποίησης, η υλοποίησης πρόσβασης με εφαρμογές και οι ενσωμάτωση όλων των δικλείδων ασφαλείας που θα διασφαλίζουν το νομικό & κανονιστικό πλαίσιο για μία μεγάλη Επιχείρηση. Όσον αφορά την Ασφάλεια Πληροφοριακών Συστημάτων Το επιστημονικό πεδίο που καλύπτεται είναι η Διοίκηση της Ασφάλειας ΠΣ, η μεθοδολογία ανάπτυξής Πληροφοριακού Συστήματος έχοντας ενσωματωμένη την Ασφάλεια ΠΣ και η εμπλοκή της σε όλο τον κύκλο ζωής λογισμικού. Υπάρχει εμπλοκή μεγάλου μέρους μεθόδων & μεθοδολογιών για την εκπόνηση του έργου (ΣΔΑΠ, Πρότυπο, Πολιτικές, Ανάλυση Επικινδυνότητας, Επιλογή τεχνολογιών που διασφαλίζουν από τρωτά σημεία κλπ.). Πλέον υλοποιήθηκαν τεχνικές ανάλυσης αδυναμιών (vulnerability assessment) και δοκιμών παρείσδυσης (penetration test). Όσον αφορά την λειτουργικότητα του Πληροφοριακού συστήματος υλοποιείται διαχείριση αιτημάτων πρόσβασης και αυτοματοποιείται η δημιουργία λογαριασμών χρηστών με interface σε LDAP σύστημα. Στόχος είναι η συγκέντρωση των αιτημάτων για την διευκόλυνση των ελεγκτών, η κάλυψη της αρχής μη αποποίησης (ψηφιακές υπογραφές), η διευκόλυνση της εκπαίδευσης νέου τεχνικού προσωπικού, η βελτίωση του χρόνου ανταπόκρισης αιτημάτων που προκύπτουν και η ενδυνάμωση της ποιότητας των υπηρεσιών υποστήριξης όσον αφορά την πρόσβαση σε πλήθος εφαρμογών μίας επιχείρησης και η διαφύλαξη της επιχείρησης από διαρροή δεδομένων. Το σύστημα επιτρέπει την αυτοματοποιημένη ροή των αιτημάτων από

τον τελικό χρήστη προς το κέντρο διαχείρισης, την καταγραφή και συστηματοποίηση των διαδικασιών με ψηφιακές εγκρίσεις. Υπάρχει πληροφόρηση της πορείας και της κατάστασης των αιτημάτων προς όλους τους εμπλεκομένους. Εφαρμόζονται τεχνικές διαφύλαξης των δεδομένων σε όλες τους τις καταστάσεις (data at rest, data in motion, data in use). Στα τεχνικά πλεονεκτήματα του συστήματος συγκαταλέγονται: η χρήση σύγχρονων τεχνολογιών εφαρμογών ιστού (Angular, Java Spring, i Text και επεκτάσεων) που κάνουν εύχρηστη και γρήγορη την διεπαφή χρήστη και η δρομολόγηση των αιτημάτων.

Λέξεις κλειδιά: Προσβάσεις, Ροή, Ασφάλεια Δεδομένων, Δεδομένα σε αποθήκευση, Δεδομένα σε μετακίνηση

Secure Automation System Development for Access Requests Management (Authorization Ticketing System) for Applications and Services of a Company

Boura Christine – Keskempes Athanasios

Full Name	Full Name	Full Name
Supervisor	Advisor 1	Advisor 2
Dr. Rizomiliotis Panagiotis	Dr. Mitrou Lilian	Dr. Kokolakis Spiros
University of the Aegean	University of the Aegean	University of the Aegean

Summary: The subject of diploma paper is the secure creation of an Information System for implementig authorization requests with digital signed approvals. Features about the secure information system that are covered by the project have to do with: the automation, the centralization, the administration of a ticketing information system, MIS, the IT security segregation of duties, the security of the data at rest and of the data in motion. By such an Information System is given Enforcement to a large Company in order to help the internal and external auditors.

Concerning the Security of Information Systems the scientific Basic parts of the security field about an information system that are covered are the following: Security Administration, Secure Information System development methodology followed in all the parts of software life cycle. There is an involvement of it security methods and methodologies for the preparation of the project (ISMS, Model, Policies, Risk Analysis, Selection of technologies that ensure vulnerabilities etc.). Also implemented weaknesses analysis techniques (vulnerability assessment) and intrusion tests (penetration test).

Regarding the functionality of the IT system covered subjects such as: the management of access requests, the automation of authorization management on LDAP, the approvals (digital signed) for the requests needed for auditors, improvement of request response time, the improvement of the support services quality.

The system allows the automated flow of requests from the end user to the control center involving digital signed approvals. There is information about the ticket state on all

stakeholders. Techniques like information preservation and data in all their state (data at rest, data in motion, data in use) used.

The technical advantages of the system include: the use of modern Web technologies (java with Angular, Java Spring, iText and extensions) that make convenient and fast user interface and the routing of requests.

Key words: Authorization, Ticketing, Data_Security, Data_at_Rest, Data_in_motion

Τεχνολογίες – Σύνοψη Περιεχομένου

Η πτυχιακή περιλαμβάνει κείμενο, υλοποίηση σε γλώσσα Java με τεχνολογίες Angular, Java Spring, Hibernate – Object Relational Mapping ORM, Java Persistence API (JPA) για τα entity, Oracle RDBMS, Oracle 12c – Liquid Base – H2 RDBMS, HTML5, CSS3, Web Socket, Elastic Search (μηχανή αναζήτησης), Secure data «at rest, in motion – in transit, in use»

Αναλυτικά οι τεχνολογίες που καλύπτονται είναι:

- Oracle RDBMS & database v. 12.2.0.2 on linux DB server Oracle RHEL (on vmware virtual environment) – Liquid Base (on java Spring that initiate the db schema) – H2 (on java Spring for development) RDBMS
- Hibernate – Object Relational Mapping ORM, Java Persistence API (JPA), Web Socket
- HTML5
- CSS3
- Angular
- Java Spring
- Web Socket (on Angular web tcp connection between client & server)

MVC

- **Model**: Java Classes
- **View** (Angular JS - bootstrap)
- **Controller** (Spring Controller)

Για την σχεδίαση χρησιμοποιήθηκε η μεθοδολογία ICONIX (requirement analysis, design , implementation , testing). Δημιουργήθηκαν βασικά UML διαγράμματα (use case diagrams). Το αποτέλεσμα είναι να υπάρχουν στην εφαρμογή υποσυστήματα που θα κάλυπταν:

- Security Management
- User Authorization System Administration
- Ticketing - Workflow
- MIS – Reporting – Statistics
- Automatic User Account Connection on AD LDAP – SAP etc
- Authorization Auditing Administration

- Digital Signatures
- Application Management (portfolio of business applications & the roles of each one)
- Security Business Role Management
- Endpoint Inventory Management
- HR Management
- Helthcheck of infrastructure (all components)

Ευχαριστίες

Ευχαριστούμε πολύ τις οικογένειές μας που μας στήριξαν καθώς και τους διδάσκοντες που συνέβαλαν στο όλο εγχείρημά μας.

Ένα σκωτσέζικο ρητό αναφέρει

«Το να μεταδίδεις τη γνώση, σημαίνει να ανάβεις από το λυχνάρι σου τα κεριά των άλλων χωρίς να στερείσαι τίποτα από τη φλόγα σου»

Πίνακας περιεχομένων

Πίνακας Εικόνων

Πίνακες:

1. Εισαγωγή – Σκοπός

1.1 Εισαγωγή

Οι σύγχρονοι ειδικοί στη διοίκηση των επιχειρήσεων υποστηρίζουν ότι η επιχειρησιακή γνώση, η τεχνολογία, η πληροφορία, τα πληροφοριακά συστήματα και οι χρήστες μιας επιχείρησης αφορούν σημαντικά περιουσιακά στοιχεία της. Η ύπαρξη πληροφοριακών συστημάτων επιτρέπει τη συλλογή, αποθήκευση, επεξεργασία και διάχυση της πληροφορίας και της γνώσης στα διάφορα τμήματα της επιχείρησης. Η Πληροφορία αφορά περιουσιακό στοιχείο της επιχείρησης. Οι χρήστες που την διαχειρίζονται πρέπει να ακολουθούν βασικές αρχές ασφάλειας όπως την αρχή των ελαχίστων προνομίων, του ελαχίστου της γνώσης, της μη αποποίησης και της αναλογικότητας. Η Ασφάλεια της Πληροφορίας και η διαφύλαξη της Εμπιστευτικότητας, της Ακεραιότητας και τις Διαθεσιμότητάς (CIA) θωρακίζουν μια επιχείρηση ενώ ταυτόχρονα προφυλάσσουν την φήμη της και την έκθεσή της σε νομικές και οικονομικές εμπλοκές.

Απαραίτητες δικλείδες ασφαλείας όσον αφορά την ηλεκτρονική πληροφορία είναι:

Η ύπαρξη και η εφαρμογή ενός πλαισίου Ασφάλειας Πληροφοριακών Συστημάτων με βάση τις βέλτιστες πρακτικές (πχ ISO/IEC 27001) που πρέπει να διαθέτει κάθε σύγχρονη Επιχείρηση,

Η χρήση σύγχρονων μεθόδων - τεχνικών & τεχνολογιών Πληροφοριακών Συστημάτων για την ενδυνάμωση της Ασφάλειάς τους (χρήση κώδικα που αντιμετωπίζει γνωστές λογικές ευπάθειες ιστού όπως το sql injection, XSS, CSRF, έλεγχοι ευπαθειών και δοκιμές παρείσδυσης, κρυπτογράφηση κτλ).

Η Διαφύλαξη των ηλεκτρονικών πληροφοριών μέσω της ενδυνάμωσης των πληροφοριακών συστημάτων που τις διαχειρίζονται με σκοπό την αντιμετώπιση πιθανών διαρροών δεδομένων, προσωπικών ευαίσθητων προσωπικών δεδομένων, εταιρικών δεδομένων και ευαίσθητων εταιρικών δεδομένων.

Η Ενεργοποίηση τεχνικών ενδυνάμωσης που αφορούν την χρήση προσβασιμότητας, τις τεχνικές μη αποποίησης, του ελαχίστου της γνώσης, των ελαχίστων προνομίων κτλ.

Η Ενεργοποίηση αυτοματοποιημένων διαδικασιών για γρηγορότερη ανταπόκριση (πχ διαγραφές σημείων που μπορεί να είναι τρωτά όπως πχ λογαριασμός χρήστη που έχει αποχωρήσει από την Επιχείρηση).

Ενεργοποίηση καταγραφής και ελέγχου του πληροφοριακού συστήματος με βάση το νομικό και κανονιστικό πλαίσιο.

Μια σημαντική διασφάλιση της εμπιστευτικότητας γίνεται με την χρήση προσωπικών λογαριασμών χρηστών για πληροφοριακά συστήματα και υπηρεσίες, με την απονομή ρόλων και με τον διαχωρισμός καθηκόντων (Segregation Of Duties) ανάλογα με την κάθε επιχειρησιακή ανάγκη. Επιπλέον για ένα πληροφοριακό σύστημα η ασφάλειά του αφορά διεργασία που ενσωματώνεται στο στάδιο του σχεδιασμού του «secure on design». Αυτό την καθιστά ως «build in» χωρίς όμως να αποκλείει την ενδυνάμωσή της στον μέλλον «add on» όσον αφορά νέες απειλές που θα εμφανιστούν στο μέλλον. Στην εποχή της αυτοματοποίησης η διαδικασία της διαχείρισης πρόσβασης καθώς και του ελέγχου αυτής πρέπει να γίνεται σύντομα. Με αυτόν τον τρόπο διαφυλάσσεται η επιχείρηση από πιθανή διαρροή δεδομένων και από μη εξουσιοδοτημένες προσβάσεις (όπως για παράδειγμα ένας χρήστης που έχει απομακρυνθεί από την επιχείρηση και πρέπει ο λογαριασμός που του έχει αποδοθεί για πρόσβαση σε πληροφοριακά συστήματα κρίσιμα και μη, να απενεργοποιηθεί). Όλα τα παραπάνω βασίζονται πάνω στις επιχειρησιακές απαιτήσεις (business objectives).

Ως εκ τούτου η πτυχιακή εργασία έχει ως στόχο τον σχεδιασμό και την υλοποίηση ενός ασφαλούς πληροφοριακού συστήματος διαχείρισης και αυτοματοποιημένης υλοποίησης αιτημάτων πρόσβασης χρηστών (επιχειρησιακών και προνομιακών) σε εφαρμογές, υπηρεσίες, σε λειτουργικά συστήματα, σε βάσεις δεδομένων και πληροφοριακές υποδομές (πχ δίκτυο) μίας μεγάλης επιχείρησης.

Με το πέρας της υλοποίησης το σύστημα θα πρέπει:

Να προσφέρει αυτοματοποίηση των αιτημάτων πρόσβασης.

Να υλοποιεί σύνδεση αυτόματα με συστήματα όπως για παράδειγμα LDAP Active Directory, web εφαρμογές κτλ.

Πρέπει να υλοποιεί κεντρική διαχείριση και συλλογή δεδομένων. Πρέπει να έχει εύρος σε όλους του επιχειρησιακούς χρήστες και εφαρμογές.

Πρέπει να παρέχει σύγχρονη και ασφαλή γραφική παρακολούθηση της πορείας αιτημάτων πρόσβασης.

Πρέπει να διαχειρίζεται τις διαγραφές λογαριασμών χρηστών που έχουν απομακρυνθεί από την επιχείρηση μέσω διασυνδέσεων με το πληροφοριακό σύστημα ανθρωπίνου δυναμικού της Επιχείρησης.

Στην λειτουργικότητα του πληροφοριακού συστήματος υπάρχουν επιπλέον, MIS reporting, στατιστικά, παροχή πληροφόρησης για το μητρώο εφαρμογών της επιχείρησης και διεργασία αίτησης πρόσβασης σε αυτές από τους χρήστες. Η αίτηση πρόσβασης περιέχει την αποδοχή χρήστη, την έγκριση προϊσταμένου, και την έγκριση ιδιοκτήτη της εφαρμογής με χρήση ψηφιακής υπογραφής. Μετά από τις εγκρίσεις υλοποιείται η αυτόματη δρομολόγηση του αιτήματος σε ομάδα εξειδικευμένων τεχνικών (ticketing) για να υλοποιήσουν το αίτημα.

Πλέον των παραπάνω γίνεται ψηφιακή καταγραφή των αιτημάτων δίνοντας σε όλους τους εμπλεκόμενους την δυνατότητα παρακολούθησης της πορείας και της κατάστασης του αιτήματος (workflow) με ταυτόχρονη στατιστική παρουσίαση της παροχής των υπηρεσιών και της ζήτησης εφαρμογών.

Τελικός στόχος είναι από την μία να μπορεί να αυτοματοποιηθεί η διαδικασία αιτημάτων και η διαχείριση λογαριασμών χρηστών αλλά από την άλλη να γίνεται υποστήριξη της διαδικασίας του ελέγχου των λογαριασμών χρηστών και βελτίωση του χρόνου ανταπόκρισης. Παράλληλα υπάρχει η διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων (authorization, encryption).

1.2 Σκοπός

1.2.1 Φάσεις - Ενότητες

Η ανάπτυξη του συστήματος ακολούθησε την διαδικασία ανάπτυξης πληροφοριακών συστημάτων (ICONIX) η οποία περιλαμβάνει τις ακόλουθες φάσεις: α) συλλογή απαιτήσεων, β) ανάλυση απαιτήσεων, γ) σχεδιασμό συστήματος, δ) υλοποίηση, ε) εγκατάσταση, έλεγχο και αξιολόγηση από τους τελικούς χρήστες, στ) συνολική αξιολόγηση του συστήματος ως προς τους στόχους που τέθηκαν αρχικά.

Η διαδικασία εμπλουτίστηκε και με τις συνιστώσες που αφορούν την Ασφάλεια. Έτσι μεταξύ της ανάλυσης απαιτήσεων και του σχεδιασμού του συστήματος προστέθηκε μία επιπλέον φάση η οποία αφορούσε το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Εδώ ορίστηκε το πρότυπο ασφάλειας (ISO/IEC 27001), έγινε μελέτη Πολιτικών Ασφάλειας για την Επιχείρηση (αναδιοργάνωση τους ή υλοποίηση νέων) και υλοποιήθηκε μία Ανάλυση Επικινδυνότητα και Επιχειρησιακών Επιπτώσεων με το Πληροφοριακό σύστημα να εξετάζεται σε ιδεατή μορφή εφόσον δεν έχει ακόμα υλοποιηθεί. Η έκθεση που προέκυψε συνέβαλε στην επιλογή των τεχνολογιών που θα χρησιμοποιηθούν και έθεσε το επίπεδο κινδύνου στο αποδεκτό με βάση τις επιχειρησιακές ανάγκες και απαιτήσεις «business objectives».

Πριν την παραγωγική λειτουργία υλοποιήθηκε μία επιπλέον Ανάλυση Επικινδυνότητας. Στην φάση αυτή υλοποιήθηκαν ένα Vulnerability Assessment και ένα Penetration Test.

Οι φάσεις μετά την ενσωμάτωση των θεμάτων Ασφάλειας έγιναν:

α) συλλογή απαιτήσεων

β) ανάλυση απαιτήσεων

γ) σχεδιασμός και υλοποίηση Ασφάλειας Πληροφοριών (Σύστημα Διαχείρισης Ασφάλειας Πληροφορικών – ISMS, Πολιτικές, Ανάλυση Επικινδυνότητας, BIA)

δ) σχεδιασμός συστήματος

ε) υλοποίηση

ζ) Έλεγχος Ασφάλειας (RA, Vulnerability Assessment, Penetration Test, Risk Analysis)

η) εγκατάσταση, έλεγχος και αξιολόγηση από τους τελικούς χρήστες

θ) συνολική αξιολόγηση του συστήματος ως προς τους στόχους που τέθηκαν αρχικά

Για τις πρώτες δύο φάσεις που αφορούν τη **συλλογή** και την **ανάλυση των απαιτήσεων** του συστήματος έγιναν τα ακόλουθα:

Διαμορφώθηκαν κατάλληλα ερωτηματολόγια (βλ. Παράρτημα Α) τα οποία συμπληρώθηκαν από επιλεγμένους χρήστες. Κατά την ανάλυση των απαιτήσεων, δημιουργήθηκε συγκεντρωτικό διάγραμμα περιπτώσεων χρήσης το οποίο συμπληρώθηκε από αναλυτική περιγραφή κάθε περίπτωσης χρήσης. Μια επισκόπηση των αποτελεσμάτων της ανάλυσης απαιτήσεων δίνεται στο κεφάλαιο 3.

Στο κεφάλαιο 4 αναπτύχθηκε η τρίτη φάση, η οποία αφορά την εισαγωγή της Ασφάλειας Πληροφοριακών Συστημάτων ως σημαντικό πυλώνα στον κύκλο ζωής Λογισμικού. Στην Φάση αυτή ορίστηκε το πρότυπο Ασφάλειας που ακολουθήθηκε - ISO/IEC 27001/2013.

Συντάχθηκαν έγγραφα που αφορούν την Ασφάλεια όπως η Πολιτική Ασφάλειας με τις επιμέρους εμπλεκόμενες πολιτικές.

Επιλέχθηκε η μεθοδολογία ανάλυσης Επικινδυνότητας και συντάχθηκαν έγγραφα που αφορούν την Διαχείριση κινδύνων όπως, Πολιτική Διαβάθμισης Πληροφοριακών Πόρων & Επιχειρησιακής Συνέχειας, Ανάλυσης Επικινδυνότητας και υλοποιήθηκε και μία ανάλυση επιχειρησιακής επιπλοκής (Business Impact Analysis). Στην φάση ικανοποιείται η αρχή της ασφάλειας κατά τον σχεδιασμό «security on design» και υλοποιείται ενσωμάτωσή της στον κύκλο ζωής λογισμικού «built in security»

Μετά τα αποτελέσματα της Ανάλυσης Επικινδυνότητας, πραγματοποιήθηκε **έρευνα για τα εργαλεία** που θα μπορούσαν να χρησιμοποιηθούν για την ανάπτυξη του πληροφοριακού συστήματος με έμφαση στα εργαλεία διαχείρισης αιτημάτων. Τα αποτελέσματα της έρευνας αυτής παρουσιάζονται στο κεφάλαιο 2.

Συνδυάζοντας την ανάλυση απαιτήσεων, τις απαιτήσεις ασφάλειας πληροφοριακών συστημάτων και την επισκόπηση των διαθέσιμων εργαλείων και λύσεων, κρίθηκε απαραίτητη η δημιουργία μιας ολοκληρωμένης εφαρμογής που θα συνδυάζει:
Εφαρμογή πολιτικών διαδικασιών και προτύπων, πιστοποίηση, ασφαλή αυτοματοποίηση των διεργασιών, αντιμετώπιση πιθανών διαρροών δεδομένων προσωπικών, ευαίσθητων προσωπικών, εταιρικών και ευαίσθητων εταιρικών, κρυπτογράφηση, μη αποποίηση και καταγραφή.

Πλέον των παραπάνω οι Περιπτώσεις Χρήσης αφορούν:

- Single Sign On
- Διαχείριση αιτημάτων
- Ροές και Reporting αιτημάτων
- Εγκρίσεις – Αιτήσεις ψηφιακά υπογεγραμμένες.
- Διαχείριση επιχειρησιακών ρόλων ασφάλειας.
- Διαχείριση χρηστών
- Στατιστικά
- Διαχείριση Εφαρμογών – Μητρώο Εφαρμογών
- Διαχείριση Ρόλων των Εφαρμογών του Μητρώου
- Διασύνδεση με το Ανθρώπινο Δυναμικό

Όπως ήδη περιγράφηκε υλοποιήθηκε μία ανάλυση επικινδυνότητας πριν την φάση του σχεδιασμού καθώς σημαντικός στόχος είναι να υλοποιηθεί η εφαρμογή έχοντας ενσωματωμένη την Ασφάλεια Πληροφοριακών Συστημάτων (Security on Design - Build In) με σκοπό την διαφύλαξη της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας.

Η φάση του **σχεδιασμού** του πληροφοριακού συστήματος βασίστηκε στην ανάλυση απαιτήσεων και έλαβε υπόψη τα συμπεράσματα της μελέτης των συστημάτων και της Ασφάλειας Πληροφοριακών Συστημάτων. Ακολούθησε τις αρχές της μεθοδολογίας ICONIX κα έθεσε συνοπτικά τις λειτουργίες και την αρχιτεκτονική του συστήματος, τη σχεδίαση της βάση δεδομένων, και τη σχεδίαση και διασύνδεση των υποσυστημάτων του. Στο κεφάλαιο 5 παρουσιάζονται τα σημαντικότερα στοιχεία αυτής της φάσης.

Η επόμενη φάση που παρουσιάζεται στο κεφάλαιο 6, αφορά την **υλοποίηση** του συστήματος, τη διασύνδεση με τα εξωτερικά συστήματα. Στη φάση αυτή χρησιμοποιήθηκαν:

α) το Java Spring MVC για την ανάπτυξη του συστήματος (model, view, controller)

β) τεχνολογίες AngularJS (view)

γ) bootstap για την ενσωμάτωση εύχρηστων GUI components στις σελίδες της εφαρμογής (view).

δ) Oracle 12c (12.2.0.2) σε Oracle Enterprise Linux server για την οργάνωση και διαχείριση των δεδομένων. Σε αυτή την φάση ενεργοποιήθηκαν όλες οι δικλείδες Ασφαλείας (εφαρμόζεται το model). Κρυπτογραφήθηκε όλο το σχήμα της εφαρμογής.

Οι λεπτομέρειες της φάσης του **ελέγχου ασφάλειας** του συστήματος παρουσιάζονται στο κεφάλαιο 7. Περιέχουν τον έλεγχο ευπαθειών και τις δοκιμές παρείσδυσης που υλοποιήθηκαν καθώς και τις δικλείδες ασφαλείας που εφαρμόστηκαν μετά από τα ευρήματα για την ενδυνάμωση της ασφάλειας. Σημεία που δεν ενδυναμώθηκαν αφορούσαν ρίσκο που αναγνωρίστηκε από τον Ιδιοκτήτη της Εφαρμογής και την Επιχείρηση.

Στην επόμενη φάση της **εγκατάστασης και ελέγχου** του συστήματος, έγινε πιλοτική χρήση, διόρθωση σφαλμάτων (alpha testing). Στη συνέχεια ακολούθησε μια σύντομη φάση δοκιμής του συστήματος από επιλεγμένους χρήστες της επιχείρησης και συγκεκριμένα εισαγωγή στο σύστημα, νέων αιτημάτων από χρήστες και ακολουθήθηκε όλο το workflow αιτήματος, έγκρισης, υλοποίησης (αυτόματης και χειρονακτικής). Στη δεύτερη φάση δοκιμών (beta testing) διορθώθηκαν όσα επιπλέον σφάλματα εντοπίστηκαν, βελτιώθηκε η σχεδίαση των διεπαφών και δόθηκε η δυνατότητα σε ανθρώπους της επιχείρησης και μελλοντικούς χρήστες, να έρθουν σε επαφή με το πληροφοριακό σύστημα. Στα πλαίσια αυτής της φάσης περιλαμβάνεται και η ανάπτυξη της κατάλληλης τεκμηρίωσης του συστήματος, όπως εγχειρίδιο χρήσης, τεχνικά πρότυπα (technical standards) κλπ. Τα αποτελέσματα αυτής της φάσης παρουσιάζονται στο κεφάλαιο 8 με αναλυτική περιγραφή της ολοκλήρωσης του συστήματος και της αξιολόγησης από τους χρήστες.

Επιπλέον για την ανάπτυξη του πληροφοριακού συστήματος έγινε και η **αξιολόγηση του συστήματος** ως προς τους στόχους που τέθηκαν αρχικά. Η αξιολόγηση έγινε από τη διεύθυνση της επιχείρησης. Για τις ανάγκες της παρούσας εργασίας, στο κεφάλαιο 8 παρουσιάζεται μια συνολική αποτίμηση της προσπάθειας που έγινε και καταγράφονται τα γενικά συμπεράσματα και γίνονται προτάσεις για μελλοντική ενασχόληση επέκτασης του θέματος.

2. Μελέτη/έρευνα συστημάτων και εργαλείων

2.1 Διαχείριση αιτημάτων πρόσβασης

Η διαχείριση της πρόσβασης χρηστών σε μεγάλο πλήθος εφαρμογών και για μεγάλο πλήθος χρηστών αποτελεί σημαντική δραστηριότητα για μια επιχείρηση. Έχοντας οργανώσει κατάλληλα τη αυτοματοποίηση των αιτημάτων και της αυτοματοποίηση της διαχείρισης λογαριασμού χρήστη μπορεί:

- Να διαχειρίζεται με ομοιόμορφο τρόπο τις διεργασίες που αφορούν την διαχείριση πρόσβασης σε εφαρμογές του μητρώου εφαρμογών της επιχείρησης.
- Να αποφεύγει τη σπατάλη πόρων σε εργασίες που επαναλαμβάνονται συχνά και για τις οποίες μπορεί να αξιοποιήσει αυτοματοποίηση (LDAP και άλλων εφαρμογών).
- Να οργανώσει καλύτερα τους πόρους της και το χρόνο της
- Να βελτιώσει και να επιταχύνει την κατάρτιση των νέων τεχνικών διαχείρισης προσβάσεων

Σημαντικό πρόβλημα από την έλλειψη αυτοματοποίησης είναι η χρονοβόρες διαδικασίες, η καθυστέρηση της επίτευξης των επιχειρησιακών στόχων, η πιθανότητα διαρροής της πληροφορίας, η αδυναμία παρακολούθησης στατιστικών πρόσβασης, η δυσκολία της τροφοδότησης των ελεγκτικών μηχανισμών. Για το σκοπό αυτό ένα τέτοιο σύστημα θα πρέπει να ενταχθεί στην καθημερινή δραστηριότητα.

Οι λύσεις που έχει κανείς στη διάθεσή του όταν σχεδιάζει ένα νέο πληροφοριακό σύστημα, είναι συνήθως δύο: είτε να ολοκληρώσει υπάρχοντα εργαλεία τα οποία θα καλύπτουν το καθένα ένα μέρος των αναγκών της επιχείρησης είτε να αναπτύξει εξ' αρχής ένα πληροφοριακό σύστημα που να ταιριάζει απόλυτα στις ανάγκες του.

Η πρώτη επιλογή οδηγεί πολύ γρήγορα σε λύση η οποία όμως δεν καλύπτει το 100% των αρχικών αναγκών και κατά συνέπεια απαιτεί από την επιχείρηση να αποδεχτεί τροποποιήσεις και περικοπές στους αρχικούς στόχους της. Η δεύτερη επιλογή, απαιτεί πολύ περισσότερους πόρους και χρόνο για να υλοποιηθεί. Για το σκοπό της εργασίας κρίθηκε σκόπιμο να μελετηθούν οι υπάρχουσες έτοιμες λύσεις, και να αξιοποιηθούν όσο το δυνατόν περισσότερο. Παρόλα αυτά όπως ανέδειξε η μελέτη που θα παρουσιαστεί ακολούθως καμία έτοιμη λύση δεν μπορούσε να καλύψει τις αρχικές απαιτήσεις λόγο του ιδιαίτερου περιβάλλοντος, του σύνθετου και διαφορετικού των τεχνολογιών του μεγάλου όγκου και του κόστους. Για το σκοπό αυτό όλες οι απαιτήσεις καλύφθηκαν με την εξ αρχής δημιουργία λογισμικού.

2.2 Συστήματα Διαχείρισης Πρόσβασης χρηστών σε Εφαρμογές και Υπηρεσίες του Μητρώου Εφαρμογών μίας Επιχείρησης

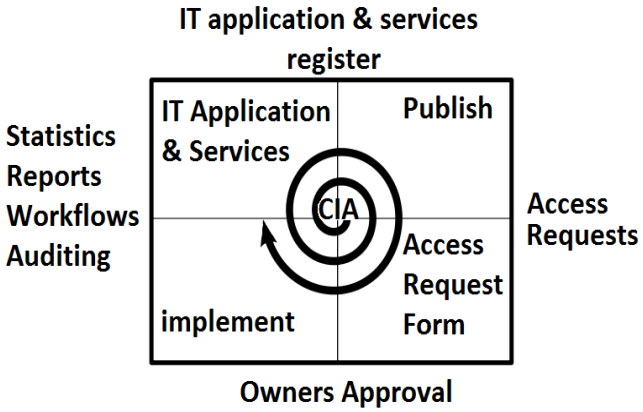
Συστήματα διαχείρισης πρόσβασης (**Authorization Managment**) ονομάζονται τα συστήματα που επιτρέπουν την αυτοματοποίηση αιτήματος πρόσβασης σε αντικείμενο του μητρώου εφαρμογών μίας επιχείρησης. Παράλληλα παρέχουν υπηρεσία μη αποποίησης αιτήματος, διαφύλαξης εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Παρέχουν ενημέρωση χρηστών για την κάθε εφαρμογή, για τις πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων της Επιχείρησης. Παρέχουν αυτοματοποιημένη διαχείριση λογαριασμών χρηστών μέσω Interfaces με συστήματα LDAP και συστήματα του Μητρώου Εφαρμογών της Επιχείρησης. Παρέχουν διαχείριση τεχνογνωσίας για την χειρωνακτική υλοποίηση κάθε αιτήματος πρόσβασης με καταγραφή της διαδικασίας. Παρέχουν πληροφόρηση για την ροή και την κατάσταση που βρίσκεται το αίτημα. Για παράδειγμα ο ιδιοκτήτης μίας εφαρμογής μπορεί να δει τα αιτήματα που τον αφορούν και την μεγαλύτερη ζήτηση εφαρμογών. Παρέχει στατιστικά γραφήματα και καταγραφή που μπορεί να βοηθήσει την διεργασία των ελεγκτικών μηχανισμών εφόσον η Επιχείρηση επίκειται σε σχετικές διαδικασίες (πχ ενταγμένη στο χρηματιστήριο).

Τα αναμενόμενα οφέλη για την επιχείρηση μπορούν να συνοψιστούν στα ακόλουθα:

- Πληρέστερη γνώση για τις εφαρμογές και υπηρεσίες Πληροφοριακών Συστημάτων του μητρώου εφαρμογών μίας Μεγάλης Επιχείρησης και αξιοποίηση της τεχνογνωσίας σχετικά με το μητρώο εφαρμογών και των διαδικασιών υλοποίησης των αιτημάτων (User Awareness).
- Αυτοματοποίηση αιτημάτων πρόσβασης στις εφαρμογές και υπηρεσίες Πληροφοριακών Συστημάτων (Γρηγορότερη απενεργοποίηση λογαριασμών χρηστών που έχουν απομακρυνθεί).
- Ταχύτερη εξυπηρέτηση (ικανοποίηση των πελατών – χρηστών).
- Δυνατότητα έκδοσης στατιστικών και report σε όλα τα επίπεδα πρόσβασης (χρήστες, ιδιοκτήτες εφαρμογών, διαχειριστές τεχνικοί, εσωτερικοί και εξωτερικοί Ελεγκτές, Αυτοματοποιημένες διεργασίες).
- Αύξηση της παραγωγικότητας στην επιχείρηση (εξέλιξη – ικανοποίηση πελατών).

- Ενημέρωση της ιεραρχίας για τις αυξημένες ανάγκες σε συγκεκριμένα σημεία ή την μειωμένες ανάγκες σε κάποια άλλα (human resources) καθώς και την αναγκαιότητα ή μη μίας εφαρμογής ή υπηρεσίας από τον οργανισμό.
- Δυνατότητα της εφαρμογής των πολιτικών ασφαλείας (usernames, passwords, encryption) όσον αφορά τους λογαριασμούς χρηστών καθώς αυτό θα αντιμετωπίζεται κεντρικά.

Η διαδικασία με την οποία εξελίσσεται και διογκώνεται διαρκώς η αναγκαιότητα της χρήσης του πληροφοριακού συστήματος από την επιχείρηση σε όλα της τα επίπεδα, ακολουθεί μια επαναλαμβανόμενη ροή, όπως φαίνεται στην εικόνα που ακολουθεί και αφορά τη δημιουργία, τερματισμό και μεταβολή εφαρμογών & υπηρεσιών Πληροφοριακών Συστημάτων και την κοινοποίηση στο εσωτερικό της επιχείρησης κ.ο.κ.



Εικόνα 1 Η διαδικασία διαχείρισης των αιτημάτων πρόσβασης σε πληροφοριακά συστήματα και υπηρεσίες

Για να γίνει πιο κατανοητή η ανάγκη για ένα σύστημα Διαχείρισης αιτημάτων πρόσβασης σε πληροφοριακά συστήματα μίας μεγάλης επιχείρησης καθώς και της αυτοματοποίησης δημιουργίας των λογαριασμών πρόσβασης, παραθέτω τα ακόλουθα παραδείγματα:

- Ένας χρήστης θα προσπαθούσε να ενημερωθεί για την ύπαρξη πληροφοριακών συστημάτων και υπηρεσιών μέσω της ιεραρχίας του και θα υπήρχε μείωση της παραγωγικότητα στον οργανισμό εφόσον δεν υπάρχει αυτοματοποιημένη διαδικασία.

- Ένας χρήστης θα αναγκαζόταν να υλοποιήσει αίτημα χωρίς αυτοματοποιημένη διαδικασία (πιθανά με χειρόγραφη αίτηση) το οποίο θα έπρεπε να λάβει κατάλληλες εγκρίσεις από τις ιεραρχία του και από τον ιδιοκτήτη της εφαρμογής ή υπηρεσίας (εσωτερικό ή εξωτερικό ταχυδρομείο, χειρόγραφες υπογραφές, καθυστέρηση)
- Ένας χρήστης θα αναγκαζόταν να αναζητά μέσω της ιεραρχίας ή μέσω τηλεφωνικών κλήσεων την έκβαση του αιτήματός του και δεν θα υπήρχε δυνατότητα παρακολούθησης της μέσω αυτοματοποιημένου workflow.
- Οι ιδιοκτήτες εφαρμογών θα έπρεπε να έχουν δικούς τους τρόπους διαχείρισης και παρακολούθησης των αιτημάτων πρόσβασης σε εφαρμογές και υπηρεσίες που επιμελούνται.
- Η τεχνογνωσία των τεχνικών πληροφορικής που ασχολούνται με την διαχείριση χρηστών θα έπρεπε να διατηρείται με διάφορους τρόπους και να μεταδίδεται μέσω συστημάτων των ειδικών τμημάτων.

Εικόνα 2 Γραφική εμφάνιση της πολυπλοκότητας και των αναγκών μίας σύγχρονης Επιχείρησης

2.3 Αξιοποίηση αυτοματοποιημένου συστήματος αιτημάτων πρόσβασης σε εφαρμογές και υπηρεσίες Πληροφορικής.

Η αξιοποίηση του συστήματος αφορά την ενημέρωση των χρηστών για το μητρώο εφαρμογών και υπηρεσιών του οργανισμού, την ταχύτητα υλοποίησης των αιτημάτων τους για πρόσβαση, την καταγραφή τεχνογνωσίας σχετικά με την διαδικασίας πρόσβασης, την αυτοματοποιημένη υλοποίηση λογαριασμών χρηστών σε συστήματα LDAP, και εφαρμογών του Μητρώου της Επιχείρησης και την κάλυψη όλων των απαραίτητων καθημερινών δραστηριοτήτων. Πολύ συχνά λοιπόν, οι επιχειρήσεις ζητούν από τα πληροφοριακά συστήματα διαχείρισης αιτημάτων να ενσωματώνουν τα παραπάνω στις επιμέρους διαδικασίες.

Η διαδικασία διαχείρισης αιτημάτων πρόσβασης σε εφαρμογές και υπηρεσίες πληροφορικής μια μεγάλης επιχείρησης είναι αρκετά σύνθετη και περιλαμβάνει πολύ περισσότερα πράγματα από μια απλή αίτηση πρόσβασης. Πρέπει να ακολουθούνται οι Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων του οργανισμού. Εμπλέκονται εγκρίσεις και τεχνικές μη αποποίησης. Εμπλέκονται τεχνικές διαχωρισμού καθηκόντων (SoD Segregation of Duties). Εμπλέκονται τεχνικές που ακολουθούν παγκόσμια πρότυπα όπως το ISO/IEC 27001. Εμπλέκονται προσωπικά και εταιρικά δεδομένα που πρέπει να διαφυλαχθούν από πιθανές κακόβουλες διεργασίες. Εμπλέκονται οι αρχές του ελαχίστου της γνώσης, την αναλογικότητας και των ελαχίστων προνομίων. Στόχος του πληροφοριακού συστήματος της Πτυχιακής είναι να καταγράψει και να οργανώσει όλα τα παραπάνω με τρόπο που να εξυπηρετήσει την αποδοτικότερη διαχείριση αιτημάτων πρόσβασης σε πληροφοριακά συστήματα. Για το λόγο αυτό, είναι απαραίτητο να ενσωματώνει:

α) την πρόσβαση στο μητρώο εφαρμογών
β) την αυτοματοποίησης των αιτημάτων
γ) την καταγραφή και την ιστορικότητα
δ) τον διαχωρισμό των ρόλων ασφάλειας πληροφοριακών συστημάτων
ε) εργαλεία γραφικής παρακολούθησης της έκβασής ενός αιτήματος
ζ) εργαλεία identity management με αυτοματοποιημένες διαδικασίες και interfaces.

Για το σκοπό αυτό η μελέτη των συστημάτων που έγινε στα πλαίσια της εργασίας, με εστίαση σε εργαλεία που εντάσσονται στις πιο πάνω κατηγορίες.

2.3.1 Εργαλεία ticketing για τη διαχείριση αιτημάτων (Διερεύνηση)

Μια από τις βασικές εργασίες της επιχείρησης είναι η καταγραφή και εξυπηρέτηση αιτημάτων πρόσβασης από τεχνικά τμήματα ασφάλειας και διαχείρισης χρηστών. Κάθε αίτημα πρέπει να καταχωρείται, να παίρνει αριθμό και να δρομολογείται στην κατάλληλη ομάδα τεχνικών. Για την κάλυψη των θεματικών ενοτήτων που πραγματεύεται το πληροφοριακό σύστημα διαχείρισης αιτημάτων πρόσβασης και αυτοματοποίησης δημιουργίας των λογαριασμών είναι αναγκαία η χρήση και ο συντονισμός συστημάτων όπως:

- **Ticketing system** HP Service Desk (Αναφορές)
- **Identity Management System** (Αναφορές)
- **Workflow System** (Αναφορές)
- **Reporting & MIS** System όπως για παράδειγμα το Qlikview & Business Objects (Αναφορές)
- **Wiki** System (όπως για παράδειγμα το Media Wiki) (Αναφορές)
- **SIEM** (Αναφορές)

Καθώς: για κάθε ένα από τα παραπάνω θα έπρεπε να γίνει;

- παραμετροποίηση και προσαρμογή του στις επιχειρησιακές ανάγκες
- εναρμόνιση της συνεργασίας του με όλα τα υπόλοιπα παραπάνω λογισμικά,
- εκπαίδευση χρήσης σε όλο το προσωπικό της επιχείρησης
- συνεργασία με το υπάρχον LDAP της επιχείρησης
- έλεγχος ασφάλειας του
- ανανέωση των patches που το αφορούν
- πιθανές άδειες χρήσεις

Αποφασίστηκε από την ομάδα να αναπτυχθεί νέο πληροφοριακό σύστημα με έμφαση στην υποστήριξη του ελεύθερου λογισμικού και του λογισμικού ανοικτού κώδικα (ΕΛ/ΛΑΚ).

Επιλέχθηκε η λύση της προσαρμοσμένης υλοποίησης του ασφαλούς πληροφοριακού συστήματος πρόσβασης σε εφαρμογές μιας Επιχείρησης που διαθέτει χιλιάδες χρήστες εφαρμογών καθώς τα θετικά που θα αποκοιμίσουν είναι τα ακόλουθα:

- θα καλύπτει μέρος από την λειτουργικότητά των παραπάνω λογισμικών που διερευνήθηκαν και θα είναι προσαρμοσμένο στις ανάγκες της επιχείρησης. Όπως ήδη αναφέρθηκε, η προμήθεια λογισμικών που ενσωματώνουν όλες τις απαιτήσεις που καλείται να αντιμετωπίσει η εφαρμογή που θα αναπτυχθεί και η παραμετροποίηση τους για συνεργασία προσδίδει μεγάλο διαχειριστικό κόστος και προσπάθεια σε σχέση με την εξ αρχής υλοποίηση ενός συστήματος που θα καλύψει της λειτουργικές απαιτήσεις του θέματος.
- Θα έχει δυνατότητα μελοντικής επέκτασης της λειτουργικότητας με επέμβαση στον κώδικα (ΕΛ/ΛΑΚ).
- θα συνεργαστεί μέσω interface & web Services με υπάρχοντα συστήματα (Help Desk, LDAP, εφαρμογές εμπορικές και custom, SIEM).
- Το κόστος υλοποίησης των λειτουργικών απαιτήσεων είναι πολύ μικρό σε σχέση με το πλήθος των Εφαρμογοχρηστών.
- Θα γίνει χρήση της Ασφάλειας σχετικά με μεγάλες εμπορικές βάσεις δεδομένων και θα μελετηθούν οι τεχνικές κρυπτογράφησης και αυτοματοποίησης.
- Θα διερευνηθούν και θα συντονιστούν διαδικασίες πληροφοριακών συστημάτων (web services, interfaces).
- Θα υλοποιηθεί έρευνα σύγχρονων τεχνολογιών ανάπτυξης ασφαλούς πληροφοριακού συστήματος και θα γίνει ενσωμάτωση της ασφάλειας πληροφοριακών συστημάτων από την έναρξη κύκλου ζωής του λογισμικού και θα μελετηθούν και θα υλοποιηθούν δικλείδες που προτείνονται από παγκόσμια πρότυπα. Θα αναπτυχθεί το λογισμικό στο πλαίσιο της διαφύλαξης της Εμπιστευτικότητας της Ακεραιότητας και της διαθεσιμότητας ακολουθώντας τις οδηγίες που δίνει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.
- Θα υλοποιηθεί πλαίσιο της Διοίκησης Ασφάλειας Πληροφοριακών Συστημάτων (Διαχείριση Επικινδυνότητας, αναδιοργάνωση Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων, καταγραφής επιχειρησιακών επιπτώσεων BIA &

διαδικασία ανάκαμψης πληροφοριακού συστήματος από καταστροφή DRP). Θα προσδοθεί τεχνογνωσία πάνω στην διαδικασία που ακολουθείται.

- Θα ενσωματωθούν στην υλοποίηση παράγοντες όπως η αυτοματοποίηση η ταχύτερη υλοποίηση ενός αιτήματος, η ανάγκη διατήρησης της τεχνογνωσίας η ασφαλής πρόσβαση, η αύξηση της παραγωγικότητας, η προστασία των επιχειρησιακών απαιτήσεων και η ευέλικτη προσαρμογή σχετικά με τους ελεγκτικούς μηχανισμούς.
- Θα εφαρμοστούν οι αρχές της αναλογικότητας – του ελαχίστου της γνώσης – της κρυπτογραφίας – της μη αποποίησης.
- Θα ακολουθηθεί το νομικό πλαίσιο που έχει σχέση με τα προσωπικά και τα ευαίσθητα εταιρικά δεδομένα.

3. Καταγραφή και ανάλυση απαιτήσεων

3.1 Καταγραφή απαιτήσεων - ερωτηματολόγια

Για την καταγραφή των αρχικών απαιτήσεων της εφαρμογής σχεδιάστηκε κατάλληλα ερωτηματολόγια μέσω του web (google doc forms https://docs.google.com/forms) τα οποία στάλθηκαν σε χρήστες της επιχείρησης μέσω ηλεκτρονικού ταχυδρομείου (ΠΑΡΑΡΤΗΜΑ Α).

Το πρώτο ερωτηματολόγιο αναφέρεται σε χρήστες εφαρμογών (business users) της επιχείρησης. Το δεύτερο ερωτηματολόγιο αναφερόταν σε τεχνικούς οι οποίοι διαχειρίζονται τις προσβάσεις στις εφαρμογές (authorization administrators).

Σκοπός των δύο ερωτηματολογίων μέσα από τα είκοσι τρία (23) ερωτήματα είναι να αντλήσει την πληροφορία που αποκαλύπτει το μέγεθος της αναγκαιότητας, τα πιθανά προβλήματα διαδικασιών, την πιθανή εμφάνιση τρωτότητας τσε θέματα ασφάλειας ης υπάρχουσας διαδικασίας και την άποψη μίας άλλης μορφής αντιμετώπισης της υπάρχουσας διαδικασίας.

Αναλυτικά οι ερωτήσεις για τα δύο ερωτηματολόγια εμφανίζονται στο (ΠΑΡΑΡΤΗΜΑ Α).

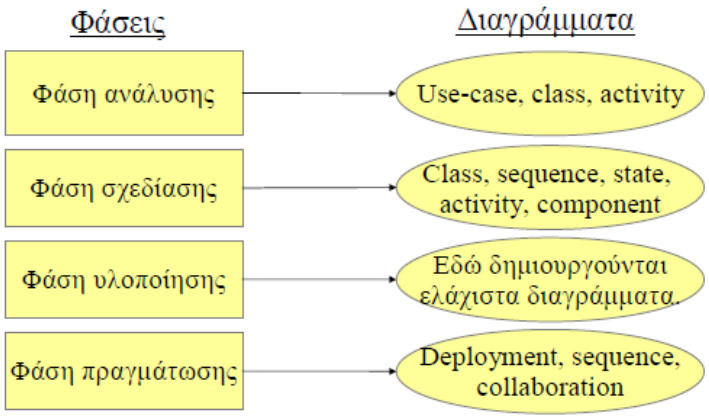
Σε δείγμα 100 χρηστών οι απαντήσεις επιβεβαίωσαν την αναγκαιότητα της αυτοματοποίησης και την ύπαρξης μιας προσαρμοσμένης εφαρμογής που να έχει τα χαρακτηριστικά που πραγματεύεται η πτυχιακή.

3.2 Ανάλυση απαιτήσεων

Για την ανάπτυξη της εργασία χρησιμοποιήθηκε η μεθοδολογία ανάπτυξης λογισμικού ICONIX. Αφενός η διαδικασία είναι επαναληπτική διότι επιτρέπει την παραγωγή λειτουργικού κώδικα για κάθε μια περίπτωση χρήσης του συστήματος ξεχωριστά. Σε κάθε επανάληψη, θα εξετάζεται μια νέα περίπτωση χρήσης που θα καταλήγει στην προσθήκη λειτουργικότητας στο τελικό προϊόν. Αυτή η διαδικασία επιτρέπει την επιστροφή από ένα στάδιο της διαδικασίας ανάπτυξης (πχ σχεδιασμό) σε προηγούμενα (πχ ανάλυση απαιτήσεων)

- Οι απαιτήσεις των χρηστών του συστήματος διατυπώθηκαν σε αρχικό κείμενο ως απαιτήσεις υψηλού επιπέδου.
- Με βάση την συγκεκριμένη μεθοδολογία με χρήση της UML (Unified Modeling Language) έγινε η δημιουργία των διαγραμμάτων Περιπτώσεων Χρήσης (Use Case Diagram)
- Επίσης περιγράφηκαν αναλυτικά με την κατάλληλη διαμόρφωση που ακολουθεί η ICONIX όλες οι περιπτώσεις χρήσεις (ΠΑΡΑΡΤΗΜΑ Γ) θα συνοδεύσουν με επιπλέον τεχνικό έγγραφο την πτυχιακή.
    - Περιπτώσεις χρήσης (Use Cases)

Σε κάθε μια εκ των 4 φάσεων τα διαγράμματα που δημιουργήθηκαν είναι τα ακόλουθα:



Εικόνα 3 Φάσεις της μεθοδολογίας ICONIX

3.2.1 Απαιτήσεις υψηλού επιπέδου (High level requirements specification)

Σε αυτό το σημείο γίνεται η αρχική διατύπωση των απαιτήσεων από την πλευρά του αιτούντα – πελάτη ή της διοίκησης.

Το λογισμικό που πρόκειται να αναπτυχθεί αφορά ένα πληροφορικό σύστημα για την χρήση του με τεχνική SSO, την υλοποίηση αιτημάτων πρόσβασης με βάση το μητρώο εφαρμογών και υπηρεσιών της επιχείρηση, την αυτοματοποίηση ενός αιτήματος χρήστη, την καταγραφή της πορείας του, την διατήρηση της ιστορικότητας των αιτημάτων, την επεξεργασία και διαχείριση του από την αρμόδια ομάδα, την κάλυψη των ενδιάμεσων εγκρίσεων, την χρήση ψηφιακών υπογραφών για την κάλυψη της αρχής μη αποποίησης, την διαχείριση ρόλων εφαρμογών για την κάλυψη των αρχών του ελαχίστου της γνώσης, την κάλυψη των αρχών της διαφύλαξης της εμπιστευτικότητας και της ακεραιότητας προσωπικών δεδομένων και την διατήρηση στοιχείων (logging, auditing). Το πληροφοριακό σύστημα θα τροφοδοτείται με πληροφορίες από τους εμπλεκόμενους χρήστες, εγκριτικά όργανα και το τεχνικό προσωπικό διαχείρισης. Η εφαρμογή θα χρησιμοποιείτε επίσης για παρακολούθηση από τους εμπλεκόμενους και για εξαγωγή στατιστικών στοιχείων εμφάνισης αναγκών ανά τμήμα με σκοπό την ενδυνάμωση των εφαρμογών.

Σημαντική είναι η

- Λειτουργία με SSO.
- Λειτουργία Μητρώου Εφαρμογών και Υπηρεσιών και διαχείριση των ρόλων τους.
- Λειτουργία του διαχωρισμού καθηκόντων.
- Η χρήση ψηφιακής υπογραφής (μη αποποίηση εγκριτικών μελών)
- Η χρήση ροών εργασιών (tickets) και η παρακολούθηση της κατάστασης των αιτημάτων.
- Διαχείριση χρηστών.
- Διαχείριση του περιβάλλοντος της εφαρμογής.
- Δυνατότητα Καταγραφής, Παρακολούθησης κινήσεων.
- Στατιστικά, Ιστορικότητα και Reporting
- Στατιστικά για την ανώτερη ιεραρχία.
- Έλεγχος της λειτουργίας των μηχανημάτων του συστήματος για την διαφύλαξη της διαθεσιμότητας.

- Διαχείριση του προφίλ από τον ίδιο τον χρήστη.
- Διασύνδεση με τα Πληροφοριακά συστήματα για την υλοποίηση του αιτήματος από τους τεχνικούς διαχείρισης προσβάσεων.

3.2.2 Συνοπτική Περιγραφή των ρόλων της εφαρμογής

Οι ρόλοι που υπάρχουν στην εφαρμογή είναι:

- Ο ρόλος του **user** που κάνει τα εξείς:
  - Μπορεί να αιτηθεί πρόσβαση σε εγγραφή του μητρώου εφαρμογών
  - Μπορεί να αιτηθεί πρόσβαση για κάποιον σε εγγραφή συνεργάτη στο μητρώου εφαρμογών
  - Μπορεί να διαχειριστεί το προφίλ του
  - Μπορεί να παρακολουθεί την πορεία του/των αιτημάτων του και να έχει ιστορικότητα
  - Αιτείται δημιουργία, μεταβολή, διαγραφή
- Ο ρόλος του **Ιδιοκτήτη εφαρμογών:**
  - Λαμβάνει αυτόματα τα αιτήματα των χρηστών για τις εφαρμογές που είναι ορισμένος από την επιχείρηση ως ο αρμόδιος υπεύθυνος επεξεργασίας.
  - Εγκρίνει αιτήματα έχοντας εφαρμόσει την διαφύλαξη του διαχωρισμού καθηκόντων και βάζει την ψηφιακή του υπογραφή στο κάθε ένα από αυτά
  - Μπορεί να παρακολουθεί την πορεία του/των αιτημάτων που έχουν σχέση με αυτόν και έχει ιστορικότητα
  - Ορίζει συνεργάτη του ο οποίος θα ελέγχει τις λειτουργίες διαχωρισμού καθηκόντων αι θα υλοποιεί όλους τους ελέγχους ορθότητας των αιτημάτων
- Ο ρόλος **Βοηθού Ιδιοκτήτη**
  - Υλοποιεί ότι ο ιδιοκτήτης και τον συνεπικουρεί
- Ο ρόλος **Διαχειριστή Χρηστών**
  - Υλοποιεί τα αιτήματα
  - Παρακολουθεί την πορεία τους και υλοποιεί όσα δεν έχει αναλάβει άλλος τεχνικός έχοντας παράλληλα ιστορικότητα
  - Συμμετέχει σε ομάδα τεχνικών διαχείρισης πρόσβασης για τις εφαρμογές που του έχει ανατεθεί η διαχείριση χρηστών.

- Ο ρόλος **MIS** αναλαμβάνει
    - Με τον ρόλο αυτό η ανώτερη ιεραρχία παρακολουθεί στατιστικά στοιχεία.
- Ο ρόλος **Διαχειριστή της Εφαρμογής** αναλαμβάνει
    - Την διαχείριση της εφαρμογής διαχείρισης αιτημάτων
    - Την διαχείριση των ροών εργασιών

Πλέον των παραπάνω όλοι οι ρόλοι και όλοι οι χρήστες θα πρέπει να έχουν την δυνατότητα να διαχειρίζονται το προφίλ τους (εμφάνιση, εισαγωγή στοιχείων που επιθυμούν όπως τηλέφωνο, διεύθυνση εταιρική, στοιχεία σταθμού εργασίας) .

Ως εκ τούτου οι Λειτουργικοί ρόλοι της Εφαρμογής είναι:

3.2.3 Λειτουργικοί Ρόλοι Εφαρμογής

Οι λειτουργικοί ρόλοι που υπάρχουν στην εφαρμογή είναι οι ακόλουθοι:

- User (U) Απλός Χρήστης
- Director (D) Προϊστάμενος
- Auditor - Ελεγκτής Owner (AU)
- Owner (O) – Ιδιοκτήτης Εφαρμογής
- MIS (MIS) – BOK ή Director & κάτω όλα τα αιτήματα
- Request Processor (RP) – Διαχειριστής Αιτημάτων (ΔΧ)
- Application Manager (AM) – Διαχειριστής Μητρώου Εφαρμογών
- Application Role Manager (ARM) – Διαχειριστής Ρόλων Εφαρμογών
- Human Resource Management (HR) – Διαχ. Μεταβολών HR
- Application Super User (Admin) - Διαχειριστής Εφαρμογής

3.2.3.1 User (U) Απλός Χρήστης (Περιπτώσεις Χρήσης)

Αφορά απλούς χρήστες που υπάρχει πιθανότητα να μην έχουν LDAP πρόσβαση και είναι οι ακόλουθοι:

- Όλοι οι χρήστες του ενδοδικτύου με κωδικό μητρώου της Επιχείρησης
- Εξωτερικοί συνεργάτες

Οι χρήστες αυτοί θα έχουν στην εφαρμογή τις ακόλουθες δυνατότητες

- Σελίδα διαχείρισης των αιτημάτων και ιστορικής αναδρομής τους

- Σελίδες προβολής ροής και κατάστασης αιτημάτων αλλά και αποδοχής όπου υπάρχει εμπλοκή

ΑΝΑΛΥΣΗ ΛΕΙΤΟΥΡΓΙΩΝ

Για νέο χρήστη που δεν έχει AD user λογαριασμό θα γίνεται η παρακάτω διαδικασία:

1. Θα δρομολογείται από το HR αίτημα προς το τμήμα διαχείρισης χρηστών μέσω διασύνδεσης. Θα δίνεται έγκριση και θα δρομολογείται στον διαχειριστή χρηστών για να υλοποιείται η δημιουργία του λογαριασμού ενδοδικτύου.

Αν αφορά εξωτερικό συνεργάτη.

1. Θα υλοποιείται αίτημα από τον director για εξωτερικούς συνεργάτες. Θα πρέπει να αναφέρει στην αίτηση έναρξη και λήξη σύμβασης.
2. Θα προχωράει στο τμήμα διαχείρισης χρηστών και θα υλοποιείται από έναν request processor αφού θα κάνει τον έλεγχο
3. Αυτόματα μέσω του συστήματος και συγκριμένα του πίνακα outside_workers ο οποίος διασυνδέεται με τον sn_creator θα ελέγχει την λήξη σύμβασης και θα κάνει lock τον χρήστη και θα δημιουργεί αιτήματα προς τους Ιδιοκτήτες Εφαρμογών κλειδώματος των λογαριασμών πρόσβασης του. Με την έγκριση θα υλοποιείται από τους διαχειριστές χρηστών.

3.2.3.2 Director (D) Προϊστάμενος

Αφορά εν δυνάμει απλούς χρήστες.

Αφορά τους υπεύθυνους τμημάτων στην Επιχείρηση που επιπλέον των δυνατοτήτων του απλού χρήστη μπορούν να κάνουν και τα ακόλουθα:

1. Δημιουργία αιτήματος για άλλους
2. Θα μπορεί να βλέπει τα αιτήματά του με δυνατότητα λειτουργίας φίλτρων, που έχει κάνει για τους συνεργάτες του Εγκεκριμένα, Απορριφθέντα

3.2.3.3 Auditor - Ελεγκτής Owner (AU)

Αφορά βοηθό του Ιδιοκτήτη για κάθε εφαρμογή ο οποίος μπορεί να κάνει ότι ένας απλός χρήστης (πιθανά και ένας προιστάμενος) αλλά επιπλέον δέχεται και όλα τα αιτήματα του ιδιοκτήτη που τον έχει ορίσει και τον βοήθάει στην έρευνα για εγκρίσεις

3.2.3.4 Owner (O) – Ιδιοκτήτης Εφαρμογής

Αφορά εν δυνάμει απλό user που έχει οριστεί από την Επιχείρηση ως ο Ιδιοκτήτης μίας Εφαρμογής.

3.2.3.5 MIS (MIS) – BOK ή Director &

1. Θα μπορεί να βλέπει τα αιτήματά με φίλτρα, του τμήματος που ανήκει Εγκεκριμένα, Απορριφθέντα
2. Στατιστικά - Θα υπάρχει δυνατότητα επιλογής application

3.2.3.6 Request Processor (RP) – Διαχειριστής Αιτημάτων (ΔΧ)

Αφορά ρόλο που κάνει διαχείριση χρηστών. Ο ρόλος και η εφαρμογή δίνεται στον Διαχειριστή Χρηστών για να υλοποιεί προσβάσεις για εφαρμογές της Επιχείρησης.

3.2.3.7 Application Role Manager (ARM) – Διαχειριστής Ρόλων Εφαρμογών

Αφορά ρόλο που θα διαχειρίζεται το Μητρώο με τις Εφαρμογές και Υπηρεσίες που διαθέτει η Επιχείρηση.

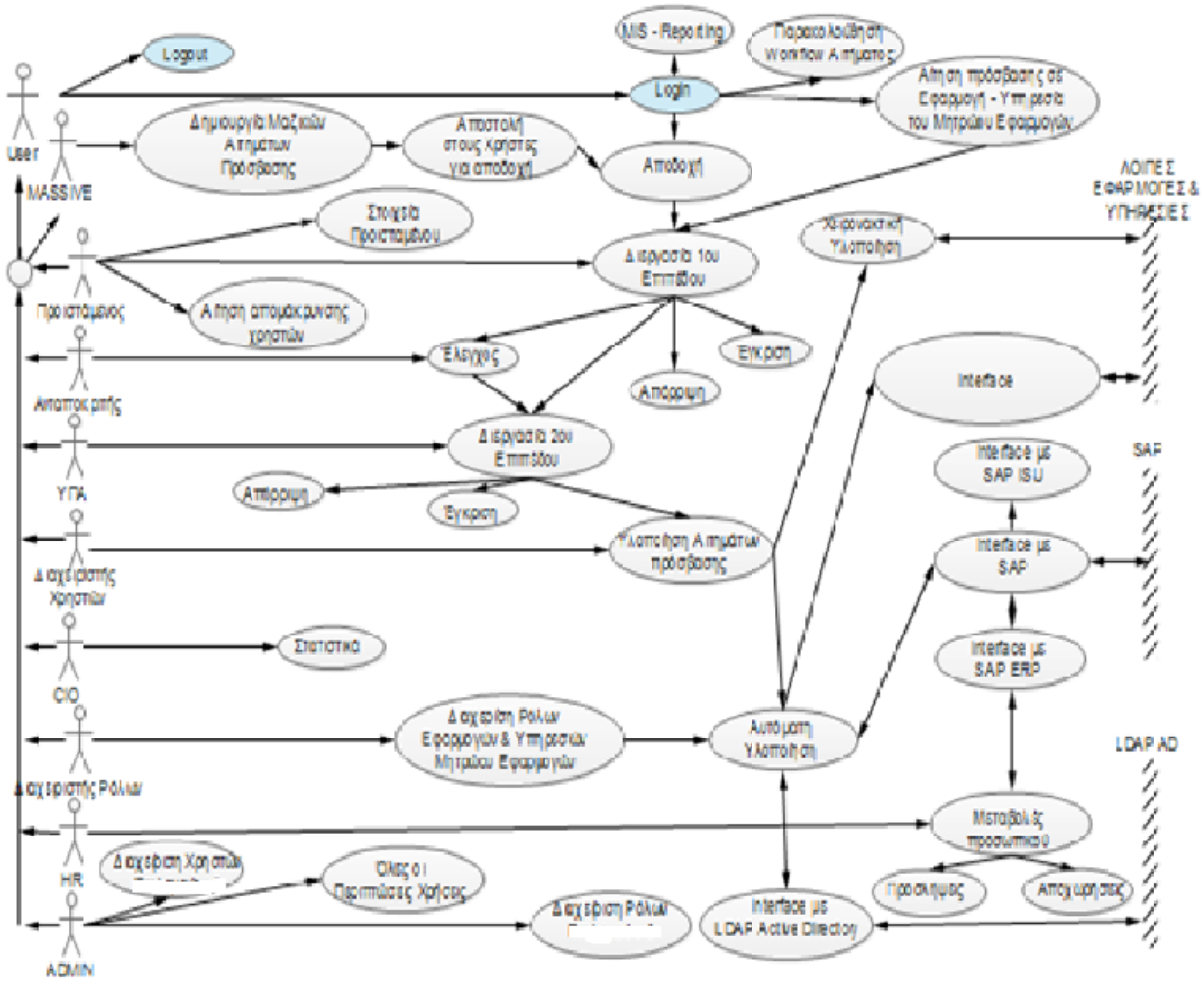
3.2.3.8 Human Resource Management (HR) – ΔΑΝΠΟ Διαχ. Μεταβολών HR

Αφορά την Διαχείριση των Υπαλλήλων της Επιχείρησης. Ανήκει στο HR.

3.2.3.9 Application Super User (Admin) - Διαχειριστής Εφαρμογής (RPM)

Αφορά τον διαχειριστή της Εφαρμογής SAT (Secure Authorization Ticketing)

3.2.4 Συγκεντρωτικό Διάγραμμα Περιπτώσεων Χρήσης



Εικόνα 4 Διάγραμμα Περιπτώσεων Χρήσης

3.2.5 Αναλυτική περιγραφή Περιπτώσεων Χρήσης

Στον Πίνακα που υπάρχει στο τέλος της πτυχιακής ΠΑΡΑΡΤΗΜΑ Γ, εμφανίζονται όλες οι περιπτώσεις χρήσης που προέκυψαν από την ανάλυση απαιτήσεων. Η αναλυτική περιγραφή για λόγους χώρου δεν μπορεί να παρουσιαστεί στο παρόν κείμενο. Στη συνέχεια αναφέρονται ενδεικτικά με ανάλυση οι πιο χαρακτηριστικές από αυτές. Μέσα από αυτές τις περιπτώσεις χρήσεις, οι οποίες αποτυπώνονται όπως καταγράφηκαν στα διάφορα στάδια ανάπτυξης του πληροφοριακού συστήματος, γίνεται εμφανές ότι υπάρχουν εκλεπτύνσεις και διορθώσεις στην αρχική και στις ενδιάμεσες καταγραφές με στόχο το όσο το δυνατόν καλύτερο τελικό αποτέλεσμα. Το σύνολό τους υπάρχει στην ομάδα έργου και μπορεί να διατεθεί εφόσον ζητηθεί.

3.2.6 Περιπτώσεις χρήσης (παραδείγματα)

Οι περιπτώσεις χρήσης που περιγράφονται αναλυτικά (Σύνδεση στο σύστημα, Δημιουργία αιτήματος, Παρακολούθηση πορείας αιτήματος, Έγκριση/Απόρριψη αιτήματος από τον Ιδιοκτήτη και Διαχείριση/Υλοποίηση αιτήματος) αφορούν διεργασίες που χρησιμοποιούνται από τους χρήστες, και τους τεχνικούς διαχείρισης προσβάσεων συστηματικά.

ΣΥΝΔΕΣΗ ΧΡΗΣΤΗ ΣΤΟ ΣΥΣΤΗΜΑ – CONNECT

ΠΡΟΔΙΑΓΡΑΦΗ ΠΕΡΙΠΤΩΣΗΣ ΧΡΗΣΗΣ

1. **Τίτλος Περίπτωσης χρήσης:**

   Σύνδεση χρήστη στο πληροφοριακό σύστημα

1.1 Σύντομη περιγραφή:

Σε αυτήν την περίπτωση χρήσης περιγράφεται η διαδικασία σύνδεσης ενός χρήστη στο πληροφοριακό σύστημα.

1.2. Χειριστές:

Χρήστες εσωτερικού δικτύου της Επιχείρησης (Active Directory Users)

2. **Ροή γεγονότων**

2.1.Βασική ροή

1. Ο χρήστης επιλέγει το url της εφαρμογής.
2. Στην οθόνη εμφανίζεται φόρμα για εισαγωγή των στοιχείων του χρήστη με τα οποία συνδέεται στο εσωτερικό δίκτυο της Επιχείρησης (Active Directory)
3. Ο χρήστης συμπληρώνει τα στοιχεία του (user name & password)
4. Το σύστημα ελέγχει αν τα στοιχεία είναι τα ορθά με βάση την υποδομή του LDAP MS AD και τα βρίσκει σωστά.
5. Το σύστημα συνδέει τον χρήστη στην εφαρμογή.
6. Το σύστημα εμφανίζει στον χρήστη τα στοιχεία του, τους ρόλους του και πρόσθετες πληροφορίες που ο χρήστης επιθυμεί να καταχωρήσει στο σύστημα.
7. Το σύστημα έχει υλοποιήσει σύνδεση με την βάση δεδομένων και έχει αφιερώσει ένα session στον χρήστη (tread)

1.1.Εναλλακτικές ροές

2.2.1.. Εναλλακτική ροή 1

1. Στο σημείο 3 της ορθής ροής ο χρήστης συμπληρώνει λανθασμένα στοιχεία (username ή password).
2. Το σύστημα εμφανίζει μήνυμα στον χρήστη «η αυθεντικοποίηση απέτυχε. Παρακαλώ προσπαθήστε ξανά».
3. Το σύστημα επιστρέφει στην ορθή ροή στο σημείο 4.

3. Μη λειτουργικές απαιτήσεις

Δεν υπάρχουν σε αυτήν την περίπτωση χρήσης

4. Κατάσταση εισόδου

1. Ο χρήστης είναι συνδεμένος στο εσωτερικό δίκτυο της επιχείρησης.

5.. Κατάσταση εξόδου

1. Ο χρήστης είναι συνδεμένος στο εσωτερικό δίκτυο της επιχείρησης. Ο χρήστης μετά την επιτυχή έκβαση της περίπτωσης χρήσης είναι συνδεδεμένος στην εφαρμογή.

ΔΗΜΙΟΥΡΓΙΑ ΑΙΤΗΜΑΤΟΣ ΠΡΟΣΒΑΣΗΣ

ΠΡΟΔΙΑΓΡΑΦΗ ΠΕΡΙΠΤΩΣΗΣ ΧΡΗΣΗΣ

1. Τίτλος Περίπτωσης χρήσης:

Δημιουργία αιτήματος

1.1 Σύντομη περιγραφή:

Σε αυτήν την περίπτωση χρήσης ο χρήστης υλοποιεί ένα αίτημα για πρόσβαση είτε δική του σε εφαρμογή είτε για νέο υπάλληλο της επιχείρησης.

1.2. Χειριστές:

Χρήστες εσωτερικού δικτύου της Επιχείρησης (Active Directory Users)

Ροή γεγονότων

1.1 Βασική ροή

1. Το σύστημα εμφανίζει πεδίο αναζήτησης εφαρμογής για την οποία θα γίνει το αίτημα πρόσβασης (μητρώο εφαρμογών και υπηρεσιών)
2. Ο χρήστης συμπληρώνει στο πεδίο την εφαρμογή ή επιλέγει την εφαρμογή ή υπηρεσία.

3. Το σύστημα εμφανίζει οθόνη που είναι ήδη συμπληρωμένα τα στοιχεία του αιτούντα.
4. Ο χρήστης συμπληρώνει τον επιχειρησιακό αριθμό μητρώου του προϊσταμένου του.
5. Ο χρήστης συμπληρώνει εφόσον το επιθυμεί και σχόλια στο πεδίο σχολίων.
6. Ο χρήστης υποβάλει το αίτημα.
7. Το σύστημα δρομολογεί το αίτημα στον προϊστάμενο για έγκριση.
8. Το σύστημα ενημερώνει την ροή αιτήματος με την κατάσταση «σε αναμονή χρώματος πορτοκαλί» σε κάθε σημείο έγκρισης.

2.2 Εναλλακτικές ροές

2.2.1.. Εναλλακτική ροή 1

1. Ο χρήστης επιλέγει άλλη λειτουργικότητα.

2. Το σύστημα τον δρομολογεί στην αρχική οθόνη της άλλης λειτουργικότητας.

4. **Μη λειτουργικές απαιτήσεις**

Δεν υπάρχουν σε αυτήν την περίπτωση χρήσης

5. **Κατάσταση εισόδου**

Ο χρήστης είναι ήδη συνδεδεμένος στην εφαρμογή.

6. **Κατάσταση εξόδου**

Ο χρήστης έχει κάνει αίτημα πρόσβασης σε εφαρμογή ή υπηρεσία του μητρώου εφαρμογών.

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΠΟΡΕΙΑΣ ΑΙΤΗΜΑΤΟΣ

ΠΡΟΔΙΑΓΡΑΦΗ ΠΕΡΙΠΤΩΣΗΣ ΧΡΗΣΗΣ

1. **Τίτλος Περίπτωσης χρήσης:**

Παρακολούθηση πορείας αιτήματος που έχει γίνει από κάποιο χρήστη του εσωτερικού δικτύου

1.1 Σύντομη περιγραφή:

Σε αυτήν την περίπτωση χρήσης περιγράφεται η διαδικασία που ένας χρήστης βλέπει την πορεία του αιτήματος του.

1.2. Χειριστές:

Χρήστες εσωτερικού δικτύου της Επιχείρησης (Active Directory Users)

3. **Ροή γεγονότων**

2.1.Βασική ροή

1. Ο χρήστης είναι συνδεδεμένος στην εφαρμογή.
2. Από το μενού επιλέγει τα νέα αιτήματα.
3. Στην οθόνη του χρήστη εμφανίζεται το αίτημά του και χρωματική αναπαράσταση που δείχνει από ποιους έχει εγκριθεί και αν έχει υλοποιηθεί. Η χρωματική αναπαράσταση είναι πράσινη εφόσον το αίτημά του έχει εγκριθεί, πορτοκαλί αν εκκρεμεί έγκριση και κόκκινη αν έχει απορριφθεί.

1.2.Εναλλακτικές ροές

2.2.1.. Εναλλακτική ροή 1

1. Ο χρήστης επιλέγει άλλη λειτουργικότητα στο σημείο 2.
2. Το σύστημα δρομολογείται στην νέα λειτουργικότητά που έχει ζητηθεί.

3. Μη λειτουργικές απαιτήσεις

Δεν υπάρχουν σε αυτήν την περίπτωση χρήσης

4. Κατάσταση εισόδου

1. Ο χρήστης είναι συνδεμένος στο εσωτερικό δίκτυο της επιχείρησης και στην εφαρμογή.

5.. Κατάσταση εξόδου

1. Ο χρήστης είναι συνδεμένος στο εσωτερικό δίκτυο της επιχείρησης. Ο χρήστης μετά την επιτυχή έκβαση της περίπτωσης χρήσης είναι συνδεδεμένος στην εφαρμογή και παρακολουθεί την έκβαση της ροής «workflow».

ΕΓΚΡΙΣΗ/ΑΠΟΡΡΙΨΗ ΑΙΤΗΜΑΤΟΣ ΑΠΟ ΤΟΝ ΙΔΙΟΚΤΗΤΗ ΕΦΑΡΜΟΓΗΣ

ΠΡΟΔΙΑΓΡΑΦΗ ΠΕΡΙΠΤΩΣΗΣ ΧΡΗΣΗΣ

2. Τίτλος Περίπτωσης χρήσης:

Έγκριση ή απόρριψη αιτήματος από τον ιδιοκτήτη εφαρμογής.

1.1 Σύντομη περιγραφή:

Σε αυτήν την περίπτωση χρήσης περιγράφεται η διαδικασία που ο ιδιοκτήτης μίας εφαρμογής για την οποία έχει οριστεί ως υπεύθυνος επεξεργασίας, εγκρίνει ή απορρίπτει ένα αίτημα που τον αφορά.

1.2. Χειριστές:

Χρήστες εσωτερικού δικτύου της Επιχείρησης (Active Directory Users)

4. Ροή γεγονότων

2.1.Βασική ροή

1. Ο ιδιοκτήτης της εφαρμογής είναι συνδεδεμένος στην σύστημα.
2. Από το μενού επιλέγει με βάση τον ρόλο του «ΥΠΑ» τα νέα αιτήματα.
3. Στην οθόνη του χρήστη εμφανίζεται το αίτημά που του έχει αποσταλεί με την έγκριση του προϊσταμένου και την έγκριση του βοηθού του.
4. Ο ιδιοκτήτης επιλέγει το αίτημα και του ανοίγει pdf.
5. Ο ιδιοκτήτης το εγκρίνει με την χρήση της ψηφιακής του υπογραφής.
6. Ο ιδιοκτήτης το υποβάλει προς υλοποίηση.
7. Το σύστημα ενημερώνει την ροή με την κατάσταση έγκρισης (χρωματική αναπαράσταση πράσινη από τον ιδιοκτήτη).
8. Το σύστημα δρομολογεί το αίτημα στο τεχνικό τμήμα για υλοποίηση.

1.3.Εναλλακτικές ροές

2.2.1.. Εναλλακτική ροή 1

1. Στο σημείο 7 ο ιδιοκτήτης αφού δει τα στοιχεία του αιτήματος κλείνει το pdf.
2. Ο χρήστης απορρίπτει το αίτημα.
3. Το σύστημα ενημερώνει την κατάσταση της ροής με την απόρριψη (χρωματική αναπαράσταση κόκκινη). Το αίτημα δεν δρομολογείται στο τεχνικό τμήμα.

2.2.2.. Εναλλακτική ροή 2

Στο σημείο 6 εμφανίζεται το αίτημα που ανήκει στον ιδιοκτήτη χωρίς την αξιολόγηση του βοηθού του (σε αναμονή – πορτοκαλί). Συνεχίζει στην βασική ροή από το βήμα 7.

3. Μη λειτουργικές απαιτήσεις

Δεν υπάρχουν σε αυτήν την περίπτωση χρήσης

4. Κατάσταση εισόδου

Ο χρήστης είναι συνδεμένος στο εσωτερικό δίκτυο της επιχείρησης και στην εφαρμογή.

5.. Κατάσταση εξόδου

Η ροή του αιτήματος έχει σταματήσει με απόρριψη. Ο χρήστης μπορεί να ενημερωθεί από τα ιστορικά που διατηρεί το σύστημα και την ροή του.

ΔΙΑΧΕΙΡΙΣΗ/ΥΛΟΠΟΙΗΣΗ ΑΙΤΗΜΑΤΟΣ

ΠΡΟΔΙΑΓΡΑΦΗ ΠΕΡΙΠΤΩΣΗΣ ΧΡΗΣΗΣ

3. Τίτλος Περίπτωσης χρήσης:

Υλοποίηση αιτήματος από το αρμόδιο τμήμα.

1.1 Σύντομη περιγραφή:

Σε αυτήν την περίπτωση χρήσης περιγράφεται η διαδικασία που ο τεχνικός διαχειριστής χρηστών εντοπίζει το αίτημα μέσα από το ticket. Ο τεχνικός το αναλαμβάνει και το υλοποιεί.

1.2. Χειριστές:

Χρήστες εσωτερικού δικτύου της Επιχείρησης (Active Directory Users) που διαθέτουν τον ρόλο του

Τεχνικού διαχειριστή χρηστών.

5. Ροή γεγονότων

2.1.Βασική ροή

1. Ο τεχνικός ασφάλειας προσβάσεων επιλέγει από το μενού τα νέα αιτήματα.
2. Του εμφανίζονται τα αιτήματα που έχουν εγκριθεί και αφορούν εφαρμογές που του έχει οριστεί να κάνει την διαχείριση των χρηστών.
3. Ο τεχνικός επιλέγει το αίτημα και αυτό κλειδώνεται με αποτέλεσμα να μην μπορεί να το αναλάβει άλλος τεχνικός διαχειριστής χρηστών.
4. Ο τεχνικός υλοποιεί το αίτημα και ενημερώνει το σύστημα ότι υλοποιήθηκε.
5. Το σύστημα καταχωρεί στην ροή την κατάσταση υλοποίησης.

1.4.Εναλλακτικές ροές

2.2.1.. Εναλλακτική ροή 1

1. Στο σημείο 4 ο τεχνικός απελευθερώνει το αίτημα προς επίλυση με σχολιασμό λόγο αδυναμίας υλοποίησης (escalation).

2. Το σύστημα επιστρέφει στο βήμα 2 της κανονικής ροής.

3. Μη λειτουργικές απαιτήσεις

Δεν υπάρχουν σε αυτήν την περίπτωση χρήσης

4. Κατάσταση εισόδου

2. Ο χρήστης είναι συνδεμένος στην εφαρμογή και έχει τον ρόλο υλοποίησης αιτημάτων.

5.. Κατάσταση εξόδου

2. Το αίτημα έχει υλοποιηθεί.

3.3 Κλάσεις Εφαρμογής (όγκος & ασφάλεια)

Οι κλάσεις της Εφαρμογής είναι πάνω από 200 με 24000 γραμμές. Περιέχουν συνοπτικά το business logic, το configuration της Βάσης Δεδομένων (αρχικοποίηση), την εμφάνιση των ιστοσελίδων στον χρήστη και ενσωματώνουν δικλείδες ασφαλείας από την μεριά του κώδικα σε επίπεδο url και σε επίπεδο συνάρτησης.

- SQL Injection (Angular)
- JSON Hijacking Protection (Angular)
- Cross Site Request Forgery (XSRF/CSRF) (Angular)
- Firewall στα URL (Java Spring)
- Functional Security (Java Spring)
- JWT AUTHENTICATION (Json Web Token) – (Angular, Java Spring)
- SPRING COOKIE THREAT PROTECTION – CTP (Angular, Java Spring)

Χρήση JWT & προστασία από vulnerabilities:

- Cross-domain/CORS cookies + CORS δεν επιτρέπουν

την υλοποίηση αιτημάτων σε άλλα domain

- Replay Attacks προστασία από επιθέσεις παλαιών

token που έχουν υποκλαπεί από τρίτους

- Statelessδεν αποθηκεύεται στη μεριά του server

κάποιο αναγνωριστικό του χρήστη (header, payload, signatures)

- CSRF δεν χρειάζεται κάποια ιδιαίτερη προστασία για τα cross-site requests, εκτός από την

προτεινόμενη αποθήκευσή του στο sessionStorage του browser

4. Ασφάλεια Πληροφοριακού Συστήματος

Στην φάση που αφορά την Ασφάλεια του Πληροφοριακού Συστήματος έγινε ο σχεδιασμός και η υλοποίηση της Ασφάλειας Πληροφοριών (Σύστημα Διαχείρισης Ασφάλειας Πληροφορικών – ISMS, Πλαίσιο και επιμέρους Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων, Ανάλυση Επικινδυνότητας & Επιπτώσεων) με πρότυπο ISO/IEC 27001. Τα μέτρα και οι κατηγορίες που αφορούν το παραπάνω πρότυπο εμφανίζονται στο ΠΑΡΑΡΤΗΜΑ Δ.

Συντάχθηκαν έγγραφα που αφορούν την Ασφάλεια όπως Πολιτική Ασφάλειας που περιέχει και τις επιμέρους εμπλεκόμενες πολιτικές με βάση το ISO/IEC 27001/2013ΠΑΡΑΡΤΗΜΑ Δ.

Επιλέχθηκε η μεθοδολογία ανάλυσης Επικινδυνότητας και υλοποιήθηκε και μία ανάλυση επιχειρησιακής επιπλοκής (Business Impact Analysis). Στην φάση ικανοποιείται η αρχή της ασφάλειας κατά τον σχεδιασμό «security on design» και υλοποιείται ενσωμάτωσή της στον κύκλο ζωής λογισμικού «built in security»

Πλέον των παραπάνω σχεδιάστηκαν τα βασικά σημεία που θα έπρεπε η Εφαρμογή να ακολουθήσει για να καλύψει το θέμα που πραγματεύεται το κεφάλαιο.

Αυτά είναι:

4.1 Δικλείδες Ασφαλείας που εφαρμόστηκαν για θέματα Διοίκησης Ασφάλειας Πληροφοριακού Συστήματος

- **Διαφύλαξη της εμπιστευτικότητας** καθώς η πληροφορία πρέπει να αποκαλύπτεται μόνο σε εξουσιοδοτημένα άτομα ή οντότητες. Για την διαφύλαξή της υλοποιήθηκε η πιστοποιημένη είσοδος στις εφαρμογές με την διασύνδεση με το LDAP της Επιχείρησης.
- **Διαφύλαξη της Ακεραιότητας** καθώς τα δεδομένα πρέπει να διατηρούνται χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα υλοποιείται η αποτροπή της πρόσβασης σε άτομα χωρίς άδεια έτσι ώστε η πληροφορία να παραμένει ακριβής και πλήρης. Για την διαφύλαξη της ακεραιότητας εφαρμόζονται τεχνικές παρακολούθησης πρόσβασης κρυπτογράφησης, Ψηφιακές Υπογραφές, διαχωρισμός καθηκόντων & διαβαθμισμένη πρόσβαση χρηστών.

- Εφαρμόστηκε **η Αρχή Ελαχίστων Προνομίων.** Τα προνόμια χρηστών περιορίζονται στα απολύτως απαραίτητα για την εκτέλεση των καθηκόντων τους.
- Εφαρμόστηκε **η Αρχή Περιορισμού της Γνώσης.** Τα δικαιώματα πρόσβασης των χρηστών περιορίζονται στην ελάχιστη γνώση για την εκτέλεση των καθηκόντων τους.
- Εφαρμόστηκε **η Αρχή αναλογικότητας.** Διατηρούνται τα απολύτως απαραίτητα δεδομένα
- **Αρχή μη Αποποίησης** (πχ Ψηφιακές Υπογραφές) - Η Ασφαλής Διάταξη που χρησιμοποιήθηκε είναι πιστοποιημένη κατά FIPS 140-2 level 3 & Common Criteria EAL4+ ως απομακρυσμένη λύση διακομιστή ψηφιακών υπογραφών βασισμένη σε H/W (hardware based remote signing server solution) με πρότυπα ασφαλείας (κατά NIST, ITU, ETSI, CC κλπ.).
- Έγινε ανάλυση επικινδυνότητας **πριν την υλοποίηση** και τεχνική ανάλυση επικινδυνότητας πριν την παραγωγή.

4.2 Δικλείδες Ασφαλείας που εφαρμόστηκαν για τεχνικά θέματα Ασφάλειας Πληροφοριακού Συστήματος

- Έγινε κρυπτογράφηση των δεδομένων στο επίπεδο της ΒΔ (**tablespace encryption Transparent Data Encryption TDE – Oracle Wallet**).

  Η διαδικασία είναι:

  1 Πριν ακόμα δημιουργηθεί το tablespace & ο schema user στην ΒΔ oracle υλοποιούμε έναν κατάλογο στον χρήστη RDBMS του λειτουργικού συστήματος που θα φιλοξενήσει το wallet και τον δηλώνουμε στο αρχείο παραμέτρων της με την ονομασία sqlnet.ora.

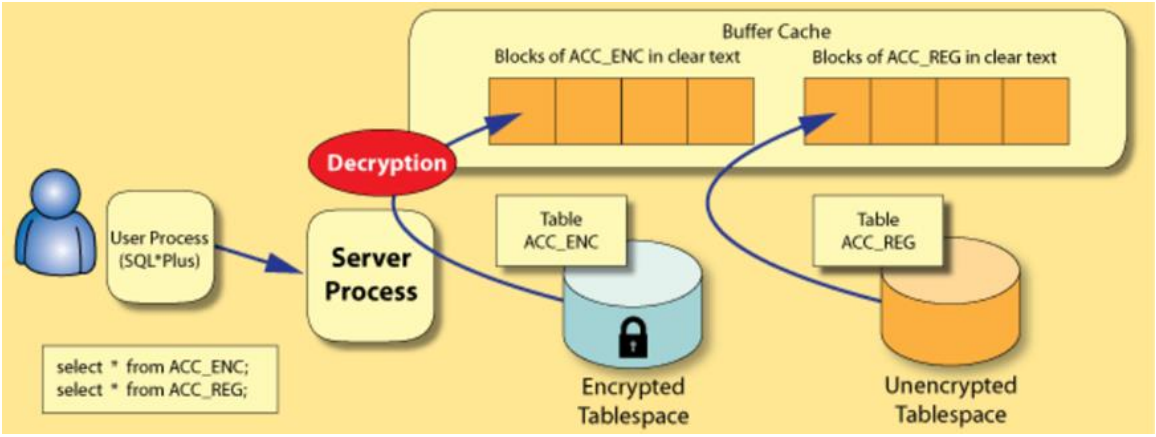
  2 Στην συνέχεια μέσα από το περιβάλλον sql εντολών της, την sqlplus με δικαιώματα syskm χρήστη (χρήστη key management) για τα κλειδιά του wallet δημιουργούνται τα tablespace με την κωδικοποίηση που θέλουμε να κρυπτογραφήσουμε. Οι επιλογές κρυπτογράφησης είναι AES 128, AES 192, AES 256 3 key Triple DES 168 bits key. Επίσης υπάρχει η δυνατότητα να κρυπτογραφηθεί μόνο ένα πεδίο ενός πίνακα με χρήση SALT που αφορά

ψευδοτυχαίο αριθμό. Τέλος για θέματα ακεραιότητας πίνακα μπορεί να χρησιμοποιηθεί είτε SHA1 είτε NAC.

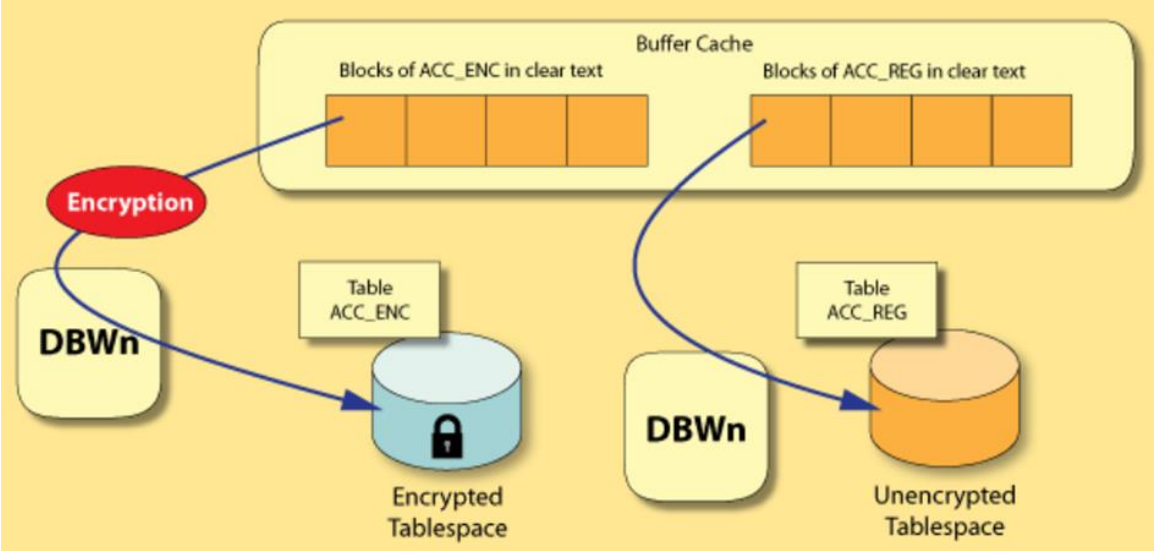
3 Μετά δημιουργείται ο schema user (ιδιοκτήτης αντικειμένων βάσης) και του δίνεται ως tablespace το παραπάνω.

Το wallet είναι ένας τρόπος για να αποθηκεύεις στην oracle τα κλειδιά (private keys) και για αυτό τον λόγο χρειάζεται και το wallet κλειδί. Είτε αφορά το TDE είτε το ssh για την διασύνδεση της database με τον application server το wallet λειτουργεί ως θεματοφύλακας private keys. Για την υλοποίηση του wallet απαιτείται ένα κλειδί «passphrase» ώστε να έχουμε την δυνατότητα να έχουμε πρόσβαση στα certificates. Για παράδειγμα ένα certificate είναι αυτό που χρησιμοποιείται για την επικοινωνία μεταξύ του application server & του database server. Το κλειδί με το οποίο έχουμε κρυπτογραφήσει το wallet συμμετρικά (AES192) φυλάσσεται σε usb αφαιρούμενο δίσκο. Για λόγους αποφυγής μοναδικού σημείου αστοχία δημιουργείται αντίγραφο που φυλάσσεται σε disaster site.

Το TDE προστατεύει τα δεδομένα στην κατάσταση «data at rest» δηλαδή από διαρροή δεδομένων που είναι αποθηκευμένα στην βάση.



Εικόνα 5 Ανέβασμα των data από το κρυπτογραφημένο Tablespace στην μνήμη



Εικόνα 6 Κατέβασμα των δεδομένων από την μνήμη στο κρυπτογραφημένο tablespace

Έγινε χρήση TLS/SSL για την ασφαλή χρήση στην εφαρμογή (https). Ασφαλής επικοινωνία client server. Χρησιμοποιήθηκε RSA 2048 bit και το ssl connection είναι 256 bit. Χρησιμοποιείται η πιστοποιημένη CA στο εύρος του ενδοδικτύου. Η διαδικασία του Key Exchange γίνεται όπως αυτό περιγράφεται στο url https://tools.ietf.org/html/rfc4346#appendix-F.1.1.

Αναλυτικά έγινε (σχετικά με την κρυπτογραφημένη επικοινωνία):

Λειτουργία Πρωτοκόλλου SSL/TLS. Μόλις καλούμε μια σελίδα https:// ο browser στέλνει τα στοιχεία του στο server με τις εκδόσεις SSL και TLS που υποστηρίζει, τους αλγόριθμους για την κρυπτογράφηση δεδομένων, και τα στοιχεία που αφορούν το session (πχ ημερομηνία και ώρα έναρξης) και γενικά όσα στοιχεία χρειάζεται για να γίνει η σύνδεση. Στην συνέχεια ο web server της σελίδας στέλνει τα αντίστοιχα στοιχεία του όσον αφορά το SSL/TLS, τους αλγόριθμους, το session κλπ. και το ψηφιακό πιστοποιητικό του (digital certificate). Μετά ο browser ελέγχει:

- Αν το ψηφιακό πιστοποιητικό/digital certificate προέρχεται από μια πιστοποιημένη Certificate Authority (CA) – Αρχή Πιστοποίησης
- Αν ισχύει ακόμα
- Αν συνδέεται με το site που έχουμε μπει.

Εφόσον όλα είναι ορθά, ο server στέλνει το δημόσιο κλειδί στον browser (2048 bit) και ο browser χρησιμοποιεί το δημόσιο κλειδί για να δημιουργήσει ένα τυχαίο συμμετρικό κλειδί (session id 32 byte).

Το συμμετρικό αυτό κλειδί αποστέλλεται στο server, και χρησιμοποιείται σε όλη τη διάρκεια της σύνδεσης (session) για την κρυπτογράφηση δεδομένων τύπου συμμετρικού κλειδιού (AES 256). Μόλις γίνει αποσύνδεση (πχ log-out ή λήξει το session), ο υπολογιστής μας και ο web server καταστρέφουν το Συμμετρικό κλειδί. Σε μία επόμενη – νέα σύνδεση, θα δημιουργηθεί ένα εντελώς νέο συμμετρικό κλειδί. Ο αλγόριθμος κρυπτογράφησης του δημόσιου/ασύμετρου κλειδιού που χρησιμοποιείται με το TLS είναι ο RSA.

- Angular & Spring από **Cross-site scripting – XSS Injection** (π.χ. αφορά ευπάθεια που επιτρέπει κλοπή κωδικών/λογαριασμών κλπ προσωπικών δεδομένων, Αλλαγή ρυθμίσεων του site, κλοπή των *cookies, ψ*εύτικη διαφήμιση):

  Ένας τρόπος για να γίνεται sql injection είναι η προσπάθεια του να μεταβληθεί το DOM (Document Object Model) μέσω κακόβουλου java script κώδικα. Με την χρήση της Angular δεν γίνεται χρήση του DOM από την HTML για την παρουσίαση των δεδομένων από την ιστοσελίδα. Η Angular δεν το επιτρέπει καθώς τα δεδομένα τα προβάλει μέσω ng-bind που είναι ένα διαφορετικός τρόπος διαχείρισης (echo) του μοντέλου των object που χρησιμοποιεί.

```
<li>
    <label for="auditorColumns">
        <input ng-model="auditorColumns" id="auditorColumns"
</li>
```

Εικόνα 7 Αφορά την δήλωση στον html κώδικα της Angular είναι το γνωστό GET

- Angular Έγινε διαφύλαξη από **SQL Injection** (δεν επιτρέπεται σε κακόβουλο να αλλάξει ότι θέλει στην βάση δεδομένων ή και να πάρει πληροφορίες)

- Angular **JSON Hijacking Protection** Το JSON Hijacking γίνεται εφόσον ο server έχει πρόθεμα σε όλα τα JSON αιτήματα το string ")]}',\n". Η Angular αυτόματα βγάζει πριν την επεξεργασία των JSON το πρόθεμα και δεν επιτρέπει την εκμετάλλευση της ευπάθειας.

- Spring Angular **JWT AUTHENTICATION (JASON WEB TOKEN)** STATELESS SECURITY MECHANISM (για προστασία από cookie) αφορά την εξέλιξη του OATH2 που το χρησιμοποιεί το facebook (προστασία που δίνει το spring). Το OATH αφορά τεχνική που κάνει USER AUTHENTICATION. Αντί να βάζουμε cookies ενεργοποιούμε το OAUTH. Είναι μέρος του Spring χρησιμοποιείται στο backend

- Spring **COOKIE THREAT PROTECTION** (CTP αφορά κακόβουλη ενέργεια μέσω της οποίας μπορεί να υποκλαπεί η προσβασιμότητα.). Η λύση που χρησιμοποιείται αφορά την δημιουργία νέου cookie κάθε φορά που ο χρήστης συνδέεται στο σύστημα. Αφορά προστασία που δίνεται από το backend spring. & Angular

- Angular – Spring Έγινε διαφύλαξη από **Cross Site Request Forgery (XSRF/CSRF)** που αφορά επίθεση που αναγκάζει τον τελικό χρήστη να εκτελέσει ανεπιθύμητες ενέργειες σε μια εφαρμογή δικτύου στην οποία είναι πιστοποιημένος. (προστασία που δίνει η Angular – front end και το Spring Backend)

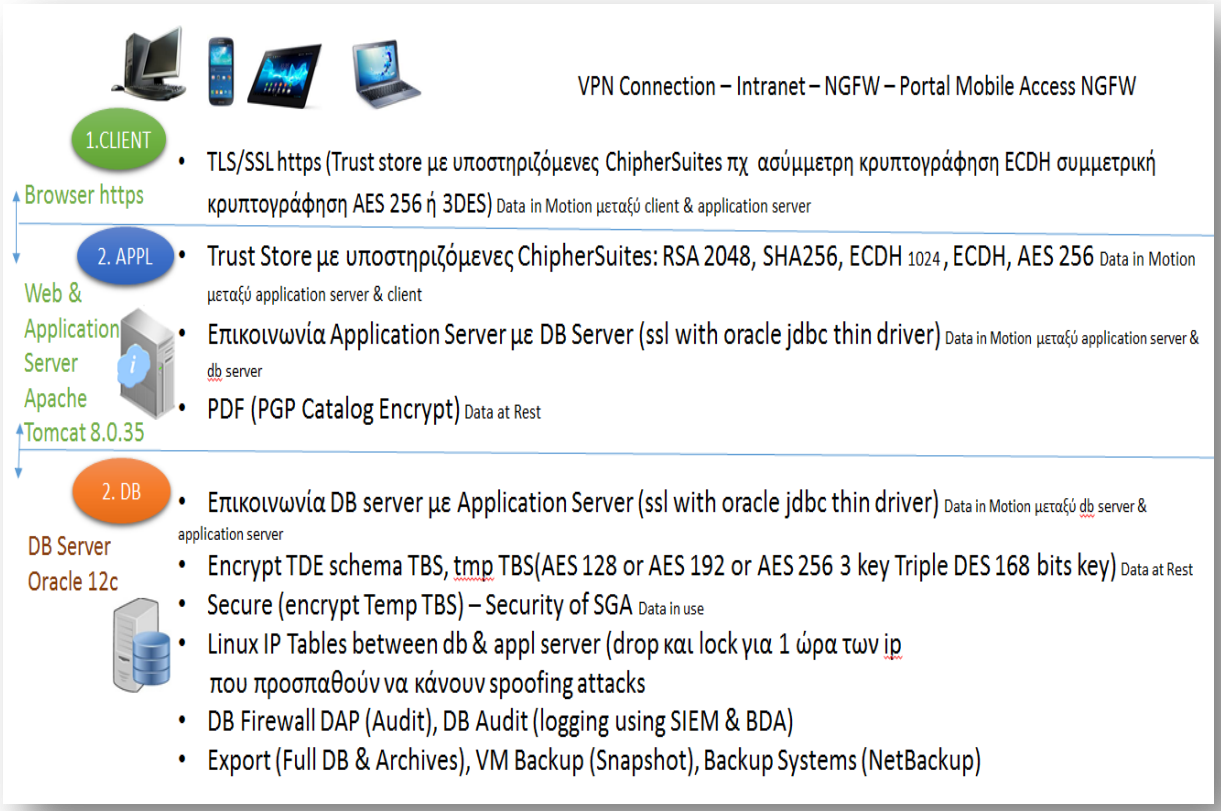
  Μέσω λειτουργιών που δίνονται από το Spring έχει γίνει χρήση ενός φίλτρου που αφορά την διασφάλιση από XSRF της Angular. Είναι το CSRF του Spring (διαφορετική ονομασία). Εδώ γίνεται χρήση την κεφαλίδα δεν είναι αυτό που σχετίζεται με την συνεδρία του χρήστη, ο διακομιστής θα πρέπει να απορρίψει την αίτηση. Με την αξιοποίηση του χαρακτηριστικού XSRF αυτό διασφαλίζεται. Κατά τη διάρκεια της σύνδεσης: Γίνεται δημιουργία του διακριτικού CSRF, και συνδέεται με την συνεδρία του χρήστη. Στέλνεται ως απάντηση σύνδεσης όπως το cookie XSRF-TOKEN. Έτσι επιβεβαιώνεται ότι για όλες τις εισερχόμενες αιτήσεις API υπάρχει κεφαλίδα X-XSRF-TOKEN, και ότι η αξία της επικεφαλίδας είναι το διακριτικό που συνδέεται με την συνεδρία του χρήστη (αφορά ένα εισιτήριο που δημιουργείται για την αυθεντικοποίηση από τον server ότι μιλάει με τον client που γνωρίζει).

- **Spring Functional Security**. Μία επιπλέον διασφάλιση είναι το φίλτρο με το annotation @Secured() στις συναρτήσεις. Μέσω αυτού γίνεται ο έλεγχος του δικαιώματος για την εκτέλεση ή όχι της συνάρτησης. Χρήση του γίνεται στο java Spring.

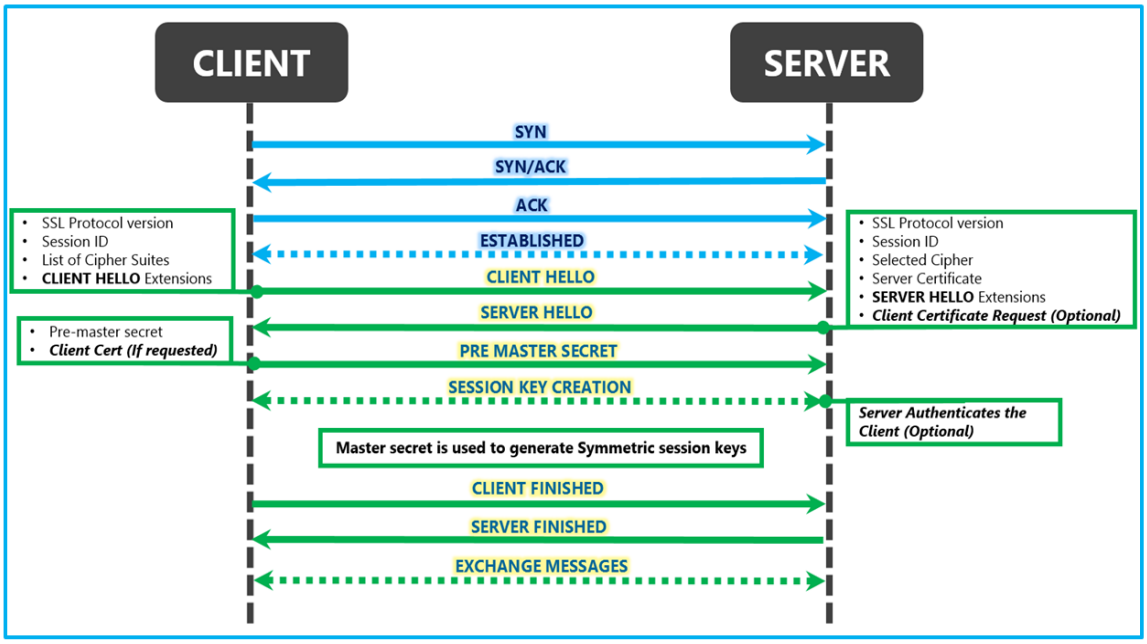
- **Spring Λογική firewall στα URL**. Έλεγχος σε μορφή firewall (url filtering). Αν το url που αιτείται ο χρήστης εμπίπτει σε κάποιο κανόνα που θέλει συγκεκριμένα credentials είτε απορρίπτεται και ελέγχεται ο επόμενος κανόνας που αν έχει τα credentials ενεργοποιείται. Ο τελευταίο κανόνας είναι reject. Οι κανόνες υπάρχουν στην κλάση security configuration του backend Spring.

- **Linux IP tables** (για την διαφύλαξη της Βάσης Δεδομένων SQL μόνο από backend). Μέσω αυτού επιτρέπεται μόνο η επικοινωνία μεταξύ DB Server & Application Server στην πόρτα 1521, όπως επίσης γίνεται drop και lock για 1 ώρα των ip που προσπαθούν να κάνουν spoofing attacks.

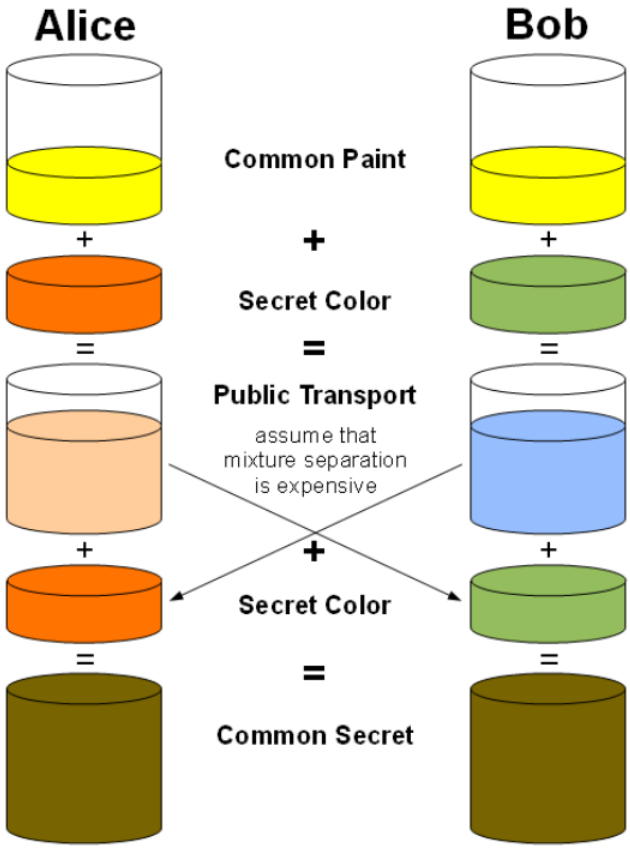
- Κρυπτογράφηση των δεδομένων κατά την επικοινωνία μεταξύ των db & webapp server & μεταξύ του webapp & των Client με τεχνικές όπως εμφανίζοναι στην παρακάτω εικόνα (data in motion, data at rest).



Εικόνα 8 Κρυπτογράφηση (data at rest, data in motion & δικλείδες data in use)



Εικόνα 9 SSL χειραψία μεταξύ του client & του Server (ή ίδια λειτουργία γίνεται και μεταξύ του DB & WEBAPP server



Εικόνα 10 Encryption common secret key for symmetric new encryption handshake Diffie Helman (για ανταλλαγή κλειδιών που χρησιμοποιούμε στον AES)

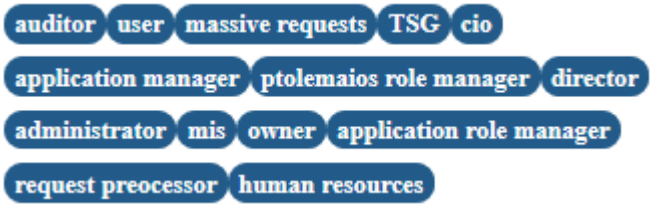
5. Σχεδίαση συστήματος

5.1 Επισκόπηση τεχνολογιών

Το σύστημα περιλαμβάνει την σχεδίαση και την κατασκευή εφαρμογής σύγχρονων τεχνολογιών (Virtualization – vmware 5.5 , Oracle Linux 7.1., Oracle 12c 12.1.0.2.0,. JAVA Spring MVC (spring secure), Front End – Angular JS, Restfull web socket, Hybernate – Elastic Search, html5, Bootstap - CSS3 , E Draw, AD LDAP SSO, iText Lib for pdf) με γλώσσα κώδικα web Application Java Spring και με την χρήση Angular Τα δεδομένα θα φυλάσσονται σε database server με rdbms oracle. 12c. Αποφασίστηκε η χρήση του συγκεκριμμένου rdbms καθώς ο όγκος είναι πολύ μεγάλος και αφορά υλοποίηση που θα εξυπηρετήσει μεγάλη Επιχείρηση.

Στο σύστημα υλοποιείται μηχανισμός ελεγχόμενης πρόσβασης χρηστών με ρόλους απλού χρήστη εσωτερικού δικτύου της επιχείρησης, προϊσταμένου, Ιδιοκτήτη εφαρμογών,

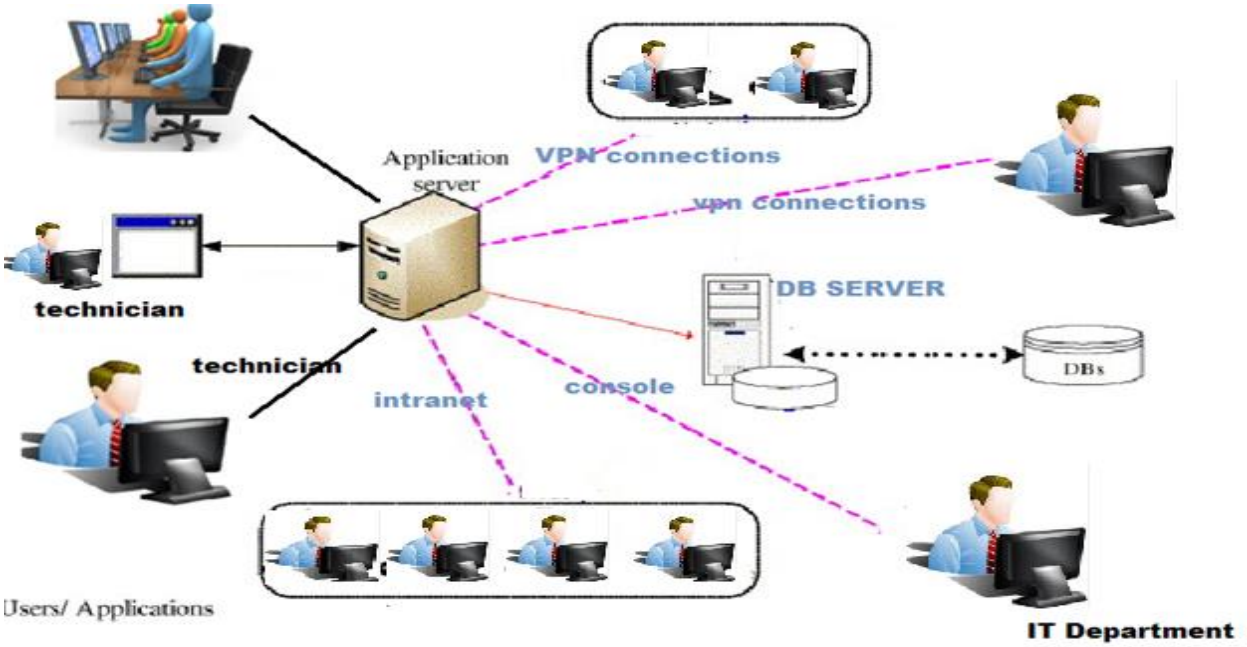
βοηθού ιδιοκτήτη εφαρμογών, MIS, τεχνικού ασφάλειας διαχείρισης χρηστών, διαχειριστή συστήματος. Οι τεχνικές ονομασίες τους θα είναι αυτές που εμφανίζονται στην εικόνα που ακολουθεί.



Εικόνα 11 Ρόλοι Εφαρμογής

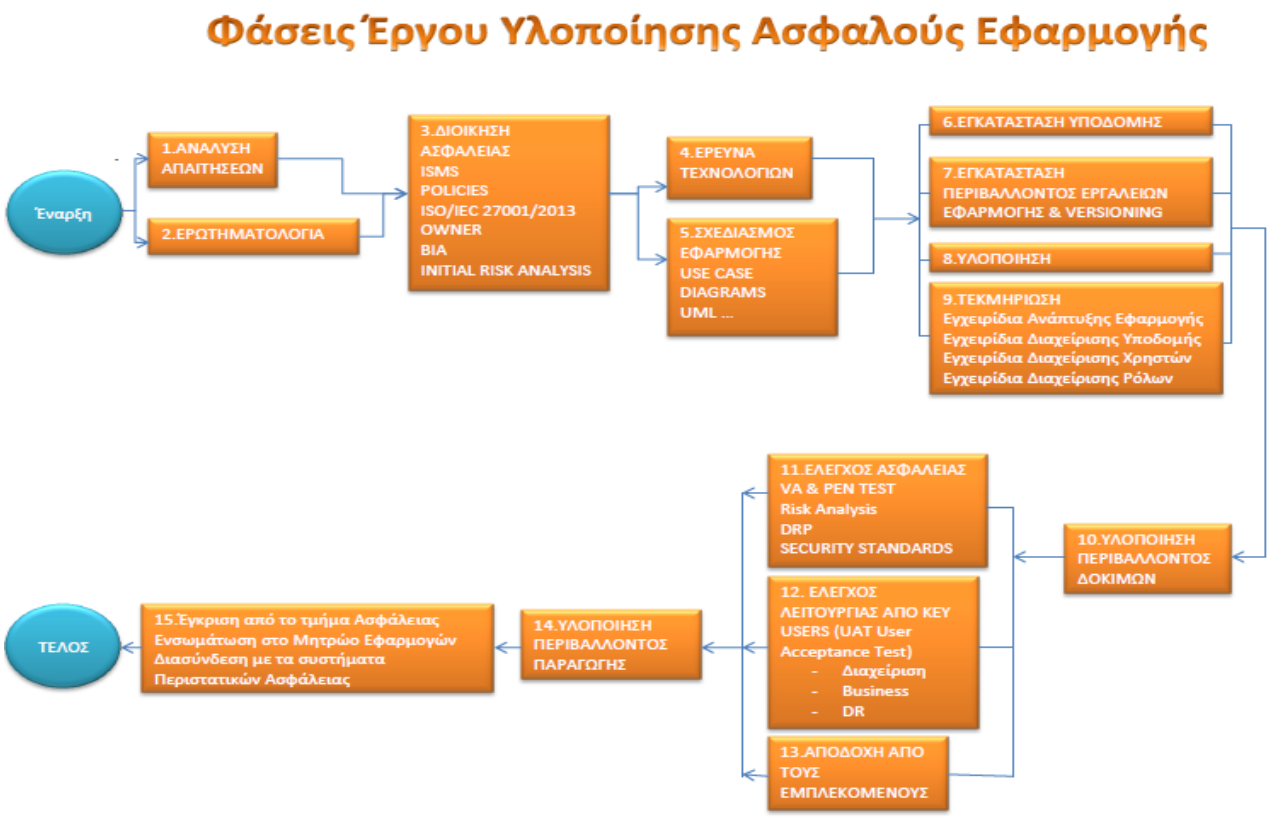
Στο σύστημα υπάρχει η λειτουργία ροής αιτημάτων με διαδικασίες αυτόματης δρομολόγησης (**workflow)**. Η λειτουργία αυτή εξυπηρετεί με την ενημέρωση ανά πάσα στιγμή των χρηστών για την πορεία και την κατάσταση του αιτήματός τους.

Το σύστημα παρέχει στατιστικά (**statistics**), υλοποιεί διαδικασίες **ticketing**. Και εξυπηρετεί το authorization & το μητρώο εφαρμογών για μεγάλο όγκο εφαρμογών και χρηστών εντός της επιχείρησης.



Εικόνα 12 Αρχιτεκτονική Εφαρμογής

Για την εκπόνησή του έργου δημιουργήθηκε ένα διάγραμμα με τις υπο-εργασίες (φάσεις) που θα έπρεπε να υλοποιηθούν όπως ακολουθεί στην επόμενη εικόνα.



Εικόνα 13 Φάσεις Έργου

5.2 Ανάλυση Επικινδυνότητας - Μελέτη για την ανάπτυξη της Μεθόδου

5.2.1 Μεθοδολογία – Εισαγωγή

Η μέθοδος της Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριακών Συστημάτων, αποτελεί ένα από τα συστατικά στοιχεία ενός Πλαισίου Ασφάλειας και περιλαμβάνει τη μεθοδολογική προσέγγιση που απαιτείται για την αναγνώριση και αποτελεσματική διαχείριση των κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριακών πόρων μίας μεγάλου μεγέθους επιχείρησης. Η μεθοδολογία η οποία βασίζεται στα διεθνή και αναγνωρισμένα πρότυπα όπως ISO 27001:2013 (ΠΑΡΑΡΤΗΜΑ Δ), ISF, NIST SP800-30, ISO27005:2011 αφορά μία ολοκληρωμένη προσέγγιση στην διαχείριση κινδύνων και στηρίζεται στην Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων (ΠΑΡΑΡΤΗΜΑ Η).

Η προσέγγιση αντιμετωπίζει την επικινδυνότητα ασφάλειας πληροφοριακών συστημάτων ως ζητήματα που αφορούν ολόκληρη την Επιχείρηση, εξετάζοντας το κόστος για την εφαρμογή μέτρων προστασίας σε συνάρτηση με τα οφέλη που προκύπτουν από τη μείωση των κινδύνων. Τα οφέλη εφαρμογής της διαδικασίας αυτής συνοψίζονται ως εξής:

- ✓ Εφαρμόζεται διαδικασία που επιτρέπει στην Επιχείρηση να επικεντρωθεί στην επίτευξη των επιχειρησιακών της στόχων (Business Objectives), μέσω της εξασφάλισης ενός αποδεκτού επιπέδου κινδύνων.
- ✓ Παρέχει στην Επιχείρηση/Οργανισμό μέσα από μία ανάλυση κόστους - οφέλους:
  - τη δυνατότητα εκτίμησης της αξίας των πληροφοριακών της πόρων
  - την αναγνώριση των απειλών και αδυναμιών
  - την εκτίμηση των σχετικών κινδύνων
  - την επιλογή των μέτρων προστασίας για τη μείωση αυτών
- ✓ Δημιουργεί ένα οργανωμένο και ελεγχόμενο ασφαλές περιβάλλον , μέσα στο οποίο η Επιχείρηση θα διαχειρίζεται την πληροφορία με διαφύλαξη της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητάς της.

5.2.2 Σκοπός και Εύρος

Σύμφωνα με το Πλαίσιο Ασφάλειας Πληροφοριακών Συστημάτων, η αξιολόγηση των κινδύνων ασφάλειας Πληροφοριακού Συστήματος αφορά μία κρίσιμη διεργασία μέσω της οποίας αρχικά αναγνωρίζονται και στην συνέχεια αντιμετωπίζονται οι κίνδυνοι οι οποίοι απειλούν την ασφάλεια των πληροφοριακών πόρων (assets). Μέσω αυτής της μεθόδου συμμορφώνεται η Επιχείρηση με εσωτερικές και εξωτερικές κανονιστικές απαιτήσεις (compliance). Επιπλέον λαμβάνει αποφάσεις με βάση το συνολικό επίπεδο αποδεκτού κινδύνου το οποίο δεν θα πρέπει να έχει απόκλιση από τον εναπομείναντα κίνδυνο εφόσον εφαρμοστούν τα μέτρα αντιμετώπισης. Η προσέγγιση που υλοποιείται οδηγεί την Αξιολόγηση Κινδύνων μέσω μιας ολιστικής προσέγγισης, σε επιτυχή έκβαση. Βασικός στόχος είναι :

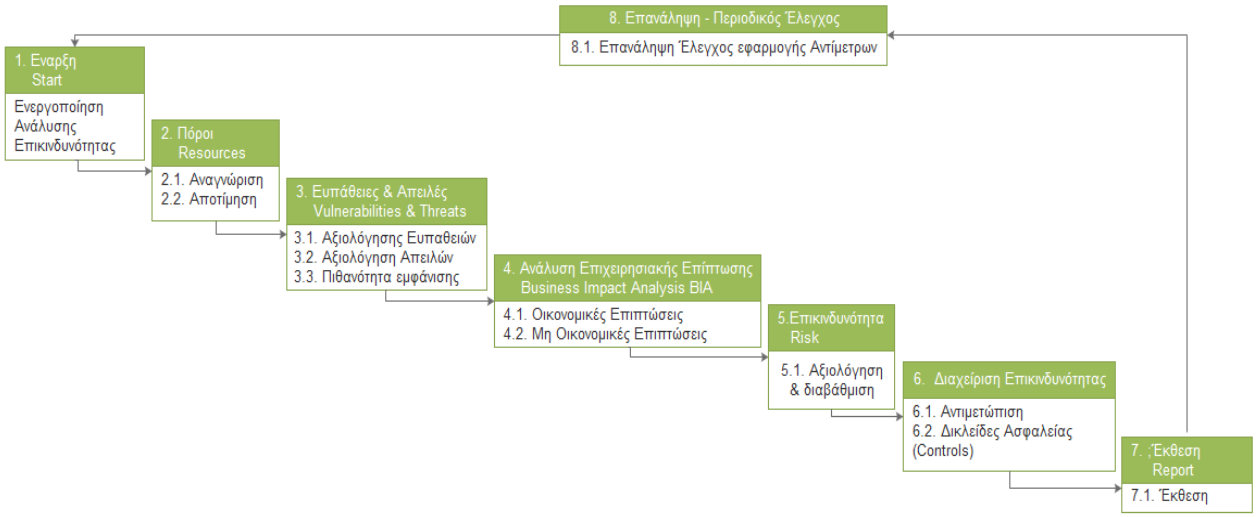
- ✓ Η αναγνώριση των κρίσιμων Πληροφοριακών Πόρων (Assets),
- ✓ Η αναγνώριση – αξιολόγηση της πιθανότητας εκμετάλλευσης των υπαρχόντων ευπαθειών (vulnerabilities) από απειλές (threats).

- ✓ Η αξιολόγηση των οικονομικών και μη, επιπτώσεων (BIA - Business Impact Analysis).
- ✓ Ο καθορισμός και η διαβάθμιση του κινδύνου των πληροφοριακών πόρων, ώστε να υλοποιηθεί και εφαρμοστή το κατάλληλο σχέδιο αντιμετώπισης κινδύνων,
- ✓ Η πρόταση δικλείδων ασφάλειας που αποτρέπουν τις απειλές,
- ✓ Η ελαχιστοποίηση του εναπομείναντα κινδύνου στο αποδεκτό επίπεδο που ζητείται από την επιχειρησιακή απαίτηση,
- ✓ Η ενδυνάμωση της περιοδικής παρακολούθησης και αναφορά των περιστατικών ασφαλείας που αφορούν εντοπισμένους κινδύνους ασφαλείας.
- ✓ Η εφαρμογή ενός οδηγού που θα εφαρμόζει τις αρχές διαχείρισης της εφαρμογής μίας μεθοδολογίας ανάλυσης επικινδυνότητας έτσι ώστε να υπάρχει αύξηση του οφέλους και μείωση των κινδύνων στο αποδεκτό όριο που επιθυμεί η Επιχείρηση / Οργανισμός.
- ✓ Η συνεργασία και η Ευθυγράμμιση της Διοίκησης και των ενδιαφερόμενων μερών με τους Επιχειρησιακούς στόχους (Business Objectives), μέσω συχνής επικοινωνίας, παρακολούθηση αποτελεσμάτων, μεθοδολογίας και εφαρμογής δικλείδων ασφαλείας για την μείωση του κινδύνου θέτοντας τον εναπομείναντα κίνδυνο σε αποδεκτά για την Επιχείρηση επίπεδα.

Καθώς για την αξιολόγηση και την αποδοχή ή απόρριψη με την παράλληλη αναγνώριση του εναπομείναντα κινδύνου πρέπει να υπάρχει ορισμένος ιδιοκτήτης Πληροφοριακού Συστήματος πριν την περιγραφή της μεθοδολογίας ορίζεται ως ιδιοκτήτης ο Υπεύθυνος του Τμήματος Διαχείρισης Χρηστών και το πρότυπο που ακολουθείται είναι το ISO/IEC 27001.

5.2.3 Φάσεις Μεθοδολογίας

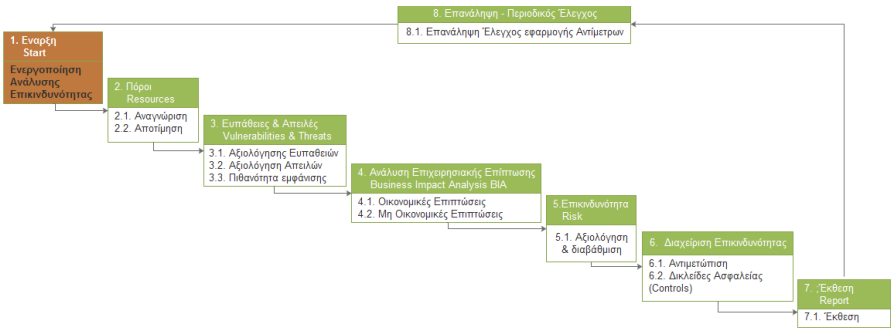
Ακολουθούν οι φάσεις της μεθοδολογίας



Εικόνα 14 Μεθοδολογία Αξιολόγησης Κινδύνων Ασφάλειας Πληροφοριών

Στις παρακάτω ενότητες θα αναπτυχθεί η ιδέα της μεθοδολογία και θα αναλυθούν οι φάσεις της.

5.2.3.1 Έναρξη Ανάλυσης Επικινδυνότητας για το Ασφαλές Πληροφοριακό Σύστημα «Διαχείρισης Πρόσβασης σε Εφαρμογές και Υπηρεσίες Πληροφοριακών Συστημάτων μίας μεγάλης Επιχείρησης (Secure Authorization Ticketing SAT»



Εικόνα 15 Έναρξη Ανάλυσης Επικινδυνότητας

Στην Φάση έναρξης δίνεται μία μικρή περιγραφή του Πληροφοριακού Συστήματος που από εδώ και στο εξής θα αναφέρεται ως ΠΣ και δημιουργείται και η γραφική

αναπαράσταση της υποδομής του και της συνεργασίας των μερών μεταξύ τους αλλά και με την υπόλοιπη κεντρική υποδομή του οργανισμού (για παράδειγμα intranet, DMZ). Επίσης καταγράφεται η έκδοση της επαναληπτικής διαδικασίας της μεθοδολογίας. Το ΠΣ αφορά ένα Ασφαλές Σύστημα Διαχείρισης Πρόσβασης σε Εφαρμογές και Υπηρεσίες Πληροφοριακών Συστημάτων μίας μεγάλης Επιχείρησης. Για συντομία από εδώ και έπειτα το Ασφαλές Πληροφοριακό σύστημα θα ονομάζεται «Secure Authorization Ticketing - SAT».

Το έγγραφο με την Αρχική Ανάλυσης επικινδυνότητας πριν τον σχεδιασμό και την υλοποίηση του συστήματος εμφανίζεται στα Παραρτήματα (ΠΑΡΑΡΤΗΜΑ Ε).

Η Τελική Ανάλυση Επικινδυνότητας πριν την παραγωγική του λειτουργία αφορά τους Πίνακες 10 του Παραρτήματος Ε με εμπλουτισμό asset σε πραγματικό επίπεδο (Σύστημα Web Logic Host, Database Host, Web Logic Security Service, Application).

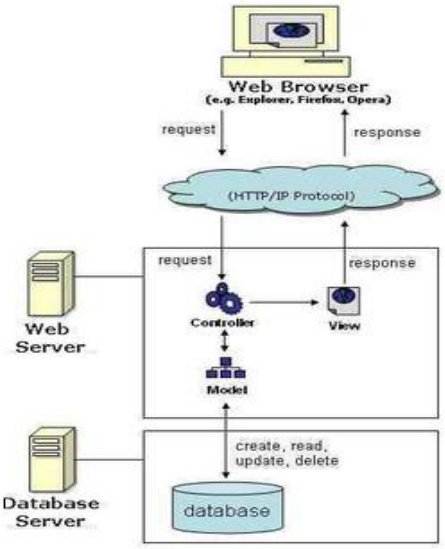
5.2.3.1.1 Περιγραφή Συστήματος

Το Πληροφοριακό Σύστημα αφορά ένα ασφαλές ticketing κεντρικό σύστημα το οποίο επικεντρώνεται καθαρά στην πρόσβαση χρηστών σε εφαρμογές και υπηρεσίες μίας μεγάλης Επιχείρησης/Οργανισμού. Πέραν της βασικής λειτουργικότητας έχει λειτουργίες MIS, Reporting, Workflow, Statistics και αυτοματοποιημένης δημιουργίας λογαριασμών σε συστήματα LDAP υλοποιώντας με αυτό τον τρόπο identity management διεργασίες. Συμπεριλαμβάνει τεχνικές κρυπτογράφησης και ψηφιακών υπογραφών.

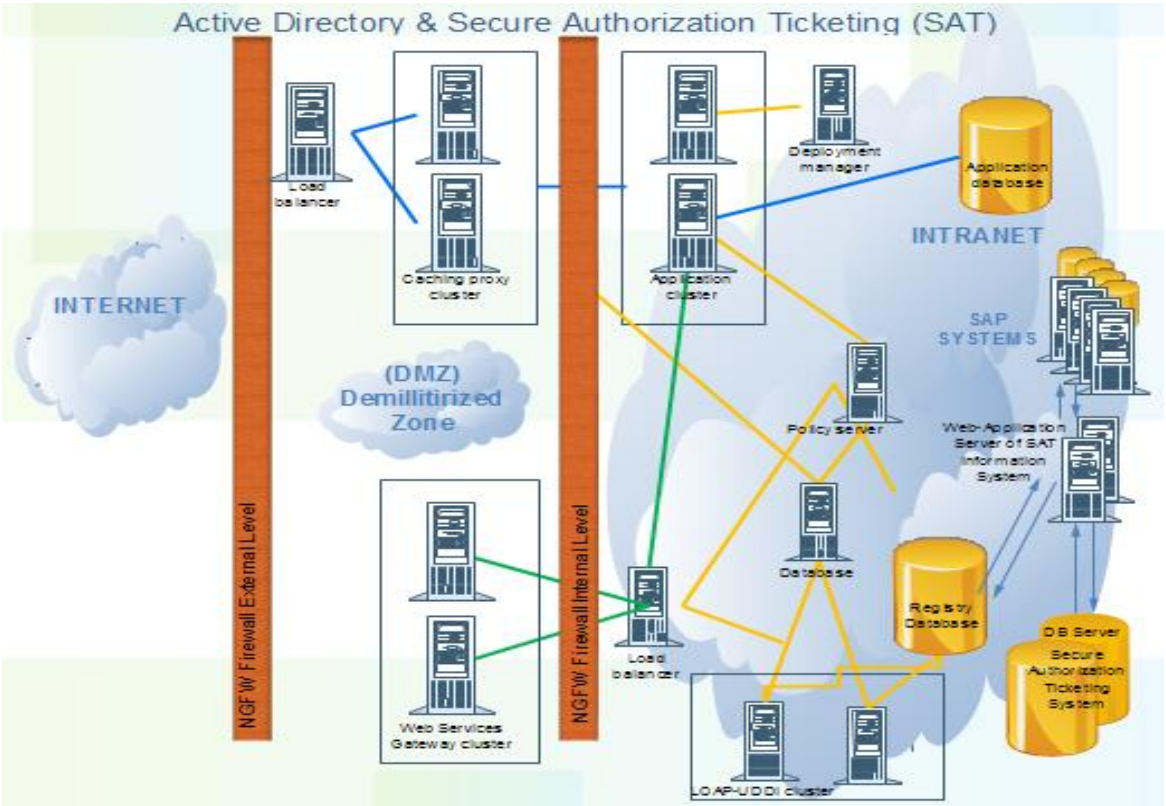
5.2.3.1.2 Αναπαράσταση Αρχιτεκτονικής

Το Πληροφοριακό Σύστημα θα υλοποιηθεί στον εσωτερικό δίκτυο της Επιχείρησης. Θα έχουν σε αυτό πρόσβαση όλοι οι χρήστες του εσωτερικού δικτύου. Επίσης το σύστημα έχει αλληλεπίδραση με την υπηρεσία LDAP MS Active Directory και με πληροφοριακά συστήματα της Επιχείρησης (πχ SAP, Web Applications κ.τ.λ).

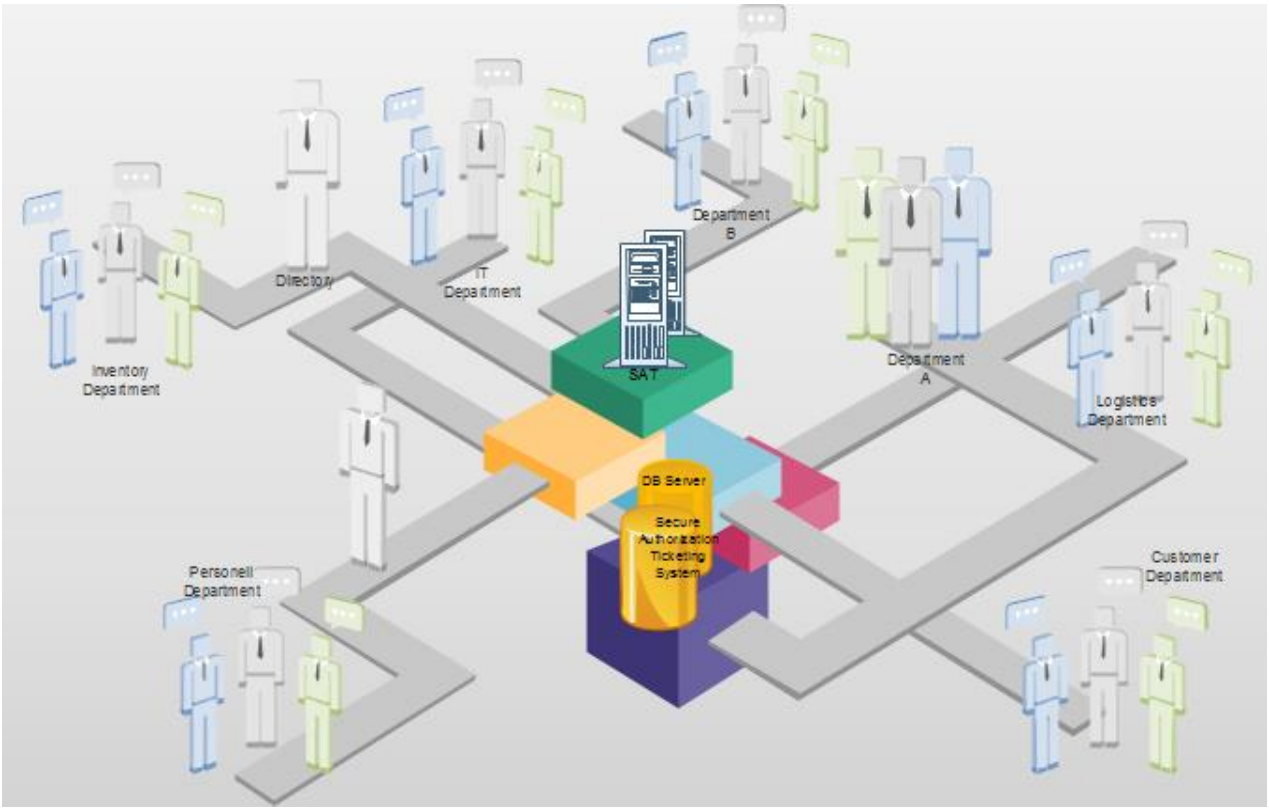
Το σύστημα θα σχεδιαστεί να λειτουργεί σε MVC (Model View Controller αρχιτεκτονική). Θα είναι εγκατεστημένο στο intranet του οργανισμού. Η πρόσβαση σε αυτό θα γίνεται μόνο από τους εσωτερικούς χρήστες ενώ για εξωτερικούς χρήστες θα γίνεται αίτημα μέσω email προς έναν λογαριασμό του συστήματος και θα παρακολουθείται από το κεντρικό τμήμα διαχείρισης προσβασιμότητας στα πληροφοριακά συστήματα και υπηρεσίες.



Εικόνα 16 Μοντέλο MVC το οποίο θα χρησιμοποιηθεί στο SAT

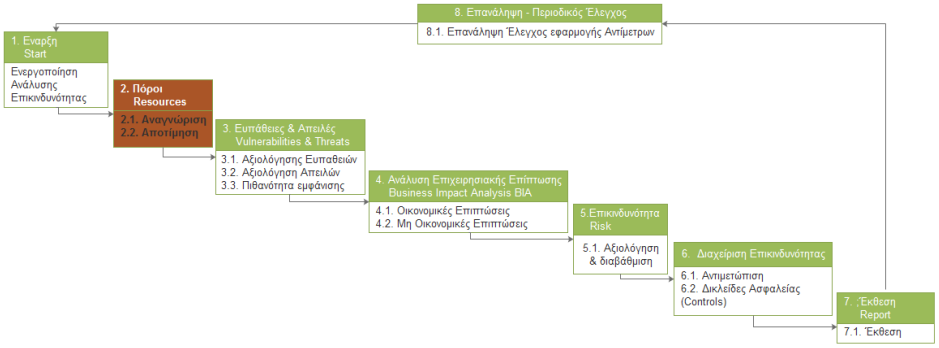


Εικόνα 17 Architecture of AD & SAT



Εικόνα 18 Up Level Workflow of SAT

5.3 Μελέτη Ανάλυση Επικινδυνότητας – Βήματα



Εικόνα 19 Πόροι Ανάλυσης Επικινδυνότητας

5.3.1.1.1 Αναγνώριση Πόρων (Involved Assets)

Σε αυτό το βήμα αναγνωρίζονται οι Πόροι (Πληροφοριακοί, Ανθρώπινοι κτλ) καθώς και οι διεργασίες που αφορούν το εν λόγω πληροφοριακό σύστημα. Εφόσον υπάρχουν διασυνδέσεις μέσω διεπαφών (interfaces) με άλλα πληροφοριακά συστήματα θα πρέπει να υπάρξει

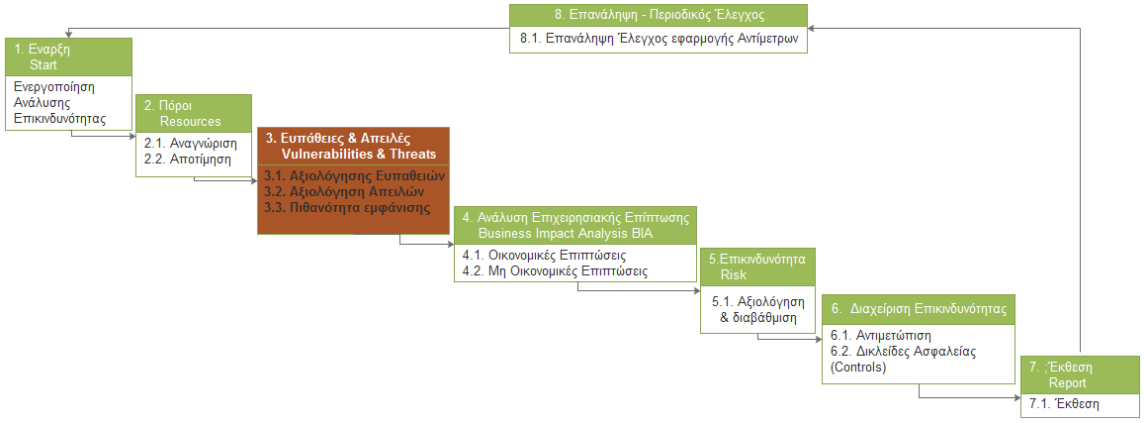
αναγνώριση και των Πληροφοριακών Πόρων τους. Το βήμα αυτό αφορά την βάση της διαχείρισης επικινδυνότητας καθώς η ορθή αναγνώριση πόρων θα οδηγήσει και στην επιτυχής έκβαση της αξιολόγησης επικινδυνότητας με γνώμονα την τελική διασφάλιση του Πληροφοριακού Συστήματος.

Η αξιολόγηση της κρισιμότητας και της αξίας κάθε πόρου για την Επιχείρηση και η ιεράρχηση διεργασιών οργανώνεται μέσω μιας αρχικής εκτίμησης των πόρων. Σημαντικά σημεία είναι η αναγνώριση των πόρων τόσο από την πλευρά του πληροφοριακού συστήματος (SAT) αλλά και από την πλευρά της επιχειρηματικής διεργασίας. Ακολουθούν οι ερμηνείες των επιχειρησιακών και τεχνικών πληροφοριών.

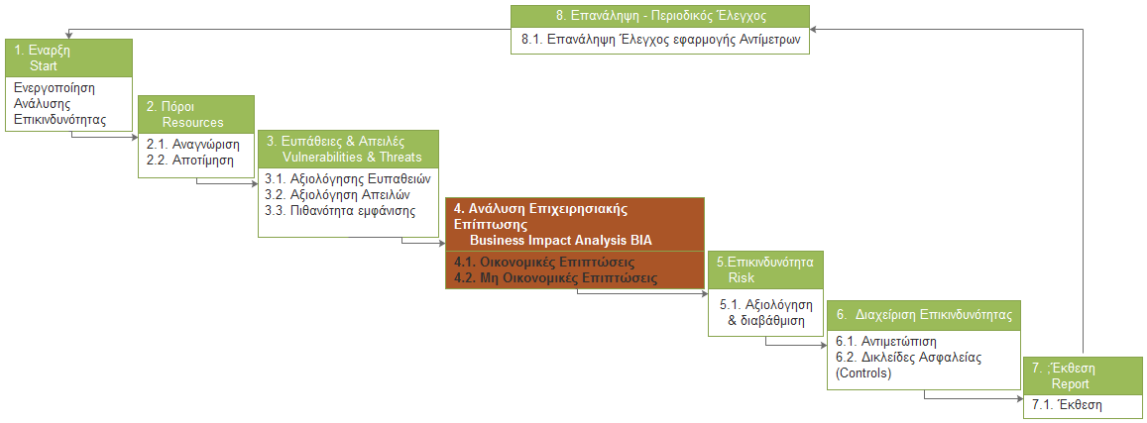
Ερμηνεία Ορολογιών Αξιολόγησης Πληροφοριακού Συστήματος	Ανάλυση Αναφοράς	Είδος Πληροφόρησης
Πληροφοριακός Πόρος & Περιγραφή του	(Επιχειρησιακή Λειτουργία, διεργασία ή ενέργεια που υποστηρίζεται, όνομα εφαρμογής, χαρακτηριστικά πληροφορίας)	Επιχειρησιακή
Εύρος Εφαρμογής	(Επιχείρηση, Τμήμα)	Επιχειρησιακή
Τύπος Πληροφοριακού Μέσου	(Πληροφοριακό Σύστημα, Πληροφορίες σε έντυπη μορφή)	Επιχειρησιακή
Ιδιοκτήτης Πόρου	(Ιδιοκτήτης Πληροφοριακού Αγαθού, Τμήμα)	Επιχειρησιακή
Πληροφορίες που Αποθηκεύονται/Επεξεργάζονται	(Κρίσιμες Επιχειρησιακές πληροφορίες, Προσωπικά Ευαίσθητα και μη δεδομένα, Εταιρικά Δεδομένα Ευαίσθητα και μη, πνευματική ιδιοκτησία, άλλες ευαίσθητες πληροφορίες, δεδομένα πιστωτικών καρτών)	Επιχειρησιακή
Διαβάθμιση Πληροφοριών/Πληροφοριακού Συστήματος (Information System Gradation)	(Κρίσιμες, Ευαίσθητες, Μη-Κρίσιμες)	Επιχειρησιακή
Είδος Χρηστών	(Χρήστες Επιχείρησης, Εξωτερικοί Συνεργάτες, Τρίτα Μέρη, Πελάτες, Κοινό)	Επιχειρησιακή
Αριθμός επιχειρησιακών	(Υψηλός, Μεσαίος, Χαμηλός)	Επιχειρησιακή

Συναλλαγών		
Ροή Πληροφοριών (Data Workflow)	(Εισαγωγή, επεξεργασία, αποθήκευση, μετάδοση)	Τεχνική
Διασυνδέσεις/ Εξαρτήσεις από άλλα Συστήματα (Interfaces)	(Υποστηρικτικά συστήματα (e.g. digital signatures, backup) , βάσεις δεδομένων , Διασυνδέσεις και διεπαφές που αλληλοεπιδρούν και συνεργάζονται με τις διαδικασίες/πόρους του ΠΣ)	Τεχνική
Τοποθεσία Κεντρικού ή Αποκεντρωμένου Πληροφοριακού Συστήματος και Διασυνδεδεμένων Πληροφοριακών Συστημάτων.	(Υπολογιστικό Κέντρο «Site-Computer Room» Τμήμα, Φιλοξενία σε εξωτερικό ενοικιαζόμενο χώρο, Νέφος (Cloud))	Τεχνική
Είδος προμήθειας Πληροφοριακού Συστήματος	(Ανεπτυγμένο εντός Επιχείρησης «custom internal», Ανάθεση ανάπτυξης σε προμηθευτές «custom external», Εμπορικό Λογισμικό Πακέτο, Τροποποιημένο Λογισμικό Πακέτο, Λογισμικό ανοικτού κώδικα, Υπηρεσία εσωτερικά του Οργανισμού, Υπηρεσία στον Νέφος)	Τεχνική
Διαχείριση και τεχνική Υποστήριξη	(Εσωτερικά από λειτουργούς της επιχείρησης, εντός της επιχείρησης από εξωτερικούς συνεργάτες, απομακρυσμένη υποστήριξη από εξωτερικούς συνεργάτες)	Τεχνική
Πλατφόρμα	(Υλικό, middleware, λειτουργικό σύστημα, βάση δεδομένων)	Τεχνική
Είδος πρόσβασης	(Εσωτερικό δίκτυο, Παγκόσμιο Ιστό - Internet, απομακρυσμένη πρόσβαση)	Τεχνική
Ασφάλεια/Ρόλος και εμπλοκή Ασφάλειας, Κατηγορία Δικτύων, Διαβάθμιση Χρηστών	(Υποδομή ασφαλείας/διαχείρισης, εσωτερικά/δημόσια δίκτυα, επίπεδα εμπιστοσύνης χρηστών)	Τεχνική

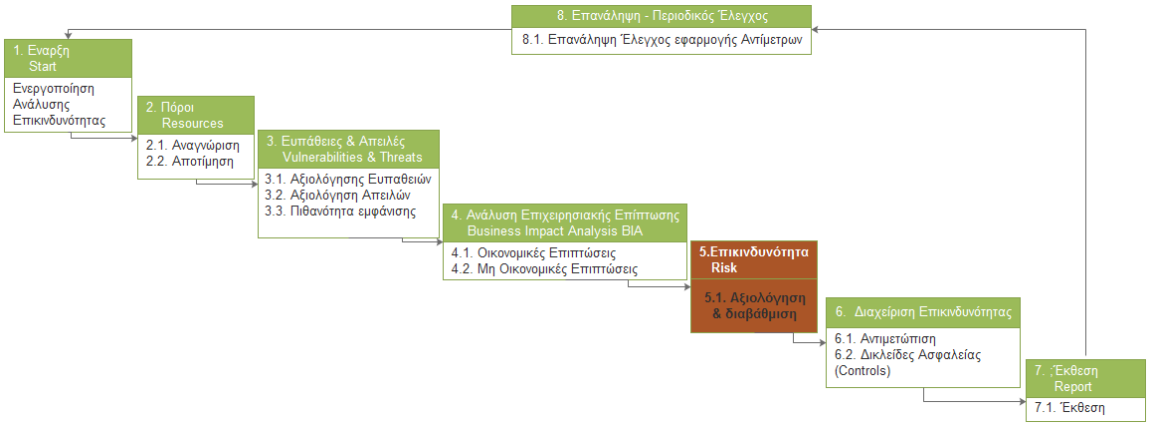
Πίνακας 1 Συλλογή Πληροφοριών για την Ανάλυση Επικινδυνότητας



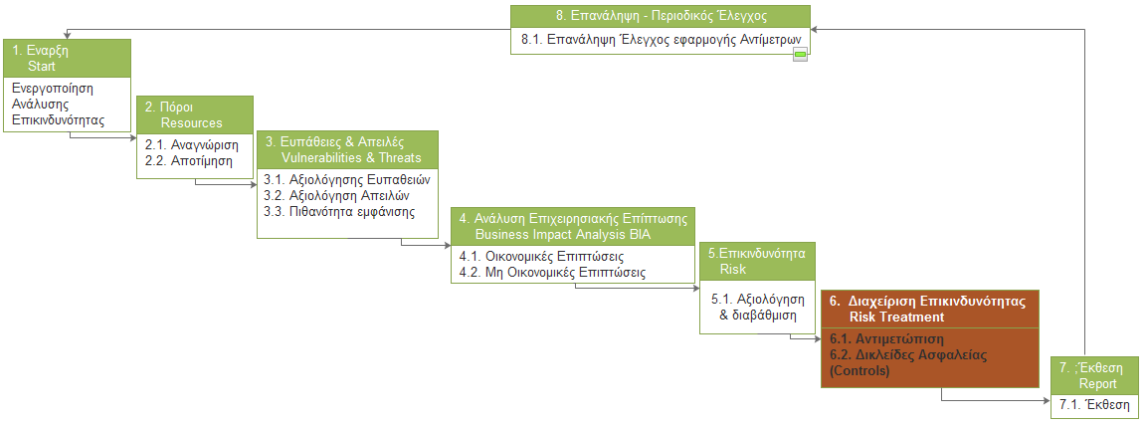
Εικόνα 20 Ανάλυση Επικινδυνότητας – Βήμα: Ευπάθειες και απειλές



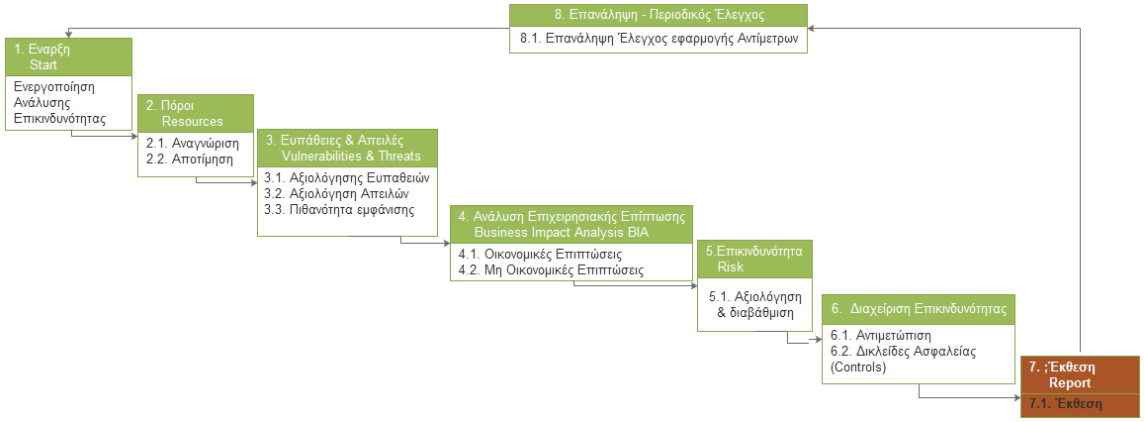
Εικόνα 21 Ανάλυση Επικινδυνότητας – Βήμα: Ανάλυση Επιχειρησιακής Επίπτωσης



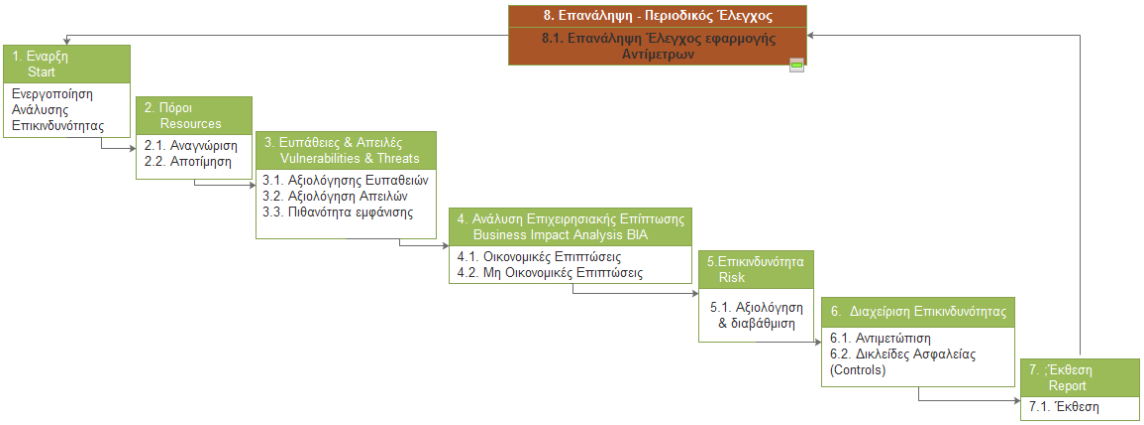
Εικόνα 22 Ανάλυση Επικινδυνότητας – Βήμα: Επικινδυνότητα



Εικόνα 23 Ανάλυση Επικινδυνότητας – Βήμα: Διαχείριση Επικινδυνότητας



Εικόνα 24 Ανάλυση Επικινδυνότητας – Βήμα: Δημιουργία Έκθεσης



Εικόνα 25 Ανάλυση Επικινδυνότητας – Βήμα: Επανάληψη και Έλεγχος

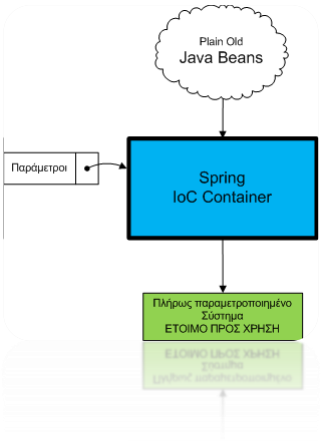
6. Υλοποίηση

6.1 Περιβάλλοντα υλοποίησης – μέθοδοι - μεθοδολογίες

1.1.1. Περιβάλλον ανάπτυξης και αιτιολόγηση επιλογής.

Ο κώδικας αναπτύχθηκε στο περιβάλλον (emulator) Spring. Η επιλογή έγινε γιατί πέραν του τυπικού MVC design pattern που διαθέτει παρέχει και τεχνικές (δικλείδες ασφαλείας) για την ενδυνάμωση των τρωτών σημείων που εκμεταλλεύονται συνήθως κακόβουλοι σε εφαρμογές ιστού (web)1. Μπορεί να χρησιμοποιηθεί για την ανάπτυξη ενός συστήματος που διαθέτει: controller, ομάδα components business layer, σημείων επικοινωνίας με τη βάση και framework που αναλαμβάνει όλες αυτές τις εργασίες.

Η επιλογή των Enterprise Java Beans αποτελούσε μονόδρομο τα τελευταία χρόνια. Αυτά απαιτούσαν πολλά resources. Πριν μία δεκαετία υλοποιήθηκαν ενέργειες για την δημιουργία ενός lightweight framework και δημιουργήθηκε το Spring Framework.



Αφορά ελαφρύ Java/J2EE πλαίσιο εφαρμογών που βασίζεται σε κώδικα που δημοσιεύθηκε στο βιβλίο «Expert One-on-One J2EE Design and Development» από τον βασικό συντελεστή του framework, Rod Johnson. Αποτελεί μία δυνατή λύση για τη διαχείριση ρυθμίσεων της εφαρμογής, που βασίζεται σε JavaBeans εφαρμόζοντας την αρχιτεκτονική αρχή του Inversion of Control. Έχει ένα γενικό abstraction layer για τη διαχείριση transactions που επιτρέπει pluggable transactions managers. Έχει ένα JDBC abstraction layer και ενσωματώνει ένα πλήθος διαδεδομένων τεχνολογιών όπως το Hibernate, JDO, Apache OJB, λειτουργικότητα Aspect Oriented Programming (AOP) προγραμματιστικό υπόδειγμα στο οποίο οι δευτερεύουσες λειτουργίες διαχωρίζονται από το business logic της εφαρμογής. Έχει εύκολο δικό του, Model View Controller Web framework με πολλαπλές τεχνολογίες στο View κομμάτι. Επιπλέον έχει διαδικασίες για authentication / authorisation που υποστηρίζουν διάφορα προτόκολα (πχ LDAP). Έχει Remote Access framework με λειτουργίες RemTo Spring Framework που αποτελείται από έναν Container βασισμένο στο Inversion of Control (IoC) ή Dependency Injection. Πρόκειται για μία τεχνική όπου σε ένα κομμάτι εφαρμογής υποδεικνύεται ποια άλλα κομμάτια μπορεί να χρησιμοποιεί. Για όλες τις

[1] Κεφάλαιο 4 στο οποίο αναπτύσσεται η Ασφάλεια του Πληροφοριακού Συστήματος

εφαρμογές που χτίζονται πάνω στο Spring, ο Container αποτελεί την καρδιά του συστήματος και όλα τα Java Beans που περιέχει γίνονται instantiated, παραμετροποιούνται και συναρμολογούνται από τον Container. Αντιπροσωπεύει τον Spring IoC container και υπάρχουν πάρα πολλές υλοποιήσεις ανάλογα με τον τύπο εφαρμογής (stand-alone, web κτλ.)

1.1.2. Εγκατάσταση και prerequisites.

Απαραίτητο για να λειτουργήσει το περιβάλλον είναι το τελευταίο JDK της Oracle, από την Spring το Spring Framework και το Maven. Μετά την εγκατάσταση του JDK ορίζουμε στο πspring STS το workgroup που θα λειτουργήσουμε την εφαρμογή SAT.

Στην συνέχεια έγινε η ανάπτυξη της εφαρμογής σε περιβάλλον ανάπτυξης Java Spring Angular. Για την υποστήριξη του data at rest δημιουργήθηκε στο RDBMS ένα instance και ένα σχήμα χρήστη oracle (oracle v12c). Οι server φιλοξενούνται σε εικονικές μηχανές με Hypervisor τεχνολογία ESXI VMWARE. Ο db server έχει λειτουργικό σύστημα Linux και ο web app Windows 2012 τελευταίο patch & Tomcat.

Αναλυτικά έγιναν:

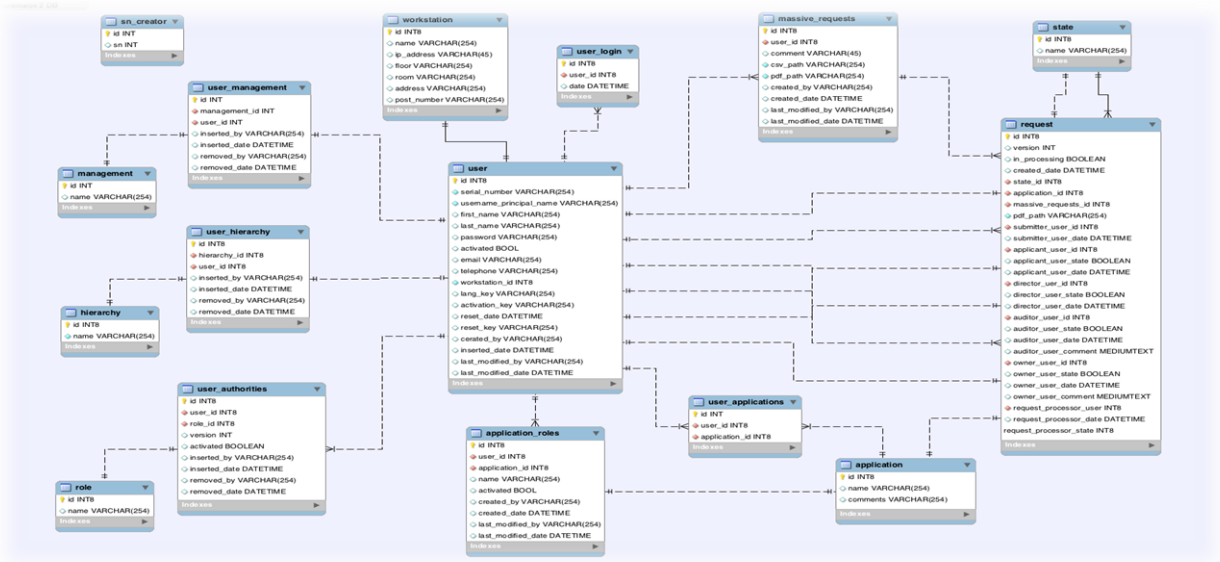
- Εγκατάσταση του Hypervisor (ESXI) VMWARE.
- Δημιουργία εικονικών μηχανών με ΛΣ LINUX & Windows 2012.
- Εγκατάσταση του rdbms Oracle 12c και δημιουργία του wallet TDE
- Δημιουργία του σχήματος της βάσης και διασύνδεση της μέσω των τεχνολογιών JPA - Hibernate – Liquid Base (με κρυπτογραφημένο TBS).
- Εγκατάσταση του Spring and Angular JS
- Υλοποίηση κώδικα.

6.2 Υλοποίηση της ΒΔ

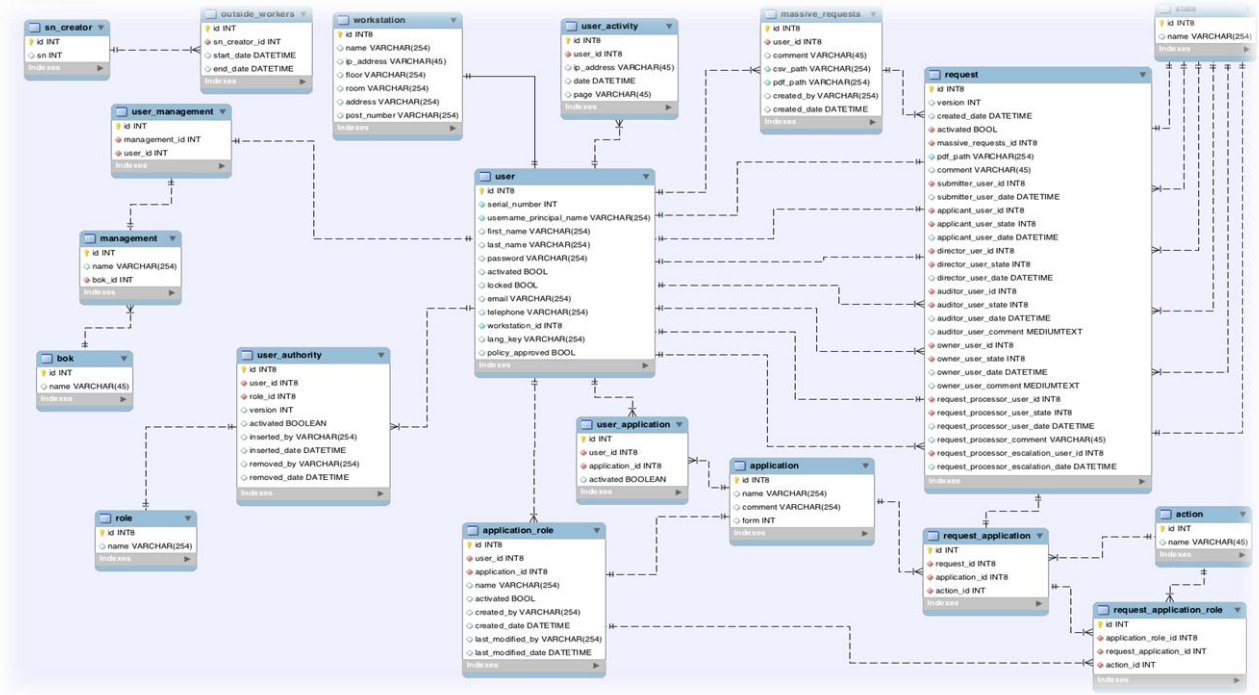
Το σχήμα της βάσης δημιουργήθηκε στην Oracle μετά το τέλος της φάσης σχεδίασης. Οι πίνακες δημιουργούνται αυτόματα με την ενεργοποίηση του ticketing συστήματος και σε αυτούς φορτώνονται αυτόματα δεδομένα initialization. Στην λειτουργικότητα της εφαρμογής η Βάση Δεδομένων που έχει αναπτυχθεί στο πλαίσιο κάλυψης του functionality της εφαρμογής (σχήμα) μπορεί να υλοποιηθεί επιπλέον της Oracle στους ακόλουθους τύπους:

- MySQL
- H2 (βάση στην μνήμη για λόγους δοκιμών και ανάπτυξης)
- Postgresql

Περιέχει properties, sequences, tables, indexes, constraints, foreign keys και loaddata. Ανάλυσή τους και ένα παράδειγμα του xml που δημιουργεί το σχήμα εμφανίζεται στο ΠΑΡΑΡΤΗΜΑ Β.



Εικόνα 26 Αρχικό Σχήμα ΒΔ



Εικόνα 27 Τελικό Σχήμα ΒΔ

6.3 Σύνδεση εφαρμογής με ΒΔ

Για την σύνδεση γίνεται χρήση του jdbc thin driver της oracle. Σε ένα αρχείο yaml διατηρούνται οι κωδικοί πρόσβασης και το σχήμα ως data at rest (application server). Διαφυλάσσονται με την πλήρη κρυπτογράφηση που έχει γίνει στο full pgp disk encryption στον application server. Η σύνδεση db & we app γίνεται μέσω secure tcp connection με χρήση ssl. Με key generator έχουμε δημιουργήσει ένα ζευγάρι κλειδιών (ιδιωτικό, δημόσιο) με κωδικοποίηση RSA 2048. Το ζευγάρι αυτό το εμφωλιάζουμε μέσα στο wallet του db server (oracle). Στο trust store του webapp διατηρείται το public κλειδί (αυτό που περιγράφτηκε παραπάνω). Ο webapp δημιουργεί ένα session key (ψευδοτυχαίο), το κρυπτογραφεί με το παραπάνω public κλειδί και το στέλνει στον db server. Ο db server το αποκρυπτογραφεί και έτσι δημιουργείται το session handshake για την ασφαλή επικοινωνία των δεδομένων του session (με συμμετρική κρυπτογράφηση όπου το passphrase είναι το session id).

6.4 Σημαντικά σημεία που υλοποιήθηκαν – Ομαδοποίηση λειτουργιών (υποσυστήματα) στα οποία χωρίστηκαν οι περιπτώσεις χρήσης για την διευκόλυνση της υλοποίησης.

Για την υλοποίηση της εφαρμογής ομαδοποιήθηκαν οι περιπτώσεις χρήσης σε **ομάδες λειτουργιών (υποσυστήματα)**.

Το κεντρικό σημείο της εφαρμογής είναι η Δημιουργία Αιτημάτων (**Authorization Request**). Όμως για να μπορέσει να λειτουργήσει ευέλικτα και με ασφάλεια εφαρμόστηκε σύστημα ασφάλειας πρόσβασης χρηστών (**Security management**) το οποίο διασυνδέεται με το LDAP της Επιχείρησης. Παράλληλα για να υπάρξει ουσιαστική παρακολούθηση του ticket στο σύστημα λειτουργεί μέθοδος ροών (**Workflows**). Για να υπάρχει πληρέστερη καταγραφή γίνεται **Logging, Auditing**. Υπάρχει χρήση Ψηφιακών Υπογραφών (**Digital Signatures)**. Για όλες τις περιπτώσεις χρήσεις έχει υλοποιηθεί σύστημα **reporting – list**. Στατιστικά (**MIS**). Περιβάλλον διαχείρισης συστήματος (**Application Administration**).

6.5 Παραδείγματα επεξήγησης της διαδικασίας δημιουργίας μίας περίπτωσης χρήσης για την υλοποίηση Δημιουργίας αιτήματος το οποίο αναπτύχθηκε σε προηγούμενο κεφάλαιο (use cases).

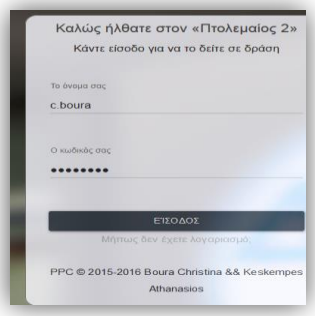
1. Σύνδεση στο σύστημα (απλός χρήστης – διαχειριστής)
2. Δημιουργία αιτήματος πρόσβασης
3. Ροή Αιτήματος και έγκριση αιτήματος από τον Προϊστάμενο
4. Ορισμός ιδιοκτήτη εφαρμογής και ανταποκριτή ασφάλειας για την εφαρμογή
5. Έγκριση από ανταποκριτή ασφάλειας ή έγκριση από τον Ιδιοκτήτη της Εφαρμογής
6. MIS
7. Υλοποίηση αιτήματος από τον διαχειριστή χρηστών και διασύνδεση με την εφαρμογή
8. Διαχείριση ρόλων SAT και απόδοση σε χρήστη
9. Απόδοση ρόλου (user – owner)
10. Αλλαγή στοιχείων στο profile (στοιχεία BOK)
11. Δημιουργία εφαρμογών

6.5.1 Σύνδεση στο σύστημα (user – administrator)

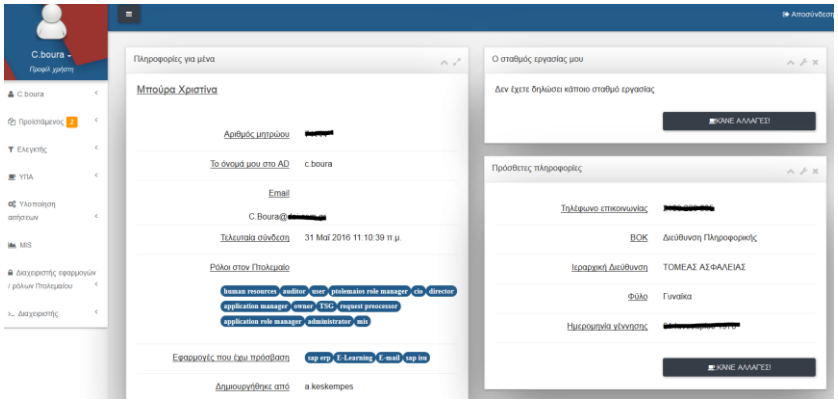
Περίληψη Λειτουργίας

Ένας υπάλληλος της Επιχείρησης καλεί το σύστημα ticketing authorization. Ο τεχνικός καλεί το url της εφαρμογής και του εμφανίζεται η αρχική οθόνη. Ο χρήστης δίνει το username και το συνθηματικό πρόσβασης. Το σύστημα ελέγχει αν είναι τα στοιχεία του LDAP ορθά. Ανάλογα με τον ρόλο του το σύστημα του εμφανίζει το αντίστοιχο μενού.

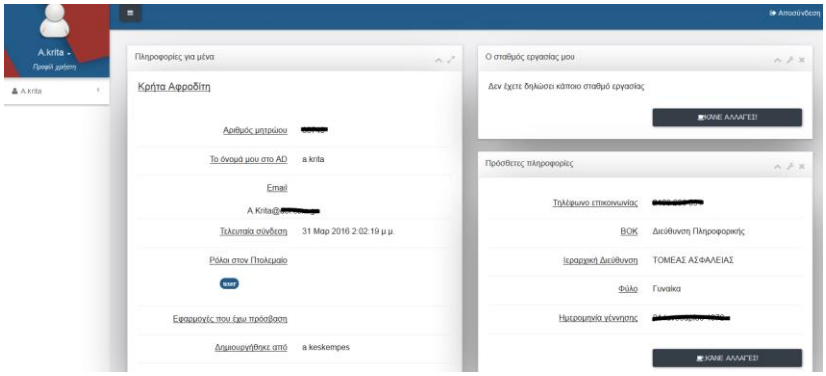
Εικόνες Λειτουργίας



Εικόνα 28 Είσοδος χρήστη στο σύστημα διαχείρισης αιτημάτων πρόσβασης



Εικόνα 29 Περιβάλλον Διαχειριστή μετά την είσοδο



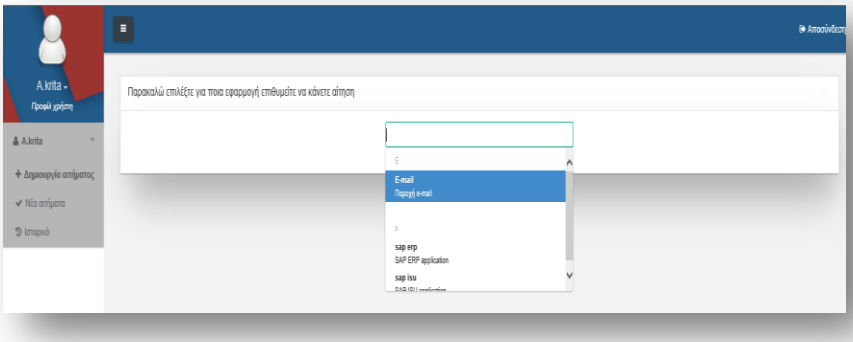
Εικόνα 30 Περιβάλλον Απλού Χρήστη

6.5.2 Δημιουργία αιτήματος πρόσβασης

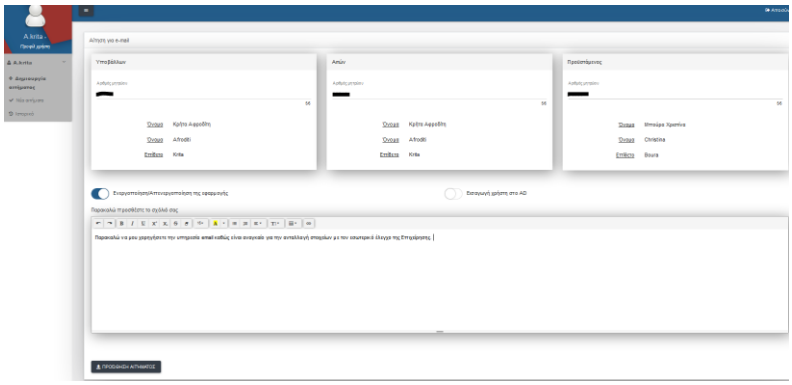
Περίληψη Λειτουργίας

Ένας υπάλληλος της Επιχείρησης είναι ήδη συνδεδεμένος στο σύστημα ticketing authorization. Επιλέγει από το μενού του την δημιουργία αιτήματος. Το σύστημα του εμφανίζει μία λίστα στην οποία πρέπει να επιλέξει την εφαρμογή για την οποία αιτείται πρόσβαση. Επιλέγει την εφαρμογή και πατάει <ENTER>. Το σύστημα του εμφανίζει μία οθόνη που περιέχει τα στοιχεία του υποβάλλοντα, του αιτούντα και αναμένει να του δοθεί από τον χρήστη ο ειδικός αριθμός μητρώου του Προισταμένου. Επιλέγει τους ρόλους. Στην περίπτωση που θέλει να γράψει σχόλιο το σύστημα εμφανίζει κατάλληλο πεδίο. Με το κουμπί προώθηση αιτήματος ενεργοποιείται το ticket.

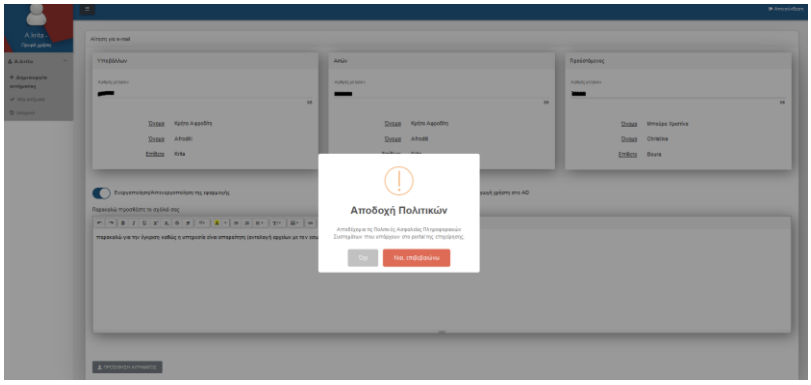
Εικόνες Λειτουργίας



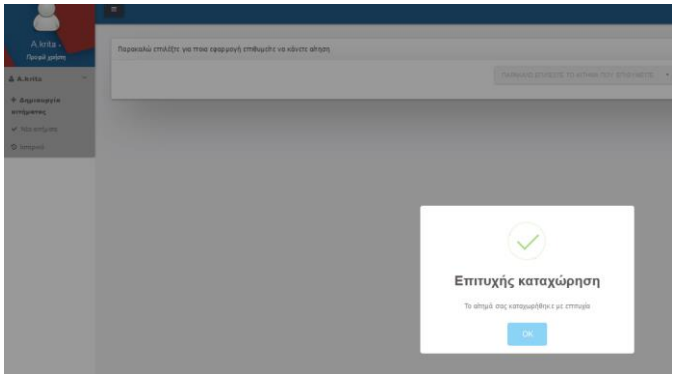
Εικόνα 31 Δημιουργία αιτήματος και επιλογή από το Μητρώο Εφαρμογών ή Υπηρεσιών



Εικόνα 32 Δημιουργία αιτήματος Αρχική Λειτουργία



Εικόνα 33 Αποδοχή



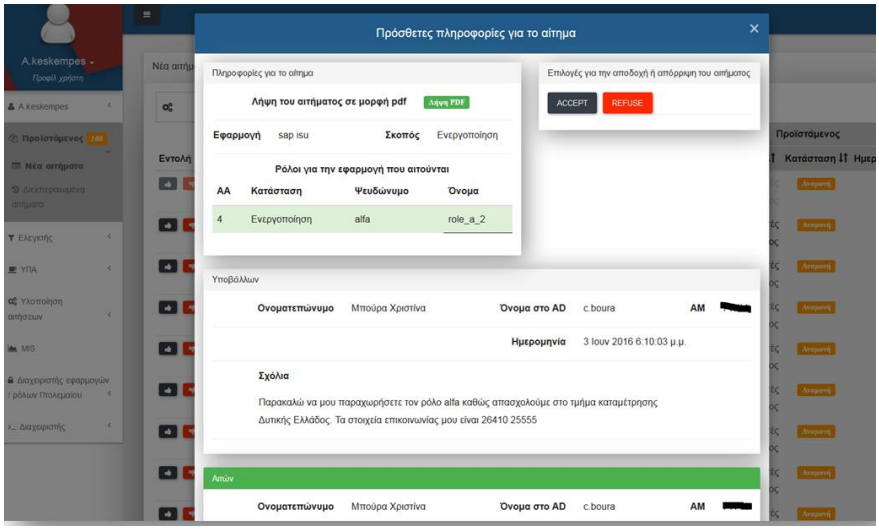
Εικόνα 34 Επιτυχής καταχώρηση αιτήματος χρήστη

6.5.3 Έγκριση αιτήματος από τον προϊστάμενο

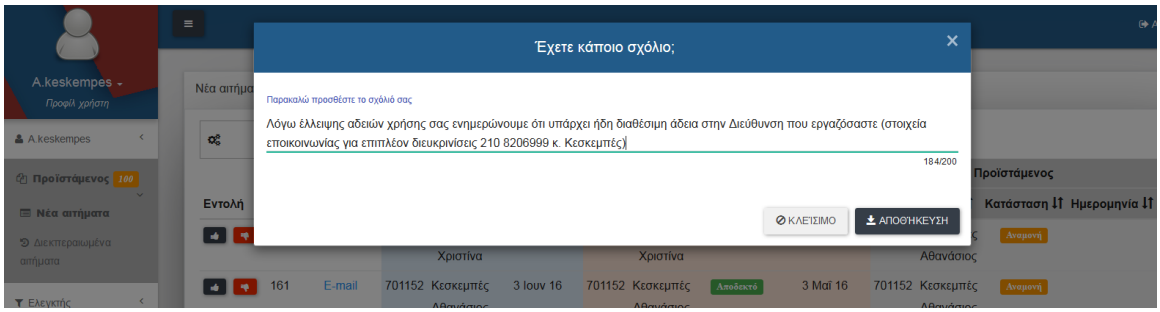
Περίληψη Λειτουργίας

Τα αιτήματα που στέλνει ο χρήστης σε έναν προϊστάμενο, μπορεί να τα εγκρίνει (ACCEPT) ή να τα απορρίψει (REFUSE) ο προϊστάμενος με την κατάλληλη αιτιολόγηση η οποία καταγράφεται.

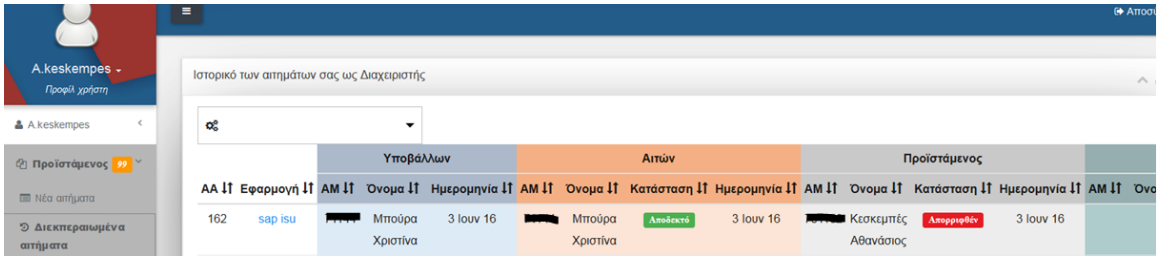
Εικόνες Λειτουργίας



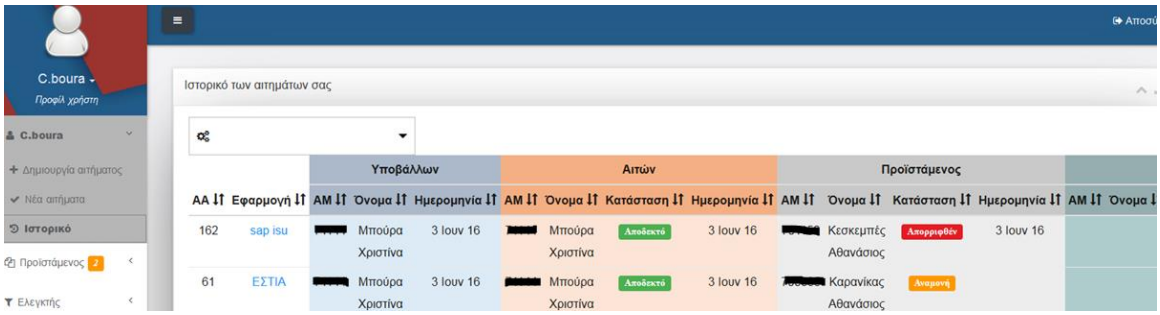
Εικόνα 35 Προϊστάμενος (έγκριση ή απόρριψη αιτήματος από συνεργάτη του)



Εικόνα 36 Αιτιολόγηση απόρριψης ή έγκρισης από τον προϊστάμενο



Εικόνα 37 Αποτέλεσμα που βλέπει ο προϊστάμενος στην ροή των αιτήματός που του έχουν έρθει (ticket)



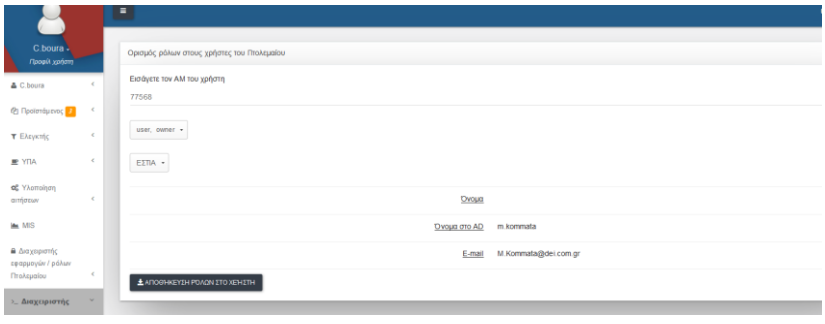
Εικόνα 38 Αποτέλεσμα που βλέπει ο χρήστης στην ροή των αιτημάτων που έχει στείλει (ticket)

6.5.4 Ορισμός ιδιοκτήτη εφαρμογής και ανταποκριτή ασφάλειας της εφαρμογής

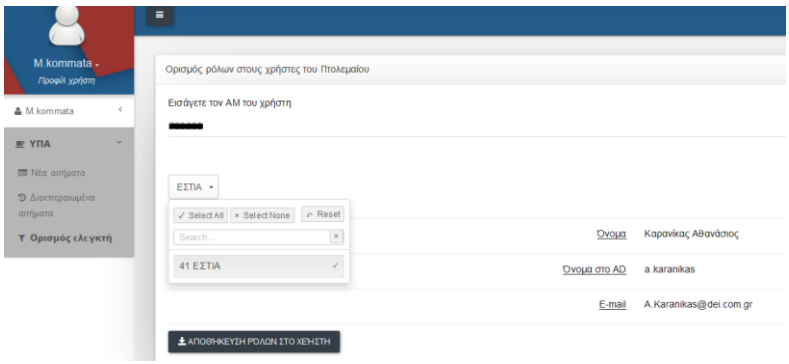
Περίληψη Λειτουργίας

Ο Διαχειριστής του πληροφοριακού συστήματος μπορεί να ορίσει Ιδιοκτήτη Υπεύθυνο Πληροφοριακού Αγαθού. Τα αιτήματα που αφορούν έναν ιδιοκτήτη (ΥΠΑ) εφαρμογής μπορούν να τα βλέπουν ο ίδιος αλλά και οι βοηθοί του. Ο ρόλος του καθένα από τους παραπάνω τους δίνει την δυνατότητα να δουν ποια αιτήματα χρειάζονται αξιολόγηση και έγκριση και αποδοχή ή απόρριψη. Με αυτό τον τρόπο η ροή είτε προχωράει και έχει πράσινη χρωματική απόχρωση στους παραπάνω ρόλους ή απορρίπτεται και σταματάει με κόκκινη χρωματική απόχρωση. Σε κάθε περίπτωση πρέπει να υπάρχει καταγραφή και αιτιολόγηση από τους παραπάνω ρόλους για την ενέργειά τους.

Εικόνες Λειτουργίας



Εικόνα 39 ορισμός ιδιοκτήτη εφαρμογής



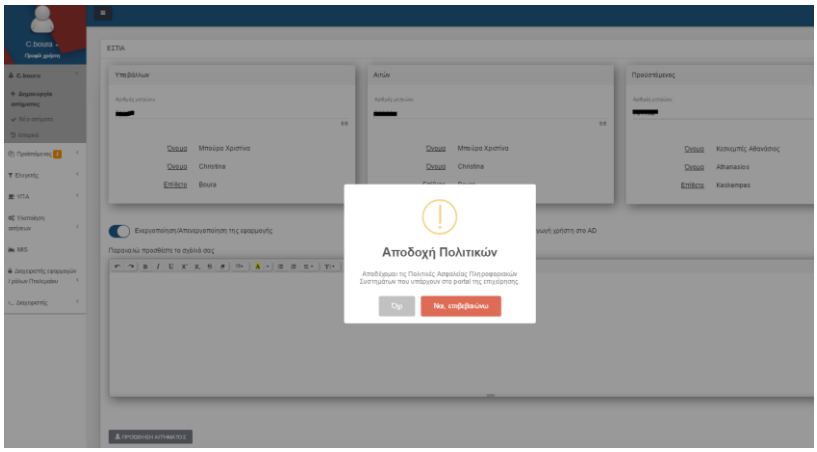
Εικόνα 40 ορισμός ανταποκριτή ασφάλειας από τον ιδιοκτήτη εφαρμογής

6.5.5 Ροή αιτήματος και έγκριση από ανταποκριτή ασφάλειας ή έγκριση από τον ιδιοκτήτη της Εφαρμογής

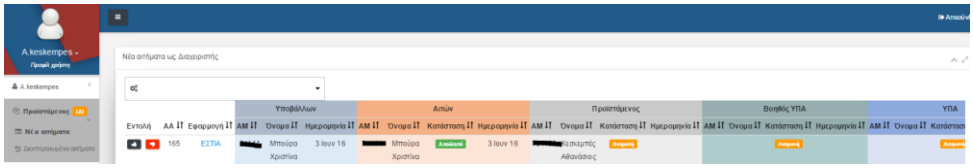
Περίληψη Λειτουργίας

Τα αιτήματα που αφορούν έναν ιδιοκτήτη εφαρμογής μπορούν να τα βλέπουν ο ίδιος αλλά και οι βοηθοί του που έχουν οριστεί ως «ανταποκριτές ασφάλειας» από το μενού του ιδιοκτήτη. Οι βοηθοί μπορούν να υλοποιούν μία ανάλυση πριν από τον ιδιοκτήτη και να του αναφέρουν με την κατάλληλη αιτιολόγηση έτοιμη την έγκριση ή απόρριψη του αιτήματος. Το κάθε αίτημα που είναι σε αναμονή προς έλεγχο έχει χρώμα πορτοκαλί. Στην περίπτωση που απορριφθεί λαμβάνει χρωματισμό κόκκινο από τον ρόλο που το έχει απορρίψει. Στην περίπτωση που έχει εγκριθεί λαμβάνει χρώμα πράσινο και δρομολογείται στο επόμενο flow του ticket για τις σχετικές ενέργειες.

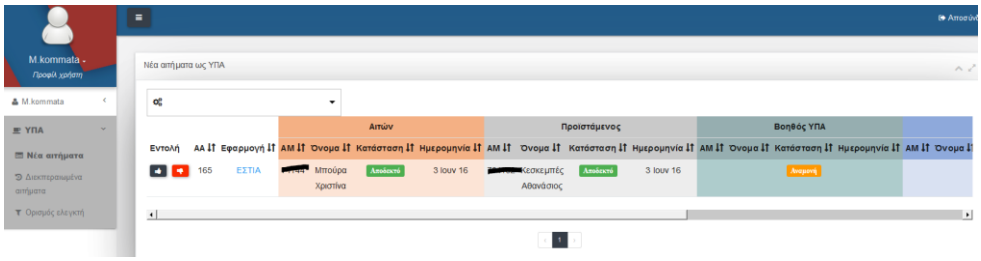
Εικόνες Λειτουργίας



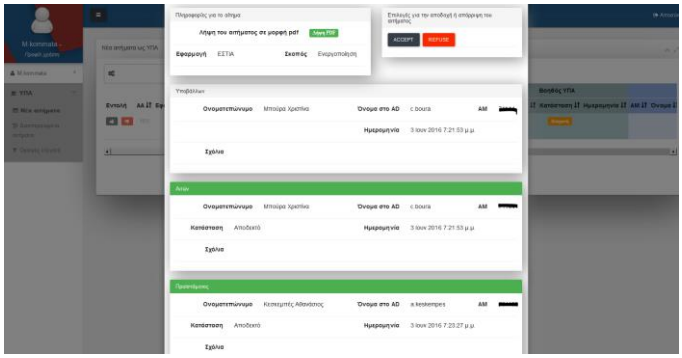
Εικόνα 41 αίτημα για πρόσβαση σε εφαρμογή



Εικόνα 42 κατάσταση αιτήματος πρόσβασης (ticket αναμονή στον προϊστάμενο)



Εικόνα 43 κατάσταση αιτήματος αναμονή στον ανταποκριτή ασφάλειας εφαρμογής



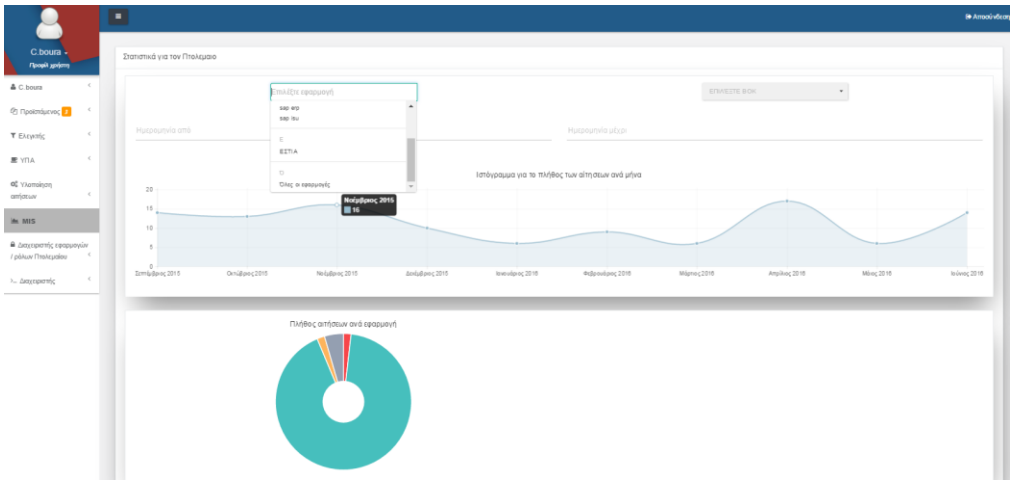
Εικόνα 44 κατάσταση αιτήματος διερεύνηση από τον ιδιοκτήτη εφαρμογής (έγκριση ή απόρριψη με αιτιολόγηση)

6.5.6 MIS

Περίληψη Λειτουργίας

Μέσω του ρόλου MIS μπορεί ο χρήστης που διαθέτει τον ρόλο (πχ CIO) να δει την κίνηση των αιτημάτων του και να επιλέξει φίλτρα αναζήτησης (χρόνο, μητρώο εφαρμογών).

Εικόνες Λειτουργίας



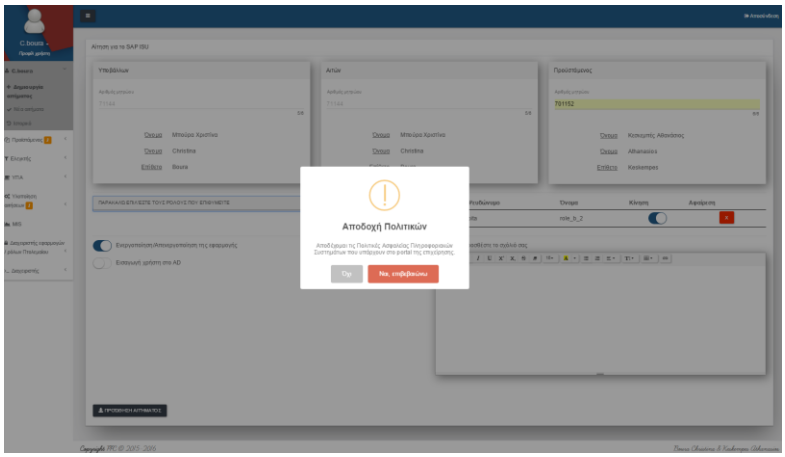
Εικόνα 45 Γραφική πληροφόρηση κίνησης αιτημάτων πρόσβασης

6.5.7 Υλοποίηση αιτήματος από τον διαχειριστή χρηστών και διασύνδεση με την εφαρμογή υλοποίησης αιτήματος

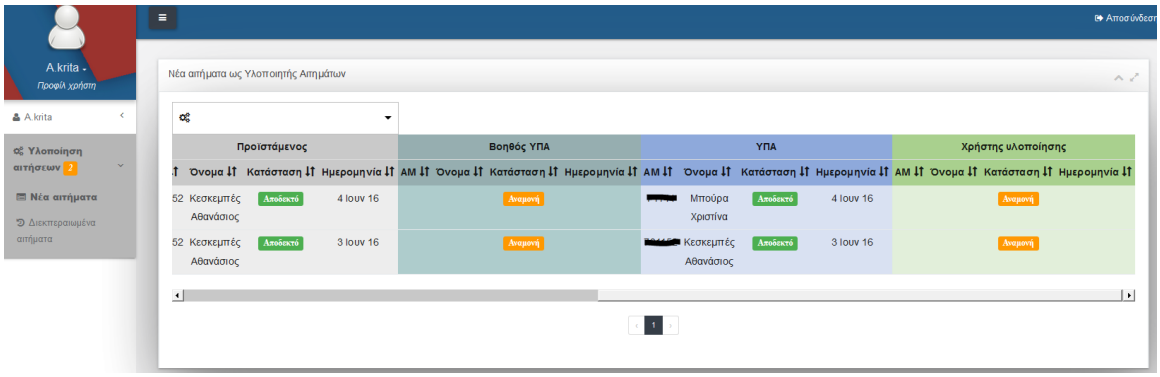
Περίληψη Λειτουργίας

Τα αιτήματα καταλήγουν σε διαχειριστές χρηστών που μπορούν μέσα από την εφαρμογή να διασυνδεθούν στο αντίστοιχο πληροφοριακό σύστημα και να υλοποιήσουν το αίτημα πρόσβασης εφόσον έχει λάβει τις εγκρίσεις στο workflow του ticket.

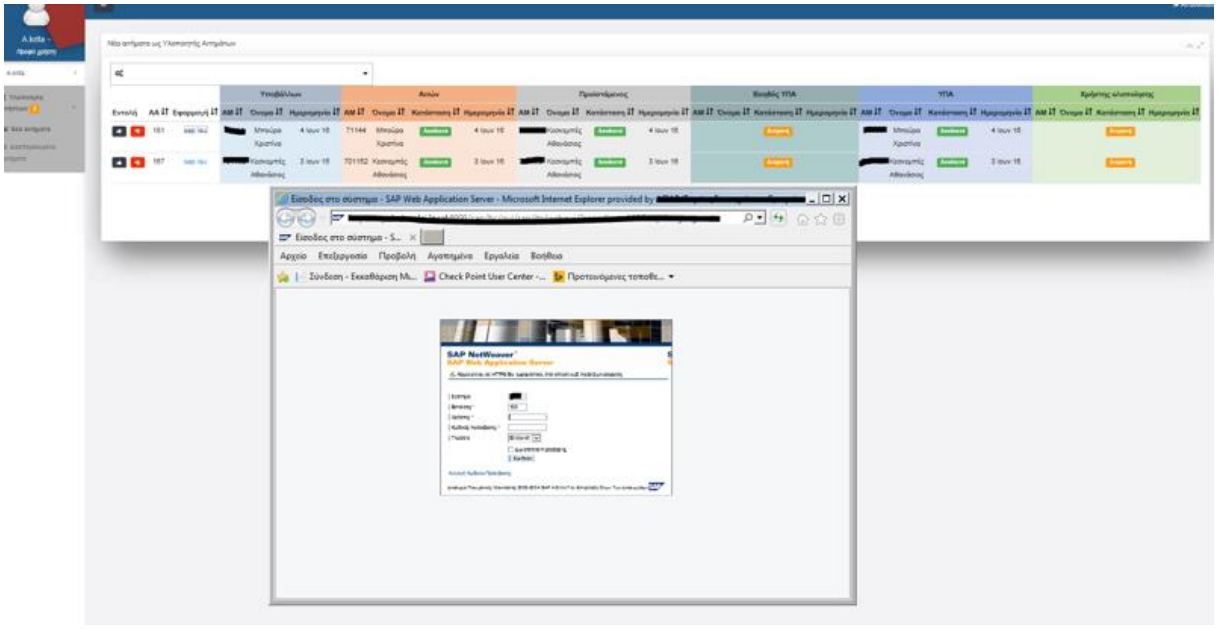
Εικόνες Λειτουργίας



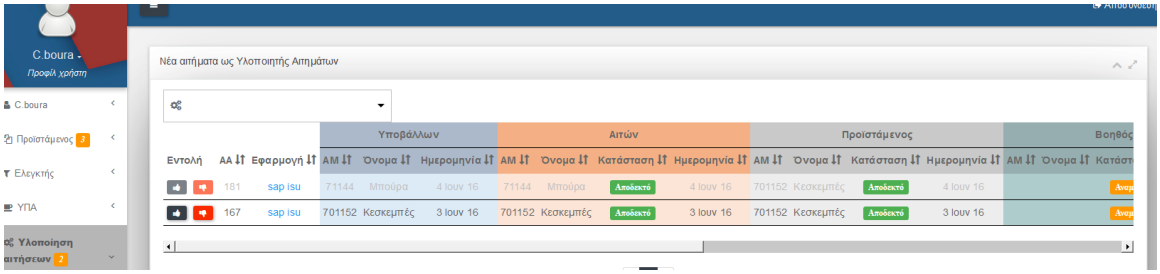
Εικόνα 46 Δημιουργία αιτήματος που αφού προχωρήσει με τις εγκρίσεις του ticket πηγαίνει σε διαχειριστή χρηστών



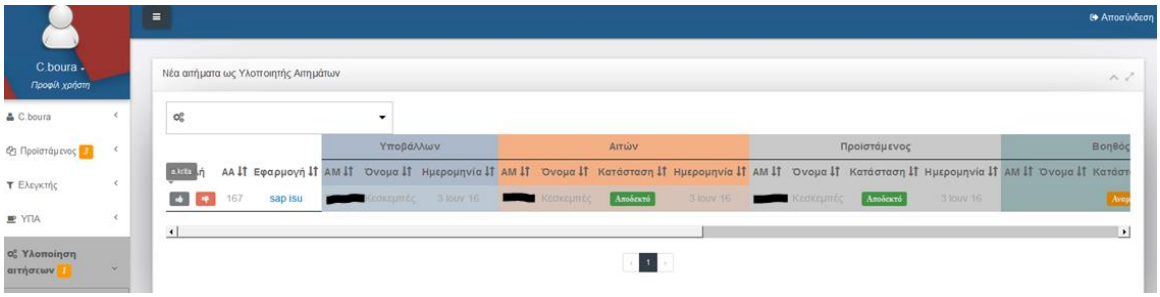
Εικόνα 47 Αίτημα που βρίσκεται σε αναμονή για υλοποίηση από Διαχειριστή Χρηστών



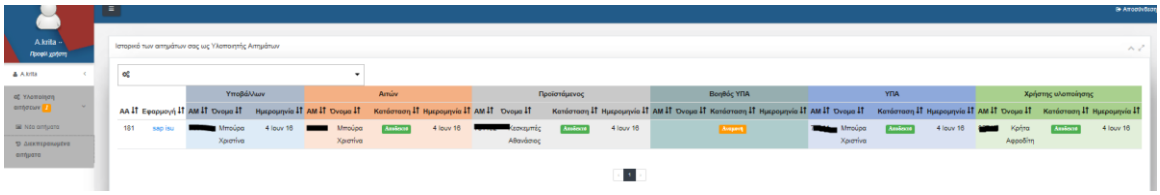
Εικόνα 48 Έναρξη υλοποίησης αιτήματος από τον διαχειριστή χρηστών μέσα από την εφαρμογή SAT



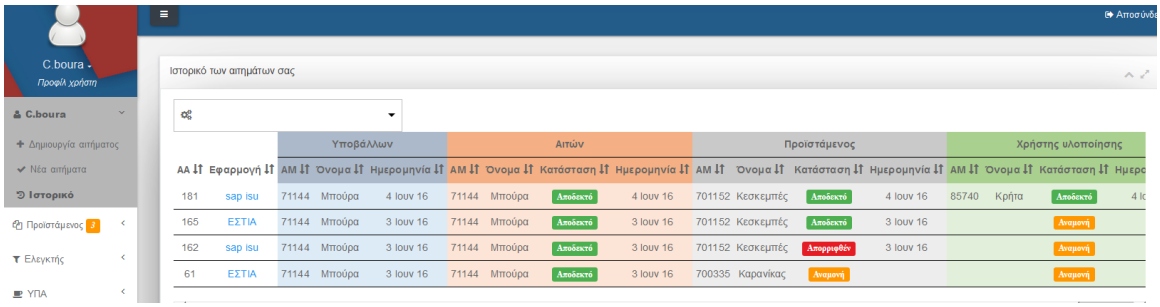
Εικόνα 49 Εφόσον το αίτημα έχει ξεκινήσει να διαχειρίζεται από έναν διαχειριστή χρηστών στους υπόλοιπους διαχειριστές δεν επιτρέπεται να το επεξεργαστούν (αχνή εμφάνισή του στην λίστα με τα αιτήματα που τον αφορούν)



Εικόνα 50 Εμφάνιση pop up (hover) με τον τεχνικό διαχειριστή χρηστών που υλοποιεί το αίτημα και το έχει κλειδώσει στο ticket.



Εικόνα 51 Εμφάνιση στο ticket του υλοποιημένου αιτήματος καθώς και του τεχνικού υλοποίησης.



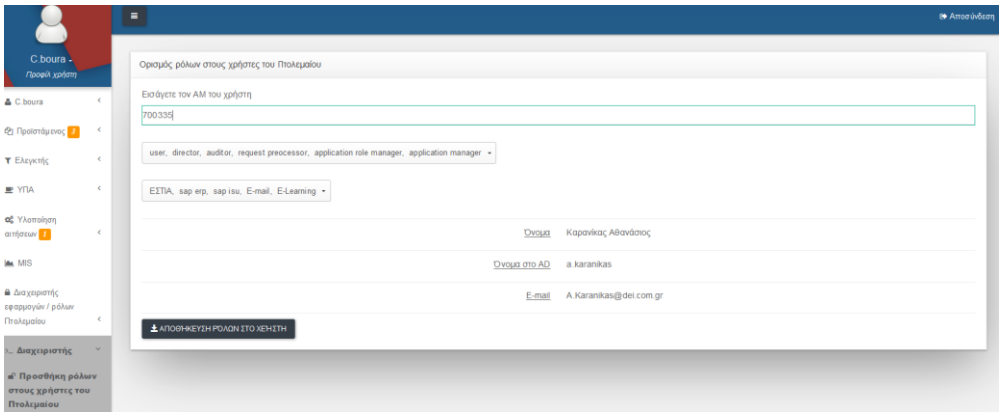
Εικόνα 52 Ιστορικό αιτημάτων χρήστη (εμφάνιση όλων των ticket) με εμφάνιση των υλοποιημένων, των απορριφθέντων και των με αναμονή προς υλοποίηση.

6.5.8 Απόδοση ρόλου (user – owner) & εφαρμογών για διαχειριστές

Περίληψη Λειτουργίας

Αφορά ρόλο που έχει ο διαχειριστής της εφαρμογής Secure Authrization Ticket (SAT).

Εικόνες Λειτουργίας



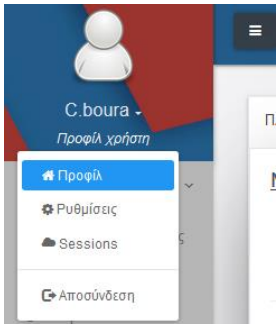
Εικόνα 53 απόδοση ρόλων του SAT και εφαρμογών για τους τεχνικούς διαχείρισης χρηστών.

6.5.9 Αλλαγή στοιχείων στο profile & τις ρυθμίσεις (πχ στοιχεία προσωπικά)

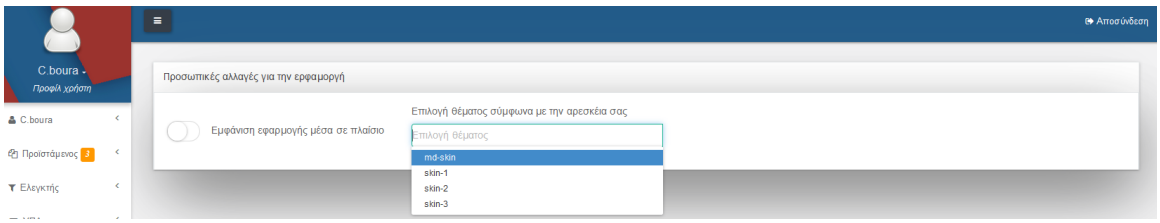
Περίληψη Λειτουργίας

Όλοι οι χρήστες (όλων των τύπων) μπορούν να υλοποιήσουν μεταβολές στα στοιχεία του profile τους αλλά και στην εμφάνιση της εφαρμογής.

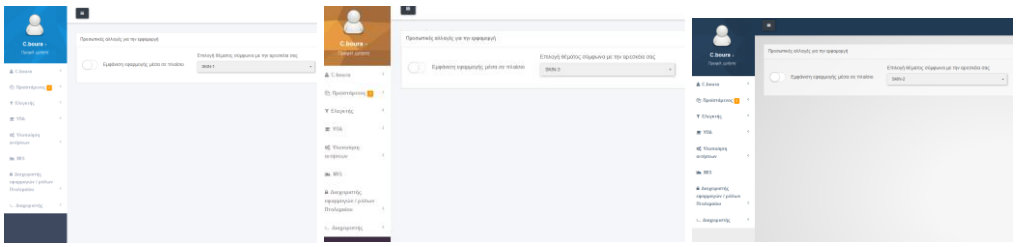
Εικόνα Λειτουργίας



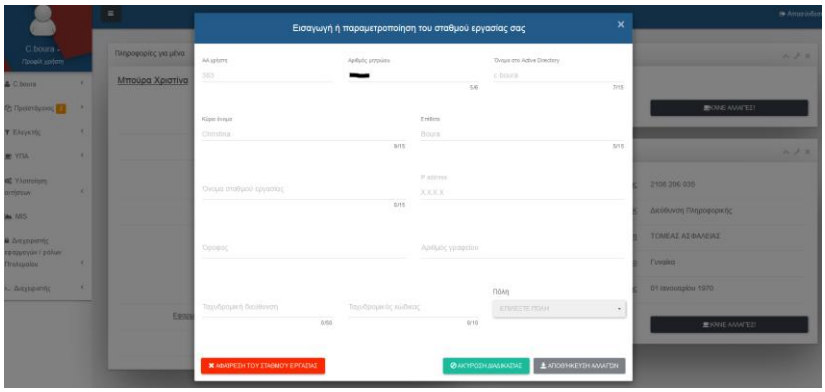
Εικόνα 54 Διαχείριση προφίλ



Εικόνα 55 Διαχείριση της μορφής που θα εμφανίζεται η εφαρμογή



Εικόνα 56 Μορφές που μπορεί να έχει η εφαρμογή (μεταβολή σε ρυθμίσεις)



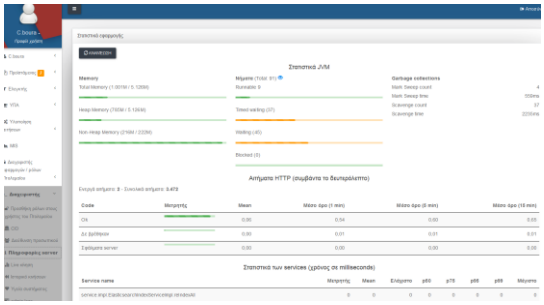
Εικόνα 57 Στοιχεία που αφορούν το inventory των τελικών σταθμών εργασίας χρηστών

6.5.10 Διαχείριση Συστήματος

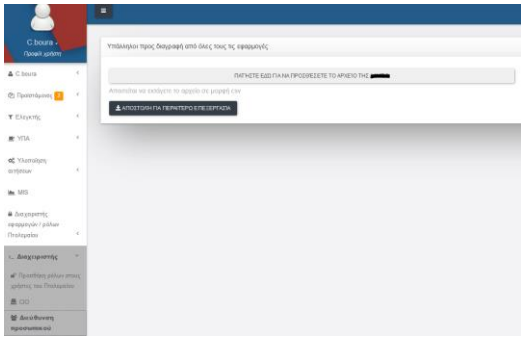
Περίληψη Λειτουργίας

Μέσω της διαχείρισης του συστήματος μπορεί να γίνει η διαχείριση του Μητρώου Εφαρμογών της Επιχείρησης, η διαχείριση των ρόλων τους, η παρακολούθηση των Server (health check) και το auditing σε επίπεδο εφαρμογής και πινάκων (ποιος χρήστης έχει κάνει ποια μεταβολή ή ενημέρωση κτλ) και άλλες διαχειριστικές διεργασίες. Ενδεικτικά ακολουθούν μερικές εικόνες λειτουργιών.

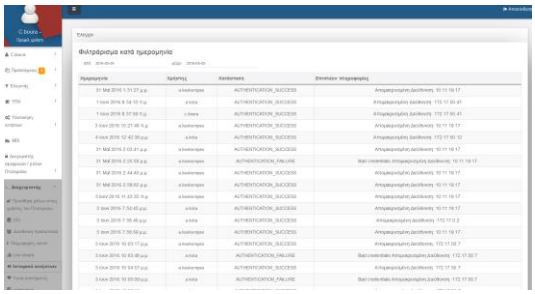
Εικόνες Λειτουργίας



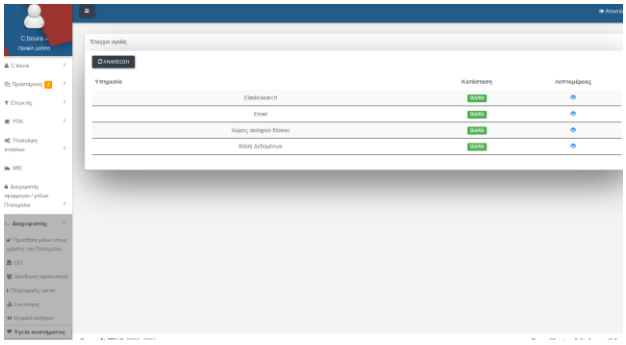
Εικόνα 58 Στατιστικά διαχειριστών SAT



Εικόνα 59 Εισαγωγή αρχείων από το HR



Εικόνα 60 Καταγραφή - Auditing (συνδέσεων και κινήσεων)



Εικόνα 61 Υγεία Συστήματος

7. Σχολιασμός χρηστών για την Εφαρμογή (Secure Authorization Ticketing – SAT)

Συμεωνίδης Ιωάννης

Συνεργάζομαι με την κ. Μπούρα. Ο κ. Κεσκεμπές αφορά νέο συνεργάτη. Η απασχόληση τους εξειδικεύεται στην Ασφάλεια Πληροφοριακών Συστημάτων. Η Χριστίνα ασχολείται με το παραπάνω αντικείμενο. Εκδήλωσε το ενδιαφέρον υλοποίησης ενός Ασφαλούς Συστήματος διαχείρισης αιτημάτων πρόσβασης και αυτοματοποίησής τους εντός μίας Επιχείρησης με εύρος σε όλη την υποδομή. Η εφαρμογή υλοποιήθηκε ακολουθώντας όλες τις φάσεις ανάπτυξης λογισμικού και είναι σε τελικό στάδιο. Αυτοματοποιεί λειτουργίες και βοηθάει

για την επίλυση πολλών κανονιστικών διαδικασιών. Στο έργο της υλοποίησής της είχε σημαντική συμμετοχή ο κ. Κεσκεμπές. Είναι ένα σύγχρονο και ασφαλές πληροφοριακό σύστημα.

Συμεωνίδης Ιωάννης
Υποστήριξη Πληροφοριακών Συστημάτων

Σπυρόπουλος Ιωάννης

Γνωρίζω την κ. Μπούρα Χριστίνα αρκετά χρόνια. Ο κ. Κεσκεμπές Αθανάσιος είναι συνεργάτης μας το τελευταίο χρονικό διάστημα. Έχει ήδη ανταποκριθεί πέραν από τις προσδοκίες μας τεχνολογικά. Η Χριστίνα είναι συνεπής και άτομο που της αρέσει να διερευνά τις νέες τεχνολογίες είτε σε επίπεδο πληροφοριακής υποδομής είτε σε επίπεδο λειτουργικών συστημάτων και βάσεων δεδομένων. Τα τελευταία χρόνια ασχολείται με την Ασφάλεια Πληροφοριακών Συστημάτων και διερευνά όλα τα σημεία όπως την Διοίκηση της, την χρήση τεχνολογιών που διασφαλίζουν τις εφαρμογές και τα πληροφοριακά συστήματα και τις αρμοδιότητες του ελέγχου πληροφοριακών συστημάτων, την αναζήτηση ευπαθειών και την υλοποίηση δοκιμών παρείσδυσης. Ο Θανάσης έχει δείξει ένα μεγάλο ενδιαφέρον και ανταπόκριση στα θέματα που αφορούν την Ασφάλεια Πληροφοριακών Συστημάτων. Μου έδειξαν την εφαρμογή που έχουν αναπτύξει. Αφορά κάτι που μπορεί να χρησιμοποιηθεί σε μεγάλες Επιχειρήσεις που ο αριθμός των εφαρμογών και των εφαρμογοχρηστών είναι πολύ μεγάλος. Αυτοματοποιούν διαδικασίες και λύνουν πολλά προβλήματα που έχουν να κάνουν με τα θέματα συμμόρφωσης και τις Ελεγκτικές Αρχές.
Η εφαρμογή είναι σε τελικό στάδιο. Υπάρχει σκοπός να χρησιμοποιηθεί για την διαχείριση των ροών του authorization.

Γιάννης Σπυρόπουλος
Υποστήριξης Κεντρικών Συστημάτων

Μπαλαφούτα Κωνσταντίνα

Γνωρίζω την κ. Μπούρα Χριστίνα τα τελευταία τρία χρόνια. Ο κ. Κεσκεμπές Αθανάσιος πρόσφατα έχει συνεργαστεί μαζί μας. Η Χριστίνα έχει ως όραμα να ενεργοποιήσει τεχνολογίες που καλύπτουν τα σημεία της Ασφάλειας Πληροφοριακών Συστημάτων. Μία από τις σκέψεις της τα τελευταία χρόνια είναι η υλοποίηση μίας εφαρμογής που θα αυτοματοποιήσει τις διεργασίες αιτημάτων χρηστών σε εφαρμογές. Αυτό θα βοηθούσε πάρα πολύ καθώς εξυπηρετεί βασικά θέματα Ασφάλειας Πληροφοριών. Ο όγκος χρηστών και των εφαρμογών που διαχειρίζομαι είναι πάρα πολύ μεγάλος. Εισηγμένες εταιρείες στο χρηματιστήριο ελέγχονται όσον αφορά την συμμόρφωσή τους σε θέματα authorization και ένα σύστημα σαν και αυτό που αναπτύσσει η Χριστίνα και ο Θανάσης βοηθάει πάρα πολύ τόσο στα θέματα ταχύτητας, όσο και στην αυτοματοποίηση, μη αποποίηση, διαφύλαξη, καταγραφή και εκπαίδευση νέων συνεργατών. Η εφαρμογή έχει ολοκληρωθεί. Υπάρχει σκοπός να χρησιμοποιηθεί για την διαχείριση των ροών του authorization. Θα λύσει πολλά προβλήματα.

Μπαλαφούτα Κωνσταντίνα
Υπεύθυνη Τεχνικός Ασφάλειας τμήματος Διαχείρισης χρηστών και Μητρώου Εφαρμογών

Κορφιάτη Αλεξάνδρα

Η κ. Μπούρα συνεργάζεται μαζί μου τα τελευταία 3 χρόνια σχετικά με θέματα Ασφάλειας Πληροφοριακού Συστήματος για όλες τις εφαρμογές Ανθρωπίνου Δυναμικού. Καθώς οι εφαρμογές που διαχειρίζεται η Διεύθυνση που ανήκω έχουν προσωπικά και ευαίσθητα προσωπικά θέματα είναι για εμάς αναγκαίο να εφαρμόζουμε τις απαραίτητες δικλείδες ασφαλείας και να τα προστατεύσουμε. Υπάρχει συνεργασία με την ομάδα της στην οποία συμμετέχει ο κ. Κεσκεμπές και έχει υλοποιηθεί ένα πληροφοριακό σύστημα το οποίο αυτοματοποιεί τα αιτήματα πρόσβασης. Η ηλεκτρονική μορφή, οι ψηφιακές υπογραφές και η η παρακολούθηση των ροών βοηθούν πολύ καθημερινές διεργασίες εξειδικευνένων τμημάτων. Η Χριστίνα και ο Θανάσης υλοποίησαν την ιδέα του ticketing συστήματος διαχείρισης προσβάσεων και θα βοηθήσει πολύ.

Κορφιάτη Αλεξάνδρα
Επιχειρησιακή Υπεύθυνη Ανθρωπίνου Δυναμικού

Κρήτα Αφροδίτη

Η κ. Μπούρα και ο κ. Κεσκεμπές έχουν υλοποιήσει ένα πληροφοριακό σύστημα που θα επιλύσει πολλά προβλήματα που έχουν σχέση με την διαχείριση χρηστών. Είμαι διαχειρίστρια χρηστών σε πολλές εφαρμογές. Το πρόβλημα που υπάρχει είναι η καθυστέρηση υλοποίησης ενός αιτήματος (πχ απομάκρυνση υπαλλήλου από την Επιχείρηση). Η εφαρμογή που έχει υλοποιηθεί θα μπορούσε να χρησιμοποιηθεί και να λύσει θέματα όπως το παραπάνω.

Κρήτα Αφροδίτη
Τεχνικός Ασφάλειας Πληροφοριακών Συστημάτων

Ρηγάκη Γαρυφαλιά

Συνεργάζομαι άμεσα με την κ. Μπούρα. Ασχολούμαι με τον έλεγχο πληροφοριακών Συστημάτων. Έχει υλοποιήσει σε συνεργασία με τον κ. Κεσκεμπε ένα πληροφοριακό σύστημα που θα επιλύσει πολλά προβλήματα που έχουν σχέση με το authorization. Είμαι IT auditor. Ένα από τα προβλήματα που συναντάει κάποιος ελεγκτής είναι οι χρήστες που έχουν απομακρυνθεί από μια Επιχείρηση. Χρειάζεται κάποιος χρόνος για να ενημερώνονται οι διαχειριστές χρηστών. Η νέα εφαρμογή αυτοματοποίησης των αιτημάτων πρόσβασης που υλοποιούν η κ. Μπούρα και ο κ. Κεσκεμπές θα μπορούσε να βοηθήσει πολύ το έργο των ελεγκτών. Σημαντικό πλέον σημείο είναι και η ύπαρξη της ψηφιακής υπογραφής για την κάλυψη της αρχής μη αποποίησης. Παρακολούθησα πολύ την φάση του ελέγχου που υλοποίησαν στην εφαρμογή και είδα τα λογισμικά δοκιμών παρείσδυσης και ελέγχου ευπαθειών. Έχουν κάνει πολύ σημαντική δουλειά και έχουν καλύψει την εφαρμογή σε πάρα πολλά σημεία όσον αφορά την Ασφάλεια Πληροφοριακών Συστημάτων.

Ρηγάκη Γαρυφαλιά
Υπεύθυνη Ελέγχου Ασφάλειας Πληροφοριακών Συστημάτων (IT Auditor)

Σούφλας Δημήτριος

Ασχολούμαι με τον Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων. Οι πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων, η ανάλυση Επικινδυνότητας τους, η Επιχειρησιακή τους επίπτωση είναι καθημερινές μου λειτουργίες. Η κ. Μπούρα και ο κ. Κεσκεμπές υλοποίησαν κάτι πολύ σημαντικό. Η εφαρμογή που έχουν αναπτύξει θα μπορούσε να ενδυναμώνει την Ασφάλεια σε όλο το επίπεδο μίας Επιχείρησης. Εισάγει μία δικλείδα ασφαλείας που είναι η αυτοματοποίηση και η διαχείριση λογαριασμών πρόσβασης σε γρήγορο χρόνο. Ένα εγκεκριμμένος λογαριασμός από έναν υπεύθυνο επεξεργασίας πρέπει να έχει καλύψει τον διαχωρισμό καθηκόντων, την ελάχιστη γνώση που πρέπει να έχει ο χρήστης με βάση την επιχειρησιακή απαίτηση καθώς τα ελάχιστα προνόμια που είναι αναγκαία για την δουλειά του.

Σούφλας Δημήτριος
Τεχνικών Ασφάλειας ΠΣ - Πολιτικών Προτύπων, Διαχείρισης Κινδύνων και Ανάλυσης Επικινδυνότητας

Καλπούζος Στέργιος

Ασχολούμαι με τους ελέγχους ευπαθειών και τις δοκιμές παρείσδυσης (VA & PENETRATION TESTS) σε πληροφοριακά συστήματα. Η εφαρμογή που ανέπτυξαν η Χριστίνα και ο Θανάσης δεν άπτεται του αντικειμένου μου αλλά καλύπτει πολλά και ποικίλα προβλήματα που υπάρχουν στα σημεία του authorization. Συμμετείχα ως UAT key user στις τελικές δοκιμές λειτουργίας και πραγματικά έχει πολύ ενδιαφέρουσα τεχνολογία. Java Spring & Angular σε συνδυασμό με την Oracle αφορούν σύγχρονα εργαλεία. Πάρα πολύ καλή εργασία με κάλυψη σε πολλά σημεία όσον αφορά την Ασφάλεια των Πληροφοριακών Συστημάτων.

Καλπούζος Στέργιος
Τεχνικός Ασφάλειας - IT Auditor

Κίγκας Νικόλαος

Ασχολούμαι με τεχνικό έλεγχο για κενά ασφαλείας σε πληροφοριακά συστήματα (va, penetration, logging, auditing). Συμμετείχα ως χρήστης δοκιμών στην νέα εφαρμογή που ανέπτυξε ο Θανάσης και η Χριστίνα. Σημαντικό έργο. Πολύ καλές τεχνολογίες. Πάρα πολύ καλή εργασία.

Κίγκας Νικόλαος
Τεχνικός Ασφάλειας - IT Auditor

8. Έλεγχος

8.1 Έλεγχος Ασφάλειας Πληροφοριακού Συστήματος

Η επόμενη Φάση της μεθοδολογίας του συστήματος «Secure Authorization Ticketing – SAT» αφορά τον έλεγχο που γίνεται για την ασφάλεια και την ορθή λειτουργία του.
Για την φάση αυτή χρησιμοποιήθηκαν εργαλεία ελέγχου ευπαθειών και δοκιμών παρείσδυσης. Τα εργαλεία που διερευνήθηκαν είναι τα ακόλουθα:

GFI Languard (Network security scanner and patch management)
Accunetix va & pen test crawler
Nexpose
Metasploit
SQL MAP for SQL INJECTION
Wire Shark (packet injection - sniffing)
Χρησιμοποιήθηκαν τα ακόλουθα (ΠΑΡΑΡΤΗΜΑ Ζ):
OWASP ZAP
GFI

Τα εργαλεία εμφάνισαν ύπαρξη ευπαθειών. Διορθώθηκαν από την ομάδα Ανάπτυξης και έγινε επανάληψη των ελέγχων.

Η εφαρμογή εξετάστηκε από εξειδικευμένους χρήστες και υλοποιήθηκαν τα User Acceptance Test. Οι αρχικοί στόχοι επιτεύχθηκαν και η εφαρμογή είναι έτοιμη για να ενταχθεί σε παραγωγή.

9. Συμπεράσματα

9.1 Συμπεράσματα μετά το πέρας της υλοποίησης και της δοκιμαστικής λειτουργίας

Η πτυχιακή εργασία ξεκίνησε με έναυσμα την αυτοματοποίηση επιχειρησιακής διαδικασίας που λόγο της πολυπλοκότητάς της, λόγο του όγκου των εμπλεκόμενων σημείων (πλήθος εφαρμογών, πλήθος χρηστών εφαρμογών, έλλειψη τεχνικής αντιμετώπισης κ.α.) και λόγο της ανάγκης διατήρησης στοιχείων μη αποποίησης και εξυπηρέτησης των ελεγκτικών μηχανισμών αποτέλεσε μία ενδιαφέρουσα πρόκληση. Ο στόχος ήταν ο σχεδιασμός και η υλοποίηση πληροφοριακού συστήματος διαχείρισης αιτημάτων πρόσβασης του Τμήματος Πληροφορικής μίας μεγάλης επιχείρησης που θα επέτρεπε την σύνδεση με το LDAP της αλλά και με άλλα Πληροφοριακά Συστήματα. Θα κάλυπτε την διαχείριση του μητρώου εφαρμογών της, θα υλοποιούσε την διαχείριση αιτημάτων πρόσβασης, θα είχε ιστορικότητα, και στατιστικά αιτημάτων, θα κάλυπτε την παρακολούθηση της πορείας και της κατάστασης ενός σχετικού αιτήματος, θα έκανε την υλοποίηση αιτήματος πρόσβασης. Στόχος ήταν η αυτοματοποίηση τους και η υλοποίησή τους σε λιγότερο χρόνο και διατήρηση κεντρικά της πληροφορίας που θα χρησιμοποιείται σε ελεγκτικούς μηχανισμούς (σε ψηφιακή μορφή με χρήση ψηφιακής υπογραφής). θα κάλυπτε τον διαχωρισμό καθηκόντων. Όπως φάνηκε και από τα σχόλια των χρηστών που αναφέρθηκαν πιο πάνω, η εργασία πέτυχε σε μεγάλο βαθμό τους αρχικούς στόχους της.

Η πτυχιακή εργασία μας έδωσε την δυνατότητα να μάθουμε τεχνολογίες πληροφορικής που έως τώρα μας ήτανε μερικώς ή εντελώς άγνωστες. Αυτές αφορούν τις τεχνολογίες που παρουσιάστηκαν σε προηγούμενα κεφάλαια (hypervisors, λειτουργικά συστήματα, Βάση δεδομένων, περιβάλλοντα ανάπτυξης εφαρμογής Eclipse for Spring (Backend) και WebStorm for Angular Development (frontend)). Ο όγκος του κώδικα επεκτείνεται σε πάνω από 200 κλάσεις με 20000 γραμμές κώδικα και έχει σημεία που ενδυναμώνουν την Ασφάλεια μίας εφαρμογής από ευπάθειες ιστού. Η Βάση σχεδιάστηκε και υλοποιήθηκε από το Liquid Base για να διατηρείται και auditing στις αλλαγές του σχήματος και αποτυπώθηκε πέραν από την Oracle, σε H2 (java sql database – used on ram), για διευκόλυνση στο περιβάλλον ανάπτυξης.

Ο σημαντικότερος στόχος που πετύχαμε ήταν η εκμάθηση όλων των παραπάνω μέσα από τις ανάγκες τις πτυχιακής. Τις παραπάνω τεχνολογίες καθώς και μέρος της εφαρμογής θα τα χρησιμοποιήσουμε στην συνέχεια της επαγγελματικής μας καριέρας.

Αποκομίσαμε γνώση που αφορά την υλοποίηση μίας ασφαλούς εφαρμογής με ενσωματωμένη την ασφάλεια πληροφοριακού συστήματος από την έναρξη λήψης της ιδέας του έως το πέρας της υλοποίησής του (λειτουργία δικτύου, βάσεις δεδομένων, κρυπτογράφηση, διασφάλιση από ευπάθειες ιστου κ.α.).

Όσο αφορά την επιχείρηση, το σύστημα κρίθηκε ενδιαφέρον και με προοπτικές υιοθέτησης. Παρόλα αυτά η ανάπτυξή του σε πραγματικές συνθήκες απαιτεί την δοκιμή από εξειδικευμένη ομάδα χρηστών (User Acceptance Test) που θα ενδυναμώσει τις απαιτήσεις και τους στόχους της επιχείρησης, τη στρατηγική, το κόστος και τα αναμενόμενα οφέλη από την χρήση της.

Η έρευνα, η ανάλυση και ο σχεδιασμός της εφαρμογής έλαβε μέρος σε μεγάλη διάρκεια όλο το διδακτικό έτος. Η υλοποίηση της εφαρμογής ξεκίνησε στο πέρας του φθινοπώρου και διήρκησε όλη την περίοδο του χειμώνα και της άνοιξης του διδακτικού έτους. Ο χρόνος που καταναλώθηκε για την υλοποίηση δεν ήτανε τόσος όσος χρειαζόταν ώστε να εφαρμοστεί στο μέγιστο το functionality μιας τέτοιας εφαρμογής. Σημειωτέο του ότι όλες σχεδόν οι τεχνολογίες ήταν άγνωστες και χρειάστηκε πάρα πολύς χρόνος ώσπου να γίνει κατανοητή η λειτουργικότητα και η συνδεσιμότητα τους. Υπήρχε μόνο η γνώση της Java που είχαμε από το προπτυχιακό και το μεταπτυχιακό ενώ δεν είχαμε διδαχτεί στο παρελθόν αυτές τις νέες τεχνολογίες Java Spring – Angular - Oracle. Η διάθεση είναι η εφαρμογή να επεκταθεί και στην διαχείριση κωδικών πρόσβασης προνομιακών λογαριασμών αλλά και σε ότι αναφέρεται στο επόμενο section.

9.2 Προτάσεις - Επιπλέον υλοποιήσεις σχετικές με το project μελλοντικά.

- Υποσύστημα διαχείρισης των διαχειριστικών – προνομιακών λογαριασμών με encryption & decryption και με διατήρηση των προνομιακών προσβάσεων σε κρυπτογραφημένη μορφή για την διαχείριση τους κεντρικά.
- Υποσύστημα για την διαχείριση της αποθήκης των τελικών σταθμών εργασίας της επιχείρησης καθώς και της καταγραφής των χρεώσεών τους.
- Υλοποίηση τεχνικών Single Sign On και Identity Management.

- Αυτοματοποίηση της υλοποίησης του authorization μέσα από το πληροφοριακό σύστημα σε εμπορικές και custom εφαρμογές του μητρώου.
- Ενδυνάμωση των στατιστικών και της παρακολούθησης.
- Data Masking (Εφαρμογή στα δεδομένα του πληροφοριακού συστήματος).
- Ενδυνάμωση των τεχνικών data at rest & data in motion και της προστασία των δεδομένων σε επίπεδο μνήμης (data in use).
- Ασφάλειας Πληροφοριακών Συστημάτων και Load Balancing.
- Redis Token Server
- Load Balancing

Ευχαριστίες

- Ευχαριστούμε τις οικογένειές μας για την στήριξη που μας έδωσαν στην προσπάθεια μας.
- Ευχαριστούμε επιβλέποντα Δρ. Ριζομιλιώτη και του συμβούλους Δρ. Μήτρου και Δρ. Κοκκολάκη για την ευκαιρία που μας έδωσαν να ασχοληθούμε με το θέμα της πτυχιακής.
- Ευχαριστούμε τους συναδέλφους μας καθώς και τους συνεργάτες μας στον χώρο εργασίας οι οποίοι έλαβαν μέρος στα ερωτηματολόγια, και στην δοκιμή της εφαρμογής κατά το τελικό της στάδιο.

10. ΠΑΡΑΡΤΗΜΑΤΑ

10.1 Παράρτημα Α : Ερωτηματολόγια για το «Ασφαλές σύστημα αυτοματοποίησης και διαχείρισης αιτημάτων πρόσβασης στα Πληροφοριακά συστήματα της Επιχείρησης» - Secure Authorizaton Ticketing (SAT)

10.1.1 Ερωτηματολόγιο Business Users

ΟΝΟΜΑ:

ΗΜΕΡΟΜΗΝΙΑ :

1. **Είσαστε χρήστης πληροφοριακού συστήματος στην Επιχείρηση που εργάζεστε;** *
   - ΝΑΙ
   - ΟΧΙ
2. **Σας παρέχονται υπηρεσίες πληροφοριακών υποδομών της επιχείρησης (πχ Internet, Email)**
   - ΝΑΙ
   - ΟΧΙ
   - ΔΕΝ ΓΝΩΡΙΖΩ
3. **Η επιχείρηση που εργάζεστε διαθέτει LDAP σύστημα;**

   Active Directory
   - ΝΑΙ
   - ΟΧΙ
   - ΔΕΝ ΓΝΩΡΙΖΩ
4. **Σε πόσες Εφαρμογές ή Υπηρεσίες είσαστε πληροφοριακός χρήστης;**
   - 0
   - 1-5
   - 5-10
   - >10
5. **Ποιό είναι το πλήθος των υπαλλήλων στην Επιχείρησης που εργαζόσαστε;** *
   - < 500

- >500 & <1000
- >1000 & <5000
- >5000 & <10000
- >10000
- ΔΕΝ ΓΝΩΡΙΖΩ

6. Με ποιό τρόπο γίνονται τα αιτήματα πρόσβασης σας σε εφαρμογές και υπηρεσίες;

Υπηρεσίες είναι οτιδήποτε παρέχεται ως ψηφιακή παροχή από την Επιχείρησης

1. Email στην ομάδα authorization
2. Αίτηση που αποστέλεται με ταχυδρομείο
3. Ψηφιακή αίτηση που συμπληρώνεται και υπογράφεται από τον προιστάμενο

- Αυτοματοποιημένη διαδικασία workflow που λαμβάνει εγκρίσεις προισταμένων & υπεύθυνου επεξεργασίας
- Other:

7. Υπάρχει διαδικασία παρακολούθησης της πορείας του αιτήματός σας;

- ΝΑΙ
- ΟΧΙ

8. Πόσος χρόνος χρειάζεται για να υλοποιηθεί το αίτημά σας;

Μέσος όρος

- Υλοποιείται μέσα στην Ημέρα
- Υλοποιείται μέσα στην Εβδομάδα
- Υλοποιείται μέσα στον μήνα
- Other:

9. Έχετε ιστορικό για τα αιτήματα πρόσβασης σε εφαρμογές και υπηρεσίες τα οποία έχετε ζητήσει;

Χειρόγραφο ή ψηφιακό με τις υπογραφές και τις εγκρίσεις τους

- ΝΑΙ
- ΟΧΙ ΓΙΑ ΟΛΑ
- ΟΧΙ

10. Έχετε ποτέ αιτηθεί πρόσβαση και η αίτησή σας έχει χαθεί;

- NAI
- OXI

11. **Τί από τα παρακάτω θεωρείτε ότι θα μπορούσε να σας διευκολύνει εφόσον η διαδικασία που υλοποιείται για αιτήματα πρόσβασης στις εφαρμογές & Υπηρεσίες της Επιχείρησης γινόταν με αυτόματη διαδικασία;**

    Στην διαδικασία θα περιλαμβανόταν ψηφιακή συμπλήρωση αιτήματος, επιλογή εφαρμογών και υπηρεσιών, επιλογή ρόλων, ροή παρακολούθησης αιτήματος, ροή εγκρίσεων, ψηφιακές υπογραφές, αυτόματη ειδοποίηση

    - Παραγωγικότητα
    - Ασφάλεια
    - Εκσυγχρονισμός
    - Διατήρηση Ιστορικότητας
    - Other:

12. **Γνωρίζετε περιπτώσεις που απομακρύνθηκε συνάδελφός σας από την Επιχείρηση αλλά οι λογαριασμοί του έχουν διατηρηθεί;**
    - τουλάχιστον μία περίπτωση
    - πάνω από μία περίπτωση
    - πάνω από πέντε περιπτώσεις
    - Other:

10.1.2 Ερωτηματολόγιο for Authorization Administrators

ΟΝΟΜΑ:

ΗΜΕΡΟΜΗΝΙΑ :

1. **Σε πόσα Πληροφοριακά Συστήματα Διαχειρίζεστε Χρήστες στην Επιχείρηση που Εργάζεστε;** *
    - <10
    - >10 & <50
    - >50 & <100
    - >100
2. **Ποιούς τύπους αφορούν οι χρήστες που διαχειριζόσαστε;** *
    - Business users

- System Administrators
- DataBase Administrators
- Application Administrators
- Networik Administrators
- Security Administrators
- Other:

3. Η επιχείρηση που εργάζεστε διαθέτει LDAP σύστημα;

Active Directory

- NAI
- OXI
- ΔΕΝ ΓΝΩΡΙΖΩ

4. Πόσους business application users διαθέτει η Επιχείρηση σας;

- <500
- >500 & <1000
- >1000 & <5000
- >5000 & <10000
- >10000 & <50000
- >50000

5. Ποιό είναι το πλήθος των υπαλλήλων στην Επιχείρησης που εργαζόσαστε; *

- < 500
- >500 & <1000
- >1000 & <5000
- >5000 & <10000
- >10000
- ΔΕΝ ΓΝΩΡΙΖΩ

6. Με ποιό τρόπο γίνονται τα αιτήματα πρόσβασης σας σε εφαρμογές και υπηρεσίες;

Υπηρεσίες είναι οτιδήποτε παρέχεται ως ψηφιακή παροχή από την Επιχείρησης

- Email στην ομάδα authorization
- Αίτηση που αποστέλεται με ταχυδρομείο
- Ψηφιακή αίτηση που συμπληρώνεται και υπογράφεται από τον προιστάμενο

- Αυτοματοποιημένη διαδικασία workflow που λαμβάνει εγκρίσεις προισταμένων & υπεύθυνου επεξεργασίας
- Other:

7. **Υπάρχει διαδικασία παρακολούθησης της πορείας των αιτημάτων από τους εμπλεκομένους;**

   - ΝΑΙ
   - ΟΧΙ
   - Other:

   Πόσος χρόνος χρειάζεται για να υλοποιηθεί το αίτημά σας;

   Μέσος όρος

   - Υλοποιείται μέσα στην Ημέρα
   - Υλοποιείται μέσα στην Εβδομάδα
   - Υλοποιείται μέσα στον μήνα
   - Other:

8. **Έχετε ιστορικό για τα αιτήματα πρόσβασης σε εφαρμογές και υπηρεσίες τα οποία έχετε διαχειριστεί;**

   Χειρόγραφο ή ψηφιακό με τις υπογραφές και τις εγκρίσεις τους

   - ΝΑΙ
   - ΟΧΙ ΓΙΑ ΟΛΑ
   - ΟΧΙ

9. **Έχετε ποτέ αιτηθεί πρόσβαση και η αίτησή σας έχει χαθεί;**

   - ΝΑΙ
   - ΟΧΙ

10. **Τί από τα παρακάτω θεωρείτε ότι θα μπορουσε να σας διευκολύνει εφόσον η διαδικασία που υλοποιείται για αιτήματα πρόσβασης στις εφαρμογές & Υπηρεσίες της Επιχείρησης γινόταν με αυτόματη διαδικασία;**

    Στην διαδικασία θα περιλαμβανόταν ψηφιακή συμπλήρωση αιτήματος από τον χρήστη, επιλογή εφαρμογών και υπηρεσιών, επιλογή ρόλων, ροή παρακολούθησης αιτήματος, ροή εγκρίσεων, ψηφιακές υπογραφές, αυτόματη ειδοποίηση διαχειριστών

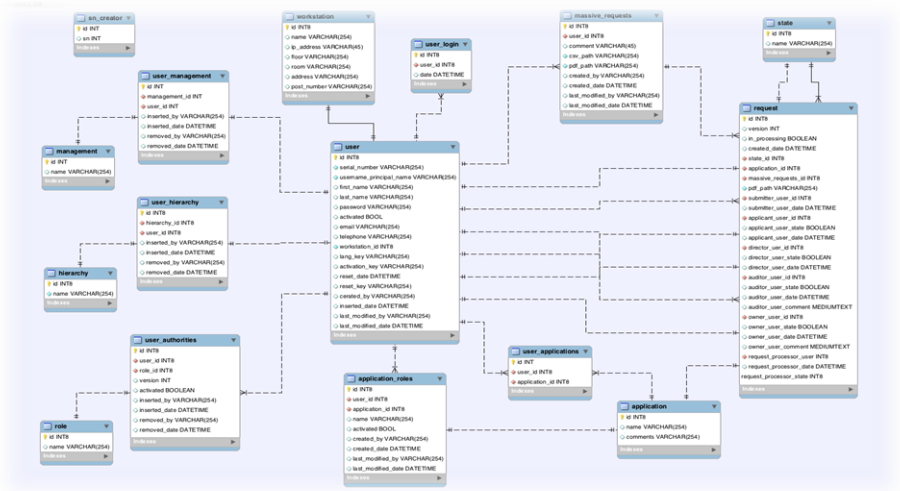
μέσω email ή sms, αυτόματη δρομολόγηση στο σύστημα υλοποίησης αιτήματος ή στο SSO & Identity Managment System

- Παραγωγικότητα
- Ασφάλεια
- Εκσυγχρονισμός
- Διατήρηση Ιστορικότητας
- Other:

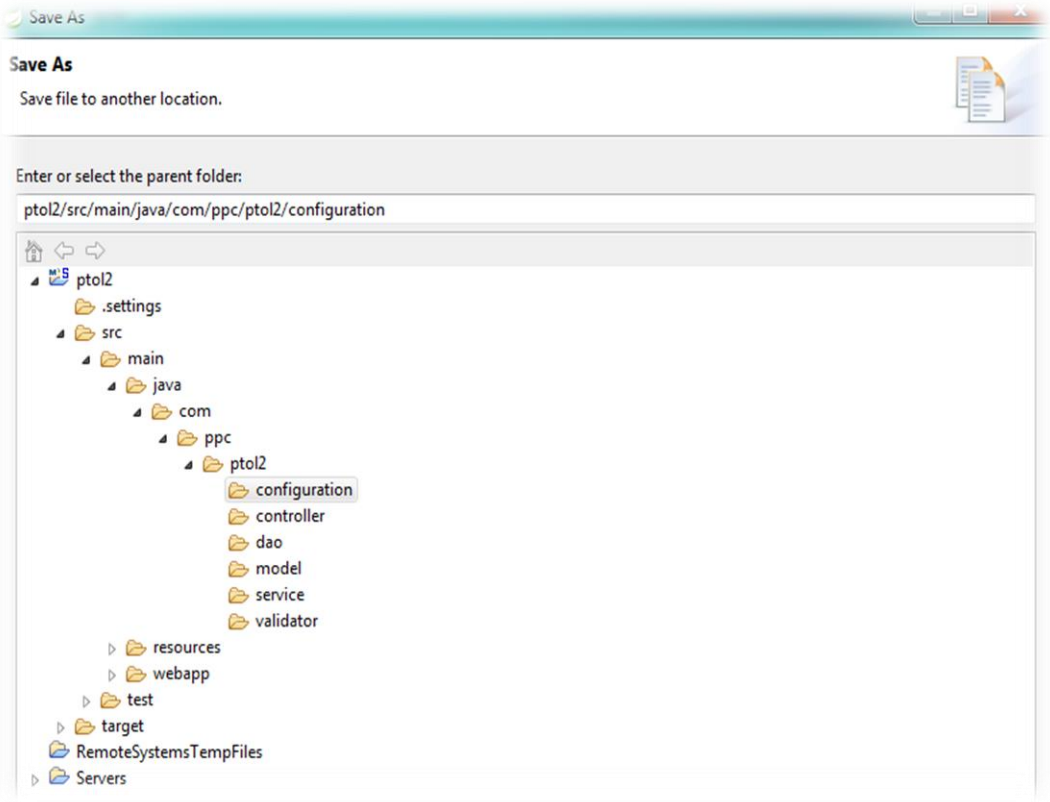
11. Γνωρίζετε περιπτώσεις που απομακρύνθηκε συνάδελφός σας από την Επιχείρηση αλλά οι λογαριασμοί του έχουν διατηρηθεί;

- τουλάχιστον μία περίπτωση
- πάνω από μία περίπτωση
- πάνω από πέντε περιπτώσεις
- Other:

10.2 Παράρτημα Β : Βάση Δεδομένων



Εικόνα 62 Βάση Δεδομένων



Εικόνα 63 Spring Αρχιτεκτονική & σημείο που υπάρχει το XML που δημιουργεί την ΒΔ

10.2.1 Αντικείμενα Βάσης Δεδομένων

10.2.1.1 Sequences

- seq_******_user Sequence number για τον πίνακα *****_user
- seq_request Sequence number για τον πίνακα *****_user

- seq_role Sequence number για τον πίνακα *******_user
- seq_per_aud_eve Sequence number για τον πίνακα *******_user
- seq_per_aud_eve_data Sequence number για τον πίνακα *******_user
- seq_sn_generator_702 Αφορά μετρητή που ξεκινάει από το 702000 (ειδικοί χρήστες)
- seq_sn_generator_802 Αφορά μετρητή που ξεκινάει από το 802000 (ειδικοί χρήστες)

10.2.1.2 Tables

- user_activity καταγραφή των κινήσεων του χρήστη (κάθε ρόλος – όλα τα login)
- Entityaudit_event καταγραφή όλων των κινήσεων στην βάση σε οποιοδήποτε πίνακα
- application εδώ καταχωρούνται όλες οι εφαρμογές στις οποίες γίνεται διαχείριση χρηστών
- application_role εδώ καταχωρούνται στοιχεία που αφορούν το ποιος έκανε upload csv και συνδέεται με τον role που έχει όλους τους ρόλους των εφαρμογών εφόσον διαθέτουν ρόλους
- audit_rev_entity revision (όταν γίνει μία αλλαγή στο request κρατάει μία έκδοση - versioning
- vok διατηρεί τα τμήματα
- vok_category διατηρεί την ομαδοποίηση των τμημάτων
- massive_request τον υπεύθυνο για το μαζικό αίτημα, το csv αρχείο & παίρνει ένα id που συνδέεται με πολλά MSVREC
- persistent_audit_event αφορά την ΒΠ και αλλαγές που γίνονται και δίνει δυνατότητα για rollback MASTER
- persistent_audit_event_data (many to many και δημιουργείται από την ίδια την java) αφορά την ΒΠ και αλλαγές που γίνονται και δίνει δυνατότητα για rollback DETAIL
- hr_uploaded_files για μαζικό upload των csv με τις αποχωρήσεις (ΔΑΝΠΟ)
- persistent_token καταγραφή των login (διαγράφεται κάθε δύο ημέρες) μέχρι 10 session (σαν cookies)
- *******_user τα στοιχεία των χρηστών
- request αφορά μεγάλο όγκο που διατηρείται και έχει πληροφορία για όλα τα request
- operational_areas περιέχει τις επιχειρησιακές περιοχές
- request_application έχει σύνδεση με το request 1-1 και αναφέρει της εφαρμογή που ζητά το request
- request_application_role έχει τους ρόλους που αιτείται ο χρήστης για τον MASTER appl DETAIL
- role έχει όλους τους ρόλους
- state καταστάσεις που βρίσκεται το request (pending, completed)
- user_operational_area επιχειρησιακή περιοχή του χρήστη
- user_application εφαρμογές στις οποίες έχει πρόσβαση ο request processor, auditor,owner
- user_authority οι ρόλοι του SAT
- user_management Το BOK που έχει επιλέξει ότι ανήκει ο χρήστης συνδέεται με τον πίνακα VOK & VOK category
- user_workstation αφορά πληροφορία που θα χρειαστεί για την αποθήκη των PC
- City οι πόλεις της Ελλάδος

Πίνακας 2 Sequences & Tables (DB)

10.2.1.3 XML για τους πίνακες που δημιουργούνται στην ΒΔ

Τα αρχικοποιημένα δεδομένα δεν παρατίθενται στο έγγραφο για λόγους ασφάλειας.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<!-- BOURA CHRISTINE - KESKEMPES ATHANASIOS DB STRUCTURE FOR SAT II APPLICATION -->
<!-- 2015-2016 THE APPLICATION IS ABOUT AUTOMATION OF AUTHORIZATION REQUESTS WITH STATISTICS AUDITING WORKFLOWS & DIGITAL SIGNATURES -->

  <databaseChangeLog xmlns="http://www.liquibase.org/xml/ns/dbchangelog" xmlns:ext="http://www.liquibase.org/xml/ns/dbchangelog-ext"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.liquibase.org/xml/ns/dbchangelog-ext
http://www.liquibase.org/xml/ns/dbchangelog/dbchangelog-ext.xsd http://www.liquibase.org/xml/ns/dbchangelog http://www.liquibase.org/xml/ns/dbchangelog/dbchangelog-3.4.xsd">

<!-- PROPERTYs – ΣΤΑΘΕΡΑ -->
                    <property name="now" value="now()" dbms="mysql,h2" />
                    <property name="now" value="current_timestamp" dbms="postgresql" />
                    <property name="now" value="sysdate" dbms="oracle" />
                    <property name="autoIncrement" value="true" dbms="mysql,h2,postgresql,oracle" />
                    <property name="floatType" value="float4" dbms="postgresql, h2" />
                    <property name="floatType" value="float" dbms="mysql, oracle" />

                    <changeSet author="akeske" id="30122015000009">

 <!-- SEQUENCEs -->
                        <createSequence sequenceName="seq_******_user" cycle="false" incrementBy="1" startValue="1" />
        <createSequence sequenceName="seq_request" cycle="false" incrementBy="1" startValue="1" />
        <createSequence sequenceName="seq_role" cycle="false" incrementBy="1" startValue="1" />
        <createSequence sequenceName="seq_per_aud_eve" cycle="false" incrementBy="1" startValue="1" />
        <createSequence sequenceName="seq_per_aud_eve_data" cycle="false" incrementBy="1" startValue="1" />
        <createSequence sequenceName="seq_sn_generator_702" cycle="false" incrementBy="1" startValue="702000" />
        <createSequence sequenceName="seq_sn_generator_802" cycle="false" incrementBy="1" startValue="802000" />

<!-- TABLE  sn_generator -->
<createTable tableName="sn_generator">
            <column name="new_sn" type="bigint">
               <constraints nullable="false" />
            </column>
            <column name="created_by" type="varchar(255)">
               <constraints nullable="false" />
            </column>
            <column defaultValueComputed="${now}" name="created_date" type="timestamp"></column>
            <column name="last_modified_by" type="varchar(255)" />
            <column name="last_modified_date" type="timestamp" />
        </createTable>

<!-- TABLE  user_activity -->
        <createTable tableName="user_activity">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="date" type="timestamp" />
            <column name="page" type="varchar(255)"></column>
            <column name="description" type="varchar(255)"></column>
            <column name="ip_address" type="varchar(50)"></column>
            <column name="user_id" type="bigint" />
        </createTable>

<!-- TABLE  audit_event -->
        <createTable tableName="audit_event">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="request_id" type="bigint"> <constraints nullable="false" />  </column>
            <column name="request_type" type="varchar(255)"> <constraints nullable="false" /> </column>
```

```
            <column name="action" type="varchar(20)"> <constraints nullable="false" /> </column>
            <column name="request_value" type="clob" />
            <column name="commit_version" type="integer" />
            <column name="modified_by" type="varchar(100)" />
            <column name="modified_date" type="timestamp">  <constraints nullable="false" /> </column>
        </createTable>

        <dropDefaultValue tableName="audit_event" columnName="modified_date" columnDataType="datetime" />

<!-- TABLE  application -->
        <createTable tableName="application">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="comment" type="varchar(500)" />
            <column name="url" type="varchar(255)" />
            <column name="name" type="varchar(50)"> <constraints nullable="false" /> </column>
            <column name="created_by" type="varchar(255)"> <constraints nullable="false" />  </column>
            <column defaultValueComputed="${now}" name="created_date" type="timestamp"> <constraints nullable="false" /> </column>
            <column name="last_modified_by" type="varchar(255)" />
            <column name="last_modified_date" type="timestamp" />
            <column name="form" type="varchar(10)" />
            <column name="form_title" type="varchar(255)" />
            <column name="form_checkbox" type="varchar(255)" />
            <column name="pdf_summary" type="varchar(255)" />
        </createTable>

<!-- TABLE  application_role -->
        <createTable tableName="application_role">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="created_by" type="varchar(255)"> <constraints nullable="false" /> </column>
            <column defaultValueComputed="${now}" name="created_date" type="timestamp"> <constraints nullable="false" /> </column>
            <column name="last_modified_by" type="varchar(255)" />
            <column name="last_modified_date" type="timestamp" />
            <column name="name" type="varchar(50)"> <constraints nullable="false" />  </column>
            <column name="alias" type="varchar(50)" />
            <column name="application_id" type="bigint" />
            <column name="user_id" type="bigint" />
            <column name="activated" type="bit" />
        </createTable>

<!-- TABLE  audit_rev_entity -->
        <createTable tableName="audit_rev_entity">
            <column name="id" type="int" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="timestamp" type="bigint"> <constraints nullable="false" /> </column>
            <column name="changed_by" type="varchar(255)" />
        </createTable>

<!-- TABLE  vok -->
        <createTable tableName="vok">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column defaultValue="" name="name" type="varchar(100)"> <constraints nullable="false" /> </column>
            <column name="vok_category_id" type="bigint" />
        </createTable>

<!-- TABLE  vok_category -->
        <createTable tableName="vok_category">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column defaultValue="" name="name" type="varchar(100)"> <constraints nullable="true" />
            </column>
        </createTable>

<!-- TABLE  massive_request -->
        <createTable tableName="massive_request">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"><constraints primaryKey="true" nullable="false" /></column>
            <column name="created_by" type="varchar(255)"><constraints nullable="false" /></column>
```

```
            <column defaultValueComputed="${now}" name="created_date" type="timestamp"><constraints nullable="false" /></column>
            <column name="last_modified_by" type="varchar(255)" />
            <column name="last_modified_date" type="timestamp" />
            <column name="pdf_path" type="varchar(255)"><constraints nullable="true" /></column>
            <column name="csv_path" type="varchar(255)"><constraints nullable="false" /></column>
            <column name="comment" type="varchar(500)"><constraints nullable="true" /></column>
            <column name="user_id" type="bigint" />
        </createTable>

<!-- TABLE  persistent_audit_event -->
        <createTable tableName="persistent_audit_event">
            <column name="event_id" type="bigint" autoIncrement="${autoIncrement}" > <constraints primaryKey="true" nullable="false" /> </column>
            <column name="principal" type="varchar(255)"> <constraints nullable="false" /> </column>
            <column name="event_date" type="timestamp" />
            <column name="event_type" type="varchar(255)" />
        </createTable>

<!-- TABLE  persistent_audit_evt_data -->
        <createTable tableName="persistent_audit_evt_data">
            <column name="event_id" type="bigint"> <constraints nullable="false" />  </column>
            <column name="value" type="varchar(255)" />
            <column name="name" type="varchar(255)"> <constraints nullable="false" /> </column>
        </createTable>

<!-- TABLE  hr_uploaded_files -->
        <createTable tableName="hr_uploaded_files">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false"/> </column>
            <column name="completed" type="bit" />
            <column name="file" type="blob" > <constraints nullable="false" /> </column>
            <column name="file_content_type" type="varchar(50)"> <constraints nullable="false" /> </column>
            <column name="user_id" type="bigint"> <constraints nullable="false" /> </column>
        </createTable>

<!-- TABLE  persistent_token -->
        <createTable tableName="persistent_token">
            <column name="series" type="varchar(255)"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="ip_address" type="varchar(39)" />
            <column name="token_date" type="timestamp" />
            <column name="token_value" type="varchar(255)"> <constraints nullable="false" /> </column>
            <column name="user_agent" type="varchar(255)" />
            <column name="user_id" type="bigint" />
        </createTable>

<!-- TABLE  ******_user -->
        <createTable tableName="******_user">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" />  </column>
            <column name="created_by" type="varchar(255)"> <constraints nullable="false" /> </column>
            <column defaultValueComputed="${now}" name="created_date" type="timestamp"> <constraints nullable="false" /> </column>
            <column name="gender" type="varchar(255)" />
            <column name="template_css" type="varchar(255)" />
            <column name="template_box" type="bit" />
            <column name="last_modified_by" type="varchar(255)" />
            <column name="last_modified_date" type="timestamp" />
            <column name="account_non_expired" type="bit" />
            <column name="account_non_locked" type="bit" />
            <column name="activation_key" type="varchar(20)" />
            <column name="email" type="varchar(50)" />
            <column name="first_name" type="varchar(50)" />
            <column name="lang_key" type="varchar(5)" />
            <column name="last_name" type="varchar(50)" />
            <column name="user_principal_name" type="varchar(255)"> <constraints nullable="false" /> </column>
            <column name="password" type="varchar(255)"> <constraints nullable="false" /> </column>
            <column name="birthday" type="timestamp" />
            <column name="reset_date" type="timestamp" />
```

```
            <column name="reset_key" type="varchar(20)" />
            <column name="serial_number" type="varchar(20)"> <constraints nullable="false" /> </column>
            <column name="phone" type="varchar(20)" />
        </createTable>

<!-- TABLE  request -->
        <createTable tableName="request">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="version" type="integer" />
            <column name="pdf_path" type="varchar(255)"> <constraints nullable="true" /> </column>
            <column name="applicant_date" type="timestamp" />
            <column name="auditor_comment" type="varchar(500)" />
            <column name="auditor_date" type="timestamp" />
            <column name="director_date" type="timestamp" />
            <column name="owner_comment" type="varchar(500)" />
            <column name="owner_date" type="timestamp" />
            <column name="request_processor_date" type="timestamp" />
            <column defaultValueComputed="${now}" name="submitter_date" type="timestamp"> <constraints nullable="false" /> </column>
            <column name="applicant_state_id" type="bigint" />
            <column name="applicant_user_id" type="bigint" />
            <column name="auditor_state_id" type="bigint" />
            <column name="auditor_user_id" type="bigint" />
            <column name="director_state_id" type="bigint" />
            <column name="director_user_id" type="bigint" />
            <column name="massive_request_id" type="bigint" />
            <column name="owner_state_id" type="bigint" />
            <column name="owner_user_id" type="bigint" />
            <column name="request_processor_state_id" type="bigint" />
            <column name="request_processor_user_id" type="bigint" />
            <column name="submitter_user_id" type="bigint" />
        </createTable>

<!-- TABLE  operational_areas -->
        <createTable tableName="operational_areas">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" />  </column>
            <column name="alias_id" type="bigint" />
            <column name="name" type="varchar(255)" />
        </createTable>

<!-- TABLE  request_application -->
        <createTable tableName="request_application">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="request_id" type="bigint" />
            <column name="application_id" type="bigint" />
            <column name="activated" type="bit" />
        </createTable>

<!-- TABLE  request_application_role -->
        <createTable tableName="request_application_role">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="application_role_id" type="bigint" />
            <column name="request_application_id" type="bigint" />
            <column name="activated" type="bit" />
        </createTable>

<!-- TABLE  role -->
        <createTable tableName="role">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="name" type="varchar(50)"> <constraints nullable="false" /> </column>
            <column name="alias" type="varchar(50)" />
        </createTable>

<!-- TABLE  state -->
        <createTable tableName="state">
```

```
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="name" type="varchar(50)" />
        </createTable>

<!-- TABLE  user_operational_area -->
        <createTable tableName="user_operational_area">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="user_id" type="bigint"> <constraints nullable="false" /> </column>
            <column name="operational_area_id" type="bigint"> <constraints nullable="false" />
            </column>
        </createTable>

<!-- TABLE  user_application -->
        <createTable tableName="user_application">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"> <constraints primaryKey="true" nullable="false" /> </column>
            <column name="user_id" type="bigint"> <constraints nullable="false" />  </column>
            <column name="application_id" type="bigint"> <constraints nullable="false" /> </column>
            <column name="created_by" type="varchar(255)"> <constraints nullable="false" /> </column>
            <column defaultValueComputed="${now}" name="created_date" type="timestamp"> <constraints nullable="false" /> </column>
            <column name="last_modified_by" type="varchar(255)" />
            <column name="last_modified_date" type="timestamp" />
        </createTable>

<!-- TABLE  user_authority -->
        <createTable  tableName="user_authority"> <column  name="id"  type="bigint"  autoIncrement="${autoIncrement}"> <constraints  primaryKey="true"  nullable="false"
/></column>
            <column name="created_by" type="varchar(50)"> <constraints nullable="false" /> </column>
            <column defaultValueComputed="${now}" name="created_date" type="timestamp"> <constraints nullable="false" /> </column>
            <column name="last_modified_by" type="varchar(50)" />
            <column name="last_modified_date" type="timestamp" />
            <column name="activated" type="bit" />
            <column name="version" type="bigint" />
             <column name="role_id" type="bigint"> <constraints nullable="false" /> </column>
            <column name="user_id" type="bigint" />
        </createTable>

<!-- TABLE  user_management -->
         <createTable tableName="user_management">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"><constraints primaryKey="true" nullable="false" /></column>
            <column name="name" type="varchar(255)" />
            <column name="vok_id" type="bigint"><constraints nullable="false" /></column>
            <column name="user_id" type="bigint"><constraints nullable="false" /></column>
        </createTable>

<!-- TABLE  user_workstation -->
        <createTable tableName="user_workstation">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"><constraints primaryKey="true" nullable="false" /></column>
            <column name="name" type="varchar(255)" />
            <column name="office" type="varchar(6)" />
            <column name="floor" type="varchar(4)" />
            <column name="ip_address" type="varchar(39)" />
            <column name="address" type="varchar(255)" />
            <column name="city_id" type="bigint" />
            <column name="post_code" type="varchar(10)" />
            <column name="user_id" type="bigint" />
        </createTable>

<!-- TABLE  city -->
        <createTable tableName="city">
            <column name="id" type="bigint" autoIncrement="${autoIncrement}"><constraints primaryKey="true" nullable="false" /> </column>
            <column name="name" type="varchar(255)" />
        </createTable>

<!-- EXTRA CONTSTAINTS -->
```

```
        <addUniqueConstraint columnNames="serial_number" constraintName="uk_****_user_serial_number" tableName="*****_user" />
        <addUniqueConstraint columnNames="email" constraintName="uk_****_user_email" tableName="*******_user" />
        <addUniqueConstraint columnNames="user_principal_name" constraintName="uk_****_user_user_princ_name" tableName="*****_user" />
        <addUniqueConstraint columnNames="pdf_path" constraintName="uk_request_pdf" tableName="request" />
        <addUniqueConstraint columnNames="pdf_path" constraintName="uk_massive_request_pdf" tableName="massive_request" />

<!-- INDEXES -->
<!-- INDEX idx_persistent_audit_event -->
        <createIndex indexName="idx_persistent_audit_event" tableName="persistent_audit_event" unique="false">
          <column name="principal" type="varchar(255)" />
          <column name="event_date" type="timestamp" />
        </createIndex>

<!-- INDEX idx_city -->
        <createIndex indexName="idx_city" tableName="city"><column name="id" /> <column name="name" /> </createIndex>

<!-- INDEX idx_persistent_audit_evt_data -->
        <createIndex indexName="idx_persistent_audit_evt_data" tableName="persistent_audit_evt_data" unique="false"> <column name="event_id" type="bigint" />
</createIndex>

<!-- INDEX idx_activity_user_user -->
        <createIndex indexName="idx_activity_user_user" tableName="user_activity"><column name="user_id" /> </createIndex>

<!-- INDEX idx_user_authority_ptol_user -->
        <createIndex indexName="idx_user_authority_ptol_user" tableName="user_authority"><column name="user_id" /> </createIndex>

<!-- INDEX idx_user_authority_role -->
        <createIndex indexName="idx_user_authority_role" tableName="user_authority"><column name="role_id" /> </createIndex>

<!-- INDEX idx_operational_areas -->
        <createIndex indexName="idx_operational_areas" tableName="operational_areas"><column name="id" /> </createIndex>

<!-- INDEX idx_cities -->
        <createIndex indexName="idx_cities" tableName="city"> <column name="id" /> </createIndex>

<!-- INDEX idx_user_app_app -->
        <createIndex indexName="idx_user_app_app" tableName="user_application"><column name="application_id" /> </createIndex>

<!-- INDEX idx_user_app_user -->
        <createIndex indexName="idx_user_app_user" tableName="user_application"><column name="user_id" /> </createIndex>

<!-- INDEX idx_applicant_state -->
        <createIndex indexName="idx_applicant_state" tableName="request"> <column name="applicant_state_id" /> </createIndex>

<!-- INDEX idx_applicant_user -->
        <createIndex indexName="idx_applicant_user" tableName="request"> <column name="applicant_user_id" /> </createIndex>

<!-- INDEX idx_app_roles_ptol_user -->
        <createIndex indexName="idx_app_roles_ptol_user" tableName="application_role"><column name="user_id" /> </createIndex>

<!-- INDEX idx_app_roles_app -->
        <createIndex indexName="idx_app_roles_app" tableName="application_role"><column name="application_id" /> </createIndex>

<!-- INDEX idx_auditor_state -->
        <createIndex indexName="idx_auditor_state" tableName="request"><column name="auditor_state_id" /> </createIndex>

<!-- INDEX idx_auditor_user -->
        <createIndex indexName="idx_auditor_user" tableName="request"><column name="auditor_user_id" /> </createIndex>

<!-- INDEX idx_director_state -->
        <createIndex indexName="idx_director_state" tableName="request"><column name="director_state_id" /> </createIndex>

<!-- INDEX idx_director_user -->
        <createIndex indexName="idx_director_user" tableName="request"><column name="director_user_id" />
```

```
        </createIndex>

<!-- INDEX idx_mass_request_user -->
        <createIndex indexName="idx_mass_request_user" tableName="request"> <column name="massive_request_id" /> </createIndex>

<!-- INDEX idx_mass_requests_ptol_user -->
        <createIndex indexName="idx_mass_requests_ptol_user" tableName="massive_request"> <column name="user_id" /> </createIndex>

<!-- INDEX idx_owner_state -->
        <createIndex indexName="idx_owner_state" tableName="request"><column name="owner_state_id" /> </createIndex>

<!-- INDEX idx_owner_user -->
        <createIndex indexName="idx_owner_user" tableName="request"> <column name="owner_user_id" /> </createIndex>

<!-- INDEX idx_pers_token_pers_user -->
        <createIndex indexName="idx_pers_token_pers_user" tableName="persistent_token"> <column name="user_id" /> </createIndex>

<!-- INDEX idx_user_work_ptol -->
        <createIndex indexName="idx_user_work_ptol" tableName="user_workstation"> <column name="user_id" /> </createIndex>

<!-- INDEX idx_request_processor_state -->
        <createIndex indexName="idx_request_processor_state" tableName="request"> <column name="request_processor_state_id" /> </createIndex>

<!-- INDEX idx_request_processor_user -->
        <createIndex indexName="idx_request_processor_user" tableName="request"> <column name="request_processor_user_id" /> </createIndex>

<!-- INDEX idx_submitter_user -->
        <createIndex indexName="idx_submitter_user" tableName="request"> <column name="submitter_user_id" /> </createIndex>

<!-- INDEX idx_user_vok_vok -->
        <createIndex indexName="idx_user_vok_vok" tableName="user_management"><column name="vok_id" /></createIndex>

<!-- INDEX idx_user_management_ptol_user -->
        <createIndex indexName="idx_user_management_ptol_user" tableName="user_management"><column name="user_id" /></createIndex>

<!-- FOREIGN KEYS -->
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="user_operational_area" constraintName="fk_user_op_area_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="operational_area_id" baseTableName="user_operational_area" constraintName="fk_user_op_area_op_areas"
deferrable="false" initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="operational_areas" />
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="hr_uploaded_files" constraintName="fk_hr_files_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="request_id" baseTableName="request_application" constraintName="fk_req_appl_request" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="request" />
        <addForeignKeyConstraint baseColumnNames="application_id" baseTableName="request_application" constraintName="fk_req_appl_appl" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="application" />
        <addForeignKeyConstraint baseColumnNames="application_role_id" baseTableName="request_application_role" constraintName="fk_req_ap_rol_ap_rol"
deferrable="false" initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="application_role" />
        <addForeignKeyConstraint baseColumnNames="request_application_id" baseTableName="request_application_role" constraintName="fk_req_ap_rol_req_ap"
deferrable="false" initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="request_application" />
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="user_activity" constraintName="fk_activity_user_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="user_authority" constraintName="fk_user_authority_ptol_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="role_id" baseTableName="user_authority" constraintName="fk_user_authority_role" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="role" />
        <addForeignKeyConstraint baseColumnNames="city_id" baseTableName="user_workstation" constraintName="fk_city_user_work" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="city" />
        <addForeignKeyConstraint baseColumnNames="vok_category_id" baseTableName="vok" constraintName="fk_vok_vok_cat" deferrable="false" initiallyDeferred="false"
onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="vok_category" />
        <addForeignKeyConstraint baseColumnNames="application_id" baseTableName="user_application" constraintName="fk_user_app_app" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="application" />
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="user_application" constraintName="fk_user_app_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
```

```
        <addForeignKeyConstraint baseColumnNames="applicant_state_id" baseTableName="request" constraintName="fk_applicant_state" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="state" />
        <addForeignKeyConstraint baseColumnNames="applicant_user_id" baseTableName="request" constraintName="fk_applicant_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="application_role" constraintName="fk_app_roles_ptol_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="application_id" baseTableName="application_role" constraintName="fk_app_roles_app" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="application" />
        <addForeignKeyConstraint baseColumnNames="event_id" baseTableName="persistent_audit_evt_data" constraintName="fk_audit_event" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="event_id" referencedTableName="persistent_audit_event" />
        <addForeignKeyConstraint baseColumnNames="auditor_state_id" baseTableName="request" constraintName="fk_auditor_state" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="state" />
        <addForeignKeyConstraint baseColumnNames="auditor_user_id" baseTableName="request" constraintName="fk_auditor_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="director_state_id" baseTableName="request" constraintName="fk_director_state" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="state" />
        <addForeignKeyConstraint baseColumnNames="director_user_id" baseTableName="request" constraintName="fk_director_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="massive_request_id" baseTableName="request" constraintName="fk_mass_request_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="massive_request" />
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="massive_request" constraintName="fk_mass_requests_ptol_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="owner_state_id" baseTableName="request" constraintName="fk_owner_state" deferrable="false" initiallyDeferred="false"
onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="state" />
        <addForeignKeyConstraint baseColumnNames="owner_user_id" baseTableName="request" constraintName="fk_owner_user" deferrable="false" initiallyDeferred="false"
onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="persistent_token" constraintName="fk_pers_token_pers_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="user_workstation" constraintName="fk_user_work_ptol" onDelete="NO ACTION"
onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="request_processor_state_id" baseTableName="request" constraintName="fk_request_processor_state" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="state" />
        <addForeignKeyConstraint baseColumnNames="request_processor_user_id" baseTableName="request" constraintName="fk_request_processor_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="submitter_user_id" baseTableName="request" constraintName="fk_submitter_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="user_id" baseTableName="user_management" constraintName="fk_user_management_ptol_user" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="******_user" />
        <addForeignKeyConstraint baseColumnNames="vok_id" baseTableName="user_management" constraintName="fk_user_vok_vok" deferrable="false"
initiallyDeferred="false" onDelete="NO ACTION" onUpdate="NO ACTION" referencedColumnNames="id" referencedTableName="vok" />

    </changeSet>

    </databaseChangeLog>
```

10.3 Παράρτημα Γ : Περιπτώσεις χρήσης Εφαρμογής Secure Authorization Ticketing

Περιπτώσεις Χρήσης (Use Cases)
Σύνδεση χρήστη στο πληροφοριακό σύστημα
Δημιουργία αιτήματος πρόσβασης
Ιστορικό αιτημάτων (Reports τα αιτήματα μου)
Νέα αιτήματα (που εγκρίνει ο προϊστάμενος) έρχονται με βάση την δήλωση του αιτούντα
Διεκπεραιωμένα αιτήματα προϊσταμένου (Reports)
Νέα αιτήματα (ΑΑΠΑ)
Διεκπεραιωμένα αιτήματα ΑΑΠΑ (Reports)
Νέα αιτήματα ΥΠΑ
Διεκπαιραιωμένα αιτήματα ΥΠΑ (Reports)
Ορισμός ΑΑΠΑ (για κάθε εφαρμογή ΥΠΑ)
Διαχειριστής χρηστών νέα αιτήματα – Υλοποίηση αιτημάτων από το αρμόδιο τμήμα
Διαχειριστής Χρηστών Διεκπεραιωμένα Αιτήματα (report)
mis (στατιστικά)
Διαχείριση Εφαρμογών (Δήλωση Εφαρμογής)
Διαχείριση Ρόλων ανά Εφαρμογή (Ρόλοι των εφαρμογών)
Παρακολούθηση πορείας αιτήματος από χρήστη
Διαχείριση χρηστών (authorization tickets)
Διαχείριση Ρόλων (authorization tickets)
Διεύθυνση Προσωπικού (HR) UPLOAD USERS FOR DELETION
Προφίλ Χρήστη
Ρυθμίσεις περιβάλλοντος
Ψηφιακή υπογραφή αίτησης
LDAP με MS AD
Authorization
Έγκριση/Απόρριψη αιτήματος από τον ιδιοκτήτη

Πίνακας 3 Περιπτώσεις Χρήσης Εφαρμογής (use cases)

10.4 Παράρτημα Δ : Controls ISO/IEC 27001:2013

Ανάλυση μέτρων ανά κατηγορία κατά ISO 27001	
CLAUSE	**TITLE**
5.1	Information security policy
5.1.1	Information security policy document
5.1.2	Review of the information security policy
6.1	Internal organization
6.1.1	Management commitment to information security
6.1.2	Information security co-ordination
6.1.3	Allocation of information security responsibilities
6.1.4	Authorization process for information processing facilities
6.1.5	Confidentiality agreements
6.1.6	Contact with authorities
6.1.7	Contact with special interest groups
6.1.8	Independent review of information security
6.2	External parties
6.2.1	Identification of risks related to external parties
6.2.2	Addressing security when dealing with customers
6.2.3	Addressing security in third party agreements
7.1	Responsibility for assets
7.1.1	Inventory of assets
7.1.2	Ownership of assets
7.1.3	Acceptable use of assets
7.2	Information classification
7.2.1	Classification guidelines
7.2.2	Information labelling and handling
8.1	**Prior to employment**
8.1.1	Roles and responsibilities
8.1.2	Screening
8.1.3	Terms and conditions of employment
8.2	During employment

8.2.1	Management responsibilities
8.2.2	Information security awareness, education and training
8.2.3	Disciplinary process
8,3	Termination or change of employment
8.3.1	Termination responsibilities
8.3.2	Return of assets
8.3.3	Removal of access rights
9.1	Secure areas
9.1.1	Physical security perimeter
9.1.2	Physical entry controls
9.1.3	Securing offices, rooms and facilities
9.1.4	Protecting against external and environmental threats
9.1.5	Working in secure areas
9.1.6	Public access, delivery and loading areas
9.2	**Equipment security**
9.2.1	Equipment siting and protection
9.2.2	Supporting utilities
9.2.3	Cabling security
9.2.4	Equipment maintenance
9.2.5	Security of equipment off-premises
9.2.6	Secure disposal or re-use of equipment
9.2.7	Removal of property
10.1	Operational procedures and responsibilities
10.1.1	Documented operating procedures
10.1.2	Change management
10.1.3	Segregation of duties
10.1.4	Separation of development, test and operational facilities
10.2	Third party service delivery management
10.2.1	Service delivery
10.2.2	Monitoring and review of third party services

10.2.3	Managing changes to third party services
10.3	System planning and acceptance
10.3.1	Capacity management
10.3.2	System acceptance
10.4	Protection against malicious and mobile code
10.4.1	Controls against malicious code
10.4.2	Controls against mobile code
10.5	**Back-up**
10.5.1	Information back-up
10,6	**Network security management**
10.6.1	Network controls
10.6.2	Security of network services
10.7	**Media handling**
10.7.1	Management of removable computer media
10.7.2	Disposal of media
10.7.3	Information handling procedures
10.7.4	Security of system documentation
10,8	**Exchanges of information**
10.8.1	Information exchange policies and procedures
10.8.2	Exchange agreements
10.8.3	Physical media in transit
10.8.4	Electronic messaging
10.8.5	Business information systems
10.9	**Electronic commerce services**
10.9.1	Electronic commerce
10.9.2	On-line transactions
10.9.3	Publicly available systems
10.1	**Monitoring**
10.10.1	Audit logging
10.10.2	Monitoring system use

10.10.3	Protection of log information
10.10.4	Administrator and operator logs
10.10.5	Fault logging
10.10.6	Clock synchronization
11.1	**Business requirement for access control**
11.1.1	Access control policy
11.2	**User access management**
11.2.1	User registration
11.2.2	Privilege management
11.2.3	User password management
11.2.4	Review of user access rights
11.3	**User responsibilities**
11.3.1	Password use
11.3.2	Unattended user equipment
11.3.3	Clear desk and clear screen policy
11.4	**Network access control**
11.4.1	Policy on use of network services
11.4.2	User authentication for external connections
11.4.3	Equipment identification in the network
11.4.4	Remote diagnostic and configuration port protection
11.4.5	Segregation in networks
11.4.6	Network connection control
11.4.7	Network routing control
11.5	**Operating system access control**
11.5.1	Secure log-on procedure
11.5.2	User identification and authentication
11.5.3	Password management system
11.5.4	Use of system utilities
11.5.5	Session time-out

11.5.6	Limitation of connection time
11.6	**Application and information access control**
11.6.1	Information access restriction
11.6.2	Sensitive system isolation
11.7	**Mobile computing and teleworking**
11.7.1	Mobile computing and communications
11.7.2	Teleworking
12,1	**Security requirements of information systems**
12.1.1	Security requirements analysis and specification
12.2	**Correct processing in applications**
12.2.1	Input data validation
12.2.2	Control on internal processing
12.2.3	Message integrity
12.2.4	Output data validation
12.3	**Cryptographic controls**
12.3.1	Policy on the use of cryptographic controls
12.3.2	Key management
12.4	**Security of system files**
12.4.1	Control of operational software
12.4.2	Protection of system test data
12.4.3	Access control to program source code
12.5	**Security in development and support processes**
12.5.1	Change control procedures
12.5.2	Technical review of applications after operating system changes
12.5.3	Restrictions on changes to software packages
12.5.4	Information leakage
12.5.5	Outsourced software development
12.6	**Technical vulnerability management**
12.6.1	Control of technical vulnerabilities
13,1	**Reporting information security events and weaknesses**

13.1.1	Reporting information security events
13.1.2	Reporting security weaknesses
13,2	**Management of information security incidents and improvements**
13.2.1	Responsibilities and procedures
13.2.2	Learning from information security incidents
13.2.3	Collection of evidence
14,1	**Information security aspects of business continuity management**
14.1.1	Including information security in the business continuity management process
14.1.2	Business continuity and risk assessment
14.1.3	Developing and implementing continuity plans including information security
14.1.4	Business continuity planning framework
14.1.5	Testing, maintaining and re-assessing business continuity plans
15.1	**Compliance with legal requirements**
15.1.1	Identification of applicable legislation
15.1.2	Intellectual property rights (IPR)
15.1.3	Protection of organizational records
15.1.4	Data protection and privacy of personal information
15.1.5	Prevention of misuse of information processing facilities
15.1.6	Regulation of cryptographic controls
15.2	**Compliance with security policies and standards and technical compliance**
15.2.1	Compliance with security policy and standards
15.2.2	Technical compliance checking
15.3	**Information systems audit considerations**
15.3.1	Information systems audit controls
15.3.2	Protection of information systems audit tools

10.5 Παράρτημα Ε : Initial Risk Assessment (Ανάλυση Επικινδυνότητας)

10.5.1 Εισαγωγή

Με την παρούσα Ανάλυση Επικινδυνότητας της Εφαρμογής υλοποιείται η αρχική μελέτη κατά το στάδιο του σχεδιασμού της αρχιτεκτονικής πριν από την επιλογή των τεχνολογιών που θα χρησιμοποιηθούν για την υλοποίηση. Για λόγους συντομίας από εδώ και πέρα η Επιχείρηση <ΟΝΟΜΑΣΙΑ ΕΠΙΧΕΙΡΗΣΗΣ> θα αναφέρεται ως «**Επιχείρηση**» και η Εφαρμογή SAT θα ονομάζεται «**Πληροφοριακό Σύστημα**».

Το πληροφοριακό σύστημα θα εκτείνεται σε όλο το εύρος του οργανισμού. Οι χρήστες του θα έχουν κατάλληλους ρόλους που θα διαχωρίζουν τις εργασίες τους και θα έχουν την δυνατότητα να κάνουν:

Είσοδο, Έξοδο, δημιουργία αιτήματος, αποδοχή αιτήματος, έγκριση αιτημάτων, απόρριψη αιτημάτων, αίτηση απομάκρυνσης ή μετακίνησης (μαζικά αιτήματα), MIS, Διαχείρισης ρόλων εφαρμογών, Διαχείριση χρηστών εφαρμογών, Διαχείριση ρόλων και χρηστών του Πληροφοριακού Συστήματος, παρακολούθηση στατιστικών, αυτόματες διεργασίες με SAP & AD, auditing, χρήση ψηφιακής υπογραφής.

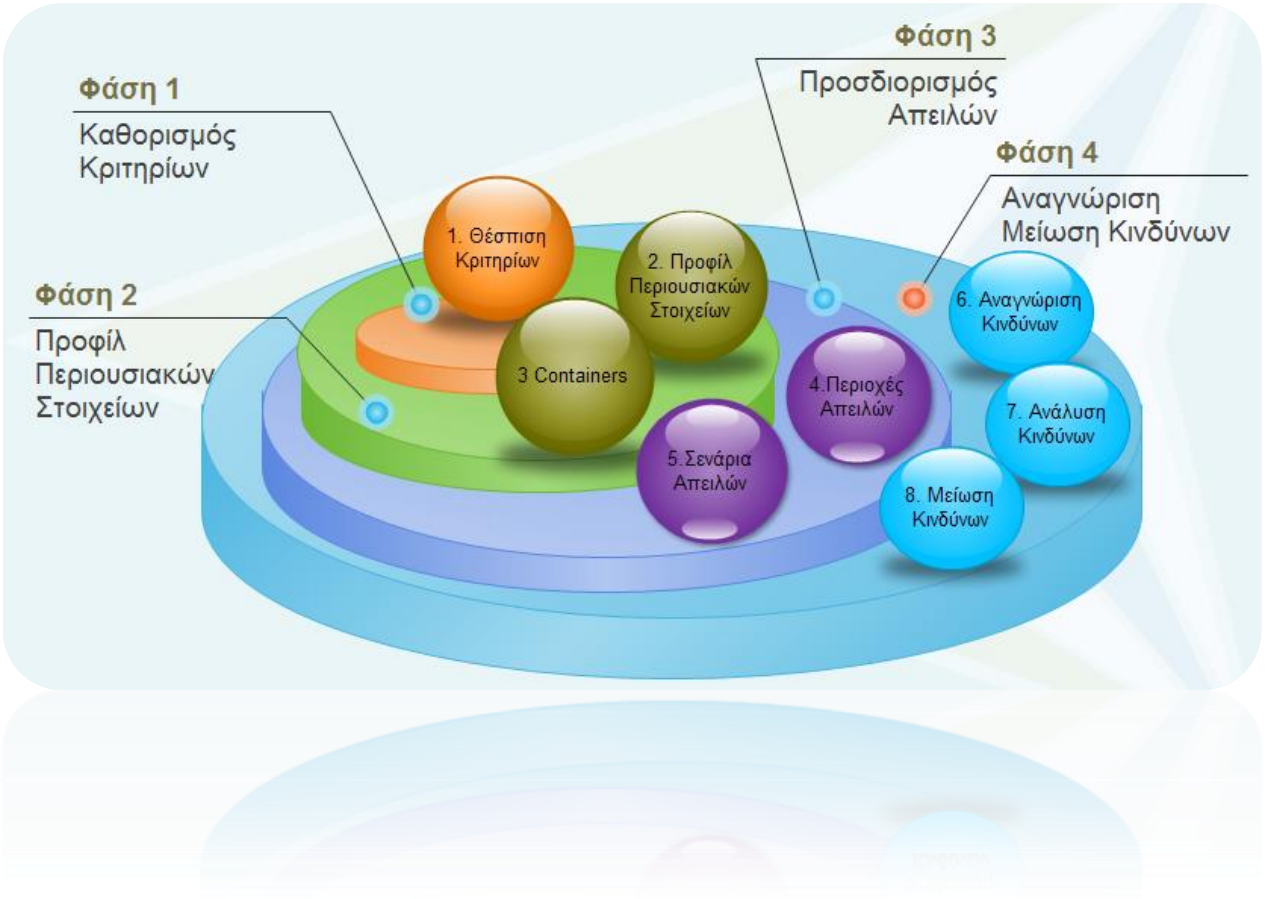
Η πιθανότητα του να συμβεί ένα περιστατικό ασφάλειας επί το οικονομικό κόστος το οποίο θα επωμιστεί η Επιχείρηση αφορά την Επικινδυνότητα. Ο σκοπός που υλοποιείται η τρέχουσα αναφορά είναι η υλοποίηση του παραπάνω προγραφομένου ασφαλούς Πληροφοριακού Συστήματος. Η αναφορά θα εξεταστεί από τον ιδιοκτήτη του Πληροφοριακού Συστήματος. Το τμήμα Ασφάλειας της Επιχείρησης και ο Ιδιοκτήτης θα λάβουν τις κατάλληλες δικλείδες Ασφαλείας έτσι ώστε να μειωθεί ο υπάρχον κίνδυνος που θα εμφανίζει η αναφορά και να μείνει ο εναπομείναντας κίνδυνος στα αποδεκτά όρια ρίσκου. Η μεθοδολογία που θα ακολουθηθεί θα είναι η Octave Allegro.

10.5.2 Η μέθοδος Octave Allegro

Ο σχεδιασμός της μεθόδου παρέχει την δυνατότητα ευρείας αξιολόγησης του λειτουργικού κινδύνου που υπάρχει σε ένα εταιρικό περιβάλλον. Επιτρέπει χωρίς την αναγκαιότητα εκτεταμένης γνώσης εκτίμησης κινδύνων να δίνονται ισχυρά αποτελέσματα. Η πληροφορία αφορά ιδιοκτησία της Επιχείρησης. Για κάθε περιουσιακό στοιχείο που συμβάλει στην δημιουργία της, την επεξεργασίας της, την μετάδοσή της και

την αποθήκευσή της υπάρχουν ευπάθειες και τρωτά σημεία αλλά και απειλές που τις εκμεταλλεύονται. Η μέθοδος αναλύει όλα τα παραπάνω.

Αποτελείται από τέσσερις φάσεις που αναπτύσσονται σε οκτώ βήματα (εικόνα 1). Στην πρώτη φάση αναπτύσσονται μέσω των διαδικασιών της εταιρείας τα κριτήρια μέτρησης των κινδύνων. Στην δεύτερη φάση υλοποιούνται τα προφίλ των assets και των containers που τα περιέχουν. Επιπλέον σε αυτή την φάση καθορίζονται τα όρια των asset. Στην Τρίτη φάση προσδιορίζονται οι απειλές για κάθε περιουσιακό στοιχείο (asset). Στην τέταρτη φάση καταγράφονται και αναλύονται οι κίνδυνοι για κάθε περιουσιακό στοιχείο (asset). Επιπλέον σε αυτή την φάση υλοποιείται ο μετριασμός του κινδύνου.



Εικόνα 64 Φάσεις και Βήματα της Μεθοδολογίας Octave Allegro

10.5.3 Περιγραφή και ανάλυση των οκτώ (8) βημάτων της μεθοδολογίας Octave Allegro

10.5.3.1 Θέσπιση Κριτηρίων Μέτρησης Κινδύνου - Establish Risk Measurement Criteria (Βήμα 1)

Σε αυτό το βήμα καθορίζονται τα κριτήρια με την χρήση των οποίων θα γίνει η αξιολόγηση των επιπτώσεων κινδύνου. Εδώ η Επιχείρηση κατηγοριοποιεί την σημαντικότητα των επιπτώσεων σε σχέση με του επιχειρησιακούς στόχους (business objectives). Η μέθοδος έχει επτά (7) φύλλα εργασίας.

10.5.3.2 Ανάπτυξη προφίλ Πληροφοριακών Περιουσιακών Στοιχείων - Develop an Information Asset Profile (Βήμα 2)

Εδώ δημιουργείται το προφίλ για τα πληροφοριακά περιουσιακά στοιχεία της Επιχείρησης και γίνεται η παράσταση των πληροφοριών σε σχέση με το κάθε περιουσιακό στοιχείο (μοναδικά χαρακτηριστικά, όρια, απαιτήσεις ασφάλειας κτλ.). Είναι η βάση για τις απειλές και τους κινδύνους που αναλύονται στην συνέχεια.

10.5.3.3 Ορισμός των container περιουσιακών Στοιχείων - Identify Information Asset Container (Βήμα 3)

Εδώ αναλύονται τα μέρη αποθήκευσης, μεταφοράς και επεξεργασίας των πληροφοριών των περιουσιακών στοιχείων. Τα όρια που βρίσκονται τα container είναι εντός της Επιχείρησης (σε μερικές περιπτώσεις υπάρχει και όριο εκτός της Επιχείρησης – cloud).

10.5.3.4 Θέσπιση Κριτηρίων Μέτρησης Κινδύνου - Establish Risk Measurement Criteria (Βήμα 4)

Εδώ εντοπίζονται οι κινδύνοι που μπορεί να απειλήσουν ένα περιουσιακό στοιχείο. Σημαντικό ρόλο παίζει η πιθανότητα εμφάνισης μίας απειλής – κινδύνου κάτω από κάποιες συνθήκες και καταστάσεις όσον αφορά το περιουσιακό στοιχείο.

10.5.3.5 Θέσπιση Κριτηρίων Μέτρησης Κινδύνου - Establish Risk Measurement Criteria (Βήμα 5)

Αφορά συνέχεια του τέταρτου βήματος και εμφανίζει την επέκταση σε πιθανά σενάρια απειλών. Επιπρόσθετα εξετάζονται και οι απειλές που μπορεί να υπάρχουν αλλά αφορούν ένα ευρύτερο φάσμα.

10.5.3.6 Θέσπιση Κριτηρίων Μέτρησης Κινδύνου - Establish Risk Measurement Criteria (Βήμα 6)

Εδώ αναφέρονται οι συνέπειες που θα υπάρχουν στην Επιχείρηση κατά την πιθανότητα εμφάνισης κάποιας από τις παραπάνω απειλές (φήμη, οικονομική απώλεια κλπ) . Με βάση την ακόλουθη σχέση γίνεται ο υπολογισμός του κινδύνου.

10.5.3.7 Θέσπιση Κριτηρίων Μέτρησης Κινδύνου - Establish Risk Measurement Criteria (Βήμα 7)

Εδώ υπολογίζεται ποσοτικά η επήρεια που έχει η απειλή στην Επιχείρηση. Ο βαθμός κινδύνου σε σχέση με την πιθανότητα που υπάρχει για την εμφάνισή του συνδυάζονται με την κατηγορία κρισιμότητας των τομέων που επηρεάζει και του εύρους των συνεπειών προς την Επιχείρηση που θέτουν πρόβλημα επιχειρησιακής συνέχειας. Ιεραρχούνται οι επιπτώσεις και ταξινομούνται οι κίνδυνοι με βάση τις Επιχειρησιακές ανάγκες (business objectives).

Για να υπολογιστεί ο κίνδυνος συμμετέχουν η προτεραιότητα και ο βαθμός επίπτωσης στην κάθε περιοχή επίπτωσης. Ο βαθμός επίπτωσης είναι Υψηλός (3), Μεσαίος (2) και Χαμηλός (1). Πολλαπλασιάζεται η προτεραιότητα με τον βαθμό επίπτωσης και βγαίνει ο βαθμός κινδύνου ανά περιοχή επίπτωσης. Ο συνολικός βαθμός κινδύνου προκύπτει από την άθροιση των βαθμών κινδύνου των επιμέρους περιοχών επίπτωσης.

Βαθμός Επίπτωσης	
Υψηλός	3
Μέτριος	2
Χαμηλός	1

10.5.3.8 Θέσπιση Κριτηρίων Μέτρησης Κινδύνου - Establish Risk Measurement Criteria (Βήμα 8)

Στο βήμα αυτό το οποίο είναι και το τελευταίο , η εταιρεία απαιτεί τον μετριασμό για την επικινδυνότητα που έχει εντοπιστεί (βαθμός κινδύνων ανά περιοχή επίπτωσης) μέσω στρατηγικής αντιμετώπισης.

Residual Risk = Inheritance Risk + Controls

Στον **Πίνακα** που ακολουθεί εμφανίζονται τέσσερις (4) ομάδες επικινδυνότητας με βάση την προσέγγιση που αφορά τον μετριασμό, την αποτροπή ή την Αποδοχή του Κινδύνου.

Ανάλογα με την ομάδα που μία απειλή ανήκει καθορίζεται η Προσέγγιση και ο τρόπος που αντιμετωπίζεται.

Ομάδα Επικινδυνότητας	Προσέγγιση (Αποτροπή, Μετριασμός, Αποδοχή)
Ομάδα 1	Αποτροπή
Ομάδα 2	Αποτροπή/Μετριασμός
Ομάδα 3	Μετριασμός/Αποδοχή
Ομάδα 4	Αποδοχή

Πίνακας 4 Προσέγγιση Μετριασμός, Αποτροπή, Αποδοχής Κινδύνου

Στον πίνακα που ακολουθεί οργανώνονται σε κατηγορίες οι απειλές. Οι απειλές εμφανίζονται με βάση την συνολική βαθμολογία τους και την πιθανότητα να συμβούν. Οι απειλές κατατάσσονται στις ομάδες επικινδυνότητας του πίνακα 2.

ΑΠΕΙΛΕΣ			
	Βαθμολογία		
Πιθανότητα	**0-20**	**21-29**	**30-44**
Υψηλή	**Ομάδα 3** (Μετριασμός/Αποδοχή)	**Ομάδα 2** (Αποτροπή/Μετριασμός)	**Ομάδα 1** (Αποτροπή)
Μεσαία	**Ομάδα 4** (Αποδοχή)	**Ομάδα 3** (Μετριασμός/Αποδοχή)	**Ομάδα 2** (Αποτροπή/Μετριασμός)
Χαμηλή	**Ομάδα 4** (Αποδοχή)	**Ομάδα 4** (Αποδοχή)	**Ομάδα 3** (Μετριασμός/Αποδοχή)

Για τους κινδύνους που υπάρχει αποδοχή είναι πολύ σημαντικό να πραγματοποιείται επιπλέον έλεγχος για τις επιπτώσεις στην εταιρεία.

10.5.3.9 Εφαρμογή της Μεθόδου OCTAVE Allegro

Αρχικά κρίνεται σοβαρό και αναγκαίο να προσδιοριστεί το κρίσιμο περιουσιακό αγαθό. Αυτό προκύπτει από συνεντεύξεις με ερωτηματολόγια προς το προσωπικό της εταιρείας. Η επιλογή της αυτοματοποιημένης και κεντρικής διαχείρισης των ψηφιακά υπογεγραμμένων αιτημάτων πρόσβασης σε πληροφοριακά συστήματα και υπηρεσίες της εταιρείας έγινε γιατί αφορά κρίσιμη υπηρεσία για την Επιχείρηση καθώς διαθέτει πάνω από 100000 χρήστες εφαρμογών και ελέγχεται από auditors για την ορθότητα των πληροφοριακών της υπηρεσιών. Μία δικλείδα αφορά την διαφύλαξη της εμπιστευτικότητας και της ακεραιότητας της πληροφορίας. Αυτή διαφυλάσσεται με τις αρχές των ελαχίστων προνομίων (authorization) και του ελαχίστου της γνώσης (least to know – role based applications). Επίσης αναγκαία είναι η διαφύλαξη της αρχής μη αποποίησης που γίνεται με τις ψηφιακές υπογραφές. Πλέον η δικλείδα για την διαφύλαξη της ακεραιότητας και της εμπιστευτικότητας με την χρήση της κρυπτογραφίας και auditing είναι αναγκαία. Καθώς ο όγκος των δεδομένων είναι τεράστιος οδηγούμαστε στην αυτοματοποίηση των διεργασιών και την κεντρική διαχείριση. Αποτελεί υπηρεσία που χρησιμοποιείται από όλο το προσωπικό της εταιρείας.. Καθώς θα εφαρμοστεί η ανάλυση επικινδυνότητας πρίν τον σχεδιασμό του συστήματος θα ελεγχθούν με βάση το ISO/IEC 27001 και θεματικές που έχουν σχέση με την Διοίκηση της Ασφάλειας Πληροφοριακού Συστήματος.

10.5.4 Κρίσιμο Περιουσιακό Στοιχείο – Υπηρεσία Αυτοματοποίησης και Ψηφιακής Υπογραφής Εγκρίσεων Αιτημάτων Πρόσβασης Σε Εφαρμογές.

10.5.5 Καθορισμός Κριτηρίων Μέτρησης Κινδύνου

10.5.5.1 AllegroWorksheet 1	**Κριτήρια μέτρησης κινδύνου** **Φήμη / εμπιστοσύνη**		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Φήμη ***(Προσωπικό)***	Αφορά χαμηλή επήρεια στην φήμη της Επιχείρησης (μικρή ή καθόλου προσπάθεια ή δαπάνη για την αποκατάστασή της).	Αφορά μέτρια επήρεια στην φήμη της Επιχείρησης (απαιτείται μικρή προσπάθεια ή δαπάνη για να αποκατασταθεί).	Αφορά υψηλή επήρεια στην φήμη της Επιχείρησης (απαιτείται μεγάλη προσπάθεια ή δαπάνη για να αποκατασταθεί)
Φήμη ***(Προμηθευτές)***	Αφορά χαμηλή επήρεια στην φήμη της Επιχείρησης (μικρή ή καθόλου προσπάθεια ή δαπάνη για την αποκατάστασή της	Αφορά μέτρια επήρεια στην φήμη της Επιχείρησης (απαιτείται μικρή προσπάθεια ή δαπάνη για να αποκατασταθεί).	Αφορά υψηλή επήρεια στην φήμη της Επιχείρησης (απαιτείται μεγάλη προσπάθεια – με δαπάνη πάνω από 50.000€ για να αποκατασταθεί)
Φήμη ***(Εξωτερικοί Συνεργάτες)***	Αφορά χαμηλή επήρεια στην φήμη της Επιχείρησης (μικρή ή καθόλου προσπάθεια ή δαπάνη για την αποκατάστασή της	Αφορά μέτρια επήρεια στην φήμη της Επιχείρησης (απαιτείται μικρή προσπάθεια ή δαπάνη για να αποκατασταθεί	Αφορά υψηλή επήρεια στην φήμη της Επιχείρησης (απαιτείται μεγάλη προσπάθεια – με δαπάνη πάνω από 50.000€ για να αποκατασταθεί)
Φήμη ***(Πελάτες – Ευρύ κοινό)***	Αφορά χαμηλή επήρεια στην φήμη της Επιχείρησης (μικρή ή καθόλου προσπάθεια ή δαπάνη για την αποκατάστασή της	Αφορά χαμηλή επήρεια στην φήμη της Επιχείρησης (απαιτείται πολύ μεγάλη προσπάθεια ή δαπάνη με κόστος που υπερβαίνει το ποσό των 100.000 € για να αποκατασταθεί).	Αφορά καταστροφή της φήμης της Επιχείρησης (η αποκατάσταση υπερβαίνει το ποσό του 1.000.000 €)

10.5.6 Allegro Worksheet 2	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ** **ΠΡΟΣΤΙΜΑ ΚΑΙ ΑΓΩΓΕΣ**		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**

Πρόστιμα - Αγωγές	Επιβολή προστίμων – αγωγών μικρότερη από 5.000€.	Επιβολή προστίμων – αγωγών μεταξύ 5.000€ και 50.000€ .	Επιβολή προστίμων – αγωγών > από 50.000€.

10.5.6.1 ***Allegro Worksheet 3***	**ΚΡΙΤΗΡΙΑ ΜΈΤΡΗΣΗΣ ΚΙΝΔΎΝΟΥ ΟΙΚΟΝΟΜΙΚΆ**		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Λειτουργικά Έξοδα	Αύξηση μικρότερη του 5% σε ετήσιες λειτουργικές δαπάνες	Αύξηση μεταξύ 5% και 10% σε ετήσιες λειτουργικές δαπάνες.	Αύξηση περισσότερο από 10% σε ετήσιες λειτουργικές δαπάνες.
Απώλεια Εσόδων	Ετήσια οικονομική απώλεια μικρότερη των 1.000.000 €.	Ετήσια οικονομική απώλεια 1.000.000€ - 5.000.000€	Ετήσια οικονομική απώλεια μεγαλύτερη από 5.000.000€

10.5.6.2 ***Allegro Worksheet 4***	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΥΓΕΙΑ**		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ασφάλειας και υγείας	Δεν υπάρχουν επιπτώσεις		

10.5.6.3 Allegro Worksheet 5	**ΚΡΙΤΗΡΙΑ ΜΈΤΡΗΣΗΣ ΚΙΝΔΎΝΟΥ ΠΑΡΑΓΩΓΙΚΌΤΗΤΑ**		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ώρες Εργασίας Προσωπικού	Οι ώρες εργασίας του προσωπικού δεν αυξάνονται περισσότερο από 5%.	Οι ώρες εργασίας του προσωπικού αυξάνονται μεταξύ 5% και 20%.	Οι ώρες εργασίας του προσωπικού αυξάνονται περισσότερο από 20%.
Ώρες Εργασίας Εξειδικευμένου Προσωπικού (Τεχνικοί, Προγραμματιστές, Προνομιούχοι Χρήστες)	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται ελάχιστα όχι περισσότερο από 1%.	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται μεταξύ 10% και 15%	Οι ώρες εργασίας του εξειδικευμένου προσωπικού αυξάνονται περισσότερο από 15%
Ώρες Εργασίας Ανώτερων Στελεχών	Οι ώρες εργασίας των ανωτέρων	Οι ώρες εργασίας των ανωτέρων	Οι ώρες εργασίας των ανωτέρων στελεχών

	στελεχών δεν αυξάνονται περισσότερο από 1%	στελεχών αυξάνονται μεταξύ 1% και 10%	αυξάνονται περισσότερο από 10%.

10.5.6.4 Allegro Worksheet 6	**ΚΡΙΤΗΡΙΑ ΜΕΤΡΗΣΗΣ ΚΙΝΔΥΝΟΥ ΟΡΙΖΟΝΤΑΙ ΑΠΟ ΤΟΝ ΧΡΗΣΤΗ**		
Περιοχή Επίπτωσης	**Χαμηλή**	**Μέτρια**	**Υψηλή**
Ορίζονται από τον χρήστη	Δεν υπάρχουν επιπτώσεις		

10.5.6.5 Allegro Worksheet 7	**ΠΡΟΤΕΡΑΙΟΠΟΊΗΣΗ ΤΩΝ ΠΕΡΙΟΧΏΝ ΕΠΙΠΤΩΣΕΩΝ**
Προτεραιότητα	**Περιοχές επιπτώσεων**
3	**ΦΗΜΗ / ΕΜΠΙΣΤΟΣΎΝΗ ΠΕΛΑΤΩΝ**
1	**ΠΡΌΣΤΙΜΑ ΚΑΙ ΑΓΩΓΈΣ**
4	**ΟΙΚΟΝΟΜΙΚΆ**
-	**ΥΓΕΊΑ ΚΑΙ ΑΣΦΆΛΕΙΑ**
2	**ΠΑΡΑΓΩΓΙΚΌΤΗΤΑ**
-	**ΟΡΊΖΕΤΑΙ ΑΠΌ ΤΟΝ ΧΡΉΣΤΗ**

1 **χαμηλός βαθμός επίπτωσης**
4 **μέγιστος βαθμός επίπτωσης**

10.5.7 Ανάπτυξη του Προφίλ των Περιουσιακών Στοιχείων

10.5.7.1 Allegro Worksheet 8	**ΠΡΟΦΊΛ ΚΡΊΣΙΜΟΥ ΠΕΡΙΟΥΣΙΑΚΟΎ ΣΤΟΙΧΕΊΟΥ**	
(1) Κρίσιμο Περιουσιακό Στοιχείο	**(2) Αιτιολογία Επιλογής**	**(3) Περιγραφή - Σκοπός**

Υποδομή Πληροφοριακού Συστήματος «Secure Authorization Ticketing»	Η υποδομή του Πληροφοριακού Συστήματος περιέχει τα Συστήματα και τις υποδομές που είναι αναγκαίες για να καλύψουν τον όγκο για πάνω από δέκα χιλιάδες χρήστες, πάνω από διακόσια Πληροφοριακά Συστήματα και πάνω από 100.000 χρήστες εφαρμογών. Καθώς αφορά Ανάλυση επικινδυνότητας πριν την υλοποίηση του ΠΣ η υποδομή αναφέρεται σε ιδεατό επίπεδο.	Περιλαμβάνει: - Προσωπικά Δεδομένα Χρηστών - Ευαίσθητα Εταιρικά Δεδομένα o Πληροφορία για όλες τις εφαρμογές της επιχείρησης o Πληροφορία για όλους τους ρόλους των εφαρμογών και των πληροφοριακών υπηρεσιών της Επιχείρησης. o Στοιχεία Προσωπικού - Αιτήματα πρόσβασης σε εφαρμογές - Ψηφιακές Υπογραφές - Περιλαμβάνουν εκκρεμεί αιτήματα.
(4)Ιδιοκτήτης/ες		
Διοίκηση της Επιχείρησης		
(5) Απαιτήσεις Ασφάλειας		
✓ **Εμπιστευτικότητα**	Μόνο το εξουσιοδοτημένο προσωπικό μπορεί να δει αυτές τις πληροφορίες.	
✓ **Ακεραιότητα**	Κανείς δεν μπορεί να τροποποιήσει αυτές τις πληροφορίες πέραν του εξουσιοδοτημένου προσωπικού και των εξουσιοδοτημένων διαδικασιών.	
✓ **Διαθεσιμότητα**	Αυτό το περιουσιακό στοιχείο πρέπει να είναι διαθέσιμο για το προσωπικό για την διεκπεραίωση των εργασιών τους, όπως: για παράδειγμα αιτήματα πρόσβασης και παρακολούθηση ιστορικότητας του τι έχουν αιτηθεί.	
✓ **Άλλο**	Αυτό το αγαθό διαφυλάσσει το κανονιστικό πλαίσιο της Επιχείρησης και τις αρχές μη αποποίησης.	
(6) Σημαντικότερες Απαιτήσεις Ασφάλειας		
✓ **Εμπιστευτικότητα**	✓ **Ακεραιότητα**	✓ **Διαθεσιμότητα** ✓ **Άλλο**

10.5.8 Προσδιορισμός "Container" Περιουσιακών Στοιχείων

Υποδομή Πληροφοριακού Συστήματος

10.5.8.1 Allegro Worksheet 9a	**ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΤΕΧΝΙΚΑ)**
ΕΣΩΤΕΡΙΚΑ	

ΠΕΡΙΓΡΑΦΗ "CONTAINER"	ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ
Σύστημα Web Logic Host	Πληροφοριακές Υποδομές
Network Connections	Πληροφοριακές Υποδομές
Database Host	Πληροφοριακές Υποδομές
Web Logic Security Service	Πληροφοριακές Υποδομές
Application	Πληροφοριακές Υποδομές
ΕΞΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**

10.5.8.2 Allegro Worksheet 9b	**ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΦΥΣΙΚΑ)**
ΕΣΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
Δεν υπάρχει σχετική υποδομή	Πληροφοριακές Υποδομές
ΕΞΩΤΕΡΙΚΑ	
ΠΕΡΙΓΡΑΦΗ "CONTAINER"	**ΙΔΙΟΚΤΗΤΗΣ/ΤΕΣ**
	-

10.5.8.3 Allegro Worksheet 9c	**ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΑΝΘΡΩΠΙΝΟ ΔΥΝΑΜΙΚΟ)**
ΕΣΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΟΝΟΜΑ/ΡΟΛΟΙ/ΑΡΜΟΔΙΟΤΗΤΕΣ	**ΤΜΗΜΑ / ΤΟΜΕΑΣ**
Προνομιακοί Χρήστες Υποδομών	ΕΠΙΧΕΊΡΗΣΗ
Προνομιακοί Χρήστες Διαχείρισης Εφαρμογής	ΕΠΙΧΕΊΡΗΣΗ
Επιχειρησιακοί Χρήστες	ΕΠΙΧΕΊΡΗΣΗ
Διαχειριστές Δικτύων	ΕΠΙΧΕΊΡΗΣΗ
ΕΞΩΤΕΡΙΚΟ ΠΡΟΣΩΠΙΚΟ	
ΠΡΟΜΗΘΕΥΤΕΣ, ΕΞΩΤΕΡΙΚΟΙ ΣΥΝΕΡΓΑΤΕΣ ΚΤΛ	**ΟΡΓΑΝΙΣΜΟΣ**

10.5.9 Προσδιορισμός των Συνθηκών που λαμβάνονται υπόψη / Σεναρίων Απειλής και Αναγνώριση Κινδύνων

10.5.10 1ο Σενάριο (Information Security Policies)

<table>
<tr><td colspan="3">10.5.10.1 Allegro - Worksheet 10</td><td colspan="4">ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ</td></tr>
<tr><td></td><td></td><td>Περιουσιακό Στοιχείο</td><td colspan="4">Υποδομή του Πληροφοριακού Αγαθού της Επιχείρησης & περιβάλλον που θα φιλοξενηθεί</td></tr>
<tr><td rowspan="10">Κίνδυνοι Περιουσιακών Στοιχείων</td><td></td><td>Τομείς Ενδιαφέροντος</td><td colspan="4">Πολιτικών Ασφαλείας ΠΣ</td></tr>
<tr><td rowspan="8">Απειλή</td><td>(1) Δράστης (Actor)</td><td colspan="4">Αφορά εσωτερικούς ή εξωτερικούς χρήστες που υλοποιούν κακόβουλη ενέργεια είτε από πρόθεση είτε από άγνοια και επικαλούνται έλλειψη πολιτικών ασφάλειας.</td></tr>
<tr><td>(2) Μέσα (Means)</td><td colspan="4">Ο Δράστης θα χρησιμοποιήσει οποιοδήποτε asset της πληροφοριακής υποδομής και θα εκμεταλλευτεί οποιαδήποτε αδυναμία υπάρχει.</td></tr>
<tr><td>(3) Κίνητρο (Motive)</td><td colspan="4">Το κίνητρο του Δράστη θα είναι η αποκόμιση οφέλους μέσω της διαταραχής της φήμης της Επιχείρησης, μέσω έκθεση της σε οικονομικό επίπεδο, μέσω εμπλοκής της σε νομικά θέματα, μέσω έκθεσής της σε πρόστιμα και μηνύσεις και μέσω μείωσης της παραγωγικότητας.</td></tr>
<tr><td>(4) Αποτέλεσμα (Outcome)</td><td colspan="4">✓ Αποκάλυψη
✓ Τροποποίηση
✓ Διακοπή
✓ Καταστροφή</td></tr>
<tr><td>(5) Απαιτήσεις Ασφάλειας
(Security Requirements)</td><td colspan="4">Οι απαιτήσεις ασφαλείας θα διαταραχτούν λόγω της μη συμμόρφωσης με το εταιρικό πλαίσιο ασφάλειας και την εταιρική πολιτική, των δικαιωμάτων πρόσβασης, την απώλεια της προστασίας της Ακεραιότητας, της εμπιστευτικότητας, της μη αποποίησης και της διαθεσιμότητας. Ειδικά για τους τεχνικούς προνομιακούς χρήστες διαταράσσονται οι έννοιες τις ανάκαμψης από καταστροφή, της επιχειρησιακής συνέχειας, των αντιγράφων ασφαλείας, της κρυπτογραφίας.</td></tr>
<tr><td>(6) Πιθανότητα (Probability)</td><td>❑ Υψηλή</td><td>✓ Μεσαία</td><td>❑ Χαμηλή</td><td></td></tr>
<tr><td colspan="2" rowspan="2">(7) Επιπτώσεις
(Consequences)</td><td colspan="4">(8) Σημαντικότητα/ Σπουδαιότητα (Severity)</td></tr>
<tr><td>Περιοχή Επίπτωσης</td><td>Βαθμός Κινδύνου (Value)</td><td>Βαθμός Αποτίμησης (Score)</td></tr>
</table>

	Διαρροή, Τροποποίηση, απώλεια της διαθεσιμότητας, απώλεια της επιχειρησιακής συνέχειας, πλαστοπροσωπία απώλεια της αρχής μη αποποίησης.	Φήμη – Εμπιστοσύνη Πελατών	Υψηλός	9
		Οικονομικά	Μικρή	4
		Παραγωγικότητα	Υψηλός	6
		Ασφάλεια & Υγεία	-	0
		Πρόστιμα & Αγωγές	Μέτριος	2
		Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου				**21**
(9) Αντιμετώπιση Κινδύνου				
❑ Αποδοχή		❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:				
Επιχειρησιακό Περιβάλλον που θα υποστηρίξει το Πληροφοριακό Σύστημα		• Επικαιροποίηση του πλαισίου Ασφάλειας Πληροφοριακών Συστημάτων της Επιχείρησης και του προτύπου που χρησιμοποιείται. Προτείνεται το ISO/IEC 27001:2013 • Επικαιροποίηση των πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων με βάση το τελευταίο πρότυπο που αναφέρεται παραπάνω. • Επιθεώρηση Εγγράφων από αρχή πιστοποίησης με βάση το πρότυπο ISO 27001:2013.		
Εσωτερικό Δίκτυο		• Δεν είναι απαραίτητη κάποια επιπλέον ενέργεια.		

10.5.11 2ο Σενάριο (Organization of Information Security)

10.5.11.1 Allegro - Worksheet 10			**ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ**
		Περιουσιακό Στοιχείο	**Υποδομή του Πληροφοριακού Αγαθού της Επιχείρησης**
Κίνδυνο	**Απειλή**	Τομείς Ενδιαφέροντος	***Έλλειψη μελέτης Ασφάλειας Πληροφοριακών Συστημάτων (Ανάλυση Επικινδυνότητας, Σχέδιο Ανάκαμψης από Καταστροφή, Επιχειρησιακή Συνέχεια)***

	(1) Δράστης (Actor)	Εσωτερικοί ή εξωτερικοί χρήστες που υλοποιούν κακόβουλη ενέργεια είτε από πρόθεση είτε από άγνοια εκμεταλλευόμενοι ευπάθειες που δεν έχουν αναλυθεί και αντιμετωπιστεί.		
	(2) Μέσα (Means)	Οποιαδήποτε αδυναμία την οποία μπορεί να εκμεταλλευτεί κίνδυνος που αφορά φυσική ή τεχνική πηγή. Δεν γίνεται ανάλυση κινδύνων πριν από την ανάπτυξη/υλοποίηση νέων Πληροφοριακών Συστημάτων		
	(3) Κίνητρο (Motive)	Αποκόμιση οφέλους διαταραχής φήμης, οικονομικής απώλειας, νομικής επίπτωσης – προστίμων μηνύσεων και μείωση παραγωγικότητας.		
	(4) Αποτέλεσμα (Outcome)	✓ Αποκάλυψη ✓ Τροποποίηση	✓ Διακοπή ✓ Καταστροφή	
	(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Πιθανά οργανωτικά και επιχειρηματικά ζητήματα μπορούν να οδηγήσουν σε αυξημένη επικινδυνότητα. Χρειάζεται να γίνει αξιολόγηση των αναγκών ασφάλειας και να γίνει ανάλυση επικινδυνότητας των κινδύνων στο πλαίσιο της επιχείρησής. Λαμβάνοντας υπόψη τις ποικιλίες και τους περιορισμούς των σημερινών μεθόδων αξιολόγησης της ασφάλειας, είναι εύκολο να γίνει σύγχυση, όταν γίνεται προσπάθεια να επιλεγεί η κατάλληλη μέθοδος για την αξιολόγηση των πληροφοριών κινδύνων που την ασφάλεια σας. Οι περισσότερες από τις μεθόδους αρχίζουν με την υποδομή πληροφορικής και επικεντρώνονται στα τρωτά σημεία χωρίς να λάβουν υπόψη τους κινδύνους που αφορούν τους επιχειρηματικούς στόχους του οργανισμού. Ως εκ τούτου θα ληφθούν σε μεγάλο βαθμό υπόψη οι επιχειρηματικοί στόχοι. Τα παραπάνω είναι αναγκαία για να γίνουν γνωστές οι ευπάθειες του πληροφοριακού συστήματος και για να οριστούν οι ειδικές δικλείδες ασφαλείας που θα εφαρμοστούν για να μειώσουν τον κίνδυνο. Πρέπει να γίνει ανάλυση κινδύνων πριν από την ανάπτυξη/υλοποίηση του νέου Πληροφοριακού Συστήματος		
	(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ Μεσαία	❑ Χαμηλή
(7) Επιπτώσεις (Consequences)		**(8)** Σημαντικότητα/ Σπουδαιότητα (Severity)		
		Περιοχή Επίπτωσης	**Βαθμός Κινδύνου** (Value)	**Βαθμός Αποτίμησης** (Score)
		Φήμη – Εμπιστοσύνη Πελατών	Μεσαίος	6
		Οικονομικά	-	0

		Παραγωγικότητα	Μεσαία	4
		Ασφάλεια & Υγεία	-	0
		Πρόστιμα & Αγωγές	-	0
		Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου				**10**
(9) Αντιμετώπιση Κινδύνου				
❑ Αποδοχή		❑ Αναβολή	✓ Μείωση	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:				
Πληροφοριακό Σύστημα		Υλοποίηση Ανάλυση Επικινδυνότητας.Risk Assessment πριν από την Σχεδίαση του Πληροφοριακού Συστήματος (Θα συμπεριλαμβάνονται Έγγραφο επιχειρησιακών επιπτώσεων έτσι ώστε να ενσωματωθούν και οι επιχειρησιακοί στόχοι «BIA», Εκμετάλλευση Ευπαθειών «Vulnerability Assessment»). Πλέον του παραπάνω πρέπει να υλοποιηθούν Σχέδιο Ανάκαμψης από Καταστροφή και ανάλυση Επιχειρησιακών Επιπτώσεων		
Εσωτερικό Δίκτυο				

10.5.12 3ο Σενάριο (Access Control)

10.5.12.1 Allegro - Worksheet 10			**ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ**
		Περιουσιακό Στοιχείο	**Υποδομή του Πληροφοριακού Αγαθού της Επιχείρησης**
Κίνδυνοι Περιουσιακών Στοιχείων	**Απειλή**	Τομείς Ενδιαφέροντος	***Πλαστοπροσωπία ταυτότητας επιχειρησιακού χρήστη (εφαρμογής),***
		(1) Δράστης (Actor)	Δυσαρεστημένος υπάλληλος ή κάποιος που ενεργεί εις βάρος της εταιρίας.
		(2) Μέσα (Means)	Υποκλέπτοντας την ταυτότητα ενός χρήστη θα μπορούσε να γίνει διαρροή στοιχείων, καταστροφή τους. κ.α.
		(3) Κίνητρο (Motive)	Αποκόμιση οικονομικού οφέλους, ηθική ικανοποίηση, .
		(4) Αποτέλεσμα (Outcome)	✓ **Αποκάλυψη** ❑ Καταστροφή ✓ **Τροποποίηση** ✓ **Διακοπή**

	(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφαλείας θα μπορούσαν να παραβιαστούν υποκλέπτοντας την ταυτότητα κάποιου εξουσιοδοτημένου χρήστη ο οποίος είχε τα στοιχεία του σε εμφανές σημείο ή με άντλησή τους ψηφιακά εφόσον δεν είναι διαφυλαγμένα με δικλείδες ασφαλείας. Πλέον αυτού αν δεν υπάρχουν ρόλοι θα έχει ο κακόβουλος πρόσβαση σε όλα τα δεδομένα της εφαρμογής αλλά και θα γνωρίζει στοιχεία για όλες τις εφαρμογές της επιχείρησης.		
	(6) Πιθανότητα (Probability)	❑ Υψηλή	❑ Μεσαία	✓ Χαμηλή
	(7) Επιπτώσεις (Consequences)	**(8)** Σημαντικότητα/ Σπουδαιότητα (Severity)		
		Περιοχή Επίπτωσης	**Βαθμός Κινδύνου** (Value)	**Βαθμός Αποτίμησης** (Score)
	Εκτιμάτε ότι θα υπάρξει οικονομική απώλεια για την εταιρία λαμβάνοντας υπόψη περιπτώσεις αιτήματος πρόσβασης σε κρίσιμη εφαρμογή και γνωστοποίηση της απάντησης στον χρήστη που έχει κάνει υποκλοπή. Αυτό θα εκθέσει την πρόσβαση σε περιεχόμενο ευαίσθητων εταιρικών πληροφοριών. Σε περίπτωση αποκάλυψης πληροφοριών επηρεάζεται η φήμη της εταιρίας και ενδέχεται να υπάρξουν νομικές κυρώσεις.	Φήμη – Εμπιστοσύνη Πελατών	Υψηλός	9
		Οικονομικά	Μέτριος	8
		Παραγωγικότητα	-	0
		Ασφάλεια & Υγεία	-	0
		Πρόστιμα & Αγωγές	Μέτριος	2
		Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου				**19**
(9) Αντιμετώπιση Κινδύνου				
❑ Αποδοχή	❑ Αναβολή	✓ **Μείωση**	❑ Μεταφορά	
Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:				
Σύστημα	• User Awareness για τα θέματα Ασφάλειας των Πληροφοριακών Συστημάτων και για τις υποχρεώσεις των χρηστών όσον αφορά τους λογαριασμούς πρόσβασης και τους κωδικούς τους πρόσβασης (πχ ότι είναι προσωπικοί καθώς και ότι μπορούν να έχουν κυρώσεις όσον αφορά το νομικό και κανονιστικό πλαίσιο σε κάθε εμπλοκή)			

	• Διαχωρισμός των καθηκόντων και ύπαρξη ρόλων με βάση τους τύπους χρηστών και τους ρόλους ασφάλειας της Επιχείρησης. • Χρήση LDAP και SSO για να υπάρχει καταγραφή των προσβάσεων (των πιστοποιημένων από το εταιρικό HR χρηστών) • Κρυπτογράφηση των κωδικών πρόσβασης • Ισχυροί κωδικοί πρόσβασης με ελάχιστο μήκος 8 χαρακτήρων με ένα Κεφαλαίο λατινικό γράμμα, τουλάχιστον έναν αριθμό και 2 ειδικούς χαρακτήρες. • Αλλαγή των κωδικών πρόσβασης κάθε 2 μήνες, διατήρηση λίστας παλαιότητας πέντε κωδικών πρόσβασης & μηχανισμός κλειδώματος λογαριασμού έπειτα από τρεις αποτυχημένες προσπάθειες • Χρήση SIEM & DAP εργαλείων για καταγραφή των κινήσεων
Εσωτερικό Δίκτυο	• User Awareness για τα θέματα Ασφάλειας των Πληροφοριακών Συστημάτων και για τις υποχρεώσεις των χρηστών όσον αφορά τους λογαριασμούς πρόσβασης και τους κωδικούς • Μηχανισμός ασφάλειας καταγραφής στοιχείων για το ποιος έχει αιτηθεί πρόσβαση στο σύστημα και πότε. • Έλεγχος δραστηριοτήτων χρηστών και ενημέρωση ότι η κίνηση τους καταγράφεται • Ανασκόπηση αποτυχημένων προσπαθειών πρόσβασης • Ενημέρωση διαχειριστών για θέματα Ασφάλειας και ειδικότερα για την δημιουργία ισχυρών κωδικών.

10.5.13 4ο Σενάριο (Communications Security)

<table>
<tr><td colspan="3">10.5.13.1 Allegro - Worksheet 10</td><td colspan="3">ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ</td></tr>
<tr><td></td><td></td><td>Περιουσιακό Στοιχείο</td><td colspan="3">Υποδομή του Πληροφοριακού Αγαθού της Επιχείρησης</td></tr>
<tr><td rowspan="11">Κίνδυνοι Περιουσιακών Στοιχείων</td><td rowspan="7">Απειλή</td><td>Τομείς Ενδιαφέροντος</td><td colspan="3">Υποκλοπή ή και διακοπή από/σε σημείο επικοινωνίας μεταξύ των συστημάτων της υποδομής του πληροφοριακού συστήματος</td></tr>
<tr><td>(1) Δράστης (Actor)</td><td colspan="3">Κακόβουλος προς την Επιχείρηση (εσωτερικός ή εξωτερικός)</td></tr>
<tr><td>(2) Μέσα (Means)</td><td colspan="3">Λόγω ευπαθειών και της μεθόδου eavesdropping όπου ο κακόβουλος κρυφακούει και παρακολουθεί την επικοινωνία η εκμετάλλευση κενού ασφαλείας κατά το data in motion “data in transit”</td></tr>
<tr><td>(3) Κίνητρο (Motive)</td><td colspan="3">Αποκόμιση οικονομικού οφέλους και επίπτωση στην φήμη της Επιχείρησης</td></tr>
<tr><td>(4) Αποτέλεσμα (Outcome)</td><td colspan="3">✓ Αποκάλυψη ❑ Διακοπή
❑ Τροποποίηση ❑ Καταστροφή</td></tr>
<tr><td>(5) Απαιτήσεις Ασφάλειας (Security Requirements)</td><td colspan="3">Οι απαιτήσεις ασφάλειας θα μπορούσαν να παραβιαστούν σε ένα από τα κανάλια επικοινωνίας</td></tr>
<tr><td>(6) Πιθανότητα (Probability)</td><td>❑ Υψηλή</td><td>✓ Μεσαία</td><td>❑ Χαμηλή</td></tr>
<tr><td colspan="2" rowspan="2">(7) Επιπτώσεις (Consequences)</td><td colspan="3">(8) Σημαντικότητα/ Σπουδαιότητα (Severity)</td></tr>
<tr><td>Περιοχή Επίπτωσης</td><td>Βαθμός Κινδύνου (Value)</td><td>Βαθμός Αποτίμησης (Score)</td></tr>
<tr><td colspan="2" rowspan="5"></td><td>Φήμη–Εμπιστοσύνη Πελατών</td><td>Μεσαία</td><td>6</td></tr>
<tr><td>Οικονομικά</td><td>Χαμηλή</td><td>4</td></tr>
<tr><td>Παραγωγικότητα</td><td>-</td><td>0</td></tr>
<tr><td>Ασφάλεια & Υγεία</td><td>-</td><td>0</td></tr>
<tr><td>Πρόστιμα & Αγωγές</td><td>-</td><td>0</td></tr>
</table>

		Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου				**10**
(9) Αντιμετώπιση Κινδύνου				
❑ Αποδοχή		❑ Αναβολή	✓ Μείωση	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:				
Σύστημα		• Χρήστη ενημερωμένου πιστοποιητικού στο web Logic TLS/SSL • Κρυπτογραφημένη επικοινωνία μεταξύ του Client και του Application – Web Server. Για την μοναδική αμφίδρομη επικοινωνία του Application – Web Server & του DB Server με σκοπό την αποφυγή spoofing επιθέσεων πρέπει να γίνει ενεργοποίηση του Linux IP Tables		
Εσωτερικό Δίκτυο		• Εσωτερική Χρήση της υπηρεσίας στο Επιχειρησιακό δίκτυο • Χρήση κρυπτογραφημένου πρωτοκόλλου στο δίκτυο που φιλοξενεί το Πληροφοριακό Σύστημα.		

10.5.14 5ο Σενάριο (Physical & Environmental Security)

10.5.14.1 Allegro - Worksheet 10			**ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ**
		Περιουσιακό Στοιχείο	**Υποδομή του Πληροφοριακού Αγαθού της Επιχείρησης**
Κίνδυνοι Περιουσιακών Στοιχείων	**Απειλή**	Τομείς Ενδιαφέροντος	***Απουσία disaster υποδομής, Αστοχία Υλικού***
		(1) Δράστης (Actor)	Φυσική αιτία, τεχνικό Πρόβλημα, Κακόβουλη ενέργεια στο μηχανογραφικό κέντρο που φιλοξενεί την Υποδομή.
		(2) Μέσα (Means)	Απουσία disaster υποδομής & έλλειψη resources.
		(3) Κίνητρο (Motive)	Φυσικές αιτίες, τεχνική δυσλειτουργία, κακόβουλη ενέργεια
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ✓ Διακοπή ❑ Τροποποίηση ✓ Καταστροφή
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφάλειας μπορούν να παραβιαστούν αν δεν υπάρχει disaster recovery plan

	(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ Μεσαία	❑ Χαμηλή
	(7) Επιπτώσεις (Consequences)	**(8)** Σημαντικότητα/ Σπουδαιότητα (Severity)		
		Περιοχή Επίπτωσης	**Βαθμός Κινδύνου** (Value)	**Βαθμός Αποτίμησης** (Score)
	Απώλεια της υπηρεσίας, Απώλεια της Φήμης και της Εμπιστοσύνης Απώλεια της Παραγωγικότητας	Φήμη–Εμπιστοσύνη Πελατών	Μεσαία	6
		Οικονομικά	-	0
		Παραγωγικότητα	Υψηλή	6
		Ασφάλεια & Υγεία	-	0
		Πρόστιμα & Αγωγές	-	0
		Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου				**12**

(9) Αντιμετώπιση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ Μείωση	❑ Μεταφορά

Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:

Συστήματα	• Υλοποίηση σχέδιο ανάκαμψης από καταστροφή – ΣΑΚ με την διαδικασία ανάκαμψης (σε cold site). Πρέπει να έχουν προσδιοριστεί τα RTO, RPO από τον ιδιοκτήτη της εφαρμογής καθώς και των στοιχείων των διαχειριστών και των λειτουργιών που θα χρειαστούν για το ΣΑΚ. • Υλοποίηση της Υποδομής σε περιβάλλον εικονικοποίησης VM. Διατήρησή της με την χρήση snapshot. • Online Backup – archive log mode db & χρήση cold site για επαναφορά στον αποδεκτό RTO. • Backup θα πρέπει να γίνεται στον database server και στον application server • Τα backup θα πρέπει να είναι διπλά και να διατηρούνται και στα 2 site της Επιχείρησης (primary & disaster).
Εσωτερικό Δίκτυο	Δικτυακή δρομολόγηση στο εναλλακτικό site. Αποδεκτός χρόνος μη λειτουργίας της υπηρεσίας είναι 8

	ώρες.

10.5.15 6ο Σενάριο (Systems Acquisition, Development & Maintenance)

Allegro - Worksheet 10			**ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ**
		Περιουσιακό Στοιχείο	**Εφαρμογή - Application του Πληροφοριακού Αγαθού της Επιχείρησης**
Κίνδυνοι Περιουσιακών Στοιχείων	**Απειλή**	Τομείς Ενδιαφέροντος	*Απουσία ασφαλούς κώδικα. (πχ επιτρέπει ευπάθειες SQL Injection, XSS, RFI, CSRF).*
		(1) Δράστης (Actor)	Κακόβουλος εσωτερικά ή εξωτερικά της Επιχείρησης
		(2) Μέσα (Means)	*Απουσία ασφαλούς κώδικα με το οποίο θα λειτουργεί η εφαρμογή.*
		(3) Κίνητρο (Motive)	*Κακόβουλη ενέργεια (κλοπή ταυτότητας, πρόσβαση σε ευαίσθητες ή εμπιστευτικές πληροφορίες, κατασκοπία πλοήγησης των χρηστών, ψεύτικη διαφήμιση) για εκβιασμό, αποκόμιση οικονομικού οφέλους, ηθική ικανοποίηση. Αποκόμιση οφέλους διαταραχής φήμης, οικονομικού, νομικού – προστίμων μηνύσεων και μείωση παραγωγικότητας.*
		(4) Αποτέλεσμα (Outcome)	✓ Αποκάλυψη ❑ Διακοπή ✓ Τροποποίηση ❑ Καταστροφή

		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	*Ύπαρξη ευπαθειών που εκμεταλλεύονται ύπαρξη SQL injection: Η εφαρμογή επιτρέπει την χρήση αποθηκευμένων διαδικασιών που εκτελούνται με απευθείας σύνδεση στη βάση δεδομένων και χρήση sql injection χωρίς την χρήση παραμέτρων* *Ύπαρξη ευπαθειών που εκμεταλλεύονται ύπαρξη Cross-Site Scripting (XSS Injection): Κώδικας ευπαθής σε XSS επιθέσεις Η εφαρμογή δίνει την δυνατότητα ανάρτησης και χρήσης script από τον server έτσι ώστε όταν ο χρήστης συνδεθεί στον server να τρέχει το κακόβουλο script.* o *Reflected XSS: Ο ίδιος ο χρήστης του website εξαπατάται εφόσον ο κακόβουλος τον πείσει να πατήσει πάνω σε κάποιο ειδικά διαμορφωμένο link, το οποίο έχει ενσωματωμένο στο URL του ένα κακόβουλο payload.* o *Persistent XSS: Το payload αποθηκεύεται στη βάση δεδομένων του website και φορτώνεται αυτόματα από τον κώδικα των ιστοσελίδων με αποτέλεσμα να υπάρχει δυσλειτουργία σε όλους τους επισκέπτες του website.* o *DOM-based XSS: το payload εκτελείται στο DOM (Document Object Model) αντί να αποτελεί μέρος του html κώδικα που εμφανίζεται στον browser του θύματος. Αυτό σημαίνει ότι η ιστοσελίδα δεν μεταβάλλεται , αλλά ο κώδικας από την πλευρά του client (δηλαδή του επισκέπτη) εκτελείται με διαφορετικό τρόπο εξαιτίας της κακόβουλης τροποποίησης στο περιβάλλον DOM. Αυτό δίνει την δυνατότητα για την υποκλοπή της ενεργής συνεδρία (Session hijacking) με σκοπό την κατάληψη μιας ενεργής συνεδρίας. Βασική βλέψη η παράκαμψη του ελέγχου ταυτότητας.* *Ύπαρξη ευπαθειών που εκμεταλλεύονται ύπαρξη Remote File Inclusion (RFI): Η εφαρμογή επιτρέπει να στέλνεται κώδικας από απομακρυσμένο σημείο τοπικά στην εφαρμογή. Ο χρήστης εισάγει δεδομένα σε μία φόρμα αποθηκεύονται σε αρχείο που ενσωματώνεται σε ένα πρόγραμμα για να μπορεί να ανακτηθεί μετά. Ο κακόβουλος μπορεί να μπερδέψει το πρόγραμμα μέσω της δυνατότητας include που έχουν οι web εφαρμογές. Η εφαρμογή επιτρέπει είτε να τρέχει κώδικας που στέλνεται απομακρυσμένα στον server με αποτέλεσμα ο κακόβουλος να έχει πλήρη πρόσβαση στον server για να συλλέξει πληροφορίες και τροποποιεί ό,τι επιθυμεί, είτε τρέχει ο κώδικας τοπικά στον client, με την μορφή javascript και και ο κακόβολος αλλάζει τον τρόπο που επικοινωνεί ο server με τον client. Επιπλέον η εφαρμογή επιτρέπει στον κακόβουλο να κλέψει τα cookies του χρήστη. Η χρήση http & php εμφανίζουν σχετικές ευπάθειες.* *Ύπαρξη ευπαθειών που εκμεταλλεύονται ύπαρξη Cross Site Request Forgery (CSRF) ενεργοποίηση μέσω κακόβουλου Link.*

	(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ Μεσαία	❑ Χαμηλή
	(7) Επιπτώσεις (Consequences)	**(8)** Σημαντικότητα/ Σπουδαιότητα (Severity)		
		Περιοχή Επίπτωσης	**Βαθμός Κινδύνου** (Value)	**Βαθμός Αποτίμησης** (Score)
		Φήμη –Εμπιστοσύνη Πελατών	Υψηλός	9
		Οικονομικά	-	0
		Παραγωγικότητα	Υψηλός	6
		Ασφάλεια & Υγεία	-	0
		Πρόστιμα & Αγωγές	-	0
		Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου				**15**

(9) Αντιμετώπιση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ Μείωση	❑ Μεταφορά

Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:

Σύστημα	○ Ενημέρωση των χρηστών περιοδικά για τις ευπάθειες που αναφέρονται στο τρέχον σενάριο (**IT Security User Awareness)**. ○ Κάθε παράμετρος που περνάει στην βάση δεδομένων μέσω κάποιας εντολής SQL, θα πρέπει να είναι επικυρωμένη ή αλλιώς θα δεσμεύονται μεταβλητές που θα χρησιμοποιούνται υποχρεωτικά ○ Χρήση **WAF** web application firewalling ○ Χρήση **https** ○ Μη χρήση PHP ○ Penetration Test της εφαρμογής ○ Χρήση κώδικα που προστατεύει από: ○ **Cross-site scripting – XSS Injection** (π.χ. κλοπή κωδικών/λογαριασμών κλπ προσωπικών δεδομένων, Αλλαγή ρυθμίσεων του site, κλοπή των *cookies*, ψεύτικη διαφήμιση): ▪ Ένας τρόπος για να γίνεται sql injection είναι η προσπάθεια του να μεταβληθεί το DOM (Document Object Model) μέσω κακόβουλου java script κώδικα. Με την χρήση της

	Angular δεν γίνεται χρήση του DOM από την HTML για την παρουσίαση των δεδομένων από την ιστοσελίδα. Η Angular δεν το επιτρέπει καθώς τα δεδομένα τα προβάλει μέσω ng-bind που είναι ένα διαφορετικός τρόπος διαχείρισης (echo) του μοντέλου των object που χρησιμοποιεί. ○ **SQL Injection** (επιτρέπεται σε κακόβουλο να αλλάξει ότι θέλει στην βάση δεδομένων ή και να πάρει πληροφορίες) ○ **JSON Hijacking Protection** Το JSON Hijacking γίνεται εφόσον ο server έχει πρόθεμα σε όλα τα JSON αιτήματα το string ")]}',\n". ○ **JWT AUTHENTICATION (JASON WEB TOKEN)** STATELESS SECURITY MECHANISM (για προστασία από cookie) αφορά την εξέλιξη του OATH2 που το χρησιμοποιεί το facebook (προστασία που δίνει το spring). Το OATH αφορά τεχνική που κάνει USER AUTHENTICATION. Αντί να βάζουμε cookies ενεργοποιούμε το OAUTH. ○ **SPRING COOKIE THREAT PROTECTION** (CTP αφορά κακόβουλη ενέργεια μέσω της οποίας μπορεί να υποκλαπεί η προσβασιμότητα.). Η λύση που χρησιμοποιείται αφορά την δημιουργία νέου cookie κάθε φορά που ο χρήστης συνδέεται στο σύστημα. ○ **Cross Site Request Forgery (XSRF/CSRF)** που αφορά επίθεση που αναγκάζει τον τελικό χρήστη να εκτελέσει ανεπιθύμητες ενέργειες σε μια εφαρμογή δικτύου στην οποία είναι πιστοποιημένος. ○ **Functional Security**. Αν δεν υπάρχει, δεν δίνει διασφάλιση. Δεν γίνεται φίλτρο με το annotation @Secured() στις συναρτήσεις. Μέσω αυτού γίνεται ο έλεγχος του δικαιώματος για την εκτέλεση ή όχι της συνάρτησης. ○ **Spring Λογική firewall στα URL.** Έλεγχος σε μορφή firewall (url filtering). Αν το url που αιτείται ο χρήστης εμπίπτει σε κάποιο κανόνα που θέλει συγκεκριμένα credentials είτε απορρίπτεται και ελέγχεται ο επόμενος κανόνας που αν έχει τα credentials ενεργοποιείται. Ο τελευταίο κανόνας είναι reject. Οι κανόνες υπάρχουν στην κλάση security configuration του backend Spring.
Εσωτερικό Δίκτυο	

10.5.167ο Σενάριο (Κρυπτογράφηση - Cryptography)

<table>
<tr><td colspan="3">10.5.16.1 Allegro - Worksheet 10</td><td colspan="3">ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ</td></tr>
<tr><td></td><td></td><td>Περιουσιακό Στοιχείο</td><td colspan="3">Υποδομή όλα τα data at rest– Βάση Δεδομένων του Πληροφοριακού Αγαθού της Επιχείρησης & pdf στον application server</td></tr>
<tr><td rowspan="9">Κίνδυνοι Περιουσιακών Στοιχείων</td><td rowspan="7">Απειλή</td><td>Τομείς Ενδιαφέροντος</td><td colspan="3">Υποδομή Βάση Δεδομένων</td></tr>
<tr><td>(1) Δράστης (Actor)</td><td colspan="3">Κακόβουλος</td></tr>
<tr><td>(2) Μέσα (Means)</td><td colspan="3">Πρόσβαση από κακόβουλο και χρήση default λογαριασμών της ΒΔ. Εκμετάλλευση των δεδομένων στο επίπεδο data at rest.</td></tr>
<tr><td>(3) Κίνητρο (Motive)</td><td colspan="3">Αποκόμιση οφέλους διαταραχής φήμης, οικονομικού, νομικού – προστίμων μηνύσεων και μείωση παραγωγικότητας.</td></tr>
<tr><td>(4) Αποτέλεσμα (Outcome)</td><td colspan="3">✓ Αποκάλυψη ✓ Διακοπή
✓ Τροποποίηση ✓ Καταστροφή</td></tr>
<tr><td>(5) Απαιτήσεις Ασφάλειας (Security Requirements)</td><td colspan="3">Οι απατήσεις ασφάλειας θα μπορούσαν να παραβιαστούν στην βάση δεδομένων από έλλειψη κρυπτογράφησης</td></tr>
<tr><td>(6) Πιθανότητα (Probability)</td><td>❑ Υψηλή</td><td>✓ Μεσαία</td><td>❑ Χαμηλή</td></tr>
<tr><td colspan="2" rowspan="2">(7) Επιπτώσεις (Consequences)</td><td colspan="3">(8) Σημαντικότητα/ Σπουδαιότητα (Severity)</td></tr>
<tr><td>Περιοχή Επίπτωσης</td><td>Βαθμός Κινδύνου (Value)</td><td>Βαθμός Αποτίμησης (Score)</td></tr>
<tr><td colspan="2" rowspan="6"></td><td>Φήμη–Εμπιστοσύνη Πελατών</td><td>Μεσαίος</td><td>6</td></tr>
<tr><td>Οικονομικά</td><td>Μεσαίος</td><td>8</td></tr>
<tr><td>Παραγωγικότητα</td><td>Υψηλός</td><td>6</td></tr>
<tr><td>Ασφάλεια & Υγεία</td><td>-</td><td>0</td></tr>
<tr><td>Πρόστιμα & Αγωγές</td><td></td><td></td></tr>
<tr><td>Ορίζονται από τον χρήστη</td><td>-</td><td>0</td></tr>
<tr><td colspan="5">Συνολικός Βαθμός Κινδύνου</td><td>20</td></tr>
</table>

(9) Αντιμετώπιση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ Μείωση	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:			
Σύστημα	• Κλείδωμα των default λογαριασμών του RDBMS & του instance • Κρυπτογράφηση του σχήματος της Βάσης Δεδομένων που φιλοξενεί την εφαρμογή • Data Masking (Αφορά λύση που δεν επιτρέπει σε προνομιακούς χρήστες της βάσης να δουν τα πραγματικά δεδομένα). • Σύστημα Data Base audit protection. Μέσω αυτού θα γίνεται καταγραφή όλων των προσβάσεων στην βάση δεδομένων (τόσο για χρήστες συστήματος, όσο και για χρήστες βάσης αλλά και για τελικούς χρήστες).		
Εσωτερικό Δίκτυο			

10.5.178ο Σενάριο (Human Resources Security) (Asset Management)

10.5.17.1 Allegro - Worksheet 10			**ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ**
		Περιουσιακό Στοιχείο	**Πληροφοριακό Σύστημα του Πληροφοριακού Αγαθού της Επιχείρησης**
Κίνδυνοι Περιουσιακών Στοιχείων	**Απειλή**	Τομείς Ενδιαφέροντος	***Έλλειψη εξειδικευμένου προσωπικού διαχειριστών***
		(1) Δράστης (Actor)	Κακόβουλος που εκμεταλλεύεται την έλλειψη διαχειριστών
		(2) Μέσα (Means)	Έλλειψη ανθρώπινου δυναμικού
		(3) Κίνητρο (Motive)	Εκμετάλλευση Μοναδικού Σημείου Αστοχίας σχετικά με το εξειδικευμένο προσωπικό και θέλει να αποκομίσει όφελος από την διαταραχή φήμης, να έχει οικονομική απαίτηση, εκμετάλλευση που θα έχει νομική εμπλοκή – πρόστιμα και μηνύσεις ή/και μείωση παραγωγικότητας.
		(4) Αποτέλεσμα (Outcome)	❑ Αποκάλυψη ✓ Διακοπή ❑ Τροποποίηση ✓ Καταστροφή
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Ο κακόβουλος μπορεί να αφορά γνώστη του μοναδικού σημείου αστοχίας, να αφορά προσκείμενο πρόσωπο (εντός του εργασιακού ή εκτός του εργασιακού χώρου) ο οποίος θα εκμεταλλευτεί Denial Of Service μέσω spoofing, bot, net zombie.

	(6) Πιθανότητα (Probability)	❑ Υψηλή	✓ Μεσαία	❑ Χαμηλή
	(7) Επιπτώσεις (Consequences)	**(8)** Σημαντικότητα/ Σπουδαιότητα (Severity)		
		Περιοχή Επίπτωσης	**Βαθμός Κινδύνου** (Value)	**Βαθμός Αποτίμησης** (Score)
		Φήμη–Εμπιστοσύνη Πελατών	Υψηλή	6
		Οικονομικά	-	-
		Παραγωγικότητα	Υψηλή	6
		Ασφάλεια & Υγεία	-	0
		Πρόστιμα & Αγωγές	-	-
		Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου				**12**

(9) Αντιμετώπιση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ Μείωση	❑ Μεταφορά

Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:	
Σύστημα	• Πρόσληψη εξειδικευμένου προσωπικού (τουλάχιστον 2 διαχειριστές υποδομής & 2 προγραμματιστές) - Τεκμηρίωση της Εφαρμογής, των περιπτώσεων χρήσης - της λειτουργίας και όλων των σημείων Εναλλακτικά μπορούν να χρησιμοποιηθούν υπηρεσίες υποστήριξης εξωτερικές από εταιρεία, εφόσον έχει υπογράψει τα κατάλληλα συμβόλαια εμπιστευτικότητας NDA με την Επιχείρηση. • Το πληροφοριακό σύστημα θα πρέπει να προστατεύεται από firewall (NGFW) που θα διαθέτει IPS, AntiBot
Εσωτερικό Δίκτυο	

10.5.189ο Σενάριο (έλλειψη διαδικασιών)

10.5.18.1 Allegro - Worksheet 10			**ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ**		
		Περιουσιακό Στοιχείο	**Εφαρμογή του Πληροφοριακού Αγαθού της Επιχείρησης**		
Κίνδυνοι Περιουσιακών Στοιχείων		Τομείς Ενδιαφέροντος	***Έλλειψη διαδικασιών για την λειτουργία της εφαρμογής***		
		(1) Δράστης (Actor)	Κακόβουλος εντός της επιχείρησης ή καλόβουλος με εμπλοκή χωρίς πρόθεση		
		(2) Μέσα (Means)	Αστοχία στην λειτουργία - λάθος χειρισμός		
		(3) Κίνητρο (Motive)	Εφόσον αφορά κακόβουλο το κίνητρο μπορεί να αφορά δυσαρέσκεια υπαλλήλου. Εφόσον αφορά ενέργεια που υλοποιείται χωρίς πρόθεση η ενέργεια αφορά άγνοια.		
		(4) Αποτέλεσμα (Outcome)	✓ Αποκάλυψη ✓ Τροποποίηση	✓ Διακοπή ✓ Καταστροφή	
		(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφάλειας αφορούν καταγραφή των διαδικασιών (λειτουργίας εφαρμογής και διαχειριστικών), των εμπλεκομένων interfaces, BIA BCP & DRP εγγράφων.		
	Απειλή	**(6) Πιθανότητα** (Probability)	❑ Υψηλή	✓ Μεσαία	❑ Χαμηλή
	(7) Επιπτώσεις (Consequences)		**(8)** Σημαντικότητα/ Σπουδαιότητα (Severity)		
			Περιοχή Επίπτωσης	**Βαθμός Κινδύνου** (Value)	**Βαθμός Αποτίμησης** (Score)
			Φήμη – Εμπιστοσύνη Πελατών	-	-
			Οικονομικά	-	-
			Παραγωγικότητα	Υψηλή	6
			Ασφάλεια & Υγεία	-	0
			Πρόστιμα & Αγωγές	-	0
			Ορίζονται από τον χρήστη	-	0

Συνολικός Βαθμός Κινδύνου			**6**
(9) Αντιμετώπιση Κινδύνου			
❑ Αποδοχή	❑ Αναβολή	✓ Μείωση	❑ Μεταφορά
Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:			
Σύστημα	• Τεκμηρίωση διαδικασιών (λειτουργίας εφαρμογής, διαχείρισης εφαρμογής) • Τεκμηρίωση Λειτουργίας Πληροφοριακού Συστήματος - Εκπαίδευση χρηστών επιχειρησιακών και προνομιακών • Συγγραφή εγγράφου Επιχειρησιακής Συνέχειας. • Συγγραφή Σχεδίου Ανάκαμψης από καταστροφή. • Συγγραφή εγγράφου που αναλύει την Επίπτωση της Επιχείρησης από την Έλλειψη της Εφαρμογής.		
Εσωτερικό Δίκτυο			

10.5.1910ο Σενάριο (Compliance)

10.5.19.1 Allegro - Worksheet 10			**ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ**
		Περιουσιακό Στοιχείο	**Πληροφοριακό Σύστημα του Πληροφοριακού Αγαθού της Επιχείρησης**
Κίνδυνοι Περιουσιακών Στοιχείων	**Απειλή**	Τομείς Ενδιαφέροντος	***Έλλειψη ενημέρωσης των χρηστών (εφαρμογής και προνομιακών) για τα θέματα Ασφάλειας***
		(1) Δράστης (Actor)	Κακόβουλος εντός της επιχείρησης ή καλόβουλος με εμπλοκή χωρίς πρόθεση
		(2) Μέσα (Means)	Αστοχία στην λειτουργία - λάθος χειρισμός - διαμοιρασμός των κωδικών πρόσβασης
		(3) Κίνητρο (Motive)	'Αποκόμιση οφέλους οικονομικού, ηθικού με πρόθεση ή χωρίς. Εφόσον αφορά κακόβουλο το κίνητρο μπορεί να αφορά δυσαρέσκεια υπαλλήλου. Εφόσον αφορά ενέργεια που υλοποιείται χωρίς πρόθεση η ενέργεια αφορά άγνοια.
		(4) Αποτέλεσμα (Outcome)	✓ Αποκάλυψη ✓ Τροποποίηση ✓ Διακοπή ✓ Καταστροφή

	(5) Απαιτήσεις Ασφάλειας (Security Requirements)	Οι απαιτήσεις ασφάλειας μπορούν να παραβιαστύν – με εκμετάλλευση πρόσβασης		
	(6) Πιθανότητα (Probability)	❑ Υψηλή	❑ Μεσαία	✓ Χαμηλή
	(7) Επιπτώσεις (Consequences)	**(8)** Σημαντικότητα/ Σπουδαιότητα (Severity)		
		Περιοχή Επίπτωσης	**Βαθμός Κινδύνου** (Value)	**Βαθμός Αποτίμησης** (Score)
		Φήμη – Εμπιστοσύνη Πελατών	Υψηλή	9
		Οικονομικά	Υψηλή	12
		Παραγωγικότητα	Υψηλή	6
		Ασφάλεια & Υγεία	-	0
		Πρόστιμα & Αγωγές	-	-
		Ορίζονται από τον χρήστη	-	0
Συνολικός Βαθμός Κινδύνου				**27**
(9) Αντιμετώπιση Κινδύνου				
❑ Αποδοχή	❑ Αναβολή	✓ Μείωση	❑ Μεταφορά	
Για τους κινδύνους που αποφασίστηκε να αντιμετωπιστούν με έναν από τους παραπάνω τρόπους πρέπει να γίνουν τα ακόλουθα:				
Σύστημα	• User awareness σε θέματα Ασφάλειας Πληροφοριακών Συστημάτων τόσο των επιχειρησιακών χρηστών όσο και των προνομιακών χρηστών περιοδικά (τουλάχιστον μία φορά τον χρόνο)			
Εσωτερικό Δίκτυο				

Ανάλυση Επικινδυνότητας - Κατάσταση πριν την παραγωγή: Στην συνέχεια εμφανίζεται η επανάληψη της Ανάλυσης Επικινδυνότητας σε τεχνικό επίπεδο (περιληπτική) σε πίνακα (λόγω περιορισμού λέξεων πτυχιακής) και αφορά την κάλυψη του πίνακα 10 της μεθόδου Octave (10 ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ).

Περιουσιακό στοιχείο	Τομέας Ενδιαφέροντος	Δράστης	Μέσο	Κίνητρο	Αποτέλεσμα αποκάλυψη, διακοπή, καταστροφή, τροποποίηση	Πιθανότητα Υψηλή 3 Μεσαία 2 Χαμηλή 1	Επιπτώσεις 3. Φήμη 4. Οικονομικά 2. Παρα/τητα 1. Πρόστιμα & Αγωγές	Βαθμ. Κινδύνου	Αντιμετώπιση	Αντίμετρα	Κατάσταση πριν την παραγωγή
Web Appl & db Server	Πλαστοπροσωπία	από άτομα εντός της Επιχείρησης	Τρωτά σημεία του SAT ή υποκλοπή εξουσιοδοτήσεων	οικονομικό	αποκάλυψη, τροποποίηση	Χαμηλή 1	3x1 + 4x1	7	Μείωση	User Awareness, κρυπτογραφηση, authorization	**εφαρμόστηκε**
Web Appl & db Server	Πλαστοπροσωπία	από άτομα εκτός της Επιχείρησης	Τρωτά σημεία του SAT ή υποκλοπή εξουσιοδοτήσεων	οικονομικό	αποκάλυψη, τροποποίηση	Χαμηλή 1	3x1 + 4x1	7	Μείωση	User Awareness, κρυπτογραφηση, authorization	**εφαρμόστηκε**
Web Appl & db Server	Χρήστη του Συστήματος χωρίς εξουσιοδότηση	από κακόβουλους εντός/εκτός Επιχείρησης	Μέσω αδυναμιών του SAT ή υποκλοπής εξουσιοδοτήσεων	οικονομικό	αποκάλυψη, τροποποίηση	Χαμηλή 1	3x1 + 4x1	7	Μείωση	authorization, ρολοι, κρυπτογράφηση	**εφαρμόστηκε**
Web Appl & db Server	Παρακολούθηση επικοινωνιών	Κακόβουλος man in the middle	Μέσω ύπαρξης σχετικών ευπαθειών και της μεθόδου eavesdropping όπου ο κακόβουλος κρυφακούει και παρακολουθεί την επικοινωνία η εκμετάλλευση κενού ασφαλείας κατά το data in motion “data in transit”	οικονομικό	αποκάλυψη	Χαμηλή 1	3x1 + 2x1	5	Μείωση	κρυπτογράφηση σε επίπεδο data in motion - data on transit (μεταξύ db & application server & μεταξύ webapp & client	**εφαρμόστηκε**

Web Appl & db Server	Δυσχέρεια, παρεμπόδιση και αποτυχία της επικοινωνίας	Κακόβουλος man in the middle	Μέσω ύπαρξης σχετικών ευπαθειών και της μεθόδου eavesdropping όπου ο κακόβουλος κρυφακούει και παρακολουθεί την επικοινωνία η εκμετάλλευση κενού ασφαλείας κατά το data in motion "data in transit"	οικονομικό	διακοπή	Χαμηλή 1	3x1 + 2x1	5	Μείωση	κρυπτογράφηση σε επίπεδο data in motion - data on transit (μεταξύ db & application server & μεταξύ webapp & client - ύπαρξη RTO 8 ωρών	**εφαρμόστηκε**
Web Appl & db Server	Εισαγωγή ιού	Κακόβουλος εντός ή εκτός της Επιχείρησης	Μέσω πρόσβασης που έχει στην υποδομή	οικονομικό	καταστροφή	Χαμηλή 1	3x1 + 2x1	5	Μείωση	full disk encryption, authorization σην υποδομή	**εφαρμόστηκε**
Web Appl & db Server	Βλάβη Server	Αστοχία Υλικού	Αστοχίας Υλικού	κανένα	καταστροφή	Χαμηλή 1	3x1 + 2x1	5	Μείωση	Εικονικοποίηση, vm snapshots, backup, export, εναλλάκτικό cold site, online archive log db	**εφαρμόστηκε**
Web Appl & db Server	Διακοπή ηλεκτροδότησης	Αστοχία	Αστοχία	κανένα	διακοπή	Χαμηλή 1	3x1 + 2x1	5	Μείωση	Εικονικοποίηση, vm snapshots, backup, export, εναλλάκτικό cold site, online archive log db	**εφαρμόστηκε**
Web Appl & db Server	Λάθη χρήστη	Χρήστης της εφαγμογής	Λάθος εισαγωγή δεδομενων	κανένα	τροποποίηση	Μεσαία 2	3x1 + 1x1	4	Μείωση	user awareness, εγχειρίδια χρήσης χρηστών, αμυντικός προγραμματισμός	**εφαρμόστηκε**

Web Appl & db Server	Φυσική καταστροφή (πυρκαγιά, Πλημμύρα, Σεισμός)	Φυσική καταστροφη	Αδυναμία στους χώρους που φιλοξενούν την υποδομή	κανένα	καταστροφή	Χαμηλή 1	3x1 + 4x1 + 1x1	8	Αποδοχή	Εικονικοποίηση, vm snapshots, backup, export, εναλλάκτικό cold site, online archive log db	**εφαρμόστηκε**
Web Appl & db Server	Κλοπή δεδομένων	Κακόβουλος εντός ή εκτός της Επιχείρησης	Μέσω τρωτών σημείων της υποδομής	οικονομικό	αποκάλυψη	Χαμηλή 1	3x1 + 4x1 + 1x1	8	Μείωση	κρυπτογράφηση (data at rest) & data in motion	**εφαρμόστηκε**
Web Appl & db Server	Ηθελημένη ζημιά από κακόβουλο εντός της Επιχείρησης	Κακόβουλος εντός της Επιχείρησης	Αδυναμία στους χώρους που φιλοξενούν την υποδομή	οικονομικό	καταστροφή, δακοπή	Χαμηλή 1	3x1	3	Μείωση	Εικονικοποίηση, vm snapshots, backup, export, εναλλάκτικό cold site, online archive log db	**εφαρμόστηκε**

10.6 Παράρτημα Ζ: Ασφάλεια Πληροφοριακού Συστήματος (Business Impact Analysis, Vulnerability Assessment, Penetration Test)

10.6.1 Ανάλυση Επιχειρησιακών Επιπτώσεων – Business Impact Analysis (BIA)

- **Πληροφοριακό σύστημα** «Secure Authorization Ticketing – SAT»
- **Ιδιοκτήτης**: Επιχείρηση
- **Περιγραφή λειτουργίας**: Αυτοματοποίηση & Διαχείριση αιτημάτων πρόσβασης σε εφαρμογές της Επιχείρησης.
- **Συστήματα**: Web Server, Application Server, DB Server, Hypervisor, Backup
- **Δεδομένα**: LDAP Account, Αιτήσεις προσβάσεων, Ψηφιακές Υπογραφές, δεδομένα Χρηστών για όλο το εύρος της Επιχείρησης, Μητρώο Εφαρμογών, Ρόλους για κάθε εφαρμογή του Μητρώου, Διασυνδέσεις με τις εφαρμογές του Μητρώου.
- **Περιγραφή**: Αφορά πληροφοριακό σύστημα διαχείρισης και αυτοματοποιημένης υλοποίησης αιτημάτων πρόσβασης χρηστών σε εφαρμογές της επιχείρησης. Προσφέρει αυτοματοποίηση των αιτημάτων πρόσβασης. Υλοποιεί σύνδεση αυτόματα με συστήματα και κεντρική διαχείριση και συλλογή δεδομένων. Έχει εύρος σε όλους του επιχειρησιακούς χρήστες και εφαρμογές της Επιχείρησης.

10.6.1.1 Πότε και γιατί έχουμε τη μεγαλύτερη κρισιμότητα, φόρτο εργασίας.

Καθώς το σύστημα έχει εύρος σε όλη την Επιχείρηση και εξυπηρετεί όλο το πλήθος των χρηστών του εσωτερικού LDAP της Επιχείρησης για ένα πολύ μεγάλο μητρώο εφαρμογών, το φόρτο εργασίας υπάρχει πάντα κατά τις εργάσιμες ώρες. Η κρισιμότητά του όσον αφορά την διαθεσιμότητά του είναι μέτρια. Μπορούν δηλαδή οι χρήστες να αντέξουν ένα RTO των οχτώ ωρών.

Αλληλεπιδράσεις και Πληροφορίες Λειτουργίας.

Αλληλοεπιδρά με το LDAP (credentials) και με το εσωτερικό σύστημα HR της Επιχείρησης καθώς και με όλα τα πληροφοριακά συστήματα του μητρώου εφαρμογών που φιλοξενεί και διατηρεί στοιχεία αιτήσεων για άλλους χρήστες.

Εξαγόμενες πληροφορίες.

Αρχεία pdf με ψηφιακή υπογραφή που αφορούν τις αιτήσεις χρηστών.

Πιθανές αποφάσεις, που απαιτούν κατάλληλη πληροφόρηση.

Στατιστικά στοιχεία και πληροφόρηση για κινητικότητα σε αιτήματα πρόσβασης εφαρμογών. Αιτήσεις διαγραφών λόγω αποχώρησης υπαλλήλων από την επιχείρηση.

Κατηγορίες επιπτώσεων:

ΚΑΤΗΓΟΡΙΕΣ ΕΠΙΠΤΩΣΕΩΝ		
High	οι επιπτώσεις είναι κρίσιμες, για τη λειτουργία της Επιχείρησης.	Οι επιπτώσεις αφορούν τις κάτωθι κατηγορίες (ενδεικτικά): • Επιχειρησιακές επιπτώσεις • Την Φήμη της εταιρίας
Medium	οι επιπτώσεις δημιουργούν προβλήματα στη λειτουργία του	

	οργανισμού.	• Μη συμμόρφωση με συμβατικές υποχρεώσεις της εταιρίας • Μη συμμόρφωση με το κανονιστικό πλαίσιο
Low	οι επιπτώσεις δεν είναι σημαντικές για τη λειτουργία του οργανισμού.	

10.6.1.2 *Διαθεσιμότητα Επιχειρησιακών λειτουργιών / υπηρεσιών*

Απώλεια Διαθεσιμότητας Επιχειρησιακών λειτουργιών / υπηρεσιών					
Επιχειρησιακή λειτουργία / Υπηρεσία	Μέχρι 1 ώρα	Από 1 ώρα μέχρι 1 μέρα	Από 1 μέρα μέχρι 1 εβδομάδα	Από 1 εβδομάδα μέχρι 1 μήνα	Από 1 μήνα και πέρα
	Χαμηλή	Χαμηλή	Μεσαία	Μεσαία	Υψηλή

Συμπληρώστε αν υπάρχει Υψηλό η Μεσαίο επίπεδο

- Κανονιστική και συμβατική συμμόρφωση:
  - Περιγραφή: Διαρροή ευαίσθητων προσωπικών δεδομένων
  - Κόστος: Πρόστιμα κατά περίπτωση
- Επιχειρησιακή Λειτουργία:
  - Περιγραφή: καθυστέρηση λειτουργιών της
- Εμπιστοσύνη πελατών /προμηθευτών/ προσωπικού, Φήμη εταιρίας:
  - Περιγραφή: κλονίζεται η εμπιστοσύνη του προσωπικού

10.6.1.3 *Διαθεσιμότητα Συστημάτων (RTO)*

Απώλεια Διαθεσιμότητας Συστημάτων					
Σύστημα	Μέχρι 1 ώρα	Από 1 ώρα μέχρι 1 μέρα	Από 1 μέρα μέχρι 1 εβδομάδα	Από 1 εβδομάδα μέχρι 1 μήνα	Από 1 μήνα και πέρα
	Χαμηλή	Χαμηλή	Μεσαία	Μεσαία	Υψηλή

Συμπληρώστε αν υπάρχει Υψηλό η Μεσαίο επίπεδο

- Εμπιστοσύνη πελατών /προμηθευτών/ προσωπικού, Φήμη εταιρίας:
  - Περιγραφή: κλονίζεται η εμπιστοσύνη του προσωπικού

10.6.1.4 *Ακεραιότητα Συστημάτων (CONFIDENTIALITY)*

Απώλεια Ακεραιότητας Συστημάτων				
Σύστημα	Low	Medium	High	Σχόλια/Παρατηρήσεις
Webservers		X		
Database Server			X	
Application Server		X		

Συμπληρώστε αν υπάρχει Υψηλό η Μεσαίο επίπεδο

- Κανονιστική και συμβατική συμμόρφωση:
  - Περιγραφή: Μετατροπή στοιχείων κρίσιμων σε δεδομένα προσωπικά και ευαίσθητα προσωπικά μέσω Πλαστοπροσωπία και μεταβολή αιτημάτων έτσι ώστε να αποκτηθεί πρόσβαση σε κρίσιμα πληροφοριακά συστήματα. Δυνατότητα πρόσβασης μέσω διασυνδέσεων με όλα τα πληροφοριακά συστήματα της Επιχείρησης. Τα παραπάνω θέτουν σε νομικές, κανονιστικές και οικονομικές κυρώσεις την Επιχείρηση.
- Επιχειρησιακή Λειτουργία & Εμπιστοσύνη εμπλεκομένων (φήμη):
  - Περιγραφή: Πλαστοπροσωπία και μεταβολή αιτημάτων έτσι ώστε να αποκτηθεί πρόσβαση σε κρίσιμα πληροφοριακά συστήματα - κλονίζεται η εμπιστοσύνη όλων των παραπάνω
  - Κόστος: κατά περίπτωση

10.6.1.5 Διαθεσιμότητα Δεδομένων (RPO)

Απώλεια Διαθεσιμότητας Δεδομένων (μη δυνατότητα ανάκτησης από αντίγραφα ασφαλείας)					
Πληροφορίες/ Δεδομένα	Μέχρι 1 ώρα	Από 1 ώρα μέχρι 1 μέρα	Από 1 μέρα μέχρι 1 εβδομάδα	Από 1 εβδομάδα μέχρι 1 μήνα	Από 1 μήνα και πέρα
	Μεσαίο	Μεσαίο	Μεσαίο	Μεσαίο	Μεσαίο

Συμπληρώστε αν υπάρχει Υψηλό η Μεσαίο επίπεδο

Κανονιστική και συμβατική συμμόρφωση, Επιχειρησιακή Λειτουργία, Εμπιστοσύνη εμπλεκομένων & φήμη Επιχείρησης:

- Περιγραφή: Χρηματιστήριο – Κεφαλαιαγορά (External Auditors) - κλονίζεται η εμπιστοσύνη όλων των παραπάνω
- Κόστος: Κατά περίπτωση

10.6.1.6 Ακεραιότητα Δεδομένων (INTEGRITY)

Απώλεια Ακεραιότητας Δεδομένων				
Σύστημα	Low	Medium	High	Σχόλια/Παρατηρήσεις
Database Server		X		Αιτήσεις Πρόσβασης με ψηφιακή υπογραφή

Συμπληρώστε αν υπάρχει Υψηλό η Μεσαίο επίπεδο

Κανονιστική και συμβατική συμμόρφωση, Επιχειρησιακή Λειτουργία, Εμπιστοσύνη εμπλεκομένων & φήμη Επιχείρησης:

- Περιγραφή: Χρηματιστήριο – Κεφαλαιαγορά (External Auditors) - κλονίζεται η εμπιστοσύνη όλων των παραπάνω
- Κόστος: Κατά περίπτωση

10.6.1.7 Εμπιστευτικότητα Δεδομένων (Confidentiality)

Απώλεια Εμπιστευτικότητας Δεδομένων (εσκεμμένη ή μη)				
Πληροφορίες/ Δεδομένα	Low	Medium	High	Σχόλια/Παρατηρήσεις
Data Base Server	**X**			
webserver	**X**			
Application server	**X**			

Συμπληρώστε αν υπάρχει Υψηλό η Μεσαίο επίπεδο

Δεν υπάρχει έκθεση

10.6.1.8 Ελάχιστες απαιτήσεις προσωπικού, για ανάκαμψη και λειτουργία, σε περίπτωση καταστροφής:

Επαναφορά συστημάτων			
Σύστημα	**Πλήθος ατόμων**	**Τύπος χρηστών**	**Παρατηρήσεις**
DB Server	1	*Διαχειριστής ΒΔ*	Μπούρα Χριστίνα
Application Server	1	Διαχειριστής Συστήματος	Κεσκεμπές Αθανάσιος
Web Server	1	Διαχειριστής Συστήματος	Κεσκεμπές Αθανάσιος
Hypervisor	1	Διαχειριστής Συστήματος	Μπούρα Χριστίνα
Σύστημα Backup	1	Διαχειριστής Συστήματος	Κεσκεμπές Αθανάσιος

Λειτουργικές ανάγκες			
Εργασία	**Πλήθος ατόμων**	**Τύπος χρηστών**	**Παρατηρήσεις**
Καθημερινή υποστήριξη	4	Διαχειριστές	Σύστημα, ΒΔ, Εφαρμογή

10.6.1.9 Υποστηρικτικά Συστήματα

10.6.1.9.1 Υποστηρικτικά Συστήματα, καθημερινής λειτουργίας. Hypervisor για την υποστήριξη των εικονικών μηχανών, εσωτερικό δίκτυο, σύστημα αντιγράφων ασφαλείας.

10.6.1.9.2 Ελάχιστες απαιτήσεις υποδομής συστημάτων για τη βασική λειτουργία, σε έκτακτες περιπτώσεις. Η υποδομή που περιγράφεται παραπάνω

10.6.1.9.3 Για πόσο διάστημα μπορεί (αν είναι εφικτό) να συνεχίσει η λειτουργία χωρίς τα υποστηρικτικά συστήματα. (Θεωρήστε την περίπτωση με τη μεγαλύτερη κρισιμότητα και φόρτο εργασίας). Χωρίς τον Hypervisor δεν μπορεί να λειτουργήσει καθόλου η υπηρεσία.

***Επιμέρους σχόλια*:**

10.6.1.10 ΧΡΗΣΤΕΣ ΣΥΣΤΗΜΑΤΟΣ

1. Αριθμός και Κατηγορίες χρηστών: 12000 χρήστες, 8 τεχνικοί διαχειριστές.
2. Πόσα άτομα είναι τα ελάχιστα για τη βασική λειτουργία: 8 τεχνικοί (2 Διαχειριστές Συστημάτων και Βάσεων Δεδομένων, 2 διαχειριστές πληροφοριακού συστήματος, 4 διαχειριστές χρηστών)
3. Πόσα άτομα είναι τα ελάχιστα για την επιδιόρθωση της λειτουργίας, σε περίπτωση ολικής καταστροφής: 2 τεχνικοί (Διαχειριστές συστημάτων, βάσεων δεδομένων, Hypervisor, Backup και Εφαρμογής)

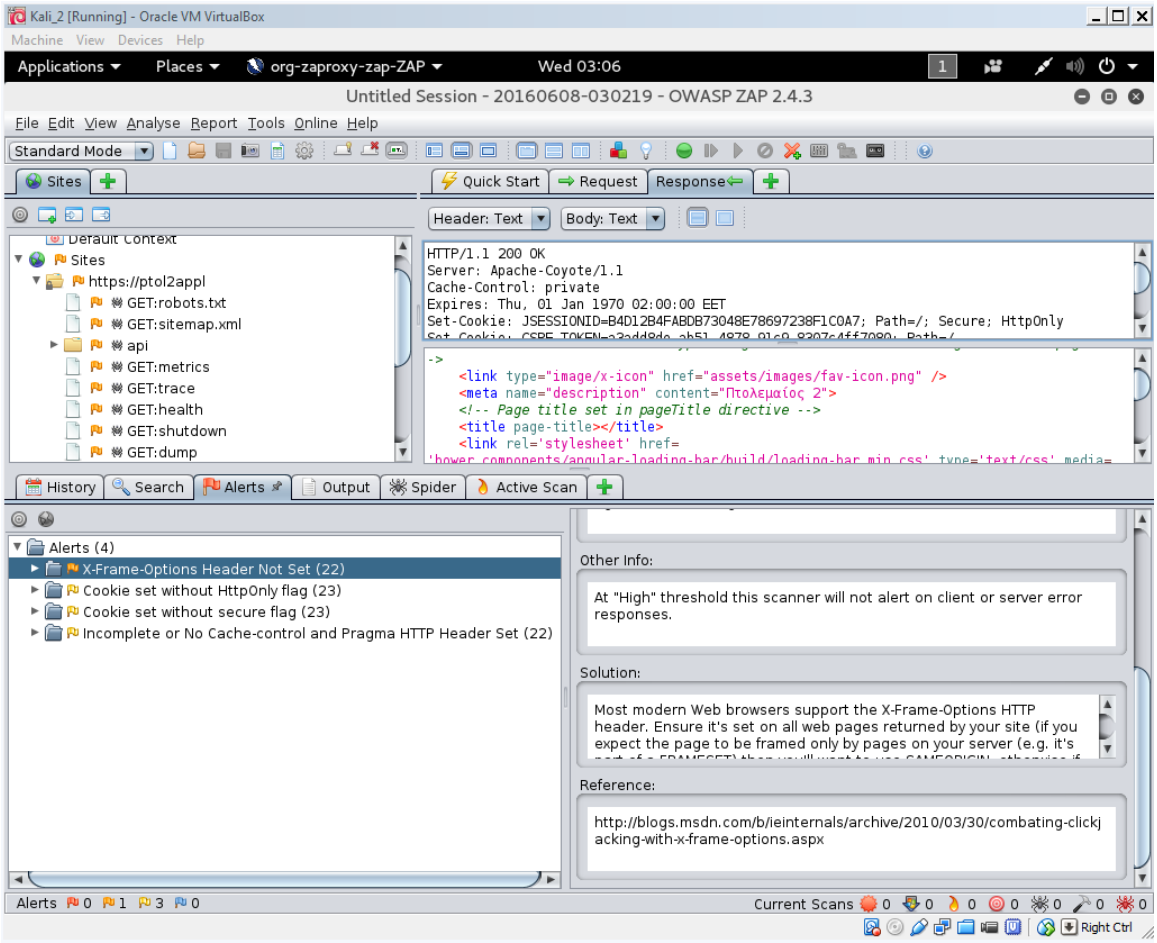
Υπεύθυνος Συνέντευξης
Μπούρα Χ. - Κεσκεμπές Αθ.

Συνεντευξιαζόμενος
Υπεύθυνος Τμήματος
Διαχείρισης Χρηστών

10.6.2 Αποτίμηση Ευπαθειών (Vulnerability Assessment) & Εκμετάλλευση Ευπαθειών - Δοκιμες Παρύσδεισης (Penetration Test)

Λογισμικά που χρησιμοποιήθηκαν – ευπάθειες που βρέθηκαν :

10.6.2.1 OWASP ZAP

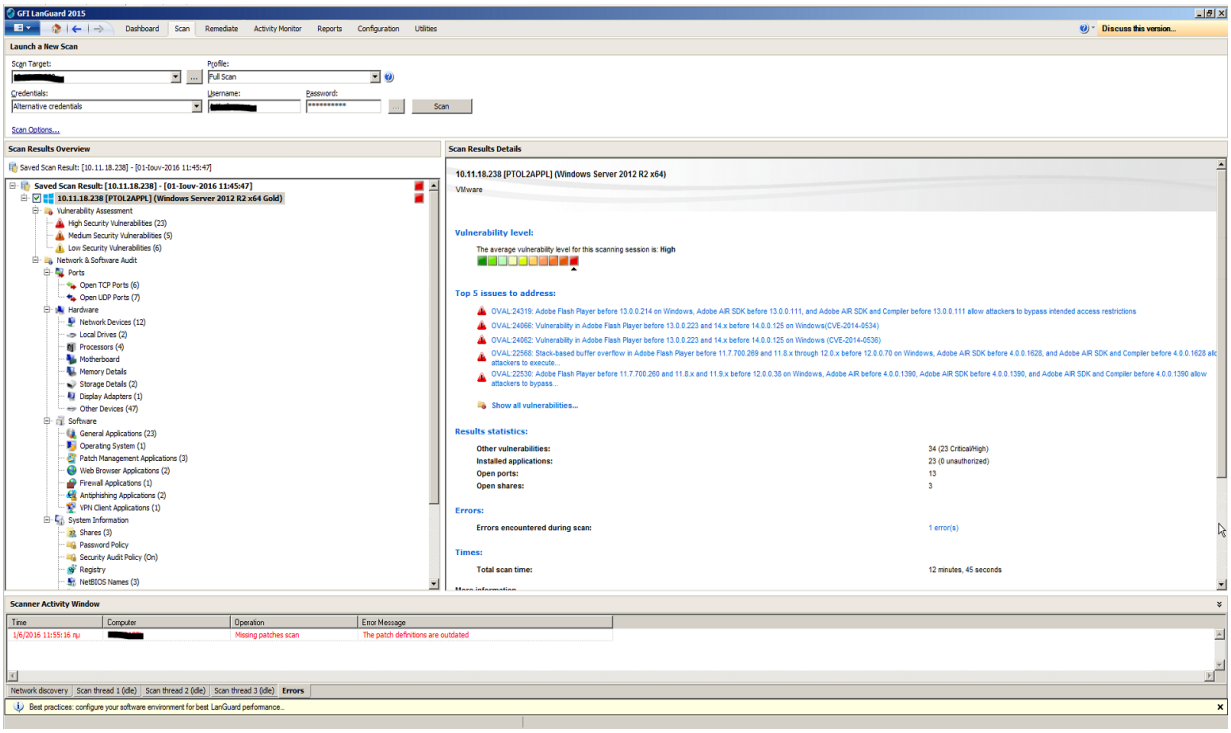


Εικόνα 65 VA OWASP ZAP

Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Low (Medium)	Cookie set without HttpOnly flag
Low (Medium)	Cookie set without secure flag
Medium (Medium)	X-Frame-Options Header Not Set

Resolved

10.6.2.2 GFI



Εικόνα 66 VA GFI env

Εικόνα 67 VA GFI graphs

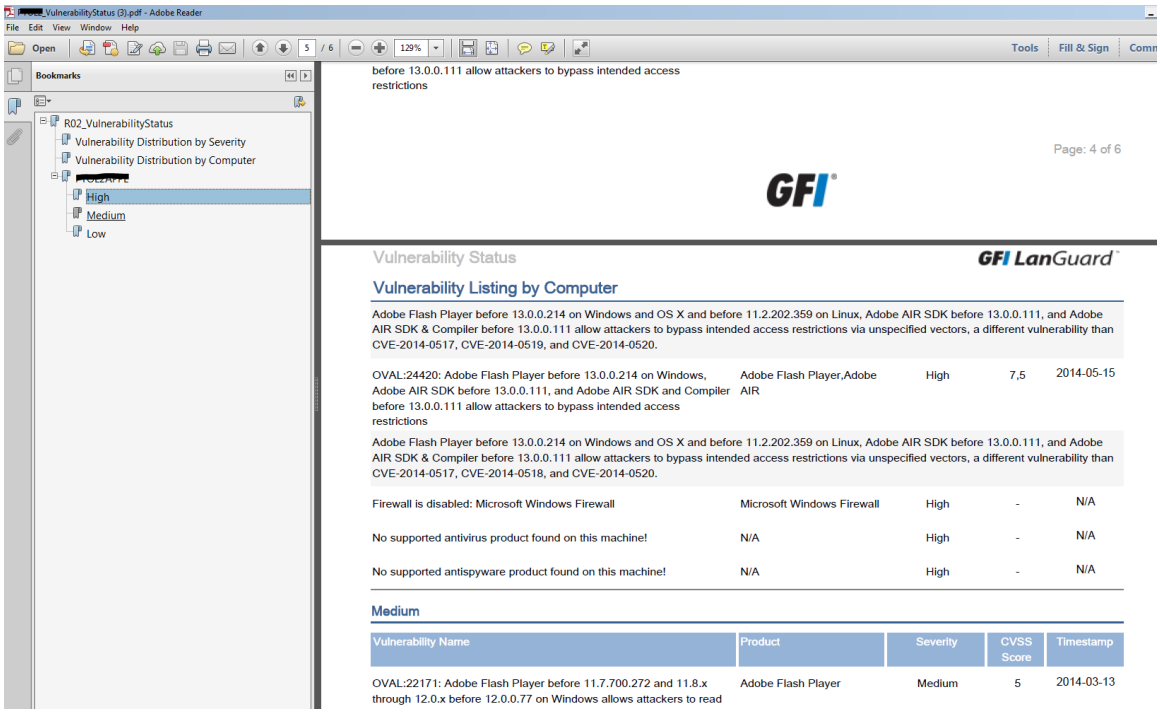
Καθώς υπάρχει περιορισμός στο μέγεθος της πτυχιακής ακολουθούν ενδεικτικά παραδείγματα των High & Mediut του Συστήματος από το report του παραπάνω εργαλείου. Τα ευρήματα αντιμετωπίστηκαν πρίν την παραγωγική λειτουργία.

Vulnerability Status — GFI LanGuard

Vulnerability Listing by Computer

Adobe Flash Player before 11.7.700.260 and 11.8.x and 11.9.x before 12.0.0.38 on Windows and Mac OS X and before 11.2.202.335 on Linux, Adobe AIR before 4.0.0.1390, Adobe AIR SDK before 4.0.0.1390, and Adobe AIR SDK & Compiler before 4.0.0.1390 allow attackers to defeat the ASLR protection mechanism by leveraging an "address leak."			
OVAL:24066: Vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows(CVE-2014-0534)	Adobe Flash Player,Adobe AIR	High	7,5	2014-04-11
Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0535.			
OVAL:24062: Vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows (CVE-2014-0536)	Adobe Flash Player,Adobe AIR	High	10	2014-04-11

Εικόνα 68 VA GFI Adobe



Εικόνα 69 VA GFI System

10.7 Παράρτημα Η: Πλαίσιο και Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων που συγγράφηκαν έτσι ώστε να καλύψουν το έργο.

10.7.1 Πλαίσιο Ασφάλειας (Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων)

10.7.1.1 Εισαγωγή

Το παρόν έγγραφο περιέχει το Πλαίσιο Ασφάλειας και τις Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων για την διαφύλαξη της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας της πληροφορίας.

10.7.1.2 Σκοπός και εύρος εφαρμογής των Πολιτικών

Σκοπός των Πολιτικών Ασφάλειας είναι να θέσουν τις βασικές αρχές και τους κανόνες για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και της πληροφορίας της επιχείρησης από ευπάθειες και κινδύνους.

10.7.1.3 Σύνταξη και αναθεώρηση της Πολιτικής

Υπεύθυνος για τον σχεδιασμό και την σύνταξη των πολιτικών είναι το τμήμα Ασφάλειας Πληροφοριακών Συστημάτων της Επιχείρησης. Οι πολιτικές πρέπει να αναθεωρούνται κατ' ελάχιστον κάθε δύο χρόνια.

10.7.1.4 Ενημέρωση, Συμμόρφωση και ρόλοι ασφάλειας & εύρος Εφαρμογής της Πολιτικής

Το τμήμα Ασφάλειας εφαρμόζει την Πολιτική, ενημερώνει τους εμπλεκομένους και Ελέγχει την συμμόρφωση τους με αυτή. Οι εμπλεκόμενοι ρόλοι Ασφάλειας που εμφανίζονται παρακάτω,

- Ο Ιδιοκτήτης του Πληροφοριακού Αγαθού (owner) που αφορά και τον υπεύθυνο εκτέλεσης με βάση τον νόμο περί προσωπικών δεδομένων (CEO)
- Ο υπεύθυνος του τμήματος Πληροφορικής που αφορά τον υπεύθυνο επεξεργασίας για τα πληροφοριακά συστήματα της Επιχείρησης (CIO)
- Ο υπεύθυνος Ανθρωπίνου Δυναμικού (CHRO)
- Ο υπεύθυνος του τμήματος νομικών Υπηρεσιών (CLO)
- Ο υπεύθυνος του τμήματος Ασφάλειας Πληροφοριακών Συστημάτων (CITSO)
- Οι υπάλληλοι και οι εξωτερικοί συνεργάτες

έχουν υποχρέωση συμμόρφωσης με την Πολιτική Κάθε παραβίαση της, εκθέτει την Επιχείρηση όσον αφορά την φήμη της αλλά επιφέρει και έκθεση οικονομική και νομική. Συνέπεια αυτού είναι η χρήση του δικαιώματος της Επιχείρησης επιβολής κυρώσεων όπως ο νόμος ορίζει.

Το εύρος εφαρμογής των Πολιτικών Ασφάλειας της Επιχείρησης αφορά όλα τα πληροφοριακά συστήματά της.

10.7.1.5 Εμπλεκόμενα μέρη

Οι Εμπλεκόμενοι είναι αφενός οι παραπάνω ρόλοι Ασφάλειας Πληροφοριακών Συστημάτων, αφετέρου όμως είναι:

Η Διοίκηση της Επιχείρησης, Το τμήμα Πληροφορικής, Το τμήμα Ασφάλειας Πληροφοριακών Συστημάτων, Το τμήμα Νομικών, Οι ιδιοκτήτες των εφαρμογών, Οι εργαζόμενοι, Οι εξωτερικοί συνεργάτες

10.7.1.6 Ονομασίες Πολιτικών Ασφάλειας

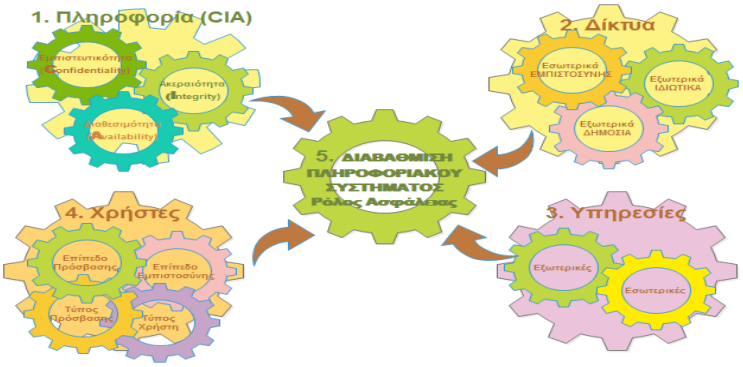
Διαβάθμισης και Διαχείρισης Πληροφοριακών Πόρων (P001)
Κρυπτογράφησης (P002)
Διαχείρισης Επικινδυνότητας Πληροφοριακών Συστημάτων P003
Δικτύων (P004)
Λειτουργίας Πληροφοριακών Συστημάτων & Υπηρεσιών (P005)
Συνεργασιών με τρίτους (P006)
Φυσικής Ασφάλειας (P007)
Περιστατικών Ασφάλειας (P008)
Πρόσβασης Χρηστών (P009)
Προστασίας από κακόβουλο Λογισμικό (P010)
Νέων Πληροφοριακών Συστημάτων (P011)
Φορητών Συσκευών (P012)
Μεταβολών Πληροφοριακών Συστημάτων (P013)

10.7.1.1.Πολιτική Ασφάλειας Διαβάθμισης Πληροφοριακών Πόρων

Εισαγωγή Πολιτικής Διαβάθμισης Πληροφοριακών Πόρων – P001

Οι εκάστοτε πληροφοριακοί πόροι αναφέρονται στην Πληροφορία, στα Συστήματα, στα δίκτυα, στους ανθρώπους που τα διαχειρίζονται (διαχειριστές, τεχνικούς) και στους ανθρώπους που τα χρησιμοποιούν (χρήστες). Η διαβάθμιση αναλύεται και εφαρμόζεται για τις παρακάτω Θεματικές ενότητες:

ΑΑ	Θεματική Ενότητα Πληροφοριακού Πόρου που χρήζει διαβάθμισης
1	**Πληροφορία**
2	**Δίκτυα**
3	**Υπηρεσίες**
4	**Χρήστες**
5	**Πληροφοριακά Συστήματα**



Μέθοδος Διαβάθμισης Πληροφοριακών Πόρων

Σώμα Πολιτικής P001

Διαβάθμιση της Πληροφορίας

Τα βασικά τρία κριτήρια για την εκτίμηση της αξίας της πληροφορίας (αποτίμηση) είναι η Εμπιστευτικότητα, η Ακεραιότητα και η Διαθεσιμότητα.

Διαβάθμιση ως προς το κριτήριο της Εμπιστευτικότητας

Η κλίμακα διαβάθμισης που εμφανίζεται παρακάτω αφορά την επίπτωση που θα έχει στην πληροφορία η παραβίαση της ασφάλειας από πρόσβαση που δεν έχει επέλθει από εξουσιοδότηση (παραβίαση) με αποτέλεσμα να γίνει αποκάλυψη της πληροφορίας και κατά συνέπεια διαρροή της.

Επίπεδο Διαβάθμισης	Λεκτικό Επιπέδου Διαβάθμισης	Περιγραφή Διαβάθμισης
1	ΧΡΗΣΗΣ ΧΩΡΙΣ ΠΕΡΙΟΡΙΣΜΟ	Οι πληροφορίες που ανήκουν σε αυτό το επίπεδο διαβάθμισης δεν απειλούνται με την γνωστοποίησή τους. Χρησιμοποιούνται και αποκαλύπτονται ελεύθερα χωρίς να δημιουργούν κάποιο πρόβλημα στην Επιχείρηση. Για παράδειγμα σε αυτό το επίπεδο ανήκουν τα δελτία τύπου και οι πληροφορίες που αναρτώνται στην ιστοσελίδα της Επιχείρησης προς δημόσια χρήση.
2	ΧΡΗΣΗΣ ΕΝΤΟΣ ΕΠΙΧΕΙΡΗΣΗΣ	Οι πληροφορίες που ανήκουν σε αυτό το επίπεδο διαβάθμισης μπορούν να χρησιμοποιηθούν μόνο από εσωτερικούς χρήστες της Επιχείρησης με βάση αρχή του ελαχίστου της γνώσης. Η γνωστοποίηση της πληροφορίας αυτής λόγω μη εξουσιοδότησης δεν επιτρέπεται, όμως δεν προκαλεί σοβαρή επίπτωση στην Επιχείρηση. Για παράδειγμα στις πληροφορίες του επιπέδου διαβάθμισης δύο (2) ανήκουν τα έγγραφα εσωτερικής επικοινωνίας, οδηγίες, εκπαιδευτικό υλικό κ.λ.π.
3	ΕΜΠΙΣΤΕΥΤΙΚΟ	Οι πληροφορίες που ανήκουν σε αυτό το επίπεδο διαβάθμισης αφορούν πληροφορίες που η αξία τους είναι σοβορή για την Επιχείρηση αλλά έχουν ταυτόχρονα την μικρότερη ευαισθησία επίπτωσης συγκριτικά με τα επίπεδα τέσσερα (4) και πέντε (5). Η αποκάλυψη της πληροφορίας της τρέχουσας διαβάθμισης σε μη εξουσιοδοτημένους χρήστες μπορεί να επιφέρει στην Επιχείρηση απώλειες οικονομικές, νομικές και απώλεια φήμης. Για παράδειγμα σε αυτές τις πληροφορίες ανήκουν τα προσωπικά δεδομένα προσωπικού, πελατών, προμηθευτών καθώς και σχέδια της Επιχείρησης (επενδυτικά) κλπ..
4	ΑΚΡΩΣ ΕΜΠΙΣΤΕΥΤΙΚΟ	Οι ευαίσθητες επιχειρησιακές πληροφορίες που ανήκουν σε αυτό το επίπεδο διαβάθμισης έχουν μεγάλη αξία για την Επιχείρηση. Η πρόσβαση σε αυτές υλοποιείται με περιορισμό. Βασικές αρχές προστασίας τους είναι η αρχή του ελαχίστου και του περιορισμού της γνώσης Η διαρροή και η χωρίς εξουσιοδότηση γνωστοποίηση τους θέτουν την Επιχείρηση σε σοβαρό κίνδυνο με την πιθανότητα διακοπής δραστηριοτήτων και επιπτώσεις στους μετόχους, στο προσωπικό, στους πελάτες και τους συνεργάτες της Επιχείρησης. Σημαντικά σημεία που βάλονται είναι η φήμη της Επιχείρησης,, υπάρχουν οικονομικές απώλειες και πιθανότητα νομικής εμπλοκής. Για παράδειγμα στις πληροφορίες αυτής της διαβάθμισης ανήκουν εταιρικά μυστικά για μελλοντική στρατηγική της Επιχείρησης, Πληροφορίες για κρίσιμες επενδύσεις, Πληροφορίες για τιμολογιακή πολιτική, νέα προιόντα και εμπορικά μυστικά, Αρχιτεκτονική Πληροφοριακών Συστημάτων, Χρηματοοικονομικές Πληροφορίες, οικονομιά αποτελέσματα καθώς και συναλλαγές πρό δημοσίευσης, ονόματα χρηστών και κωδικοί πρόσβασης σε κρίσιμα συστήματα.
5	ΑΠΟΡΡΗΤΟ	Οι πολύ ευαίσθητες επιχειρησιακές πληροφορίες που ανήκουν σε αυτό το επίπεδο διαβάθμισης μπορεί να επηρεάσει την αγορά που κινείται η ςΕπιχείρηση. Η διαρροή τους καθώς και η μη εξουσιοδοτημένη γνωστοποίησή τους μπορεί να επιφέρει πάρα πολύ σοβαρή επίπτωση στην Επιχείρηση. Η πρόσβαση επιτρέπεται σε περιορισμένο αριθμό χρηστών. Για παράδειγμα εξαγορές, επενδύσεις, χρηματιστηριακά δεδομένα ανήκουν σε αυτό το επίπεδο διαβάθμισης.

Πίνακας 1.1. Διαβάθμιση της Πληροφορίας ως προς το κριτήριο της Εμπιστευτικότητας

Διαβάθμιση ως προς το κριτήριο της Ακεραιότητας

Η διαβάθμιση της Ακεραιότητας (Integrity) της πληροφορίας αφορά την μεταβολή της χωρίς εξουσιοδότηση λόγω κακόβουλης η μη υπαιτιότητας εμφανίζεται στον παρακάτω πίνακα:

Επίπεδο Διαβάθμισης	Λεκτικό Επιπέδου Διαβάθμισης	Περιγραφή Διαβάθμισης
1	ΠΟΛΥ ΧΑΜΗΛΟ	Οι πληροφορίες συμπεριλαμβανομένης της υποδομής που φιλοξενούνται δεν αφορούν κρίσιμες επιχειρησιακές λειτουργίες και η κακόβουλη μεταβολή τους δεν έχει αντίκτυπο στην Επιχείρηση.
2	ΧΑΜΗΛΟ	Οι πληροφορίες συμπεριλαμβανομένης της υποδομής που φιλοξενούνται δεν αφορούν κρίσιμες επιχειρησιακές λειτουργίες οι οποίες είναι συγκεκριμενες. Η κακόβουλη μεταβολή τους δεν έχε σημαντικό αντίκτυπο στην Επιχείρηση.
3	ΜΕΣΑΙΟ	Οι πληροφορίες συμπεριλαμβανομένης της υποδομής που φιλοξενούνται αφορούν σοβαρές για την Επιχείρησης διεργασίες. Η κακόβουλη μεταβολή της πληροφορίας επιρεάζει την φήμη και την εμπιστοσύνη στην Επιχείρηση και την επηρεάζουν αρνητικά οικονομικά και νομικά.
4	ΥΨΗΛΟ	Οι πληροφορίες συμπεριλαμβανομένης της υποδομής που φιλοξενούνται αφορούν πολύ σοβαρές και απαραίτητες για την Επιχείρησης διεργασίες. Η κακόβουλη μεταβολή της πληροφορίας επιρεάζει την φήμη της Επιχείρησης και την επηρεάζουν αρνητικά οικονομικά και νομικά με σοβαρές επιπτώσεις στην αγορά . Η κακόβουλη και μη εξουσιοδοτημένη μεταβολή τους επηρεάζει σοβαρά τους μετόχους τους πελάτες το προσωπικό και τις συνεργασίες της Επιχείρησης.
5	ΠΟΛΥ ΥΨΗΛΟ	Οι πληροφορίες συμπεριλαμβανομένης της υποδομής που φιλοξενούνται αφορούν κρίσιμες διεργασίες της Επιχείρησης. Η κακόβουλη μεταβολή τους μπορεί να θέσει θέμα επιχειρησιακής συνέχειας με πάρα πολύ σοβαρές επιπτώσεις σε θέματα φήμης, θέματα οικονομικά και νομικά.

Πίνακας 1.2. Διαβάθμιση της Πληροφορίας ως προς το κριτήριο της Ακεραιότητας

Διαβάθμιση ως προς το κριτήριο της Διαθεσιμότητας

Η απώλεια της Διαθεσιμότητας (Availability) της Πληροφορίας (φυσική ή ψηφιακή μορφή) έχει δύο χρονικές μετρικές: α) Το Επιθυμητό Σημείο Ανάκτησης (**R**ecovery **P**oint **O**bjective) και τον Επιθυμητό Χρόνο Ανάκτησης (**R**ecovery **T**ime **O**bjective). Στο πίνακα που ακολουθεί διαβαθμίζεται η Διαθεσιμότητα:

Επίπεδο Διαβάθμισης	Λεκτικό Επιπέδου Διαβάθμισης	Περιγραφή Διαβάθμισης Πληροφορίας	
1	ΠΟΛΥ ΧΑΜΗΛΟ	**Φυσική**: Αφορά επιχειρησιακές Λειτουργίες της Επιχείρησης. Υπάρχουν εναλλακτικές μεθόδοι ανάκτησηςτης Πληροφορίας και οι λειτουργίες τις επιχείρησης αποκαθίστανται το περισσότερο στο χρονικό διάστημα ενός μήνα (**30 ημέρες**).	
		Ψηφιακή (RPO) = 7 ημέρες	**Ψηφιακή (RTO) = 7 ημέρες**
		Πρέπει να υπάρχει ενημέρωση των Πληροφοριακών Συστημάτων με δεδομένα 7 ημερών τουλάχιστον.	Ανάκτηση εντός τουλάχιστον 7 ημερών.
2	ΧΑΜΗΛΟ	**Φυσική**: Αφορά συγκεκριμένες επιχειρησιακές λειτουργίες. Υπάρχει ανοχή απώλειας και εναλλακτική ανάκτηση με κόστος. Αποκατάσταση πρέπει να γίνεται το περισσότερο εντός ενός δεκαημέρου (**10 ημέρες**).	
		Ψηφιακή (RPO) = 3 ημέρες	**Ψηφιακή (RTO) = 3 ημέρες**
		Τα πληροφοριακά συστήματα πρέπει να είναι ενημερωμένα με τα δεδομένα του τελευταίου τριημέρου.	Απαιτείται η ανάκτηση των δεδομένων εντός τριών ημερών.
3	ΜΕΣΑΙΟ	**Φυσική**: Αφορά σημαντικές επιχειρησιακές λειτουργίες. Υπάρχει μικρότερη ανοχή απώλειας. Υπάρχει εναλλακτική ανάκτηση με κόστος. Η αποκατάσταση πρέπει να γίνει το πολύ εντός πενθημέρου (**5 ημέρες**).	
		Ψηφιακή (RPO) = 2 ημέρες	**Ψηφιακή (RTO)**
		Τα πληροφοριακά συστήματα πρέπει να είναι ενημερωμένα με τα δεδομένα του τελευταίου διημέρου.	Απαιτείται η ανάκτηση των δεδομένων εντός διημέρου.
4	ΥΨΗΛΟ	**Φυσική**: Αφορά απαραίτητες επιχειρησιακές λειτουργίες. Υπάρχει μικρότερη ανοχή απώλειας. Υπάρχει εναλλακτική ανάκτηση με κόστος. Η αποκατάσταση πρέπει να γίνει το πολύ εντός μίας ημέρας (**1 ημέρα**).	
		Ψηφιακή (RPO) = 5 ώρες	**Ψηφιακή (RTO) = 5 ώρες**
		Τα πληροφοριακά συστήματα πρέπει να είναι ενημερωμένα με τα δεδομένα των τελευταίων 5 ωρών	Απαιτείται η ανάκτηση των δεδομένων εντός 5 ωρών
5	ΠΟΛΥ ΥΨΗΛΟ	**Φυσική**: Αφορά κρίσιμες επιχειρησιακές λειτουργίες. Υπάρχει ελέχιστη ανοχή απώλειας. Υπάρχει εναλλακτική ανάκτηση με πολύ μεγάλο κόστος. Η συνέπεια που θα έχει η Επιχείρηση σε μή ανάκτηση είναι σοβαρή. Η αποκατάσταση πρέπει να γίνει το πολύ εντός 12 ωρών (**12 ώρες**).	
		Ψηφιακή (RPO) = Μηδενική απώλεια	**Ψηφιακή (RTO) = Άμεση ανάκτηση**
		Απαιτείται μηδενική απώλεια δεδομένων	Απαιτείται άμεση ανάκτηση δεδομένων.

Πίνακας 1.3. Διαβάθμιση της Πληροφορίας ως προς το κριτήριο της Διαθεσιμότητας

Διαβάθμιση ως προς τα δίκτυα φιλοξενίας και διασύνδεσης

Η διαβάθμιση που έχει ένα Πληροφοριακό σύστημα βασίζεται στα δίκτυα τα οποία το εξυπηρετούν και τα δίκτυα με τα οποία συνεργάζεται.

Η διαβάθμιση αναλύεται στον πίνακα που ακολουθεί:

Δίκτυο που Διασυνδέεται το ΠΣ / Δίκτυο που Ανήκει το ΠΣ	Εσωτερικά Δίκτυα Trusted Internal Networks	Εξωτερικά Δίκτυα Δημόσια Public External Networks	Εξωτερικά Δίκτυα Ιδιωτικά Private External Networks
Εσωτερικά Δίκτυα Trusted Internal Networks	Ασφαλές	Κρίσιμο	Κρίσιμο
Εξωτερικά Δίκτυα Δημόσια Public External Networks	Κρίσιμο	Ασφαλές	Ευαίσθητο
Εξωτερικά Δίκτυα Ιδιωτικά Private External Networks	Κρίσιμο	Ευαίσθητο	Ασφαλές

Πίνακας 2.1. Διαβάθμιση Δικτύου που επηρεάζει το Πληροφοριακό Σύστημα

Διαβάθμιση ως προς τις Υπηρεσίες

Ο δεύτερος πυλώνας που επηρεάζει ένα πληροφοριακό σύστημα είναι οι ψηφιακές υπηρεσίες που το εξυπηρετούν , όπως για παράδειγμα η single sign on διασύνδεση με Active Directory.

Στο πίνακα που ακολουθεί εμφανίζεται η διαβάθμιση εμπιστοσύνης που αφορά τις υπηρεσίες:

Υπηρεσία που που Διασυνδέεται το ΠΣ	Διαβάθμιση
Εσωτερική Υπηρεσία	Ασφαλές
Εξωτερική Ιδιωτική Υπηρεσία	Ευαίσθητο
Εξωτερική Δημόσια Υπηρεσία	Κρίσιμο

Πίνακας 3.1. Διαβάθμιση Δικτύου που επηρεάζει το Πληροφοριακό Σύστημα

Διαβάθμιση ως προς τους Χρήστες Πληροφοριακού Συστήματος

Οι χρήστες που έχουν πρόσβαση σε ένα Πληροφοριακού Συστήματος όπως «Λειτουργικό Σύστημα, Βάσεις Δεδομένων, Προγράμματα και Εφαρμογή» είναι ένας από τους σοβαρότερους παράγοντες που πρέπει να λαμβάνονται υπόψη για την κατηγοριοποίηση και την διαβάθμιση του.

	Έμπιστος	Περιορισμένης Εμπιστοσύνης	Μη Έμπιστος
Τεχνικός χρήστης Εσωτερικός			
Τεχνικός χρήστης Εξωτερικός			
Χρήστης Απλός			
Χρήστης Προνομιακός			
Χρήστης Πλήρους Πρόσβασης			
Χρήστης Περιορισμένης Πρόσβασης			

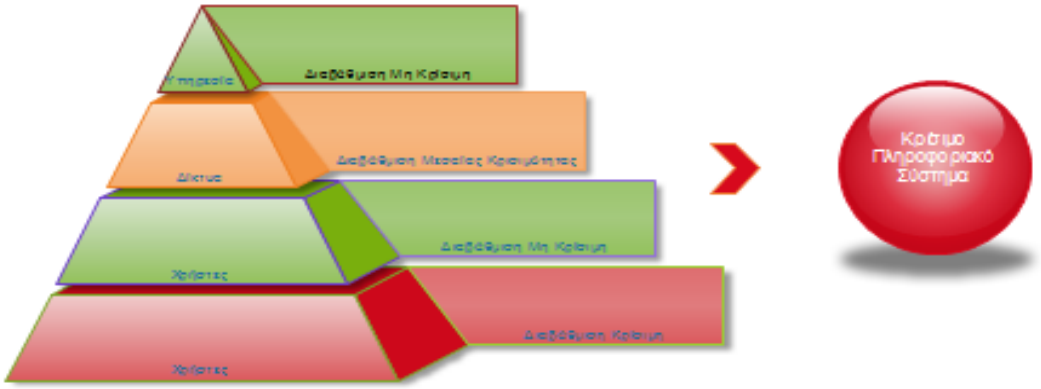
Επίπεδο Διαβάθμισης
Χαμηλό (Επιτρέπεται η πρόσβαση & Ελέγχεται (logs))
Μεσαίο (Επιτρέπεται η πρόσβαση για περιορισμένο χρόνο σε έκτακτες περιπτώσεις με καταγραφή (logs))
Υψηλό (Δεν επιτρέπεται η πρόσβαση)

Πίνακας 4.1. Διαβάθμιση με βάση το προφίλ χρήστη του Πληροφοριακού Συστήματος

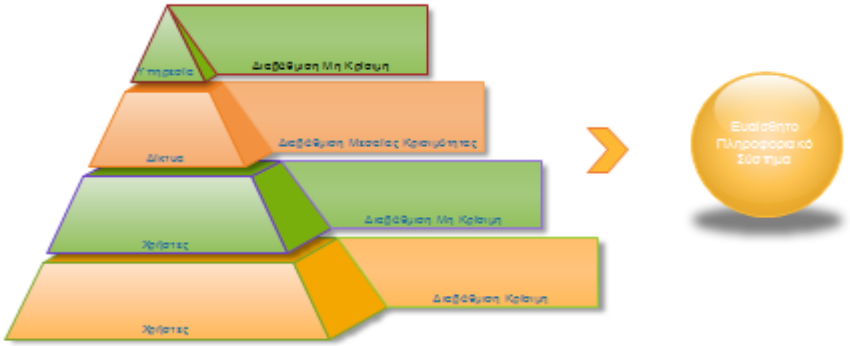
Διαβάθμιση Πληροφοριακού Συστήματος

Οι πληροφορίες ενός Πληροφοριακού Συστήματος, τα δίκτυα και οι υπηρεσίες που το εξυπηρετούν, οι διασυνδέσεις του, καθώς και οι προσβάσεις χρηστών αφορούν τις συνιστώσες που το επηρεάζουν με τις εκάστοτε διαβαθμίσεις επικινδυνότητας τους.

Ακολουθούν παραδείγματα του αποτελέσματος της μέγιστης διαβάθμισης κρισιμότητας που μπορεί να έχει ένα Πληροφοριακό Σύστημα:



Εικόνα 5.1. Διαβάθμιση Κρισιμότητας Πληροφοριακών Συστημάτων ως αποτέλεσμα τις μέγιστης κρισιμότητας των βασικών του Συνιστωσών (παράδειγμα 1^{ο})



Εικόνα 5.2. Διαβάθμιση Κρισιμότητας Πληροφοριακών Συστημάτων ως αποτέλεσμα τις μέγιστης κρισιμότητας των βασικών του Συνιστωσών (παράδειγμα 2^{ο})

Εικόνα 5.3. Διαβάθμιση Κρισιμότητας Πληροφοριακών Συστημάτων ως αποτέλεσμα τις μέγιστης κρισιμότητας των βασικών του Συνιστωσών (παράδειγμα 2^{ο})

Πίνακας 5.1. Διαβάθμιση Κρισιμότητας Πληροφοριακών Συστημάτων και αναγκαιότητα ύπαρξης του Ρόλου Ασφάλειας Πληροφοριακών Συστημάτων

10.7.1.2. Πολιτική Ασφάλειας Κρυπτογράφησης (Cryptography Policy)

Σώμα Πολιτικής Κρυπτογράφησης P002

Κρυπτογράφηση

Με την χρήση της κρυπτογράφησης διασφαλίζεται η Πληροφορία όσον αφορά την εμπιστευτικότητα και την ακεραιότητα της. Το τμήμα Ασφάλειας ΠΣ της Επιχείρησης παρακολουθεί την τεχνολογία της κρυπτογράφησης και επιλέγει σύγχρονους αλγορίθμους που διασφαλίζουν την εμπιστευτικότητα και την ακεραιότητα της πληροφορίας της Επιχείρησης. Δεδομένα για τα οποία υπάρχει επιχειρησιακή απαίτηση και ευαίσθητα προσωπικά δεδομένα πρέπει να κρυπτογραφούνται κατά την αποθήκευσή τους και την διακίνησή «data at rest & data in motion-transit». Οι φορητές συσκευές πρέπει να εφαρμόζουν τεχνολογία ολικής κρυπτογράφηση του αποθηκευτικού τους χώρου όπου αυτό επιτρέπεται από την τεχνολογία .

Δημόσιο κλειδί - Υποδομή

Πρέπει να διασφαλίζεται η συμμόρφωση με το εθνικό και διεθνές νομικό και κανονιστικό πλαίσιο καθώς και με τις οδηγίες και αποφάσεις των αρχών. Η υποδομή δημόσιου κλειδιού καθώς η πιστοποίηση των δημοσίων κλειδιών πρέπει να υλοποιείται από εσωτερική αρχή πιστοποίησης ή από πιστοποιημένη τρίτη οντότητα. Πρέπει να διασφαλίζεται η διαθεσιμότητα της υποδομής δημοσίου κλειδιού.

Ιδιωτικό κλειδί

Πρέπει να εφαρμόζεται κατάλληλη προστασία των ιδιωτικών κλειδιών από τον κάθε εμπλεκόμενο. Η απώλειά του κλειδιού μπορεί να δημιουργήσει απώλεια της

διαθεσιμότητας όσον αφορά την Πληροφορία για της οποίας την διαφύλαξη έχει γίνει χρήση του.

Ψηφιακές Υπογραφές

Πρέπει να υπάρχει αυστηρός περιορισμός της πρόσβασης σε ιδιωτικά κλειδιά των οποίων γίνεται χρήση σε ψηφιακές υπογραφές. Η ψηφιακή υπογραφή αναγνωρίζεται μόνο όταν υλοποιείσαι από έγκυρη αρχή πιστοποίησης.

Διαχείριση κλειδιών

Δημιουργία Διατήρηση. Ανανέωση κλειδιού και κατάργησή του

Για την δημιουργία κλειδιού πρέπει να χρησιμοποιούνται οι κατάλληλοι κρυπτογραφικοί αλγόριθμοι ώστε να εξασφαλίζονται η εμπιστευτικότητα του μηνύματος και η πιστοποίηση του αποστολέα. Η διάρκεια ενός κλειδιού πρέπει να είναι αντίστοιχη με τον βαθμό κρισιμότητας και εμπιστευτικότητας των δεδομένων. Κλειδιά για τα οποία υπάρχει ο ενδοιασμός παραβίασης καθώς και κλειδιά των οποίων δεν υπάρχει αναγκαιότητα ανακαλούνται και καταστρέφονται.

10.7.1.3.Πολιτική Ασφάλειας Διαχείρισης Επικινδυνότητας ΠΣ

Σώμα Πολιτικής

Αξιολόγηση Επικινδυνότητας Ασφάλειας Πληροφοριακών Συστημάτων

Σε αυτή την πολιτική παρουσιάζεται η μεθοδολογία η οποία είναι απαραίτητη για την αξιολόγηση και την διαχείριση της επικινδυνότητας σχετικά με τους πόρους των πληροφοριακών συστημάτων της Επιχείρησης.

Εύρος και Χρόνος που υλοποιείται Ανάλυση Επικινδυνότητας

Όσον αφορά το εύρος, αξιολόγηση επικινδυνότητας πρέπει να υλοποιείται μετά την ανάλυση απαιτήσεων για νέες εφαρμογές, πριν την προμήθεια νέων συστημάτων είτε αναπτύσσονται εσωτερικά της επιχείρησης είτε αφορούν προμήθεια. Επιπλέον πρέπει να υλοποιείται σε νέες υπηρεσίες, νέες διαδικασίες, που λειτουργούν εσωτερικά της επιχείρησης ή εξωτερικά μέσω συνεργασιών. Ακόμα πρέπει να υλοποιείται σε κρίσιμες νέες τεχνολογίες και υπηρεσίες καθώς και συνεργασίες εσωτερικές και εξωτερικές.

Αρμοδιότητα και Διεξαγωγή Αξιολόγησης Επικινδυνότητας

Αρμόδιοι για την έναρξη μίας τέτοιας δράσης είναι η Διοίκηση της Επιχείρησης αλλά και οι ιδιοκτήτες των Εφαρμογών καθώς και ο Τομέας Ασφάλειας Πληροφοριακών Συστημάτων

Αναλυτικά πρέπει να γίνεται Αποτίμηση Πληροφοριακών Πόρων, Αξιολόγηση Ευπαθειών, Αξιολόγηση Απειλών, Διαβάθμιση Επικινδυνότητας, Μητρώο Επικινδυνότητας, Σχέδιο Δικλείδων Ασφαλείας για την αντιμετώπιση της Επικινδυνότητας. Το αποτέλεσμα των παραπάνω θα είναι μία αναφορά που θα εμφανίζει στους υπεύθυνους τους κινδύνους και τις δικλείδες ασφαλείας. που θα πρέπει να εφαρμοστούν.

Ελεγκτικοί μηχανισμοί

Πρέπει να υλοποιούνται δοκιμές ευπάθειας και έλεγχοι σχετικά με την εφαρμογή των δικλείδων ασφαλείας που εγκρίνονται προς εφαρμογή με σκοπό να ενδυναμώνονται τα πληροφοριακά συστήματα.

Δοκιμές Παρείσδυσης (Vulnerability Assessment), αξιολόγηση Ευπαθειών (Penetration Test) και περιορισμοί τους

Δοκιμές Παρείσδυσης και αξιολόγησης ευπαθειών, πρέπει να υλοποιούνται σε όλη την υποδομή, τα λειτουργικά συστήματα και τις βάσεις, τα υποστηρικτικά πληροφοριακά συστήματα, τις υποδομές ασφάλειας, σε κρίσιμα αποκεντρωμένα συστήματα που φιλοξενούνται από επιχειρησιακές διευθύνσεις, προσωπικούς υπολογιστές και σε φορητό πληροφοριακό εξοπλισμό πάντα διασφαλίζοντας την Επιχειρησιακή Συνέχεια.

Στάδια δοκιμών Παρείσδυσης και αξιολόγησης ευπαθειών.

Αρχικά πρέπει:

- να γίνεται ενημέρωση των τεχνικών εμπλεκομένων τμημάτων.
- να γίνεται συμφωνία και να λαμβάνεται έγκριση από τον ιδιοκτήτη πληροφοριακού αγαθού.
- να ορίζεται ο τύπος της δοκιμής (white box, black box).
- να διασφαλίζεται η επιχειρησιακή συνέχεια και η διαθεσιμότητα και να υπάρχουν αντίγραφα ασφαλείας.
- να γίνεται έρευνα για τρωτά σημεία στα κεντρικά λειτουργικά συστήματα, στις βάσεις δεδομένων, στο εσωτερικό δίκτυο της Επιχείρησης, στις ιστοσελίδες, στις διασυνδέσεις
- να γίνεται έρευνα για πόρτες και για τρωτά σημεία σε επίπεδο προγραμματιστικό και επίπεδο κώδικα.

Ακολουθεί προσπάθεια εκμετάλλευσης των ευπαθειών για παρείσδυση και συντάσσεται αναφορά που παραδίδεται στην Διοίκηση της Επιχείρησης και στον Ιδιοκτήτη της Εφαρμογής. Σε αυτή την έκθεση είναι κατηγοριοποιημένες οι ευπάθειες και αναφέρονται οι δικλείδες ασφαλείας που πρέπει να εφαρμοστούν για την επίλυση των ευπαθειών. Στην συνέχεια με εγκρίσεις υλοποιούνται διεργασίες εφαρμογής των δικλείδων ασφαλείας που έχουν εγκριθεί.

Τεχνολογίες Ελέγχου Τρωτότητας και Ευπαθειών

- ✓ Οι τεχνολογίες που χρησιμοποιούνται για την αξιολόγηση τρωτότητας και ευπαθειών πρέπει να διαχειρίζονται από το τμήμα Ασφάλειας Πληροφοριακών Συστημάτων και πρέπει να δημιουργείται τεκμηρίωση της δράσης και μέσω αυτής να δημιουργείται η τελική αναφορά. Αυτή πρέπει να περιέχει τον σκοπό, το εύρος και την Μεθοδολογία που θα ακολουθηθεί και θα πρέπει να γίνεται καταγραφή, τεκμηρίωση και αναλυτική περιγραφή επεξήγηση και κατηγοριοποίηση, της κρισιμότητας όλων των τρωτών σημείων και τον αδυναμιών που παρατηρήθηκαν κατά την διάρκεια των ελέγχων. Ακολουθεί αναφορά στις διορθωτικές διεργασίες που πρέπει να γίνουν προς τους εμπλεκομένους.

Διαχείριση Έκθεσης Ελέγχου

- ✓ Οι εκθέσεις ελέγχου και τα έγγραφα που περιέχουν πληροφορίες δοκιμών Διείσδυσης και αξιολόγησης ευπαθειών είναι Εμπιστευτικά Διαχειρίζονται από το Τμήμα Ασφάλειας Πληροφοριακών Συστημάτων και γνωρίζονται ως εμπιστευτικά έγγραφα μόνο στα αρμόδια εμπλεκόμενα μέρη.

Διαχείριση Ευπαθειών

- ✓ Το τμήμα Ασφάλειας πρέπει να διαχειρίζεται και να αξιολογεί την εφαρμογή ή όχι των ενημερώσεων ασφάλειας. Πρέπει να υπάρχει κεντρική υποδομή μαζικής δρομολόγησης των ενημερώσεων ασφάλειας προς τους τελικούς σταθμούς εργασίας. Για την οργάνωση και την παρακολούθηση της αντιμετώπισης των ευπαθειών το τμήμα Ασφάλειας ΠΣ πρέπει να διατηρεί ενημερωμένο μητρώο που θα περιέχει όλα τα πληροφοριακά συστήματα.

Η παρακολούθηση των ευπαθειών πρέπει να γίνεται από εργαλεία αυτόματης ανίχνευσης ευπαθειών και αυτόματης αντιμετώπισής τους (SIEM, UBA, IDS/IPS, BDA).

10.7.1.4. Πολιτική Δικτύων (Network Policy)

Σώμα Πολιτικής

Το δίκτυο που χρησιμοποιείται ή υλοποιείται από την Επιχείρηση πρέπει να είναι διαβαθμισμένο.

Οι διαχειριστές που είναι υπεύθυνοι για κάθε συσκευή του δικτύου καθώς και για κάθε δίκτυο πρέπει να είναι κατά το ελάχιστο δύο για την διαφύλαξη της αρχής της μοναδικής αστοχίας του ανθρώπινου παράγοντα (Single Point of Failure).

Στο τμήμα Ασφάλειας Πληροφοριακών Συστημάτων πρέπει να διατηρείται μητρώο δικτύων της Επιχείρησης σε κρυπτογραφημένη ψηφιακή μορφή η οποία θα αφορά κρίσιμη και εμπιστευτική πληροφορία. Εναι αρμόδιο για τον συντονισμό και την εφαρμογή της αρχιτεκτονικής ασφάλειας του δικτύου και της εφαρμογής των αρχών του ελαχίστου προνομίου «least privilege» και του ελαχίστου της γνώσης «least need to know». Πρέπει να υπάρχει διαβάθμιση και διαχωρισμός των δικτύων με σχετική κατηγοριοποίηση «Segmentation».

Πρέπει να εξασφαλίζεται η διαθεσιμότητα των δικτύων με κατάλληλη αρχιτεκτονική.
Οι δικτυωμένες συσκευές της Επιχείρησης πρέπει να χρησιμοποιούν ιδιωτικές διευθύνσεις IP και στην περίπτωση που πρέπει να επικοινωνούν με εξωτερικά δίκτυα, πρέπει να εφαρμόζεται η τεχνική Μετάφραση Διεύθυνσης Δικτύου (NAT) ασφάλειας περιμέτρου. Η εξωτερική πύλη πρέπει να έχει δημόσια διεύθυνση για την εξωτερική διεπαφή με το διαδίκτυο.

Πρωτόκολλα Δικτύων

Η τεχνολογία μέσω της οποίας διασφαλίζεται η χρήση των δικτύων για την Επιχείρηση είναι η Ανοικτή Διασύνδεση Συστημάτων – OSI. Δεν επιτρέπονται οι συνδέσεις πληροφοριακών συστημάτων που βρίσκονται στο εταιρικό δίκτυο με το δίκτυο του παγκόσμιου ιστού (internet). Οι συνδέσεις αυτές θα γίνονται με την χρήση αναχωμάτων ασφαλείας επόμενης γενεάς και με την χρήση διαβαθμισμένης αποστρατικοποιημένης ζώνης.
Η πρόσβαση σε πληροφοριακά συστήματα από χρήστες εκτός του εταιρικού δικτύου μέσω διαδικτύου (πχ ιστοσελίδα) θα γίνεται μέσω της αποστρατικοποιημένης ζώνης όπου θα φιλοξενεί τα συστήματα αυτά.

Τεχνικές Ασφάλειας Δικτύου

Τεχνικές που πρέπει το τμήμα Ασφάλειας να χρησιμοποιεί και να εφαρμόζει για την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας της Πληροφορίας είναι τα αναχώματα Ασφαλείας επόμενης γενιάς (NGFW), τα συστήματα αποτροπής Εισβολής (IPS), τα συστήματα προστασίας από Ιούς, τα συστήματα παρακολούθησης διακίνησης ευαίσθητης πληροφορίας (DLP) με βάση το νομικό και κανονιστικό πλαίσιο και την κατάλληλη ενημέρωση των εμπλεκομένων, τα συστήματα προστασίας διαθεσιμότητας και αποτροπής μαζικής άρνησης υπηρεσίας (DoS, DDoS), τα συστήματα ελέγχου διαδικτυακού περιεχομένου, τα συστήματα αποτροπής της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας, με συστήματα παρακολούθησης περιστατικών ασφαλείας (SIEM, BDA, UBA), με τεχνικές αυθεντικοποίησης και με ασφαλή πρωτόκολλα (πχ https). Για την απομακρυσμένη σύνδεση πρέπει να υλοποιούνται τεχνικές απομακρυσμένης σύνδεσης (VPN), με την χρήση μοναδικού κωδικού πρόσβασης «one time password» ή token. Η δικτυακή πρόσβαση πρέπει να παρακολουθείται με τεχνολογία παρακολούθησης πρόσβασης δικτύου «NAC».

Καταγραφή - Παρακολούθηση

Πρέπει να γίνεται χρήση αναχωμάτων ασφαλείας «NGFW», να υπάρχει λογισμικό αποτροπής επιθέσεων «IPS», λογισμικό καταγραφής περιστατικών ασφάλειας και ανάλυσης απειλών σε πραγματικό χρόνο για διαφύλαξη από άρνηση υπηρεσίας «Dos» ή μαζική άρνηση υπηρεσίας «DDoS» και έναντι γνωστών και άγνωστων απειλών. Πρέπει να αναγνωρίζονται όλες οι εσφαλμένες προειδοποιήσεις «fault positives». Πρέπει να υλοποιούνται έλεγχοι για ανοικτές πόρτες στο δίκτυο από ειδικά εργαλεία «network security scanners»

Διαδίκτυο

Το διαδίκτυο είναι ένα δίκτυο χαμηλής εμπιστοσύνης. Η πρόσβαση των χρηστών της Επιχείρησης στον παγκόσμιο ιστό «Διαδίκτυο» πρέπει να φιλτράρεται και να διαφυλάσσεται το εσωτερικό δίκτυο της Επιχείρησης πχ χρήση διαμεσολαβητή «Proxy», Κρυπτογράφηση, Τεχνικές Αποτροπής εισβολών, Τεχνικές πρόβλεψης και εντοπισμού εισβολών «IDS/IPS», τεχνικές προστασίας κακόβουλου λογισμικού και ανεπιθύμητου/κακόβουλου ηλεκτρονικού ταχυδρομείου.

10.7.1.5.Πολιτική Ασφάλειας Λειτουργίας Πληροφοριακών Συστημάτων

Σώμα Πολιτικής

Η επιχείρηση διαθέτει σε όσους εμπλέκονται με τα πληροφοριακά της συστήματα ένα σύνολο εφαρμογών και υπηρεσιών με στόχο την σύγχρονη, αυτόματη και ευέλικτη λειτουργία των επιχειρησιακών διεργασιών. Οι εμπλεκόμενοι πρέπει να ακολουθούν όλες τις δικλείδες ασφαλείας που η Επιχείρηση ορίζει έτσι ώστε να διαφυλάσσεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα της Πληροφορίας.

Χρήση Πληροφοριακών Συστημάτων

Οι λογαριασμοί χρηστών της Επιχείρησης για την πρόσβαση σε πληροφοριακά συστήματα και υπηρεσίες (όπως το διαδίκτυο και το ηλεκτρονικό ταχυδρομείο) είναι αυστηρά προσωπικοί και εμπιστευτικοί. Οι χρήστες είναι υπεύθυνοι για την διαφύλαξη των λογαριασμών τους και λογοδοτούν για την κάθε κακόβουλη ενέργεια από αμέλειά τους. Δεν πρέπει να χρησιμοποιούν λογαριασμούς που ανήκουν σε άλλους χρήστες. Επίσης δεν πρέπει να γνωστοποιούν τον λογαριασμό τους σε τρίτους ακόμα και αν τίθεται θέμα επιχειρησιακής Συνέχειας. Στην περίπτωση που αποδειχτεί ότι ευπάθεια ή αδυναμία έχει λειτουργήσει και έχει γίνει διαρροή λογαριασμού χρήση και κωδικού πρόσβασης δεν είναι υπόλογος ο χρήστης. Στην περίπτωση που υπάρχει υπόνοια από τον χρήστη διαρροής των στοιχείων πρόσβασής του σε εφαρμογή θα πρέπει να ειδοποιείται άμεσα το τμήμα Ασφάλειας Πληροφοριακών Συστημάτων. Δεν πρέπει να χρησιμοποιείται από τον χρήστη ο λογαριασμός του, το εταιρικό ηλεκτρονικό του ταχυδρομείο και ο κωδικός πρόσβασής του σε υπηρεσίες και κοινωνικά δίκτυα του κυβερνοχώρου που δεν έχει εμπλοκή η Επιχείρηση. Όλοι οι υπολογιστές θα πρέπει να κλειδώνουν αυτόματα μετά από 10 λεπτά μη χρήσης.

Κάθε χρήστης πληροφοριακού συστήματος και υπηρεσίας της Επιχείρησης πρέπει να συμμορφώνεται με όλες τις Πολιτικές Ασφάλειας, να χρησιμοποιεί τα πληροφοριακά συστήματα ακολουθώντας τις αρχές των ελαχίστων προνομίων και του ελαχίστου της γνώσης. Στην περίπτωση μετακίνησής του και μακροχρόνιας απουσίας του ή συνταξιοδότησής του θα πρέπει σε συνεννόηση με τον προϊστάμενο του να το γνωρίζει στο αρμόδιο τμήμα διαχείρισης χρηστών.

Πρόσβαση στο διαδίκτυο

Η επιχείρηση διαθέτει με λογισμικό φιλτραρίσματος που αφορά την πρόσβαση στο διαδίκτυο με σκοπό να διαφυλάξει την φήμη της, κάθε νομική και οικονομική εμπλοκή της και κάθε έκθεση σε

κακόβουλο λογισμικό που θα πλήξει την εταιρική πληροφορία της και τα προσωπικά δεδομένα που διατηρεί. Αποκλείονται σελίδες που δημιουργούν πρόβλημα με την κανονιστική και νομοθετική συμμόρφωση της..

Κωδικοί Πρόσβασης

Πρέπει να εφαρμόζονται αυτόματες δικλείδες ασφαλείας έτσι ώστε: να γίνεται αλλαγή κωδικού πρόσβασης περιοδικά, να υπάρχει πολυπλοκότητα, να υπάρχει μήκος όπως οι βέλτιστες πρακτικές ορίζουν και να κλειδώνεται ο λογαριασμός σε πέντε λανθασμένες προσπάθειες. Δεν πρέπει να υπάρχει ο ίδιος κωδικός χρήστη σε όλες τις εφαρμογές εκτός αν υπάρχει μοναδικό σημείο πρόσβασης για όλες τις εφαρμογές (SSO).

Κινητός Πληροφοριακός Εξοπλισμός

Εάν διαθέτουν κινητό εξοπλισμό προσωπικό ή εξοπλισμό ο οποίος του έχει διατεθεί από την Επιχείρηση θα πρέπει να διασυνδέεται με λύσεις MDM και να εφαρμόζεται κρυπτογράφηση στον εξοπλισμό. Σε περίπτωση απώλειας του εξοπλισμού που διαθέτει εταιρική πληροφορία θα πρέπει να γίνεται αμέσως αναφορά στο τμήμα Ασφάλειας Πληροφοριακών Συστημάτων.

Απαγορευμένες Λειτουργίες

Δεν επιτρέπεται: η χρήση των κοινωνικών δικτύων, η απομακρυσμένη διαχείριση, η εγκατάσταση και χρήση επικοινωνίας στο διαδίκτυο πέραν αυτής που παρέχεται από την επιχείρηση, η εγκατάσταση λογισμικού το οποίο δεν ανήκει στο λογισμικό που διαθέτει η επιχείρηση, η υποκλοπή των κωδικών πρόσβασης άλλων χρηστών καθώς και η υποκλοπή διαχειριστικών κωδικών πρόσβασης, η χρήση δικτύων ομότιμων κόμβων (P2P) και η χρήση μηχανισμού ανωνυμίας στον κυβερνοχώρο.(π.χ. TOR, proxy client).

Ενημερώσεις (User Awareness)

Οι χρήστες πρέπει να είναι ενημερωμένοι για τα θέματα ασφάλειας και την ορθή χρήση των πληροφοριακών συστημάτων.

10.7.1.6.Πολιτική Ασφάλειας Συνεργασιών με Τρίτους

Σώμα Πολιτικής

Η επιχείρηση διαθέτει στο προσωπικό της, στους εξωτερικούς συνεργάτες της, στους πελάτες της και στους προμηθευτές της ένα σύνολο εφαρμογών και υπηρεσιών με στόχο την σύγχρονη, αυτόματη και ευέλικτη λειτουργία των επιχειρησιακών διεργασιών. Για την παροχή όλων των παραπάνω υπηρεσιών υπάρχει αναγκαιότητα εμπλοκής τρίτων.

Συμφωνητικά (NDA), Αξιολόγηση και έλεγχος

Οι Τρίτοι πρέπει να υπογράφουν κατά την έναρξη συνεργασίας τους με την Επιχείρηση συμφωνητικά τα οποία θα ορίζουν τα επίπεδα της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας της υπηρεσίας και θα πρέπει να δεσμεύονται νομικά ότι κάθε διαρροή ή κίνδυνος που αφορά την έκθεση της Επιχείρησης σε θέματα φήμης της, νομικά και οικονομικά με αποδεδειγμένη εμπλοκή τους, θέτει την Επιχείρηση να απαιτήσει κάθε δικαίωμά της όπως ο νόμος ορίζει. Πρέπει να ενημερώνονται από το τμήμα Ασφάλειας Πληροφοριακών Συστημάτων για τα θέματα Ασφάλειας Πληροφοριακών Συστημάτων και για τις πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων. Συνεργάζονται σε ελέγχους που γίνονται από το τμήμα Ασφάλειας Πληροφοριακών Συστημάτων με βάση το όρο του δικαιώματος διενέργειας ελέγχων από την Επιχείρηση στα Πληροφοριακά Συστήματα, τις Εφαρμογές και τις Υπηρεσίες που παρέχονται προς αυτήν και βρίσκονται σε εγκαταστάσεις τρίτων χρησιμοποιώντας το δικό της προσωπικό ή εξωτερικό πιστοποιημένο ελεγκτή (auditor).

Η Επιχείρηση πρέπει να αξιολογεί τους εξωτερικούς συνεργάτες ως προς της φήμη τους, τις προηγούμενες συνεργασίες τους, ως προς την αποδεδειγμένη ορθή εκτέλεση προηγούμενων παρόμοιων έργων, ως προς την εμπειρία των τεχνικών του με βάση ειδικές πιστοποιήσεις, το πλήθος των τεχνικών (Single Point of Failure), την ποιότητα παροχής υπηρεσιών με βάση το πρότυπο ISO 9001.

Λήξη

Κατά την λήξη συνεργασίας με τρίτους πρέπει να απενεργοποιούνται όλοι οι κωδικοί πρόσβασής τους.

Εξωτερικοί Συνεργάτες - Προμηθευτές

Οι εξωτερικοί συνεργάτες που παρέχουν υπηρεσίες υποστήριξης εντός της Επιχείρησης πρέπει να παραδίδουν πλήρη τεκμηρίωση για κάθε νέο σύστημα που αναπτύσσουν εντός της Επιχείρησης.

10.7.1.7.Πολιτική Φυσικής Ασφάλειας

Σώμα Πολιτικής

Η επιχείρηση διαθέτει στο προσωπικό της, στους εξωτερικούς συνεργάτες της, στους πελάτες της και στους προμηθευτές της ένα σύνολο εφαρμογών και υπηρεσιών με στόχο την σύγχρονη, αυτόματη και ευέλικτη λειτουργία των επιχειρησιακών διεργασιών. Για την παροχή όλων των παραπάνω υπηρεσιών υπάρχει αναγκαιότητα χρήσης ειδικών χώρων και πληροφοριακών συστημάτων που της ανήκουν αλλά και η λειτουργία εξωτερικών χώρων και πληροφοριακών υπηρεσιών που χρησιμοποιεί με την μορφή αγορά υπηρεσίας. Όσον αφορά τις ιδιόκτητες εγκαταστάσεις και τα πληροφοριακά συστήματα πρέπει να ακολουθούνται όλες οι δικλείδες

ασφαλείας για την προστασία από φυσικές απειλές (απώλεια ενέργειας, πυρκαγιά, πλημμύρα, σεισμός κλπ. Για τις εγκαταστάσεις που αφορούν εξωτερικές υπηρεσίες που παρέχονται στην Επιχείρηση πρέπει να ζητούνται τα παραπάνω μέσω των συμβολαίων που γίνονται κατά την σύμβαση της υπηρεσίας (SLA, NDA).

Εξωτερική Περίμετρος & Επιλογή Μηχανογραφικού Κέντρου

Πρέπει να υπάρχει εξωτερική περίφραξη με έντονο φωτισμό και παρακολούθηση μέσω αισθητήρων κίνησης, φυλάκων και κλειστού κυκλώματος τηλεόρασης, καμερών κλπ (το σύστημα πρέπει να έχει την κατάλληλη έγκριση από την Αρμόδια Αρχή – ΑΠΔΠΧ). Πρέπει να υπάρχει σύστημα συναγερμού για όλα τα σημεία που μπορούν να παραβιαστούν με σκοπό την κακόβουλη πρόσβασης καθώς και σύστημα διασύνδεσης με τις αρμόδιες αρχές που θα ενεργοποιείται από τον αρμόδιο φύλακα Θα πρέπει επίσης να υπάρχει προειδοποιητική σήμανση ότι ο χώρος μαγνητοσκοπείται.

Τα μηχανογραφικά κέντρα της Επιχείρησης πρέπει να βρίσκονται σε σημείο που είναι προστατευμένο από φυσικές καταστροφές. Το πρωτεύων και το δευτερεύων μηχανογραφικό κέντρο πρέπει να βρίσκονται σε διαφορετικά σεισμογενή σημεία και να μη βρίσκεται σε περιοχές που έχουν μεγάλη επικινδυνότητα καταστροφής.

Φυσικές απειλές

Σεισμός: Το μηχανογραφικό κέντρο πρέπει να βρίσκεται σε μη ευαίσθητα σεισμογενή σημεία ή ρήγματα. Επίσης πρέπει να ακολουθεί βέλτιστα πρότυπα αντισεισμικού κτιρίου (EC8-EN1998). Τα πληροφοριακά συστήματα πρέπει να είναι τοποθετημένα και ακινητοποιημένα με τέτοιο τρόπο πάνω στο δάπεδο ώστε να μην επηρεάζονται από την κίνηση κατά την διενέργεια σεισμού. Πρέπει να υπάρχει σχέδιο επανάκτησης όλων των συστημάτων σε περίπτωση ολικής καταστροφής του μηχανογραφικού κέντρου από εναλλακτικό μηχανογραφικό κέντρο (disaster site) μέσα στα αποδεκτά για το κάθε ένα χρονικά όρια (RPO, RTO).

Πλημμύρα: Το μηχανογραφικό κέντρο πρέπει να μην βρίσκεται σε υπόγειο. Τα πληροφοριακά συστήματα και οι πληροφοριακοί πόροι πρέπει να τοποθετούνται σε κατάλληλα σημεία, ώστε να μην κινδυνεύουν από πιθανές διαρροές στα δίκτυα ύδρευσης-αποχέτευσης ή από είσοδο νερού από εξωτερικά παράθυρα. Πρέπει να υπάρχει σύστημα υδρανίχνευσης. Το σύστημα θα έχει και εναλλακτική πηγή ενέργειας που θα λειτουργεί με την χρήση UPS ενώ στην περίπτωση που δεν λειτουργεί και αυτή θα αντλεί ρεύμα από γεννήτρια η οποία λειτουργεί αυτόνομα.

Πυρκαγιά: Πρέπει να υπάρχει σύστημα αυτόματης ανίχνευσης καπνού και φωτιάς σε όλα τα σημεία του χώρου του μηχανογραφικού κέντρου. Το υλικό πυρόσβεσης δεν πρέπει να καταστρέφει τα πληροφοριακά συστήματα. Το μηχανογραφικό κέντρο πρέπει να είναι δημιουργημένο από υλικά που αντέχουν την φωτιά. Πρέπει να περιέχει ηλεκτρικές γειώσεις και τα καλώδια πρέπει να περνάνε από υπερυψωμένο δάπεδο ή σε εσωτερική ψευδοροφή. Πρέπει να υπάρχουν σημεία εξαερισμού και μονάδες ψύξης.

Το προσωπικό πρέπει: να έχει κατάλληλη εκπαίδευση και να μεριμνά τόσο σε προσωπικό επίπεδο αλλά και για τρίτους, να είναι ενημερωμένο για τα σημεία (πινακίδες) που

αναφέρονται τα τηλέφωνα έκτακτης ανάγκης, να γνωρίζει την κατάλληλη ειδοποίηση έκβασης πυρκαγιάς και να γνωρίζει για την έξοδο κινδύνου. Η πρόσβαση εισόδου και εξόδου στο μηχανογραφικό κέντρο πρέπει να καταγράφονται.

Επιθέσεις-Βανδαλισμοί:

Πρέπει να αποφεύγεται η επιλογής της τοποθεσίας του μηχανογραφικού κέντρου να βρίσκεται δίπλα σε σημεία που γίνονται συχνά διαδηλώσεις.

Σχέδιο Εκκένωσης Υποδομών

Πρέπει να υπάρχει έγγραφο που να αναγράφει για κάθε υποδομή:

- το σχέδιο του χώρου την διαδικασία εκκένωσης
- τους ορισμένους υπεύθυνους εκκένωσης και τους ρόλους αυτών (
- πληροφορίες όπως τηλέφωνα έκτακτης ανάγκης
- Οδηγίες για πρώτες βοήθειες και ανταπόκρισης για κάθε είδους περίπτωση φυσικής καταστροφής (σεισμό, πλημμύρα, πυρκαγιά, επιθέσεις-βανδαλισμοί)

Το έγγραφο έκτακτης εκκένωσης λόγω φυσικής καταστροφής πρέπει να δοκιμάζεται με συμμετοχή όλου του προσωπικού κάθε έξι μήνες.

Παροχή Ενέργειας

Πρέπει να διαφυλάσσεται η πιθανότητα μοναδικού σημείου αστοχίας (Single Point of Failure) και να υπάρχουν επίπεδα εναλλακτικών μορφών παροχής ενέργειας. Το πρώτο επίπεδο πρέπει να είναι η παροχή ηλεκτρικής ενέργειας. Το δεύτερο επίπεδο πρέπει να είναι η χρήση ειδικών μπαταριών (ups) οι οποίες πρέπει να ελέγχονται συχνά με ειδικά συστήματα για το αποδεκτό επίπεδο φόρτισής τους, Το τρίτο επίπεδο θα αφορά γεννήτριες που λειτουργούν με εναλλακτικές μορφές ενέργειας.

10.7.1.8.Πολιτική Περιστατικών Ασφάλειας

Σώμα Πολιτικής

Η επιχείρηση διαθέτει στο προσωπικό της, στους εξωτερικούς συνεργάτες της, στους πελάτες της και στους προμηθευτές της ένα σύνολο εφαρμογών και υπηρεσιών με στόχο την σύγχρονη, αυτόματη και ευέλικτη λειτουργία των επιχειρησιακών διεργασιών. Είναι σημαντικό να υλοποιείται αποτελεσματική αναγνώριση, αξιολόγηση, επίλυση, τεκμηρίωση και αναφορά των περιστατικών ασφάλειας πληροφοριών, τα οποία προέρχονται από το εσωτερικό ή το εξωτερικό περιβάλλον της.

Πλαίσιο Περιστατικών Ασφάλειας Πληροφοριακών Συστημάτων και επικοινωνία τους

Πρέπει να είναι ορισμένο το πλαίσιο διαχείρισης περιστατικών ασφάλειας πληροφοριών μέσω του οποίου πρέπει να υπάρχει διαδικασία για τη διαχείριση περιστατικών ασφάλειας και Ομάδα διαχείρισης περιστατικών ασφάλειας πληροφοριών μαζί με ρόλους και αρμοδιότητες της (από εδώ και στο εξής θα αναφέρεται ως Ομάδα). Πρέπει να αναγράφεται η

κατηγοριοποίηση ανάλογα με την κρισιμότητα των εμπλεκόμενων πληροφοριακών συστημάτων, ενός περιστατικού Ασφάλειας Πληροφοριακού Συστήματος. Με βάση αυτό πρέπει να περιγράφεται η ενεργοποίηση εναλλακτικών λύσεων για την διασφάλισης της Επιχειρησιακής Συνέχειας. Πρέπει να υλοποιείται ενημέρωση χρηστών σχετικά με τα περιστατικά ασφάλειας και την αντίδραση που θα πρέπει να έχουν όσον αφορά την επικοινωνία αυτών με τις κατάλληλες οδηγίες.

Αξιολόγηση Περιστατικών Ασφάλειας Πληροφοριακών Συστημάτων και αντιμετώπισή τους

Σε περίπτωση που διαπιστωθεί κάποιο περιστατικό ασφάλειας πληροφοριών θα πρέπει να συγκροτείται η Ομάδα, να ενεργοποιηθεί το πλαίσιο αντιμετώπισης Περιστατικών Ασφάλειας Πληροφοριακών Συστημάτων και να συλλογή και ανάλυση όλων των σχετικών Πληροφοριών. Στην συνέχεια αξιολογείται αν πρόκειται για λανθασμένη ειδοποίηση (false alarm).

Μετά την επιβεβαίωσή του και τις επιχειρησιακές επιπτώσεις που έχει πρέπει να εξετάζεται η βαρύτητα των συνεπειών και το πλήθος και το είδος των πληροφοριών που επηρεάζονται.

Πρέπει να γίνει συλλογή και ανάλυση των δεδομένων τα οποία θα αποκαλύψουν την αιτία έτσι ώστε να μπορέσει η αρμόδια ομάδα να το ενεργήσει με τον κατάλληλο τρόπο για την αντιμετώπιση του κινδύνου. Το περιστατικό πρέπει να απομονωθεί, να αντιμετωπιστεί, και να γίνει επαναφορά της ορθής λειτουργίας.

Η ομάδα πρέπει να εξετάζει το κάθε περιστατικό ανάλογα με την κατηγοριοποίηση της κρισιμότητας των εμπλεκόμενων πληροφοριακών αγαθών αλλά και με τις επιπτώσεις που θα έχει η καθυστέρηση του χρόνου επαναφοράς στην ορθή λειτουργία. Η τελική έγκριση της απώλειας της διαθεσιμότητας δίνεται από την Διοίκηση της Επιχείρησης. Στο τέλος πρέπει να υλοποιείται από την ομάδα πλήρης τεκμηρίωση.

Διερεύνηση των Περιστατικών Ασφάλειας Πληροφοριακών Συστημάτων (Forensics)

Η δικανική ανάλυση (forensics) είναι αναγκαία για υπάρξει εικόνα όσον αφορά το περιστατικό. Μέσω αυτής διερευνούνται αποδεικτικά στοιχεία για την πηγή προέλευσης με σκοπό τις νομικές ενέργειες. Η Ομάδα πρέπει να αποφασίσει το χρόνο, το είδος, το επίπεδο της έρευνας και να ελέγξει τους εμπλεκόμενους πόρους, με βάση το κανονιστικό πλαίσιο.

Η συλλογή αποδεικτικών στοιχείων πρέπει να γίνεται με έγκυρες τεχνικές και εργαλεία τεχνολογίας, πρέπει να έχει πλήρη καταγραφή όλων των βημάτων ανάλυσης στοιχεία και πρέπει να συμμορφώνεται με όλες τις κανονιστικές απαιτήσεις ώστε τα στοιχεία να είναι αποδεκτά σε πειθαρχικές ή δικαστικές διαδικασίες. Η συλλογή πάντα θα γίνεται με την εμπλοκή του Νομικού τμήματος της Επιχείρησης.

Πρέπει να δημιουργηθεί ένα ακριβές αντίγραφο των αποδεικτικών στοιχείων (image) και οποιαδήποτε ανάλυση πρέπει να γίνει στο αντίγραφο αυτό και όχι στο πρωτότυπο (καθώς η ανάλυση των αρχικών δεδομένων μπορεί ακούσια να τα αλλοιώσει ή να τα καταστρέψει).

Πρέπει να τηρείται η αρχή της αλληλουχίας τεκμηρίωσης στοιχείων (chain of custody).

10.7.1.9.Πολιτική Ασφάλειας Πρόσβασης Χρηστών

Σώμα Πολιτικής

Η επιχείρηση διαθέτει στο προσωπικό της, στους εξωτερικούς συνεργάτες της, στους πελάτες της και στους προμηθευτές της ένα σύνολο εφαρμογών και υπηρεσιών με στόχο την σύγχρονη, αυτόματη και ευέλικτη λειτουργία των επιχειρησιακών διεργασιών. Για να μπορέσει να διασφαλιστεί η Εμπιστευτικότητα, η Ακεραιότητα και η Εμπιστευτικότητα περιγράφονται οι βασικοί κανόνες που πρέπει να ακολουθούνται έτσι ώστε να υπάρχει ορθή διαχείρισης της πρόσβασης των χρηστών στα πληροφοριακά συστήματα, στις υπηρεσίες και στην πληροφοριακή υποδομή.

Τα παραπάνω βασίζονται σε αρχές όπως:

- Ανάγκης της γνώσης «need-to-know»: Μέσω αυτής η γνώση της πληροφορίας αφορά στα πρόσωπα τα οποία έχουν την αρμοδιότητα και τα καθήκοντα να την γνωρίζουν.
- Ανάγκης της Χρήσης «need-to-use»: Μέσω αυτής χειρισμός της πληροφορίας αφορά στα πρόσωπα τα οποία έχουν την αρμοδιότητα και τα καθήκοντα να την να τον υλοποιούν.
- Ανάγκη της απόδοσης ελαχίστων προνομίων.

Επίσης η πρόσβαση στην πληροφορία επηρεάζεται από την διαβάθμισή της και την ανάγκη της διατήρησής της.

Πρέπει να επιτυγχάνεται ο έλεγχος πρόσβασης των χρηστών στην πληροφορία μέσω του επιχειρησιακού τους ρόλου (business role). Επίσης πρέπει να υπάρχει διαχωρισμός καθηκόντων (SoD), πρέπει να υπάρχει ονοματισμένη πρόσβαση, πρέπει να υπάρχει διαχείριση χρηστών και τμήμα υποστήριξής τους και πρέπει να γίνεται έλεγχος πρόσβασης χρηστών αλλά και των δικαιωμάτων πρόσβασής τους περιοδικά.

Πρόσβαση Χρηστών

Κάθε πληροφοριακό σύστημα είναι διαβαθμισμένο από την Επιχείρηση με βάση τους χρόνους ανάκτησης της από την περίπτωση καταστροφής (RTO). Η Επιχείρηση πρέπει να ορίζει έναν ιδιοκτήτη (υπεύθυνος επεξεργασίας) για την κάθε εφαρμογή. Το τμήμα Πληροφορικής της Επιχείρησης (υπεύθυνος εκτέλεσης) και οι δραστηριότητες που υλοποιεί είναι πάντοτε με την έγκριση του Ιδιοκτήτη όπως και η πρόσβαση χρηστών. Οι χρήστες διακρίνονται σε εσωτερικούς χρήστες, σε εξωτερικούς συνεργάτες και σε τρίτους. Απλές προσβάσεις αλλά και προνομιακές μπορούν να έχουν όλοι οι χρήστες εκτός από τους τρίτους.

Η πρόσβαση των χρηστών γίνεται είτε από το εσωτερικό Δίκτυο της Επιχείρησης είτε απομακρυσμένα με την χρήση πιστοποιητικών (πχ vpn). Για κάθε χρήστη υπάρχει ένα αναγνωριστικό ανά πληροφοριακό σύστημα (username) και πρέπει να είναι μοναδικά και προσωπικά (δεν δανείζονται).

Αυθεντικοποίηση χρηστών επιτυγχάνεται τουλάχιστον σε ένα από τα παρακάτω επίπεδα. Τα επίπεδα αυτά είναι LDAP ενδοδικτύου, Βάσης Δεδομένων, Λειτουργικού Συστήματος,

Εφαρμογής ή και Network Level Authentication. Οι προσβάσεις χρηστών πρέπει να καραγράφονται.

Ρόλοι Πρόσβασης Χρηστών

Για κάθε εφαρμογή θα πρέπει να υπάρχουν δημιουργημένοι ρόλοι οι οποίοι θα ορίζουν τις λειτουργίες που πρέπει να υλοποιούνται από έναν χρήστη με βάση τις αρμοδιότητές του στις Επιχείρηση.

Διαχείριση Πρόσβασης Χρηστών (απλών & προνομιακών)

Η Διαχείριση Ρόλων και Χρηστών για κάθε εφαρμογή και πληροφοριακό Σύστημα ή Υπηρεσία υλοποιείται κεντρικά από το τμήμα Πληροφορικής της Επιχείρησης. Για την καταγραφή των αιτημάτων και για την διατήρηση των εγκρίσεων των ιδιοκτητών Εφαρμογών (Owners) πρέπει να υπάρχει πληροφοριακό σύστημα που να διατηρεί τα αιτήματα πρόσβασης και να αυτοματοποιεί την διαδικασία με ταυτόχρονη δυνατότητα στατιστικής παρακολούθησής τους.

Για τη διαχείριση των αρμοδιοτήτων ενός λογαριασμού πρόσβασης χρήστη (δημιουργία, μεταβολή, διαγραφή) πρέπει να αιτείται ψηφιακά ο χρήστης την πρόσβαση του σε εφαρμογή και σε ρόλους αυτής και να υπάρχει μία ακολουθία εγκρίσεων με χρήση ψηφιακών υπογραφών. Πρέπει να υπάρχει για κάθε αίτημα η τελική έγκριση από τον ιδιοκτήτη της Εφαρμογής. Για τις Ψηφιακές Υπηρεσίες όπως το ηλεκτρονικό ταχυδρομείο και το διαδίκτυο ιδιοκτήτης είναι ο Προϊστάμενος του τμήματος Πληροφορικής της Επιχείρησης. Η υλοποίηση κάθε αιτήματος πρόσβασης γίνεται από τον αρμόδιο γραφείο Διαχείρισης Χρηστών του Τμήματος Πληροφορικής.

Σε περίπτωση τερματισμού απασχόλησης εργαζομένου η συνεργάτη της Επιχείρησης, η αίτηση για απενεργοποίηση λογαριασμού πρέπει να γίνεται έγκαιρα και να υλοποιείται ανάκληση δικαιωμάτων.

Στους προνομιακούς χρήστες υπάρχει πλέον των παραπάνω πιο μεγάλη παρακολούθηση (διαχειριστές των εφαρμογών, των λειτουργικών συστημάτων, των υπηρεσιών, των δικτυακών συσκευών και των πληροφοριακών συστημάτων ασφαλείας).

Κωδικοί Πρόσβασης Χρηστών

Οι κωδικοί πρόσβασης χρηστών πρέπει να έχουν μήκος και πολυπλοκότητα με βάση τις βέλτιστες παγκόσμιες πρακτικές. Η εφαρμογή πρέπει να ζητάει αυτόματα την αλλαγή τους σε κωδικούς πρόσβασης που επιθυμεί ο χρήστης κατά την αρχική σύνδεση και μόνο εφόσον έχουν δώσει ορθά τον αρχικό κωδικό.

Οι κωδικοί πρόσβασης είναι προσωπικό δεδομένο και πρέπει να διατηρούνται σε κρυπτογραφημένη μορφή τόσο στην υποδομή αλλά κατά την μεταφορά τους στο δίκτυο. Αυθεντικοποίηση δύο παραγόντων πρέπει να έχουν οι διαχειριστές.

10.7.1.10.Πολιτική Ασφάλειας Προστασίας από Κακόβουλο Λογισμικό

Σώμα Πολιτικής

Δικλείδες Ασφαλείας Προστασίας από Κακόβουλο Λογισμικό

Πρέπει για όλα τα πληροφοριακά συστήματα που ανήκουν στην Επιχείρηση, να λειτουργεί ενημερωμένο λογισμικό προστασίας από κακόβουλο λογισμικό.

Υποδομή Προστασίας από Κακόβουλο Λογισμικό

Πρέπει να υπάρχει προστασία στα σημεία εξωτερικής περιμέτρου και σε όλα τα σημεία εισόδου στο εσωτερικό δίκτυο της επιχείρησης με τείχη προστασίας επόμενης γενιάς που θα περιλαμβάνουν συστήματα ανίχνευσης και αποτροπής εισβολών. Επιπλέον πρέπει να υπάρχει προστασία στους τερματικούς σταθμούς εργασίας καθώς και πρόσβασης στο διαδίκτυο και στην χρήση του ηλεκτρονικού ταχυδρομείου. Αυτοί οι μηχανισμοί πρέπει να ανιχνεύουν το περιεχόμενο του κακόβουλου λογισμικού τουλάχιστον στο ηλεκτρονικό ταχυδρομείο (SMTP), στο διαδίκτυο (HTTP/HTTPS) και στο πρωτόκολλο μεταφοράς αρχείων (SFTP).

Για την εξειδικευμένη αυτή υποδομή προστασίας από κακόβουλο λογισμικό πρέπει να υπάρχει κεντρική διαχείριση και καταγραφή των περιστατικών.

Έλεγχος για Ανίχνευση Κακόβουλου Λογισμικού

Οι μηχανισμοί προστασίας από κακόβουλο λογισμικό αφορούν οποιοδήποτε αρχείο μεταφέρεται ηλεκτρονικά (είτε είναι εισερχόμενο ή εξερχόμενο) το οποίο πρέπει να ελέγχεται για την ύπαρξη κακόβουλου λογισμικού. Όλα τα πληροφοριακά συστήματα πρέπει να ελέγχονται από το λογισμικό προστασίας από κακόβουλο λογισμικό σε τακτά χρονικά διαστήματα.

Υποχρεώσεις υπαλλήλων και συνεργατών με την πολιτική

Όλοι οι εργαζόμενοι πρέπει να ενημερώνονται για τις αρχές της παρούσας πολιτική. ενημέρωση σε θέματα ασφάλειας που σχετίζονται με το κακόβουλο λογισμικό, ώστε να αυξηθεί η ευαισθητοποίησή τους για τους κινδύνους που συνδέονται με το κακόβουλο λογισμικό και τα μέτρα και πρακτικές που πρέπει να ακολουθούνται για την αντιμετώπισή του και την προστασία των εταιρικών πληροφοριών. Δεν επιτρέπεται η απεγκατάσταση ή τροποποίηση των ρυθμίσεων του λογισμικού προστασίας από κακόβουλο λογισμικό, και η χρήση, εγκατάσταση ή αντιγραφή στα πληροφοριακά συστήματα λογισμικού που προέρχεται από μη αξιόπιστες πηγές (π.χ. διαδίκτυο). Οι λήψεις που πραγματοποιούνται από το Διαδίκτυο για τεχνικούς λόγους πρέπει να γίνονται μόνο από τις επίσημες ιστοσελίδες των προμηθευτών. Επίσης θα πρέπει να αποφεύγεται το άνοιγμα επισυναπτόμενων αρχείων σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστες πηγές.

Διαχείριση Περιστατικών Ασφάλειας που Σχετίζονται με Κακόβουλο Λογισμικό

Αναφορά Περιστατικών Ασφάλειας

Οι εργαζόμενοι πρέπει να είναι σε εγρήγορση για την ανίχνευση συμβάντων ασφάλειας που σχετίζονται με κακόβουλο λογισμικό. Εάν υπάρχει υπόνοια ή έχει αναγνωριστεί μόλυνση κάποιου συστήματος ή υποδομής της Επιχείρησης από κακόβουλο λογισμικό (π.χ. περίεργη συμπεριφορά κάποιου συστήματος ή εμφάνιση μηνυμάτων στην οθόνη), θα πρέπει να αναφέρεται άμεσα στο τμήμα Ασφάλειας Πληροφοριακών Συστημάτων.

10.7.1.11.Πολιτική Ασφάλειας Νέων ΠΣ

Σώμα Πολιτικής

Κάθε νέα απαίτηση της Επιχείρησης που αφορά την προμήθειας νέου πληροφοριακού συστήματος, την ανάγκη τροποποίησης ή την αντικατάσταση υπάρχοντος με νέο μπορεί να υλοποιηθεί με τους ακόλουθους τρόποι προμήθειάς του: α) η αγορά του εφόσον αφορά εμπορικό προϊόν - έτοιμη λύση β) η ανάπτυξή του εντός της Επιχείρησης από εξειδικευμένο τεχνικό προσωπικό του τμήματος Πληροφοριακής, γ) η ανάθεσης της ανάπτυξης τους από εξωτερικό συνεργάτη προμηθευτή δ) η προμήθεια ανοικτού λογισμικού η λογισμικού ανοικτού κώδικα το οποίο θα υποστηρίζεται από το τμήμα Πληροφορικής της Επιχείρησης.

Ρόλοι Δεδομένων τα νέα Πληροφοριακό Σύστημα

Η Επιχείρηση θα πρέπει πριν την προμήθειά του να ορίσει ιδιοκτήτη. Η μελέτη και η ανάλυση απαιτήσεων θα γίνουν σε συνεργασία του ιδιοκτήτη του και του τμήματος πληροφορικής της Επιχείρησης. Οι παραπάνω σε συνεργασία με το τμήμα Νομικών Υπηρεσιών, πρέπει να διασφαλίζουν τη συμμόρφωση με το κανονιστικό πλαίσιο για κάθε νέο πληροφοριακό σύστημα. Επιπλέον πρέπει να υλοποιούν μελέτη ανάγκης ασφαλιστικής κάλυψης μέσω ειδικών συμβολαίων για το νέο πληροφοριακό σύστημα έτσι ώστε να καλυφθεί η επικινδυνότητα του σχετικά με την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του.

Περιβάλλον νέου Πληροφοριακού Συστήματος

Κάθε νέο πληροφοριακό σύστημα πρέπει να υλοποιείται σε περιβάλλον ανάπτυξης, να δοκιμάζεται σε ένα αντίγραφο περιβάλλον της ανάπτυξης που θα αφορά το περιβάλλον ελέγχου και θα περιέχει δεδομένα δοκιμών (data masking) και πρέπει να εντάσσεται σε παραγωγική λειτουργία σε ένα περιβάλλον αντίγραφο του περιβάλλοντος δοκιμών όσον αφορά την λειτουργικότητά του μετά από ανάλυση επικινδυνότητα και έγκρισης από τον ιδιοκτήτη του Πληροφοριακού Συστήματος.

Τύποι χρηστών νέου Πληροφοριακού Συστήματος

Κάθε νέο πληροφοριακό σύστημα έχει τους ακόλουθους τύπους χρηστών για τους οποίους θα πρέπει να υπάρχει διαχωρισμός όσον αφορά τους συγκρουόμενους ρόλους (SoD):

Επιχειρησιακούς Χρήστες (Business Users), Επιχειρησιακοί Χρήστες Δοκιμών (User Acceptance Test Users), Διαχειριστές Υποδομών (Administrators – System – DB – Network – Developers – Security – Authorization – Auditors).

Κύκλος Ζωής νέου Πληροφοριακού Συστήματος

Ιδέα – απαίτηση - έρευνα

Σε αυτή τη φάση , εκφράζεται η ανάγκη για την απόκτηση / ανάπτυξη ενός πληροφοριακού συστήματος ή εφαρμογής. Πρέπει να οριστεί η φύση του συστήματος που απαιτείται και ο λόγος για τον οποίο απαιτείται. Οι προτάσεις για απόκτηση/ ανάπτυξη ενός πληροφοριακού συστήματος πρέπει να περιλαμβάνουν περιγραφή της επιχειρησιακής ανάγκης καθώς και τα οφέλη που πρόκειται να αποκομίσει η Επιχείρηση. Σε αυτή τη φάση πρέπει να γίνει από το τμήμα Ασφάλειας Πληροφοριακών Συστημάτων μία αρχική αξιολόγηση ανάλυσης επικινδυνότητας, όπου θα καθοριστεί το περιβάλλον στο οποίο θα λειτουργήσει το επικείμενο σύστημα και τυχόν αδυναμίες ώστε να γίνει η πρώτη εκτίμηση των απαιτήσεων του συστήματος. Σε αυτή την φάση ορίζεται ο ιδιοκτήτης του νέου πληροφοριακού συστήματος. Τα αποτελέσματά της ανάλυσης επικινδυνότητας θα χρησιμοποιηθούν για την επιλογή των δικλείδων ασφαλείας και θα λάβουν την έγκριση και την αποδοχή του ρίσκου από τον ιδιοκτήτη του και από την Διοίκηση της Επιχείρησης.

Στην συνέχεια γίνεται έρευνα για το θεματικό πεδίο που μπορεί να καλύψει την λειτουργικότητα που θα υλοποιεί το νέο πληροφοριακό σύστημα. Η έρευνα γίνεται από το τμήμα πληροφορικής με την συνεπικουρία του Ιδιοκτήτη και του τμήματος Ασφάλειας Πληροφοριακών Συστημάτων. Τα αποτελέσματα της θα αξιολογηθούν και μετά από την μελέτη κόστους οφέλους θα εγκριθεί από τους παραπάνω ρόλους ο τρόπος που θα υλοποιηθεί το νέο σύστημα.

- Καθορισμός των επιχειρησιακών (λειτουργικών), τεχνικών και κανονιστικών απαιτήσεων.
- Καθορισμός των απαιτήσεων ασφάλειας με βάση τον τύπο, την κρισιμότητα και την αναμενόμενη χρήση του συστήματος. Σε αυτή την περίπτωση πρέπει να λαμβάνονται υπόψη διεθνή πρότυπα τα οποία θέτουν συγκεκριμένα κριτήρια αξιολόγησης ασφάλειας (π.χ. ISO/IEC 15408-1:2009) καθώς και κριτήρια τα οποία προέρχονται από αξιόπιστες πηγές ή/και βασίζονται σε κοινά αποδεκτές πρακτικές και μεθόδους (π.χ. το NSA).
- Συνδυασμός όλων των παραπάνω στοιχείων για την κατάρτιση μιας ενιαίας πρότασης (Πρόταση προς Έγκριση) και υποβολή στο αρμόδιο κατά περίπτωση Εγκριτικό Όργανο της Επιχείρησης.

Σχεδιασμός

Κατά την φάση του σχεδιασμού του νέου Πληροφοριακού Συστήματος πέραν της αντιμετώπιση των λειτουργικών απαιτήσεων πρέπει να ακολουθούνται οι αρχές:

πολλαπλής προστασίας σε όλα τα επίπεδα μέσω κατάλληλων ρυθμίσεων (defense in depth), πρόσβασης μόνο σε εξουσιοδοτημένους χρήστες, χρήση διαχωρισμού συγκρούσεων και διαχωρισμού των καθηκόντων (SoD), καταγραφής όλων των λειτουργιών που έχουν σχέση με την ασφάλεια ΠΣ, προστασίας της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας των Πληροφοριών, χρήσης των αρχών των ελαχίστων προνομίων, του ελαχίστου της γνώσης και της διατήρησης μόνο των δεδομένων που είναι απαραίτητα για τον σκοπό για τον οποίο υλοποιείται το σύστημα, συμμόρφωσης του Πληροφοριακού Συστήματος με ότι αφορά το νομικό και κανονιστικό πλαίσιο, διασφάλισης της αξιοπιστίας των διεργασιών και των συναλλαγών χωρίς την χρήση της απόκρυψης, χρήσης δικλείδων ασφαλείας σε όλα τα τεχνικά επίπεδα του Πληροφοριακού Συστήματος (Λειτουργικού Συστήματος, Βάσης Δεδομένων, Διακομιστή, Εφαρμογής, Επιπέδου Παρουσίασης, Δικτύου) με βάση το πλαίσιο Ασφάλειας της Επιχείρησης και των βέλτιστων πρακτικών, χρήσης αμυντικού Προγραμματισμού και παραμετροποίησης για την αντιμετώπιση του ανθρώπινου λάθους καθώς και χρήση ελέγχων ακεραιότητας για την αποφυγή αλλοίωσης δεδομένων.

Υλοποίηση

Για την υλοποίηση πρέπει να δημιουργείται ομάδα που θα αποτελείται από το Τμήμα Πληροφορικής, το τμήμα Ανάπτυξης, το τμήμα Ασφάλειας Πληροφοριακών Συστημάτων και τον Ιδιοκτήτη. Στην υλοποίηση περιλαμβάνονται: η διαχείριση του έργου (Project Management, Διαγράμματα Περιπτώσεων Χρήσης), η προμήθεια/ανάπτυξη και η παραμετροποίηση του Συστήματος, η τεκμηρίωσή του (ανάπτυξης, λειτουργίας & χρήσης, διαχείρισης), δοκιμές για την ορθότητα των λειτουργικών απαιτήσεων.

Έλεγχος

Σε αυτή την φάση γίνεται ο έλεγχος της ορθής παραγωγικής λειτουργίας πριν την έναρξή της. Λαμβάνονται υπόψη όλοι οι παράγοντες που συνεργάζονται με το νέο πληροφοριακό σύστημα. Επίσης υλοποιούνται δοκιμές παρείσδυσης και ανάλυση επικινδυνότητας.

Παραγωγική Λειτουργία, Συντήρηση και τροποποιήσεις

Μετά την ολοκλήρωση του ελέγχου μπορεί το σύστημα να ξεκινήσει να λειτουργεί παραγωγικά. Σε αυτή την φάση ενεργοποιούνται τα αντίγραφα ασφαλείας και ακολουθούνται όλες οι οδηγίες των εγγράφων Σχεδίου Ανάκαμψης από Καταστροφή (DRP), επιχειρησιακής συνέχειας καθώς και όλα τα έγγραφα λειτουργίας και διαχείρισης της εφαρμογής.

Απομάκρυνση Πληροφοριακού Συστήματος

Εφόσον ένα πληροφοριακό σύστημα πρόκειται να καταργηθεί ή να αντικατασταθεί πρέπει να υπάρχει διασφάλιση της Επιχείρησης από το τμήμα Νομικών ότι έχουν αντιμετωπιστεί όσα αναφέρονται για το νομικό, κανονιστικό και φορολογικό πλαίσιο (πχ διατήρηση τιμολογίων).

10.7.1.12.Πολιτική Ασφάλειας Φορητών Συσκευών

Σώμα Πολιτικής

Παροχή Εταιρικών Φορητών Συσκευών

Για την παροχή και χρήση φορητής συσκευής από το προσωπικό της Επιχείρησης γίνεται εκτίμηση και αιτιολόγηση από τον εκάστοτε προϊστάμενο.

Χρήση προσωπικών Φορητών Συσκευών από μισθωτούς ή εξωτερικούς συνεργάτες

Η επιχείρηση επιτρέπει την χρήση προσωπικών φορητών συσκευών σε υπαλλήλους τις και σε εξωτερικούς συνεργάτες, για την εκπλήρωση των επαγγελματικών τους υποχρεώσεων προς αυτή, εφόσον εναρμονίζονται με το πλαίσιο Ασφάλειας της Επιχείρησης.

Υπευθυνότητα Υπαλλήλων

Η χρήση των εταιρικών φορητών συσκευών επιτρέπεται αποκλειστικά και μόνο στους υπαλλήλους που το έχουν αιτηθεί οι οποίοι πρέπει να προστατεύουν τις εταιρικές φορητές συσκευές που τους έχουν παρασχεθεί καθ' όλη τη διάρκεια της περιόδου που τις χειρίζονται.

Αρχείο Εταιρικών Φορητών Συσκευών & προσωπικών Φορητών Συσκευών.

Εταιρικές και προσωπικές φορητές συσκευές

Όλες οι εταιρικές συσκευές που έχουν δοθεί σε εργαζομένους πρέπει να καταχωρούνται σε ηλεκτρονικό αρχείο.

Όλες οι προσωπικές φορητές συσκευές που έχουν αιτηθεί εργαζόμενοι να χρησιμοποιούν για την πρόσβαση σε εφαρμογές της Επιχείρησης πρέπει να καταχωρούνται σε ηλεκτρονικό αρχείο.

Ενημέρωση εμπλεκομένων σε Θέματα Ασφάλειας Φορητών Συσκευών

Πρέπει να ενημερώνονται οι χρήστες των φορητών συσκευών για τους κινδύνους που υπάρχουν από την χρήση των συσκευών. Η ενημέρωση αυτή είναι μέρος του προγράμματος εκπαίδευσης και ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών και θα πρέπει να αναθεωρείται τακτικά ώστε να αντικατοπτρίζει τις συνεχώς αναδυόμενες απειλές που σχετίζονται με τις φορητές συσκευές.

Δικαιώματα Επιχείρησης σχετικά με τις φορητές συσκευές

Η επιχείρηση έχει το δικαίωμα να διαχειριστεί την κάθε φορητή συσκευή (εταιρική ή προσωπική που χρησιμοποιείται για διαχείριση εταιρικής πληροφορίας) με λογισμικό MDM (Mobile Device Managmet) για να προστατεύσει την εταιρική πληροφορία που είναι αποθηκευμένη σε αυτή.

Στην περίπτωση που οι εμπλεκόμενοι δεν συμμορφώνονται με το πλαίσιο ασφάλειας της Επιχείρησης θα τους αφαιρείται η πρόσβαση προς τα Πληροφοριακά της συστήματα.

Οι Εμπλεκόμενοι πρέπει να αναφέρουν άμεσα στο τμήμα που διατηρεί των ηλεκτρονικό μητρώο φορητών συσκευών (τμήμα Ασφάλειας Πληροφοριακών Συστημάτων) την απώλεια ή την όποια δυσλειτουργία της συσκευής. Το γεγονός θα πρέπει να διατηρείται ως περιστατικό ασφάλειας.

Πριν την επιστροφή των συσκευών, οι εργαζόμενοι ευθύνονται για τη διαγραφή προσωπικών δεδομένων από τη συσκευή. θα πρέπει να γίνεται χρήση MDM λύσης.

Η επιχείρηση διατηρεί το δικαίωμα να εφαρμόζει στις φορητές συσκευές μηχανισμούς αυθεντικοποίησης (χρήση βιομετρικών, πολύπλοκους κωδικούς πρόσβασης που θα αλλάζουν συχνά, two factor authentication).

10.7.1.13.Πολιτική Ασφάλειας Μεταβολών ΠΣ

Σώμα Πολιτικής

Βασικά σημεία αλλαγών πληροφοριακών συστημάτων

Αλλαγές (τροποποίηση/μεταβολή, διαγραφή_ που άπτονται στην παρούσα πολιτική αφορούν τα συστήματα, τις εφαρμογές, το λογισμικό τις υποδομές των πληροφοριακών συστημάτων της Επιχείρησης και τις διαδικασίες. Για κάθε αλλαγή πρέπει η επιχείρηση να διατηρεί μητρώο μεταβολών. Θα αναγράφονται οι ημερομηνίες υλοποίησης της μεταβολής, δοκιμής της νέας υλοποίησης, μετακίνησή της στο παραγωγικό περιβάλλον με την έγκριση του ιδιοκτήτη της εφαρμογής (ψηφιακή υπογραφή).

Σημεία που πρέπει να ληφθούν υπόψη σε μία αλλαγή

Σημεία που πρέπει να λαμβάνονται υπόψη σε μία αλλαγή κατά την τελική της μετάπτωση στην παραγωγή είναι οι ώρες αιχμής, το σχέδιο επαναφοράς, οι αλληλεξαρτήσεις και οι διασυνδέσεις με άλλα συστήματα έτσι ώστε η υλοποίηση να μη θέσει σε κίνδυνο την Επιχειρησιακή Συνέχεια.

11. Αναφορές

- **Wikipedia** (2014). Software Development Process (risk analysis before development on spiral model) https://en.wikipedia.org/wiki/Software_development_process
- **Wikipedia** (2014). Oracle Database SGA & Oracle Advanced Security Features https://en.wikipedia.org/wiki/Oracle_Database
- **Oracle (2014)**. Transparent Data Encryption (Data at Rest) http://www.oracle.com/technetwork/database/options/advanced-security/index-099011.html
- **wordpress.com**. Steps to encrypt table space in 12c TDE method https://oracledb101.wordpress.com/2014/02/10/setting-up-tde-with-12c-pluggable-database/
- **Πανεπιστήμιο Μακεδονίας(2012).** Διπλωματική εργασία ανάλυσης επικινδυνότητας Τηλειατρικού ΠΣ. http://www.icte.uowm.gr/uploads/thesis/dipl_ergasia_am14.pdf
- **Angularjs.org** (2016). Angular security: Αναφορές σε σημεία για μία από τις τεχνολογίες που έχει επιλεγεί για την ανάπτυξη της εφαρμογής https://docs.angularjs.org/guide/security
- **Free e-books library** (2010) Peter Mularien - Secure your web applications against malicious intruders with this easy to follow practical guide
- ftp://ftp.heanet.ie/mirrors/sourceforge/p/ph/phpusersystem/shareDocs/ebook_1847199747_Spring_Security_3.pdf
- **HP.** Ticketing system HP Service Desk http://www8.hp.com/us/en/software-solutions/service-desk/
- **Capptera.** Top Identity Management Systems **www.capterra.com/identity-management-software**
- **PortalGuard** (http://www.capterra.com/identity-management-software/spotlight/136315/PortalGuard/PistolStar)
    - **Nervepoint** (http://www.capterra.com/identity-management-software/spotlight/134859/Access%20Manager/Nervepoint%20Technologies)

- **IDM365**
  (http://www.capterra.com/identity-management-software/spotlight/143212/IDM365/ITMC%20Soft)
- **OpenIDM**
  (http://www.capterra.com/identity-management-software/spotlight/131061/OpenIDM/ForgeRock)
- **Adaxes για active directory** (http://www.capterra.com/identity-management-software/spotlight/104322/Adaxes/Softerra)

- **lansa Workflow System**. Nervepoint Μέσω αυτού επιτρέπεται η ρύθμιση της πρόσβασης σε μία ή περισσότερες από τις οθόνες εφαρμογής / μορφές έτσι ώστε ο χρήστης έχει εύκολη πρόσβαση σε ό, τι χρειάζονται για την τρέχουσα ροή εργασιών (http://blog.lansa.com/application-modernization/workflow/selecting-workflow-management-system-company)
- **Reporting & MIS** System (όπως για παράδειγμα το Qlikview & Business Objects). http://www.qvh.gr/amea/ http://go.sap.com/greece/solution/platform-technology/analytics/business-intelligence-bi.html?campaigncode=CRM-GR16-3DI-PPC_ITAC&gclid=CIGmnfrls80CFVIZGQod5lEO9A&gclsrc=ds

- **MediaWiki. Wiki** System https://www.mediawiki.org/wiki/MediaWiki
- **WikiPedia - SIEM** https://en.wikipedia.org/wiki/Security_information_and_event_management
- **Symantec WDE** https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/3000/DOC3592/en_US/pgpWDEwin_1011_quickstart_en.pdf?__gda__=1466661302_9d9af14b86f609fb11a95dc2329e6458